

HikCentral Professional Web Client

User Manual

Legal Information

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (***https://www.hikvision.com/***).
Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

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.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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 MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Contents

Chapter 1 About This Document 1
1.1 Introduction 1
1.2 Recommended Running Environment 2
1.3 Symbol Conventions 2
Chapter 2 Login 4
2.1 First Time Login 4
2.1.1 Login for First Time for Admin User 4
2.1.2 First Time Login for Normal User 5
2.2 Login via Web Client (Administrator) 6
2.3 Login via Web Client (Employee) 7
2.4 Change Password for Reset User 8
2.5 Forgot Password 9
Chapter 3 Download Mobile Client 12
Chapter 4 Web Control 13
Chapter 5 Home Page Overview 14
5.1 Customize Navigation Bar 18
5.2 View Digital Dashboard 19
5.3 Customize Preset Workbench 20
5.4 Customize Personal Workbench 21
Chapter 6 Getting Started 23
Chapter 7 Application Summary 24
7.1 Flow Chart of Video Security 25
7.2 Flow Chart of Intelligent Analysis Report in Retail/Supermarket Scenario 27
7.3 Flow Chart of Intelligent Analysis Report in Public Scenario 29
7.4 Flow Chart of On-Board Monitoring 31
7.5 Flow Chart of Parking Lot Management 32

7.6 Flow Chart of Parking Fee Collection 34
7.7 Flow Chart of Parking Guidance Configuration 36
7.8 Flow Chart of Door Access Control 37
7.9 Flow Chart of Floor Access Control 40
7.10 Flow Chart of Visitor Management 43
7.11 Flow Chart of Time and Attendance 44
7.12 Flow Chart of Video Intercom 46
7.13 Flow Chart of Alarm Detection 48
7.14 Flow Chart of Digital Signage Management 49
7.15 Flow Chart of Interactive Flat Panel Management 50
7.16 Flow Chart of Patrol Management 52
Chapter 8 License Management 54
8.1 Activate License - Online 54
8.2 Activate License - Offline 56
8.3 Update License - Online 59
8.4 Update License - Offline 60
8.5 Deactivate License - Online 62
8.6 Deactivate License - Offline 63
8.7 View License Details 65
8.8 Set SSP Expiration Prompt 67
Chapter 9 Device and Server Management 69
9.1 Create Password for Inactive Device(s) 69
9.2 Edit Online Device's Network Information 70
9.3 Manage Encoding Device 71
9.3.1 Add Detected Online Encoding Devices 71
9.3.2 Add Encoding Device by IP Address/Domain 80
9.3.3 Add Encoding Devices by IP Segment 85
9.3.4 Add Encoding Devices by Port Segment 89

9.3.5 Add Encoding Device by Hik-Connect DDNS 93
9.3.6 Add Encoding Device by Device ID 97
9.3.7 Add Encoding Devices by Device ID Segment 100
9.3.8 Add Encoding Devices in a Batch 103
9.3.9 Add Encoding Device from the Site on Hik-Partner Pro 106
9.3.10 Limit Bandwidth for Video Downloading 111
9.3.11 Set N+1 Hot Spare for NVR 112
9.3.12 Add and Manage Applications 113
9.4 Manage Access Control Device 115
9.4.1 Add Detected Online Access Control Devices 115
9.4.2 Add an Access Control Device by IP Address/Domain 121
9.4.3 Add Access Control Devices by IP Segment 123
9.4.4 Add an Access Control Device by Device ID 126
9.4.5 Add Access Control Devices by Device ID Segment 128
9.4.6 Add Access Control Devices in a Batch 130
9.4.7 Configure Device Parameters 132
9.4.8 Privacy Settings 149
9.5 Manage Elevator Control Device 150
9.5.1 Add Detected Online Elevator Control Devices 150
9.5.2 Add an Elevator Control Device by IP Address 155
9.5.3 Add Elevator Control Devices by IP Segment 157
9.5.4 Add Elevator Control Devices in a Batch 159
9.6 Manage Video Intercom Device 160
9.6.1 Add Detected Online Video Intercom Devices 161
9.6.2 Add a Video Intercom Device by IP Address 167
9.6.3 Add Video Intercom Devices in a Batch 170
9.7 Manage Visitor Terminals 172
9.7.1 Add Detected Online Visitor Terminals 172

9.7.2 Add Visitor Terminal by IP Address 177
9.7.3 Add Visitor Terminals by IP Segment 179
9.7.4 Add Visitor Terminals in a Batch 181
9.8 Manage Payment Terminal 182
9.8.1 Add Detected Online Payment Terminals 183
9.8.2 Add Payment Terminal by IP Address 187
9.8.3 Add Payment Terminal by IP Segment 189
9.8.4 Add Payment Terminals in a Batch 191
9.9 Manage On-Board Devices 192
9.9.1 Add Detected Online On-Board Devices 192
9.9.2 Add an On-Board Device by Device ID 198
9.9.3 Add On-Board Devices by Device ID Segment 200
9.9.4 Add On-Board Devices in a Batch 203
9.10 Add a Query Terminal 204
9.11 Add an Entrance/Exit Control Device 205
9.12 Manage Guidance Terminals 207
9.12.1 Add Detected Online Guidance Terminals 208
9.12.2 Add a Guidance Terminal by IP Address 212
9.12.3 Batch Add Guidance Terminals by IP Segment 214
9.12.4 Batch Add Guidance Terminals by Port Segment 216
9.12.5 Batch Add Guidance Terminals by Template 218
9.13 Add Display Screen 219
9.14 Add Under Vehicle Surveillance System 221
9.15 Manage Security Control Device 222
9.15.1 Add Detected Online Security Control Devices 223
9.15.2 Add Security Control Device by IP Address 227
9.15.3 Add Security Control Device by Hik-Connect DDNS 229
9.15.4 Add Security Control Devices by IP Segment 232

9.15.5 Add Security Control Devices by Port Segment 233
9.15.6 Add Security Control Device by Device ID 235
9.15.7 Add Security Control Device by Device ID Segment 237
9.15.8 Batch Add Security Control Devices 238
9.15.9 Add Security Control Device from the Site on Hik-Partner Pro 240
9.15.10 Add Security Control Device via Modbus Protocol 242
9.16 Manage Fire Protection Device 244
9.16.1 Add Fire Protection Device by IP Address 244
9.16.2 Add Fire Protection Device by IP Segment 245
9.16.3 Add Fire Protection Device by Device ID 247
9.16.4 Add Fire Protection Devices by ID Segment 249
9.16.5 Add Fire Protection Devices in a Batch 250
9.17 Manage Dock Station 251
9.17.1 Add Dock Station by IP Address 252
9.17.2 Add Dock Stations by IP Segment 253
9.17.3 Add Dock Stations by Port Segment 254
9.17.4 Batch Add Dock Stations 256
9.17.5 Add Dock Station Group 257
9.18 Manage Digital Signage Terminals 260
9.18.1 Add Digital Signage Terminal 260
9.18.2 Configure Device Display Settings 271
9.18.3 Configure Device Privacy Settings 273
9.18.4 Configure Device Parameters Remotely 274
9.18.5 Upgrade Old Device Firmware 278
9.19 Manage Interactive Flat Panel 279
9.19.1 Add Online Interactive Flat Panel 279
9.19.2 Add Interactive Flat Panel by Device Serial No. 280
9.19.3 Enable General Authentication Code 282

9.20 Manage Smart Wall 284
9.20.1 Add Decoding Device 284
9.20.2 Configure Cascade 293
9.20.3 Add Smart Wall 294
9.20.4 Link Decoding Output with Window 296
9.20.5 Set Default Stream Type for Cameras on Smart Wall 297
9.21 Manage IP Speakers 298
9.21.1 Add Detected Online IP Speakers 298
9.21.2 Add IP Speaker by Serial No. 302
9.21.3 Batch Add IP Speakers 304
9.22 Manage Security Inspection Devices 305
9.22.1 Add a Detected Online Security Inspection Device 305
9.22.2 Add Security Inspection Device by Device ID 307
9.22.3 Add Security Inspection Device by IP Address 309
9.23 Network Transmission Device Management 312
9.23.1 Add Detected Online Network Transmission Devices 312
9.23.2 Add Network Transmission Device by IP Address 316
9.23.3 Import Network Transmission Devices in a Batch 318
9.24 Upgrade Device Firmware 319
9.24.1 Upgrade Device Firmware via Current Web Client 320
9.24.2 Upgrade Device Firmware via Hik-Connect 321
9.24.3 Upgrade Device Firmware via FTP 322
9.25 Restore/Reset Device Password 323
9.25.1 Reset Device Password 323
9.25.2 Restore Device's Default Password 325
9.26 Manage Recording Server 326
9.26.1 Add pStor 326
9.26.2 Add Hybrid Storage Area Network 328

9.26.3 Add Network Video Recorder 330
9.26.4 Manage Cloud Storage Server 332
9.26.5 Add pStor Cluster Service 334
9.26.6 Set N+1 Hot Spare for Hybrid SAN 336
9.27 Manage Streaming Server 338
9.27.1 Input Certificate Information to Streaming Server 338
9.27.2 Add Streaming Server 339
9.28 Add DeepinMind Server 340
9.29 Manage Scanning Device 342
9.29.1 Add a Single Scanning Device 342
9.29.2 Batch Add Scanning Devices 343
9.30 Manage Remote Site 344
9.30.1 Add Remote Site by IP Address or Domain Name 344
9.30.2 Add Remote Site Registered to Central System 347
9.30.3 Add Remote Sites in a Batch 349
9.30.4 Back Up Remote Site's Database to Central System 351
9.30.5 Edit Remote Site 352
9.30.6 View Remote Site's Changes 353
Chapter 10 Area Management 356
10.1 Add Area 356
10.1.1 Add an Area for Current Site 356
10.1.2 Add Area for Remote Site 358
10.1.3 Customize Additional Information 360
10.2 Add Element to Area 360
10.2.1 Add Camera to Area for Current Site 361
10.2.2 Add Camera to Area for Remote Site 362
10.2.3 Add Door to Area for Current Site 364
10.2.4 Add Elevator to Area for Current Site 366

10.2.5 Add Vehicle to Area for Current Site 367
10.2.6 Add Security Radar to Area for Current Site 369
10.2.7 Add Alarm Input to Area for Current Site 370
10.2.8 Add Alarm Output to Area for Current Site 372
10.2.9 Add UVSS to Area for Current Site 373
10.2.10 Add Digital Signage Screen to Area for Current Site 374
10.2.11 Add Interactive Flat Panel to Area for Current Site 375
10.2.12 Add Speaker Unit to Area for Current Site 376
10.2.13 Add Fire Detector to Area for Current Site 378
10.3 Edit Element in Area 379
10.3.1 Edit Camera for Current Site 379
10.3.2 Edit Door for Current Site 380
10.3.3 Edit Elevator for Current Site 383
10.3.4 Edit Vehicle for Current Site 386
10.3.5 Edit Security Radar for Current Site 386
10.3.6 Edit Alarm Input for Current Site 387
10.3.7 Edit Alarm Output for Current Site 388
10.3.8 Edit UVSS for Current Site 388
10.3.9 Edit Digital Signage Screen for Current Site 389
10.3.10 Edit Interactive Flat Panel for Current Site 389
10.3.11 Edit Speaker Unit for Current Site 390
10.3.12 Edit Third-Party Integrated Resource for Current Site 390
10.3.13 Edit Fire Detector for Current Site 391
10.3.14 Edit Element for Remote Site 391
10.4 Remove Element from Area 392
10.4.1 Remove Element from Area for Current Site 392
10.4.2 Remove Element from Area for Remote Site 393
Chapter 11 Person Management 394

11.1 Add Departments 394
11.2 Add Person 396
11.2.1 Add a Single Person 397
11.2.2 Batch Add Persons by Template 408
11.2.3 Import Domain Persons 413
11.2.4 Import Profile Pictures 416
11.2.5 Import Persons from Access Control Devices or Video Intercom Devices 417
11.2.6 Import Persons from Enrollment Station 422
11.3 Person Self-Registration 425
11.3.1 Set Self-Registration Parameters 426
11.3.2 Scan QR Code for Self-Registration 428
11.3.3 Review Self-Registered Person Information 429
11.4 Set Person ID Rule 430
11.5 Position Management 430
11.5.1 Add a Position 430
11.5.2 Import Positions 431
11.6 Object Missing 432
11.7 Batch Issue Cards to Persons 432
11.7.1 Set Card Issuing Parameters 433
11.8 Print Cards 435
11.9 Report Card Loss 436
11.9.1 Report Card Loss 437
11.9.2 Issue a Temporary Card to a Person 438
11.9.3 Batch Cancel Card Loss 439
11.10 Set Authentication via PIN Code 439
11.11 Manage Resigned Persons 440
11.11.1 Add Resigned Persons 440
11.11.2 Reinstate Persons 441

11.11.3 Manage Resignation Types 442
Chapter 12 Event and Alarm 443
12.1 Manage Event and Alarm 444
12.1.1 Supported Events and Alarms 444
12.1.2 Add Normal Event and Alarm 446
12.1.3 Add Combined Alarm 456
12.1.4 Add Generic Event 461
12.1.5 Add User-Defined Event 464
12.2 Set Basic Event and Alarm Parameters 465
12.2.1 Configure Receiving Schedule Template 465
12.2.2 Custom Alarm Settings 467
12.2.3 Configure Alarm Receiving Settings 471
12.2.4 Send Event and Alarm Report Regularly 472
12.3 Event and Alarm Search 474
12.3.1 Event and Alarm Overview 474
12.3.2 Search for Event and Alarm Logs 476
12.3.3 View Device Application Events 477
Chapter 13 Role and User Management 478
13.1 Add Role 478
13.2 Add Normal User 482
13.3 Import Domain Users 484
13.4 Change Password of Current User 486
13.5 Configure Permission Schedule 488
Chapter 14 System Security Settings 490
Chapter 15 System Configuration 494
15.1 Set User Preference 494
15.2 Set Printer 495
15.3 Set NTP 496

15.4 Set Active Directory 496
15.5 Device Access Protocol 499
15.6 Set Hik-Partner Pro Site Access 499
15.7 Set WAN Access 500
15.8 Set IP Address for Receiving Device Information 502
15.9 Set Records Storage Information 502
15.10 Set Holiday 503
15.11 Set Card Template 505
15.12 Set Email Template 506
15.12.1 Configure Email Account 506
15.12.2 Add Email Template for Sending Report Regularly 508
15.12.3 Add Email Template for Event and Alarm Linkage 510
15.13 Set Transfer Protocol 511
15.14 Export Service Component Certificate 512
15.15 Set Database Password 513
15.16 Configure System Hot Spare 513
15.17 Set Third-Party Integration 513
15.18 Data Interchange 514
15.18.1 Synchronize Card Swiping Records to Third-Party Database 514
15.18.2 Dump Access Records to Third-Party Database 515
15.19 Diagnose Remote Fault 517
15.20 Reset Device Network Information 518
15.21 Set Company Information 519
Chapter 16 Map Management 521
16.1 Configure Map 521
16.1.1 Set GIS Map and Icons 521
16.1.2 Add E-Map for Area 523
16.1.3 Add Hot Spot on Map 524

16.1.4 Add Hot Region on Map 531
16.1.5 Add Label on Map 532
16.1.6 Add Resource Group on Map 533
16.1.7 Add Parking Lot on Map 534
16.1.8 Add Combined Alarm on Map 535
16.1.9 Add Remote Site on GIS Map 536
16.2 Monitor on Map 536
16.2.1 View and Operate Hot Spot 537
16.2.2 Preview Hot Region 540
16.2.3 Preview Resource Group 540
16.2.4 View Remote Site Alarm 541
16.2.5 Operate Map 542
Chapter 17 AR Management 543
17.1 Add Scene 543
17.2 Add Scene to Map 545
Chapter 18 Maintenance 546
18.1 Health Monitoring 546
18.1.1 Real-Time Health Status Overview 546
18.1.2 Real-Time Health Status Overview (Topology) 549
18.1.3 Historical Health Data Overview 556
18.2 Set Basic Maintenance Parameters 559
18.2.1 Send Log Report Regularly 559
18.2.2 Set Warning Threshold for Streaming Media Usage 563
18.2.3 Set Network Timeout 564
18.2.4 Set Health Check Frequency 564
18.2.5 Set Topology Show Parameters 565
18.3 Resource Status 566
18.3.1 Camera Status 567

18.3.2 Door Status 568
18.3.3 Floor Status 568
18.3.4 Alarm Input Status 569
18.3.5 UVSS Status 569
18.3.6 Speaker Unit Status 569
18.3.7 Third-Party Integrated Resource Status 570
18.3.8 Remote Site Status 570
18.3.9 Streaming Server Status 570
18.3.10 Recording Server Status 570
18.3.11 DeepinMind Server Status 571
18.3.12 Encoding Device Status 571
18.3.13 Access Control Device Status 571
18.3.14 Elevator Control Device Status 572
18.3.15 Video Intercom Device Status 572
18.3.16 Visitor Terminal Status 572
18.3.17 On-Board Device Status 573
18.3.18 Entrance/Exit Control Device Status 573
18.3.19 Guidance Terminal Status 573
18.3.20 Security Control Device Status 573
18.3.21 Fire Protection Device Status 574
18.3.22 Dock Station Status 574
18.3.23 Decoding Device Status 574
18.3.24 IP Speaker Status 575
18.3.25 Security Inspection Device 575
18.3.26 Network Transmission Device 575
18.3.27 Digital Signage Terminal Status 575
18.3.28 Interactive Flat Panel Status 576
18.4 Log Search 576

18.4.1 Search for Server Logs 576
18.4.2 Search for Online/Offline Logs of Device 578
18.4.3 Search for Logs Stored on Device 579
18.4.4 Search for Online/Offline Logs of Resource 580
18.4.5 Search for Recording Status of Resource 582
18.4.6 Search for Call-Back Status of Resource 587
18.5 Service Manager 588
18.6 Set System Data Backup 589
18.7 Restore System Data 590
18.8 Export Configuration File 591
Chapter 19 Evidence Management Center 592
19.1 Basic Settings 592
19.2 Add Evidence 592
19.3 Manage Unlinked Files 595
19.3.1 Add and View Unlinked Files 595
19.3.2 Link Files with Evidence 597
19.4 Manage Operation Records 599
Chapter 20 Video Management 600
20.1 Video Overview 600
20.2 Video Security 601
20.2.1 Live View 601
20.2.2 Live View Toolbar Applications 604
20.2.3 PTZ Control 609
20.2.4 Playback 615
20.2.5 Manage Favorites 620
20.2.6 Manage View 621
20.2.7 Set Video Parameters 623
20.3 Picture Center 625

20.3.1 Search for Scheduled Captures 625
20.3.2 Time-Lapse Photography 626
20.4 Intelligent Recognition 627
20.4.1 Manage Face Comparison Group 627
20.4.2 Manage Intelligent Recognition Task 633
20.4.3 Applying Center 644
20.4.4 Add Task Schedule Template 645
20.5 Video Application 646
20.5.1 Configure Self-Learning Library 646
20.5.2 Configure Visual Tracking 647
20.5.3 Configure Person/Vehicle Arming 649
20.5.4 Configure Panorama Tracking 650
20.6 Video Settings 652
20.6.1 Configure Storage and Recording 652
20.6.2 Set Network Parameters 663
Chapter 21 Intelligent Analysis Report 666
21.1 Configure Scenario 666
21.2 Retail/Supermarket Scenario 666
21.2.1 View Store Report Dashboard 666
21.2.2 Manage Store 667
21.2.3 View Store Report 673
21.2.4 View Store Intelligent Analysis Report 676
21.3 Public Scenario 681
21.3.1 Customize Report Dashboard 681
21.3.2 View Intelligent Analysis Report 682
Chapter 22 On-Board Monitoring 718
22.1 Flow Chart of On-Board Monitoring 718
22.2 On-Board Monitoring Overview 719

22.3 Basic Settings 721
22.3.1 Configure Basic Parameters 721
22.3.2 Configure Route Parameters 722
22.3.3 Configure Fuel Level Monitoring Parameters 722
22.3.4 Configure Scheduled Reports 723
22.4 Driver Management 725
22.4.1 Add Drivers 725
22.4.2 Export Drivers 730
22.4.3 Add a Driver Group 731
22.4.4 Add Drivers to a Driver Group 731
22.5 Driving Rule 732
22.5.1 Configure a Fence Rule 732
22.5.2 Configure a Deviation Rule 734
22.5.3 Configure a Rule Schedule Template 735
22.6 Route Management 736
22.6.1 Manage Stops 736
22.6.2 Configure Driving Routes and Shift Schedules 738
22.6.3 Add a Stop Event Rule 742
22.7 Driving Monitoring 743
22.8 Route Monitoring 747
22.9 On-Board Monitoring Record 750
22.9.1 Search for Vehicle Tracks 750
22.9.2 Search for Driving Events 751
22.9.3 Search for Routes 752
22.9.4 Search for Fuel Level Monitoring Records 754
22.10 Statistics and Reports 755
22.10.1 Overview 755
22.10.2 Generate a Driver Analytics Report 758

22.10.3 Generate a GPS Information Report 759
22.10.4 Generate a Driving Distance Report 762
22.10.5 Generate a Driving Duration Report 764
22.10.6 Generate a Speeding Report 766
22.10.7 Generate a Stop Analytics Report 768
22.10.8 Generate a Driving Event Report 769
22.10.9 Generate a Fuel Consumption Analytics Report 771
22.10.10 Generate a Passenger Counting Report 774
22.10.11 Generate a Device Online Rate Report 775
Chapter 23 Vehicle Management 778
23.1 Manage Registered Vehicles 778
23.1.1 Add a Registered Vehicle 778
23.1.2 Batch Import Registered Vehicles 781
23.2 Manage Vehicle Lists 782
23.3 Filter and Export Visitor Vehicles 786
23.4 Manage Vehicles in Blocklist 787
23.4.1 Add a Vehicle to Blocklist 787
23.4.2 Batch Import Vehicles to Blocklist 789
23.5 Customize Vehicle Information 790
23.6 Configure Fuzzy Matching Rules for License Plate Search 792
Chapter 24 ANPR (Automatic Number Plate Recognition) 794
24.1 Search for Passing Vehicles Detected by Cameras and UVSSs 794
24.2 Generate Vehicle Analysis Report 796
24.3 Send Vehicle Analysis Reports Regularly 799
Chapter 25 Parking Management 803
25.1 Manage Parking Lot 803
25.1.1 Parking Lot Overview 805
25.1.2 Add Parking Lot 806

25.1.3 Add Entrance and Exit 809
25.1.4 Add Lane 810
25.1.5 Link Display Screen and Set Displayed Content 814
25.1.6 Configure Entry & Exit Rules 818
25.1.7 Configure Parking Fee Rules 831
25.2 Methods for Parking Charges 848
25.2.1 Top Up Parking Pass 848
25.2.2 Pay in Toll Center 850
25.3 Parking Guidance Configuration 851
25.3.1 Add a Floor to the Parking Lot 852
25.3.2 (Optional) Link Devices to the Floor 854
25.3.3 (Optional) Configure a Map for the Floor 856
25.3.4 Set Types for Parking Spaces on the Map 859
25.3.5 Mark Devices on the Map 862
25.3.6 Calibrate Parking Spaces Regularly 863
25.3.7 Parking Space Monitoring 865
25.4 Record Search 867
25.4.1 Search for Passing Vehicles Detected by Entrances & Exits 867
25.4.2 Search for Parking Records 869
25.4.3 Search for Parked Vehicles 870
25.4.4 Search for Payment Records 872
25.4.5 Search for Vehicle Top-Up and Refund Records 873
25.4.6 Search for Transaction Records of Vehicle Owner Account 875
25.4.7 Search for Work Records of Operators 876
25.4.8 Search for Coupon Records 876
25.5 Statistic and Report 877
25.5.1 Export Operation Reports of Parking Lots 878
25.5.2 Export Transaction Reports of Parking Lots 882

25.5.3 Configure Scheduled Overtime Parking Reports 883
25.6 Set Basic Parameters of Parking Management 886
25.7 Self-Service Vehicle Finding Client 889
Chapter 26 Access Control Management 891
26.1 Access Control Overview 891
26.2 Manage Access Level 892
26.2.1 Add Access Level 892
26.2.2 Assign Access Level 894
26.2.3 Apply Persons' Access Levels to Device 899
26.2.4 Clear Persons' Access Levels 900
26.2.5 Set Access Schedule Template 901
26.2.6 Enable Authentication via Password 902
26.2.7 Advanced Functions 903
26.2.8 Access Control Test 919
26.3 Door and Elevator Control 923
26.3.1 Start Live View of Access Control / Elevator Control Devices 924
26.3.2 View Real-Time Access Event 925
26.3.3 Door Control 926
26.3.4 Elevator Control 927
26.4 Subscribe to Device and Access Events 928
26.5 Set User to Receive Access Control Calls 928
26.6 Synchronize Access Records to System Regularly 929
26.7 Enable Open Door via Bluetooth 929
26.8 Search Access Records 930
26.9 Search Data Recorded on Access Control Devices and Elevator Control Devices 933
26.10 Perform Entry & Exit Counting 935
Chapter 27 Visitor Management 937
27.1 Configurations Before Visitor Management 938

27.1.1 Add a Visitor Group 938
27.1.2 Add Access Level for Visitors 939
27.1.3 Manually Apply Visitors' Access Level Settings to Visitor Terminals 940
27.1.4 Set Self-Service Reservation Parameters 940
27.1.5 Set Self-Service Check-Out Point 942
27.1.6 Add Visitor Email Template 943
27.1.7 Add Visitor Pass Template 945
27.1.8 Set Basic Parameters 949
27.1.9 Manage Entry & Exit Rule for Visitors' Vehicles 953
27.2 Watch List Management 954
27.2.1 Add Entity Type 955
27.2.2 Set Match Method 956
27.2.3 Add an Entity to the Watch List 956
27.2.4 Import Existing Visitors to the Watch List 957
27.3 Visitor Reservation 959
27.3.1 Reserve a Visitor 959
27.3.2 Batch Import the Visitor Reservation Information 963
27.3.3 Review Visitor Reservations 964
27.4 Visitor Check-In 967
27.4.1 Check In a Visitor Without Reservation 967
27.4.2 Check In a Reserved Visitor 973
27.5 Visitor Check-Out 975
27.6 View Visitor Information 977
27.7 Check Visitor Access Records 978
Chapter 28 Time & Attendance 979
28.1 Time and Attendance Overview 979
28.2 Add an Attendance Group 981
28.3 Basic Configuration 983

28.3.1 Specify Attendance Check Points 983
28.3.2 Add a Pay Code 987
28.3.3 Edit a Fixed Code 988
28.3.4 Add a Leave Rule 990
28.3.5 Configure Check-In/Check-Out via Mobile Client 992
28.3.6 Configure Storage Settings 993
28.4 Configure Attendance Rules for Global / Department / Attendance Group 993
28.4.1 Define Weekends 993
28.4.2 Configure Attendance Calculation Mode 993
28.4.3 Define Absence 994
28.4.4 Add Holidays Requiring Attendance 996
28.4.5 Calculation of Leaves 997
28.4.6 Configure Overtime Parameters 998
28.4.7 Configure Authentication Mode 1002
28.5 Add Timetable 1002
28.5.1 Add Break Timetables 1002
28.5.2 Add Timetable for Normal Shift 1004
28.5.3 Add Timetable for Flexible Shift 1007
28.6 Add Shift 1009
28.7 Manage Schedule 1010
28.7.1 Schedule Overview 1010
28.7.2 Assign Schedule to Department 1011
28.7.3 Assign Schedule to Attendance Groups 1013
28.7.4 Assign Schedule to Person 1014
28.7.5 Add Temporary Schedule 1016
28.8 Configure Calculation Mode of Attendance Results 1017
28.8.1 Manually Calculate Attendance Results 1018
28.8.2 Set Auto-Calculation Time of Attendance Results 1018

28.9 Approval Management 1018
28.9.1 Add an Approval Role 1019
28.9.2 Add a Department Approval Flow 1020
28.9.3 Add an Attendance Group Application Flow 1023
28.9.4 Add a Personal Approval Flow 1024
28.10 Application Management for Employee 1027
28.10.1 Overview of Personal Attendance Data 1027
28.10.2 Submit and View Applications 1028
28.10.3 Review Employees' Applications 1031
28.10.4 View and Export Attendance Records and Reports 1032
28.11 Application Management for Admin 1032
28.11.1 Apply for a Leave 1032
28.11.2 Apply for a Check-In/Out Correction 1033
28.11.3 Apply for Overtime 1034
28.11.4 Import Applications 1035
28.11.5 Review or Undo Applications 1035
28.12 View Attendance Records 1036
28.12.1 Import Transactions 1037
28.13 Manage Attendance Reports 1038
28.13.1 Set Display Rules for Attendance Report 1038
28.13.2 View Daily/Weekly/Monthly/Summary Attendance Reports 1038
28.13.3 Send Attendance Report Regularly 1039
28.13.4 Add a Custom Report 1041
Chapter 29 Video Intercom Management 1044
29.1 Video Intercom Overview 1044
29.2 Basic Settings of the Platform 1045
29.2.1 Add Call Recipients 1045
29.2.2 Add Call Schedule Template 1046

29.2.3 Configure General Parameters 1047
29.2.4 Add or Configure a Receiving Schedule Template 1048
29.3 Configure Device Parameters 1048
29.4 Manage Video Intercom Device 1050
29.4.1 Set Locations for Video Intercom Devices 1050
29.4.2 Apply Location to Video Intercom Devices 1051
29.5 Video Intercom Application 1052
29.5.1 Add Call Schedule for Door Stations 1052
29.5.2 Apply Call Schedule to Door Stations 1053
29.5.3 Link Resources with Indoor Stations 1053
29.6 Apply Data to Indoor Station 1058
29.6.1 Manage Notices 1058
29.6.2 Apply Software Package to Indoor Station 1059
29.7 Apply Advertisements to Door Stations 1061
29.8 View Event/Alarm Related Notices 1062
29.9 Call & Talk 1063
29.9.1 Call an Indoor Stations 1063
29.9.2 View Recents 1063
Chapter 30 Alarm Detection 1065
30.1 Alarm Detection Overview 1065
30.2 Add Security Control Partitions (Areas) from Device 1066
30.3 Configure Arming Schedule Template 1069
Chapter 31 Digital Signage Management 1070
31.1 Digital Signage Overview 1070
31.2 Content Creation 1072
31.2.1 Create Multimedia Program 1072
31.2.2 Create Video Wall Program 1079
31.2.3 Create Attendance Program 1085

31.2.4 Create People Counting Program 1088
31.2.5 Create Emergency Mustering Program 1092
31.2.6 Add Emergency Mustering Text Notification 1098
31.2.7 Add Text Message 1101
31.3 Schedule Management 1102
31.3.1 Create a Schedule 1102
31.3.2 Create a Loop Schedule 1104
31.3.3 Create a Default Schedule 1106
31.4 Content Review 1108
31.5 Content Release 1109
31.5.1 Release a Program Schedule 1109
31.5.2 Cut in Program 1110
31.5.3 View Release Records 1111
31.6 Device Control 1112
31.6.1 Control Digital Signage Terminal 1112
31.6.2 Control Video Wall 1114
31.7 Material Library 1115
31.7.1 Upload Local Material 1116
31.7.2 Create Dynamic Material 1118
31.7.3 Mange Used or Unused Materials 1119
31.8 Basic Settings 1120
31.8.1 Switch Application Mode 1120
31.8.2 Set Material Storage Location 1121
31.8.3 Configure Video Wall 1122
Chapter 32 Interactive Flat Panel Management 1124
32.1 Interactive Flat Panel Overview 1124
32.2 Content Creation 1126
32.2.1 Create Multimedia Program 1126

32.2.2 Add Emergency Mustering Text Notification 1132
32.2.3 Add Text Message 1135
32.3 Content Review 1136
32.4 View Release Records 1137
32.5 Manage Applications 1138
32.6 Control Interactive Flat Panel 1140
32.7 Material Library 1141
32.7.1 Upload Local Material 1141
32.7.2 Create Dynamic Material 1143
32.7.3 Mange Used or Unused Materials 1144
32.8 Set Material Storage Location 1146
Chapter 33 Skin-Surface Temperature Screening 1147
33.1 Temperature Screening Configuration 1147
33.1.1 Group Temperature Screening Points 1147
33.1.2 Configure Temperature Screening Parameters 1148
33.2 Real-Time Skin-Surface Temperature Monitoring 1149
33.3 Search History Temperature Screening Data 1150
33.4 Registration 1151
33.4.1 Register Person Information 1151
33.4.2 Customize Registration Template 1153
33.4.3 View Registered Person Information 1153
33.5 Search for Temperature Screening Records 1154
33.6 Generate Skin-Surface Temperature Analysis Report 1155
33.7 Configure the Scheduled Report of Screening 1157
Chapter 34 Broadcast Management 1161
34.1 Set Basic Settings for Broadcast 1161
34.2 Group Speaker Units 1162
34.3 Manage Media Files 1162

34.4 Configure Live Broadcast 1163
34.5 Search for Live Broadcast Records 1164
34.6 Add a Scheduled Broadcast Task 1165
34.7 Add a Linked Broadcast Task 1166
Chapter 35 Security Inspection Management 1169
35.1 Configure Security Inspection 1169
35.2 Add Security Inspection Channels to Area 1169
35.3 View Videos of Security Inspection 1170
35.4 Historical Data Search 1173
35.4.1 Search for Package Detection Records 1173
35.4.2 Search for Metal Detection Records 1174
35.4.3 Search for Absence Records 1175
35.5 Generate Package Detection Report 1176
35.6 Generate People Inspection Report 1176
Chapter 36 Emergency Mustering 1178
36.1 Emergency Solution Settings 1179
36.2 Start a Roll Call 1182
Chapter 37 Patrol Management 1184
37.1 Flow Chart of Patrol Management 1185
37.2 Basic Configurations for Patrol Management 1187
37.2.1 Add Exception Types for Patrol Management 1188
37.2.2 Set Parameters for Patrol Management 1188
37.3 Add Patrol Points 1189
37.4 Add Patrol Person Group 1191
37.5 Add Patrol Schedule Template 1193
37.6 Add Patrol Route 1195
37.7 Real-Time Patrol Monitoring 1198
37.8 Search for Patrol-Related Event Records 1199

37.9 Check Patrol Statistics 1201
Chapter 38 Toll Verification 1203
38.1 Basic Configuration 1203
38.2 Check Vehicle Information for Toll Verification 1203
38.3 Search for Toll Verification Records 1204
Chapter 39 Traffic Data Analysis 1206
Chapter 40 Street Data Analysis 1207
Chapter 41 Water Level Detection 1209
41.1 Search for Water Level Data 1209
41.2 Analyze Water Level Data 1210
Chapter 42 Dock Management 1212
42.1 Flow Chart of Dock Management 1212
42.2 Dashboard of Dock Management 1213
42.3 Basic Configuration 1214
42.4 Add Dock Area and Docks 1214
42.5 Dock Monitoring 1216
42.6 Search for Vehicle Data 1217
42.7 View Dock Statistics 1218
42.7.1 Generate Dock Usage Report 1218
42.7.2 Generate Dock Throughput Report 1218
42.7.3 Generate Dock Using Trend Report 1219
Chapter 43 Parcel Tracking 1220
43.1 Flow Chart 1220
43.2 Basic Configuration 1221
43.3 Add a Check Point 1222
43.4 Search for Scanning Records 1224
Chapter 44 Canteen Consumption 1225
44.1 Flow Chart 1225

44.2 Payment Overview 1227
44.3 Basic Configuration 1228
44.3.1 General Configuration 1228
44.3.2 Meal Settings 1230
44.4 Merchant Management 1232
44.5 Payment Group Management 1234
44.5.1 Add a Payment Group 1234
44.5.2 Add Persons to Payment Group 1235
44.6 Payment Strategy Management 1236
44.6.1 Add Payment Rule 1237
44.6.2 Payment Group Authorization 1238
44.6.3 Person Authorization 1239
44.7 Transaction Search 1241
44.7.1 Search for Transaction Record 1241
44.7.2 Search for Payment Record 1242
44.8 Statistics and Reports 1243
44.8.1 Group Payment Statistics 1243
44.8.2 Person Payment Statistics 1244
44.8.3 Revenue Report of Merchant 1245
44.8.4 Device Payment Statistics 1247

Chapter 1 About This Document

This user manual is intended for the administrator of the system.

The manual guides you to establish and configure the security system. Follow this manual to perform system activation, access of the system, and configuration of the monitoring task via the provided Web Client, etc. To ensure the properness of usage and stability of the system, refer to the contents below and read the manual carefully before installation and operation.

1.1 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 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. • Provides the management for the users, roles, permissions, devices, and services. • 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 C/S 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.

1.2 Recommended Running Environment

The following is recommended system requirement for running the Web Client.

CPU

Intel® Core™ I3 and above

Memory

4 GB and above

Web Browser

Internet Explorer® 11 and above, Firefox® 100 and above, Google Chrome® 100 and above, Safari® 13 and above, Microsoft® Edge 100 and above.

Note

Upgrading from V1.x to V2.x requires double available disk spaces than data stored in the database.

1.3 Symbol Conventions

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

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

Chapter 2 Login

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

Note

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 ***System Security Settings*** .

2.1 First Time Login

If this is the first time for you to login, you can choose to login as admin or normal user according to your user role.

2.1.1 Login for First Time for Admin User

By default, the system predefined the administrator user named admin. When you login via the Web Client for the first time, you are required to create a password for the admin user before you can properly configure and operate the system.

Steps

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

   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.

   Note

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

2. Enter a password and confirm the password for the admin user in the pop-up Create Password window, and click **Next**.

Note

The password strength can be checked by the system and should meet the system requirements. The default minimum password strength should be **Medium**. For setting minimum password strength, refer to ***System Security Settings*** .

Caution

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

3. Select a method for password reset verification.
   - **Email**: Click **Email → Next** and set the email address for receiving the password reset verification code.
   - **Security Question**: Click **Security Question → Next** , select three different security questions from the drop-down lists, and enter your answers accordingly.

Note

If you forget the password of your account, you can reset the password by verifying your email address or answering the security questions. Refer to ***Forgot Password*** for details.

4. Click **OK**.

   The home page of the Web Client will show if the admin password is created successfully.

Result

After you logged in, the Site Name window opens and you can set the site name for the current system as you want.

Note

You can also set it in **System → Normal → User Preference** . See ***Set User Preference*** for details.

2.1.2 First Time Login for Normal User

When you log in to the system as normal user via Web Client for the first time, you should change the initial password and set a new password for login.

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 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.

Note

You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and password.

Note

Contact the administrator for the user name and initial password.

3. Click **Log In** and the **Change Password** window opens.
4. Set a new password and confirm the password.

Note

The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***System Security Settings*** .

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.

5. Click **OK** to change the password.

Result

Web Client home page displays after you successfully logging in.

2.2 Login via Web Client (Administrator)

You can access the system via web browser and configure the system.

Steps

1. In the address bar of the web browser, input the address of the PC running SYS service and press **Enter** key.

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.

Note

You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Select the **Management** tab.
3. Enter the user name and password.
4. Click **Log In** to log in to the system.

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. For setting failed login attempts and locking duration, refer to ***System Security Settings*** .
- 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.
- The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***System Security Settings*** .
- If your password is expired, you will be asked to change your password when login. For setting maximum password age, refer to ***System Security Settings*** .

Result

Web Client home page displays after you successfully logging in to the system.

2.3 Login via Web Client (Employee)

Employees can access the system via web browser.

Before You Start

The administrator should enable self-service login (enabled by default) and set the login password (employee ID by default) 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.

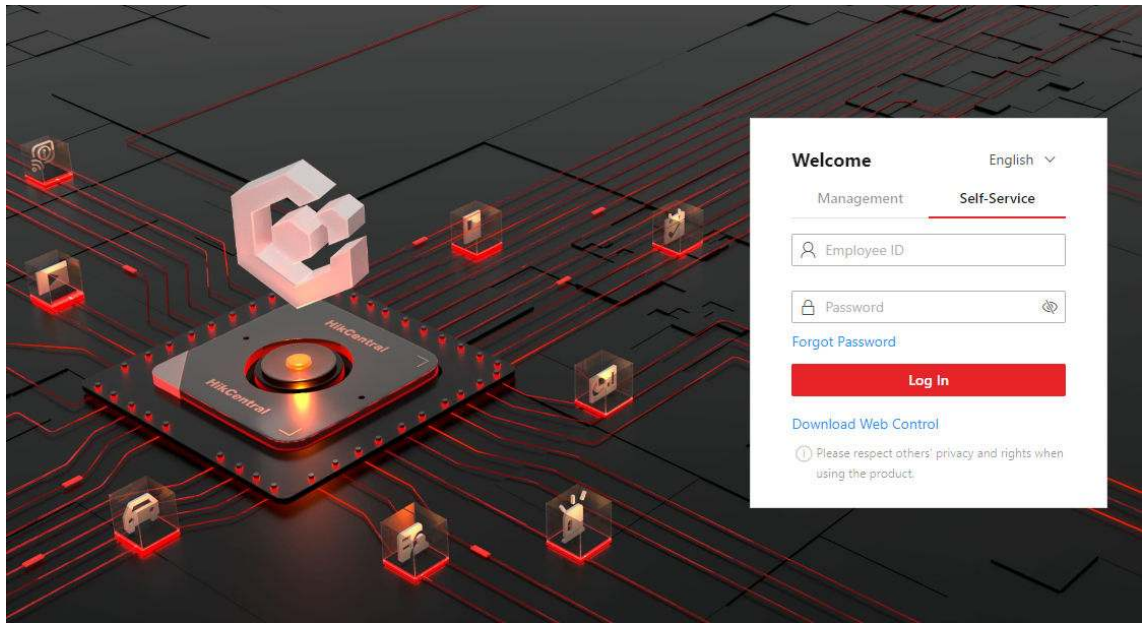


Figure 2-1 Login Page

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 upon the first login.
- If employees forget the password, they can reset new password in **Forgot Password**.
- If the password is expired, employees will be asked to change the password upon login. For setting the maximum password age, refer to ***System Security Settings*** .

Result

Web Client home page displays after employees successfully log in to the system.

2.4 Change Password for Reset User

When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral Professional via the Web Client.

Steps

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

   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.

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Enter the user name and initial password set by the administrator.
3. Click **Log In** and a **Change Password** window opens.
4. Set a new password and confirm the password.

   Note

   The password strength can be checked by the system and should meet the system requirements. If password strength is lower than the required minimum strength, you will be asked to change your password. For setting minimum password strength, refer to ***System Security Settings*** .

   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.

5. Click **OK**.

Result

Web Client home page displays after you successfully changing the password.

2.5 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 select and answer the corresponding questions, click **Next**, and set and confirm your new password.

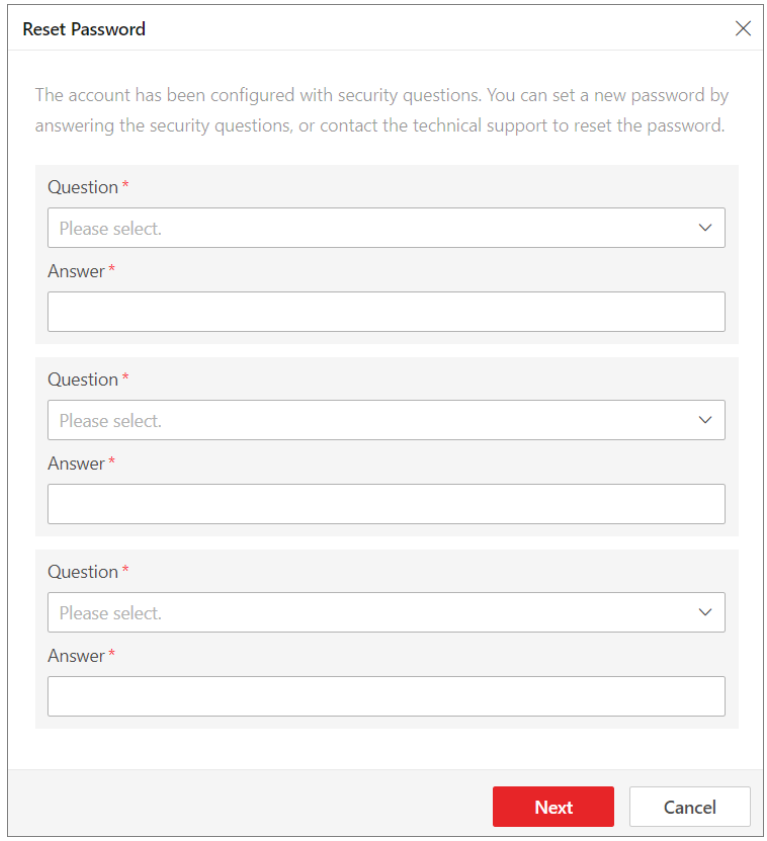


Figure 2-2 Reset Password for admin User via Security Questions

   - 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.

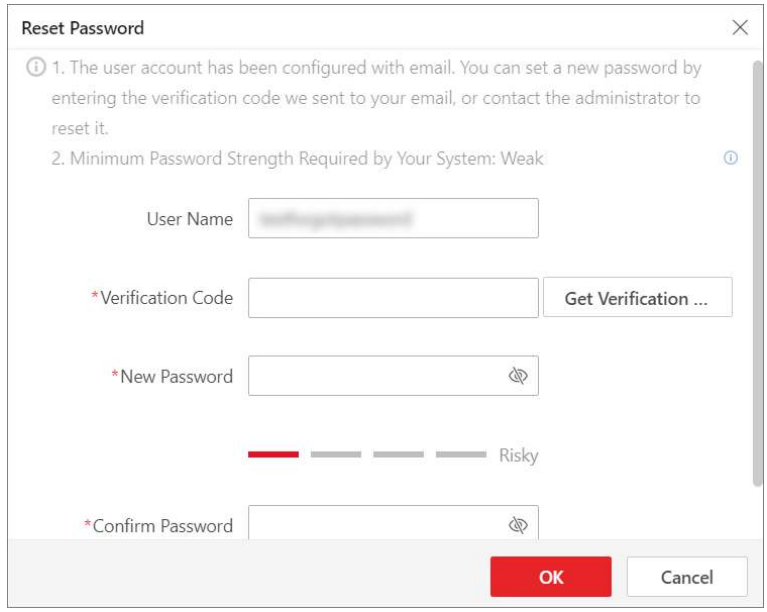


Figure 2-3 Reset Password via Verification Code

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 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 ***System Security Settings*** .

Caution

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

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

4. Click **OK**.

Chapter 3 Download Mobile Client

On the login page of Web Client, you can scan the QR code to download the Mobile Client that is used for accessing the system via mobile terminal (e.g., mobile phone).

Perform this task when you need to download the Mobile Client.

Note

You can also search and download the Mobile Client in the App Store.

Steps

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

   Example

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

   Note

   You should configure the SYS's IP address in WAN Access of System Configuration before accessing the SYS via WAN. For details, refer to ***Set WAN Access*** .

2. Scan the corresponding QR code with your mobile terminal to download the Mobile Client.

Chapter 4 Web Control

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.

Chapter 5 Home Page Overview

The default Home page of the Web Client provides a visual overview of function modules on the platform. You can access specific modules quickly and conveniently via the Home page.

Note

After you entered the modules, tabs will appear on the top of the Web Client, you can click tabs to quickly switch modules. You can also click in the tab area to refreshthe module.

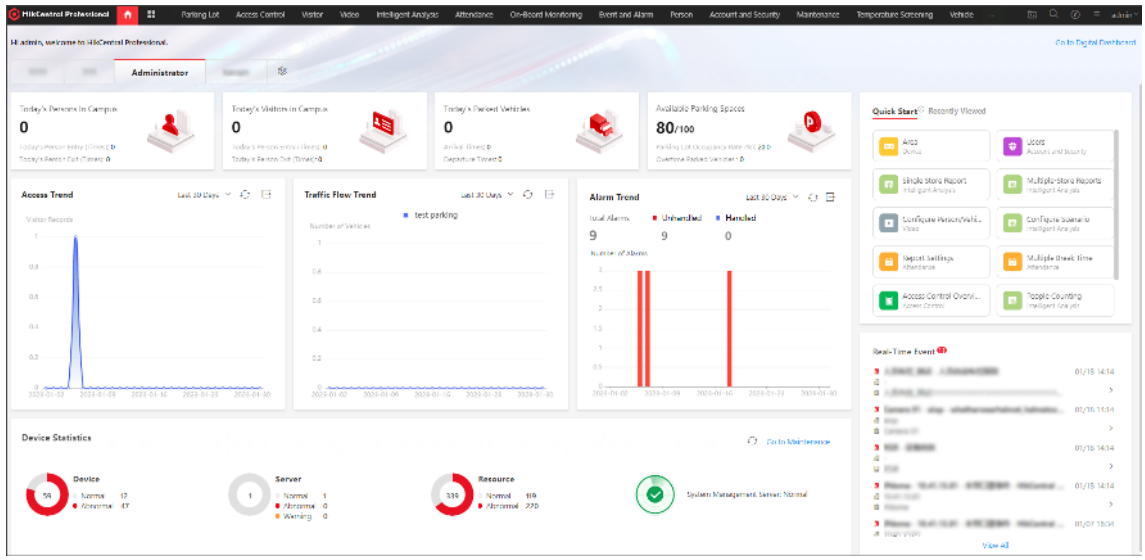


Figure 5-1 Home Page Overview

Table 5-1 Home Page Description

Section	Module	Description
Top Navigation Bar	Navigation Icon	The navigation bar shows the available functions determined by the Licenses you purchased. You can add some frequently used or important modules to the navigation bar for convenient access. See details in ***Customize Navigation Bar*** .
	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.

Section	Module	Description
	Real-Time Event	View the list of real-time events. Also, you can click an event, go to the Alarm Details page to view details and acknowledge the alarm.
	Wizard	**Video** A wizard which guides you through the management and applications of video. You can also view the flow chart which introduces the video resource management, recording configurations, and video application in ***Video Management*** . **Access Control** A wizard which guides you through the basic configurations of access control. You can also view the flow chart which introduces the configurations and operations of access control and elevator control in ***Flow Chart of Door Access Control*** . **Visitor** A wizard which guides you through the basic configurations and applications of visitor management. You can also view the flow chart which introduces the process of visitor management from reserving visitors to checking out visitors and viewing visitor information/records (see ***Flow Chart of Visitor Management***). **On-Board Monitoring** A wizard which guides you through the configuration and applications of on-board monitoring. You can also view the flow chart which introduces the management of on-board devices and vehicles, the configuration of GIS map and driving rules, driving monitoring, vehicle route and driving event search, and the report management in ***On-Board Monitoring*** . **Vehicle and Parking** A wizard which guides you through the management and applications of vehicle and parking. You can also view the flow chart which introduces the management of parking lots, vehicles, and entry & exit rules, parking

Section	Module	Description
		fee rules, parking guidance, and vehicle & record search in ***Flow Chart of Parking Guidance Configuration*** . **Alarm Detection** A wizard which guides you through the management and configurations of alarm detection. You can also view the flow chart which introduces the management of security control panels and alarm inputs, arming schedule configuration, and event & alarm management in ***Flow Chart of Alarm Detection*** . **Digital Signage** A wizard which guides you through the management and configurations of digital signage. You can also view the flow chart which introduces the management of digital signage terminals, materials, programs, and schedules, program approval, and program release in ***Flow Chart of Digital Signage Management*** . **Attendance** A wizard which guides you through the management and configurations of attendance. You can also view the flow chart which introduces the management of devices, person groups, and persons, basic attendance configuration, attendance rule configuration, and record search and handling in ***Flow Chart of Time and Attendance*** . **Patrol** A wizard which guides you through the management and configurations of patrol. You can also view the flow chart which introduces the process of patrol management from adding patrol points to real-time patrol monitoring and records/statistics search (see ***Flow Chart of Patrol Management***).
	Maintenance and Management	**License** You can view the License details, activate, upgrade, and deactivate the License if needed. For more details, refer to ***License Management*** .

Section	Module	Description
		Back Up and Restore System Data You can manually back up the data in the system, or configure a schedule to run the backup task regularly. When an exception occurs, you can restore the database if you have backed up the database. For more details, refer to ***Set System Data Backup*** and ***Restore System Data*** . **Export Configuration Data** You can export and save configuration data to your local PC. For more details, refer to ***Export Configuration File*** . **Download Installation Package** Download the installation package of other clients, such as Control Client. **About** Check the version information of the Web Client. View the License Agreement and Open-Source License Agreement.
	Account	**Change Password** Change the password of the current user. For more details, refer to ***Change Password of Current User*** . **Logout** Log out of the system and 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. For more details, refer to ***Customize Preset Workbench*** and ***Customize Personal Workbench*** . 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

Section	Module	Description
		control and management, persons, and vehicles. For more details, refer to ***View Digital Dashboard*** .

5.1 Customize Navigation Bar

To conveniently access some frequently used or important modules, you can customize the navigation bar.

Steps

1. On the top left, select to display the navigation bar and All Modules panel.

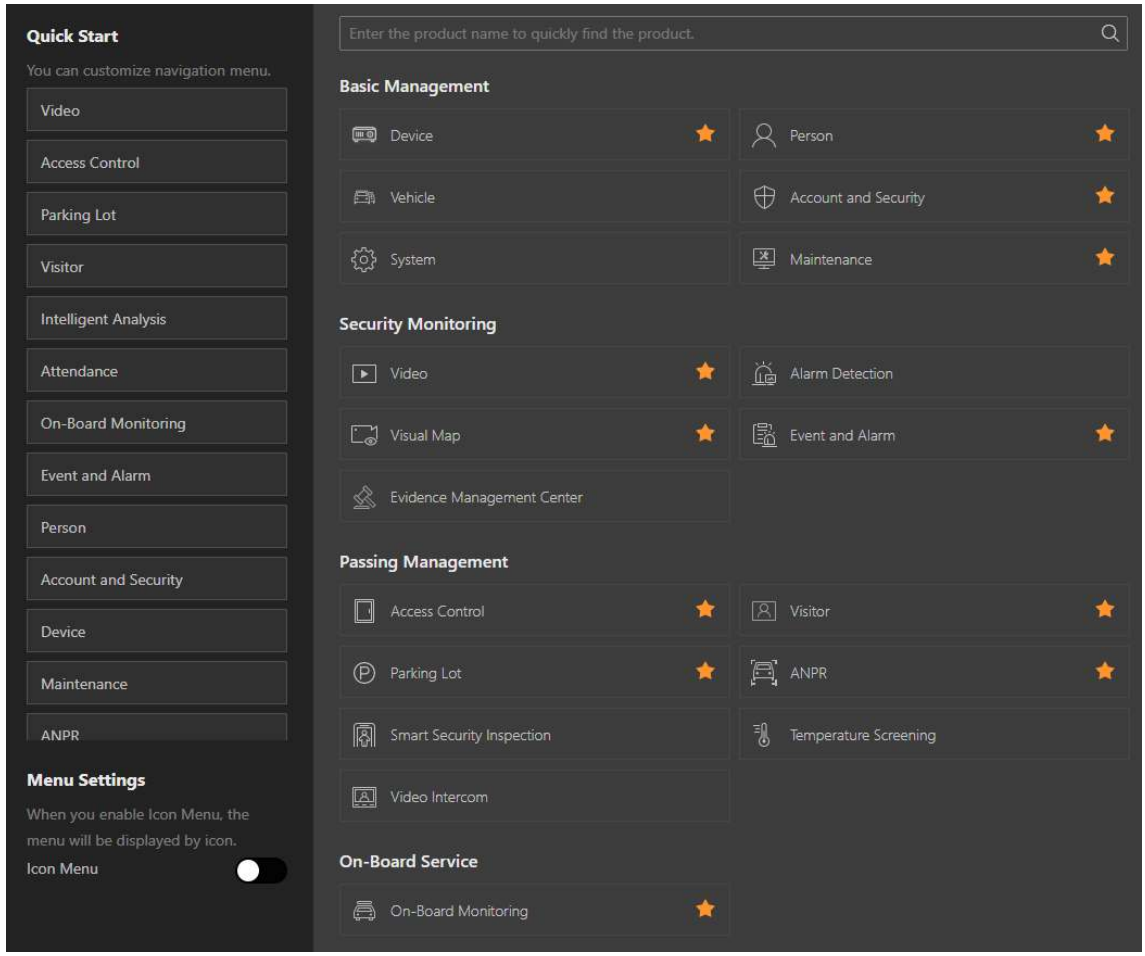


Figure 5-2 Navigation Bar and All Modules Panel

Note

On the All Modules panel, the icon beside the module name indicates that this module has been added to the left navigation bar.

2. **Optional:** Click to remove the module from the navigation bar.
3. **Optional:** In the Quick Start area, drag a module up or down to adjust the module order on the top navigation bar.
4. **Optional:** In Menu Settings area, switch on **Icon Menu**, the module name turns to be an icon displayed on the top navigation bar.

5.2 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 5-3 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.

5.3 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. For details, refer to ***Login via Web Client (Administrator)*** .

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 Configuration**.
- 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 **Edit**, select users to link with the workbench, so the workbench will be displayed on the user's Home page.

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. (Optional) Set the display size of the component.
5. Click **Save**. The added preset workbench will be displayed in the Preset Workbench pane on the Home page.

5.4 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.

Steps

1. Click to enter the Home page.

2. Click to expand the workbench configuration pane.
3. In the personal workbench area, click **Personal Workbench** to enter the Create Personal Workbench page.
4. Click to edit the workbench name.
5. **Optional:** Select an existing workbench as the template from the Copy From drop-down list.
6. Click **OK**.
7. Click + on the right side of the component.

   The component will be displayed on the right.
8. **Optional:** Drag in the lower right corner of a single component or set the display ratio (e.g., 100%, 60%, or 50%) to adjust the display size of the component.
9. Click **Save**.

   The added personal workbench will be displayed in the Personal Workbench pane on the Home page.

Chapter 6 Getting Started

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

Verify Initial Configuration of Devices and Other Servers

Before doing anything on the platform, make sure the devices (encoding devices, access control devices, recording server, and so on) you are going to use are correctly mounted and connected to the network as specified by the manufacturers. Such initial configurations are required in order to connect the devices to the platform via network.

Log In to Web Client

Refer to ***Login for First Time for Admin User*** .

Activate License

Refer to ***Activate License - Online*** or ***Activate License - Offline*** .

Add Devices to Platform and Configure Area

The platform can quickly scan your network for relevant devices, and add them. Or you can add the devices by inputting the required information manually. The devices added should be organized into areas for convenient management. Refer to ***Device and Server Management*** and ***Area Management*** .

Configure Recording Settings

You can record the video files of the cameras on the storage device according to the configured recording schedule. The schedule can be set as continuous, alarm triggered, or command triggered as desired. Refer to ***Configure Storage and Recording*** .

Configure Event and Alarm

The camera exception, device exception, server exception, alarm input, and so on, can trigger linkage actions in the platform. Refer to ***Event and Alarm*** .

Configure Users

Specify who should be able to access the platform, and how. You can set different permissions for the users to limit their operations. Refer to ***Role and User Management*** .

View How-to Videos

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 to view the how-to videos of the platform.

Chapter 7 Application Summary

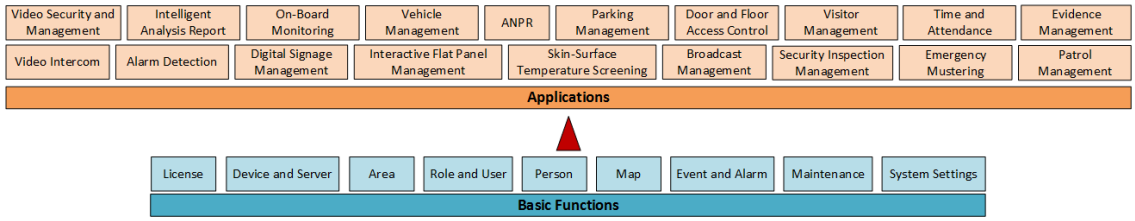


Figure 7-1 Functions and Applications in HikCentral Professional

Table 7-1 Applications in HikCentral Professional

Application	Description
Video Security and Management	Refer to ***Flow Chart of Video Security*** and ***Video Management*** for details.
Intelligent Analysis Report	Refer to ***Flow Chart of Intelligent Analysis Report in Retail/ Supermarket Scenario*** , ***Flow Chart of Intelligent Analysis Report in Public Scenario*** , and ***Intelligent Analysis Report*** for details.
On-Board Monitoring	Refer to ***Flow Chart of On-Board Monitoring*** for details.
Vehicle Management	Refer to ***Vehicle Management*** for details.
ANPR (Automatic Number Plate Recognition)	Refer to ***ANPR (Automatic Number Plate Recognition)*** for details.
Parking Management	Refer to ***Flow Chart of Parking Lot Management*** , ***Flow Chart of Parking Fee Collection*** , ***Flow Chart of Parking Guidance Configuration*** , and ***Parking Management*** for details.
Door and Floor Access Control	Refer to ***Flow Chart of Door Access Control*** , ***Flow Chart of Floor Access Control*** , and ***Access Control Management*** for details.
Visitor Management	Refer to ***Flow Chart of Visitor Management*** and ***Visitor Management*** for details.
Time and Attendance	Refer to ***Flow Chart of Time and Attendance*** and ***Time & Attendance*** for details.
Evidence Management	Refer to ***Evidence Management Center*** for details.
Video Intercom	Refer to ***Video Intercom Management*** for details.

Application	Description
Alarm Detection	Refer to ***Flow Chart of Alarm Detection*** and ***Alarm Detection*** for details.
Digital Signage Management	Refer to ***Flow Chart of Digital Signage Management*** and ***Digital Signage Management*** for details.
Interactive Flat Panel Management	Refer to ***Flow Chart of Interactive Flat Panel Management*** and ***Interactive Flat Panel Management*** for details.
Skin-Surface Temperature Screening	Refer to ***Skin-Surface Temperature Screening*** for details.
Broadcast Management	Refer to ***Broadcast Management*** for details.
Security Inspection Management	Refer to ***Security Inspection Management*** for details.
Emergency Mustering	Refer to ***Emergency Mustering*** for details.
Patrol Management	Refer to ***Flow Chart of Patrol Management*** and ***Patrol Management*** for details.

Table 7-2 Basic Functions in HikCentral Professional

Basic Function	Description
License	Refer to ***License Management*** for details.
Device and Server	Refer to ***Device and Server Management*** for details.
Area	Refer to ***Area Management*** for details.
Role and User	Refer to ***Role and User Management*** for details.
Person	Refer to ***Person Management*** for details.
Map	Refer to ***Map Management*** for details.
Event and Alarm	Refer to ***Event and Alarm*** for details.
Maintenance	Refer to ***Maintenance*** for details.
System Settings	Refer to ***System Security Settings*** and ***System Configuration*** for details.

7.1 Flow Chart of Video Security

The following flow chart shows the process of configurations and operations required for basic video security functions, such as live view and playback.

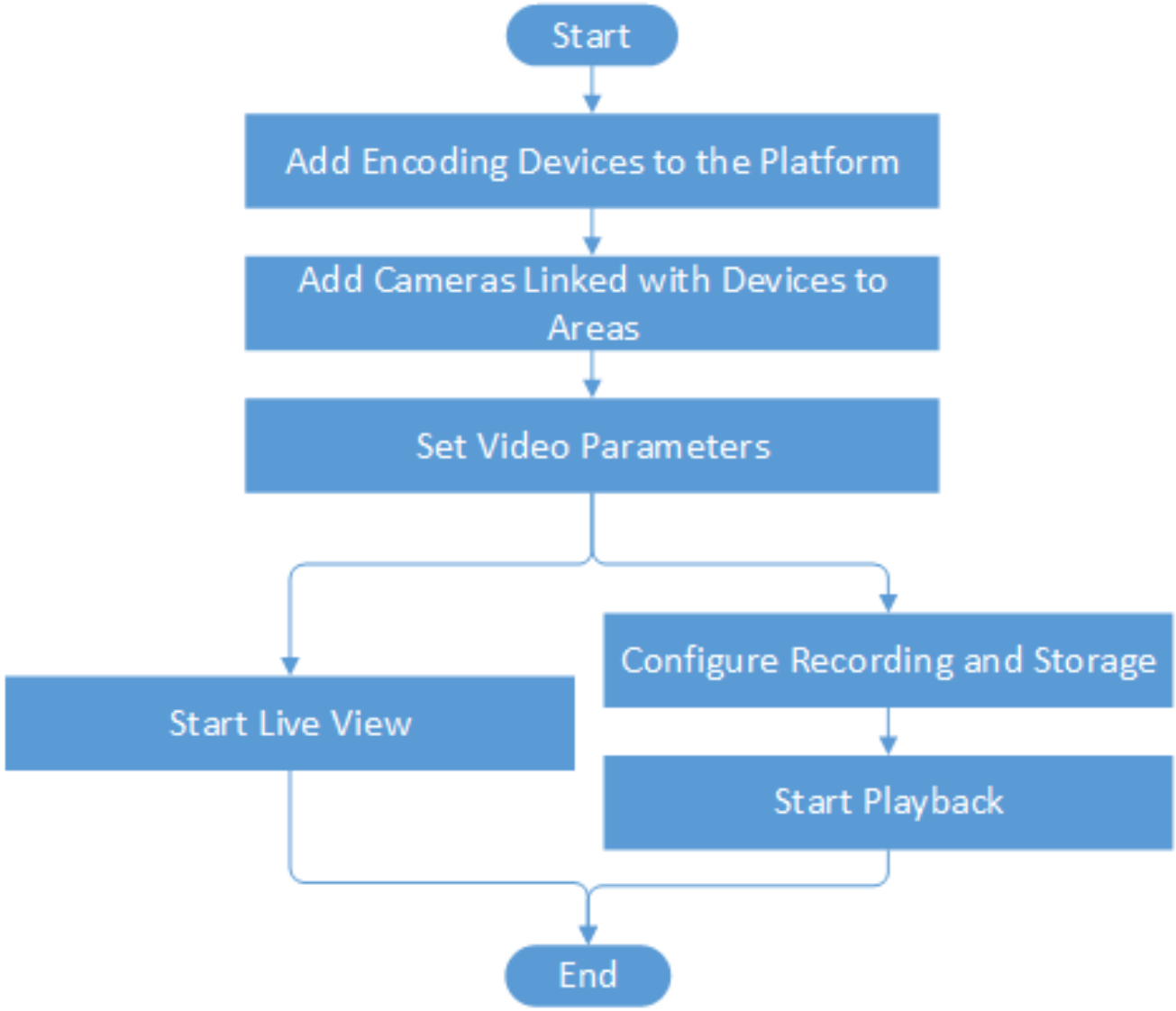


Figure 7-2 Flow Chart of Video Security

Table 7-3 Flow Chart Description

Procedure	Description
Add Encoding Devices to the Platform	Add encoding devices to the platform by online detection, IP address, port segment, **Hik-Connect DDNS**, device ID, device ID segment, etc. For details, see ***Manage Encoding Device*** .
Add Cameras Linked with Devices to Areas	Group cameras linked with encoding devices to different areas according to the locations of the devices for convenient management.

Procedure	Description
	For details, see ***Add Camera to Area for Current Site*** and ***Add Camera to Area for Remote Site*** .
Set Video Parameters	Set network parameters, picture file format, display parameters, audio parameter, and so on for video security. For details, see ***Set Video Parameters*** .
Configure Recording and Storage	Define the periods during which video recording is activated. And set the storage location for the recorded video footage and the uploaded pictures (e.g., alarm related pictures). For details about configuring recording and storage, see ***Configure Storage and Recording*** .
Start Live View or Playback	Start playing live videos or video footage of cameras. For details, see ***Live View*** or ***Playback*** .

7.2 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.

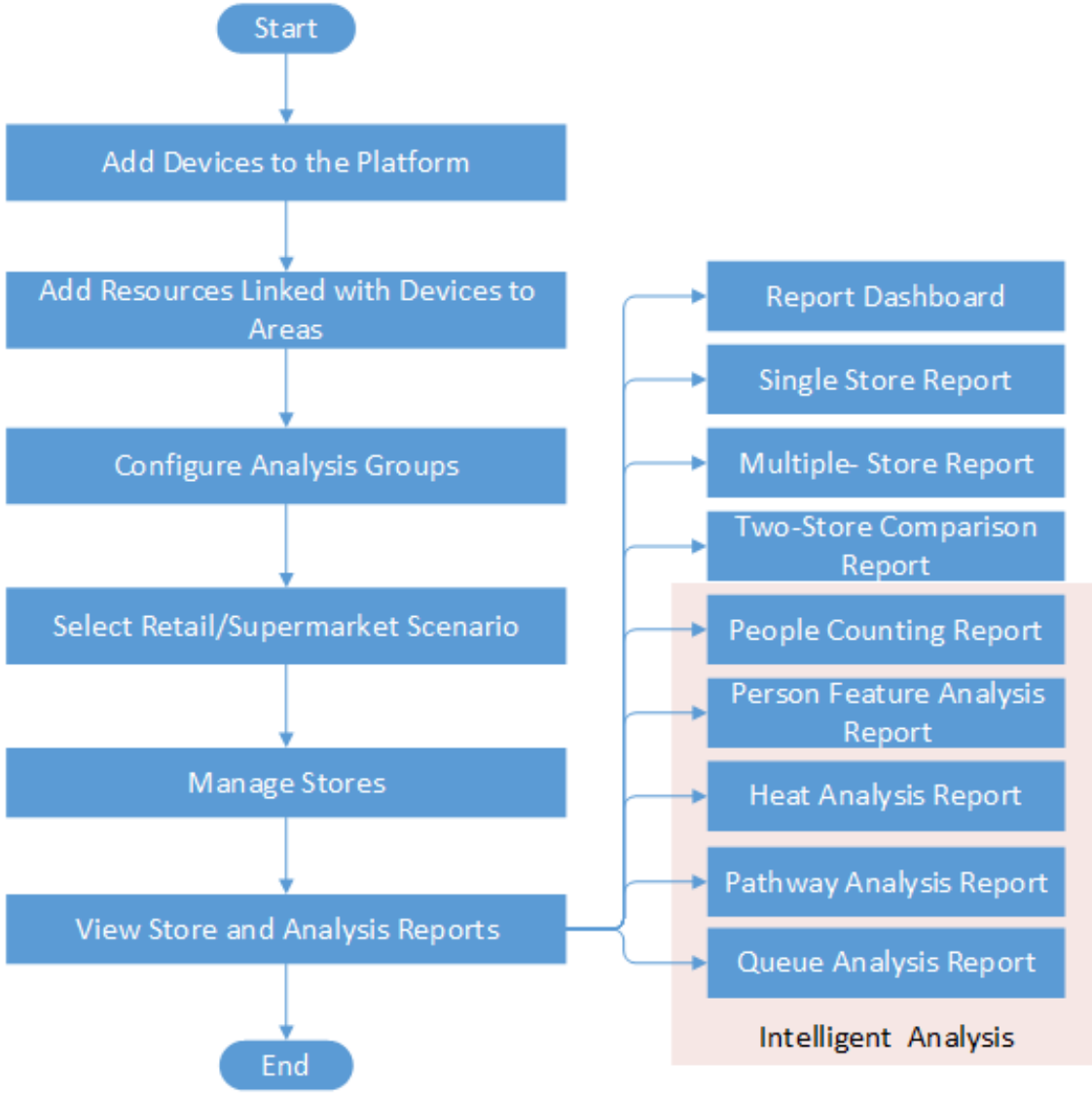


Figure 7-3 Flow Chart of Intelligent Analysis Report in Retail/Supermarket Scenario

Table 7-4 Flow Chart Description

Procedure	Description
Add Devices to the Platform	Add devices that support specific detection functions to the platform by different methods (e.g., online detection, IP address, port segment, device ID) for generating statistics reports. For details, see ***Device and Server Management*** .
Add Resources Linked with Devices to Areas	Group resources linked with devices to different areas according to the locations of the devices for convenient management.

Procedure	Description
	For details, see ***Add Element to Area*** .
Configure Analysis Groups	Group analysis resources of certain regions for calculation. For details, see ***Add People Counting Group*** , ***Add Heat Analysis Group*** , ***Add Person Feature Analysis Group*** , and ***Add Pathway Analysis Group*** .
Select Retail/Supermarket Scenario	The scenario is specially designed for stores. In this scenario, you can view reports of a store or multiple stores. For details, see ***Configure Scenario*** .
Manage Stores	Add stores to the platform and link resources to stores for generating reports of stores. For details, see ***Manage Store*** .
View Store Reports	View store reports of a single store / two stores / multiple stores and store intelligent analysis reports (including people counting reports, person feature analysis reports, heat analysis reports, pathway analysis reports, and queue analysis reports). For details, refer to ***View Store Report*** and ***View Store Intelligent Analysis Report*** .

7.3 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.

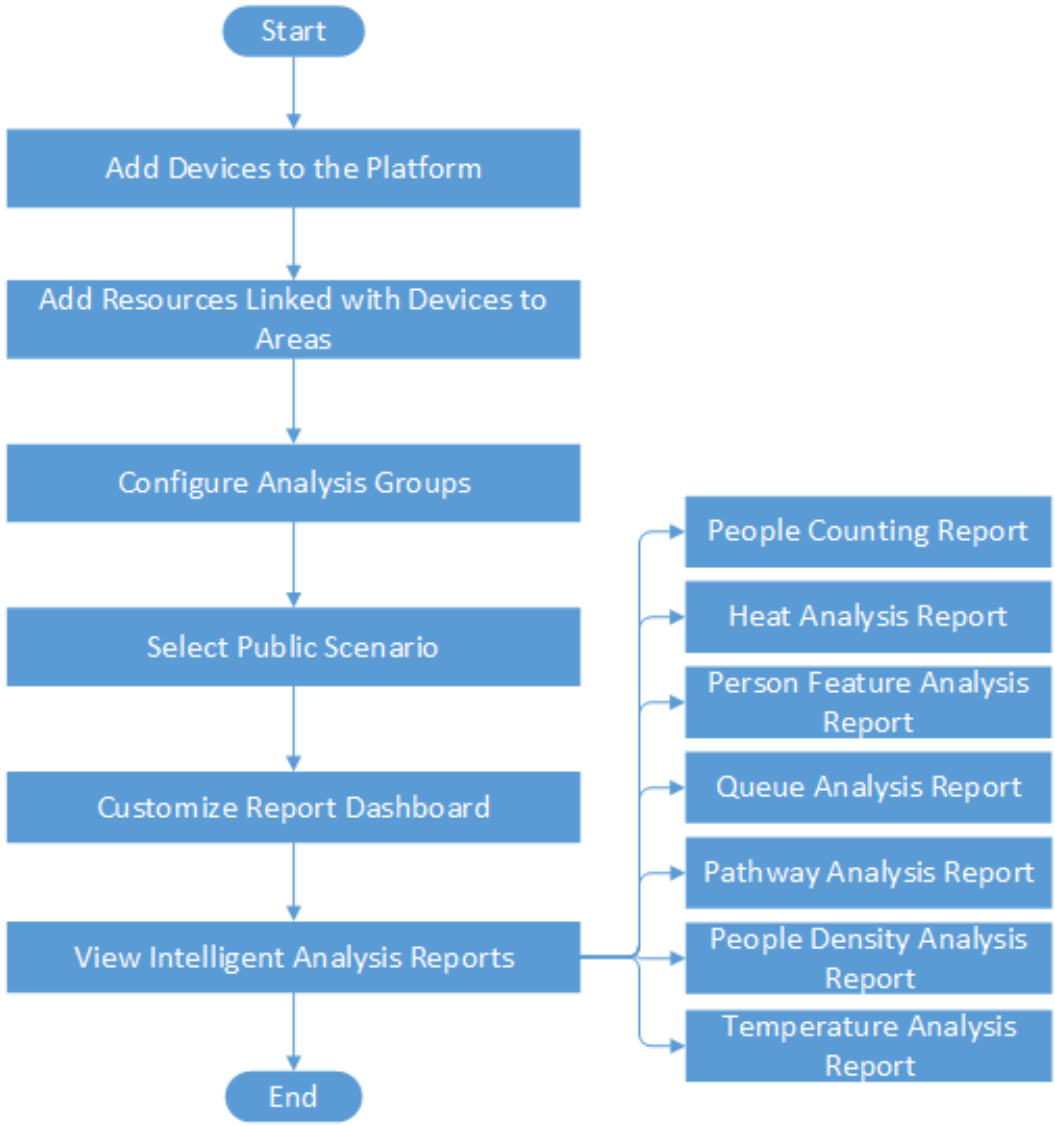


Figure 7-4 Flow Chart of Intelligent Analysis Report in Public Scenario

Table 7-5 Flow Chart Description

Procedure	Description
Add Devices to the Platform	Add devices that support specific detection functions to the platform by different methods (e.g., online detection, IP address, port segment, device ID) for generating statistics reports. For details, see ***Device and Server Management*** .
Add Resources Linked with Devices to Areas	Group resources linked with devices to different areas according to the locations of the devices for convenient management.

Procedure	Description
	For details, see ***Add Element to Area*** .
Configure Analysis Groups	Group analysis resources of certain regions for calculation. For details, see ***Add People Counting Group*** , ***Add Heat Analysis Group*** , ***Add Person Feature Analysis Group*** , and ***Add Pathway Analysis Group*** .
Select Public Scenario	In the 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. For details, see ***Configure Scenario*** .
Customize Report Dashboard	Customize a report dashboard for an at-a-glance view for the public scenario reports. For details, see ***Customize Report Dashboard*** .
View Intelligent Analysis Reports	View people counting reports, person feature analysis reports, heat analysis reports, pathway analysis reports, queue analysis reports, people density analysis reports, and temperature analysis reports. For details, see ***View Intelligent Analysis Report*** .

7.4 Flow Chart of On-Board Monitoring

The flow chart introduces the process of on-board monitoring configuration.

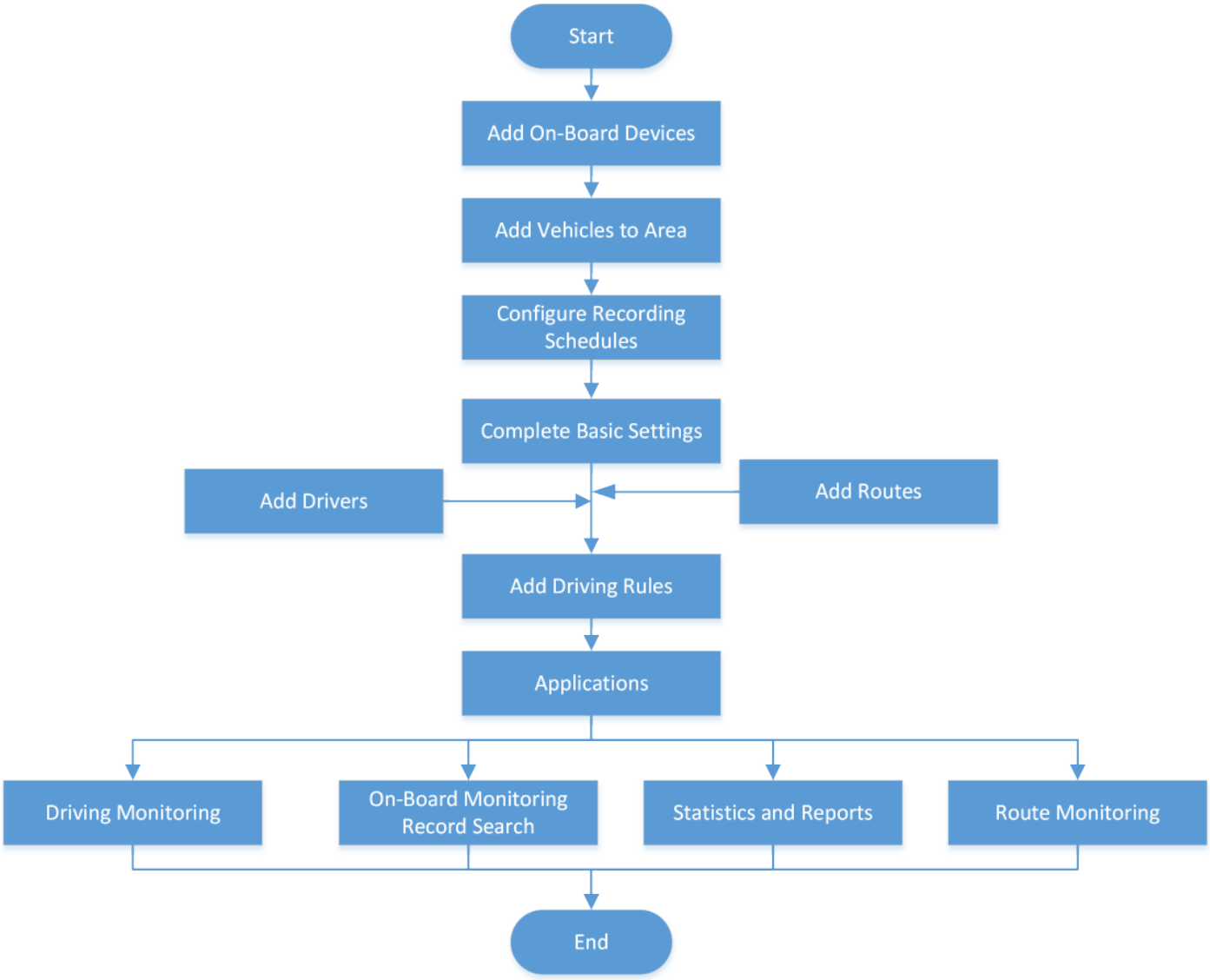


Figure 7-5 Flow Chart of On-Board Monitoring Configuration

7.5 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). Refer to ***Vehicle Management*** for details.

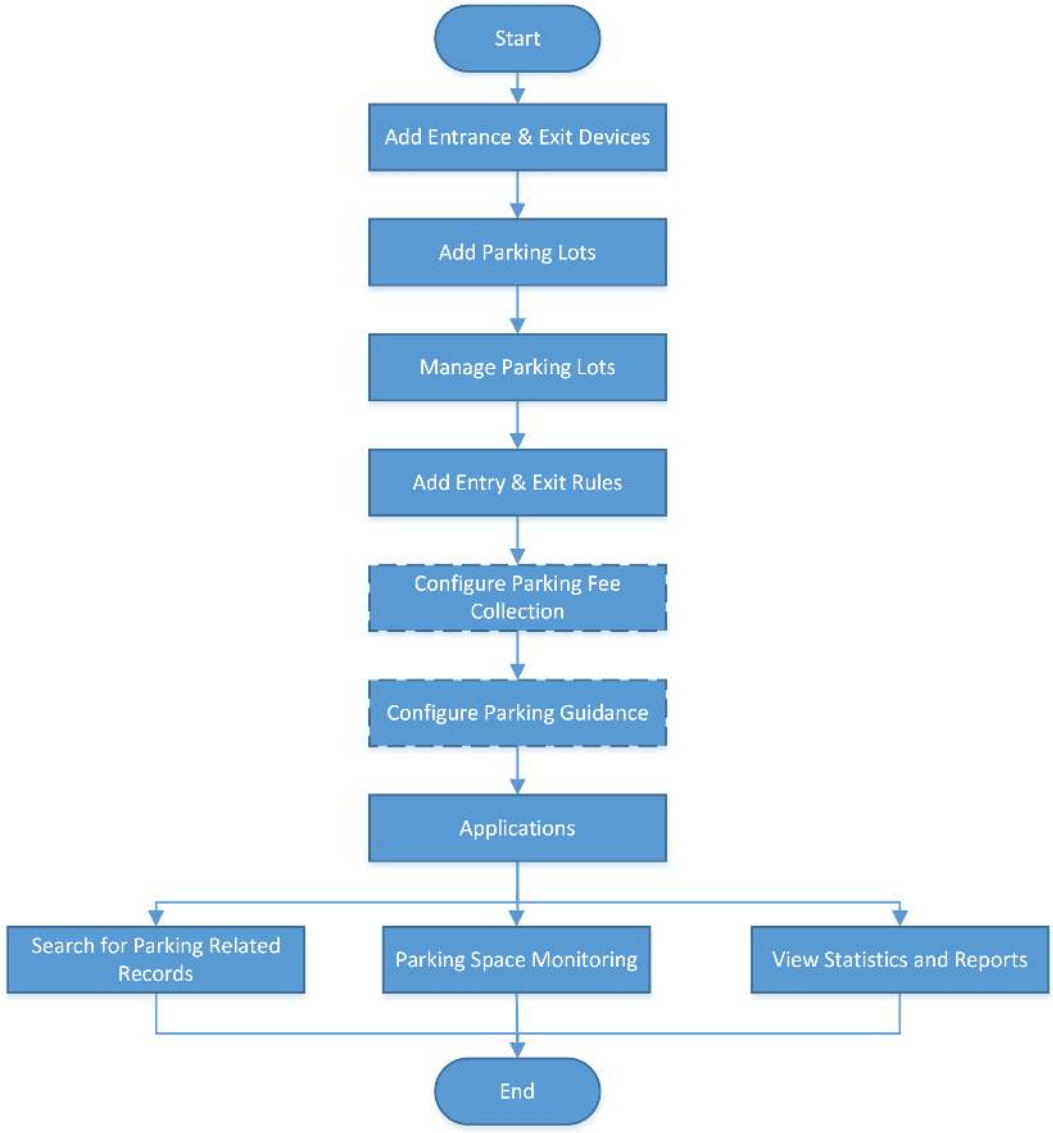


Figure 7-6 Flow Chart of Parking Lot Management

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.

7.6 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). Refer to ***Vehicle Management*** for details.

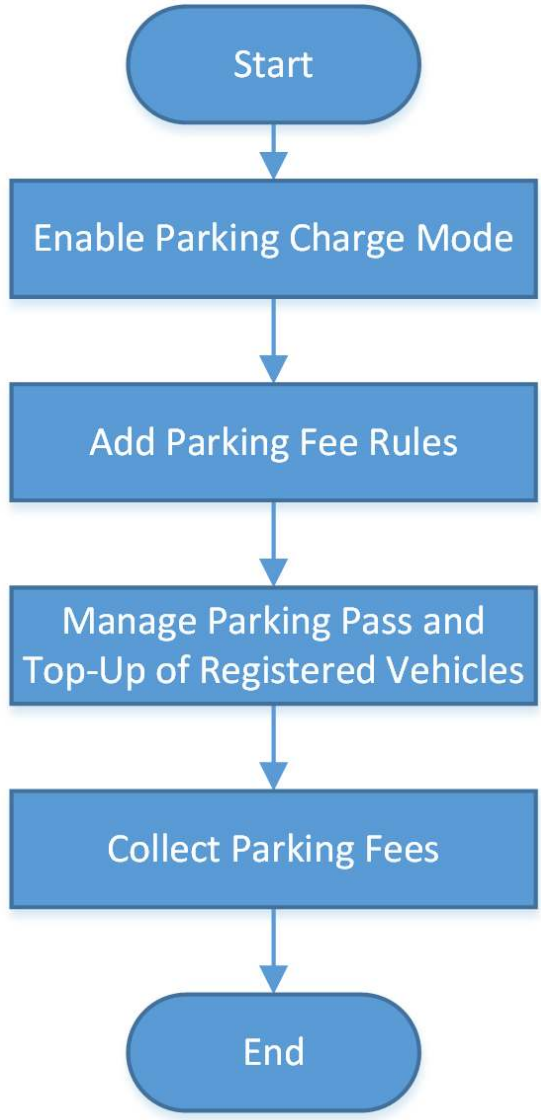


Figure 7-7 Flow Chart of Parking Fee Collection

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 first 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, and the parking fee rule for abnormal entry & exit. Once you set a rule,

Procedure	Description
	the platform will automatically 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 of Registered Vehicles	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.

7.7 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). Refer to ***Vehicle Management*** for details.

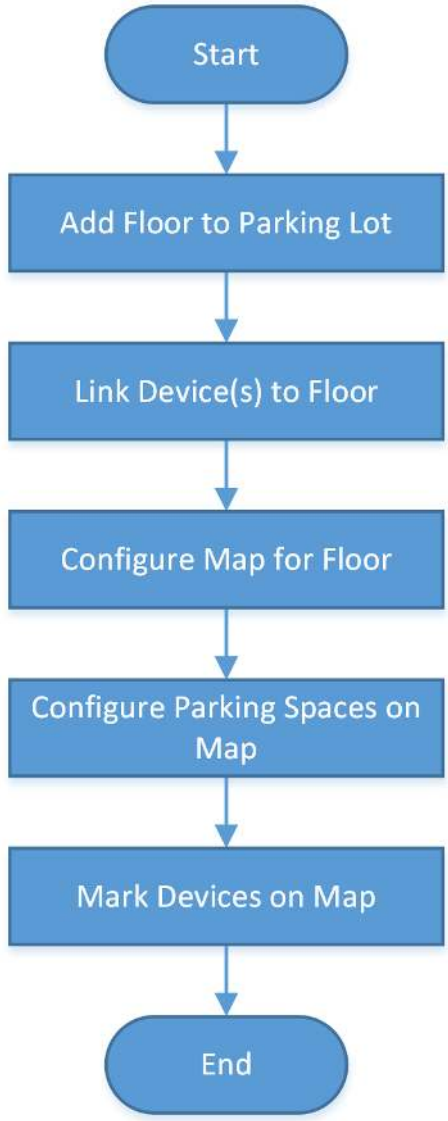


Figure 7-8 Flow Chart of Parking Guidance Configuration

Refer to ***Parking Guidance Configuration*** for details about each step.

7.8 Flow Chart of Door Access Control

The following flow chart shows the process of the configurations and operations of door access control.

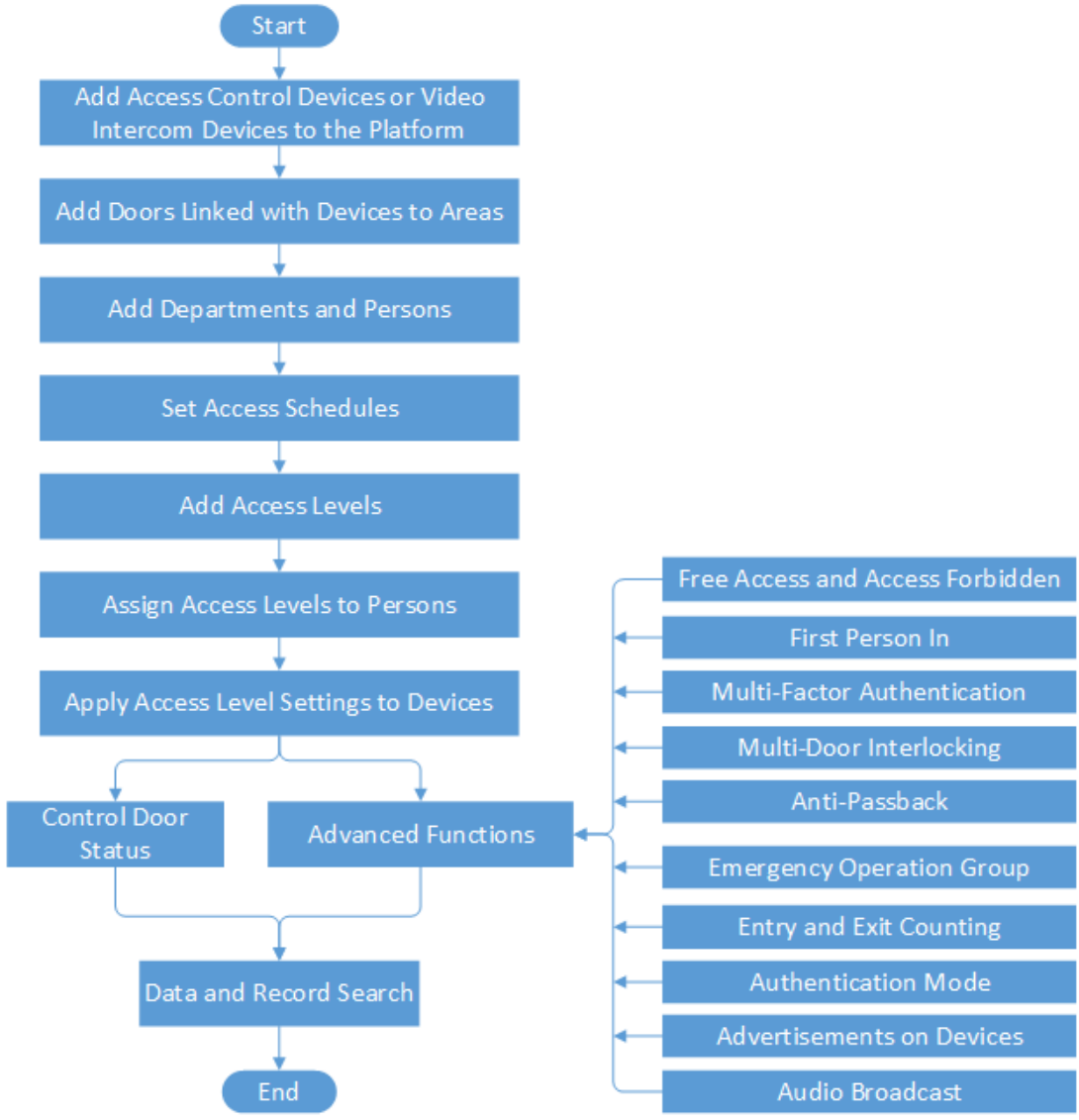


Figure 7-9 Flow Chart of Door Access Control

Note

Some functions in this flow chart need the License. For details about License, refer to ***License Management*** .

Table 7-6 Procedures of Door Access Control

Procedure	Description
Add Access Control Devices or Video Intercom Devices to the Platform	You need to add access control devices and video intercom devices to the system. For details, refer to ***Manage Access Control Device*** and ***Manage Video Intercom Device*** .
Add Doors Linked with Devices to Areas	Group doors linked with added devices for management. Refer to ***Add Door to Area for Current Site*** for details.
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 ***Manage 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*** .
Apply Access Level Settings to Devices	After setting the linkage between the persons and the access level, you need to apply the person's access level settings to the access control device of the doors linked to the access level to take effect. After that, the persons can access these doors during the authorized time period defined by the related access level. For details, refer to ***Apply Persons' Access Levels to Device*** .
Control Door Status	You can manually change the door status to locked, unlocked, remaining locked, or remaining unlocked. Refer to ***Door Control*** for details.
Advanced Functions	Refer to ***Configure Free Access and Access Forbidden Rules*** , ***Configure First Person In Rule*** , ***Configure Multi-Factor Authentication Rule*** , ***Configure Multi-Door Interlocking*** , ***Configure Area Anti-Passback Rules*** , ***Add Emergency Operation Group*** , ***Add Entry and Exit Counting Group*** ,

Procedure	Description
	Configure Authentication Mode , ***Apply Advertisement to Access Control Devices*** , and ***Add Audio Broadcast*** for details.
Data and Record Search	Refer to ***Search Access Records*** and ***Search Data Recorded on Access Control Devices and Elevator Control Devices*** for details.

7.9 Flow Chart of Floor Access Control

The following flow chart shows the process of the configurations and operations of floor access control.

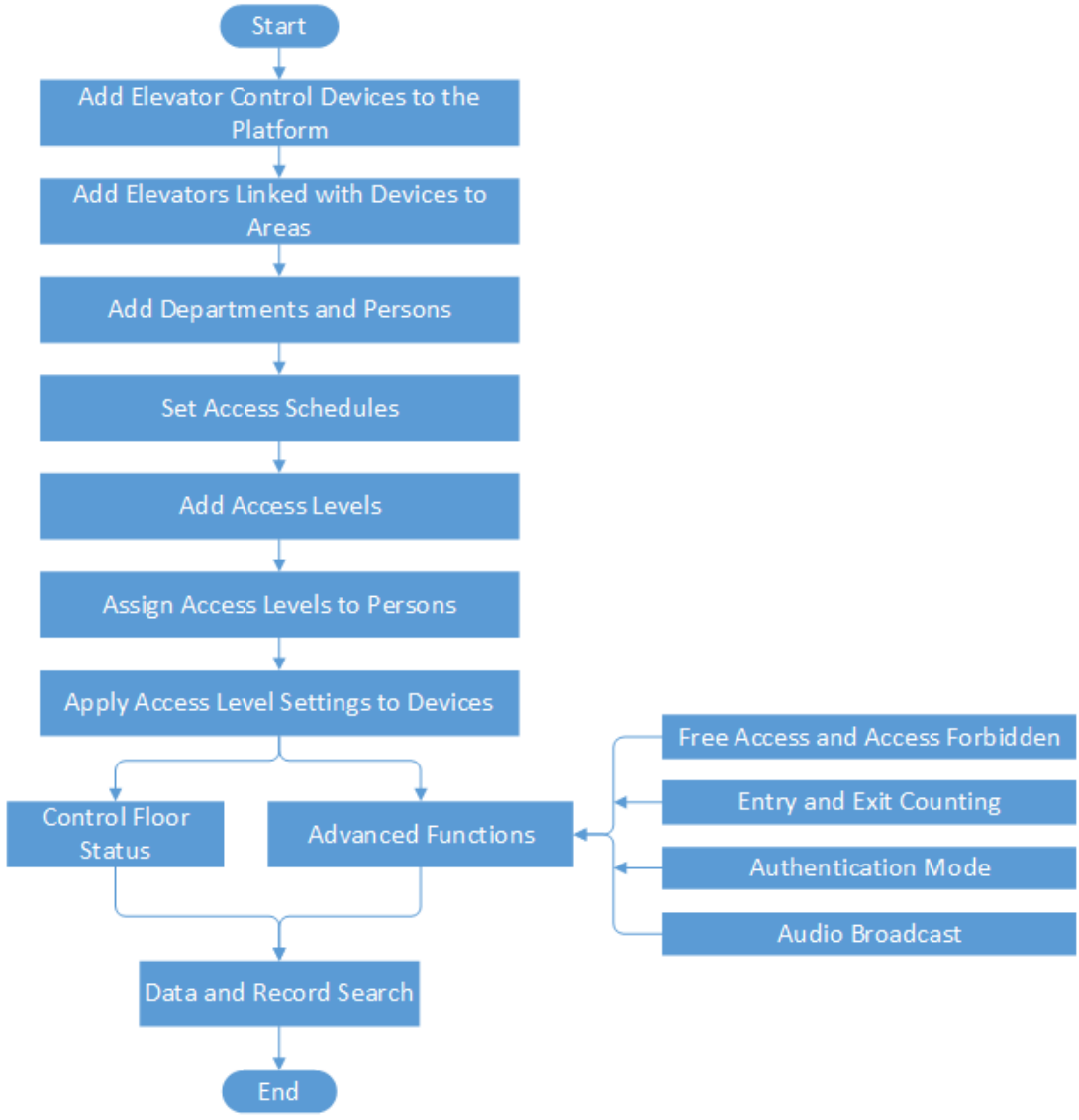


Figure 7-10 Flow Chart of Floor Access Control

Note

Some functions in this flow chart need the License. For details about License, refer to ***License Management*** .

Table 7-7 Procedures of Floor Access Control

Procedure	Description
Add Elevator Control Devices to the Platform	You need to add elevator control devices to the system. For details, refer to ***Manage Elevator Control Device*** .
Add Elevators Linked with Devices to Areas	Group elevators linked with added devices for management. Refer to ***Add Elevator to Area for Current Site*** for details.
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 ***Manage 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*** .
Apply Access Level Settings to Devices	After setting the linkage between the persons and the access level, you need to apply the person's access level settings to the elevator control device 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. For details, refer to ***Apply Persons' Access Levels to Device*** .
Control Floor Status	You can manually change the floor status to temporary access, access with credential, free access, or access forbidden. Refer to ***Elevator Control*** for details.
Advanced Functions	Refer to ***Configure Free Access and Access Forbidden Rules*** , ***Add Entry and Exit Counting Group*** , ***Configure Authentication Mode*** , and ***Add Audio Broadcast*** for details.
Data and Record Search	Refer to ***Search Access Records*** and ***Search Data Recorded on Access Control Devices and Elevator Control Devices*** for details.

7.10 Flow Chart of Visitor Management

The flow chart below shows the process of visitor settings management.

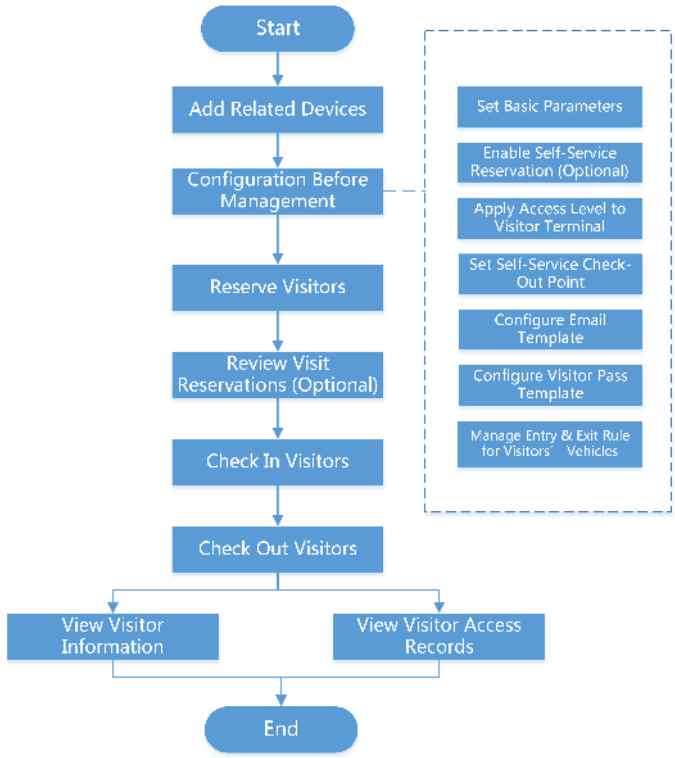


Figure 7-11 Flow Chart of Visitor Management

Table 7-8 Flow Chart Description

Procedure	Description
Add Related Devices	Add devices used for visitor reservation, check-in, check-out, authentication, etc. See ***Manage Visitor Terminals*** , ***Manage Access Control Device*** , and ***Manage Elevator Control Device*** for details.
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 ***Configurations Before Visitor Management*** 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*** .

Procedure	Description
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 the visitor information to approve or disapprove the reservation. See ***Visitor Reservation*** for details.
Visitor Check-In	The platform supports checking in visitors both with or without a reservation. See ***Check In a Visitor Without Reservation*** and ***Check In a Reserved Visitor*** for details.
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.
View and Delete Visitors	View all checked-in visitors (including those who have checked out) in the visitor list and perform other operations such as deleting visitors. See ***View Visitor Information*** for details.
Check Visitor Records	Filter and check visitor records. See ***Check Visitor Access Records*** .

7.11 Flow Chart of Time and Attendance

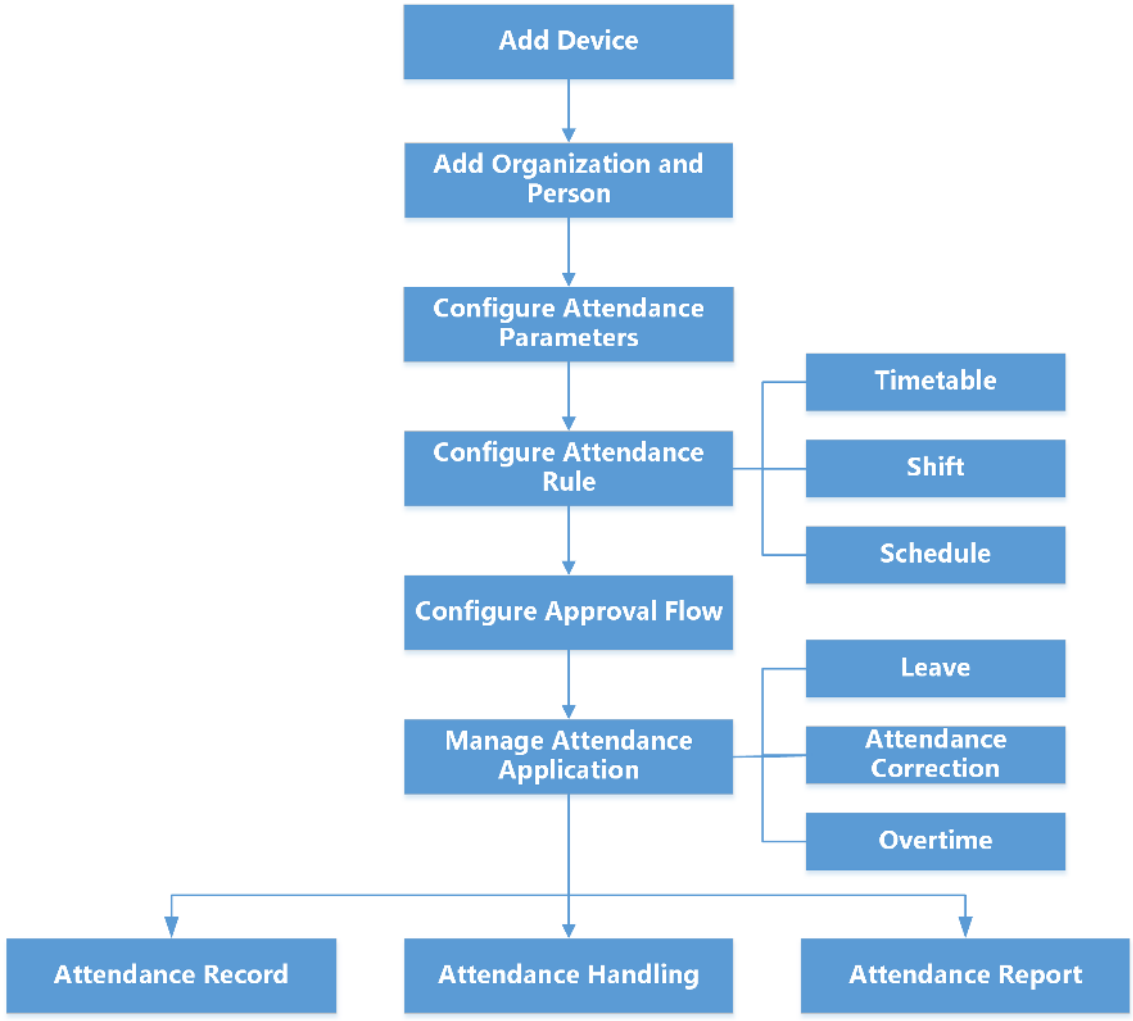


Figure 7-12 Flow Chart of Time & Attendance

- **Add Device**: Add devices (e.g., access control devices) to the platform. For more details, refer to ***Device and Server Management*** .
- **Add Organization and Person**: Add departments, attendance group, and persons. For more details, refer to ***Add Departments*** , ***Add an Attendance Group*** , and ***Add Person*** .
- **Configure Attendance Parameters**: Configure attendance check points, general rule, overtime rule, leave types, check-in/check-out via Mobile Client, display rule for report, third-party database, etc. For more details, refer to ***Configure Attendance Rules for Global / Department / Attendance Group*** , ***Configure Check-In/Check-Out via Mobile Client*** , ***Set Display Rules for Attendance Report*** , and ***Synchronize Card Swiping Records to Third-Party Database*** .
- **Configure Attendance Rule**: Add timetable (including break timetable and work timetable), shift, and schedule. For more details, refer to ***Add Timetable*** , ***Add Shift*** and ***Manage Schedule*** .
- **Configure Approval Flow**: Configure approval roles and application flows for departments / attendance groups / persons. For more details, refer to ***Approval Management*** .

- **Manage Attendance Application**: Manage applications for employees and admins. For more details, refer to ***Application Management for Employee*** and ***Application Management for Admin*** .
- **Attendance Record**, **Attendance Handling**: Search and correct attendance records, apply for leave, get devices' attendance records, manually calculate attendance results, etc. For more details, refer to ***View Attendance Records*** .
- **Attendance Report**: Export attendance report to local PC or send it via email regularly. For more details, refer to ***Manage Attendance Reports*** .

7.12 Flow Chart of Video Intercom

For the first time, you can follow the flow chart to perform configurations and operations.

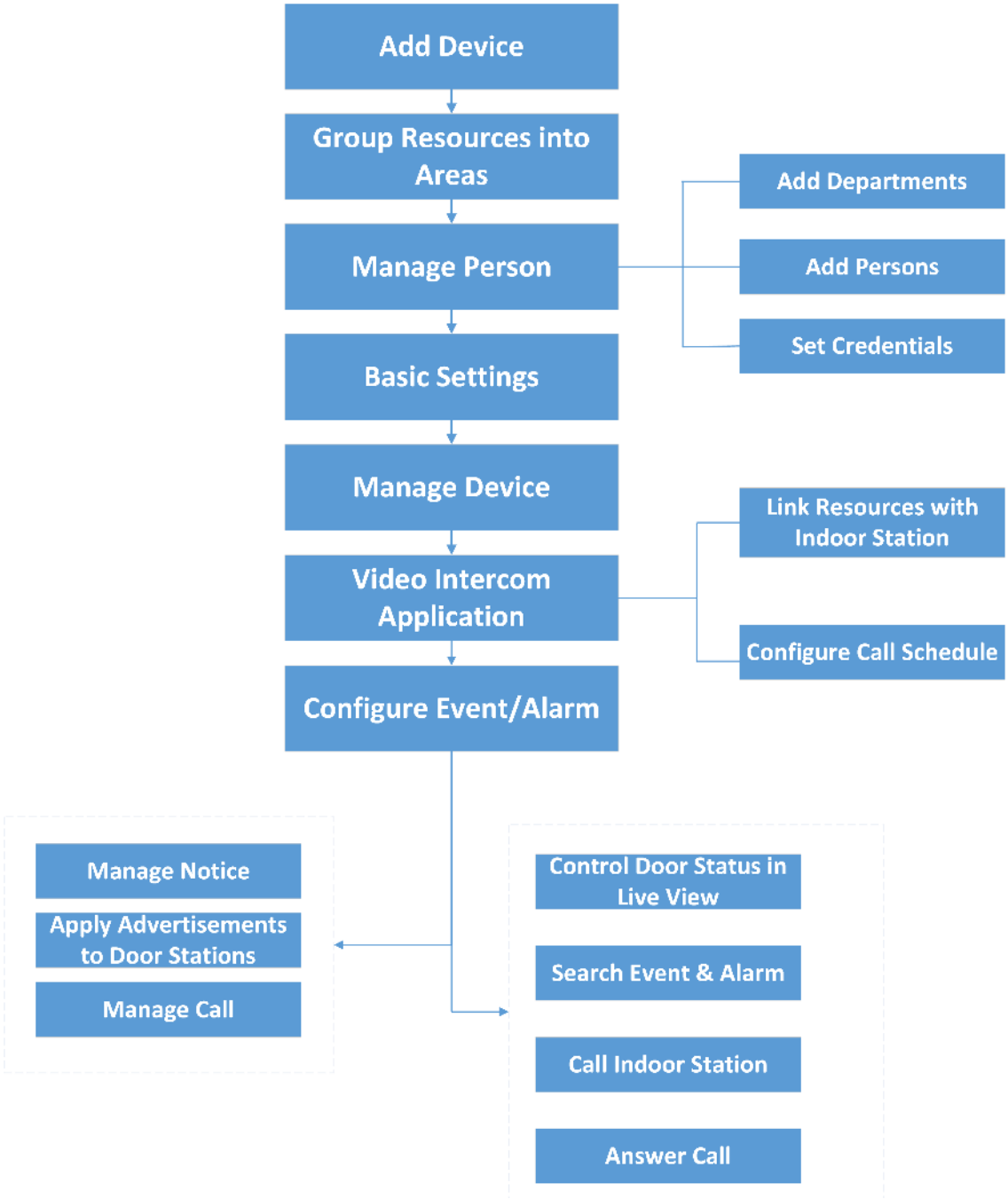


Figure 7-13 Flow Chart of Video Intercom

- **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. For more details, refer to ***Manage Video Intercom Device*** and ***Configure Device Parameters*** .
- **Group Resources into Areas**: After adding the devices to the system, you need to group the devices' resources (such as doors and cameras) into different areas according to the resources' locations. For details, refer to ***Area Management*** .
- **Manage Person**: Add departments and persons to the system, and set credential information. For details, refer to ***Person Management*** .
- **Basic Settings**: Add call recipients, add call schedule templates, add receiving schedule template, and configure call parameters. For details, refer to ***Basic Settings of the Platform*** .
- **Manage Device**: Set location information for video intercom devices and apply the settings to devices. For details, refer to ***Manage Video Intercom Device*** .
- **Video Intercom Application**: Add call schedules and apply them to devices, link resources (camera, person, and doorbell) to indoor stations. For details, refer to ***Video Intercom Application*** .
- **Configure Event / Alarm**: Configure event and alarm for video intercom resources. For more details, refer to ***Event and Alarm*** .
- **Manage Notice**: Add notices and apply them to indoor stations. For details, refer to ***Manage Notices*** .
- **Apply Advertisements to Door Stations**: Apply pictures or video to door stations as advertisements. See ***Apply Advertisements to Door Stations*** .
- **Manage Call**: Call indoor stations and view recents. Fore details, refer to ***Call & Talk*** .
- **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. For more details about related configurations and operations of the doors, refer to ***Flow Chart of Door Access Control*** .

7.13 Flow Chart of Alarm Detection

The following flow chart shows the process of the configurations and operations of alarm detection.

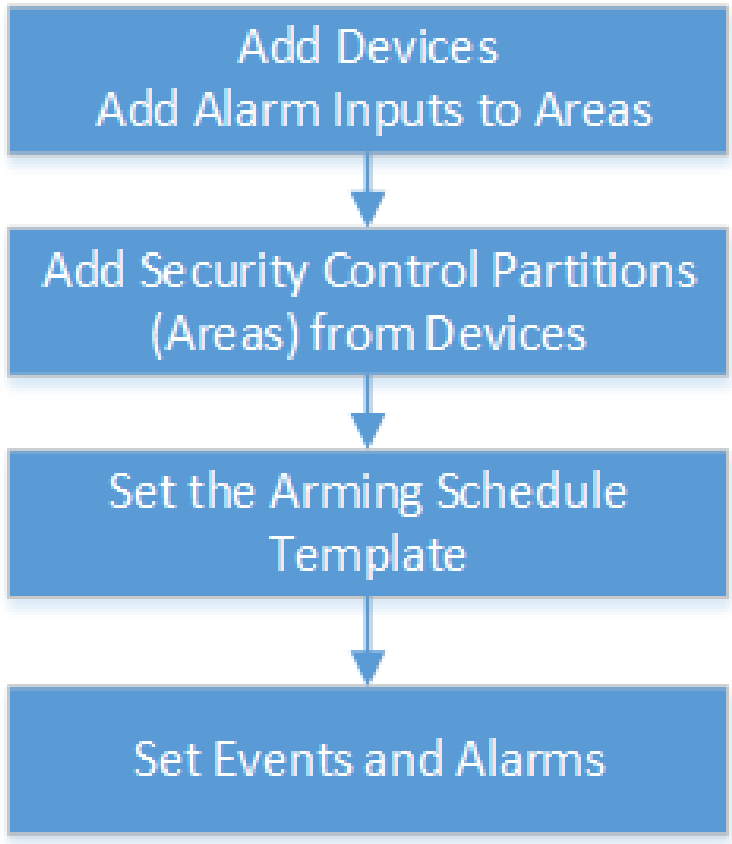


Figure 7-14 Flow Chart of Alarm Detection

- **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. Refer to ***Manage Security Control Device*** and ***Add Alarm Input to Area for Current Site*** for details.
- **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.

7.14 Flow Chart of Digital Signage Management

You can follow the flow chart below for using the digital signage module for the first time.

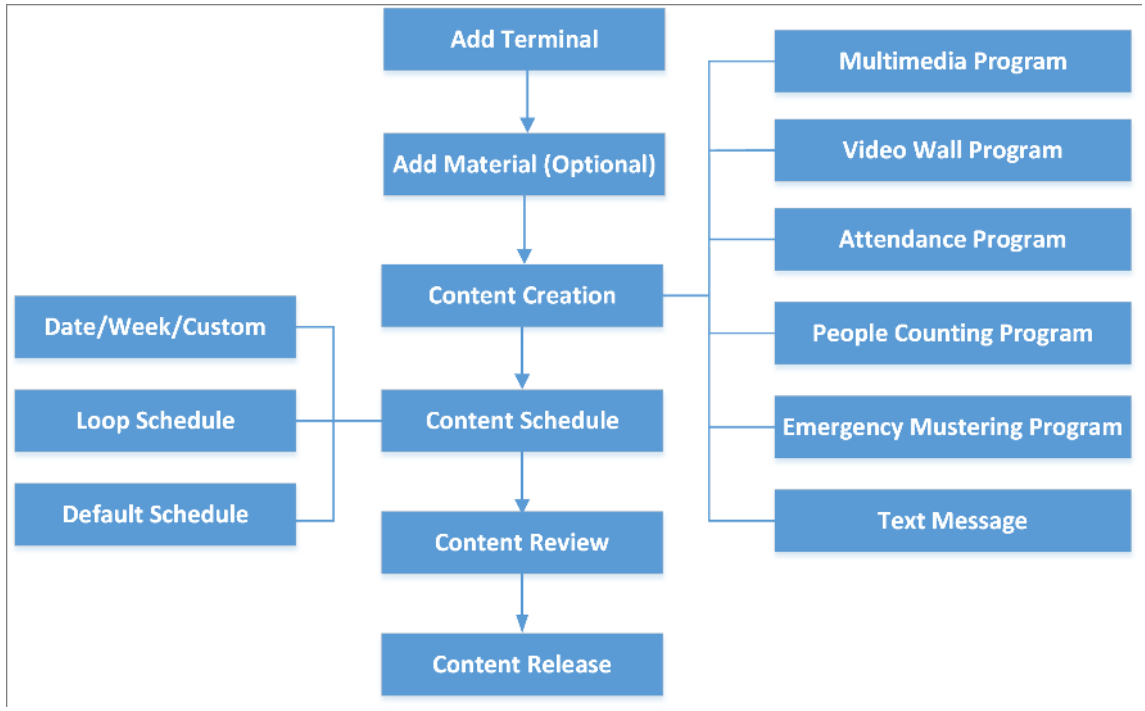


Figure 7-15 Flow Chart of Digital Signage Management

- **Add Terminal**: You should add digital signage terminals to the platform. For details, refer to ***Manage Digital Signage Terminals*** .
- **Add Material**: Material is used for creating programs. You can upload local materials from local PC, or create dynamic materials in the platform. For details, refer to ***Material Library*** .
- **Content Creation**: You can create different contents including multimedia program, video wall program, attendance program, people counting program, and so on in the platform according to the required application scenarios. For details, refer to ***Content Creation*** .
- **Content Schedule**: You should define a playing schedule for the added programs, which will then be played according to the scheduled time or method on the terminals. For details, refer to ***Schedule Management*** .
- **Content Review**: The added contents should be approved before they are used. For details, refer to ***Content Review*** .
- **Content Release**: You can view the release details and release progress of multiple tasks. After being released, the related task can take effect on the terminals. For details, refer to ***Content Release*** .

7.15 Flow Chart of Interactive Flat Panel Management

You can follow the flow chart below for using the interactive flat panel module for the first time.

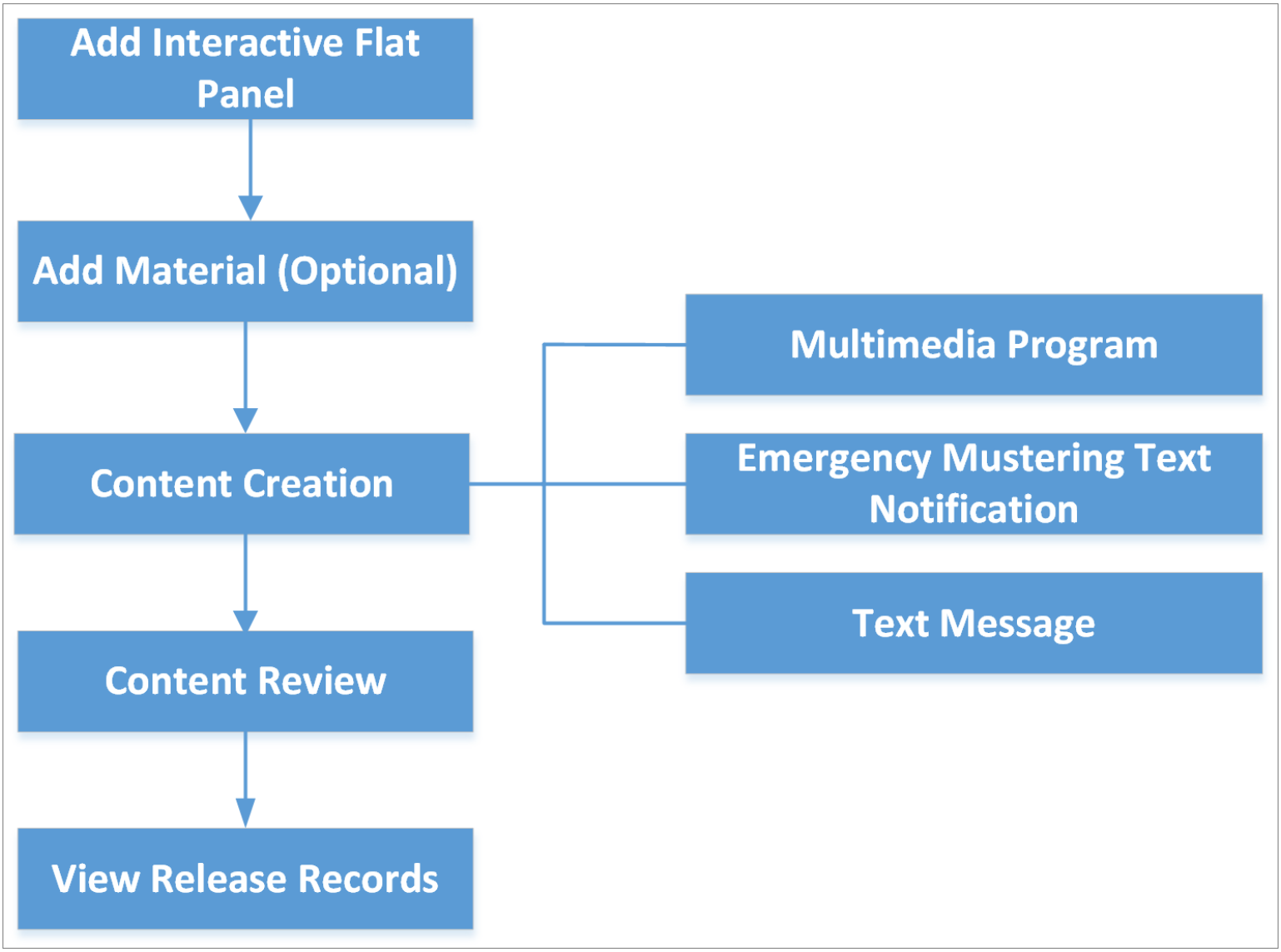


Figure 7-16 Flow Chart of Interactive Flat Panel Management

- **Add Interactive Flat Panel**: You should add interactive flat panels to the platform. For details, refer to ***Manage Interactive Flat Panel*** .
- **Add Material**: Material is used for creating multimedia programs. You can upload local materials from local PC, or create dynamic materials in the platform. For details, refer to ***Material Library*** .
- **Content Creation**: You can create contents such as multimedia program and text message in the platform according to the required application scenarios. For details, refer to ***Content Creation*** .
- **Content Review**: The added contents should be reviewed before they are used. For details, refer to ***Content Review*** .
- **View Release Records**: After the contents are reviewed, they will be released to the interactive flat panels automatically. And you can view release records of all the tasks and the details of their release status. For details, refer to ***View Release Records*** .

7.16 Flow Chart of Patrol Management

The flow chart below shows the process of configuring and managing patrols.

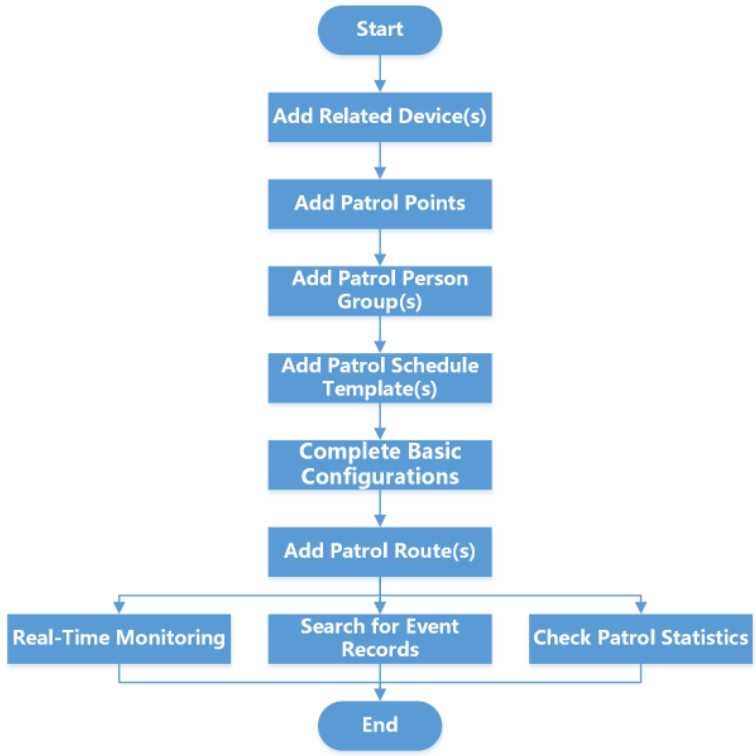


Figure 7-17 Flow Chart of Patrol Management

Table 7-9 Flow Chart Description

Step	Description
Add Related Device(s)	Add devices used for adding patrol points, real-time monitoring, etc. See ***Manage Access Control Device*** and ***Manage Encoding Device*** for details.
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.

Step	Description
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.
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.

Chapter 8 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.

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.

8.1 Activate License - Online

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

Steps

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client (Administrator)*** .
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Online Activation** to activate the License in online mode.

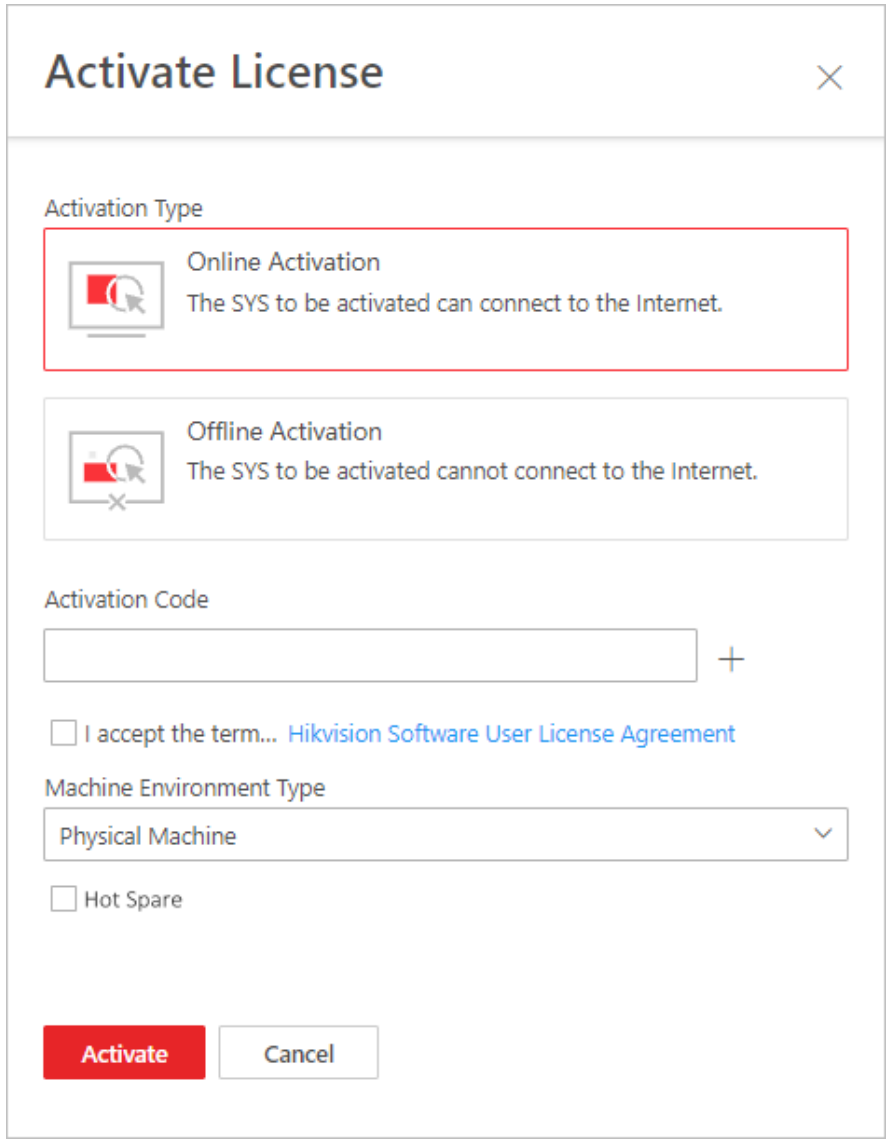


Figure 8-1 Activate License in Online Mode

4. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
6. **Optional:** Select the machine environment type.

   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.

Note

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.

7. **Optional:** Check the **Hot Spare**, select type, and enter the IP address if you want to build a hot spare system.

Note

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

8. Click **Activate**.

The email settings pane will appear after you activated the License.

9. Enter an email address for the admin user.

Note

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.

10. Set the email server parameters. See details in ***Configure Email Account*** .
11. Click **OK** to save the email settings.

8.2 Activate License - Offline

If the SYS to be activated cannot connect to the Internet, you can activate the License in offline mode.

Steps

1. Log in to HikCentral Professional via the Web Client.
2. On the Home page, click **Activate** to open the Activate License panel.
3. Click **Offline Activation** to activate the License in offline mode.

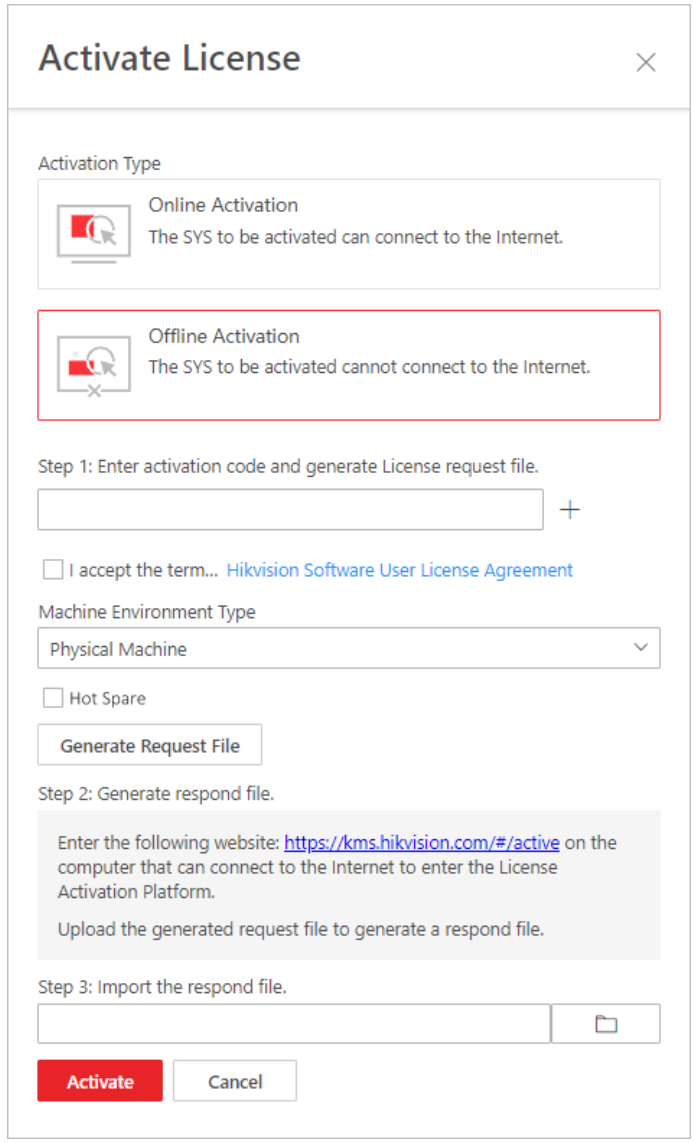


Figure 8-2 Activate License in Offline Mode

4. Enter the activation code received when you purchased your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

5. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
6. **Optional:** Select the machine environment type.

   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.

Note

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.

7. **Optional:** Check the **Hot Spare**, select type, and enter the IP address if you want to build a hot spare system.

Note

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

8. 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).

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

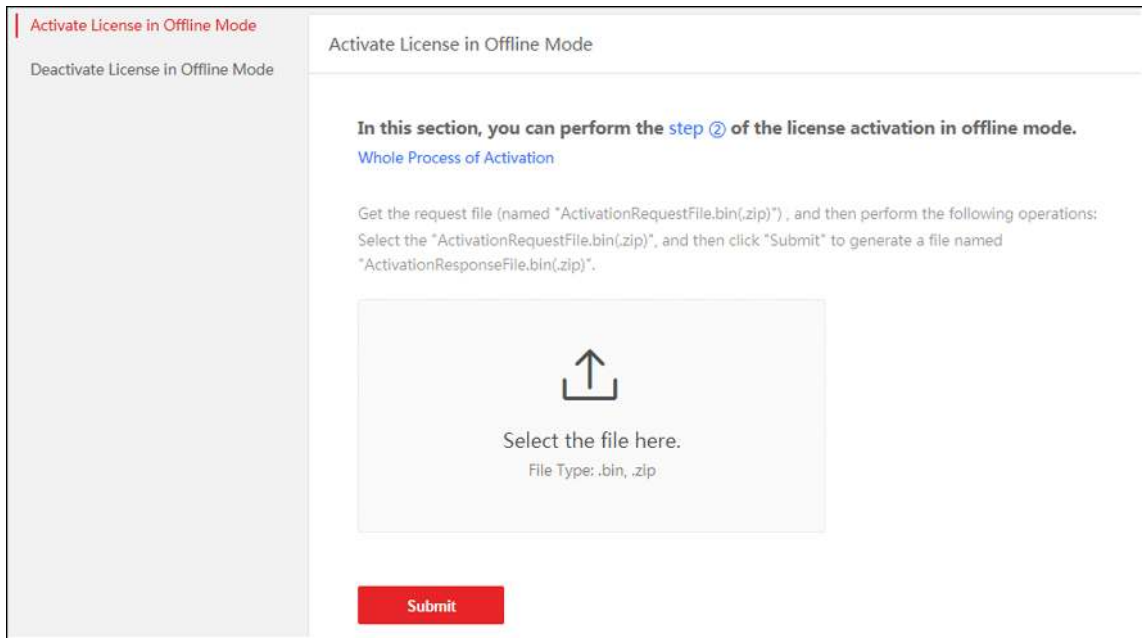


Figure 8-3 Select Request File

12. Click **Submit**.

    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).
13. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
14. In the Offline Activation panel, click and select the downloaded respond file.
15. Click **Activate**.

    The email settings pane will appear after you activated the License.
16. Enter an email address for the admin user.

    Note

    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.
17. Set the email server parameters. See details in ***Configure Email Account*** .
18. Click **OK** to save the email settings.

8.3 Update License - Online

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.

Before You Start

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

Steps

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client (Administrator)*** for details.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License pane.
4. Click **Online Update** to update the License in online mode.
5. Enter the activation code received when you purchase your License.

Note

- If you have purchased more than one Licenses, you can click + and enter other activation codes.
- The activation code should contain 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. Click **Update**.

8.4 Update License - Offline

As your project grows, you may need to increase the connectable number of devices for your HikCentral Professional. If the SYS to be updated cannot connect to the Internet, you can update the system in offline mode.

Before You Start

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

Steps

1. Log in to HikCentral Professional via the Web Client.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Update License** in the drop-down menu to open the Update License pane.
4. Click **Offline Update** to update the License in the offline mode.

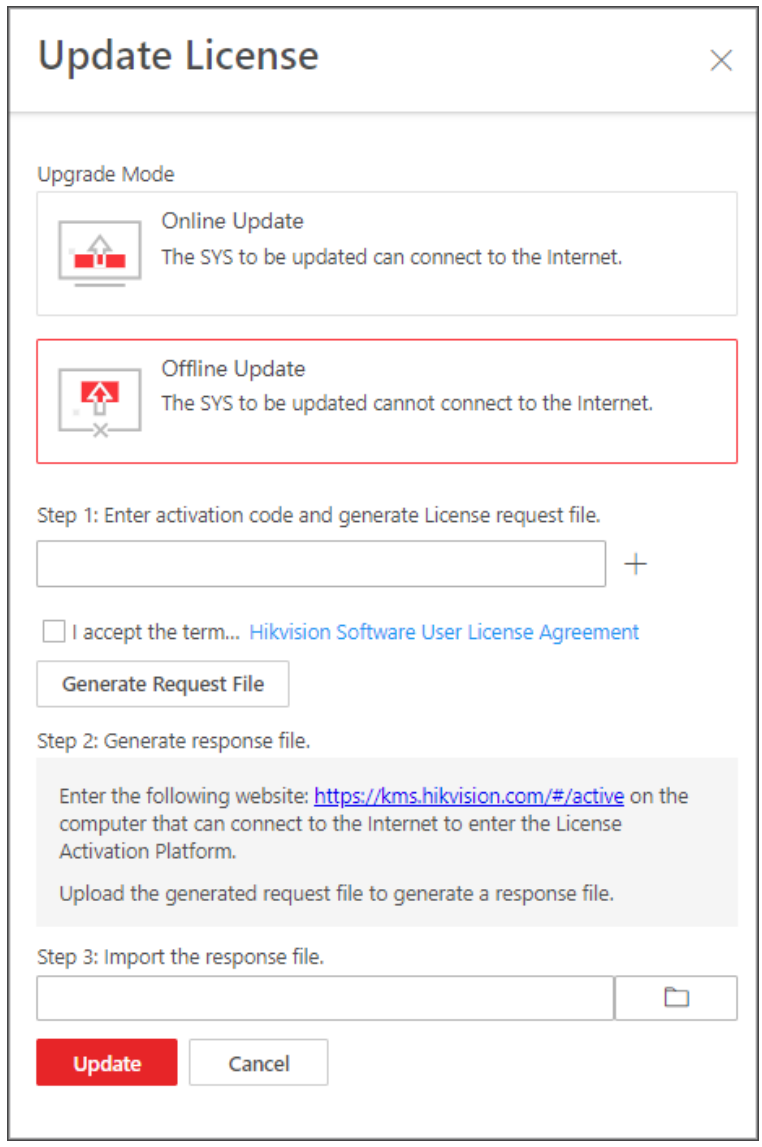


Figure 8-4 Update License in Offline Mode

5. Enter the activation code of your additional License.

Note

- If you have purchased more than one License, you can click + and enter other activation codes.
- The activation code should contain 16 characters or 32 characters (except dashes).

6. Check **I accept the terms of the agreement** to open the License Agreement panel and click **OK**.
7. 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).
8. Copy the request file to the computer that can connect to the Internet.

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

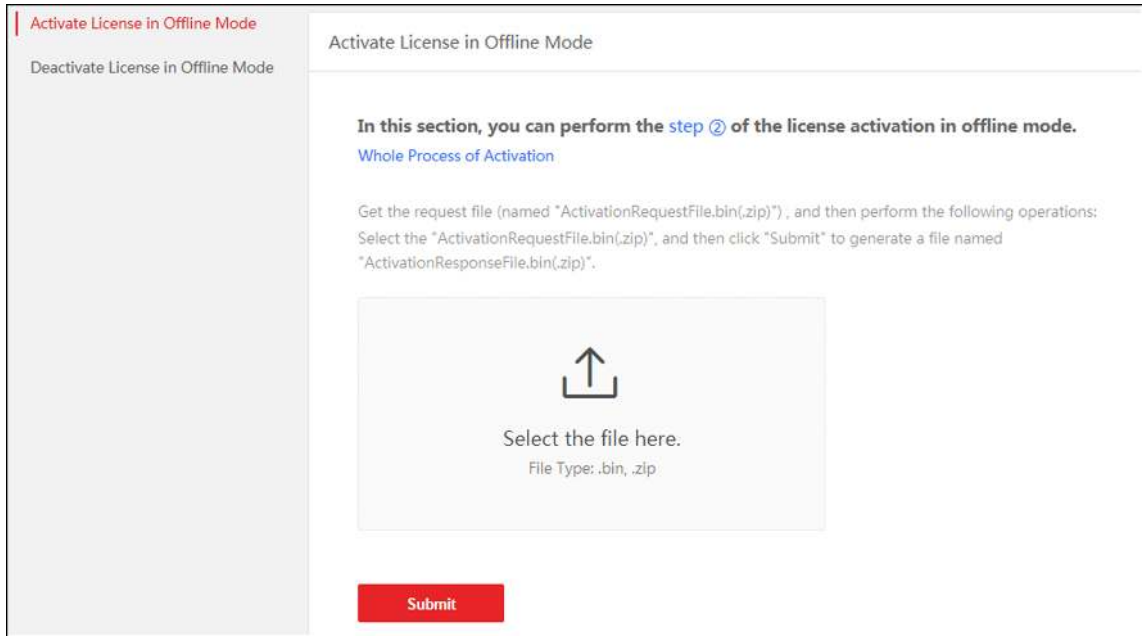


Figure 8-5 Select Request File

11. Click **Submit**.

    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).
12. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
13. In the offline update panel, click and select the downloaded respond file.
14. Click **Update**.

8.5 Deactivate License - Online

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 SYSrunning can properly connect to the Internet, you can deactivate the License in online mode.

Steps

1. Log in to HikCentral Professional via the Web Client. Refer to ***Login via Web Client (Administrator)*** .
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License panel.
4. Click **Online Deactivation** to deactivate the License in online mode.

5. Check the activation code(s) to be deactivated.
6. Click **Deactivate**.

8.6 Deactivate License - Offline

If you want to run the SYS on another computer or server, you should deactivate the SYS first and then activate the SYS again. If the SYS to be deactivated cannot connect to the Internet, you can deactivate the License in offline mode.

Steps

1. Log in to the HikCentral Professional via Web Client.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **Deactivate License** in the drop-down menu to open the Deactivate License pane.
4. Click **Offline Deactivation** to deactivate the License in offline mode.

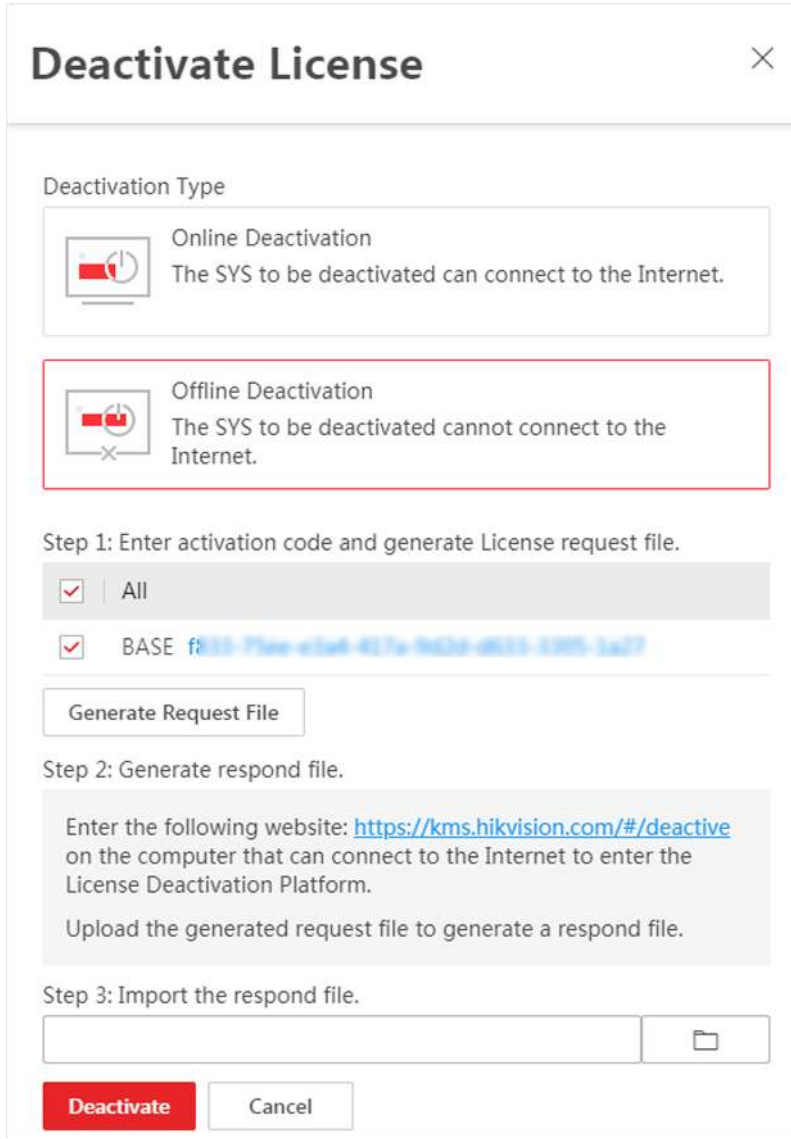


Figure 8-6 Deactivate License in Offline Mode

5. Check the activation code(s) to be deactivated.
6. Click **Generate Request File**.

Note

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).

7. Copy the request file to the computer that can connect to the Internet.
8. On the computer which can connect to the Internet, enter the following website: ***https://kms.hikvision.com/#/deactive*** .

9. Click and then select the downloaded request file.

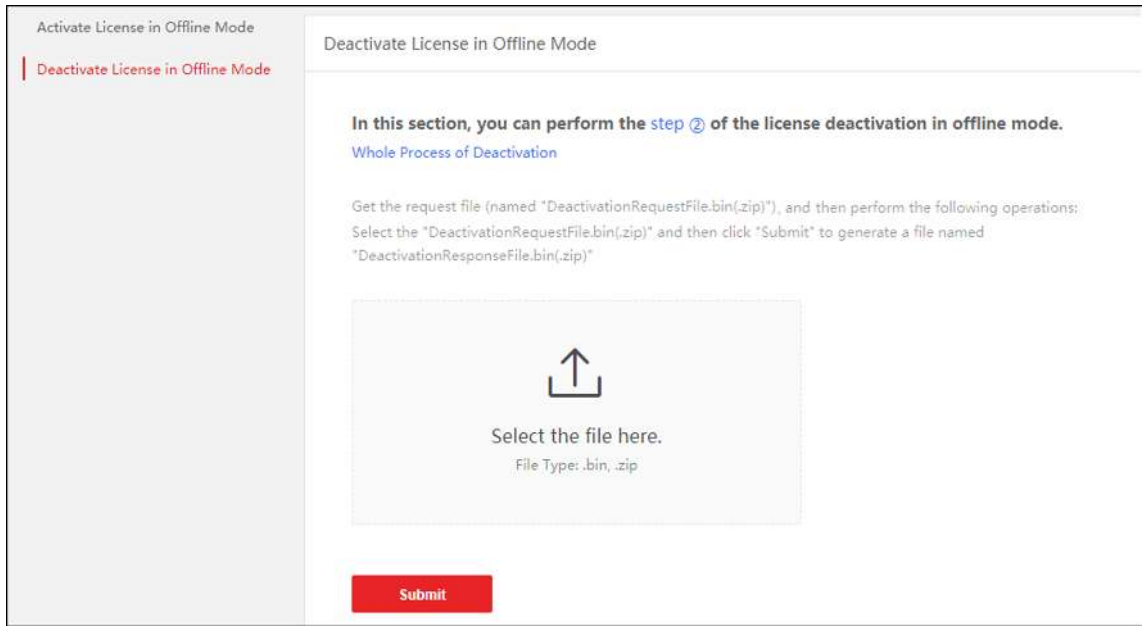


Figure 8-7 Select Request File

10. Click **Submit**.

    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).
11. Copy the respond file to the proper directory of the computer that accesses HikCentral Professional via the Web Client.
12. In the Offline Deactivation pane, click and select the downloaded respond file.
13. Click **Deactivate**.

8.7 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.

Steps

1. Log in to the HikCentral Professional via Web Client. See ***Login via Web Client (Administrator)*** for details.
2. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.
3. Click **License Details** in the drop-down menu to open the License Details pane.

   You can view the authorization details and check the expiry date of the trial License or the License you purchased.

4. **Optional:** Click › beside **Cameras (Exclude Cameras Imported from Remote Site)** to show the number of ANPR cameras / facial and human body recognition cameras / thermal cameras (report supported) / Open Network Video Interface cameras / cameras from Hik-Partner Pro / Dahua cameras / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, and click **Configuration** to select the added cameras as these types of cameras respectively.

Note

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

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

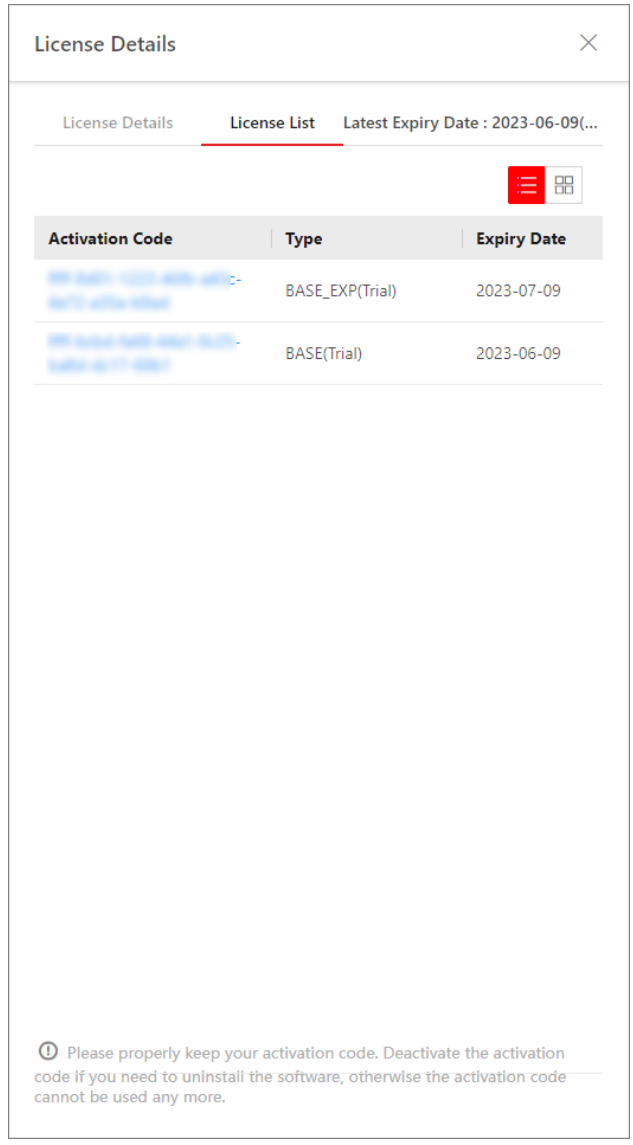


Figure 8-8 License List Page

8.8 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.

Steps

1. On the top, move the cursor to **Maintenance and Management** to show the drop-down menu.

2. Click **License Details** in the drop-down menu to open the License Details pane.
3. Go to the bottom of details list and click to enter the SSP Expiration Prompt Settings pane.
4. Set the **Overdue Reminder** switch to ON.
5. 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.

6. 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).

7. 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).

8. Click **Save**.

Chapter 9 Device and Server Management

HikCentral Professional supports multiple device or server types, such as encoding device, access control device, Remote Site, decoding device and Smart Wall. After adding them to the platform, you can manage them, configure required settings and perform further operations. For example, you can add encoding devices for live view, playback, recording settings, event configuration, etc., add access control devices for access control, time and attendance management, etc., add remote sites for central management of multiple systems, add recording servers for storing the videos, add streaming servers for getting the video data stream from the server, and add smart walls for displaying decoded video on smart wall.

9.1 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.

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 HikCentral Professional via network.
- This function should be supported by the device. Make sure the devices you want to activate support this function.

Steps

1. On the top, select **Device**.
2. Select **Device and Server** on the left.
3. Select the device to be activated.
4. In the Online Device area, view the device status and select one or multiple inactive devices.
5. Click **Activate** to open the device activation window.
6. Create a password in the password field, and confirm the password.

Caution

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

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

7. 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.

8. 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*** .

9.2 Edit Online Device's Network Information

The online devices, which have IP addresses in the same local subnet with SYS server 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 top, select **Device**.
2. Select **Device and Server** on the left.
3. Select the device type.
4. 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.
5. View the device status, and click in the Operation column of an active device.
6. Edit the device parameters, such as IP address, device port, HTTP port, subnet mask, and gateway.

Note

- If you have switched on **Used DHCP**, you can only edit the device port No.
- The parameters may vary for different device types.

7. Click .
8. Enter the device's password.
9. Click **Save**.

9.3 Manage Encoding Device

The encoding devices (e.g., camera, NVR, DVR) can be added to the system for management, including editing and deleting the devices, remote configuration, changing online devices' password, etc. You can also perform further operations based on the added devices, such as live view, video recording, and event settings,

9.3.1 Add Detected Online Encoding Devices

The system can perform an automated detection for available encoding devices in the network where the Web Client or server is located, which makes the devices' information about themselves (e.g., IP address) recognized by the system. Based on the information, you can add the devices quickly.

You can add one online devices at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add a Detected Online Encoding Device

For the detected online encoding devices, you can add the device one by one to HikCentral Professional by specifying its user name, password and some other parameters.

Before You Start

- Make sure the devices (cameras, DVRs, etc.) 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Encoding Device** on the left panel.

3. 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.

4. In the Online Device area, select **Hikvision Private Protocol**/ **Hikvision ISUP Protocol**/**ONVIF Protocol** to filter the detected online devices.

Note

- Select **Hikvision Private Protocol**/**Hikvision ISUP Protocol** to add a Hikvision device and select **ONVIF Protocol** to add a third-party device.
- To display the devices which are added to the platform via ONVIF/ISUP protocol, you can go to → **All Modules** → **General** → **System Configuration** → **Network** → **Device Access Protocol** and check **Access via ONVIF Protocol**/**Allow ISUP Registration**.

5. In the Online Device area, select the active device to be added.
6. Click **Add to Device List** to open the Add Online Device window.

Note

If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.

7. Set the required information.

Device Address

The IP address of the device, which is shown automatically.

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.

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.

Device Name

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

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

8. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
9. **Optional:** Switch on **Add Resource to Area** to import the channels of the added devices to an area.

   Note

   - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import channels to area, you cannot perform operations such as live view, playback, event settings, etc., for the cameras.
10. **Optional:** Select a Streaming Server to get the video stream of the channels via the server.

Note

- 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.

11. **Optional:** If you choose to add resources to area, switch on **Video Storage** and select a storage location for recording.

Encoding Device

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

Hybrid Storage Area Network

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

Cloud Storage Server

The video files will be stored in the Cloud Storage Server 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.

pStor Cluster Service

pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service 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 Hybrid Storage Area Network, Cloud Storage Server 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, Cloud Storage Server or pStor.

12. **Optional:** Set the quick recording schedule for added channels.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type, etc. Refer to ***Configure Recording for Cameras on Current Site*** for details.
13. Click **Add**.
14. **Optional:** Perform the following operations after adding the online device.

Remote Configurations

Click ⚙ in the Operation column to set the remote configurations of the corresponding device.

Note

For detailed operation steps about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online Hikvision devices currently.
- 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.

In the **Operation** column, click to replace the old device with the new device on the platform.

Delete Device

Select one or multiple device(s) and click 🗑 to delete.

Note

If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) 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).

Note

For details, refer to ***Limit Bandwidth for Video Downloading*** .

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

Click **N+1 Hot Spare** to set N+1 hot spare for NVRs.

Note

For details, refer to ***Set N+1 Hot Spare for NVR*** .

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. **Note** If a device is in sleep mode, the communication between the solar camera and the platform is not supported.
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
Filter Device	Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

Add Detected Online Encoding Devices in a Batch

For the detected online encoding devices, if they have the same user name and password, you can batch add multiple devices to HikCentral Professional.

Before You Start

- Make sure the devices (cameras, DVRs, etc.) 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Encoding Device** on the left panel.
3. 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 list in the Online Device area.

   Local Network

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

4. In the Online Device area, select **Hikvision Private Protocol**/ **Hikvision ISUP Protocol**/**ONVIF Protocol** to filter the detected online devices.

Note

- Select **Hikvision Private Protocol**/**Hikvision ISUP Protocol** to add a Hikvision device and select **ONVIF Protocol** to add a third-party device.
- To display the devices which are added to the platform via ONVIF/ISUP protocol, you can go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** , and check **Access via ONVIF Protocol**/**Allow ISUP Registration**.

5. In the Online Device area, select the active devices to be added.
6. Click **Add to Device List** to open the Add Online Device dialog.

Note

If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.

7. **Optional:** Switch on **Mapped Port** and enter the picture downloading port if you want to download pictures from the device.

Note

This function is only available when you select **Hikvision Private Protocol** to filter the detected online devices. By default, the port No. is 80.

8. **Optional:** Switch on **Verify Stream Encryption Key**, and enter stream encryption key in **Stream Encryption Key on Device** field.

Note

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

When you start the live view or remote playback of the camera, the client will verify the key stored in SYS server for security purpose.

9. Enter the same user name and password.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

10. **Optional:** Set the time zone for the device.
    - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

      Note

      You can click **View** to view the details of the current time zone.
    - Click **Get Device's Time Zone** to get the device's time zone.
11. **Optional:** Switch **Add Resource to Area** to on to import the channels of the added devices to an area.

    Note

    - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
    - You can create a new area by the device name or select an existing area.
    - If you do not import channels to area, you cannot perform operations such as live view, playback, and event settings, for the cameras.
12. **Optional:** Select a Streaming Server to get the video stream of the channels via the server.

    Note

    - 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.
13. Click **Add**.
14. **Optional:** Perform the following operations after adding the online devices in a batch.

Remote Configurations	Click in the Operation column to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- 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.

In the **Operation** column, click to replace the old device with the new device on the platform.

Delete Device

Select one or multiple device(s) and click to delete.

Note

If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) 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).

Note

For details, refer to ***Limit Bandwidth for Video Downloading*** .

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

Click **N+1 Hot Spare** to set N+1 hot spare for NVRs.

Note

For details, refer to ***Set N+1 Hot Spare for NVR*** .

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.

Note

If a device is in sleep mode, the communication between the solar camera and the platform is not supported.

Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
Filter Device	Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

9.3.2 Add Encoding 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.

Before You Start

Make sure the devices (cameras, DVRs, etc.) 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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding Device page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.
4. Select **Hikvision Private Protocol/ONVIF Protocol/Dahua Private Protocol** as the Access Protocol.

Note

- Select **Hikvision Private Protocol** to add a Hikvision device and select **ONVIF Protocol/Dahua Private Protocol** to add a third-party device.
- To display the devices which are added to the platform via ONVIF Protocol, you can go to → **Basic Management → System → Network → Device Access Protocol** , and check **Access via ONVIF Protocol**.

5. Select **IP Address/Domain** as the adding mode.
6. Enter the required information.

Device Address

The IP address or domain name of the device.

Encrypted Add

This function is for **Hikvision Private Protocol** only. If you check **Encrypted Add**, the SDK service port will be encrypted.

Note

After the device is added to the platform, will appear beside the device name.

Device Port

The default device port No. is 8000. If you check **Encrypted Add**, the default port No. is 8443.

Mapped Port

This function is used for downloading pictures from devices added by **Hikvision Private Protocol**. Set the **Mapped Port** switch to on and enter the picture downloading port No. that you have configured in the remote configuration page of the device. The default port No. is 80.

Verify Stream Encryption Key

This function is for **Hikvision Private Protocol** only. Switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **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. For details about getting the key, refer to the user manual of the device.

Device Name

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

User Name

The user name for administrator created when activating the device or the added non-admin users. When adding the device to HikCentral Professional using the non-admin user, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

7. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
8. **Optional:** Switch **Add Resource to Area** to on to import the channels of the added devices to an area.

   Note

   - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import channels to area, you cannot perform operations such as live view, playback, event settings, for the cameras.
9. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the channels via the server.

   Note

   - 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.
10. **Optional:** If you choose to add resources to area, switch on **Video Storage** and select a storage location for recording.

    Encoding Device

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

Hybrid Storage Area Network

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

Cloud Storage Server

The video files will be stored in the Cloud Storage Server 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.

pStor Cluster Service

pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service 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.
- You should configure the Hybrid Storage Area Network, Cloud Storage Server or pStor in advance, or its storage location cannot be displayed in the drop-down list. You can click **Add New** to add a new Hybrid Storage Area Network, Cloud Storage Server or pStor.

11. **Optional:** Set the quick recording schedule for added channels.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.
12. Finish adding the device.
    - Click **Add** to add the encoding device and back to the encoding device list page.
    - Click **Add and Continue** to save the settings and continue to add other encoding devices.
13. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

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).

Note

For details, refer to ***Limit Bandwidth for Video Downloading*** .

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

Click **N+1 Hot Spare** to set N+1 hot spare for NVRs.

Note

For details, refer to ***Set N+1 Hot Spare for NVR*** .

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.

In the **Operation** column, click to replace the old device with the new device on the platform.

Delete Device

Select one or multiple device(s) and click to delete.

Note

If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) on the platform.

Search Device

Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

Filter Device

Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** **→ Configuration** , and

then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

9.3.3 Add Encoding Devices by IP Segment

When multiple encoding 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.

Before You Start

Make sure the devices (cameras, DVRs, etc.) 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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding Device page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.
4. Select **Hikvision Private Protocol/ONVIF Protocol/Dahua Private Protocol** as the Access Protocol.

   Note

   - Select **Hikvision Private Protocol** to add a Hikvision device, while select **ONVIF Protocol/ Dahua Private Protocol** to add a third-party device.
   - To display devices which can be added to the platform via ONVIF Protocol, you need to go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** , and check **Access via ONVIF Protocol**.
5. Select **IP Segment** as the adding mode.
6. Enter the required information.

   Device Address

   Enter the start IP address and the end IP address where the devices are located.

   Encrypted Add

   This function is for **Hikvision Private Protocol** only. If you check **Encrypted Add**, the SDK service port will be encrypted.

   Note

   After the device is added to the platform, will appear beside the device name.

   Device Port

The default device port No. is 8000. If you check **Encrypted Add**, the default port No. is 8443.

Mapped Port

This function is used for downloading pictures from devices added by **Hikvision Private Protocol**. Set the **Mapped Port** switch to on and enter the picture downloading port No. that you have configured in the remote configuration page of the device. The default port No. is 80.

Verify Stream Encryption Key

This button is for **Hikvision Private Protocol** only. You can switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **Stream Encryption Key on Device** field. Then when starting live view or remote playback of the device, the client will verify the key stored inSYS server for security purpose.

Note

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

User Name

The user name for administrator created when activating the device or the added non-admin users. When adding the device to HikCentral Professional using the non-admin user, your permissions may restrict your access to certain features.

Password

The password required to access the device.

Caution

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

7. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

Note

- You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform the live view, playback, event settings, for the resources.

9. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the resources via the server.

Note

- 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.

10. Set the quick recording schedule for added resources.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.
11. Finish adding the device.
    - Click **Add** to add the devices of which the IP addresses are between the start IP address and end IP address and back to the device list page.
    - Click **Add and Continue** to save the settings and continue to add other encoding devices.
12. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

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). **Note** For details, refer to ***Limit Bandwidth for Video Downloading*** .
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	Click **N+1 Hot Spare** to set N+1 hot spare for NVRs. **Note** For details, refer to ***Set N+1 Hot Spare for NVR*** .
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Delete Device	Select one or multiple device(s) and click to delete. **Note** If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) on the platform.
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
Filter Device	Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

9.3.4 Add Encoding Devices by Port Segment

When multiple encoding 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 some other related parameters.

Before You Start

Make sure the devices (cameras, DVRs, etc.) 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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding Device page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.
4. Select **Hikvision Private Protocol**/**ONVIF Protocol**/**Dahua Private Protocol** as the access protocol.

   Note

   - Select **Hikvision Private Protocol** to add Hikvision devices and select **ONVIF Protocol**/**Dahua Private Protocol** to add third-party devices.
   - To display devices which can be added to the platform via ONVIF Protocol, you need to go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** , and check **Access via ONVIF Protocol**.
5. Select **Port Segment** as the adding mode.
6. Set the required information.

   Device Address

   Enter the IP address to add the devices which have the same IP address.

   Encrypted Add

   This function is for **Hikvision Private Protocol** only. If you check **Encrypted Add**, the SDK service port will be encrypted.

   Note

   After the device is added to the platform, will appear beside the device name.

   Device Port

   The default device port No. is 8000. If you check **Encrypted Add**, the default port No. is 8443.

   Mapped Port

This function is used for downloading pictures from devices added by **Hikvision Private Protocol**. Set the **Mapped Port** switch to on and enter the picture downloading port number that you have configured on the remote configuration page of the device. The default port number is 80.

Verify Stream Encryption Key

This button is for **Hikvision Private Protocol** only. You can switch **Verify Stream Encryption Key** to on, and enter the stream encryption key in the following **Stream Encryption Key on Device** field. Then when you start 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.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

7. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the channels of the added devices to an area.

Note

- You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform live view, playback, event settings, etc., for the channels.

9. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the channels via the server.

Note

- 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.

10. **Optional:** Set the quick recording schedule for added channels.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.
11. Finish adding the device.
    - Click **Add** to add the devices of which the port number is between the start port number and end port number and back to the device list page.
    - Click **Add and Continue** to save the settings and continue to add other devices.
12. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

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). **Note** For details, refer to ***Limit Bandwidth for Video Downloading*** .
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	Click **N+1 Hot Spare** to set N+1 hot spare for NVRs. **Note** For details, refer to ***Set N+1 Hot Spare for NVR*** .
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Delete Device	Select one or multiple device(s) and click to delete. **Note** If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) on the platform.
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
Filter Device	Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

9.3.5 Add Encoding Device by Hik-Connect DDNS

You can add encoding devices with dynamic IP addresses to the system by domain name solutions of Hik-Connect. Currently, the system only supports domain name solutions function of Hik-Connect.

Before You Start

- Make sure the devices (cameras, DVRs, etc.) 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 HikCentral Professional via network.
- Make sure you have enabled Hik-Connect service for devices to be added on the remote configuration page of the device. For details, refer to the user manual of Hik-Connect.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding Device page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.
4. Select **Hikvision Private Protocol** as the Access Protocol.
5. Select **Hik-Connect DDNS** as the adding mode.
6. **Optional:** Switch on **Mapped Port** and enter the picture downloading port No. that you have configured on the remote configuration page of the device. The default port No. is 80.
7. Select a 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.

   Note

   You can hover your cursor onto ⓘ to view details.
8. Enter the required information.

   Hik-Connect DDNS Server Address

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

   Serial No.

   Enter the serial No. of the device.

   Verification Code

   Enter the verification code of the device.

Stream Encryption Key on Device

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

Note

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

Device Name

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

Site on Hik-Partner Pro

Select a site from the drop-down list and the device will also be added to the selected site on Hik-Partner Pro.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

9. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
10. Switch on **Add Resource to Area** to import the channels of the added devices to an area.

Note

- You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform the live view, playback, event settings, etc., for the channels.

11. **Optional:** If you choose to add resources to an area, select a Streaming Server to get the video stream of the channels via the server.

Note

- 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.

12. Set the quick recording schedule for added resources.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.
13. Finish adding the device.
    - Click **Add** to add the encoding device and back to the encoding device list page.
    - Click **Add and Continue** to save the settings and continue to add other encoding devices.
14. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

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). **Note** For details, refer to ***Limit Bandwidth for Video Downloading*** .
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	Click **N+1 Hot Spare** to set N+1 hot spare for NVRs. **Note** For details, refer to ***Set N+1 Hot Spare for NVR*** .
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Delete Device	Select one or multiple device(s) and click to delete. **Note** If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) on the platform.
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. **Note** If a device is in sleep mode, the communication between the solar camera and the platform is not supported.
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
Filter Device	Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

9.3.6 Add Encoding Device by Device ID

For the encoding devices supporting ISUP, you can add them by specifying a predefined device ID, key, etc. This is a cost-effective choice when you need to manage an encoding device without fixed IP address by HikCentral Professional.

Before You Start

- Make sure the encoding 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 HikCentral Professional via network.
- Before adding devices supporting Hikvision ISUP 2.6/4.0 to the system, you need to set related configuration to allow these devices to access the system. For details, refer to ***Device Access Protocol*** .

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding Device page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.
4. Select **Hikvision ISUP Protocol** as the Access Protocol.

   Note

   To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** , and enable **Allow ISUP Registration**.
5. Select **Device ID** as the adding mode.
6. Enter the required parameters, including the device ID and device name.

   Note

   For devices supporting accessing the platform via ISUP 5.0, you should enter the ISUP login password.
7. **Optional:** Switch on **Verify Stream Encryption Key** if the device supports and enables stream encryption, and enter the stream encryption key on device.

8. **Optional:** Switch on **Picture Storage** and set the location for picture storage.

Note

- You can select Local Storage, Hybrid Storage Area Network, Cloud Storage Server, pStor, or Network Video Recorder as the storage location.
- If you select **Local Storage** as **Storage Location**, you can click **Configuration** to configure **Storage on SYS Server** for the captured pictures. For detailed information, see ***Configure Storage for Imported Pictures and Files*** .

9. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
10. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

Note

- You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- For video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform operations such as live view, playback, event settings, for the cameras.

11. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the resources via the server.

Note

- The camera(s) 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.

12. **Optional:** Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources of the device will start recording according to the schedule.
13. Finish adding the device.
    - Click **Add** to add the encoding device and back to the encoding device list page.
    - Click **Add and Continue** to save the settings and continue to add other encoding devices.
14. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click in the Operation column to set the remote configurations of the corresponding device.

Note

For detailed operation steps for the remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

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).

Note

For details, refer to ***Limit Bandwidth for Video Downloading*** .

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

Click **N+1 Hot Spare** to set N+1 hot spare for NVRs.

Note

For details, refer to ***Set N+1 Hot Spare for NVR*** .

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.

In the **Operation** column, click to replace the old device with the new device on the platform.

Delete Device

Select one or multiple device(s) and click to delete.

Note

If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) on the platform.

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.

Note

If a device is in sleep mode, the communication between the solar camera and the platform is not supported.

Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
Filter Device	Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

9.3.7 Add Encoding Devices by Device ID Segment

If you need to add multiple encoding devices which have no fixed IP addresses and support ISUP Protocol toHikCentral Professional, you can add them to HikCentral Professional at a time after configuring device ID segment for the devices.

Before You Start

- Make sure the encoding 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 HikCentral Professional via network.
- Before adding devices supporting ISUP 2.6/4.0 protocol to the system, you need to set related configuration to allow these devices to access the system. For details, refer to ***Device Access Protocol*** .

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding Device page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.
4. Select **Hikvision ISUP Protocol** as the Access Protocol.

Note

To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** , and enable **Allow ISUP Registration**.

5. Select **Device ID Segment** as the adding mode.
6. Enter the required parameters, including the start device ID and end device ID.

Note

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

7. **Optional:** Switch on **Verify Stream Encryption Key** if the device supports, and enter the stream encryption key on device.
8. **Optional:** Switch on **Picture Storage** and set the location for picture storage.

Note

- You can select Local Storage, Hybrid Storage Area Network, Cloud Storage Server, pStor, or Network Video Recorder as the storage location.
- If you select **Local Storage** as **Storage Location**, you can click **Configuration** to configure **Storage on SYS Server** for the captured pictures. For detailed information, see ***Configure Storage for Imported Pictures and Files*** .

9. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
10. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

    Note

    - You can import all the resources including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
    - For video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
    - You can create a new area by the device name or select an existing area.
    - If you do not import resources to area, you cannot perform operations such as live view, playback, event settings, for the cameras.
11. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream of the resources via the server.

Note

- The camera(s) 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.

12. **Optional:** Check **Get Device's Recording Settings** to get the recording schedule from the device and the resources of the device will start recording according to the schedule.
13. Finish adding the device.
    - Click **Add** to add the encoding device and back to the encoding device list page.
    - Click **Add and Continue** to save the settings and continue to add other encoding devices.
14. **Optional:** Perform the following operation(s) after adding devices.

Remote Configurations

Click in the Operation column to set the remote configurations of the corresponding device.

Note

For details about remote configuration, see the user manual of the device.

Change the Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

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).

Note

For details, refer to ***Limit Bandwidth for Video Downloading*** .

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

Click **N+1 Hot Spare** to set N+1 hot spare for NVRs.

Note

For details, refer to ***Set N+1 Hot Spare for NVR*** .

Replace the 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. In the **Operation** column, click to replace the old device with the new device on the platform.
Delete Device	Select one or multiple device(s) and click to delete. **Note** If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) on the platform.
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. **Note** If a device is in sleep mode, the communication between the solar camera and the platform is not supported.
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
Filter Device	Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

9.3.8 Add Encoding Devices in a Batch

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

Before You Start

Make sure the devices (cameras, DVR, etc.) 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 HikCentral Professional via network.

Perform this task when you need to add devices by importing the template which contains information of multiple devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Encoding Device** on the left panel.
3. Click **Add** to enter the Add Encoding Device page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.
4. Select **Hikvision Private Protocol/Hikvision ISUP Protocol//Dahua Private Protocol** as the access protocol.

   Note

   - Select **Hikvision Private Protocol/Hikvision ISUP Protocol** to add a Hikvision device and select **ONVIF Protocol/Dahua Private Protocol** to add a third-party device.
   - To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** , and enable **Allow ISUP Registration**.
5. Select **Batch Import** as the adding mode.
6. Click **Download Template** and save the predefined template (excel file) on your PC.
7. Open the exported template file and enter the required information of the devices to be added in the corresponding column.
8. Click and select the edited file.
9. **Optional:** Switch on **Picture Storage** and set the location for picture storage.

   Note

   - You can select Local Storage, Hybrid Storage Area Network, Cloud Storage Server, pStor, or Network Video Recorder as the storage location.
   - If you select **Local Storage** as **Storage Location**, you can click **Configure** to configure **Storage on SYS Server** for the captured pictures. For detailed information, see ***Configure Storage for Imported Pictures and Files*** .
10. **Optional:** Set the time zone for the device.
    - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

      Note

      You can click **View** to view the details of the current time zone.
    - Click **Get Device's Time Zone** to get the device's time zone.

11. Finish adding devices.
    - Click **Add** to add the devices and go back to the device list page.
    - Click **Add and Continue** to save the settings and continue to add next batch of devices.
12. **Optional:** Perform the following operation(s) after adding devices in a batch.

Remote Configurations	Click in the Operation column to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
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). **Note** For details, refer to ***Limit Bandwidth for Video Downloading*** .
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	Click **N+1 Hot Spare** to set N+1 hot spare for NVRs. **Note** For details, refer to ***Set N+1 Hot Spare for NVR*** .
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Delete Device	Select one or multiple device(s) and click to delete.

Note

If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) on the platform.

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.

Note

If a device is in sleep mode, the communication between the solar camera and the platform is not supported.

Search Device

Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

Filter Device

Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

9.3.9 Add Encoding Device from the Site on Hik-Partner Pro

If you have configured parameters for the site on Hik-Partner Pro accessing the platform, you can add encoding devices from the site on Hik-Partner Pro to the platform. Deleting devices on the platform will not delete devices from the site on Hik-Partner Pro.

Before You Start

- Make sure the devices (cameras, DVRs, etc.) 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 HikCentral Professional via network.
- Make sure you have enabled **Access Site on Hik-Partner Pro** in System Configuration and configured the required parameters. For details, refer to ***Set Hik-Partner Pro Site Access*** .

Steps

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Encoding Device** on the left panel.

3. Click **Add** to enter the Add Encoding Device page.

Note

If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.

4. Select **Hik-Partner Pro Protocol** as the access protocol.

Note

You need to first purchase a license to use the Hik-Partner Pro service.

5. Select the device source.
   - Select **New Device**, and enter the device serial No., and verification code.

Note

Make sure the new device to be added has registered to Hik-Connect. After the device is added, the corresponding site where the device is on Hik-Partner Pro will also be added.

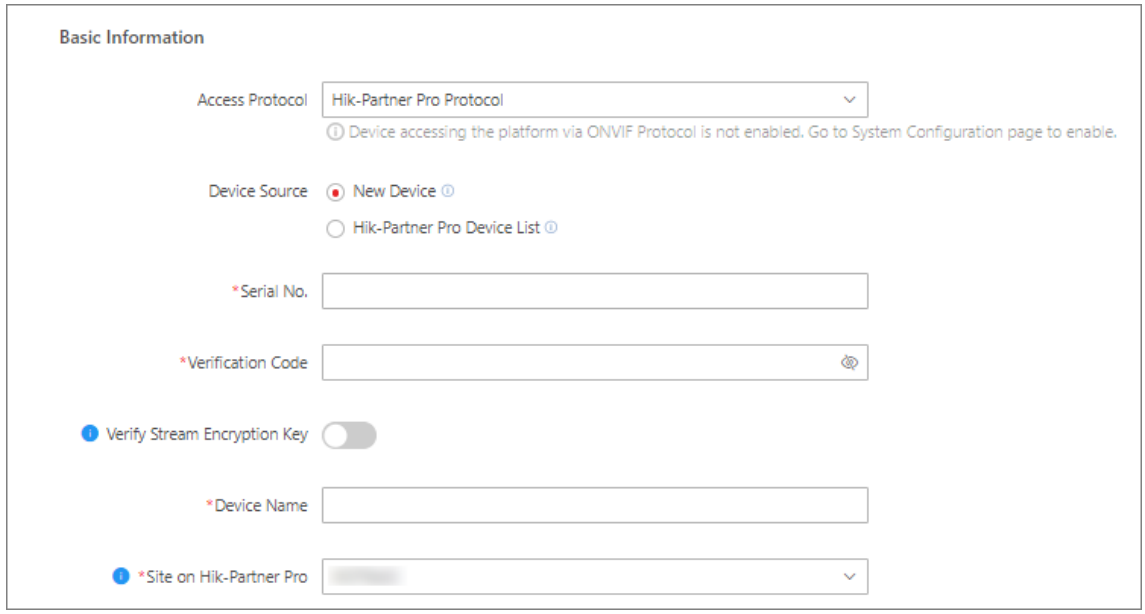


Figure 9-1 Add New Device

   - Select **Hik-Partner Pro Device List**, and select a device from the list.

Note

If the selected device is deleted from the platform, it will not be deleted from the site on Hik-Partner Pro.

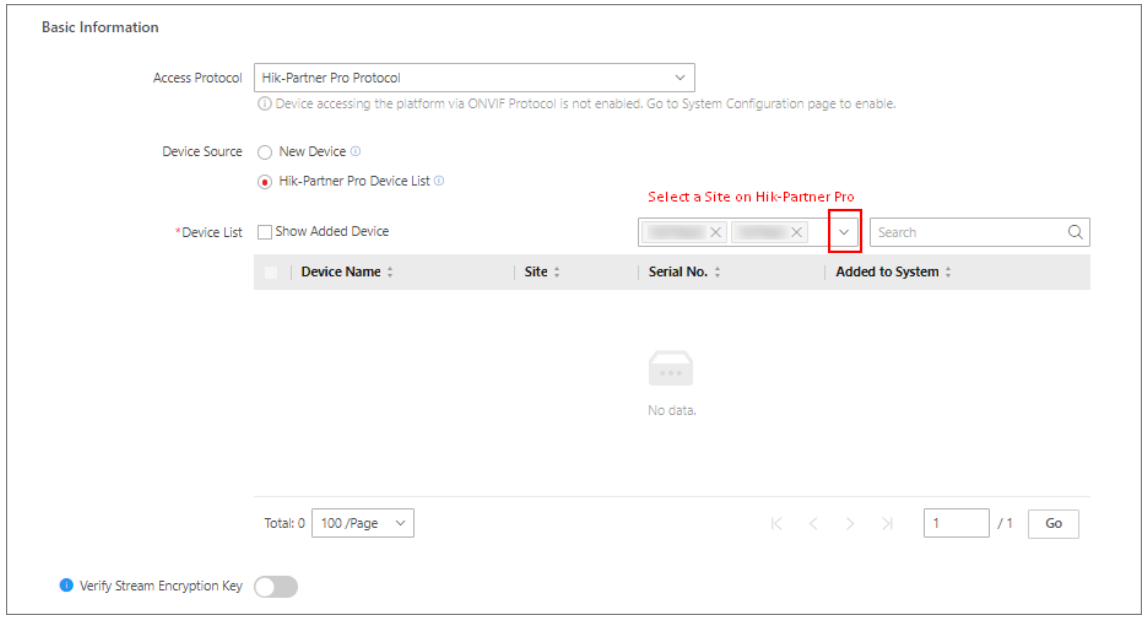


Figure 9-2 Add Device from Hik-Partner Pro Device List

6. Set device parameters.

Verify Stream Encryption Key

Switch on **Verify Stream Encryption Key**, and enter the stream encryption key on device. Then when you start 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 device. Refer to the user manual of the device to get the key.

Device Name

If you select **New Device** as the device source, you need to enter the name of the device to be added.

Note

For devices with the same name on Hik-Partner Pro, suffixes will be added automatically after the names of the devices.

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.

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

Note

You can click **View** to view the details of the current time zone.

8. **Optional:** Switch on **Add Resource to Area** to import the channels of the added devices to an area.

Note

- You can import all the channels including cameras, alarm inputs and alarm outputs, or the specified camera(s) to the corresponding area.
- You can create a new area by the device name or select an existing area.
- If you do not import channels to area, you cannot perform live view, playback, event settings, etc., for the channels.

9. **Optional:** If you need to add resources to area, select a Streaming Server to get the video stream of the channels via the server.

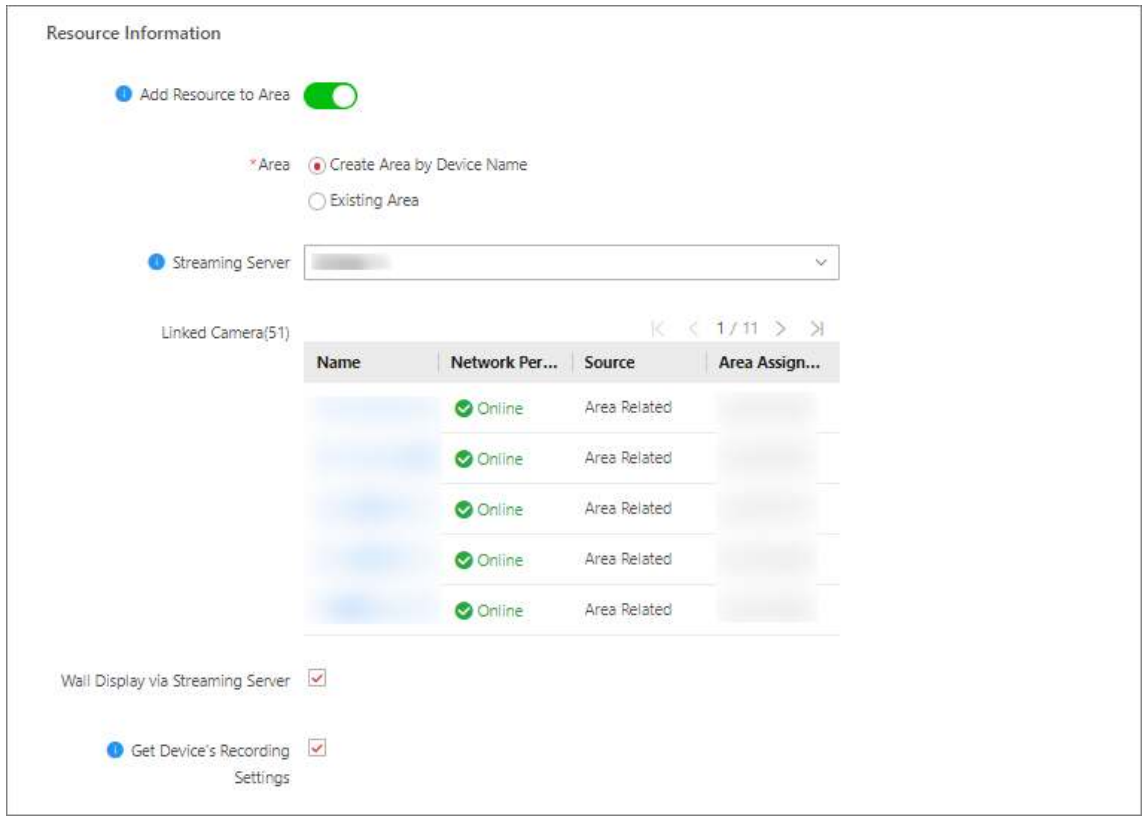


Figure 9-3 Add Resource to Area

Note

- The camera(s) related to the selected server will be displayed, you can view their information and 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.

10. **Optional:** Set the quick recording schedule for added channels.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device and the channels of the device will start recording according to the schedule.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type. Refer to ***Configure Recording for Cameras on Current Site*** for details.
11. Finish adding the device.
    - Click **Add** to add the current device and go back to the device list page.
    - Click **Add and Continue** to add the current device and continue to add other devices.
12. **Optional:** Perform the following operations after adding the device.

Remote Configurations	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
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). **Note** For details, refer to ***Limit Bandwidth for Video Downloading*** .
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	Click **N+1 Hot Spare** to set N+1 hot spare for NVRs. **Note** For details, refer to ***Set N+1 Hot Spare for NVR*** .
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Delete Device	Select one or multiple device(s) and click to delete. **Note** If you delete the device(s), the device channel(s) will also be deleted, and you will not be able to search for historic video footage of the device(s) on the platform.
Search Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
Filter Device	Click **All** in the upper left corner and select a device type to filter devices by encoding device types.

What to do next

For facial recognition cameras / ANPR cameras / thermal cameras (report supported) / water level detection PTZ camera channels / municipal enforcement PTZ camera channels / traffic device channels, click **Maintenance and Management → License Details →** › **→ Configuration** , and then select the added cameras as these types of cameras respectively. Otherwise, these cameras' functions cannot be performed normally on the platform.

9.3.10 Limit Bandwidth for Video Downloading

You can limit bandwidth for video downloading of specific NVRs to save video on the total bandwidth, and thus ensuring the fluency of main features such as live view.

Note

The NVR should be of V4.1.50 or later versions.

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

Click **Device and Server → Encoding Device** on the left panel.

Select encoding device(s) and click **Edit Bandwidth for Video Downloading** to set the bandwidth upper-limit for video downloading of the selected device(s).

9.3.11 Set N+1 Hot Spare for NVR

You can form an N+1 hot spare system with several NVRs (Network Video Recorder). The system consists of several host servers and a spare server. When the 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.

Before You Start

- At least two online NVRs should be added to form an N+1 hot spare system. For details about adding NVR, see ***Manage Encoding Device*** .
- Make sure the NVRs 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 HikCentral Professional via network.

If the N+1 hot spare settings have already been configured on the NVR, select → **Basic Management → Device** .

Select **Device and Server → Encoding Device** on the left panel.

Click **N+1 Hot Spare → Get Hot Spare Settings from Device** to upload the hot spare settings from the device to HikCentral Professional.

If the N+1 hot spare settings haven't been configured on the device, perform the following task to set N+1 hot spare for the NVR.

Steps

Note

- The N+1 hot spare function is only supported by NVRs and Hybrid Storage Area Networks. For details about configuring N+1 hot spare system with Hybrid Storage Area Networks, see ***Set N+1 Hot Spare for Hybrid SAN*** .
- The spare server cannot be selected for storing videos until it switches to host server.
- The host server cannot be set as a spare server and the spare server cannot be set as a host server.

1. On the top navigation bar, select → **Basic Management → Device** .
2. Click **Device and Server → Encoding Device → N+1 Hot Spare** to enter the N+1 Configuration page.
3. Click **Add** to set N+1 hot spare.
4. Select a NVR in the **Spare** drop-down list to set it as the spare server.
5. Select the NVR(s) in the **Host** field to set them as the host server.
6. Click **Add**.

Note

The recording schedules configured on the NVR will be deleted after setting it as the spare Recording Server.

7. Click **Apply Hot Spare Settings to Device** to apply the Hot Spare settings to the devices to take effect.
8. **Optional:** Perform the following operations after setting the hot spare.

Edit Hot Spare	Click on the Operation column, and you can edit the spare and host settings.
Delete Hot Spare	Click × on the Operation column to cancel the N+1 hot spare settings.

Note

Canceling the N+1 hot spare will cancel all the host-spare associations and clear the recording schedule on the spare server.

9.3.12 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 Applications

You can add device applications to some encoding devices.

Before You Start

- Make sure the devices you are going to use are added to the platform. For details about adding encoding device, see ***Manage Encoding Device*** .
- 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 HikCentral Professional via network.

Steps

Note

Currently not all encoding devices can be updated via device applications.

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Select **Device Application** on the left panel.
3. Click **Add Application**.
4. Select **HEOP** or **AIOP** as the application package source.
   - If you select **HEOP**, you need to upload the algorithm package.
   - If you select **AIOP**, you need to upload model library, label file, and enter model name.
5. Click **Next**, and then 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.
7. **Optional:** Perform the following operations after adding applications to device(s).

Enable/Disable Device Application	Click **Enable All** / **Disable All** to enable/disable the corresponding device application.
Add Device Application to Specific Device	Click **Add** to add a device application package for a specific device.
Refresh Device Application List	Click **Refresh** to refresh the device application list.
Delete Device Application	Click **Delete** to delete the device applications.
Import License	Click **Import License** and upload a license file to specific device(s).
Display Applications Disabled	Check **Display Applications Disabled** to only display the disabled applications.
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. **Note** 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

You can manage device applications after adding the them.

Before You Start

- Make sure the devices you are going to use are added to the platform. For details about adding encoding device, see ***Manage Encoding Device*** .
- 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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Select **Device Application** on the left panel.
3. Select **All Devices** tab.

   The devices that support updating by device applications are displayed on the left.
4. **Optional:** Perform the following operations as needed.

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. 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.
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. **Note** The icon indicates that adding device application(s) failed.
Search for Devices	On the top of the page, enter the keywords of device name or device address, and click to search devices for adding device applications.

9.4 Manage Access Control Device

You can add the access control devices to the system for access permission configuration, time and attendance management, etc.

9.4.1 Add Detected Online Access Control Devices

The active online access control devices in the same local subnet with the current Web Client or SYS server will be displayed on a list. You can add one online device one by one, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add a Detected Online Access Control Device

The platform automatically detects online access control devices on the same local subnet with the client or SYS server. You can add the detected access control devices to the platform one by one if they have different user account.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Follow the steps to add a detected online access control device to the platform.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select **Hikvision Private Protocol** and **Hikvision ISUP Protocol** to filter the detected devices by protocol types.

   Note

   Make sure you have enabled the ISUP protocol registration to allow the devices to access the system, otherwise the online devices will not be displayed. On the top, select **System**. Then, select **Network** → **Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.
5. Select an active device that you want to add to the platform.
6. Click **Add to Device List**.

   Note

   For devices whose device port No. is 8000 and HTTP port No. is 80, the **Hikvision Private Protocol** is selected as the access protocol by default. For devices whose device port No. is 0 but the HTTP port No. is 80, the **ISAPI Protocol** is selected as the access protocol.
7. Configure the basic information for the device, including access protocol, device address, device port, device name, user name, and password.

Caution

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

Note

The access protocol will not show in the following situations:

- You check more than one device in the Online Device area.
- You check only one device in the Online Device area.
  - You can select **Hikvision ISUP Protocol** in the Online Device area.
  - You can select **Hikvision Private Protocol** in the Online Device area, and device port is 0.

8. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

   Note

   - You can create a new area by device name or select an existing area.
   - You can import all the access points or specific access point(s) to the area.
   - For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.

10. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

    Note

    - Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
    - It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

11. Click **Add**.

12. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. In the **Operation** column, click to replace the old device with the new device on the platform.
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. **Note** If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter key words in the search box and click to search for a specific device.

Add Detected Online Access Control Devices in a Batch

If the detected online access control devices share the same user name and password, you can add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Access Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select **Hikvision Private Protocol** and **Hikvision ISUP Protocol** to filter the detected devices by protocol types.

   Note

   Make sure you have enabled the ISUP protocol registration to allow the devices to access the system, otherwise the online devices will not be displayed. On the top, select **System**. Then, select **Network → Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.
5. Select the active devices that you want to add to the platform.
6. Click **Add to Device List**.

   Note

   For devices whose device port No. is 8000 and HTTP port No. is 80, the **Hikvision Private Protocol** is selected as the access protocol by default. For devices whose device port No. is 0 but the HTTP port No. is 80, the **ISAPI Protocol** is selected as the access protocol.
7. Set parameters for the devices.

   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.

8. **Optional:** Set the time zone for the device.
   - **Get Device's Time Zone**

     The time zone of the device will be automatically chosen according to the region of the device.
   - **Manually Set Time Zone (The settings will be applied to the device automatically)**

     You can select a time zone of the device. The settings will be applied to the device automatically.
9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

   Note
   - You can create a new area by device name or select an existing area.
   - You can import all the access points or specific access point(s) to the area.
   - For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
10. Check **Restore Default Settings** to restore configured device parameters to default settings.

    Note
    - Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
    - It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.
11. Click **Add**.
12. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Replace Device	In the **Operation** column, click to replace the device with a new device. If the serial No. of the new device is different from that of the old one, you need to confirm the replacement.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.

Privacy Settings	You can configure privacy settings for online access control devices. For details, refer to ***Privacy Settings*** .
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.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter key words in the search box and click to search for a specific device.

9.4.2 Add an Access Control Device by IP Address/Domain

If you know the IP address/domain of the access control device you want to add to the platform, you can add the device by specifying its IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol**, **Hikvision ISUP Protocol**, or **Hikvision ISAPI Protocol** as the access protocol.
5. Select **IP Address/Domain** as the adding mode.
6. Enter the required parameters.

Note

By default, the device port number is 8000 when the access protocol is **Hikvision Private Protocol**, while the device port number is 80 when the access protocol is **Hikvision ISAPI Protocol**.

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.

7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.

9. Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.

Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

9.4.3 Add Access Control Devices by IP Segment

If the access control devices you want to add to the platform share the same user account, and they are in the same IP segment, you can add them to the platform by specifying the start/end IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Select **Device and Server → Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol** or **Hikvision ISAPI Protocol** as the access protocol.
5. Select **IP Segment** as the adding mode.
6. Enter the required information.

Note

By default, the device port number is 8000 when the access protocol is **Hikvision Private Protocol**, while the device port number is 80 when the access protocol is **Hikvision ISAPI Protocol**.

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.

7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

9. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.

- Click **Add and Continue** to add the device(s) and continue to add other devices.

10. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
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. In the **Operation** column, click ⇄ to replace the old device with the new device on the platform.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click 🔍 to search for a specific device.

9.4.4 Add an Access Control Device by Device ID

For access control devices supporting ISUP 4.0 or later protocol, you can add them by specifying a predefined device ID and key. This is a cost-effective choice when you need to manage access control devices that do not have fixed IP addresses.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.

   Note

   Make sure you have enabled the ISUP protocol registration, otherwise the protocol will not be displayed. On the top, select **System**. Then, select **Network** → **Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.
5. Select **Device ID** as the adding mode.
6. Enter the required the information.
7. **Optional:** Switch on **Picture Storage** to set the storage location for pictures.
   - Select **pStor** and select storage locations for the face picture library and captured pictures.

     Note

     This configuration only affects the facial recognition device which supports face comparison. The storage location of captured pictures and face picture libraries cannot be the same.
   - Select **Local Storage** as the storage location, click **Configure** to enable **Local Storage** and set the storage locations for pictures and files as needed.
8. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
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. In the **Operation** column, click to replace the old device with the new device on the platform.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

9.4.5 Add Access Control Devices by Device ID Segment

If you need to add multiple access control devices which support ISUP 5.0 protocol and have no fixed IP addresses to the platform, you can add them all at once after configuring a device ID segment for the devices.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.

   Note

   Make sure you have enabled the ISUP protocol registration, otherwise the protocol will not be displayed. On the top, select **System**. Then, select **Network** → **Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.
5. Select **Device ID Segment** as the adding mode.
6. Enter the required parameters.
7. **Optional:** Switch on **Picture Storage** to set the storage location for pictures.
   - Select **pStor** and select storage locations for the face picture library and captured pictures.

     Note

     This configuration only affects the facial recognition device which supports face comparison. The storage location of captured pictures and face picture libraries cannot be the same.
   - Select **Local Storage** as the storage location, click **Configuration** to enable **Local Storage** and set the storage locations for pictures and files as needed.
8. **Optional:** Set the time zone for the device.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can select a time zone of the device. The settings will be applied to the device automatically.

9. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs, alarm outputs, and access points) to an area.

Note

- You can create a new area by device name or select an existing area.
- You can import all the access points or specific access point(s) to the area.
- For the video access control terminal of a device, the camera on the terminal will also be imported to the corresponding area.
- If you do not import access points to area, you cannot perform further configurations for the access point.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. In the **Operation** column, click to replace the old device with the new device on the platform.
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.

Note

If you want to restore all the device parameters, you should 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. For details, refer to ***Privacy Settings*** .
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

9.4.6 Add Access Control Devices in a Batch

You can download and enter access control device information in the predefined spreadsheet to add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Access Control Device** on the left.
3. Click **Add** to enter the Add Access Control Device page.
4. Select **Hikvision Private Protocol**, **Hikvision ISUP Protocol**, or **Hikvision ISAPI Protocol** as the access protocol.

   Note

   Make sure you have enabled the ISUP protocol registration, otherwise the protocol will not be displayed. On the top, select **System**. Then, select **Network** → **Device Access Protocol** on the left, and switch on **Allow ISUP Registration**. Before adding devices by ISUP 2.6/4.0 protocol to the system, you need to check **Allow ISUP of Earlier Version**.
5. Select **Batch Import** as the adding mode.
6. Click **Download Template** and save the predefined spreadsheet (XLSX format) to local disk.
7. Open the spreadsheet and edit the required device information.
8. Click and select the edited spreadsheet.

9. **Optional:** Switch on **Picture Storage** to set the storage location for pictures.
   - Select **pStor** and select storage locations for the face picture library and captured pictures.

     Note

     This configuration only affects the facial recognition device which supports face comparison. The storage location of captured pictures and face picture libraries cannot be the same.
   - Select **Local Storage** as the storage location, click **Configure** to enable **Local Storage** and set the storage locations for pictures and files as needed.

   Setting picture storage location is not required for devices added via **Hikvision ISAPI Protocol**.
10. **Optional:** Set the time zone for the device.

    Get Device's Time Zone

    The time zone of the device will be automatically chosen according to the region of the device.

    Manually Set Time Zone (The settings will be applied to the device automatically)

    You can select a time zone of the device. The settings will be applied to the device automatically.
11. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
12. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. For details, refer to ***Privacy Settings*** .
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.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

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. In the **Operation** column, click to replace the old device with the new device on the platform.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

9.4.7 Configure Device Parameters

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

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.

Before You Start

Make sure you have wired the third-party card readers to the access control device or elevator control device.

Steps

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.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Access Control Device** or **Device and Server** → **Elevator Control Device** on the left.
3. Click in the Operation column to enter the configuration page of a device.
4. Switch on **Custom Wiegand**.
5. Configure the Wiegand parameters.

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.

Before You Start

The function should be supported by the device.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Device and Server → Access Control Device** on the left panel.
3. Click in the Operation column to enter the configuration page of an access control device.
4. Set Wiegand parameters.
   1) Select a Wiegand protocol in the list, and click in the Operation column to pop up a window of Wiegand information.
   2) On the pop-up window, set Wiegand parameters.

      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 or 34-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.

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

Configure Device Actions for Access Event

You can set the linkage actions of an access control device or elevator control device for the device's events, so that when a specific event occurs, the device can execute actions such as capturing a picture, recording video footage, triggering alarm output, triggering buzzer, arming/disarming zones, locking/unlocking access points, etc.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** or **Device and Server → Elevator Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Event Linkage** as the linkage type.
   2) Select an event type from the **Event Type** drop-down list and then select a specific event.

Note

- If you select **Alarm Input Event**, you need to select an alarm input.
- If you select **Door Event**, you need to select an access point.
- If you select **Card Reader Event**, you need to select a card reader.

6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point 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.

7. Click **Save** to add the linkage.
8. **Optional:** Perform further operations on linkages.

Delete a Linkage	Click to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click to edit the linkage.

Configure Device Actions for Card Swiping

You can set the linkage actions of an access control device or elevator control device for card swiping, so that when the device detects a specific card, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc. In this way, you can monitor the behaviors and whereabouts of the card holder.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Card Linkage** as the linkage type.
   2) Select a card from the **Card No.** drop-down list.
   3) Select a card reader from the **Card Reader** drop-down list.
6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point 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.

7. Click **Save** to add the linkage.
8. Perform further operations on linkages.

Delete a Linkage	Click to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click to edit the linkage.

Configure Device Actions for Person ID

You can set the linkage actions of an access control device or elevator control device for person ID, so that when the device detects the credentials of the person, it can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc. In this way, you can monitor the behaviors and whereabouts of the person.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** or **Device and Server → Elevator Control Device** on the left.
3. Click in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Configure event source.
   1) Select **Person Linkage** as the linkage type.
   2) Select a person ID from the **Person** drop-down list.
   3) Select a card reader from the **Card Reader** drop-down list.
6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point 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.

7. Click **Save** to add the linkage.
8. Perform further operations on linkages.

Delete a Linkage	Click to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click to edit the linkage.

Configure Device Actions for MAC Address

You can set access control device's linkage actions for MAC address of mobile devices, so that when the device detects a specific MAC address, the device can execute actions such as capturing a picture, triggering alarm output, triggering buzzer, locking/unlocking access point, etc.

Steps

Note

This feature requires device support. Parameters vary with different device types and models.

1. On the top, select **Device**.
2. Select **Device and Server → Access Control Device** on the left.
3. Click ⚙ in the Operation column to enter the configuration page of a device.
4. Click **Add** in the Linkage section.
5. Select **MAC Linkage** as the linkage type, and then edit the MAC address.
6. Configure 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 access point (door or barrier) when the specified event is triggered.

Lock

Lock the access point when the specified event is triggered.

Remain Unlocked

The access point will remain unlocked when the specified event is triggered.

Remain Locked

The access point 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.

7. Click **Save** to add the linkage.
8. Perform further operations on linkages.

Delete a Linkage	Click to delete the linkage.
Delete All Linkages	Click **Delete All** to delete all linkages.
Edit Linkage	Click to edit the linkage.

Configure 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.

Steps

1. In the top left corner of the Home page, select → **Device** → **Device and Server** → **Access Control Device** , or → **Device and Server** → **Elevator Control Device** .
2. Click on the Operation column to enter the configuration page of a device.
3. In Card Swiping section, configure card swiping parameters.

Note

Parameters vary with different device types and models.

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.

Note

For details about linking a camera to an access point, see ***Edit Door for Current Site*** or ***Edit Elevator for Current Site*** .

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.

Note

For details about configuring picture storage settings, see ***Edit Door for Current Site*** or ***Edit Elevator for Current Site*** .

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.

Configure Other Parameters

You can configure other parameters for an access control device, such as device time and turnstile parameters.

Note

Device support required. Parameters vary with different device types and models.

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 Screening** 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.

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.

Electrostatic Discharge Testing Settings

Resistance Threshold of Hand

Enter two values between 100 KΩ and 10,000 KΩ. The resistance of the hand to be detected should be within the configured range.

Resistance Threshold of Foot

Enter two values between 100 KΩ and 10,000 KΩ. The resistance of the foot to be detected should be within the configured range.

Not Allowed If Resistance Exceeds Threshold

If checked, the turnstile door will not open when the resistance exceeds the above configured threshold.

Linked Device IP Address

Enter the IP address of the MinMoe face recognition terminal to be linked, and then information such as the electrostatic discharge testing result will be displayed on the terminal.

Communication Timeout Threshold with Electrostatic Discharge Detector

Configure the communication timeout threshold between the turnstile and the electrostatic discharge detector. If the detection time exceeds the threshold, the related event will be uploaded to the platform.

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.

9.4.8 Privacy Settings

You can configure the settings for event storage, authentication, and picture uploading and storage, and clear the pictures on the access control devices to protect the person's private information, including name, profile picture, etc.

On the top, select **Device**. Then select **Device and Server → Access Control Device** on the left.

Select one or more devices and click **Privacy Settings**.

Note

Make sure the selected device is online.

Set the following parameters as needed and click **Save**.

Event Storage

Select the mode of event storage.

Overwrite

The events stored on the device will be overwritten automatically. For example, if a device can store up to 200 events. When this limit is reached, the first event will be overwritten by the newest one, and then the second will be overwritten.

Delete Old Events Regularly

Set a time period. The events stored on the device during the period will be automatically deleted at intervals of the period.

Delete Old Events by Specified Time

Set a specific time. The events stored on the device before the specific time will be automatically deleted.

Authentication

Check the items to be displayed in authentication results.

Picture Uploading and Storage

Check the items as needed.

Upload Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be uploaded to the system.

Save Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be saved to the devices.

Save Profile Pictures

If it is checked, the profile pictures will be saved to the devices.

Upload Event and Alarm Pictures

If it is checked, the event and alarm pictures will be uploaded to the system.

Save Event and Alarm Pictures

If it is checked, the event and alarm pictures will be saved to the devices.

Upload Thermal Pictures

If it is checked, the thermal pictures will be uploaded to the system.

Save Thermal Pictures

If it is checked, the thermal pictures will be saved to the devices.

Clear Pictures Stored on Device

Clear Face Pictures

Click **Clear** to clear all face pictures.

Clear Recognized or Captured Pictures

Click **Clear** to clear all recognized pictures or captured pictures.

9.5 Manage Elevator Control Device

You can add the elevator control device to the system to control the elevator(s), such as assign the access authority of specified floors to person, control the elevator status on the Control Client.

9.5.1 Add Detected Online Elevator Control Devices

The active online elevator control devices on the same local subnet with the current Web Client or SYS server will be displayed on a list. You can add an online device at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function will be available.

Add a Detected Online Elevator Control Device

The Web Client automatically searches for online elevator control devices on the same local subnet with the client or SYS server. You can add the detected elevator control devices to the platform one by one if the devices do not share the same user account.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Elevator Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select an active device that you want to add to the platform.
5. Click **Add** to open the Add Elevator Control Device window.
6. Configure the basic information for the device, including device address, device port, device name, user name, and 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.
7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.
8. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

   Note

   - You can create a new area by device name or select an existing area.
   - If you do not import resources to an area, you cannot perform further operations for the resources.
   - Enter the range of floor number according to your application scenario.
9. **Optional:** Check **Restore Default Settings** to restore device parameters configured on the system to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

10. Click **Add**.
11. **Optional:** Perform further operations on added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click 🔍 to search for a specific device.

Add Detected Online Elevator Control Devices in a Batch

If the detected online elevator control devices share the same user account, you can add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Elevator Control Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select the active devices that you want to add to the platform.
5. Click **Add to Device List** to open the Add Elevator Control Device window.
6. Set parameters for the devices.

   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.
7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.
8. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

Note

- You can create a new area by device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the resources.
- Enter the range of floor number according to your application scenario.

9. **Optional:** Check **Restore Default Settings** to restore device parameters configured on the system to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

10. Finish adding the device(s).
    - Click **Add** to add the device(s) and return to the device management page.
    - Click **Add and Continue** to add the device(s) and continue to add other devices.
11. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	On the device list, select one or multiple devices and click **Time Zone** to edit their time zones.

Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

9.5.2 Add an Elevator Control Device by IP Address

If you know the IP address of the elevator control device you want to add to the platform, you can add the device by specifying its IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Elevator Control Device** on the left.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Select **IP Address** as the adding mode.
5. Enter the required parameters.

Note

By default, the device port number is 8000.

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.

6. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

Note

- You can create a new area by device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the resources.
- Enter the range of floor number according to your application scenario.

8. **Optional:** Check **Restore Default Settings** to restore device parameters configured on the system to default settings.

Note

Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.

9. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.
10. **Optional:** Perform further operations on the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.

Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.

9.5.3 Add Elevator Control Devices by IP Segment

If the elevator control devices you want to add to the platform share the same user account, and they are in the same IP segment, you can add them to the platform by specifying the start/end IP address, user name, and password.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Elevator Control Device** on the left.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Select **IP Segment** as the adding mode.
5. Enter the required parameters.

Note

By default, the device port number is 8000.

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.

6. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Switch on **Add Resource to Area** to import resources (including alarm inputs, alarm outputs, and floors) of elevator control device to an area.

Note

- You can create a new area by device name or select an existing area.
- If you do not import resources to an area, you cannot perform further operations for the resources.
- Enter the range of floor number according to your application scenario.

8. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.
9. **Optional:** Perform further operations on the added device(s).

Configure Device	Click in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices share the same password, you can select multiple devices to change the password together.
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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

9.5.4 Add Elevator Control Devices in a Batch

You can download and enter elevator control device information in the predefined spreadsheet to add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Elevator Control Device** on the left.
3. Click **Add** to enter the Add Elevator Control Device page.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined spreadsheet (XSLX file) to the local disk.
6. Open the spreadsheet and edit the required device information.
7. Click and select the edited spreadsheet.
8. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can select a time zone of the device. The settings will be applied to the device automatically.
9. Finish adding the device(s).
   - Click **Add** to add the device(s) and return to the device management page.
   - Click **Add and Continue** to add the device(s) and continue to add other devices.
10. **Optional:** Perform further operations on the added device(s).

Configure Device	Click in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

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.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

9.6 Manage Video Intercom Device

You can add video intercom devices (indoor station, door station, outer door station, and main station) to the system for management, including editing and deleting the devices, remote configuration, changing online devices' password, etc. You can also perform further operations such as video intercom, unlocking door remotely, etc. based on the added devices.

- **Indoor Station:** The indoor station is an intelligent terminal which can provide two-way audio, network transmission, data storage, remote unlocking, etc. It is mainly applied in the community.
- **Door Station:** The door station can send call to indoor station (residents) and main station. It is mainly applied in the community and office buildings.
- **Outer Door Station:** The outer door station can send call to indoor station (residents) and main station. It is mainly applied in the community and office buildings.
- **Main Station:** The main station is an intelligent terminal, which can be used to unlock door remotely, send call to residents and respond to residents' call. It is mainly applied in large community.

9.6.1 Add Detected Online Video Intercom Devices

The active online video intercom devices on the same local subnet with the current HikCentral Professional Web Client or SYS server will be displayed in the list. You can add an online device at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function will be available.

Add a Detected Online Video Intercom Device

The online video intercom devices on the same local subnet with the current Web Client or SYS server can be displayed in the list, and you can add the detected indoor station to the system one by one.

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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Video Intercom Device** on the left.
3. In the Online Device area, select a network type.

   Server Network

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

   Local Network

   The detected online devices on the same local subnet with the current Web Client will be listed in the Online Device area.
4. In the Online Device area, select the active device to be added.
5. Click in the Online Device area to enter the Add Video Intercom Device page.

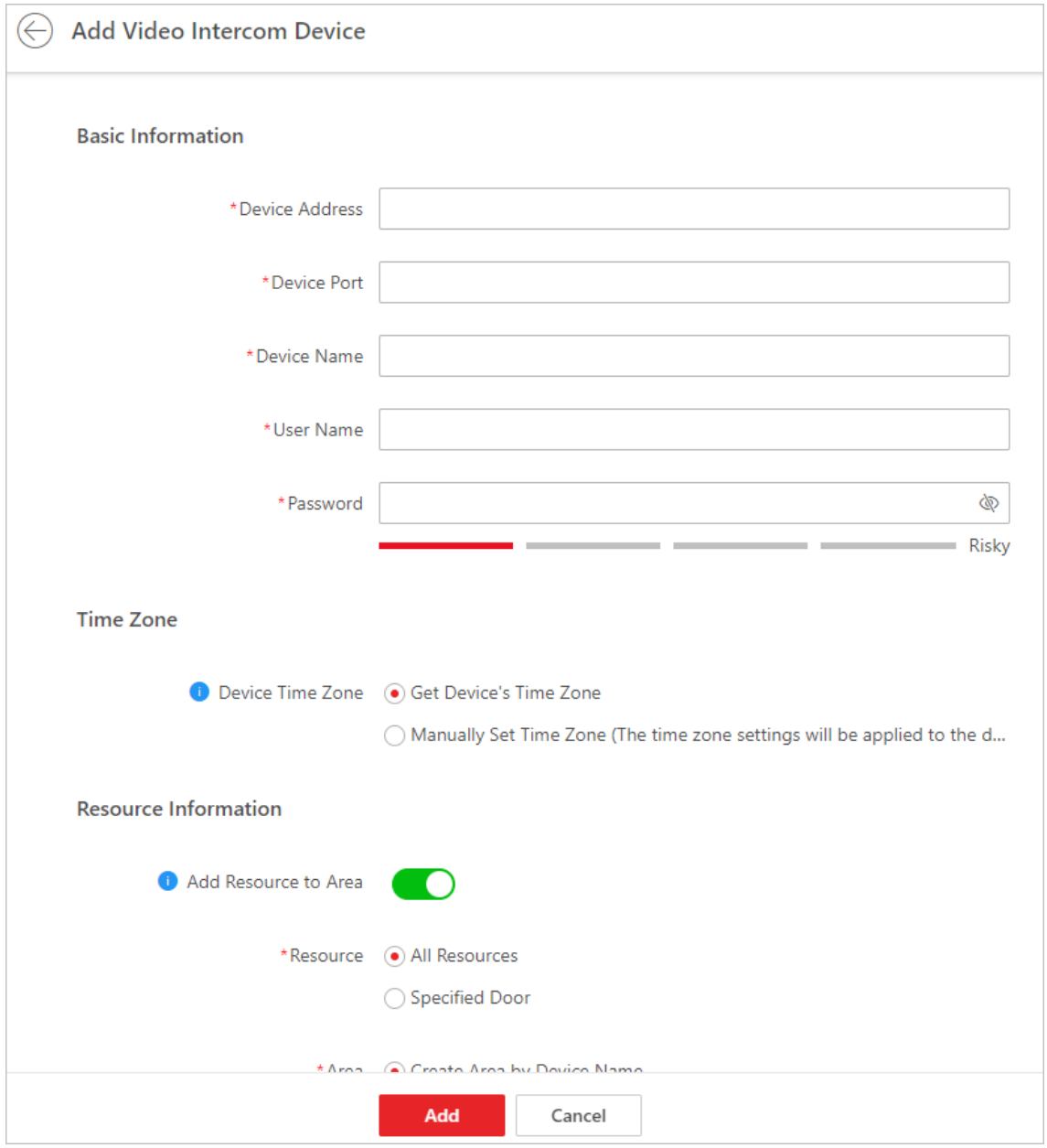


Figure 9-4 Add a Detected Online Video Intercom Device

6. Configure the basic information for the device, including device address, device port, device name, user name, and 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.

7. **Optional:** Set the time zone for the device.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
8. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

   Note

   - You can import all the alarm inputs or the specified alarm input to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform further operations for the alarm inputs.
9. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

   Note

   - Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
   - It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.
10. Click **Add**.
11. **Optional:** Perform the following operation(s) after adding the online device.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .
Change Password	Select the added device(s) and click 🔑 to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Restore Default Settings	Select the added device(s), and click to restore the configured device parameters. **Note** If you want to restore all the device parameters, you can check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

Add Detected Online Video Intercom Devices in a Batch

If the detected online video intercom devices share the same user name and password, you can add multiple devices at a time.

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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Video Intercom Device** on the left.
3. In the Online Device area, select the active devices to be added.
4. Click in the Online Device area to enter the Add Video Intercom Device page.

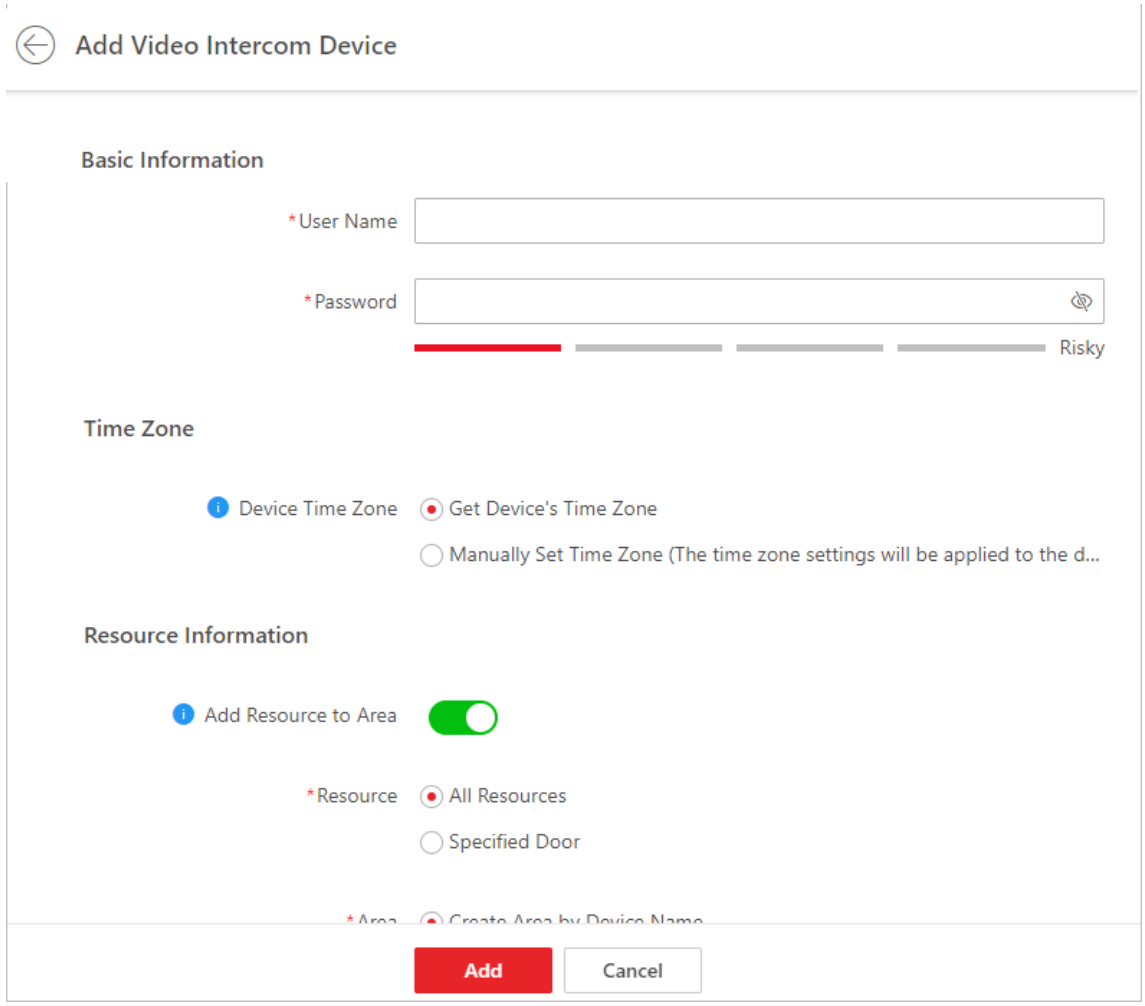


Figure 9-5 Add Detected Online Video Intercom Devices in a Batch

5. Configure the basic information for the device, including user name and 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.

6. **Optional:** Set the time zone for the device.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can select a time zone of the device. The settings will be applied to the device automatically.

7. Finish adding the devices.
   - Click **Add** to add the video intercom devices in a batch, and back to the video intercom device list page.
   - Click **Add and Continue** to save the settings and continue to add other video intercom devices.
8. **Optional:** Perform further operations for the added device(s).

Configure Device	Click ⚙ in the **Operation** column to enter the corresponding device configuration page to edit the time parameters, reboot the device, restore the device, or set other parameters. See ***Configure Device Parameters*** for detailed instructions.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices share the same password, you can select multiple devices to change the password together.

Privacy Settings	You can configure privacy settings for online video intercom devices. For details, refer to ***Privacy Settings*** .
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.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Search for Devices	Enter the keywords of device name, device address, or serial No., and click 🔍 to search for devices.

9.6.2 Add a Video Intercom Device by IP Address

When you know the IP address of a video intercom device, you can add it to the system by specifying the IP address, user name, password, etc. for management and further video intercom applications.

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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Video Intercom Device** on the left.
3. Click **Add** to enter Add Video Intercom Device page.
4. Select **IP Address** as the adding mode.

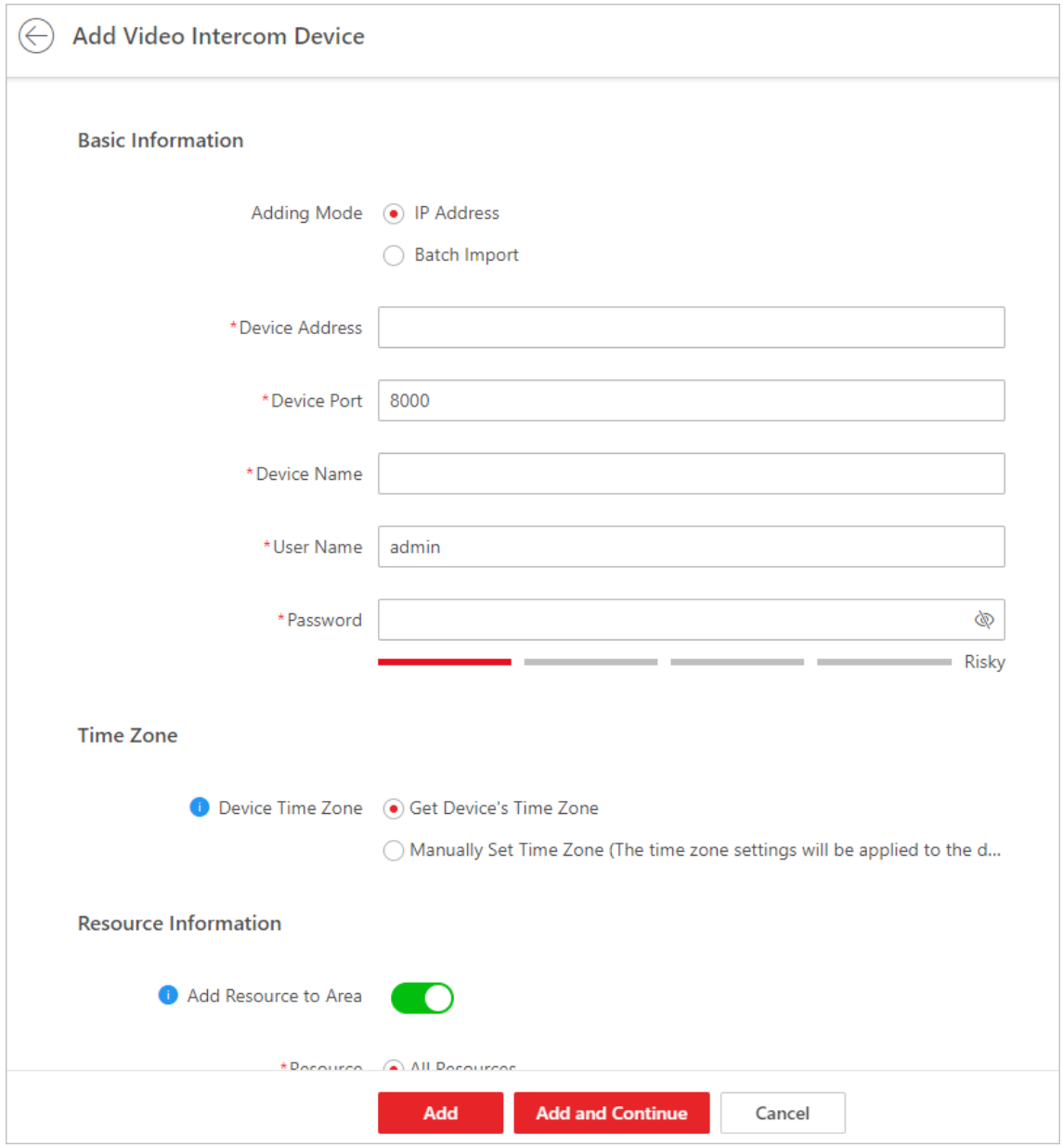


Figure 9-6 Add Video Intercom Device Page

5. Enter the required information.

Device Address

The IP address of the device.

Device Port

By default, the device port No. is 8000.

Device Name

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

Password

The password required to access the account.

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.

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

   Note

   You can click **View** to view the details of the current time zone.
7. **Optional:** Switch **Add Resource to Area** to on to import the resources of the added devices to an area.

   Note

   - You can import all the alarm inputs or the specified alarm input to the corresponding area.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform further operations for the alarm inputs.
8. **Optional:** Check **Restore Default Settings** to restore all the parameters of the device configured on the system to default settings.
9. Finish adding the device.
   - Click **Add** to add the device and back to the video intercom device list page.
   - Click **Add and Continue** to save the settings and continue to add the next device.
10. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. For details, refer to ***Configure Device Parameters*** .
Change Password	Select the added device(s) and click to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

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.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

9.6.3 Add Video Intercom Devices in a Batch

You can add video intercom devices in a batch to the system by entering the device information to the predefined template and importing the template to the system.

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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Device and Server** → **Video Intercom Device** on the left.
3. Click **Add** to enter Add Video Intercom Device page.
4. Click **Batch Import** as the adding mode.
5. Click **Download Template** to save the predefined template (Excel file) on your PC.
6. Open the exported template file and enter the required information of the devices to be added.
7. Click and select the template file.
8. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

Note

You can click **View** to view the details of the current time zone.

9. Finish adding the devices.
   - Click **Add** to add the video intercom devices in a batch, and back to the video intercom device list page.
   - Click **Add and Continue** to save the settings and continue to add other video intercom devices.
10. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
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. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or more key words in the search box and click to search for a specific device.

9.7 Manage Visitor Terminals

The visitor terminals can be added to the system for management, including editing and deleting the devices, remote configuration, etc. The platform supports multiple ways for adding visitor terminals. You can select one of them according to your need.

9.7.1 Add Detected Online Visitor Terminals

The system can perform an automated detection for available visitor terminals in the network where the Web Client or server is located, which makes the devices' information about themselves (e.g., IP address) recognized by the system. Based on the information, you can add the devices quickly.

You can add one online devices at a time, or add multiple online devices in a batch.

Add a Detected Online Visitor Terminal

For the detected online visitor terminals, you can add the devices one by one to HikCentral Professional by specifying the user name, password, and some other parameters.

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 for you to connect the devices to the HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. In the Online Device area, select a network type.

   Server Network

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

   Local Network

   The detected online devices on the same local subnet with the Web Client will be listed in the Online Device area.
3. In the Online Device area, select the active device to be added.
4. Click **Add to Device List** to open the Add Online Device page.
5. Set the required information.

   Device Address

   The IP address of the device, which is shown automatically.

Device Port

The port number of the device, which is shown automatically. The default port number is 80.

Device Name

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

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

6. **Optional:** Set the time zone for the device.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone (The settings will be applied to the device automatically)

You can manually select a time zone of the device. The settings will be applied to the device automatically.

7. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

8. Click **Add** to finish adding the device.
9. **Optional:** Perform the following operations after adding the online device.

Remote Configurations	Click to remotely configure the corresponding device.

Note

For detailed operation steps about remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set Device's Time Zone

In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.

Search for Devices

Enter one or multiple key words in the search box and click to search for a specific device.

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.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

Refresh Device Information

Select the added device and click to refresh information of the device.

Add Detected Online Visitor Terminals in a Batch

For the detected online encoding devices, if they have the same user name and password, you can batch add multiple devices to HikCentral Professional.

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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. 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 list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the Web Client will list in the Online Device area.
3. In the Online Device area, check the active devices to be added.
4. Click **Add to Device List** to open the Add Online Device page.
5. Enter the same user name and password.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

   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.
6. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can manually select a time zone of the device. The settings will be applied to the device automatically.
7. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

8. Click **Add**.
9. **Optional:** Perform the following operations after adding the online devices in a batch.

Remote Configurations	Click to remotely configure the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.
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. **Note** If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.
Refresh Device Information	Select the added device and click to refresh information of the device.

9.7.2 Add Visitor Terminal by IP Address

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.

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 HikCentral Professional via network.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. Click **Add**.
3. Select **IP Address** as the adding mode.
4. Enter the required information.

   Device Address

   The IP address of the device.

   Device Port

   By default, the device port No. is 80.

   Device Name

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

   Password

   The password required to access the account.

   Caution

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

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

You can manually select a time zone of the device. The settings will be applied to the device automatically.

6. **Optional:** Check **Restore Default Settings** to restore configured device parameters to default settings.

Note

- Not all the device parameters will be restored. Network parameters such as IP address, port No., and password will be kept.
- It is recommended that you should restore to default when adding an online device that has been added to other platforms for the first time.

7. Finish adding the device.
   - Click **Add** to add the encoding device and back to the encoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other encoding devices.
8. **Optional:** Perform the following operation(s) after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.
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. **Note** If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and**

	account information, such as user name and password. in the pop-up window.
Refresh Device Information	Select the added device and click to refresh information of the device.

9.7.3 Add Visitor Terminals by IP Segment

When multiple visitor terminals 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.

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 HikCentral Professional via network.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. Click **Add**.
3. Select **IP Segment** as the adding mode.
4. Enter the required information.

   Device Address

   Enter the start IP address and the end IP address where the devices are located.

   Device Port

   By default, the device port No. is 80.

   User Name

   The user name for administrator created when activating the device or the added non-admin users. When adding the device to HikCentral Professional using the non-admin user, your permissions may restrict your access to certain features.

   Password

   The password required to access the device.

Caution

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

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

5. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can manually select a time zone of the device. The settings will be applied to the device automatically.

6. Finish adding the device.
   - Click **Add** to add the devices of which the IP addresses are between the start IP address and end IP address and back to the device list page.
   - Click **Add and Continue** to save the settings and continue to add other encoding devices.

7. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.
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.

Note

If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.

Refresh Device Information Select the added device and click to refresh information of the device.

9.7.4 Add Visitor Terminals in a Batch

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

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 HikCentral Professional via network.

Perform this task when you need to add devices by importing the template which contains information of multiple devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **Visitor Terminal** .
2. Click **Add**.
3. Select **Batch Import** as the adding mode.
4. Click **Download Template** and save the predefined template (excel file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.
6. Click and select the edited file.
7. **Optional:** Set the time zone for the device.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone (The settings will be applied to the device automatically)

   You can manually select a time zone of the device. The settings will be applied to the device automatically.
8. Finish adding devices.
   - Click **Add** to add the devices and go back to the device list page.
   - Click **Add and Continue** to save the settings and continue to add next batch of devices.
9. **Optional:** Perform the following operation(s) after adding devices in a batch.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For detailed operation steps about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Device's Time Zone	In the device list, select one or multiple devices and click **Time Zone** to edit their time zones.
Search for Devices	Enter one or multiple key words in the search box and click to search for a specific device.
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. **Note** If you want to restore all the device parameters, you should check **Restore device parameters excluding network parameters and account information, such as user name and password.** in the pop-up window.
Refresh Device Information	Select the added device and click to refresh information of the device.

9.8 Manage Payment Terminal

You can add payment terminals to the platform for management, including editing and deleting the devices, remote configuration, etc. The platform supports multiple ways for adding payment terminals, including adding by IP address, adding by IP segment, batch adding, etc.

9.8.1 Add Detected Online Payment Terminals

The active online payment terminals on the same local subnet with the current Web Client or the server will be displayed in a list. You can add one online device at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function will be available.

Add a Detected Online Payment Terminal

The platform automatically detects online payment terminals on the same local subnet with the client or the SYS server. You can add the detected payment terminals to the platform one by one if they do not share the same user name.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Payment Terminal** on the left panel.
3. In the Online Device area, select a network type.

   Server Network

   The detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices on the same local subnet with the Web Client will be listed in the Online Device area.
4. In the Online Device area, select an active device to be added.
5. Click **Add to Device List** to open the adding online device window.
6. Set the basic information for the device.

   Device Address

   The IP address of the device, which is shown automatically.

   Device Port

   The port number of the device, which is shown automatically. The default port number is 80.

Device Name

Create a descriptive name for the device.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as the operator. When adding the device to HikCentral Professional using the non-admin account, your permission may restrict your access to certain features.

Password

The password required to access the account.

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.

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

   Note

   You can click **View** to view the details of the selected time zone.
8. **Optional:** Check **Restore Default Settings** to restore the configured device parameters to default settings.
9. Click **Add** to add the device to the device list.
10. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Refresh Device	Click ↻ in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).

Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information. **Note** If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Search for Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

Add Detected Online Payment Terminals in a Batch

For the detected online payment terminals, if they have the same user name and password, you can batch add multiple devices to the platform.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Payment Terminal** on the left panel.
3. In the Online Device area, select a network type.

   Server Network

   The detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

   The detected online devices on the same local subnet with the Web Client will be listed in the Online Device area.
4. In the Online Device area, select the active devices to be added.
5. Click **Add to Device List** to open the adding online device window.
6. Set the basic information for the device.

   User Name

The user name for administrator account created when activating the device or the added non-admin account such as the operator. When adding the device to HikCentral Professional using the non-admin account, your permission may restrict your access to certain features.

Password

The password required to access the account.

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.

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

   Note

   You can click **View** to view the details of the selected time zone.
8. Click **Add** to add the devices to the device list.
9. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Refresh Device	Click ↻ in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).
Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Search for Device Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.8.2 Add Payment Terminal by IP Address

When you know the IP address of a device, you can add it to the platform by specifying the IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Payment Terminal** on the left panel.
3. Click **Add**.
4. Select **IP Address** as the adding mode.
5. Set the basic information for the device.

   Device Address

   The IP address of the device, which is shown automatically.

   Device Port

   The port number of the device, which is shown automatically. The default port number is 80.

   Device Name

   Create a descriptive name for the device.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as the operator. When adding the device to HikCentral Professional using the non-admin account, your permission may restrict your access to certain features.

   Password

   The password required to access the account.

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.

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

   Note

   You can click **View** to view the details of the selected time zone.
7. **Optional:** Check **Restore Default Settings** to restore the configured device parameters to default settings.
8. Finish adding devices.
   - Click **Add** to add the device and go back to the device list page.
   - Click **Add and Continue** to add the device and continue to add other devices.
9. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Refresh Device	Click ↻ in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).
Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Search for Device Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.8.3 Add Payment Terminal by IP Segment

When multiple payment terminals 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.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Payment Terminal** on the left panel.
3. Click **Add**.
4. Select **IP Segment** as the adding mode.
5. Enter the required information.

Device Address

Enter the start IP address and the end IP address where the devices are located.

Device Port

The port number of the device. The default device port number is 80.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as the operator. When adding the device to HikCentral Professional using the non-admin account, your permission may restrict your access to certain features.

Password

The password required to access the device.

Caution

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

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

   Note

   You can click **View** to view the details of the selected time zone.
7. Finish adding devices.
   - Click **Add** to add the devices and go back to the device list page.
   - Click **Add and Continue** to add the devices and continue to add other devices.
8. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Refresh Device	Click ↻ in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).
Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.

Note

If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.

Search for Device Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.8.4 Add Payment Terminals in a Batch

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.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Payment Terminal** on the left panel.
3. Click **Add**.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (excel file) to your PC.
6. Open the template file and enter the required information of the devices to be added.
7. Click and select the edited file.
8. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone** to get the device's time zone.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
9. Finish adding devices.
   - Click **Add** to add the devices and go back to the device list page.
   - Click **Add and Continue** to add the devices and continue to add other devices.
10. **Optional:** Perform the following operations after adding devices.

Remote Configuration Click in the Operation column to configure the device remotely.

	Note For details about remote configuration, see the user manual of the device.
Refresh Device	Click in the Operation column to refresh the device. Click **Refresh All** to refresh all the devices in the list.
Change Password	Select the device(s), and click **Change Password** to change the password for the device(s).
Delete Device	Select the device(s), and click **Delete** to delete the selected device(s).
Set Time Zone	Select the device(s), and click **Time Zone** to set/edit the time zone of the selected device(s).
Restore Default Settings	Select the device(s), and click **Restore Default Settings** to restore the configured device parameters excluding network parameters and account information.
	Note If you want to restore all the device parameters, you should check **Restore device network parameters and account information, such as user name and password.** in the pop-up window.
Search for Device	Enter keyword(s) in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.9 Manage On-Board Devices

On-board devices are used for driving monitoring. They support live view, playback, remote configuration, alarm notification, GPS data collection, GPS positioning, etc. With on-board devices, you can not only get the GPS information of driving vehicles, but also set fence rules and deviation rules to regulate vehicles' movements (the platform will generate an event if any rule is violated). On the Web Client, you can manage on-board devices, including adding, editing, deleting, and remotely configuring them.

9.9.1 Add Detected Online On-Board Devices

The active online on-board devices on the same local subnet with the Web Client or SYS server will be displayed on the list. You can add online devices one by one or add multiple online devices in a batch.

Note

You should follow the instructions to install the web control properly and then the online device detection function will be available.

Add a Detected Online On-Board Device

The Web Client automatically searches for online on-board devices on the same local subnet with it or the SYS server. You can add detected online on-board devices to the platform one by one if they do not share the same user account.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **On-Board Device** .
2. Select a detected online on-board device from the Online Device list.
3. Click **Add to Device List**.

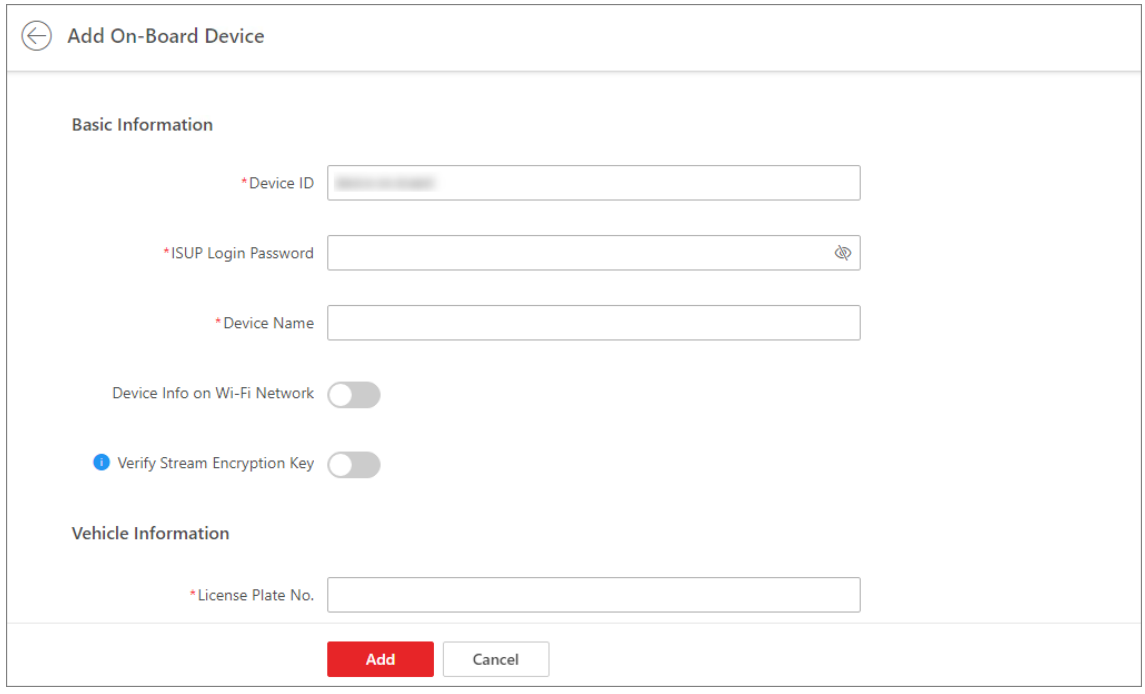


Figure 9-7 Add a Detected Online On-Board Device

4. Set basic information.

1) Enter the ISUP login password and name of the on-board device.

Caution

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

2) **Optional:** Switch on **Device Info on Wi-Fi Network** and enter the address and port of the on-board device as well as the user name and password of the Wi-Fi.

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.

3) **Optional:** Switch on **Verify Stream Encryption Key** and enter the stream encryption key set on the on-board device.

Note

The precondition is that the on-board device supports stream encryption and this feature has been enabled for it.

When starting live view or remote playback of the cameras related to the on-board device, the Client will verify the key stored in the SYS server for security purpose.

5. Set vehicle information.

1) Enter the license plate number of the vehicle the on-board device is related to.
2) Add the vehicle to an existing area or click **Add** to add it to a newly-created area.

6. Optional: Set picture storage.

1) Switch on **Picture Storage**.
2) Select a storage location.

Note

- If you select **Local Storage**, you need to click **Configure** to configure picture storage on the SYS server.
- If you select **Hybrid Storage Area Network**, **Cluster Storage**, **pStor**, or **Network Video Recorder**, you need to select a storage medium from the drop-down list.

7. Set device's time zone.

- **Get Device's Time Zone**

  The time zone of the device will be automatically chosen according to the region of the device.

- **Manually Set Time Zone**

  You can select a time zone and the settings will be applied to the device automatically.

8. Set resource information.
   1) Select a Streaming Server.
   2) **Optional:** Check **Wall Display via Streaming Server**.

   Note

   If the encoding device is not on the same network with cameras, it will get the stream for live view and playback via the Streaming Server, if they are on the same network, the encoding device can get stream directly from cameras.

   3) **Optional:** Check **Get Device's Recording Settings** to get cameras' recording settings configured on the on-board device.
9. Click **Add**.
10. **Optional:** Perform the following operations after adding the on-board device.

Edit On-Board Device	On the device list, click the name of an on-board device to edit it.
Configure On-Board Device Remotely	On the device list, click in the Operation column to configure an on-board device remotely.
Reset Device's Time Zone	In the device list, select one or multiple on-board devices and click **Time Zone** to edit their time zones.
Delete On-Board Device	Select one or multiple devices and click **Delete** to delete them.
Search for On-Board Device(s)	Enter one or multiple key words in the search box and click to search for the specified on-board device(s).

Add Detected Online On-Board Devices in a Batch

The Web Client automatically searches for online on-board devices on the same local subnet with it or the SYS server. You can batch add multiple detected online on-board devices to the platform if they share the same user account.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **On-Board Device** .
2. Select some detected online on-board devices from the Online Device list.
3. Click **Add to Device List**.

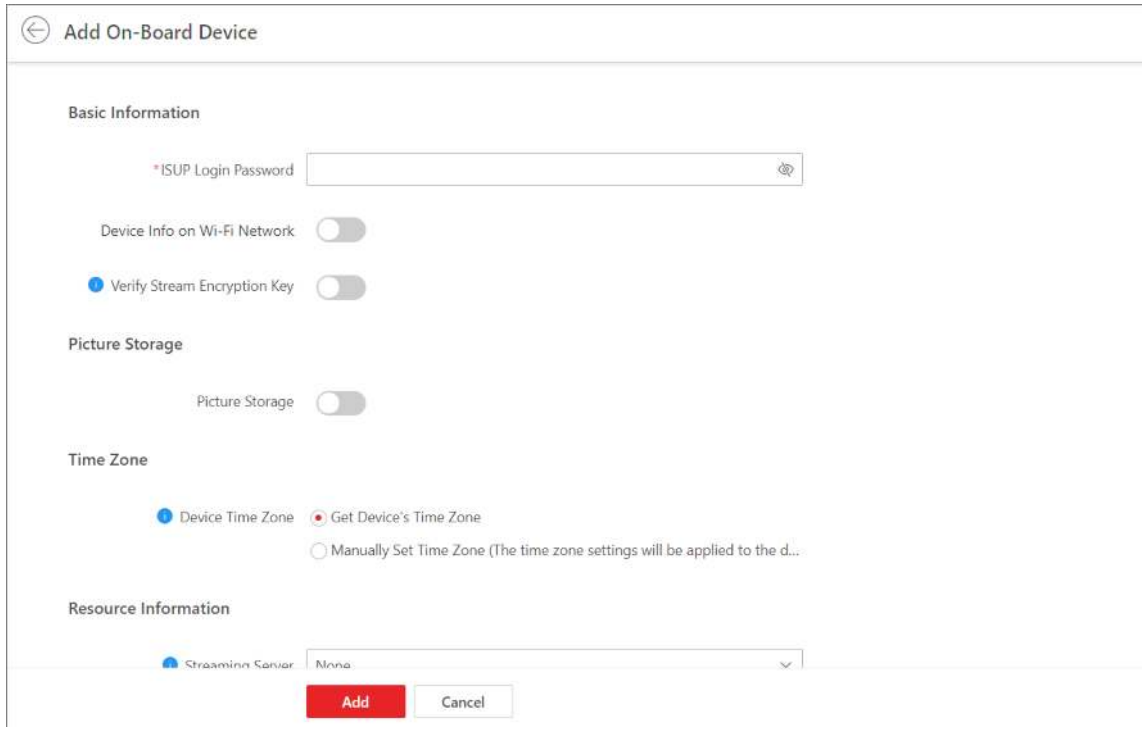


Figure 9-8 Batch Add Detected Online On-Board Devices

4. Set basic information.

1) Enter the ISUP login password of the on-board devices.

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.

2) **Optional:** Switch on **Device Info on Wi-Fi Network** and enter the address and port of the on-board devices 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.

3) **Optional:** Switch on **Verify Stream Encryption Key** and enter the stream encryption key set on the on-board devices.

Note

The precondition is that the on-board devices supports stream encryption and this feature has been enabled for them.

When starting live view or remote playback of the cameras related to the on-board devices, the Client will verify the key stored in the SYS server for security purpose.

5. **Optional:** Set picture storage.
   1) Switch on **Picture Storage**.
   2) Select a storage location.

Note

- If you select **Local Storage**, you need to click **Configure** to configure picture storage on the SYS server.
- If you select **Hybrid Storage Area Network**, **Cluster Storage**, **pStor**, or **Network Video Recorder**, you need to select a storage medium from the drop-down list.

6. Set devices' time zone.

Get Device's Time Zone

The time zone of the device will be automatically chosen according to the region of the device.

Manually Set Time Zone

You can select a time zone and the settings will be applied to the device automatically.

7. Set resource information.
   1) Select a Streaming Server.
   2) **Optional:** Check **Wall Display via Streaming Server**.

Note

If the encoding device is not on the same network with cameras, it will get the stream for live view and playback via the Streaming Server. If they are on the same network, the encoding device can get stream directly from cameras.

   3) **Optional:** Check **Get Device's Recording Settings** to get cameras' recording settings configured on the on-board device.
8. Click **Add**.
9. **Optional:** Perform the following operations after adding these on-board devices.

Edit On-Board Device	On the device list, click the name of an on-board device to edit it.
Configure On-Board Device Remotely	On the device list, click ⚙ in the Operation column to configure an on-board device remotely.
Reset Device's Time Zone	On the device list, select one or multiple on-board devices and click **Time Zone** to edit their time zones.
Delete On-Board Device	Select one or multiple devices and click **Delete** to delete them.

Search for On-Board Device(s)	Enter key words in the search box and click to search for specified on-board device(s).

9.9.2 Add an On-Board Device by Device ID

If an on-board device supports the ISUP protocol, you can add it to the platform by its device ID. This way is cost-effective when you need to manage an on-board device on the public network without a fixed IP address.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **On-Board Device** .
2. Click**Add**.

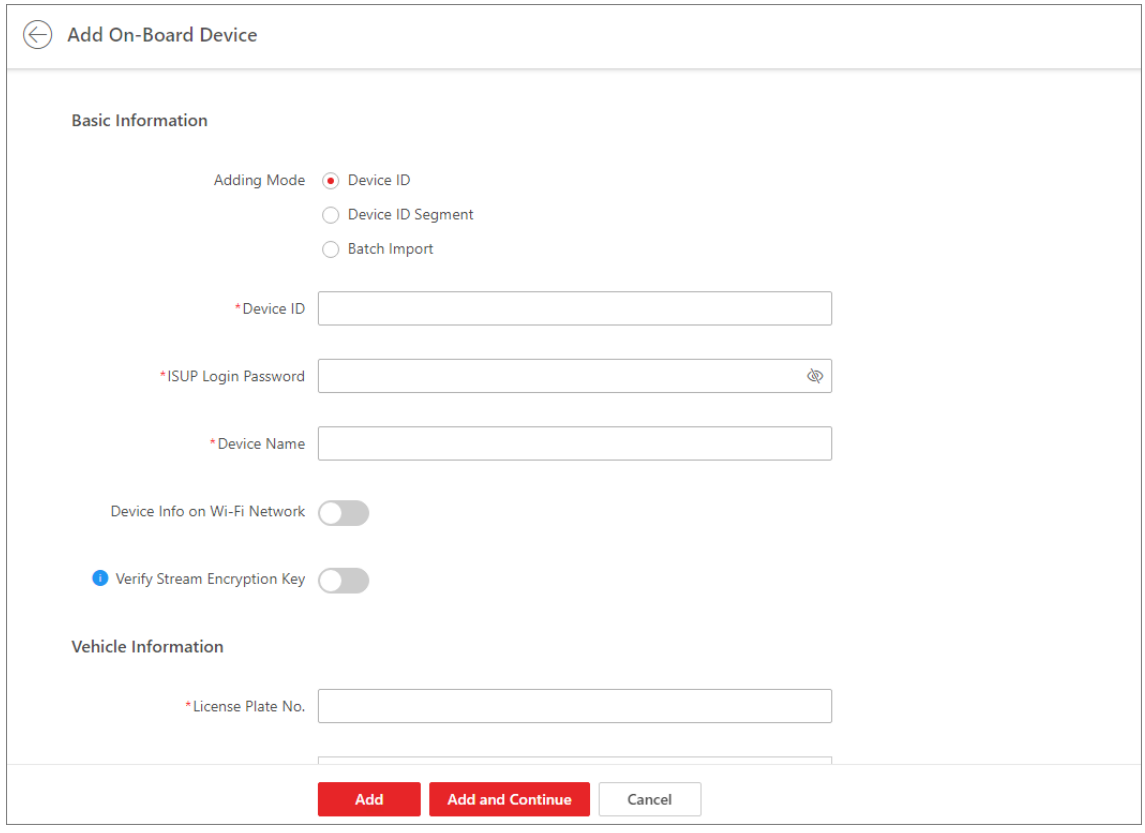


Figure 9-9 Add On-Board Device

3. Set basic information.
   1) Select **Device ID** as the adding mode.
   2) Enter the ID, ISUP login password, and name of the on-board device.
   3) **Optional:** Switch on **Device Info on Wi-Fi Network** 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.

   4) **Optional:** Switch on **Verify Stream Encryption Key** and enter the stream encryption key set on the on-board device.

      Note

      The precondition is that the on-board device supports stream encryption and this feature has been enabled for it.

      When starting live view or remote playback of the cameras related to the on-board device, the Client will verify the key stored in the SYS server for security purpose.
4. Set vehicle information.
   1) Enter the license plate number of the vehicle the on-board device is related to.
   2) Add the vehicle to an existing area or click **Add** to add it to a newly-created area.
5. **Optional:** Set picture storage.
   1) Switch on **Picture Storage**.
   2) Select a storage location.

      Note

      - If you select **Local Storage**, you need to click **Configure** to configure picture storage on the SYS server.
      - If you select **Hybrid Storage Area Network**, **Cluster Storage**, **pStor**, or **Network Video Recorder**, you need to select a storage medium from the drop-down list.
6. Set device's time zone.

   Get Device's Time Zone

   The time zone of the device will be automatically chosen according to the region of the device.

   Manually Set Time Zone

   You can select a time zone and the settings will be applied to the device automatically.
7. Set resource information.
   1) Select a Streaming Server.
   2) **Optional:** Check **Wall Display via Streaming Server**.

Note

If the encoding device is not on the same network with cameras, it will get the stream for live view and playback via the Streaming Server, if they are on the same network, the encoding device can get stream directly from cameras.

3) **Optional:** Check **Get Device's Recording Settings** to get cameras' recording settings configured on the on-board device.

8. Click **Add** to finish or click **Add and Continue** to add another on-board device.
9. **Optional:** Perform the following operations after adding the on-board device.

Edit On-Board Device	On the device list, click the name of an on-board device to edit it.
Configure On-Board Device Remotely	On the device list, click in the Operation column to configure an on-board device remotely.
Reset Device's Time Zone	On the device list, select one or multiple on-board devices and click **Time Zone** to edit their time zones.
Delete On-Board Device	Select one or multiple devices and click **Delete** to delete them.
Search for On-Board Device(s)	Enter key words in the search box and click to search for specified on-board device(s).

9.9.3 Add On-Board Devices by Device ID Segment

You can add on-board device(s) to the platform by device ID segment, and perform further operations, such as editing device settings, configuring devices remotely, deleting devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **On-Board Device** .
2. Click **Add**.
3. Select **Device ID Segment** as the adding mode.

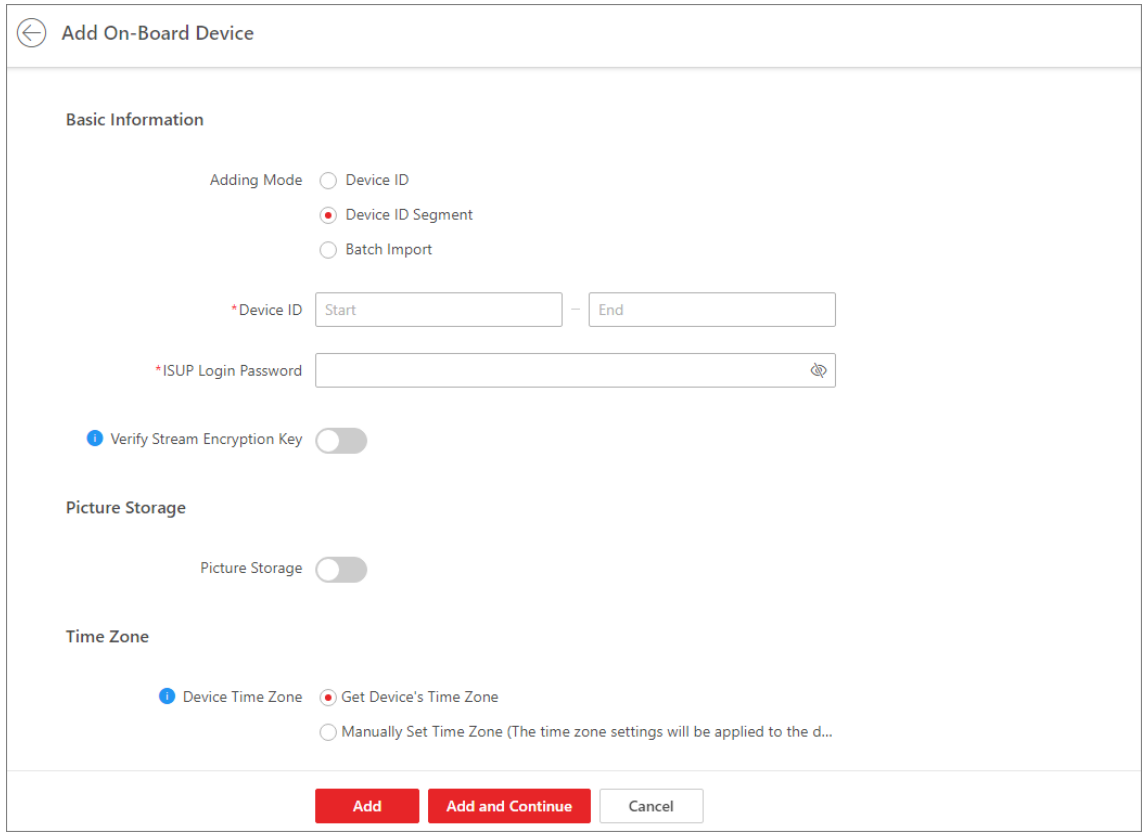


Figure 9-10 Add On-Board Device by Device ID Segment

4. Configure the basic information of the device(s).
   1) Enter the start device ID and end device ID.

   Note

   - If the start ID and end ID are the same, only one device will be added.
   - If the start ID is smaller than the end ID, multiple devices will be added with their IDs arranged in ascending order. For example, if you set the start ID and end ID to 1 and 3 respectively, then devices named 1, 2, and 3 will be added.

   2) **Optional:** Enter the ISUP login password.
   3) **Optional:** Enabled stream encryption, and switch on **Verify Stream Encryption Key** and enter the stream encryption key on the device.

   Note

   This function should be supported by the device.
5. Configure picture storage for the device(s).
   1) Switch on **Picture Storage**.
   2) Select a storage server type and a storage server from the drop-down list as the storage location.
6. **Optional:** Set the time zone for the device.

- **Get Device's Time Zone**

  The time zone of the device will be automatically chosen according to the region of the device.

- **Manually Set Time Zone (The settings will be applied to the device automatically)**

  You can select a time zone of the device. The settings will be applied to the device automatically.

7. Configure the resource information.
   1) Select a streaming server from the drop-down list.
   2) **Optional:** Check **Wall Display via Streaming Server** to use the Streaming Server to play videos on the smart wall.

   Note

   This parameter is configurable only when you select a Streaming Server in the former substep.

   3) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the device.
8. Click **Add** to finish, or click **Add and Continue** to add other device(s).
9. **Optional:** Perform the following operation(s) if needed.

Edit Device Settings	Click the name of a device in the Device Name column to edit its settings.
Delete Device	In the device list, check one or multiple devices, and click **Delete** to delete the device(s).
Configure Device Remotely	• Option 1: Click ⚙ in the Operation column to configure the device remotely. • Option 2: Click the name of a device to enter its settings page, and then click **Configuration on Device** in the upper-right corner to configure the device remotely. **Note** To support remote configuration, the device should be configured with an IP address.
Edit Device's Time Zone	On the device list, check a device, and click **Time Zone** to edit its time zone settings. You can also check multiple devices and configure the same time zone for them.
Search for On-Board Device(s)	Enter one or multiple key words in the search box and click 🔍 to search for specified on-board device(s).

9.9.4 Add On-Board Devices in a Batch

You can fill in required information of to-be-added on-board devices in an Excel file and upload it onto the platform to batch add them for management.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top left of the Web Client, click → **Device** → **Device and Server** → **On-Board Device** .
2. Click **Add**.

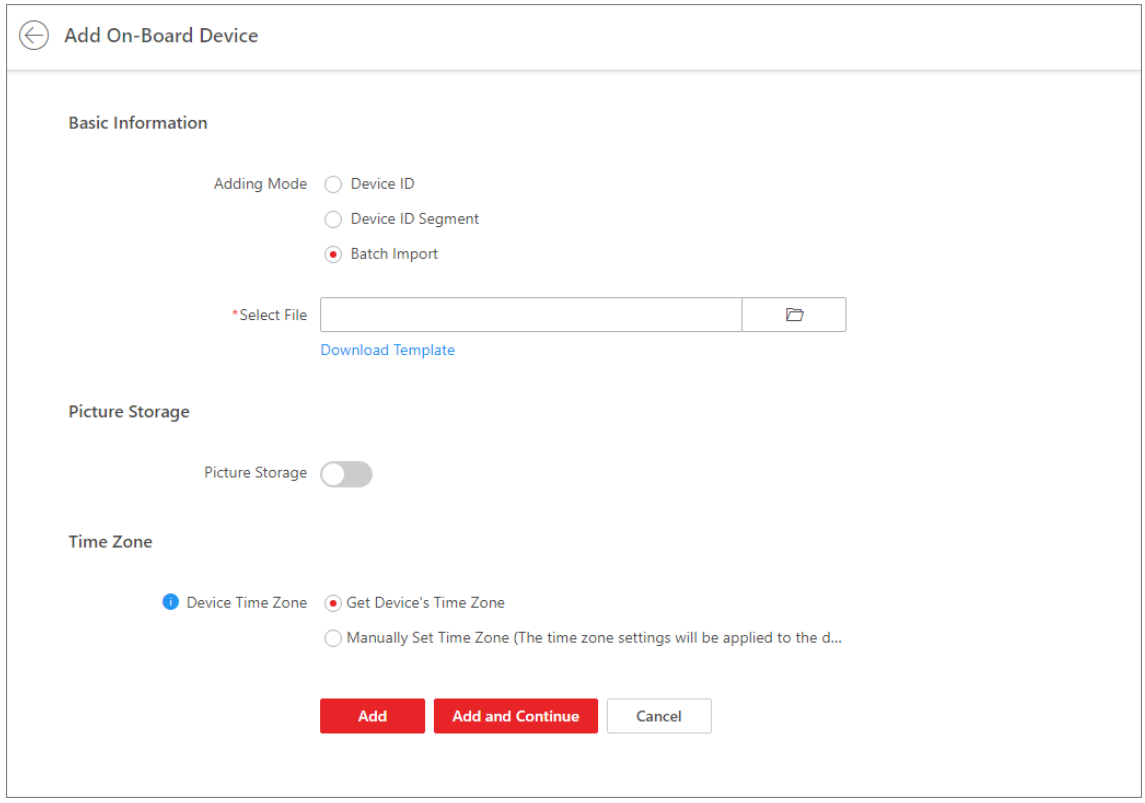


Figure 9-11 Batch Add On-Board Devices

3. Set basic information.
   1) Select **Batch Import** as the adding mode.
   2) Click **Download Template** to save the template file to your PC and fill in required information.
   3) Click to select the file and upload it to the platform.
4. **Optional:** Set picture storage.

1) Switch on **Picture Storage**.
2) Select a storage location.

Note

- If you select **Local Storage**, you need to click **Configuration** to configure picture storage on the SYS server.
- If you select **Hybrid Storage Area Network**, **Cluster Storage**, **pStor**, or **Network Video Recorder**, you need to select a storage medium from the drop-down list.

5. Set devices' time zone.
   - **Get Device's Time Zone**

     The time zone of the device will be automatically chosen according to the region of the device.
   - **Manually Set Time Zone**

     You can select a time zone and the settings will be applied to the device automatically.
6. Click **Add** to finish or click **Add and Continue** to add another batch of on-board devices.
7. **Optional:** Perform the following operations after adding these on-board devices.

Edit On-Board Device	On the device list, click the name of an on-board device to edit it.
Configure On-Board Device Remotely	On the device list, click in the Operation column to configure an on-board device remotely.
Reset Device's Time Zone	On the device list, select one or multiple on-board devices and click **Time Zone** to edit their time zones.
Delete On-Board Device	Select one or multiple devices and click **Delete** to delete them.
Search for On-Board Device(s)	Enter key words in the search box and click to search for specified on-board device(s).

9.10 Add a Query Terminal

A query terminal is installed with the Self-Service Vehicle Finding Client and is mounted in a parking lot for vehicle owners to locate and find their vehicles. On the Web Client, you can add a query terminal by its device ID and further manage it such as editing its information and removing it from the platform.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **Query Terminal** on the left navigation pane.
3. Click **Add** to enter the Add Query Terminal page.

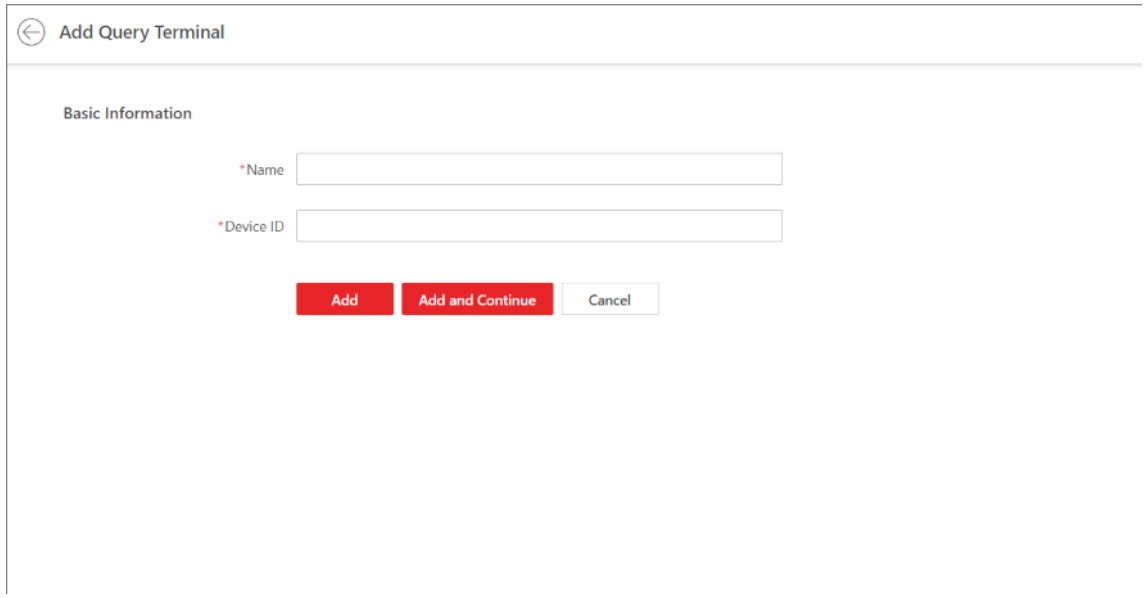


Figure 9-12 Add Query Terminal

4. Create a name for the query terminal.
5. Enter the device ID of the query terminal.
6. Click **Add** to finish, or click **Add and Continue** to add another query terminal.
7. **Optional:** Perform the following operations.

Edit Query Terminal	On the device list, click the name of a query terminal to edit it.
Delete Query Terminal	Select one or multiple query terminals, and click **Delete** to delete them.
Search for Query Terminal	Enter key words in the search box, and click to search for specified query terminal.

9.11 Add an Entrance/Exit Control Device

An entrance/exit control device is used for managing the entrance or exit of a parking lot, especially that of an unattended parking lot. After a vehicle gets a ticket or card from an entrance/exit control device, the device will control the barrier gate to open and let the vehicle enter. After the vehicle returns the ticket or card, the device will allow the vehicle to exit. Besides, if an entrance/exit control device issues cards instead of tickets, its guidance screen is configurable, which means you can configure the information displayed on it.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module,
2. Select **Device and Sever** → **Entrance/Exit Control Device** on the left navigation pane.
3. Click **Add** to enter the Add Entrance/Exit Control Device page.

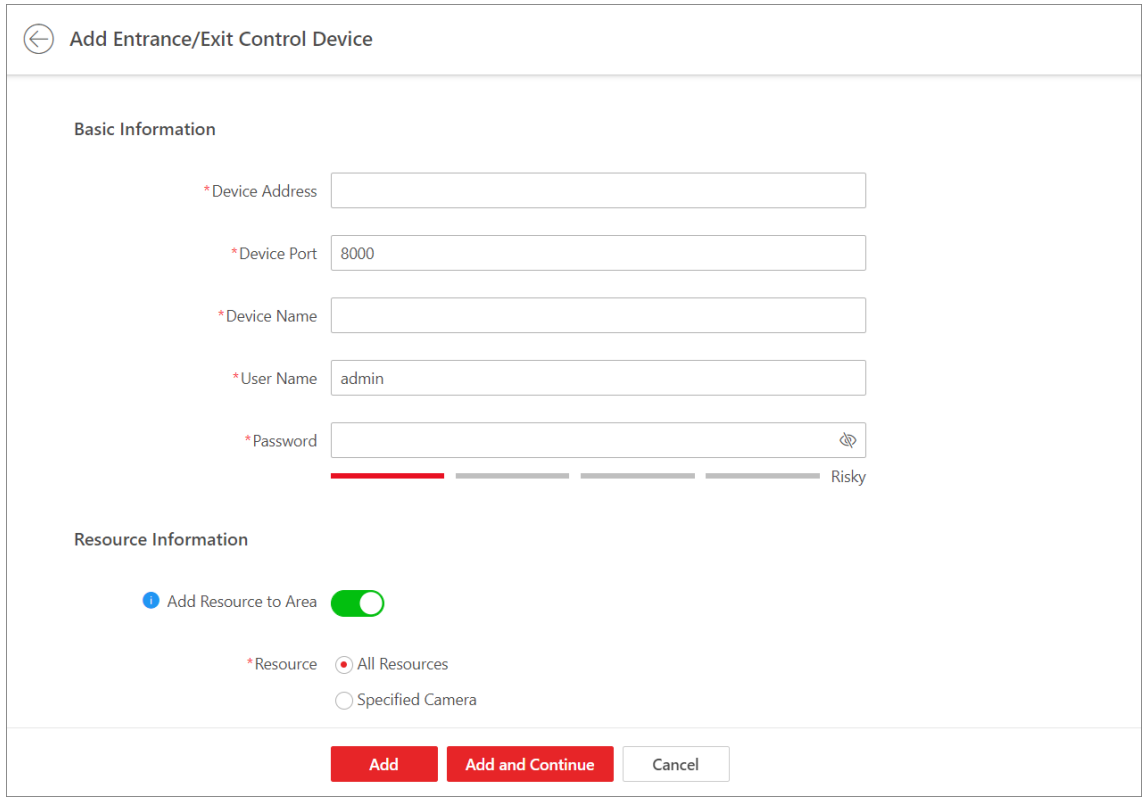


Figure 9-13 Add Entrance/Exit Control Device Page

4. In the Basic Information area, enter the IP address, port No., device name, user name, and password of the entrance/exit control device.
5. **Optional:** Add the entrance/exit control device's related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **All Resources** or **Specified Camera**.

   Note

   If you select **All Resources**, all the resources related to the entrance/exit control device will be added to an area; if you select **Specified Camera**, you need to select camera(s) to add.

   3) Select **Create Area by Device Name** or **Existing Area**.

Note

If you select **Create Area by Device Name**, an area named after the entrance/exit control device will be created, and the resource(s) will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area. For details, refer to ***Add an Area for Current Site*** .

4) Select **None** or a streaming server to get the stream for live view and playback.

Note

After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.

5) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the entrance/exit control device.

6. Click **Add** to finish or click **Add and Continue** to add another entrance/exit control device.
7. **Optional:** Perform the following operations.

Edit Entrance/Exit Control Device	In the Device Name column, click the name of an entrance/exit control device to edit it.
Delete Entrance/Exit Control Device	Select one or multiple entrance/exit control devices and click **Delete** to delete them.
Configure Entrance/Exit Control Device Remotely	In the Operation column, click to configure the entrance/exit control device remotely.
Refresh Device Information	In the Operation column, click to refresh the entrance/exit control device's information.
Search for Device	Enter a keyword in the search box and click to search for a specific device.

9.12 Manage Guidance Terminals

In Resource Management, you can add guidance terminals to the platform, check device details, change device password, and configure device parameters. While you add a guidance terminal, you can add its resources (such as connected parking cameras and alarm inputs/outputs) to areas for further configurations.

Note

After you add and manage guidance terminals int Resource Management, you can set up a parking guidance system for your parking lot. See details in ***Parking Guidance Configuration*** .

9.12.1 Add Detected Online Guidance Terminals

The platform can automatically detect the available guidance terminals on the same network where the Web Client or the SYS server is running. You can add one online terminal at a time, or batch add multiple online terminals if they have the same user name and password.

添加□个在□□□管理器

添加在□□□□，若每次需要添加一台在□□□或者添加多台用□名或密□不同的□□管理器，此□可以□□逐个添加□个在□□□管理器到系□。

Before You Start

- 确保□□已正确安装并成功□接到指定网□。□了能通□网□将□□□接至 iSecure VMS，必□□行□□的初始配置。
- 确保待添加的□□已激活。激活□□的□□步□参□。

Steps

1. 在主□左上角，□□ → **全部功能** → **通用** → **□□管理**。
2. 在左□□□ **□□和服□器** → **□□管理器**。
3. 在**在□□□**区域□□一种网□□型。

   服□器网□

   默□□□，□索与系□管理服□器位于同一网段内的在□□□，并以列表形式展□。

   本地网□

   □索与当前配置客□端位于同一网段内的在□□□，并以列表的形式展□。
4. 在**在□□□**区域勾□一个已激活的□□□行添加。
5. □□**添加至□□列表**□入添加在□□□窗口。
6. 在基本信息区域可以□置相关信息。

   □□地址

   □□ IP 地址，会自□□取。

   □□端口

   □□端口号。默□端口号□ 8000。

   名称

   □□□命名。可以通□□□名称体□□□功能或地点。

   用□名

   激活□□□□建的管理□□□用□名，或添加的非管理□□□（如操作人□□□）的用□名。

   Note

   当通□非管理□□号添加□□□，您的□限可能会受到限制。

   密□

□□□□所需的密□。

7. **Optional:** 开启**添加□源到区域**□入□□□源到一个区域。

Note

- 可以□入所有□源，包括□控点、□警□入和□警□出，或□入□□区域的特定□控点。
- 可以根据□□名称新建一个区域或□□一个已有区域。
- 若不□入□源到一个区域，就无法□行□控点相关操作。

8. **Optional:** 若□□添加□源到区域，在**流媒体服□器**中□□一个服□器，通□□服□器□取□控点的□□□流。

Note

可以勾□□**控点上□□使用流媒体**，□□上□□通□所□流媒体服□器□取□流。

9. **Optional:** 若□□添加□源到区域，开启□**像存**□并□□一个□像存□位置。

□□□□

□□文件将根据配置的□像□划存□至□□□□本地。

CVR

□□文件将根据配置的□像□划存□至 CVR 服□器上。

Note

需事先配置 CVR，否□下拉列表中不会□示以上存□方式。

10. **Optional:** 配置□□□像□划。
    - 勾□□**取□□的□像□划□置**从□□□取□像□划，□□通道将根据□□划开始□像。
    - 不勾□□**取□□的□像□划□置**，□需手□□置□像□划参数，包括□**像□划模板**、□**流□型**、□□等信息。
11. 完成□□添加。
    - 点□**添加**完成□□添加，并返回至□□列表□面。
    - 点□**添加并□□**完成□□添加，并□□添加新的□□。
12. **Optional:** 添加□□后，可□行以下操作。

□程配置	点□**操作**□中的 □程配置□□。 **Note** 关于□程配置的□□操作步□，□参考□□的用□手册。
修改密□	□中已添加的一台或多台□□并点□**修改密□**。 **Note** • 只支持更改在□海康□□的密□。 • 若多个□□的当前密□相同，可以同□修改多台□□密□。

Batch Add Detected Online Guidance Terminals

You can batch add detected online guidance terminals if the terminals have the same user name and password.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **Guidance Terminal** on the left navigation pane.
3. In the Online Device area, select a network type.

   Server Network

   All detected online devices on the same local subnet with the SYS server.

   Local Network

   All detected online devices on the same local subnet with the current Web Client.
4. Select multiple activated devices and click **Add to Device List**.
5. In the Basic Information area, edit devices' login information.

   User Name

   User name of administrator account created when activating the device, or the added non-admin account such as operator account.

   Note

   Your access to certain features might be restricted when using a non-admin account to add the device to the platform.

   Password

   Password of the account that you are logging in.

   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.

6. **Optional:** Add guidance terminals related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **Create Area by Device Name** or **Existing Area**.

   Note

   If you select **Create Area by Device Name**, an area named after guidance terminals will be created, and resources will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area. For details, refer to ***Add an Area for Current Site*** .
   3) Select **None** or a streaming server to get the stream for live view and playback.

   Note

   After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.
   4) Switch on **Video Storage** to select a storage location for recorded videos and set recording schedule for the cameras.

   Note

   - The pStor is the storage access service for managing local HDDs and logical disks.
   - The pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors.
   - Before you can select **Hybrid Storage Area Network**, **Cloud Storage**, or **pStor** from the storage location list, you should configure them. You can also click **Add New** to add a new one.
   - You can check **Get Device's Recording Settings** to get camera's recording settings configured on the guidance terminal and the linked camera(s) will start recording according to the schedule, or uncheck **Get Device's Recording Settings** and set the recording schedule for the cameras, such as recording schedule template and stream type. For details about recording schedule configuration, refer to ***Configure Recording for Cameras on Current Site*** .
7. Click **Add**.
8. **Optional:** Perform further operations after batch adding online devices.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click ⚙ in the **Operation** column to enter the remote configuration page of a device.

Refresh Device Information	In the Operation column, click to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device.

Note

- You can change the password for online HIKVISION devices only.
- If multiple devices have the same password, you can select these devices to batch change the password for them.

9.12.2 Add a Guidance Terminal by IP Address

If you know the IP address of the guidance terminal you want to add to the platform, you can add the device by specifying its IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **Guidance Terminal** on the left navigation pane.
3. Click **Add** to open the Add Guidance Terminal page.
4. Set **Adding Mode** to **IP Address**.
5. Edit the device connection and login information.

   Device Name

   Create a descriptive name for the device. For example, you can use an alias that can indicate the location or feature of the device.

   User Name

   User name of the administrator account created when activating the device, or the added non-admin account such as operator account.

   Note

   Your access to certain features might be restricted when using a non-admin account to add the device to the platform.

Password

Password of the account that you are logging in.

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.

6. **Optional:** Add the guidance terminal's related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **All Resources** or **Specified Camera**.

      Note

      If you select **All Resources**, all the resources related to the guidance terminal will be added to an area; if you select **Specified Camera**, you need to select the camera(s) to add.
   3) Select **Create Area by Device Name** or **Existing Area**.

      Note

      If you select **Create Area by Device Name**, an area named after the guidance terminal will be created, and the resource(s) will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area. For details, refer to ***Add an Area for Current Site*** .
   4) Select **None** or a streaming server to get the stream for live view and playback.

      Note

      After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.
   5) Switch on **Video Storage** to select a storage location for recorded videos and set recording schedule for the cameras.

      Note

      - The pStor is the storage access service for managing local HDDs and logical disks.
      - The pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors.

- Before you can select **Hybrid Storage Area Network**, **Cloud Storage**, or **pStor** from the storage location list, you should configure them. You can also click **Add New** to add a new one.
- You can check **Get Device's Recording Settings** to get camera's recording settings configured on the guidance terminal and the linked camera(s) will start recording according to the schedule, or uncheck **Get Device's Recording Settings** and set the recording schedule for the cameras, such as recording schedule template and stream type. For details about recording schedule configuration, refer to ***Configure Recording for Cameras on Current Site*** .

7. Click **Add** to finish or click **Add and Continue** to add another guidance terminal.
8. **Optional:** Perform further operations after adding a guidance terminal.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device. **Note** • You can change the password for online HIKVISION devices only. • If multiple devices have the same password, you can select these devices to batch change the password for them.

9.12.3 Batch Add Guidance Terminals by IP Segment

If the guidance terminals you want to add to the platform are on the same subnet and share the same port, user name, and password, you can add them by specifying the start and end IP address, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **Guidance Terminal** on the left navigation pane.
3. Click **Add** to open the Add Guidance Terminal page.
4. Set **Adding Mode** to **IP Segment**.
5. Edit the device connection and login information.

   Device Address

   Start IP address and end IP address.

   User Name

   User name of the administrator account created when activating the device, or the added non-admin account such as operator account.

   Note

   Your access to certain features might be restricted when using a non-admin account to add the device to the platform.

   Password

   Password of the account that you are logging in.

   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.
6. **Optional:** Add the guidance terminal's related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **Create Area by Device Name** or **Existing Area**.

      Note

      If you select **Create Area by Device Name**, an area named after the guidance terminal will be created, and the resource(s) will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area. For details, refer to ***Add an Area for Current Site*** .
   3) Select **None** or a streaming server to get the stream for live view and playback.

Note

After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via Streaming Server** to get the stream from the streaming server when displaying live view or playback on the smart wall.

4) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the guidance terminal.

7. Click **Add** to finish or click **Add and Continue** to add guidance terminals with another IP segment.
8. **Optional:** Perform further operations after adding guidance terminals.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device.

Note

- You can change the password for online HIKVISION devices only.
- If multiple devices have the same password, you can select these devices to batch change the password for them.

9.12.4 Batch Add Guidance Terminals by Port Segment

If the guidance terminals you want to add to the platform share the same IP address, user name, and password, but they are using different ports, you can add them by specifying the IP address, port range, user name, password, etc.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for detailed instructions on activating devices.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.

2. Select **Device and Server → Guidance Terminal** on the left navigation pane.
3. Click **Add** to open the Add Guidance Terminal page.
4. Set **Adding Mode** to **Port Segment**.
5. Edit the device connection and login information.

Device Port

Start port number and end port number of the devices.

User Name

User name of the administrator account created when activating the device, or the added non-admin account such as operator account.

Note

Your access to certain features might be restricted when using a non-admin account to add the device to the platform.

Password

Password of the account that you are logging in.

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.

6. **Optional:** Add the guidance terminal's related resource(s) to an area.
   1) In the Resource Information area, switch on **Add Resource to Area**.
   2) Select **Create Area by Device Name** or **Existing Area**.

Note

If you select **Create Area by Device Name**, an area named after the guidance terminal will be created, and the resource(s) will be added to the area. If you select **Existing Area**, you need to select an existing area to add the resource(s) to, or you can click **Add** to add a new area. For details, refer to ***Add an Area for Current Site*** .

   3) Select **None** or a streaming server to get the stream for live view and playback.

Note

After selecting a streaming server, its related camera(s) will be displayed, you can view their information and click the name of a camera to edit it. You can also check **Wall Display via**

Streaming Server to get the stream from the streaming server when displaying live view or playback on the smart wall.

4) **Optional:** Check **Get Device's Recording Settings** to get camera's recording settings configured on the guidance terminal.

7. Click **Add** to finish or click **Add and Continue** to add guidance terminals with another port segment.
8. **Optional:** Perform further operations after adding guidance terminals.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device. **Note** • You can change the password for online HIKVISION devices only. • If multiple devices have the same password, you can select these devices to batch change the password for them.

9.12.5 Batch Add Guidance Terminals by Template

You can download a predefined template and edit the guidance terminals' information in the template to add multiple devices at a time.

Before You Start

- Make sure the devices you are going to add 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 HikCentral Professional via network.
- Make sure you have activated the devices. Refer to ***Create Password for Inactive Device(s)*** for details.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **Guidance Terminal** on the left navigation pane.
3. Click **Add** to open the Add Guidance Terminal page.
4. Set **Adding Mode** to **Batch Import**.

5. Click **Download Template** to download the predefined template file (in XLSX format) to local disk.
6. In your download folder on PC, open the spreadsheet and edit the required device information.
7. On the Web Client, click and open the edited spreadsheet.
8. Click **Add** to finish or click **Add and Continue** to batch add guidance terminals by another spreadsheet.
9. **Optional:** Perform further operations after adding guidance terminals.

Edit Guidance Terminal	In the Device Name column, click the name of a guidance terminal to edit it.
Configure Device Remotely	Click in the **Operation** column to enter the remote configuration page of a device.
Refresh Device Information	In the Operation column, click to refresh a guidance terminal's information, or click **Refresh All** to refresh all the added guidance terminals' information.
Change Password	Select a device and click **Change Password** to change the password of the device.

Note

- You can change the password for online HIKVISION devices only.
- If multiple devices have the same password, you can select these devices to batch change the password for them.

9.13 Add Display Screen

Display screens can be used in places such as the entrance of a parking lot to show the real-time number of vacant parking spaces. You can add a display screen to the platform by specifying its LAN IP address.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **Display Screen** on the left navigation pane.
3. Click **Add** to open the Add Display Screen page.
4. Select a screen type (including Entrance and Exit Display Screen, Entrance Guidance Screen, and Indoor Guidance Screen) in **Device Type**.
5. Set parameters which vary among different types of display screens.

LAN IP Address

IP address assigned to the display screen on LAN.

Device Port

For entrance guidance screens and indoor guidance screens, the port No. is required.

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 9-14 Entrance Guidance Screen - One Row

Number of Directions

The number of directions supported by the indoor 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 9-15 Indoor Guidance Screen - Three Directions

6. Click **Add** to finish adding the display screen, or click **Add and Continue** to continue adding another display screen.
7. **Optional:** Perform the following operations after adding the screens.

Edit a Display Screen	In the Device Name column, click the name of a display screen to edit it.

Delete Device(s)	Check one or multiple devices in the list, and click **Delete** to delete the selected devices.
Search for Device	Enter the keyword(s) in the search box and click to search for a specific device.
Refresh Device Information	In the Operation column, click to refresh a display screen's information, or click **Refresh All** to refresh all the added display screens' information.

What to do next

- After adding an entrance and exit display screen or an entrance guidance screen, you can link a lane with the screen and configure the related information for the screen in Parking Lot Management. See details in ***Add Lane*** .
- After adding an indoor guidance screen, you can set up a parking guidance system for your parking lot in Parking Guidance Configuration. See details in ***Parking Guidance Configuration*** .

9.14 Add Under Vehicle Surveillance System

You can add Under Vehicle Surveillance System (UVSS) to the system by specifying the device IP address, port number and some other related parameters.

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 system via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management module.
2. Select **Device and Server** → **UVSS** on the left navigation pane.
3. Click **Add** to enter the Add Under Vehicle Surveillance System page.
4. Set the required basic information such as device address, device port number, and device name.
5. **Optional:** Switch on **Add Resource to Area** to import the resources of the added UVSS to an area.
   - Select **Create Area by Device Name** to create an area named after the UVSS for adding the resource(s) to the created area.
   - Select **Existing Area**, and select an existing area to add the resource(s) to.

Note

- If you select **Existing Area**, you can also click **Add** to add a new area. For details, refer to ***Add an Area for Current Site*** .
- If you do not import resources to area, you cannot perform the further configurations for the resources.

6. Click **Add** to finish adding the UVSS, or click **Add and Continue** to continue adding another UVSS.
7. **Optional:** Perform the following operations after adding UVSSs.

Edit a UVSS	In the Device Name column, click the name of a UVSS to edit it.
Delete Device(s)	Check one or multiple devices in the list, and click **Delete** to delete the selected devices.
Search for Device	Enter the keyword(s) in the search box and click to search for a specific device.
Refresh Device Information	In the Operation column, click to refresh a UVSS's information, or click **Refresh All** to refresh all the added UVSS' information.

9.15 Manage Security Control Device

You can add the security control devices to the system for managing partition, zone, arming/disarming, handling alarms,etc.

The security control device includes the security control panel, panic alarm station, Axiom wireless security control panel, security radar etc., which are widely applied to many scenarios. You can also add the channels (including cameras, alarm inputs, alarm outputs and radars) of the security control device to the area.

A security control panel is used for monitoring arming zones, handling alarm signal from the triggers, and uploading alarm reports to the central alarm monitoring station. The security control panel is very important for preventing robbery, theft or other accidents.

A panic alarm station is mainly installed in the areas with the crowd or high incidence of cases, such as school, square, tourist attraction, hospital, supermarket gate, market, station, parking lot, etc. When the emergency happens or someone asks for help, the person can press panic button to send alarm to the monitoring center, and the operator in the center will take the appropriate actions. The panic alarm station helps to realize alarm aid in emergency.

Security radar is an detecting device used to detect the target by electromagnetic wave. Security radar event will be triggered when the security radar detects object(s) entering the radar zone, and the calibration camera(s) will start to work to capture more details about this event.

9.15.1 Add Detected Online Security Control Devices

The active online security control devices in the same local subnet with the current Web Client or SYS server will be displayed on a list. You can add one online device one by one, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add a Detected Online Security Control Device

You can add the detected online security control devices, and here we introduce the process for adding single one device.

Before You Start

- Make sure the security control 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. 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 current Web Client will be listed in the Online Device area.
3. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.

   Note

   To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** and switch on **Allow ISUP Registration**.
4. In the Online Device area, select an active device to be added.
5. Click to open the Add Security Control Device window.
6. Enter the required information.

Note

The device's IP address and port number can be automatically shown in **Device Address** field and **Device Port** field.

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.

7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

   Note

   - You can select **Specified Alarm Input and Radar** and select the specified alarm inputs and radars to import to the area.
   - System will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform the further configurations for the resources.
9. Click **Add**.
10. **Optional:** Perform the following operations after adding the online device.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

Batch Add Detected Online Security Control Devices

For those detected online security control devices, if they have the same password for the same user name, you can add multiple devices at a time.

Before You Start

- Make sure the security control 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. On the top navigation bar, go to → **Basic Management** → **Device** → **Device and Server** → **Security Control Device** .
2. In the Online Device area, select a network type.

   Server Network

   The detected online devices in the same local subnet with the SYS server will list in the Online Device area.

   Local Network

   The detected online devices in the same local subnet with the Web Client will list in the Online Device area.
3. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.

   Note

   To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.
4. In the Online Device area, select the active devices to be added.

5. Click to open the Add Security Control Device window.
6. Enter the required information.

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.

7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

Note

- You can select **Specified Alarm Input and Radar** and select the specified alarm inputs or radars to import to the area.
- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform the further configurations for the resources.

9. Click **Add**.
10. **Optional:** Perform the following operations after adding the online devices in batch.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password.

Note

- You can only change the password for online HIKVISION devices currently.
- If multiple devices in the device list have the same password, you can change the password for them in a batch.

Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.15.2 Add Security Control Device by IP Address

When you know the IP address of the security control device to add, you can add the devices to the platform by specifying the IP address, user name, password, and other related parameters.

Before You Start

Make sure the security control 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 system via network.

Steps

1. On the top navigation bar, go to → **Basic Management** → **Device** → **Device and Server** → **Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **IP Address** as the adding mode.
5. Enter the required information.

Note

- By default, the device port is 8000.
- For wireless security control panels, the default port is 80.
- For alarm boxes, the default port is 502.

Device Address

Enter the IP address of the device.

Device Port

Enter the port number of the device.

Device Name

The name of the device, which can be used to describe the device function, location, etc.

User Name

The admin account (which is created when activating the device) or the non-admin account, such as the operator. If you use a non-admin account to add devices, the permissions might be limited.

Password

The password required to access the account.

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.

6. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
7. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs, and radars) of the added security control device to an area.

   Note

   - You can select **Specified Alarm Input and Radar** and select the specified alarm inputs or radars to import to the area.
   - Platform will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - Up to 64 alarm inputs can be imported in one area. If you don't import resources to area, you cannot perform further operations for the resources.
   - Up to 10 radars can be imported in one area. If you don't import radars to area, you cannot perform further operations for the radars.
8. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
9. **Optional:** Perform the following operations after adding the devices.

Note

The supported functions vary according to different device types.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.15.3 Add Security Control Device by Hik-Connect DDNS

You can add security control devices with dynamic IP addresses to the system by domain name solutions of Hik-Connect. Currently, the system only supports domain name solutions function of Hik-Connect.

Before You Start

Make sure the security control 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 system via network.

Steps

1. On the top navigation bar, go to → **Basic Management** → **Device** → **Device and Server** → **Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **Hik-Connect DDNS** as the adding mode.
5. Select a device source.

   New Device

Add a new device to both Hik-Connect and the system.

Hik-Connect DDNS Device List

Add devices managed by Hik-Connect to the system in a batch by getting the device list.

6. Set required parameters.

Hik-Connect DDNS Server Address

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

Note

If you select Hik-Connect DDNS Device List as the source type, you can click **Get Device List** to get the device list in the account.

Serial No.

For adding a new device, enter the serial No. of the device.

Verification Code

For adding a new device, enter the verification code of the device.

Device Name

The name of the device, which can be used to describe the device function, location, etc.

Site on Hik-Partner Pro

Select a site from the drop-down list and the device will also be added to the selected site on Hik-Partner Pro.

User Name

The admin account (which is created when activating the device) or the non-admin account, such as the operator. If you use a non-admin account to add devices, the permissions might be limited.

Password

The password required to access the account.

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.

7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

Note

You can click **View** to view the details of the selected time zone.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

Note

- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform the further configurations for the resources.

9. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
10. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.15.4 Add Security Control Devices by IP Segment

If the security control devices having the same port No., user name and password, and their IP addresses are between the IP segment, you can specify the start IP address and the end IP address, port No., user name, password, and other related parameters to add them.

Before You Start

Make sure the security control 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 system via network.

Steps

1. On the top navigation bar, go to → **Basic Management** → **Device** → **Device and Server** → **Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **IP Segment** as the adding mode.
5. Enter the required the information.

   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.
6. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the selected time zone.
7. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

Note

- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform the further configurations for the resources.

8. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
9. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.15.5 Add Security Control Devices by Port Segment

If the security control devices having the same user name and password, and their port No. are between the port segment, you can specify the start port No. and the end port No., user name, password, and other related parameters to add them.

Before You Start

Make sure the security control 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 HikCentral Professional via network.

Steps

1. On the top navigation bar, go to → **Basic Management** → **Device** → **Device and Server** → **Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** as the Access Protocol.
4. Select **Port Segment** as the adding mode.
5. Enter the required the information.

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.

6. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
7. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

   Note

   - System will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform the further configurations for the resources.
8. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
9. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click ⚙ to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.

Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.15.6 Add Security Control Device by Device ID

For the security control devices supporting ISUP, you can add them by specifying a predefined device ID, ISUP login password, etc. This is an economic choice when you need to manage a security control device in the public network but without fixed IP address by HikCentral Professional.

Before You Start

- Make sure the security control device 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 HikCentral Professional via network.
- Make sure you have enabled the ISUP registration function on the security control device. For details, refer to the user manual of security control device.

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision ISUP Protocol** as the access protocol.

   Note

   To allow device registration via ISUP, you need to go to → **Basic Management → System → Network → Device Access Protocol** and switch on **Allow ISUP Registration**.
4. Select **Device ID** as the adding mode.
5. Enter the required information, including device ID, ISUP login password, and device name.

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.

6. **Optional:** In the Picture Storage field, switch on **Picture Storage** and select a storage location from the drop-down list.
7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, alarm outputs and radars) of the added security control device to an area.

   Note

   - System will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to area, you cannot perform the further configurations for the resources.
9. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
10. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.15.7 Add Security Control Device by Device ID Segment

If you need to add multiple security control devices which have no fixed IP address and support ISUP to HikCentral, you can add them to HikCentral Professional at a time after configuring a device ID segment for the devices.

Before You Start

- Make sure the security control device 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 HikCentral Professional via network.
- Make sure you have enabled the ISUP registration function on the security control device. For details, refer to the user manual of security control device.

Steps

1. On the top navigation bar, go to → **Basic Management** → **Device** → **Device and Server** → **Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision ISUP Protocol** as the Access Protocol.

   Note

   To allow device registration via ISUP, you need to go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.
4. Select **Device ID Segment** as the adding mode.
5. Enter the required information, including the start device ID, the end device ID, and the ISUP login password.
6. **Optional:** In the Picture Storage field, switch on **Picture Storage**, and select a storage location from the drop-down list.
7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

Note

You can click **View** to view the details of the selected time zone.

8. **Optional:** Switch on **Add Resource to Area** to import the resources (including alarm inputs and radars) of the added security control device to an area.

Note

- System will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform the further configurations for the resources.

9. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list page.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
10. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.15.8 Batch Add Security Control Devices

You can edit the predefined template with the security control device information to add multiple devices at a time.

Before You Start

- Make sure the security control device 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 HikCentral Professional via network.
- Make sure you have enabled the ISUP registration function on the security control device when adding devices via Hikvision ISUP. For details, refer to the user manual of security control device.

Steps

1. On the top navigation bar, go to → **Basic Management** → **Device** → **Device and Server** → **Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.
3. Select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** as the Access Protocol.

   Note

   To allow device registration via ISUP, you need to go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (excel file) in your PC.
6. Open the exported template file and edit the required information of the devices to be added on the corresponding column.
7. Click and select the template file with device information.
8. **Optional:** In the Picture Storage field, switch on **Picture Storage**, and select a storage location from the drop-down list.

   Note

   This field displays only when you select **Hikvision ISUP Protocol** as the access protocol.
9. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the selected time zone.
10. Finish adding devices.
    - Click **Add** to add the devices and go back to the device list page.
    - Click **Add and Continue** to save the settings and continue to add other devices.
11. **Optional:** Perform the following operations after adding devices in a batch.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.

Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.15.9 Add Security Control Device from the Site on Hik-Partner Pro

If you have configured parameters for the site on Hik-Partner Pro accessing the platform, you can add security control devices from the site on Hik-Partner Pro to the platform. Deleting devices on the platform will not delete devices from the site on Hik-Partner Pro.

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 HikCentral Professional via network.
- Make sure you have enabled **Access on Hik-Partner Pro**. To complete related configuration, you can 1) go to → **Basic Management → System → Network → Hik-Partner Pro Access** or 2) click **Configure** in the Access Protocol area on the Add Security Control Device page. For details, refer to ***Set Hik-Partner Pro Site Access*** .

Steps

1. On the top navigation bar, go to → **Basic Management → Device → Device and Server → Security Control Device** .
2. Click **Add** to enter the Add Security Control Device page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.
3. Select **Hik-Partner Pro Protocol** as the access protocol.
4. Select the device source.
   - Select **New Device**, and enter the device serial No., verification code, and device name.

Note

Make sure the new device to be added has registered to Hik-Connect. After the device is added, the corresponding site where the device is on Hik-Partner Pro will also be added.

- Select **Hik-Parnter Pro Device List**, and select device(s) from the list.

Note

- For devices with the same name on Hik-Partner Pro, suffixes will be added to the names of the devices.
- If the selected device is deleted from the platform, it will not be deleted from the site on Hik-Partner Pro.

5. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
6. **Optional:** Switch on **Add Resource to Area** to import the resources (including cameras, alarm inputs, and alarm outputs) of the added security control device to an area.

   Note

   - You can select **Specified Alarm Input and Radar** and select the specified alarm inputs or radars to import to the area.
   - Platform will generate security control partitions in the area, based on the settings on the device.
   - You can create a new area by the device name or select an existing area.
   - Up to 64 alarm inputs can be imported in one area. If you don't import resources to area, you cannot perform further operations for the resources.
7. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list.
   - Click **Add and Continue** to save the settings and continue to add next security control device.
8. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set Time Zone	Select a device and click **Time Zone** to set its time zone.
Search Device(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.15.10 Add Security Control Device via Modbus Protocol

You can add security control devices to the platform via Modbus protocol, and the parameters you need to configure include IP address, device name, device port number, etc.

Before You Start

Make sure the security control 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 system via network.

Steps

1. In the top left corner of the Web Client, select → **All Modules** → **General** → **Resource Management** .
2. Click **Device and Server** → **Security Control Device** .
3. Click **Add** to enter the Add Security Control Device page.
4. Select **Modbus Protocol** as the Access Protocol.

   Note

   The alarm boxes can only be added to the platform via Modbus Protocol.
5. Enter the required information.

   Device Address

   Enter the IP address of the device.

   Device Port

   Enter the port number of the device.

   Device Name

   The name of the device, which can be used to describe the device function, location, etc.

   Manufacture

   Select the manufacture from the drop-down list.

Alarm Inputs

The number of alarm inputs of the device. The value range is from 1 to 65535.

Alarm Outputs

The number of alarm outputs of the device. The value range is from 1 to 65535.

Alarm Input

Set the default alarm input signal to low level or high level.

6. **Optional:** Switch on **Add Resource to Area** to import the resources of the added security control device to an area.

Note

- You can select **Specified Alarm Input and Radar** and select the specified alarm inputs or radars to import to the area.
- The platform will generate security control partitions in the area, based on the settings on the device.
- You can create a new area by the device name or select an existing area.
- Up to 64 alarm inputs can be imported to one area. If you don't import alarm inputs to an area, you cannot perform further operations for them.
- Up to 10 radars can be imported to one area. If you don't import radars to an area, you cannot perform further operations for them.

7. Finish adding the device.
   - Click **Add** to add the security control device and back to the security control device list.
   - Click **Add and Continue** to save the settings and continue to add the next security control device.
8. **Optional:** Perform the following operations after adding the devices.

Remote Configurations	Click to set the remote configurations of the corresponding device. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Set Time Zone	Select a device and click **Time Zone** to set its time zone.

Search for Device(s)	Enter a keyword in the search box in the upper right corner to quickly search for the target device(s).
Refresh Device List	Click **Refresh All** to refresh the device list.

9.16 Manage Fire Protection Device

You can add a fire protection device to the system by IP address and IP segment, and add fire protection devices in a batch. You can also manage the added devices, including editing and deleting the devices, configuring the devices remotely, changing online devices' password, etc.

9.16.1 Add Fire Protection Device by IP Address

When you know the IP address of a fire protection device, you can add it to the platform by specifying the IP address, user name, password, etc.

Before You Start
Make sure the devices to be added 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 HikCentral Professional via network.

Steps
1. In the top left corner of the platform, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Fire Protection Device** .
3. Click **Add** to enter the Add Fire Protection Device page.
4. Select **Hikvision Private Protocol** as the access protocol.
5. Select **IP Address** as the adding mode.
6. Enter the information as required (device address, device port, device name, user name, and password).

Note
The device port No. is 8000 by default.

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.

7. **Optional:** Select the time zone for device.

- **Get Device's Time Zone**: the current time zone will be applied according to the device location.
- **Manually Set Time Zone (The time zone settings will be applied to the device automatically)**: you can select a time zone from the drop-down list and click **View** to view the selected time zone details.

8. **Optional:** Switch on **Add Resource to Area** to import the resources of the added device to the area.

Note

You can create a new area by the device name or select an existing area from the area list. Also, you can click **Add** to add a new area. For details about adding a new area, refer to ***Add Area*** .

9. Finish adding the device.
   - Click **Add** to save the current device and return to the device list.
   - Click **Add and Continue** to save the current device and continue to add another device.
10. **Optional:** After adding the device, you can perform the following operations.

Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Edit Time Zone	Select one or multiple devices and click **Time Zone** to re-edit the time zone of selected device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.16.2 Add Fire Protection Device by IP Segment

When you know the IP segment of a fire protection device, you can add it to the platform by specifying the start and end IP address, device port, user name, password, etc.

Before You Start

Make sure the devices to be added 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 HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management → Device** .
2. Click **Device and Server → Fire Protection Device** .
3. Click **Add** to enter the Add Fire Protection Device page.
4. Select **Hikvision Private Protocol** as the access protocol.
5. Select **IP Segment** as the adding mode.
6. Enter the information as required (the start and end IP address, device port, device name, user name, and password).

Note

The device port No. is 8000 by default.

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.

7. **Optional:** Select the time zone for device.
   - **Get Device's Time Zone**: the current time zone will be applied according to the device location.
   - **Manually Set Time Zone (The time zone settings will be applied to the device automatically)**: you can select a time zone from the drop-down list and click **View** to view the selected time zone details.
8. **Optional:** Switch on **Add Resource to Area** to import the resources of the added device to the area.

Note

You can create a new area by the device name or select an existing area from the area list. Also, you can click **Add** to add a new area. For details about adding a new area, refer to ***Add Area*** .

9. Finish adding the device.
   - Click **Add** to save the current device and return to the device list.
   - Click **Add and Continue** to save the current device and continue to add another device.
10. **Optional:** After adding the device, you can perform the following operations.

Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Edit Time Zone	Select one or multiple devices and click **Time Zone** to re-edit the time zone of selected device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.16.3 Add Fire Protection Device by Device ID

When you know the device ID of a fire protection device, you can add it to the platform by specifying the device ID, device name, etc.

Before You Start

Make sure the devices to be added 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 HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Fire Protection Device** .
3. Click **Add** to enter the Add Fire Protection Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.
5. Select **Device ID** as the adding mode.
6. Enter the information as required.

   Device ID

   Required; 1 to 32 characters are allowed, excluding special characters such as /\:*?"<>|.

   ISUP Login Password

   Optional; 1 to 32 characters are allowed, excluding special characters such as /\:*?"<>|.

Device Name

Required; 1 to 64 characters are allowed, excluding special characters such as /\:*?"<>|.

7. **Optional:** Select the time zone for device.
   - **Get Device's Time Zone**: the current time zone will be applied according to the device location.
   - **Manually Set Time Zone (The time zone settings will be applied to the device automatically)**: you can select a time zone from the drop-down list and click **View** to view the selected time zone details.
8. **Optional:** Switch on **Add Resource to Area** to import the resources of the added device to the area.

Note

You can create a new area by the device name or select an existing area from the area list. Also, you can click **Add** to add a new area. For details about adding a new area, refer to ***Add Area*** .

9. Finish adding the device.
   - Click **Add** to save the current device and return to the device list.
   - Click **Add and Continue** to save the current device and continue to add another device.
10. **Optional:** After adding the device, you can perform the following operations.

Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Edit Time Zone	Select one or multiple devices and click **Time Zone** to re-edit the time zone of selected device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.16.4 Add Fire Protection Devices by ID Segment

When you know the device ID segment of a fire protection device, you can add it to the platform by specifying the start and end ID of device, ISUP login password, etc.

Before You Start

Make sure the devices to be added 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 HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Fire Protection Device** .
3. Click **Add** to enter the Add Fire Protection Device page.
4. Select **Hikvision ISUP Protocol** as the access protocol.
5. Select **Device ID Segment** as the adding mode.
6. Enter the information as required.

   Device ID

   Required; ranges from 0 to 999,999,999; the start ID should be smaller or equal to the end ID.

   ISUP Login Password

   Optional; 1 to 32 characters are allowed, excluding special characters such as /\:*?"<>|.
7. **Optional:** Select the time zone for device.
   - **Get Device's Time Zone**: the current time zone will be applied according to the device location.
   - **Manually Set Time Zone (The time zone settings will be applied to the device automatically)**: you can select a time zone from the drop-down list and click **View** to view the selected time zone details.
8. **Optional:** Switch on **Add Resource to Area** to import the resources of the added device to the area.

   Note

   You can create a new area by the device name or select an existing area from the area list. Also, you can click **Add** to add a new area. For details about adding a new area, refer to ***Add Area*** .
9. Finish adding the device.
   - Click **Add** to save the current device and return to the device list.
   - Click **Add and Continue** to save the current device and continue to add another device.
10. **Optional:** After adding the device, you can perform the following operations.

Remote Configurations	Click to configure the device remotely.

	Note For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s).
	Note • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Edit Time Zone	Select one or multiple devices and click **Time Zone** to re-edit the time zone of selected device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.16.5 Add Fire Protection Devices in a Batch

When there are multiple fire protection devices to be added, you can edit the predefined template containing the required device information, and import the template to HikCentral Professional to add devices in a batch.

Before You Start

Make sure the devices to be added 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 HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Fire Protection Device** .
3. Click **Add** to enter the Add Fire Protection Device page.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the file in CSV format to the local PC.
6. Open the downloaded template and enter the required information of the devices in the corresponding column.
7. Click and select the edited file.
8. **Optional:** Select the time zone for device.
   - **Get Device's Time Zone**: the current time zone will be applied according to the device location.

- **Manually Set Time Zone (The time zone settings will be applied to the device automatically)**: you can select a time zone from the drop-down list and click **View** to view the selected time zone details.

9. Finish adding the device.
   - Click **Add** to save the current device and return to the device list.
   - Click **Add and Continue** to save the current device and continue to add another device.
10. **Optional:** After adding the devices, you can perform the following operations.

Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Edit Time Zone	Select one or multiple devices and click **Time Zone** to re-edit the time zone of selected device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.17 Manage Dock Station

The dock station is a data collector which can automatically detect and back up law-enforcement data and evidence data from body camera(s) connected to it. The dock station can also be used to charge the body cameras.

After adding dock stations to the system, you can search the data (video footage, pictures, and audio files) backed up on the dock stations and download the data via the Control Client for convenient management. You can also monitor the online status of the dock stations, and perform other operations such as playing video footage backed up on the dock stations.

Note

- For more details about the dock station, see the user manual of the device.
- For details about searching video footage of the dock stations, see the *HikCentral Professional Control Client User Manual*.

9.17.1 Add Dock Station by IP Address

When you know the IP address or domain name of the dock station to be added, you can add the device to the platform by specifying the IP address, user name, password, and other related parameters.

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 HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Dock Station** on the left panel.
3. Click **Add** to enter the Add Dock Station page.
4. Select **IP Address** as the adding mode.
5. Enter the required information.

   Device Address

   IP address or domain name of the dock station.

   HTTP Port

   Enter the HTTP port of the device. By default, it is 80.

   Device Name

   Create a descriptive name for the device.

   Note

   Up to 64 characters are allowed for the device name.

   User Name

   User name of the dock station.

   Password

   Password of the account that you are logging in.
6. **Optional:** Set time zone for the dock station.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
7. **Optional:** Switch on **File Storage** to set the storage information of files uploaded by the dock station.

   Storage Location

The recording server, in which the videos and pictures will be stored according to the configured backup schedule. Two types of recording servers are supported: Hybrid Storage Area Network and pStor.

Note

You should configure the Hybrid Storage Area Network and pStor in advance, or its storage location cannot be displayed in the drop-down list.

Copyback Time

The backup schedule of files uploaded by the dock station.

8. Finish adding the dock station.
   - Click **Add** to add the current dock station and go back to the dock station list page.
   - Click **Add and Continue** to add the current dock station and add more other dock stations.
9. **Optional:** Perform the following operations.

Edit Dock Station	• Click the dock station name on the device list to edit the dock station. • Click **Copy To** to select the item (settings of time zone or storage information) to copy, and copy the selected settings of this dock station to other dock station(s).
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.
Set Time Zone	Select a dock station and then click **Time Zone** to set its time zone.
Search Dock Station(s)	Enter keywords in the search box on the upper right corner of the page to quickly search the target device(s).

9.17.2 Add Dock Stations by IP Segment

When multiple dock stations 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.

Before You Start

Make sure the dock stations 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 HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Dock Station** on the left panel.
3. Click **Add** to enter the Add Dock Station page.
4. Select **IP Segment** as the adding mode.
5. Enter the required information.

   Device Address

Enter the start IP address and the end IP address. For example, if five dock stations need to be added, and their IP address are "10.41.7.231", "10.41.7.232", "10.41.7.233", "10.41.7.234", and "10.41.7.235" respectively, you should enter ***10.41.7.231*** and ***10.41.7.235***.

HTTP Port

Enter the HTTP port number of the device. By default, it is 5651.

User Name

User name of the dock station.

Password

Password of the account that you are logging in.

6. **Optional:** Set time zone for the dock station.
   - Click **Manually Set Time Zone**, and click ⌄ to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
7. Finish adding the dock stations.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and continue to add more dock stations.
8. **Optional:** Perform the following operations.

Edit Dock Station	• Click the dock station name on the device list to edit the dock station. • Click **Copy To** to select the item (settings of time zone or storage information) to copy, and copy the selected settings of this dock station to other dock station(s).
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.
Set Time Zone	Select a dock station and then click **Time Zone** to set its time zone.
Search Dock Station(s)	Enter keywords in the search box on the upper right corner of the page to quickly search the target device(s).

9.17.3 Add Dock Stations by Port Segment

When multiple dock stations 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 some other related parameters.

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 HikCentral Professional via network.

Steps

1. In the top left corner of the platform, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Dock Station** on the left.
3. Click **Add** to enter the Add Dock Station page.
4. Select **Port Segment** as the adding mode.
5. Enter the required information.

   Device Address

   The same IP address where the devices are located.

   HTTP Port

   Enter the start port number and the end port number. For example, if there are five dock stations to be added, and their port number are 80, 81, 82, 83, and 84 respectively, you should enter ***80*** and ***84***.

   User Name

   The same user name of the dock stations.

   Password

   Password of the account that you are logging in.
6. **Optional:** Set time zone for the dock station.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
7. Finish adding the device.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and add more dock stations by port segment.
8. **Optional:** Perform the following operations.

Edit Dock Station	• Click the dock station name on the device list to edit the dock station. • Click **Copy To** to select the item (settings of time zone or storage information) to be copied, and copy the selected settings of this dock station to other dock station(s).
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.
Set Time Zone	Select a dock station and then click **Time Zone** to set its time zone.
Search Dock Station(s)	Enter keywords in the search box on the upper right corner of the page to quickly search the target device(s).

9.17.4 Batch Add Dock Stations

When there are multiple dock stations to be added to HikCentral Professional, you can download a predefined template and fill in the required information of the dock stations, and then import the template to the platform to add multiple dock stations at a time.

Before You Start
Make sure the dock stations you are going to use are correctly installed and connected to the network as specified by the manufacturer. Such initial configuration is required in order to be able to connect the device to the HikCentral Professional via network.

Steps
1. In the top left corner of the platform, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Dock Station** on the left panel.
3. Click **Add** to open the Add Dock Station page.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template (CSV file) on your PC.
6. Open the template file and enter the required information of the devices to be added in the corresponding column.
7. Click and select the template file.
8. **Optional:** Set time zone for the dock stations.
   - Click **Manually Set Time Zone**, and click to select a time zone from the drop-down list.

     Note
     You can click **View** to view the details of the current time zone.
   - Click **Get Device's Time Zone** to get the device's time zone.
9. Finish adding the dock stations.
   - Click **Add** to add the dock stations and back to the dock station list page.
   - Click **Add and Continue** to save the settings and continue to add more dock stations.
10. **Optional:** Perform the following operation(s).

Edit Dock Station	• Click the dock station name on the device list to edit the dock station. • Click **Copy To** to select the item (settings of time zone or storage information) to be copied, and copy the selected settings of this dock station to other dock station(s).
Delete Dock Station	Select dock station(s) and then click **Delete** to delete them.
Set Time Zone	Select a dock station and then click **Time Zone** to set its time zone.
Search Dock Station(s)	Enter keywords in the search box on the upper right corner of the page to quickly search the target device(s).

9.17.5 Add Dock Station Group

Dock station group is a group of persons who are linked to the same dock station(s). After linking persons to dock station(s), the videos and pictures on the persons' body cameras can be copied to these dock station(s).

Steps

Note

Up to 64 dock station groups can be added.

1. In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Dock Station** .
2. Click **Add Dock Station Group** to open Add Dock Station Group panel.

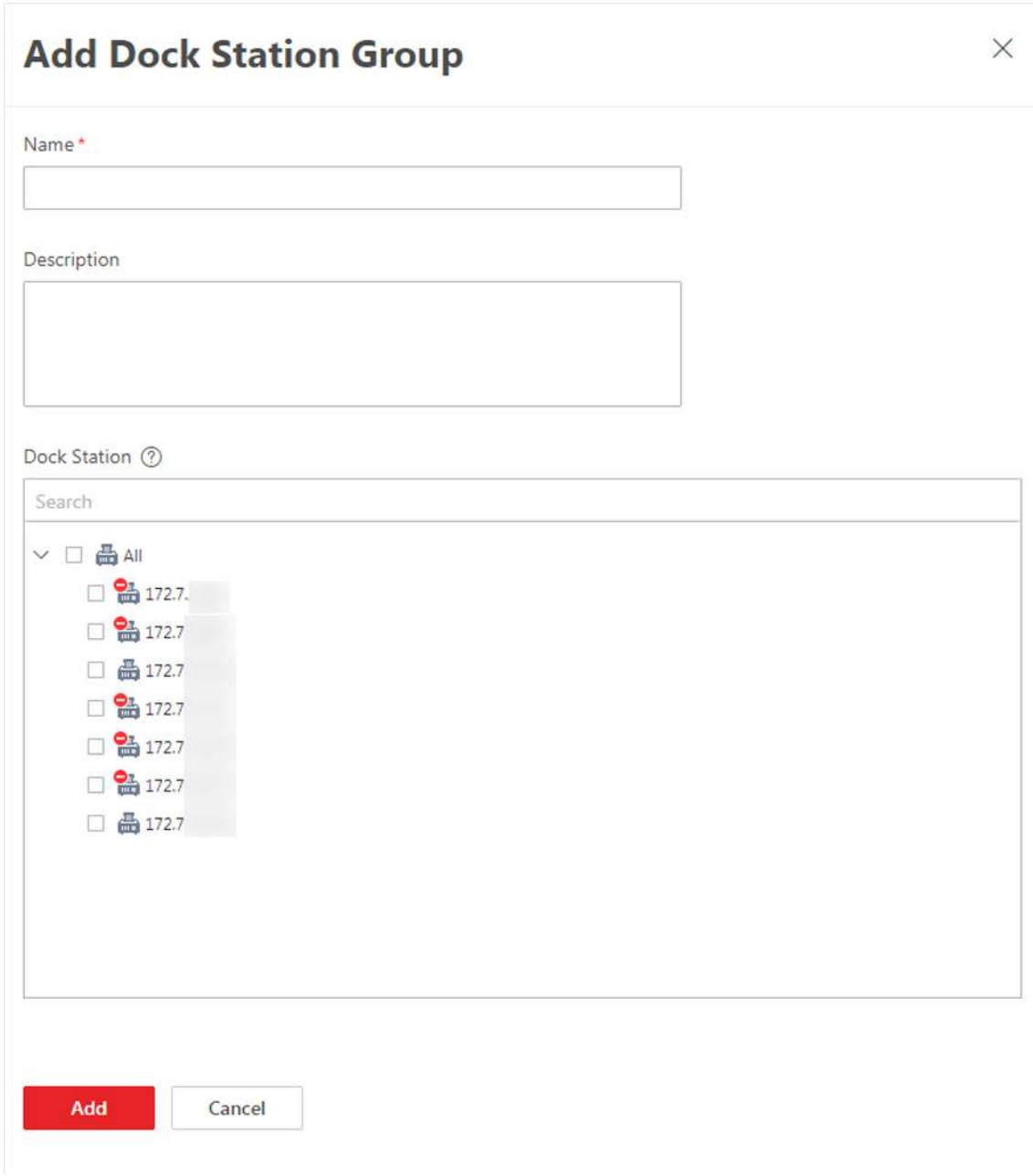


Figure 9-16 Add Dock Station Group

3. Enter the basic information.

Name

Create a name for the dock station group.

Description

Enter the descriptive information for the group. E.g., This dock station group is for security guards in Team A.

Dock Station

Select dock station(s).

4. Click **Add**.

The dock station group will be displayed in the dock station group list.

5. Add person(s) to the dock station group.

Note

Up to 200 persons can be added to one dock station group.

1) Click **Add** to open the Add Person/Person Group window.
2) Select a person group from the person group list in the window.
3) Select specific person(s) in the group.
4) Click **Add**.

The person(s) will be displayed in the person list.

Note

If applying person(s) failed, the **Applying Failed** tag will be displayed on the person profile card. You can click the person profile card to view the failure details.

6. **Optional:** Perform following operations for added dock station groups.

Edit Dock Station Group	Select a dock station group in the dock station group list and click to edit it.
Delete Dock Station Group	Select a dock station group in the dock station group list and click .
Set Person as Super User	Select a person in a dock station group and click **Set As Super User** to set the person as the super user of the dock station. **Note** Only one super user is allowed for a dock station group.
Cancel Super User	Select the super user and click **Cancel Super User**.
Check Person Applying Failure Details	Hover the cursor onto the and click **Details** to view the person applying failure details.
Re-Apply Person(s)	Hover the cursor onto the and click **Retry** to re-apply the person(s) to the dock station(s).
Delete Person(s)	Select person(s) from the person list, and then click **Delete** to delete the selected person(s). Or hover the cursor onto next to **Delete**, and then click **Delete All** to delete all persons in the group.

Only Display Person(s) Failed to Be Applied	Check **Only Display Persons Failed to Be Applied** to filter the persons whose information is failed to be applied.
Apply All Person(s)	Click **Apply All** to apply the person(s) in the person list to the dock station(s) linked to the group.

9.18 Manage Digital Signage Terminals

On the Resource Management module, you can add digital signage terminals to the platform and perform further management and operation. There are two physical forms for the digital signage terminal. One is a terminal with screen, such as vertical digital signage and wall-mounted digital signage; the other (called digital signage player) is a station which integrate the function of information release, and it can connect with LED screen, LCD screen or jointed screen as the displaying screen.

9.18.1 Add Digital Signage Terminal

You can add digital signage terminals to the platform by multiple methods: adding online terminals, adding by IP address, adding by device serial No., and adding by authentication code. After adding terminals to the platform, you can configure, manage and control the terminals.

Add Online Terminals

The platform can detect the online terminals (referred to as device in the following pages) on the same LAN as the server, and detect the device IP addresses. Based on this function, you can add the devices to the platform quickly. When the detected devices use the same user name and password, you can add the devices to the platform simultaneously.

Before You Start

- Make sure you have downloaded and installed the Web Control on the login page.
- Make sure you are in the Digital Signage mode. See details in ***Switch Application Mode*** .

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the top, select **Device**.
3. On the left navigation pane, click **Device and Server** → **Digital Signage Terminal** .
4. In the Online Device area, select **Hikvision Private Protocol** / **Hikvision ISUP Protocol** to filter the detected online devices.

Note

To display the devices which are added to the platform via ISUP protocol, you can go to → **Basic Management → System → Network → Device Access Protocol** and enable **Allow ISUP Registration**.

5. In the online device list, select one or multiple devices to be added, and then click **Add to Device List** to enter the Add Device page.
6. Set the basic information.

Note

Parameters vary according to the protocol, via which the device is added.

Device Serial No.

Enter the device serial No.

Authentication Code

Enter the authentication code of the device.

Note

The authentication code should contain 8 to 16 characters, including at least two of the following categories: upper case letters, lower case letters, and numbers.

Device Address

The IP address of the device, which can be obtained automatically.

Note

If you add multiple devices simultaneously, this parameter will not be displayed.

Device Port

The port number of the device, which can be obtained automatically.

Note

If you add multiple devices simultaneously, this parameter will not be displayed.

Device Name

The name of the device, which can be used to describe the device function, location, etc.

Note

If you add multiple devices simultaneously, this parameter will not be displayed.

User Name

The admin account (which is created when activating the device) or the non-admin account, such as the operator. If you use a non-admin account to add devices, the permissions might be limited.

Password

The password of the account.

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.

7. **Optional:** Enable **Picture Storage** to configure the storage location.

Local Storage

The pictures are stored in the SYS server.

Note

You can click **Configure** to configure the storage location for pictures and files respectively. For details, refer to ***Configure Storage for Imported Pictures and Files*** .

pStor

The pictures are stored in the pStor server.

Note

In the attendance application scene, you should enable **Picture Storage**.

8. **Optional:** Set the time zone of the device.
   - Select **Get Device's Time Zone** to get the time zone of the device.
   - Select **Manually Set Time Zone** to manually set the time zone of the device, and the time zone settings will be applied to the device automatically.
9. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

Note

You can create a new area by the device name or select an existing area. Also, you can click **Add** to add new area(s). For details, refer to ***Add an Area for Current Site*** .

10. Click **Add**.
11. **Optional:** Perform the following operations after adding devices.

Change Password	Select one or more devices, and click **Change Password** to change the password of the selected devices.

	Note If multiple devices have the same password, you can change the password for multiple devices simultaneously.
Delete Devices	Select one or more devices, and click **Delete** to delete the selected devices.
	Note If the device which has been linked to the video wall is deleted, the corresponding video wall program cannot be released.
Search Device(s)	Enter a keyword in the search box in the upper right corner of the page to quickly search the target device(s).
Configure Device Display Settings	Select one or more devices and click **Display Settings** to enter the Display Settings page. See ***Configure Device Display Settings*** for details.
Configure Device Privacy Settings	Select one or more devices, and then click **Privacy Settings** to enter the Privacy Settings page. See ***Configure Device Privacy Settings*** .
Set Time Zone	Select one or more devices, and click **Time Zone** to configure the time zone of the selected devices. You can select **Get Device's Time Zone** or **Manually Set Time Zone** according to your requirements.

Add Terminal by IP Address

If you know the IP address of the terminal (referred to as device in the following pages) to be added, you can add the device to the platform by specifying the IP address, user name, password, etc.

Before You Start
Make sure you are in the Digital Signage mode. See details in ***Switch Application Mode*** .

Steps
1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the top, select **Device**.
3. On the left navigation pane, click **Device and Server** → **Digital Signage Terminal** .
4. Click **Add** to enter the Add Device page.
5. Select the Access Protocol as **Hikvision Private Protocol**.

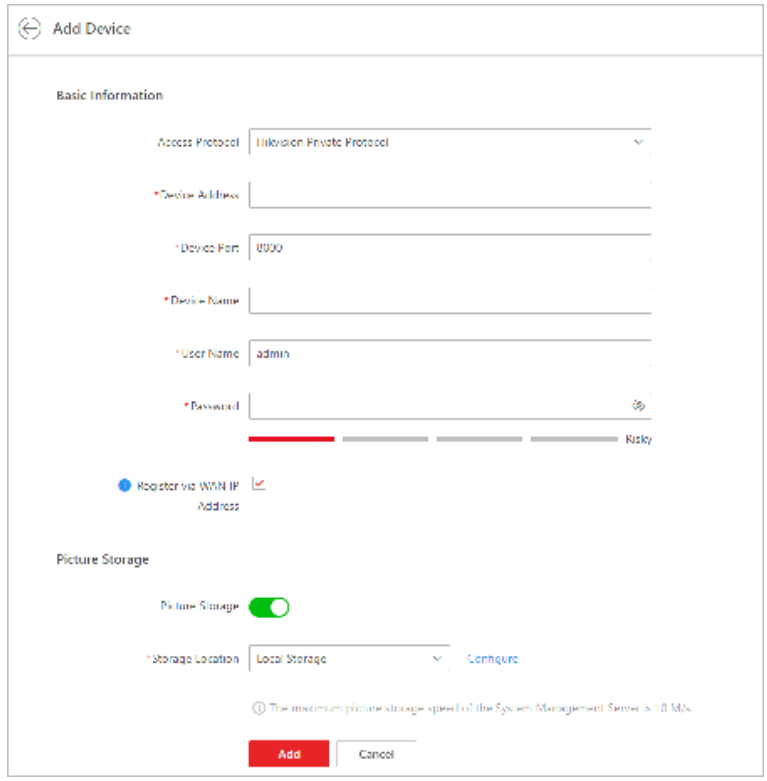


Figure 9-17 Add Terminal by IP Address

6. Set the basic information.

Device Address

Enter the IP address of the device.

Device Port

Enter the port number of the device.

Device Name

The name of the device, which can be used to describe the device function, location, etc.

User Name

The admin account (which is created when activating the device) or the non-admin account, such as the operator. If you use a non-admin account to add devices, the permissions might be limited.

Password

The password of the account.

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.

Register via WAN IP Address

The function is available when the device and the platform are not on the same LAN.

7. **Optional:** Enable **Picture Storage** to configure the storage location.

Local Storage

The pictures are stored in the SYS server.

Note

You can click **Configure** to configure the storage location for pictures and files respectively. For details, refer to ***Configure Storage for Imported Pictures and Files*** .

pStor

The pictures are stored in the pStor server.

Note

In the attendance application scene, you should enable **Picture Storage**.

8. **Optional:** Set the time zone of the device.
   - Select **Get Device's Time Zone** to get the time zone of the device.
   - Select **Manually Set Time Zone** to manually set the time zone of the device and the time zone settings will be applied to the device automatically.
9. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

Note

You can create a new area by the device name or select an existing area. Also, you can click **Add** to add new area(s). For details, refer to ***Add an Area for Current Site*** .

10. Click **Add**.
11. **Optional:** Perform the following operations after adding devices.

Change Password	Select one or more devices, and click **Change Password** to change the password of the selected devices.

	Note If multiple devices have the same password, you can change the password for multiple devices simultaneously.
Delete Devices	Select one or more devices, and click **Delete** to delete the selected devices.
	Note If the device which has been linked to the video wall is deleted, the corresponding video wall program cannot be released.
Search Device(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search the target device(s).
Configure Device Display Settings	Select one or more devices and click **Display Settings** to enter the Display Settings page. See ***Configure Device Display Settings*** for details.
Configure Device Privacy Settings	Select one or more devices, and then click **Privacy Settings** to enter the Privacy Settings page. See ***Configure Device Privacy Settings*** .
Set Time Zone	Select one or more devices, and click **Time Zone** to configure the time zone of the selected devices. You can select **Get Device's Time Zone** or **Manually Set Time Zone** according to your requirements.

Add Terminal by Device Serial No.

For the terminal (referred to as device in the following pages) supports ISUP protocol, you can add it to the platform by entering the device serial No., the authentication code, etc.

Before You Start

- Make sure you have activated the device. For details, refer to ***Create Password for Inactive Device(s)*** .
- Make sure you have configured the IP address for receiving device information on the platform, and select the current NIC as the address for receiving device information. Refer to ***Set IP Address for Receiving Device Information*** for details.
- Make sure you are in the Digital Signage mode. See details in ***Switch Application Mode*** .

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the top, select **Device**.

3. On the left navigation pane, click **Device and Server → Digital Signage Terminal** .
4. Click **Add** to enter the Add Device page.

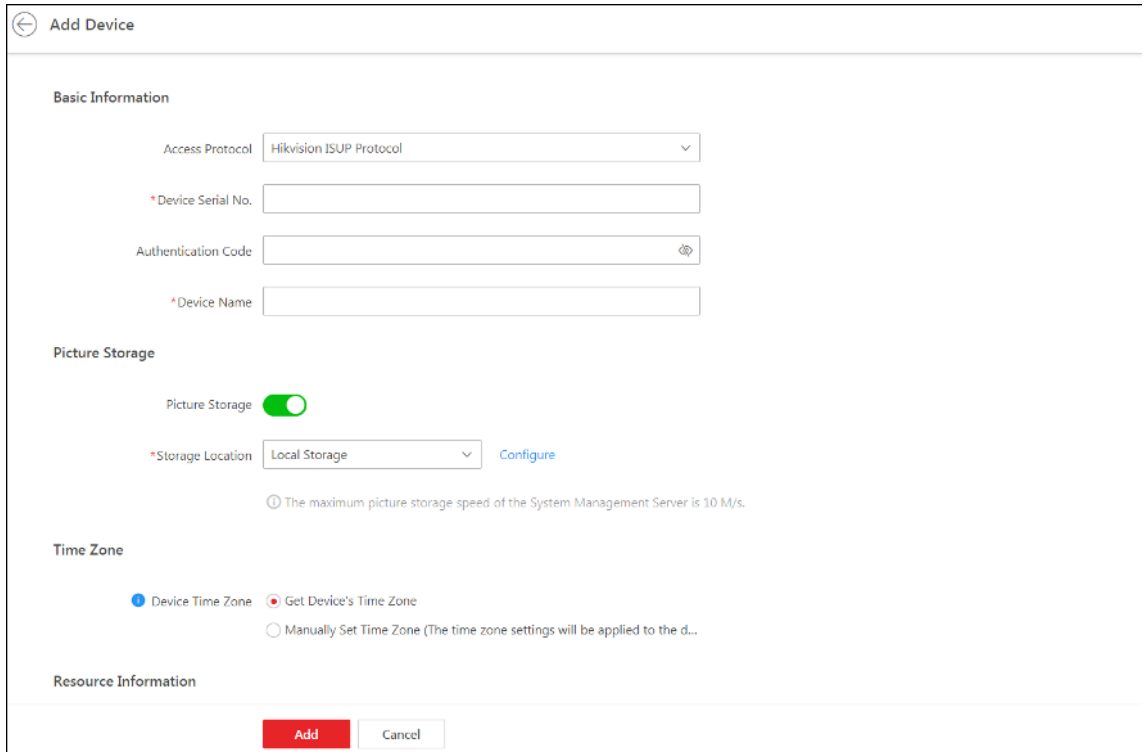


Figure 9-18 Add Terminal by Device Serial No.

5. Select **Hikvision ISUP Protocol** as the access protocol.
6. Set the basic information.

   Device Serial No.

   Enter the device serial No.

   Authentication Code

   Enter the authentication code of the device.

   Note

   The authentication code should contain 8 to 16 characters, including at least two of the following categories: upper case letters, lower case letters, and numbers.

   Device Name

   Name for the device, which can be used to describe the device function and location.
7. **Optional:** Enable **Picture Storage** to configure the storage location.

   Local Storage

   The pictures are stored in the SYS server.

Note

You can click **Configure** to configure the storage location for pictures and files respectively. For details, refer to ***Configure Storage for Imported Pictures and Files*** .

pStor

The pictures are stored in the pStor server.

Note

In the attendance application scene, you should enable **Picture Storage**.

8. **Optional:** Set the time zone of the device.
   - Select **Get Device's Time Zone** to get the time zone of the device.
   - Select **Manually Set Time Zone** to manually set the time zone of the device and the settings will be applied to the device automatically.
9. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

Note

You can create a new area by the device name or select an existing area. Also, you can click **Add** to add new area(s). For details, refer to ***Add an Area for Current Site*** .

10. Click **Add**.
11. **Optional:** Perform the following operations.

Change Password	Select one or more devices, and click **Change Password** to change the password of the selected devices. **Note** If multiple devices have the same password, you can change the password for multiple devices simultaneously.
Delete Device	Select one or more devices, and click **Delete** to delete the selected devices. **Note** If the device which has been linked to the video wall is deleted, the corresponding video wall program cannot be released.
Search Device(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search the target device(s).
Configure Device Display Settings	Select one or more devices and click **Display Settings** to enter the Display Settings page. See ***Configure Device Display Settings*** for details.

Configure Device Privacy Settings	Select one or more devices, and then click **Privacy Settings** to enter the Privacy Settings page. See ***Configure Device Privacy Settings*** .
Set Time Zone	Select one or more devices, and click **Time Zone** to configure the time zones of the selected devices. You can select **Get Device's Time Zone** or **Manually Set Time Zone** according to your requirements.

What to do next

Enter the IP address of the platform, registration port No. (7600 by default), and the authentication code on the device's registration interface. Then the device will be added to the platform automatically.

Enable General Authentication Code

For the terminal which supports ISUP, you can set general authentication code on the platform. The authentication code is used for the terminal to register on the platform by ISUP. After enabling general authentication code on the platform, you should enter the authentication code on the terminal, which can then be added to the platform automatically.

Before You Start

Make sure you are in the Digital Signage mode. See details in ***Switch Application Mode*** .

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the top, select **Device**.
3. On the left navigation pane, click **Device and Server** → **Digital Signage** .
4. Click **General Authentication Code Settings**.
5. Switch on **General Authentication Code Settings**.

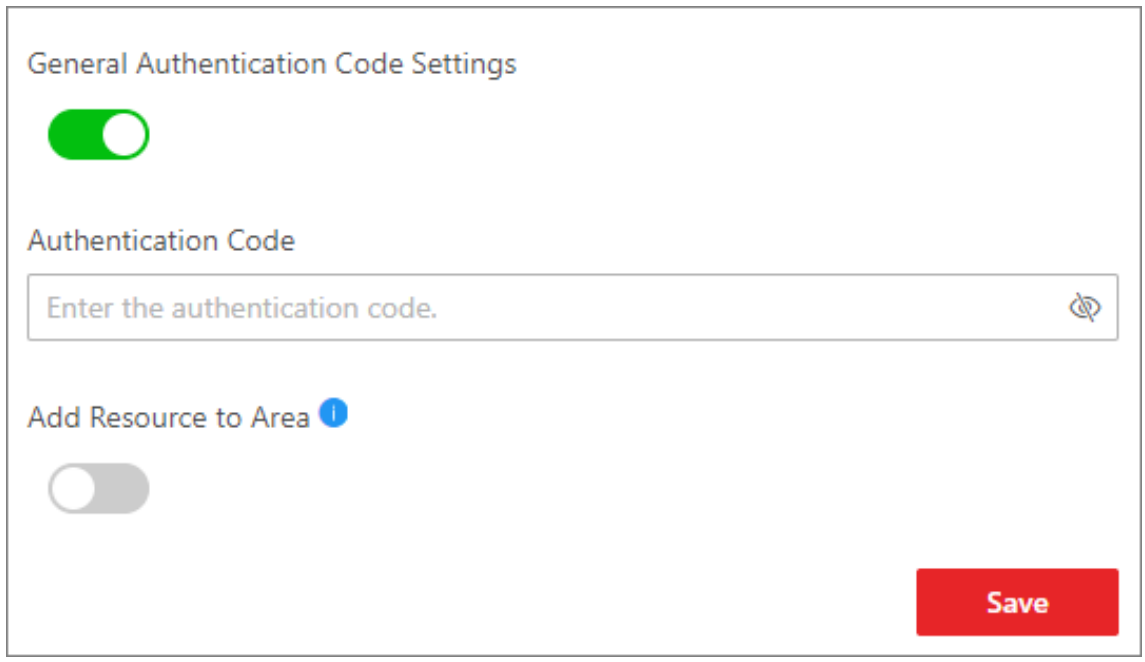


Figure 9-19 Set General Authentication Code

6. Enter the authentication code.

Note

The authentication code should contain 8 to 16 characters, including at least two of the following categories: upper case letters, lower case letters, and numbers.

7. **Optional:** Import the resources of the device to the area.
   1) Switch on **Add Resource to Area**.
   2) Select **Create Area by Device Name** or **Existing Area**.

   Create Area by Device Name

   Create a new area by the device name.

   Existing Area

   Select an existing area from the area list.

   Note

   You can create a new area by the device name or select an existing area. Also, you can click **Add** to add new area(s). For details, refer to ***Add an Area for Current Site*** .
8. Click **Save**.
9. **Optional:** Perform the following operations.

Change Password	Select one or more devices, and click **Change Password** to change the password for the selected devices.

	Note If multiple devices have the same password, you can change the password for them simultaneously.
Delete Device	Select one or more devices, and click **Delete** to delete the selected devices.
	Note If the device which has been linked to the video wall is deleted, the corresponding video wall program cannot be released.
Search Device(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search the target device(s).
Configure Device Display Settings	Select one or more devices and click **Display Settings** to enter the Display Settings page. See ***Configure Device Display Settings*** for details.
Configure Device Privacy Settings	Select one or more devices, and then click **Privacy Settings** to enter the Privacy Settings page. See ***Configure Device Privacy Settings*** .
Set Time Zone	Select one or more devices, and click **Time Zone** to configure the time zones of the selected devices. You can select **Get Device's Time Zone** or **Manually Set Time Zone** according to your requirements.

What to do next
After setting the general authentication code on the platform, you should enter the IP address of the platform, registration port number (7600 by default), and the authentication code on the terminal's registration interface. Then the terminal will be added to the platform automatically.

9.18.2 Configure Device Display Settings

After adding terminal (called device in the following pages) to the platform, you can configure the display parameters of the device remotely, including the brightness, boot logo, etc.

Before You Start
Make sure you have added terminal(s) to the platform, and the terminal(s) are online. Refer to ***Add Digital Signage Terminal*** for details.

Steps
1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the left navigation pane, click **Device and Server** → **Digital Signage Terminal** .

3. Select one or multiple device(s), and then click **Display Settings** to enter the Display Settings page.
4. Set the related parameters.

Brightness Settings

Drag the brightness bar to adjust the brightness of the screen, or manually enter the brightness value. The brightness value is 0 to100. The bigger the value, the lighter the screen.

Boot Logo

After enabled, the logo will be displayed when the terminal starts up. The logo is set on the terminal locally.

SADP

After enabled, the terminal(s) can be detected by the platform via SADP protocol, and be displayed on the online device list.

Note

- You can enable SADP protocol for either single or multiple terminal(s).
- This function should be supported by the device.

Screen Direction

0

The screen direction is 0° by default.

90

The screen direction will rotate 90° clockwise.

180

The screen direction will rotate 180° clockwise.

270

The screen direction will rotate 270° clockwise.

Enter the Password to Unlock Screen

After the screen is locked, the password is required to unlock the screen. The password is set on the terminal locally.

5. Set the timed related parameters.

Timed Startup / Shutdown

After enabled, you should select the schedule as **Daily Schedule** or **Weekly Schedule**, and then the terminal will start up or shut down according to the schedule.

a. Drag the mouse on the time bar to draw the start up time duration (blue bar) of one day. The terminal will be shut down on the other time period.

Note

- Supports drawing up to 8 time periods of one day.
- You can click the time period (blue bar), enter the start time and end time of the time period.

b. You can click **Clear** to clear the wrong time period you draw on the time bar.

Timed Volume

After enabled, you should select the schedule as **Daily Schedule** or **Weekly Schedule**, and then the terminal's volume will turned on/off according to the schedule.

a. Drag the mouse on the time bar to draw the start up time duration (blue bar) of one day. The terminal will be shut down on the other time period.

Note

- Supports drawing up to 8 time periods of one day.
- You can click the time period (blue bar), enter the start time and end time of the time period.

b. You can click **Clear** to clear the wrong time period(s) you draw on the time bar.

6. **Optional:** Click **Restore** to restore the displaying parameters to the default parameters.
7. Click **Save** to save the configuration.

9.18.3 Configure Device Privacy Settings

You can configure the privacy parameters for the device remotely, including event storage mode, authentication result display, picture uploading and storage, and clearing pictures on device, to protect the person's private information.

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page, and then click **Device and Server** → **Digital Signage Terminal** on the left navigation pane.
2. Select one or multiple device(s), and then click **Privacy Settings** to enter the Privacy Settings page. You can set the following parameters.

Event Storage

Select the mode of event storage.

Overwrite

The events stored on the device will be overwritten automatically. For example, if a device can store up to 200 events. When this limit is reached, the first event will be overwritten by the newest one, and then the second will be overwritten.

Delete Old Events Regularly

Set a time period. The events stored on the device during the period will be automatically deleted at intervals of the period.

Delete Old Events by Specified Time

Set a specific time. The events stored on the device before the specific time will be automatically deleted.

Authentication

Check the items (such as profile photo, name, and employee ID) to be displayed in authentication results.

Note

The checked items will be displayed in the released attendance program. Refer to ***Create Attendance Program*** for details on creating and releasing attendance programs.

Picture Uploading and Storage

Check to enable the features as needed.

Upload Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be uploaded to the system.

Save Recognized or Captured Pictures

If it is checked, the recognized or captured pictures will be saved to the devices.

Clear Pictures Stored on Device

Clear Face Pictures

Click **Clear** to clear all face pictures.

Clear Recognized or Captured Pictures

Click **Clear** to clear all recognized pictures or captured pictures.

3. Click **Save** to save the configuration.

9.18.4 Configure Device Parameters Remotely

After adding terminal (called device in the following pages) to the system, you can configure the parameters of the device remotely, including configuring built-in camera's parameters, linking external camera, configuring displaying settings and other parameters.

Configure Built-In Camera Parameters

Built-in camera is the camera built in the terminal. After adding a terminal to the platform, you should configure parameters for the built-in camera, such as device name, function, and face similarity.

Before You Start

Make sure at least one terminal is added to the platform, and make sure the terminal is online.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the left navigation pane, click **Device and Server** → **Digital Signage Terminal** .
3. Click on the Operation column to enter the device remote configuration page of terminal.
4. In the **Linked Device** area, click **Built-In Camera** to enter the camera parameters settings page.
5. Set the parameters.

Device Name

The device name of the built-in camera.

Function

In the drop-down list, select **Attendance**,**Live View** or **Temperature Screening**.

Attendance

The attendance function will be enabled, and the attendance data will be displayed in the attendance programs.

Live View

The live view of the camera will be displayed in the live view window of the normal programs.

Temperature Screening

Enable the temperature screening function of the camera. The real-time temperature screening is displayed on the temperature screening program.

Similarity

Set the face similarity. When the captured face picture's similarity reaches the value, it will be regarded as comparison succeeded.

Recognition Distance

It is used to control the recognition distance between the person and camera.

Wearing Mask

Select **Yes** or **No** from the drop-down list.

Yes: The camera will recognize persons wearing masks.

No: The camera will not recognize persons wearing masks.

Temperature Measurement

Check **Temperature Measurement**, then when the camera detects abnormal temperature, the corresponding prompt will be displayed on the terminal.

Mask Detection

Check **Mask Detection**, then when the camera detects people without masks, the corresponding prompt will be displayed on the terminal.

Face Detection Frame

Check **Face Detection Frame**, then when the camera detects a face, a frame will be displayed on the terminal.

Quick Capture

Check **Quick Capture**, then the camera can recognize and capture a face more frequently even if the face is far away.

6. Click **Save** to save the above settings.

Link External Device to Terminal

After adding terminals to the platform, you can link external devices such as cameras to the terminals for attendance, live view, or temperature screening.

Before You Start

- Make sure the external device has been installed properly.
- Make sure at least one online terminal is added to the platform.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the left navigation pane, click **Device and Server** → **Digital Signage Terminal** .
3. Click in the Operation column of the online device to enter the remote configuration page of the terminal.
4. In the **Linked Device** area, click **Add** to enter the Add Device page.

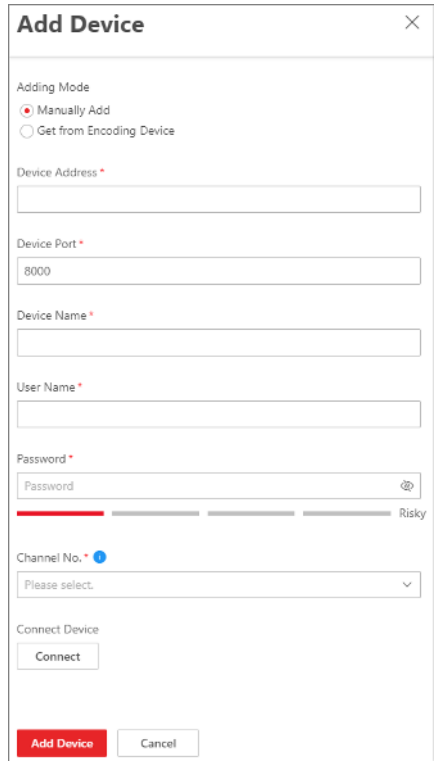


Figure 9-20 Add Device

5. Select the adding mode as **Manually Add** or **Get From Encoding Device**.
6. **Optional:** Set the following parameters when setting the adding mode as **Manually Add**.

   Device Address

   The IP address of the device.

   Device Port

   The port number of the device. By default, it is 8000.

   Device Name

   The name of the device, which can be used to describe the function, location, etc., of the device.

   User Name

   The user name of logging into the device.

   Password

   The password of the device.
7. **Optional:** Select an encoding device from the list when setting the adding mode as **Get From Encoding Device**.
8. Select the channel number of the device to be added to the terminal from the drop-down list.
9. **Optional:** Click **Connect** to connect to the device.

Note

- If you set the adding mode as **Get From Encoding Device**, the device should be online.
- After connecting to the device, you can configure the function for the selected channel. For details, refer to ***Configure Built-In Camera Parameters*** .

10. Click **Add Device**.

Configure Mode Parameters

On the remote configuration page of terminal, you can configure other parameters except for built-in camera and external camera, such as basic information, time settings, device operations, timed configuration and maintenance.

Basic Information

Device Address

Display the IP address of the terminal by default.

Subnet Mask

Display the subnet mask of the terminal by default.

Gateway

Display the gateway of the terminal by default.

Time Settings

Click to customize the time settings.
You can also select **Sync with Server Time** to synchronize time from the server.

Device Operation, Timed Settings and Maintenance

The display settings of the terminal, refer to ***Configure Device Display Settings*** for details.

9.18.5 Upgrade Old Device Firmware

For the terminal whose firmware version is old, the platform can automatically detect this terminal need to be upgraded, and you can manually upgrade the terminal's firmware.

On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page, and then click **Device and Server** → **Digital Signage Terminal** on the left navigation pane.

beside the terminal name indicates this terminal's firmware is old and firmware upgrade is required. Click to enter the Upgrade Device page.

Select the terminal(s) to be upgraded, click **Local File** to select the firmware package, and then click **Upgrade** to start upgrading.

9.19 Manage Interactive Flat Panel

You can add interactive flat panels to the platform by multiple methods: adding online interactive flat panels, adding by device serial No., and adding by general authentication code. After adding interactive flat panels to the platform, you can configure, manage and control them as needed.

Note

You can add interactive flat panels only in the Interactive Flat Panel mode. For where and how to switch the mode, refer to ***Switch Application Mode*** .

9.19.1 Add Online Interactive Flat Panel

If you have registered the interactive flat panel (referred to as device in the following pages) online on the Integrated Control App, the device can be displayed in the online device list on the platform. You can then add the device to the platform. If the online devices use the same authentication code, you can add them to the platform simultaneously.

Before You Start

- Make sure you have downloaded and installed the Web Control on the login page.
- Make sure you have switched to the Interactive Flat Panel mode. See details in ***Switch Application Mode*** .

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the top, select **Device**.
3. On the left navigation pane, click **Device and Server** → **Interactive Flat Panel** .
4. In the online device list, select one or multiple devices to be added, and then click **Add to Device List** to enter the Add Interactive Flat Panel page.
5. Set the basic information.

   Note

   - If you add one device, the device serial number will be displayed automatically. You should configure the authentication code and the device name.
   - If you add multiple devices, the device serial number and the device name will be displayed automatically. You should configure the authentication code.

   Authentication Code

   Enter the authentication code of the device.

Note

The authentication code should contain 8 to 16 characters, including at least two of the following categories: upper case letters, lower case letters, and digits.

Device Name

Name for the device, which can be used to describe the device function and location.

6. **Optional:** Set the time zone of the device.
   - Select **Get Device's Time Zone** to get the time zone of the device.
   - Select **Manually Set Time Zone** to manually set the time zone of the device and the settings will be applied to the device automatically.
7. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

Note

You can create a new area by the device name or select an existing area. Also, you can click **Add** to add new area(s). For details, refer to ***Add an Area for Current Site*** .

8. Click **Add**.
9. **Optional:** Perform the following operations.

Delete Device	Select one or more devices, and click **Delete** to delete the selected devices.
Set Time Zone	Select one or more devices, and click **Time Zone** to configure the time zone of the selected devices. You can select **Get Device's Time Zone** or **Manually Set Time Zone** as needed.
Search Device	Enter keywords in the upper right corner to search the target device(s).
Edit Device	Click a device to edit its basic information and time zone settings if needed.

9.19.2 Add Interactive Flat Panel by Device Serial No.

You can add the interactive flat panel (referred to as device in the following pages) to the platform by entering the device serial number, the authentication code, etc.

Before You Start

- Make sure you have activated the device. For details, refer to ***Create Password for Inactive Device(s)*** .
- Make sure you have configured the IP address for receiving device information on the platform, and select the current NIC as the address for receiving device information. Refer to ***Set IP Address for Receiving Device Information*** for details.
- Make sure you have switched to the Interactive Flat Panel mode. See details in ***Switch Application Mode*** .

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the top, select **Device**.
3. On the left navigation pane, click **Device and Server** → **Interactive Flat Panel** .
4. Click **Add** to enter the Add Interactive Flat Panel page.

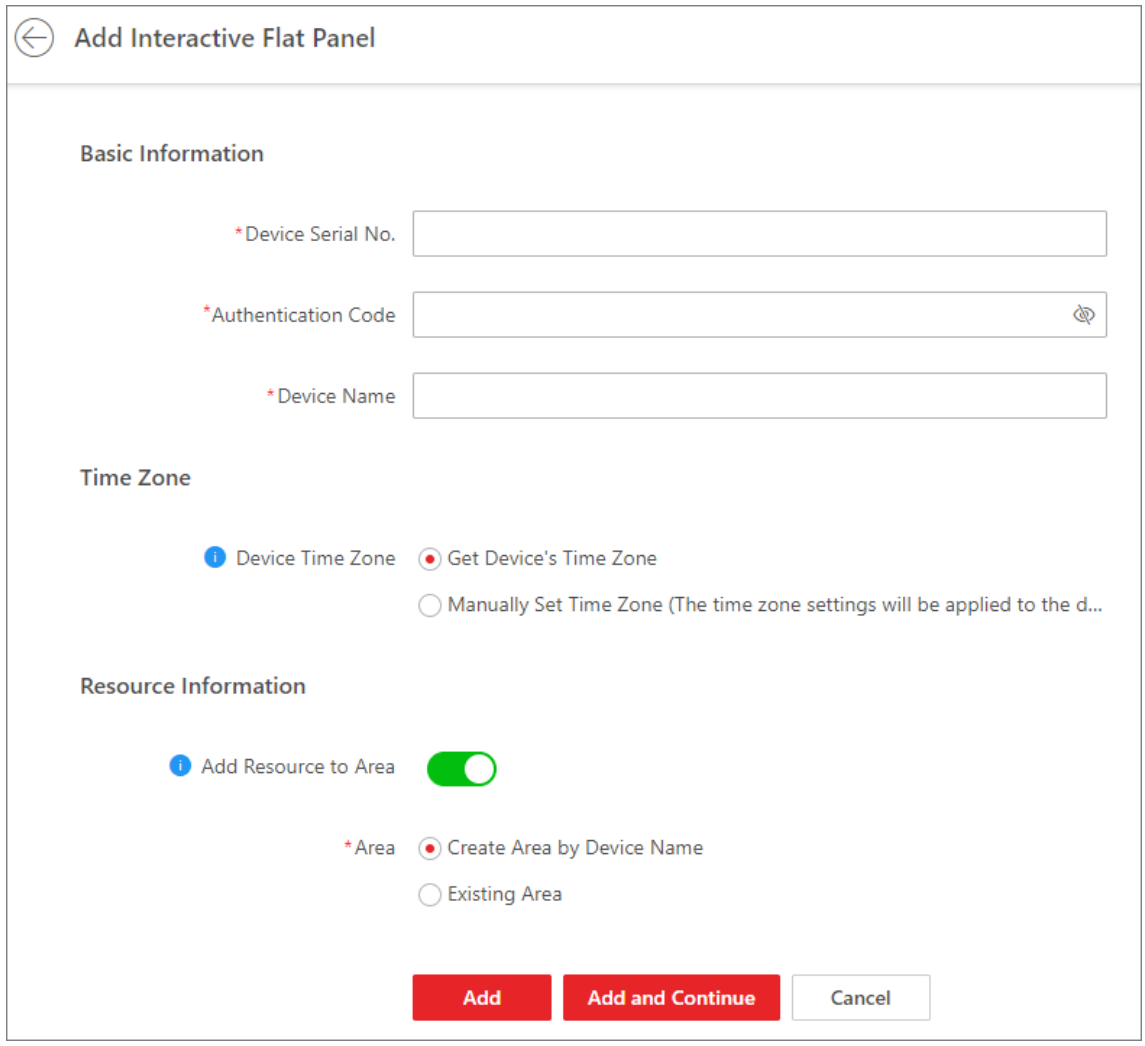


Figure 9-21 Add Interactive Flat Panel

5. Set the basic information.

Device Serial No.

Enter the device serial No.

Authentication Code

Enter the authentication code of the device.

Note

The authentication code should contain 8 to 16 characters, including at least two of the following categories: upper case letters, lower case letters, and digits.

Device Name

Name for the device, which can be used to describe the device function and location.

6. **Optional:** Set the time zone of the device.
   - Select **Get Device's Time Zone** to get the time zone of the device.
   - Select **Manually Set Time Zone** to manually set the time zone of the device and the settings will be applied to the device automatically.
7. **Optional:** Switch on **Add Resource to Area** to import the resources of the added devices to an area.

Note

You can create a new area by the device name or select an existing area. Also, you can click **Add** to add new area(s). For details, refer to ***Add an Area for Current Site*** .

8. Finish adding the device.
   - Click **Add** to add the current device and back to the device list page.
   - Click **Add and Continue** to add the current device and continue to add other devices.
9. **Optional:** Perform the following operations.

Delete Device	Select one or more devices, and click **Delete** to delete the selected devices.
Set Time Zone	Select one or more devices, and click **Time Zone** to configure the time zone of the selected devices. You can select **Get Device's Time Zone** or **Manually Set Time Zone** as needed.
Search Device	Enter keywords in the upper right corner to search for the target device(s).
Edit Device	Click a device to edit its basic information and time zone settings if needed.

What to do next

Register the interactive flat panel online: Enter the IP address of the platform, device name, registration port No. (7660 by default), and the authentication code on the Integrated Control App on the device. Then the device will be added to the platform automatically.

9.19.3 Enable General Authentication Code

You can enable and set the general authentication code on the platform, and then enter the authentication code on the interactive flat panel (referred to as device in the following pages). By this method, you can add the device to the platform.

Before You Start

Make sure you have switched to the Interactive Flat Panel mode. See details in ***Switch Application Mode*** .

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the top, select **Device**.
3. On the left navigation pane, click **Device and Server** → **Interactive Flat Panel** .
4. Click **General Authentication Code Settings**.
5. Switch on **General Authentication Code Settings**.

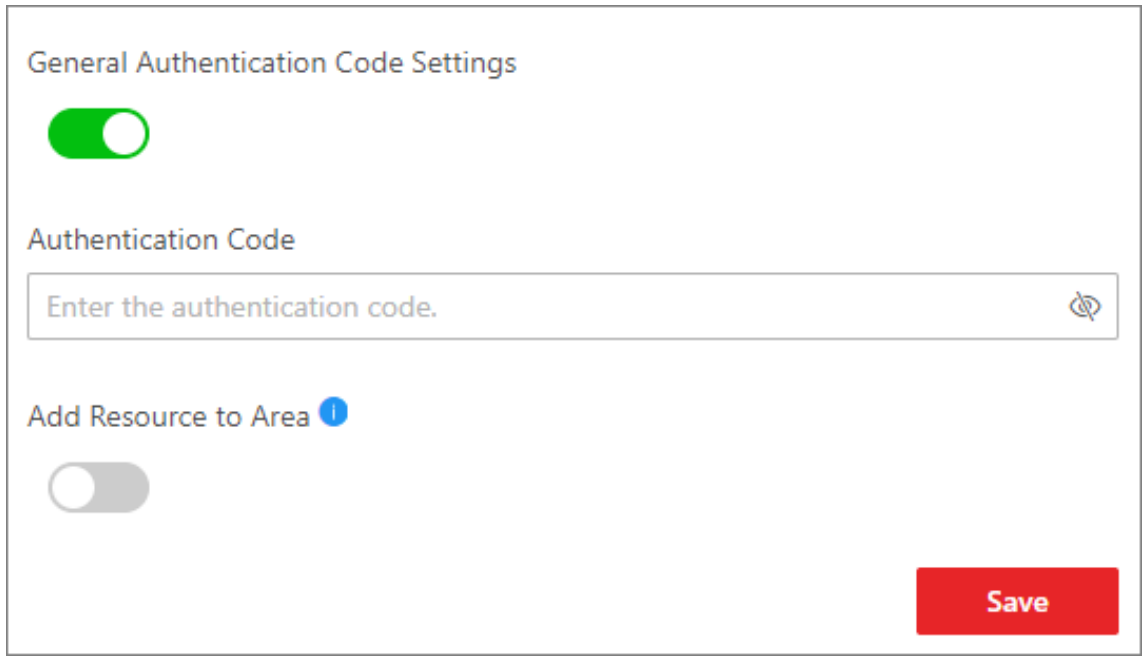


Figure 9-22 Set General Authentication Code

6. Enter the authentication code.

Note

The authentication code should contain 8 to 16 characters, including at least two of the following categories: upper case letters, lower case letters, and digits.

7. **Optional:** Import the resources of the device to the area.
   1) Switch on **Add Resource to Area**.
   2) Select **Create Area by Device Name** or **Existing Area**.

   Create Area by Device Name

   Create a new area by the device name.

   Existing Area

Select an existing area from the area list.

Note

You can create a new area by the device name or select an existing area. Also, you can click **Add** to add new area(s). For details, refer to ***Add an Area for Current Site*** .

8. Click **Save**.
9. **Optional:** Perform the following operations.

Delete Device	Select one or more devices, and click **Delete** to delete the selected devices.
Set Time Zone	Select one or more devices, and click **Time Zone** to configure the time zones of the selected devices. You can select **Get Device's Time Zone** or **Manually Set Time Zone** as needed.
Search Device	Enter keywords in the upper right corner to search for the target device(s).
Edit Device	Click a device to edit its basic information and time zone settings if needed.

What to do next

Register the interactive flat panel online: Enter the IP address of the platform, device name, registration port No. (7660 by default), and the authentication code on the Integrated Control App on the device. Then the device will be added to the platform automatically.

9.20 Manage Smart Wall

Smart wall can provide security personnel with a rich visual overview of the areas you want to keep an eye on. Before displaying the video on smart wall, you need to set up smart wall firstly, and you can also edit, delete smart wall or manage decoding devices here.

This mainly includes the following:

- Decoding devices that can be added to the system and used for decoding the video stream from the encoding devices.
- Virtual smart wall that defines the layout and the name of the smart wall.
- Link between the decoding outputs of the decoding device and the windows of the smart wall.

9.20.1 Add Decoding Device

The decoding devices can be added to the system for linking with the smart wall. You can add online decoding devices with the IP addresses within SYS server's or Web Client's subnet, and can also add decoding devices by IP address, IP segment, or by port segment.

Add Online Decoding Device

The system can perform an automated detection for available decoding devices on the network where the Web Client or SYS server is located, which makes the devices' information about themselves (e.g., IP address) recognized by the system. Based on the information, you can add the devices quickly.

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 HikCentral Professional via network.

Steps

Note

- For Google Chrome, you should install the SADP service according to the instructions and then the online device detection function is available.
- For Firefox, you should install the SADP service and import the certificate according to the instructions and then the online device detection function is available.

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. On the left pane, click **Device and Server** → **Smart Wall** .
3. Below **Decoding Device**, click **Add** to enter the Add Decoding Device page.
4. Select **Online Device** as Adding Mode.
5. In the Online Device area, select a network type.

   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.
6. Select the device(s) to be added.

   Note

   - For the inactive device, you need to create the password for it before you can add it properly. For detailed steps, see .
   - If the detected devices have the same password and user name, you can add multiple devices at a time. Otherwise, you can add them one by one.
7. **Optional:** Switch on **Set as Distributed Main Node** if needed, and select a device from the drop-down list as the main node.

Note

- It is generally used for scenarios such as large-scale command centers and exhibition halls which require thousands of decoding outputs.
- You should specify one device as the main node of the distributed devices, whereas the other devices added at the same time will become normal nodes by default. You can add new nodes to the main node later via the device editing page by clicking **Add** in the Node Details field, or via the decoding device list by hovering over the main node and clicking + .

8. Enter the required information.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

9. Finish adding the decoding device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
10. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output	Click › to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .
Edit Decoding Device	Click to edit information about the decoding device. You can also modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is, and the names of the local signal sources.
Remote Configuration	Click ··· → to set the remote configurations of the device.

Note

For detailed operations, see the user manual of the device.

Delete	Click ··· → × to delete the device.
Configure Cascade	Click behind the added video wall controller to enter the Cascading page. See ***Configure Cascade*** for details.

Add Decoding Device by IP Address

When you know the IP address of the decoding device to add, you can add the device to your system by specifying IP address, user name, password and other related parameters. This adding mode requires you to add the devices one by one, so it is a good choice if you only want to add a few devices and know all the details mentioned above.

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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. On the left pane, click **Device and Server** → **Smart Wall** .
3. Below **Decoding Device**, click **Add** to enter the Add Decoding Device page.
4. Select **IP Address** as Adding Mode.

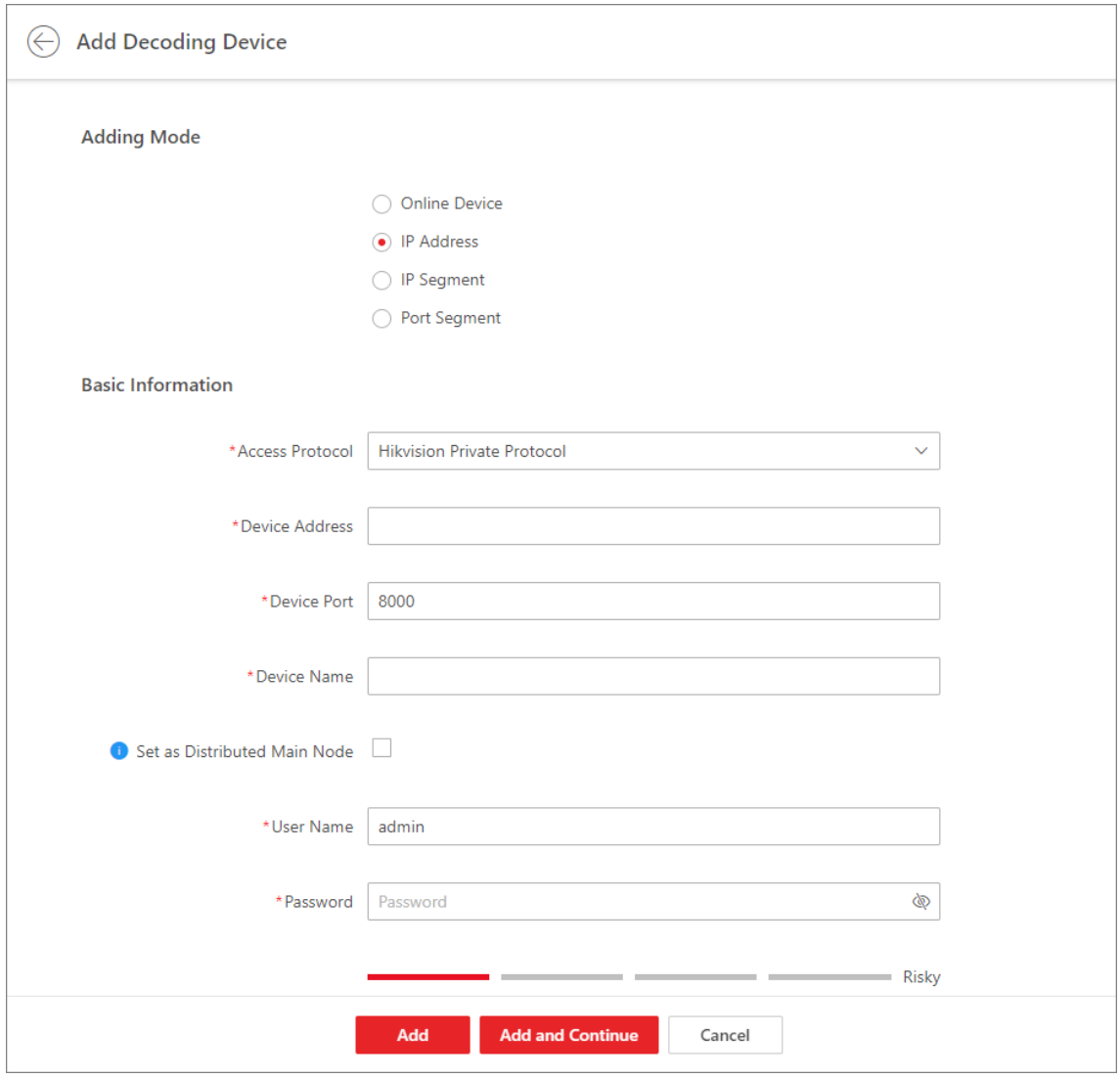


Figure 9-23 Add Decoding Device Page

5. Enter the required information.

Access Protocol

Select **Hikvision Private Protocol** to add the devices.

Device Address

The IP address of the device.

Device Port

The port number on which to scan. The default is 8000.

If the device is located behind a NAT (Network Address Translation)-enabled router or a firewall, you may need to specify a different port number. In such cases, remember to configure the router/firewall so it maps the port and IP address used by the device.

Device Name

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

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

6. **Optional:** Check **Set as Distributed Main Node** to set the device as the main node of distributed devices.

Note

- It is generally used for scenarios such as large-scale command centers and exhibition halls which require thousands of decoding outputs.
- You can add nodes to the main node later via the device editing page by clicking **Add** in the Node Details field, or via the decoding device list by hovering over the main node and clicking + .

7. Finish adding the device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
8. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output	Click > to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .
Edit Decoding Device	Click to edit information about the decoding device. You can also modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is, and the names of the local signal sources.

Remote Configuration	Click ··· → ⚙ to set the remote configurations of the device. **Note** For detailed operations, see the user manual of the device.
Delete	Click ··· → × to delete the device.
Configure Cascade	Click behind the added video wall controller to enter the Cascading page. See ***Configure Cascade*** for details.

Add Decoding Devices by IP Segment

If multiple decoding devices to add have the same port number, user name and password, but have different IP addresses, which are within a range, you can select this adding mode, and specify the IP range where your devices are located, and other related parameters. The system will scan from the start IP address to the end IP address for the devices in order to add them quickly.

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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. On the left pane, click **Device and Server** → **Smart Wall** .
3. Below **Decoding Device**, click **Add** to enter the Add Decoding Device page.
4. Select **IP Segment** as Adding Mode.
5. Enter the required information.

   Access Protocol

   Select **Hikvision Private Protocol** to add the devices.

   Device Address

   Enter the start IP address and end IP address where the devices are located.

   Device Port

   The same port number of the devices. By default, the device port No. is 8000.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

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.

6. **Optional:** Switch on **Set as Distributed Main Node** if needed, and select a device from the drop-down list as the main node.

Note

- It is generally used for scenarios such as large-scale command centers and exhibition halls which require thousands of decoding outputs.
- You should specify one device as the main node of the distributed devices, whereas the other devices added at the same time will become normal nodes by default. You can add new nodes to the main node later via the device editing page by clicking **Add** in the Node Details field, or via the decoding device list by hovering over the main node and clicking + .

7. Finish adding the device.
   - Click **Add** to add the decoding device and back to the decoding device list page.
   - Click **Add and Continue** to save the settings and continue to add other decoding devices.
8. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output	Click > to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .
Edit Decoding Device	Click to edit information about the decoding device. You can also modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is, and the names of the local signal sources.
Remote Configuration	Click ··· → to set the remote configurations of the device. **Note** For detailed operations, see the user manual of the device.
Delete	Click ··· → × to delete the device.
Configure Cascade	Click behind the added video wall controller to enter the Cascading page. See ***Configure Cascade*** for details.

Add Decoding Devices by Port Segment

When multiple decoding devices to add have the same IP address, user name and password, but have different port numbers, which are within a range, you can select this adding mode and specify the port range, IP address, user name, password, and other related parameters to add them.

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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. On the left pane, click **Device and Server** → **Smart Wall** .
3. Below **Decoding Device**, click **Add** to enter the Add Decoding Device page.
4. Select **Port Segment** as Adding Mode.
5. Enter the required information.

   Access Protocol

   Select **Hikvision Private Protocol** to add the devices.

   Device Address

   The same IP address where the devices are located.

   Device Port

   Enter the start port number and the end port number on which to scan.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

   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.
6. Finish adding the device.
   - Click **Add** to add the decoding device and back to the decoding device list page.

- Click **Add and Continue** to save the settings and continue to add other decoding devices.

After adding the decoding device, the device will display in the list on Decoding Device panel.

7. **Optional:** Perform the following operations after adding the decoding device.

View Decoding Output	Click > to show the decoding outputs. You can view the output resolution and linking status after linking the output to smart wall. For details about linking decoding output with smart wall, see ***Add Smart Wall*** .
Edit Decoding Device	Click to edit information about the decoding device. You can also modify the network location as LAN IP address or WAN IP address according to the type of the network where the device is, and the names of the local signal sources.
Remote Configuration	Click ··· → to set the remote configurations of the device. **Note** For detailed operations, see the user manual of the device.
Delete	Click ··· → × to delete the device.
Configure Cascade	Click behind the added video wall controller to enter the Cascading page. See ***Configure Cascade*** for details.

9.20.2 Configure Cascade

In some actual scenarios for large screen display, the screen number of the smart wall will exceed the decoding output number of one decoder, or the cross-decoder functions such as roaming and spanning are required. You can cascade two decoders with video wall controller to meet various display demands.

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 HikCentral Professional via network.
- The decoders' interfaces have be connected with the video wall controller's using the matched wires.
- The decoders and video wall controller are added to the HikCentral Professional. Refer to ***Add Decoding Device*** for details.

Perform this task when you need to configure cascade for the decoding devices as follows.

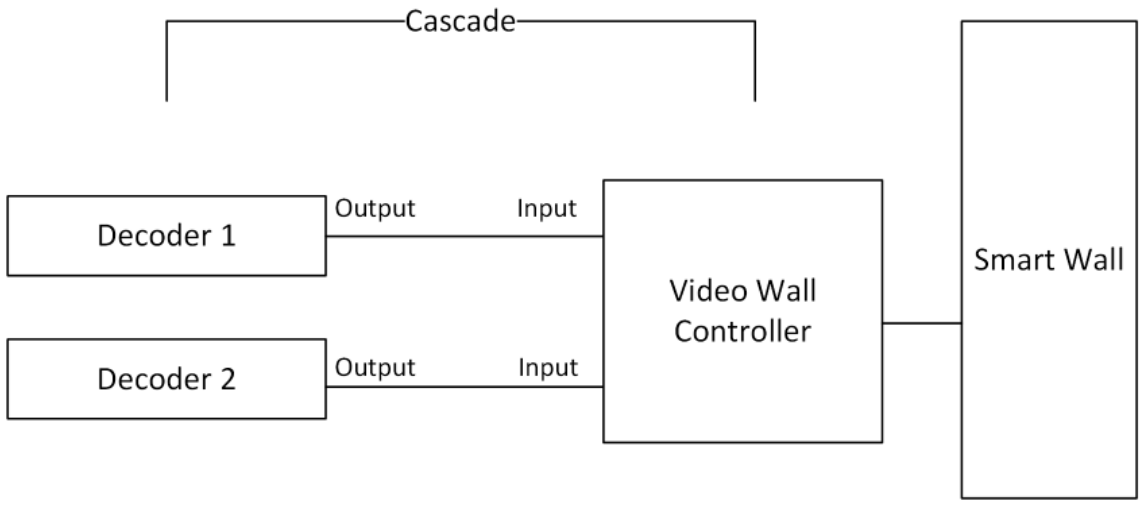


Figure 9-24 Cascade

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. On the left pane, click **Device and Server** → **Smart Wall** .
3. Click behind the added video wall controller to enter the Cascading page.

Note

Only video wall controller DS-C10S and DS-C10S-T can support this function.

4. Select the signal channel of the video wall controller and click .
5. Select the decoding output of the decoders to set it as the signal input of the video wall controller.

Note

If the decoders are cascaded with video wall controller, the spared decoding outputs of the decoders cannot be used to display on smart wall any more.

6. Click **Save** to save the cascade.

Result

After configuring cascade, you need to add a smart wall and link the decoding outputs of the video wall controller to display the signal outputs of the two decoders on the smart wall.

9.20.3 Add Smart Wall

You can add the smart wall to the system and configure its rows and columns.

Steps

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

2. On the left pane, click **Device and Server → Smart Wall** .
3. Below **Smart Wall**, click **Add** to enter the Add Smart Wall page.

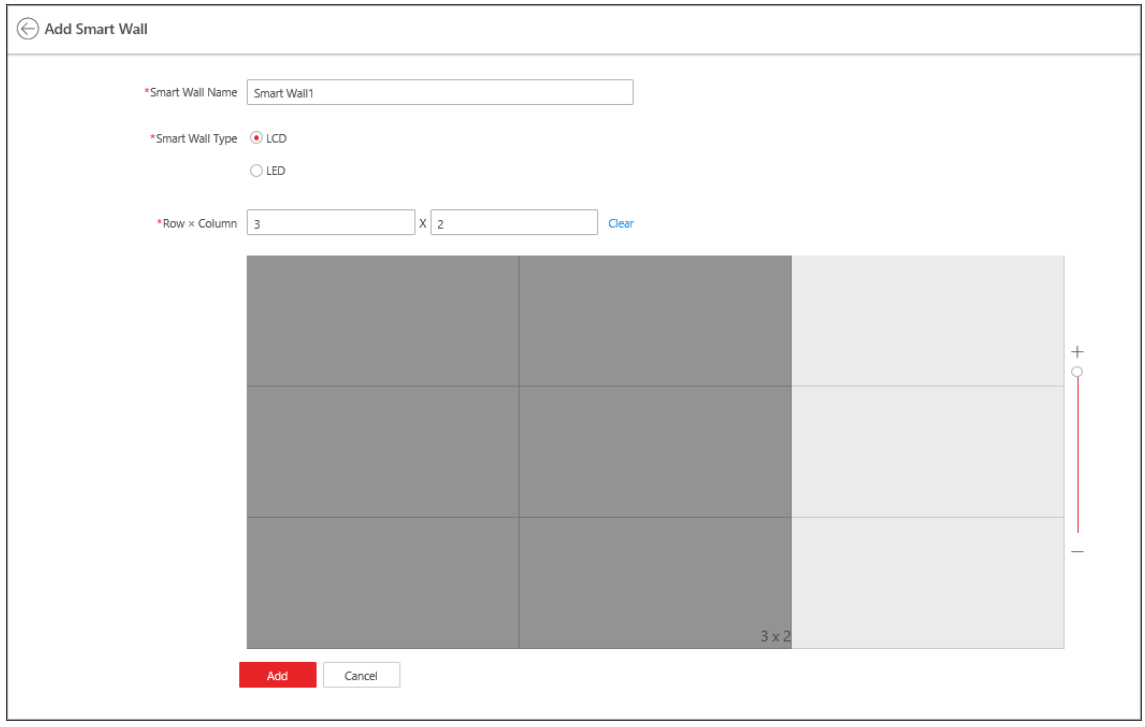


Figure 9-25 Add Smart Wall Page

4. Set the name for the smart wall.
5. If the smart wall type is **LED**, select the max. resolution of the single output in the drop-down list.

Note

You can also select **Customize** to customize the resolution.

6. Set the row number and the column number.
7. Click **Add**.
8. **Optional:** Perform the following operations after adding the smart wall.

Link Decoding Output with Window	For details about the operations, see ***Link Decoding Output with Window*** .
Edit Smart Wall	Click to edit the name of the smart wall.
Delete Smart Wall	Click × to delete the smart wall.
Set Default Stream Type	For details about setting the default stream type for cameras, refer to ***Set Default Stream Type for Cameras on Smart Wall*** .

9.20.4 Link Decoding Output with Window

After adding the decoding device and smart wall, you should link the decoding device's decoding output to the window of the smart wall.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. On the left pane, click **Device and Server** → **Smart Wall** .
3. Click › in front of a decoding device to show its decoding outputs.
4. Click › in front of a smart wall to show its windows.
5. Drag the decoding output from the Decoding Device panel to the display window of the smart wall, to configure a one-to-one correspondence.

Note

You can also press the Ctrl key and Alt key at the same time, and select two decoding outputs. All decoding outputs between the two outputs will also be selected, then you can drag all outputs to the display window.

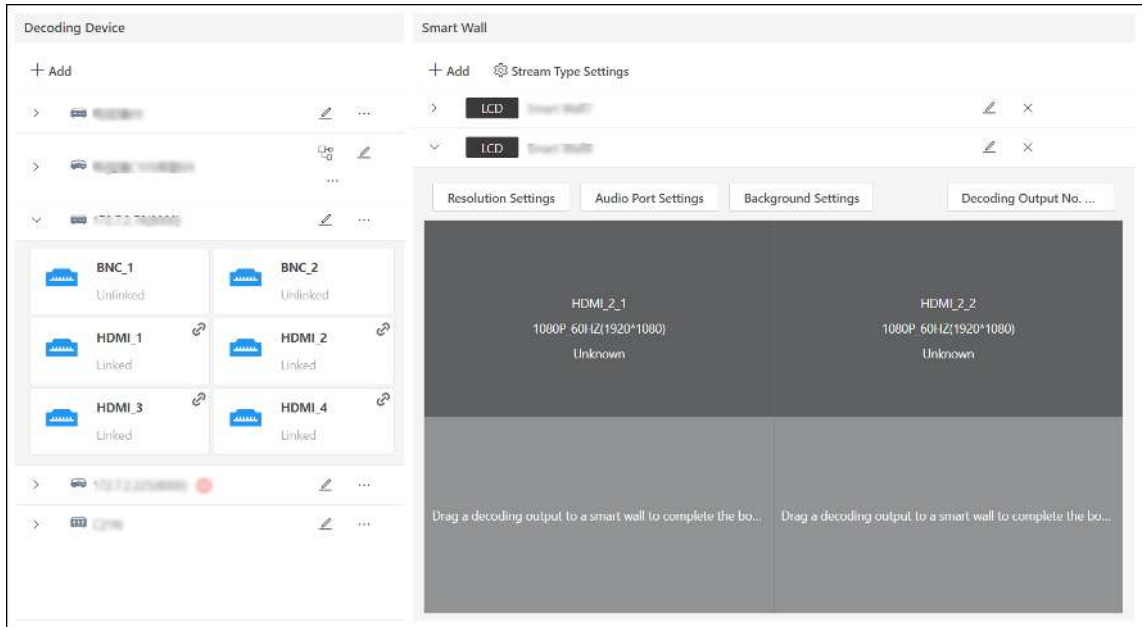


Figure 9-26 Link Decoding Device with Window

6. **Optional:** Perform the following operations after linking the decoding output with the window.

Cancel Linkage	Click on the top right corner of each window to release the linkage.
Set Resolution	Click **Resolution Settings** to select a decoding output resolution from the drop-down list.
Set Audio Port	Click **Audio Port Settings** to select an audio port.

Set Background	a. Click **Background Settings**. b. Enable **Background**. c. Select background type. - If the type is **Color**, set the background color below. - If the type is **Background Picture**, click **Upload Picture** to upload background pictures. Up to 64 pictures can be uploaded. d. Click **Save**.
Set Decoding Output No. Displayed on Screen	Click **Decoding Output No. Displayed on Screen**. After it is clicked, the decoding output No. will be displayed on the screen for 30 to 60 seconds.

9.20.5 Set Default Stream Type for Cameras on Smart Wall

According to the actual screen size, display effect, network bandwidth, or other requirements, you can set the default stream type for cameras displayed on smart wall, including main stream and sub-stream. You can also set a threshold about window division mode to switch between main stream and sub-stream automatically. The default stream type is effective for all cameras decoded and displayed on smart wall firstly.

On the top navigation bar, select → **Basic Management** → **Device** . Click **Device and Server** → **Smart Wall** on the left pane, and then click **Stream Type Settings** below **Smart Wall**.

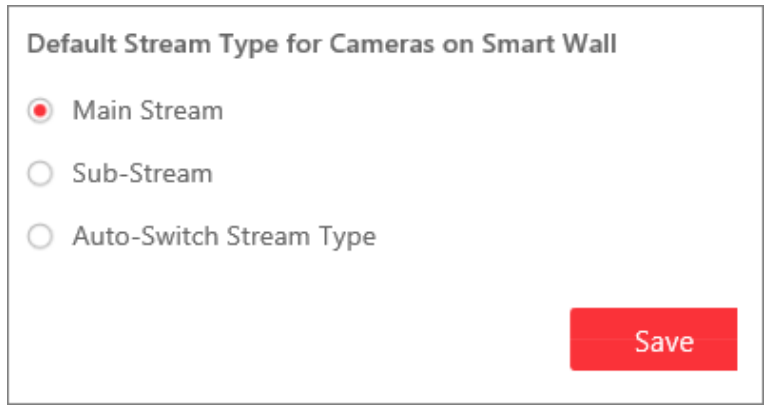


Figure 9-27 Set Default Stream Type for Cameras on Smart Wall

Main Stream

Main stream provides higher quality video, higher resolution, but brings about higher bandwidth usage. If you select main stream as default type, the live video streams of all cameras will be decoded and displayed on smart wall in main stream mode.

Sub-Stream

Sub-stream can save on bandwidth, but the video quality is lower than main stream. If you select sub-stream as default type, the live video streams of all cameras will be decoded and displayed on Smart Wall in sub-stream mode.

Auto-Switch Stream Type

If a window's proportion of the smart wall is larger than the configured threshold, the stream type will be main stream. If the proportion is smaller than the threshold, it will be switched to sub-stream. For example, if you set the threshold as ¼, when the window division turns to 5-window from 2-window, the stream type will be switched from main-stream to sub-stream.

9.21 Manage IP Speakers

You can add the IP speakers to the platform via multiple methods such as adding by IP address and IP segment. After that, you can manage the added IP speakers, including editing and deleting devices, configuring devices remotely, changing devices' passwords, etc.

9.21.1 Add Detected Online IP Speakers

The platform can automatically detect the available IP speakers on the same network where the Web Client or the SYS server is located, which makes the devices' information (e.g., IP address) recognized by the platform. Based on the information, you can add the devices quickly.

You can add one online device at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add a Detected Online IP Speaker

For the detected online IP speakers, you can add the device one by one to HikCentral Professional by specifying its user name, password and some other parameters.

Before You Start

- Make sure the IP speakers to be added 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the left navigation pane, click **Device and Server** → **IP Speaker** .

3. **Optional:** In the Online Device area, select a network type to filter the detected online devices.

   Server Network

   The detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

   Local Network

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

4. Select an active device to be added.
5. Click **Add to Device List** to open the Add Online Device window.
6. Set the required information.

   Device Address

   The IP address of the device, which displays automatically.

   Device Port

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

   Device Name

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

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to the platform using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

   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.

7. **Optional:** Switch on **Add Resource to Area** to import the resources of the device to the area.

   Note

   You can create a new area by the device name or select an existing area from the area list. Also, you can click **Add** to add a new area. For details about adding a new area, refer to ***Add Area*** .

8. Click **Add** to add the current device.
9. **Optional:** Perform the following operations.

Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Search Device	Enter a key word in the search box in the upper-right corner, and click (or press the Enter key) to search for the target device(s).
View Error Message	If there is an icon appearing beside the device name, hover the mouse cursor to the icon and view the error message. You can click **Edit**/**Refresh** to edit/refresh the device if needed.
Format SD Card	Click to format the SD card of the IP speaker.

Batch Add Detected Online IP Speakers

For the detected online IP speakers, if they have the same user name and password, you can batch add multiple devices to HikCentral Professional.

Before You Start

- Make sure the IP speakers to be added 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for details.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the left navigation pane, click **Device and Server** → **IP Speaker** .
3. **Optional:** In the Online Device area, select a network type to filter the detected online devices.

   Server Network

The detected online devices on the same local subnet with the SYS server will be listed in the Online Device area.

Local Network

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

4. Select the active devices to be added.
5. Click **Add to Device List** to open the Add Online Device window.
6. Set the required information.

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to the platform using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

7. **Optional:** Switch on **Add Resource to Area** to import the resources of the device to the area.

Note

You can create a new area by the device name or select an existing area from the area list. Also, you can click **Add** to add a new area. For details about adding a new area, refer to ***Add Area*** .

8. Click **Add** to batch add these devices.
9. **Optional:** Perform the following operations.

Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Search Device	Enter a key word in the search box in the upper-right corner, and click or press the Enter key to search for the target device(s).
View Error Message	If there is an icon appearing beside the device name, hover the mouse cursor to the icon and view the error message. You can click **Edit**/**Refresh** to edit/refresh the device if needed.
Format SD Card	Click to format the SD card of the IP speaker.

9.21.2 Add IP Speaker by Serial No.

When you know the serial No. of an IP speaker, you can add it to the platform by specifying the serial No., user name, password, etc.

Before You Start

Make sure the IP speakers to be added 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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the left navigation pane, click **Device and Server** → **IP Speaker** .
3. Click **Add** to enter the Add IP Speaker page.
4. Select **Serial No.** as the Adding Mode.
5. Enter the required information.

Device Serial No.

The serial No. of the device.

Device Name

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

User Name

The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to the platform using the non-admin account, your permissions may restrict your access to certain features.

Password

The password required to access the account.

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.

6. **Optional:** Switch on **Add Resource to Area** to import the resources of the device to the area.

Note

You can create a new area by the device name or select an existing area from the area list. Also, you can click **Add** to add a new area. For details about adding a new area, refer to ***Add Area*** .

7. Add the device.
   - Click **Add** to add the current device and return to the device list.
   - Click **Add and Continue** to add the current device and continue to add other device(s).
8. **Optional:** Perform the following operations.

Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Format SD Card	Click to format the SD card of the IP speaker.
Search Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
View Error Message	If there is an icon appearing beside the device name, hover the mouse cursor to the icon and view the error message. You can click **Edit**/**Refresh** to edit/refresh the device if needed.

9.21.3 Batch Add IP Speakers

When there are multiple IP speakers to be added, you can edit the predefined template containing the required device information, and import the template to HikCentral Professional to add devices in a batch.

Before You Start

Make sure the IP speakers to be added 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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** to enter the device management page.
2. On the left navigation pane, click **Device and Server** → **IP Speaker** .
3. Click **Add** to enter the Add IP Speaker page.
4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template to your PC.
6. Open the template file and enter the required information of the devices in the corresponding column.
7. Click and select the edited file.
8. Add the devices.
   - Click **Add** to add the current devices and return to the device list.
   - Click **Add and Continue** to add the current devices and continue to add other devices.
9. **Optional:** Perform the following operations.

Remote Configurations	Click to configure the device remotely. **Note** For details about remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click to change the password(s) for the device(s). **Note** • You can only change the password for online HIKVISION devices currently. • If the devices have the same password, you can select multiple devices to change the password for them at the same time.
Format SD Card	Click to format the SD card of the IP speaker.

Search for Device	Enter a keyword in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).
View Error Message	If there is an icon appearing beside the device name, hover the mouse cursor to the icon and view the error message. You can click **Edit/Refresh** to edit/refresh the device if needed.

9.22 Manage Security Inspection Devices

You can add security inspection devices to the platform for management, including editing and deleting devices, remote control, etc. The platform supports multiple ways for adding security inspection devices.

9.22.1 Add a Detected Online Security Inspection Device

You can only add a single detected online security inspection device to the platform at a time.

Before You Start

- Make sure the security inspection 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Security Inspection Device** .
3. 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 current Web Client will be listed in the Online Device area.
4. In the Online Device area, select **Hikvision Private Protocol** or **Hikvision ISUP Protocol** to filter the detected online devices.

Note

To display devices which can be added to the platform via ISUP, you need to go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.

5. In the Online Device area, select an active device and click **Add to Device List** to open the Add Security Inspection Device window.
6. Select a device type from the drop-down list.
7. Enter the required information.

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.

8. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
9. **Optional:** Switch on **Add Resource to Area** to import the resources of the added security inspection device to an area.

Note

- You can select all resources or the specified camera(s) to be added.
- You can create a new area by the device name or select an existing area.
- If you do not import resources to area, you cannot perform further configurations for the resources.

10. **Optional:** If you choose to add resources to area, select a Streaming Server to get the video stream.

Note

You can check **Wall Display via Streaming Server** to get stream via the selected Streaming Server when displaying live view on the smart wall.

11. **Optional:** If you choose to add resources to area, switch on **Video Storage** and select a storage location for recording.

Note

Configure the Hybrid Storage Area Network, Cloud Storage Server, or pStor in advance, or the storage location cannot be displayed in the drop-down list.

Encoding Device

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

Hybrid Storage Area Network

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

Cluster Storage

The video files will be stored in the cluster storage server 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.

pStor Cluster Service

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

12. **Optional:** Set the recording schedule for the added resources.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device.
    - Uncheck **Get Device's Recording Settings** and set the required information, including recording schedule template, stream type, etc. Refer to ***Configure Recording for Cameras on Current Site*** for details.
13. Click **Add**.
14. **Optional:** Perform the following operations for the added device(s).

Remote Configurations	Click to set the remote configurations of the device. **Note** For details about the remote configurations, refer to the user manual of the device.
Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.22.2 Add Security Inspection Device by Device ID

For the security inspection devices supporting ISUP, you can add them by specifying the predefined device ID, ISUP login password, etc. This is an economic choice when you need to manage a security inspection device in the public network without a fixed IP address.

Before You Start

- Make sure the security inspection 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Security Inspection Device** .
3. Click **Add** to enter the Add Security Inspection Device page.
4. Select **Security Inspection System**, **Analyzer** or **Walk-Through Metal Detector** as the device type from the drop-down list.
5. Select **Hikvision ISUP Protocol** as the access protocol.

Note

To allow device registration via ISUP, you need to go to → **Basic Management** → **System** → **Network** → **Device Access Protocol** and switch on **Allow ISUP Registration**.

6. Enter the required information, including device ID, ISUP login password, and device name.

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.

7. **Optional:** Switch on **Picture Storage** and select a storage location from the drop-down list.

Local Storage

The pictures will be stored in the local storage space of the platform server.

Hybrid Storage Area Network

The pictures will be stored in the Hybrid Storage Area Network.

Cluster Storage

The pictures will be stored in the cluster storage server.

pStor

The pictures will be stored in the pStor, which is the storage access service for managing local HDDs and logical disks.

Network Video Recorder

The pictures will be stored in the network video recorder.

8. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

   Note

   You can click **View** to view the details of the selected time zone.
9. **Optional:** Switch on **Add Resource to Area** to import the resources of the added security inspection device to an area.

   Note

   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to the area, you cannot perform further configurations for the resources.
10. **Optional:** If you choose to add resources to an area, select a streaming server to get the video stream.

    Note

    You can check **Wall Display via Streaming Server** to get the stream via the selected Streaming Server when displaying live view on the smart wall.
11. **Optional:** Check **Get Device's Recording Settings** to get the recording schedule from the device.
12. Finish adding the device.
    - Click **Add** to save the settings and go back to the device list page.
    - Click **Add and Continue** to save the settings and continue to add another device.
13. **Optional:** Perform the following operations for the added devices.

Remote Configurations	Click to set the remote configurations of the device. **Note** For details about the remote configurations, refer to the user manual of the device.
Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.22.3 Add Security Inspection Device by IP Address

If you know the IP address or domain name of a security inspection device, you can add it to the platform by specifying the IP address (or domain name), user name, password, etc.

Before You Start

- Make sure the security inspection 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 HikCentral Professional via network.
- The devices to be added should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operation about activating devices.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Device and Server → Security Inspection Device** .
3. Click **Add** to enter the Add Security Inspection Device page.
4. Select **Security Inspection System**, **Analyzer** or **Walk-Through Metal Detector** as the device type from the drop-down list.
5. Select **Hikvision Private Protocol** as the access protocol.
6. Enter the required information, including the device address, device name, user name, and 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.
7. **Optional:** Set the time zone for the device.
   - Click **Get Device's Time Zone**.
   - Click **Manually Set Time Zone** and select a time zone from the drop-down list.

     Note

     You can click **View** to view the details of the selected time zone.
8. **Optional:** Switch on **Add Resource to Area** to import the resources of the added security inspection device to an area.

   Note

   - You can select all resources or the specified camera(s) to be added.
   - You can create a new area by the device name or select an existing area.
   - If you do not import resources to the area, you cannot perform further configurations for the resources.
9. **Optional:** If you choose to add resources to an area, select a Streaming Server to get the video stream.

Note

You can check **Wall Display via Streaming Server** to get the stream via the selected Streaming Server when displaying live view on the smart wall.

10. **Optional:** If you choose to add resources to an area, switch on **Video Storage** and select a storage location for recording.

Note

Configure the Hybrid Storage Area Network, Cloud Storage Server, or pStor in advance, or its storage location cannot be displayed in the drop-down list.

Security Inspection Device

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

Hybrid Storage Area Network

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

Cluster Storage

The video files will be stored in the Cluster Storage Server 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.

pStor Cluster Service

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

11. **Optional:** Set the recording schedule for the added resources.
    - Check **Get Device's Recording Settings** to get the recording schedule from the device.
    - Uncheck **Get Device's Recording Settings** and set the required information, such as recording schedule template, stream type, etc. Refer to ***Configure Recording for Cameras on Current Site*** for details.
12. Finish adding the device.
    - Click **Add** to save the settings and go back to the device list page.
    - Click **Add and Continue** to save the settings and continue to add another device.
13. **Optional:** Perform the following operations for the added devices.

Remote Configurations	Click ⚙ to set the remote configurations of the device. **Note** For details about the remote configurations, refer to the user manual of the device.

Set Time Zone	Select the added device(s) and click **Time Zone** to set the time zone for the device(s).
Search for Device	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target device(s).

9.23 Network Transmission Device Management

Network transmission devices (switch, network bridge and fiber converter) can be added to the system for management, to help the system monitor the network status of the managed devices.

After the network transmission devices are added to the system, the Control Client will automatically draw a network topology according to the location of the added devices, and display the information (IP address, port No., port status and stream rate) and network link status (fluent, busy, congested, disconnected).

9.23.1 Add Detected Online Network Transmission Devices

The system can perform an automated detection for available network transmission device s in the network where the Web Client or server is located, which makes the devices' information about themselves (e.g., IP address) recognized by the system. Based on the information, you can add the devices quickly.

You can add one online devices at a time, or add multiple online devices in a batch.

Note

You should install the web control according to the instructions and then the online device detection function is available.

Add a Detected Online Network Transmission Device

When you want to add one of the detected online devices or add some of these devices with different user names and passwords, you need to select only one device every time to add it to HikCentral Professional. The IP address, port number and user name will be recognized automatically, which can reduce some manual operations in a way.

Before You Start

Make sure the network device (switch, bridge or fiber converter) you are going to use is 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 device to the HikCentral Professional via network.

Steps

1. On the top, select **Device**.

2. Select **Device and Server → Network Transmission Device** on the left.
3. In the Online Device area, select a network type.

   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.
4. In the Online Device area, select the active device to be added.
5. Click **Add to Device List** to open the Add Network Transmission Device window.
6. Set the required information.

   Device Address

   The IP address of the device, which is filled in automatically.

   Device Port

   The port number of the device, which is filled in automatically.

   Device Name

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

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

   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.

   Country Code

   The country code defines the country/region where device will be used.

Note

- You should read and agree the disclaimer to set the country code.
- The country code is required for wireless bridges.
- You cannot edit the country code of the added device on its details page.

7. Click **Add**.
8. **Optional:** Perform the following operations after adding the device.

Remote Configuration

Click in the Operation column to set the remote configurations of the corresponding device.

Note

For detailed operation steps for the remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online Hikvision devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set the System Connected Device

Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

Add Detected Online Network Transmission Devices in a Batch

For the detected online transmission network devices, if they have the same user name and password, you can add multiple devices to HikCentral Professional at a time.

Before You Start

Make sure the network devices (switches, bridges or fiber converters) 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 HikCentral Professional via network.

Steps

1. On the top, select **Device**.

2. Select **Device and Server → Network Transmission Device** on the left.
3. In the Online Device area, select a network type.

   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.
4. In the Online Device area, select the devices to be added.
5. Click **Add to Device List** to enter the Add Online Device window.
6. Enter the user name, password, and country code.

   User Name

   The user name for administrator account created when activating the device or the added non-admin account such as operator. When adding the device to HikCentral Professional using the non-admin account, your permissions may restrict your access to certain features.

   Password

   The password required to access the account.

   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.

   Country Code

   The country code defines the country/region where device will be used.

   Note

   - You should read and agree the disclaimer to set the country code.
   - The country code is required for wireless bridges.
   - For the added device, its country code cannot be edited on the device details page.
7. Click **Add**.
8. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to set the remote configurations of the corresponding device.

Note

For detailed operation steps for the remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set the System Connected Device

Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

9.23.2 Add Network Transmission Device by IP Address

When you know the IP address of a device, you can add it to the system by specifying the IP address, user name, password, etc.

Before You Start

Make sure the network device (switch, bridge or fiber converter) you are going to use is 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 device to the HikCentral Professional via network.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Network Transmission Device** on the left.
3. Click **Add** to enter the Add Network Transmission Device window.
4. Select **IP Address** as the adding mode.
5. Enter the required information.

   Device Address

   IP address of the device.

   Device Port

   The default device port number is 8000.

Device Name

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

User Name

The administrator account which is created when activating the device, or the non-administrator account, such as operator. When adding device by non-administrator, the permission might be limited.

Password

The password required to access the account.

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.

Country Code

The country code defines the country/region where device will be used.

Note

- You should read and agree the disclaimer to set the country code.
- The country code is required for wireless bridges.
- Once the device is added, its country code cannot be edited on the device details page.

6. Finish adding the device.
   - Click **Add** to add the current device and back to the device list page.
   - Click **Add and Continue** to finish adding the current device and continue adding other devices.
7. **Optional:** Perform the following operations after adding devices.

Remote Configuration	Click ⚙ in the Operation column to set the remote configurations of the corresponding device. **Note** For detailed operation steps for the remote configuration, see the user manual of the device.
Change Password	Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set the System Connected Device

Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

9.23.3 Import Network Transmission Devices in a Batch

If there are a large number of devices to be added, you can enter the device information in the pre-defined template and upload the template to add the network transmission devices in a batch.

Before You Start

Make sure the network devices (switches, bridges or fiber converters) 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 HikCentral Professional via network.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Network Transmission Device** on the left.
3. Click **Add** to enter the Add Network Transmission Device window.
4. Select the adding mode as **Batch Import**.
5. Click **Download Template** to download the template to the local PC.
6. Open the downloaded template file, and enter the required device information.
7. Click to select the edited template file.
8. Finish adding the device.
   - Click **Add** to add the current device and back to the device list page.
   - Click **Add and Continue** to finish adding the current device and continue adding other devices.
9. **Optional:** Perform the following operations after adding devices.

Remote Configuration

Click in the Operation column to set the remote configurations of the corresponding device.

Note

For detailed operation steps for the remote configuration, see the user manual of the device.

Change Password

Select the added device(s) and click **Change Password** to change the password for the device(s).

Note

- You can only change the password for online HIKVISION devices currently.
- If the devices have the same password, you can select multiple devices to change the password for them at the same time.

Set the System Connected Device

Select the device, click **System Connected Switch** to set the switch as the system connected device.

Note

System connected switch is the switch that is directly connected with the SYS server.

9.24 Upgrade Device Firmware

You can upgrade the firmwares of the devices added to the system via the current Web Client or Hik-Connect.

Via Current Web Client

The following devices are supported to be upgraded the firmwares via the current Web Client:

- Camera
- NVR (Network Video Recorder)
- DVR (Digital Video Recorder)
- Decoding Device
- Access Control Device
- Card Reader
- Security Control Panel (including AX Security Control Panel)
- Security Radar
- Indoor Station
- Door Station

Note

Upgrading the card reader linked to the door station is not supported.

- Main Station
- Guidance Terminal

Note

You can also upgrade the cameras access to the NVR in a batch.

Via Hik-Connect

The following devices are supported to be upgraded the firmwares via Hik-Connect:

- Camera
- NVR
- DVR
- Indoor Station
- Door Station

Note

Upgrading the card reader linked to the door station is not supported.

- Main Station
- Digital Signage Terminal

Note

You can also upgrade the cameras linked to the NVR in a batch.

9.24.1 Upgrade Device Firmware via Current Web Client

You can upgrade device firmware via the current Web Client.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Firmware Upgrade** on the left.
3. Select the **Via Current Web Client** tab.
4. In the **Upgrade By** field, select the upgrade method.
5. In the **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

   Example

   If you set the value to 5, up to 5 devices can be selected for batch upgrade.
6. Select an upgrade package from the local computer and then click **Next**.

   The upgradable devices will be displayed.
7. **Optional:** Filter devices by device type, device firmware version, or device model.
8. Select device(s) and then click **Next**.
9. Select an upgrade schedule to upgrade the selected device(s).
   - Select **Upgrade Now** from the **Upgrade Schedule** drop-down list to start upgrade.

- Select **Custom** from the **Upgrade Schedule** drop-down list and then customize a time period to upgrade the selected device(s).

10. Click **OK** to save the firmware upgrade settings.

    The upgrade task list will be displayed.

11. **Optional:** In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

9.24.2 Upgrade Device Firmware via Hik-Connect

You can upgrade device firmware via Hik-Connect, which is a cloud service.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Firmware Upgrade** on the left.
3. Select the **Via Hik-Connect** tab.
4. In the **Device Access Protocol** field, select the relevant protocol.
5. 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.

6. In **Simultaneous Upgrade** field, set the maximum number of devices for simultaneous upgrade.

   Example

   If you set the value to 5, up to 5 devices can be selected for batch upgrade.

7. Click **Next**.
8. 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.

   The upgradable devices will be displayed.

9. Select device(s) and click **Next** to enter the upgrade schedule page.
10. Select an upgrade schedule to upgrade the selected device(s).
    - Select **Upgrade Now** from the **Upgrade Schedule** drop-down list to start upgrade.
    - Select **Custom** from the **Upgrade Schedule** drop-down list and then customize a time period to upgrade the selected device(s).
11. Click **OK** to save the firmware upgrade settings.

    The upgrade task list will be open.

12. **Optional:** In the top right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.

9.24.3 Upgrade Device Firmware via FTP

You can upgrade device firmware via FTP.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Firmware Upgrade** on the left.
3. Select the **Upgrade Firmware via FTP** tab.
4. 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 saved 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.
5. Click **Next**.
6. Select an upgrade package from the local PC and then click **Next**.

   The upgradable device list will be displayed.
7. **Optional:** Filter devices by device type, device firmware version, or device model.
8. Select a device type and select a device from the device list.
9. **Optional:** If you select Dock Station as the device type, you need to select an upgrade object from the drop-down list.
10. Select **Upgrade Now** or **Custom** as the upgrading schedule.
11. Click **OK** to save the firmware upgrade settings.

The upgrade task list will be displayed.

12. **Optional:** In the upper-right corner of firmware upgrade page, click **Upgrade Tasks** to view the task details and control the task status.
13. **Optional:** In the upgrade task list, click × in the Operation column to delete the upgrade task.

9.25 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.

For detailed operations of restoring device's default password, refer to ***Restore Device's Default Password*** .

For detailed operations of resetting device's password, refer to ***Reset Device Password*** .

9.25.1 Reset Device Password

If you forget the password you use to access the online device, you can request for a key file from your technical support and reset the device's password through the platform.

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 HikCentral Professional via network.
- The devices should be activated. Refer to ***Create Password for Inactive Device(s)*** for details about activating devices.

Perform this task when you need to reset the device's password. Here we take creating password for the encoding device as an example.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Device and Server → Encoding Device** on the left.
3. 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.

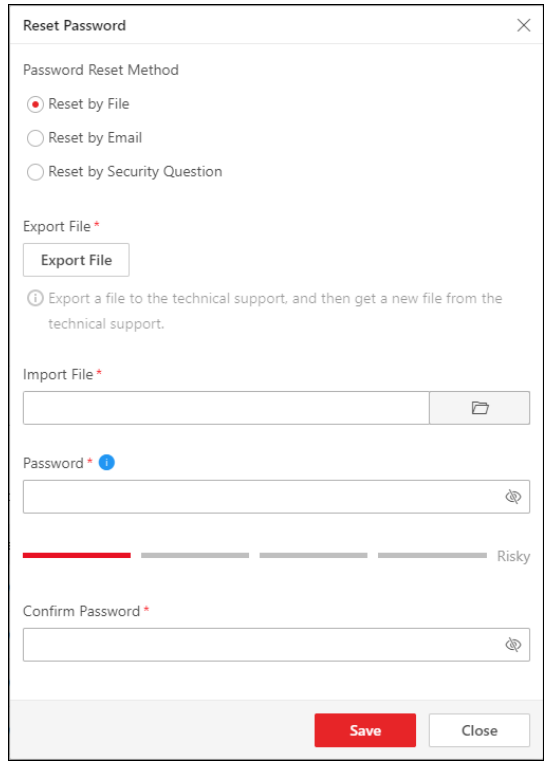


Figure 9-28 Reset Password

4. Select a password reset method:

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.

5. Click **Save** to save the change.

9.25.2 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.

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 HikCentral Professional via network.
- The devices should be activated. Refer to ***Create Password for Inactive Device(s)*** for detailed operations about activating devices.

Perform this task when you need to restore the device's default password. Here we take restoring the default password for an encoding device as an example.

Steps

1. On the top, select **Device**.
2. Click **Device and Server → Encoding Device** on the left.
3. In the Online Device area, view the device status (shown on Security column) and click in the Operation column of an active device.

   A dialog with security code pops up.
4. Enter the security code and restore the default password of the selected device.

Note

Contact our technical support to obtain a security code.

What to do next

You must change this default password to better protect against security risks, such as the unauthorized access by others to the product that may prevent the product from functioning properly and/or lead to other undesirable consequences.

Caution

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

9.26 Manage Recording Server

You can add the Recording Server to the system for storing the videos and pictures. The supported Recording Servers include Hybrid Storage Area Network, Cloud Storage Server, pStor, and NVR (Network Video Recorder), etc. You can also form an N+1 hot spare system with several Hybrid Storage Area Networks to increase the video storage reliability of system.

Note

NVR can only be used to store pictures.

9.26.1 Add pStor

You can add a pStor server as a recording server to the HikCentral Professional for storing the videos and pictures.

Before You Start

- Make sure the pStor servers 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 HikCentral Professional via network.

Steps

1. On the top, select **Device**.
2. Select **Device and Server → Recording Server** on the left.
3. Click **Add** to enter the Add Recording Server page.

   Note

   If the NTP server is not configured, a prompt message will appear on the top of the page. You can click **Configure** to set the time synchronization.
4. Select **pStor**.
5. Enter the network parameters.

Address

The pStor 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 encoding device, data can be stored on the pStor automatically.

Control Port

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

Network Port

The network port No. of the pStor 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.

6. **Optional:** Check **ANR Function** or not.

Note

This function is enabled default. If the network is disconnected between the pStor and the encoding device, data can be stored on the pStor automatically.

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

Note

You can download these two keys on the pStor server's Web Client page.

8. **Optional:** Switch on **Enable Picture Storage** for storing pictures in this pStor.

Note

You should set picture downloading port No., which is used to download pictures via the Control Client.

9. **Optional:** 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.
10. Enter the name, user name, and password of the pStor 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.

11. **Optional:** In Storage Information field, switch on **Custom Video Copy-Back** and set the start time for copy-back.

12. Finish adding the server.
    - Click **Add** to add the server and back to the server list page.
    - Click **Add and Continue** to save the settings and continue to add other servers.
13. **Optional:** Perform the following operations after adding the server.

Edit Server	Click **Name** field of the server and you can edit the information of the server and view its storage and camera information.
Delete Server	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Configure Server	Click ⚙ in the Operation column to enter the login page of the pStor server. You can log in and configure the pStor server.
Search for Server	Enter keyword(s) in the search box in the top right corner to search for the target server(s).

9.26.2 Add Hybrid Storage Area Network

You can add the Hybrid Storage Area Network (hereafter simplified as Hybrid SAN) as a recording server to the HikCentral Professional for storing the video files and pictures.

Before You Start

Make sure the Hybrid SANs 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Recording Server** on the left panel.
3. Click **Add** to enter the Add Recording Server page.

Note

If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization.

4. Select **Hybrid Storage Area Network**.
5. Enter the network parameters.

Address

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

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.

6. **Optional:** Enable picture storage function for storing pictures in this Hybrid SAN.
   1) Switch on **Enable Picture Storage**.
   2) Set picture downloading port number for downloading pictures via the Control Client. If the picture downloading port No. is not changed, use the default value.
   3) Set signaling gateway port number. If the picture downloading port number is not changed, use the default one.
   4) Enter the access key and secret key.

Note

The access key and secret key are used to download pictures via the Control Client. If required, you can contact the technical support to get them.

7. **Optional:** Switch on **Enable WAN Access** to access the server via WAN.

Note

When enabled, you should set the corresponding parameters including IP address of the server, the control port No., the network port No., etc.

8. Enter the name, user name, and password of the 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.

9. **Optional:** In the Storage Information field, switch on **Custom Video Copy-Back** and set the start time and end time for copy-back.
10. Finish adding the server.
    - Click **Add** to add the server and go back to the server list page.
    - Click **Add and Continue** to save the settings and continue to add other servers.
11. **Optional:** Perform the following operations after adding the server.

Edit Server	Click the **Name** field of the server to edit the basic information, and storage information including video expiration and storage usage: • You can switch on **Video Expiration**, select a configuration mode (configure by server / storage pool), and set the corresponding video expiration day(s).

Note

- The oldest videos will be deleted automatically after the specified expiration day(s).
- If the added storage server supports configuring video expiration by camera, the current video expiration configuration is invalid; after **Video Expiration** is enabled, the previous configuration will be invalid and the expired data will be cleared according to the current one.

- You can view the used space and free space for each storage pool.

Delete Server	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Configure Server	Click in the Operation column, and the login interface of the Hybrid SAN displays. You can log in and configure the Hybrid SAN.
One-Touch Configuration	If the Hybrid SAN has not been configured with storage settings, click in the Operation column to perform one-touch configuration before you can store the video files of the camera on the Hybrid SAN.
Search for Server	Enter a key word in the search box in the top right corner, and click (or press the Enter key) to search for the target server(s).
N+1 Configuration	Click in the top left corner to enter to N+1 configuration page. See details in ***Set N+1 Hot Spare for Hybrid SAN*** .

9.26.3 Add Network Video Recorder

You can add an Network Video Recorder (NVR) as a recording server to HikCentral Professional for storing pictures.

Before You Start

Make sure the NVRs 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 system via network.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Recording Server** on the left panel.
3. Click **Add** to enter the adding server page.

Note

If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.

4. Select **Network Video Recorder** as the server type.
5. Set the required information.

Address

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

Control Port

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

Network Port

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

Picture Download Port

The picture downloading port No. of the NVR. If it not changed, use the default value.

Signaling Gateway Port

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

6. Enter the user's access key and secret key of the NVR for downloading pictures via Control Client.

Note

- You can download these two keys on the NVR's remote configuration page.
- When the NVR is used for center storage, it only supports picture storage.

7. **Optional:** If you need to access the server via WAN, set the **Enable WAN Access** switch to ON and set the corresponding parameters which are available when you access the server via WAN.
8. Enter the name, user name, and password of the NVR.

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.

9. Finish adding the NVR.
   - Click **Add** to add the NVR and back to the server list page.
   - Click **Add and Continue** to save the settings and continue to add other NVRs.
10. **Optional:** Perform the following operations after adding the NVR.

Edit NVR	Click the **Name** field of the NVR and you can edit the information of the NVR and view its storage and camera information.
Delete NVR	Select the NVR(s) from the list, and click **Delete** to remove the selected server(s).
Configure NVR	Click in the Operation column, and the login interface of the NVR will be displayed. You can log in and configure the NVR.

9.26.4 Manage Cloud Storage Server

You can add a Cloud Storage Server as a Recording Server to the HikCentral Professional for storing the video files.

Import Service Component Certificate to Cluster Storage Server

For data security purpose, the Cluster Storage Server's certificate should be same with the SYS server's. Before adding the Cluster Storage Server to the platform, you should import the certificate stored in the SYS server to the Cluster Storage Server.

Before You Start

Make sure the Cluster Storage Server 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 HikCentral Professional via network.

Steps

Note

If the service component certificate is updated, you should export the new certificate and import it to the Cluster Storage Server again to update.

1. In the top left corner of Home page, select → **Basic Management → System** .
2. Click **Security → Service Component Certificate** on the left side.
3. Click **Export** to export the certificate stored in the SYS server.
4. Log in the configuration page of the Cluster Storage Server via web browser.
5. Click **System → Configuration → Cluster Configuration** .
6. Input the root keys salt and keys component according to the parameters in the certificate you export in Step 3.



7. Click **Set**.

What to do next

After importing the certificate to the Cluster Storage Server, you can add the server to the platform for management. See ***Add Cluster Storage Server*** for details.

Add Cluster Storage Server

You can add Cluster Storage Server as a recording server to the HikCentral Professional for storing the video files and pictures.

Before You Start

- Make sure the Cluster Storage Servers 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 HikCentral Professional via network.
- You should import the service component certificate to the Cluster Storage Server first before adding it to the system. See for details.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Device and Server → Recording Server** on the left panel.
3. Click **Add** to enter the adding server page.

   Note

   If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.
4. Select **Cluster Storage**.
5. Enter the network parameters.

   Address

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

   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.

   Signaling Gateway Port

   The signaling gateway port No. of the server. If it is not changed, use the default value.
6. Enter the user's access key and secret key of the Cluster Storage Server for searching the video files stored in this server via the HikCentral Professional Mobile Client or downloading pictures via Control Client.

   Note

   You can download these two keys on the Cluster Storage Server's configuration page (click **Virtualizing → User Management**).
7. **Optional:** Switch on **Enable Picture Storage** for storing pictures in this Cluster Storage Server.

Note

If this function is enabled, you need to set picture downloading port No., which is used to download pictures via the Control Client.

8. **Optional:** 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.
9. Enter the name, user name, and password of the 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.

10. Finish adding the server.
    - Click **Add** to add the server and back to the server list page.
    - Click **Add and Continue** to save the settings and continue to add other servers.
11. **Optional:** Perform the following operations after adding the server.

Edit Server	Click **Name** field of the server and you can edit the information of the server and view its storage and camera information.
Delete Server	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Configure Server	Click ⚙ in the Operation column, and the login interface of the Cluster Storage Server displays. You can log in and configure the Cluster Storage Server.

9.26.5 Add pStor Cluster Service

pStor cluster service is a service that can manage multiple pStors and the connected disks of pStors. When there are multiple pStors storing a large number of video files, you can add pStor cluster service to the HikCentral Professional for managing pStors. It is also an efficient way to add multiple pStors.

Before You Start

Make sure the pStor cluster services 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Recording Server** on the left panel.
3. Click **Add** to enter the Add Recording Server page.

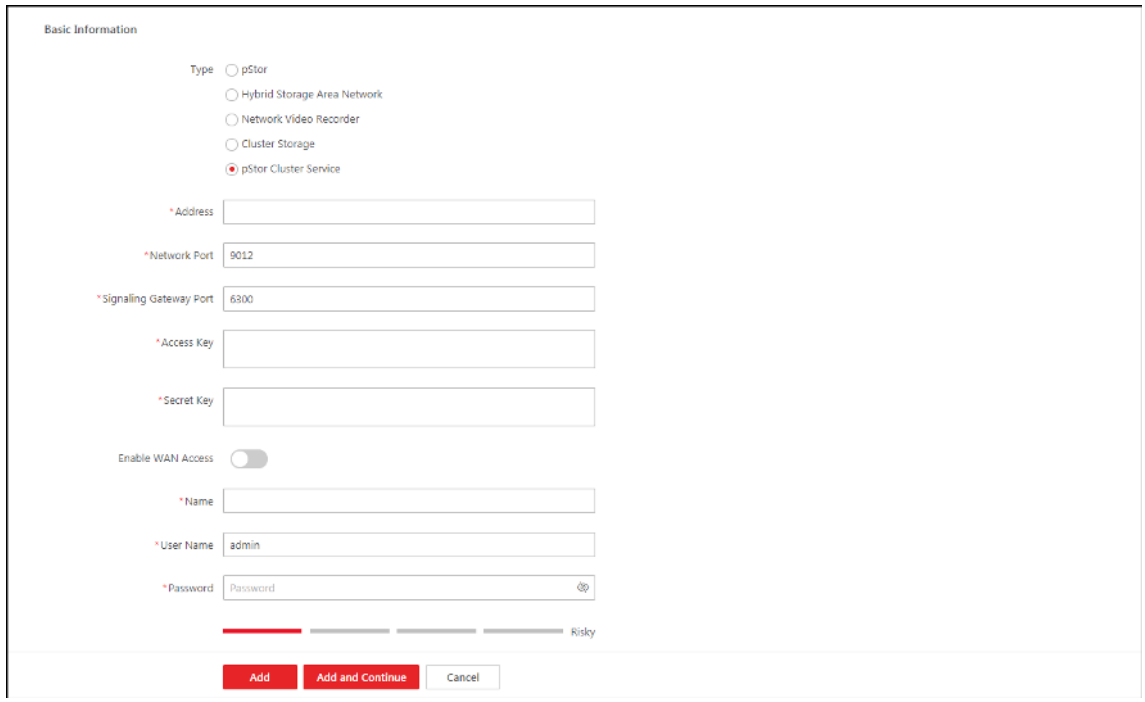


Figure 9-29 Add Recording Server Page

Note

If the NTP server is not configured, a prompt will appear on the top of the page. You can click **Configure** to set the time synchronization. See ***Set NTP*** for details.

4. Select **pStor Cluster Service**.
5. Enter the required network parameters.

   Address

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

   Network Port

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

   Signaling Gateway Port

   The signaling gateway port No. of the pStor cluster service. If it is not changed, use the default value.
6. Enter the user's access key and secret key of the pStor cluster service.

Note

You can download these two keys on the Web Client page (enter ***device's IP address: 9012*** in the browser) of pStor cluster service.

7. **Optional:** If you need to access the server via WAN, set the **Enable WAN Access** switch to on and set the corresponding parameters which are available when you access the server via WAN.
8. Enter the name, user name, and password of the pStor cluster service.

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.

9. Finish adding the server.
   - Click **Add** to add the server and back to the server list page.
   - Click **Add and Continue** to save the settings and continue to add other servers.
10. **Optional:** Perform the following operations after adding the server.

Edit Server	Click **Name** field of the server and you can edit the basic information of the server, view its connected device(s) storage information.
Delete Server	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Configure Server	Click ⚙ in the Operation column to enter the login interface of the pStor cluster service. You can log in and configure the pStor cluster service.
Search for Server	Enter keyword(s) in the search box in the top right corner to search for the target server(s).

9.26.6 Set N+1 Hot Spare for Hybrid SAN

You can form an N+1 hot spare system with several Recording Servers. The system consists of several host servers and a spare server. When the host server fails, the spare server switches into operation, and thus increasing the video storage reliability of HikCentral Professional.

Before You Start

- Make sure the Hybrid Storage Area Networks 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 HikCentral Professional via network.
- At least two online Hybrid Storage Area Networks should be added to form an N+1 hot spare system.

Steps

Note

- The N+1 hot spare function is only supported by Hybrid Storage Area Networks and NVRs. For details about configuring N+1 hot spare system with NVRs, see ***Set N+1 Hot Spare for NVR*** .
- The spare server cannot be selected for storing videos until it switches to host server.
- The host server cannot be set as a spare server and the spare server cannot be set as a host server.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Recording Server** → to enter the N+1 Configuration page.

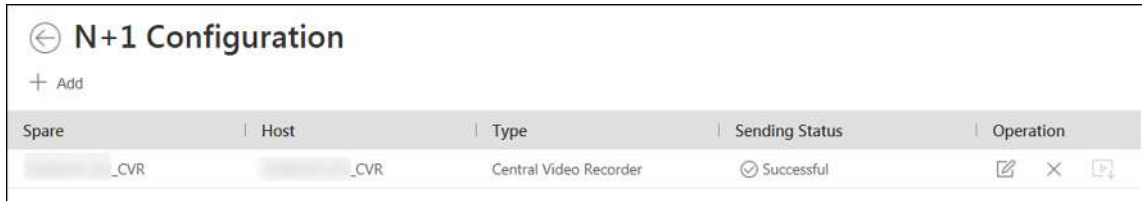


Figure 9-30 N+1 Configuration Page

3. Click **Add** to set the N+1 hot spare.
4. Select a Hybrid Storage Area Network in the Spare drop-down list to set it as the spare server.
5. Select the Hybrid Storage Area Network(s) in the Host field as the host server(s).
6. Click **Add**.

Note

The recording schedules configured on the Hybrid Storage Area Network will be deleted after setting it as the spare Recording Server.

7. **Optional:** After setting the hot spare, you can do one or more of the following.

Edit	Click on the Operation column, and you can edit the spare and host settings.
Delete	Click × on the Operation column to cancel the N+1 hot spare settings.

Note

Canceling the N+1 hot spare will cancel all the host-spare associations and clear the recording schedule on the spare server.

Send Recording Schedule	Click on the Operation column to send the recording schedule on the host server to the spare one again if the host server failed to send the recording schedule to spare server.

9.27 Manage Streaming Server

You can add the Streaming Server to the HikCentral Professional to get the video data stream from the Streaming Server, thus to lower the load of the device.

Note

For system which supports Remote Site Management, the cameras imported from Remote Site adopt the Streaming Server configured on the Remote Site by default. You are not required to add the Streaming Server to Central System and configure again.

9.27.1 Input Certificate Information to Streaming Server

For data security purpose, the Streaming Server's certificate should be the same with the SYS server's. Before adding the Streaming Server to the platform, you should enter the certificate information stored in the SYS server to the Streaming Server.

Steps

Note

If the service component certificate is updated, you should enter the new certificate information to the Streaming Server again to update.

1. Log into the Web Client on the SYS server locally.

   You will enter the Home page of the Web Client.
2. In the top left corner of Home page, select → **Basic Management** → **System** .
3. Click **Security** → **Service Component Certificate** on the left.
4. Click **Generate Again** to generate the security certificate for Streaming Server verification.

   Note

   You need to enter the account password for verification to generate the security certificate.
5. On the computer which has been installed with Streaming Service, open the Service Manager.
6. Click **Security Certificate**.

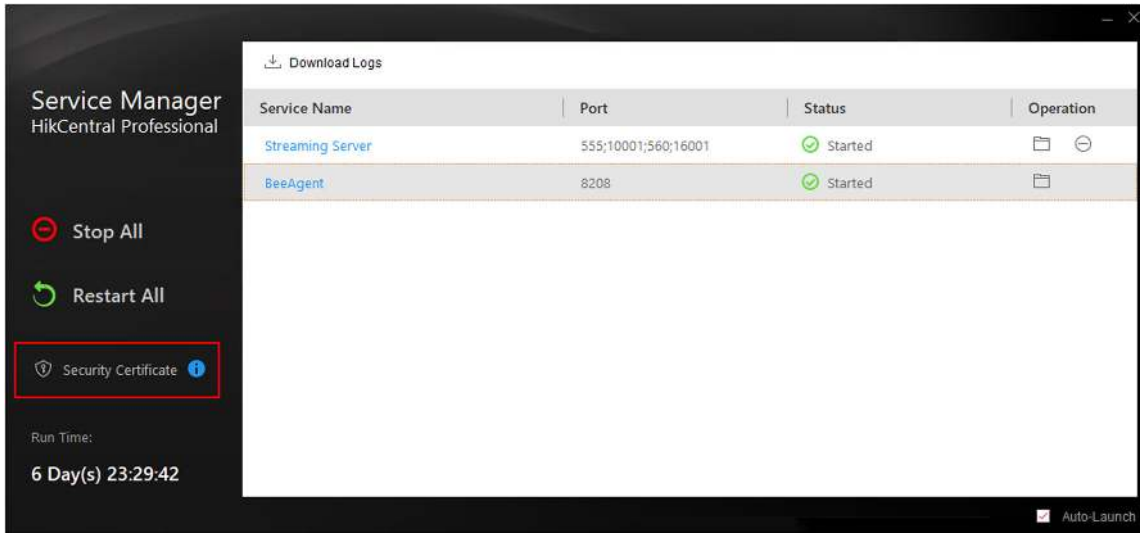


Figure 9-31 Enter Security Certificate

7. Enter the certificate information you generate in step 4.

9.27.2 Add Streaming Server

You can add a Streaming Server to the system to forward the video stream.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **Streaming Server** on the left panel.
3. Click **Add** to enter the Add Streaming Server page.
4. Enter the required information.

Name

Create a descriptive name for the server. For example, you can use an alias that can show the location or feature of the server.

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.

Real Time Streaming Port

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

Network Port

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

Web Client Streaming Port

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

Management Port (SSL)

It is used for security certificate authentication. If it is not changed, use the default value.

Web Client Streaming Port (SSL)

It is used for Web Client streaming. If it is not changed, use the default value.

RTMP Streaming Port

It is used for OpenAPI streaming. If it is not changed, use the default value.

HLS Streaming Port

It is used for OpenAPI streaming. If it is not changed, use the default value.

5. **Optional:** If you need to access the server via WAN, switch on **Enable WAN Access** and set the corresponding parameters (address, real-time streaming port, web client streaming port, ISUP streaming port (via plugin), ISUP Port for two-way audio, broadcasting port for ISUP device, web client streaming port (SSL), etc.) 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**.

6. You can switch on **Hot Spare** and set the hot spare type to Host or Spare.
7. Finish adding the Streaming Server.
   - Click **Add** to add the server and back to the server list page.
   - Click **Add and Continue** to save the server and continue to add other servers.

   The servers will be displayed on the server list. You can check the related information of the added servers on the list.
8. **Optional:** Perform the following operations after adding the streaming server.

Edit a Server	Click **Name** field of the server and you can edit the basic information of the server, view its related resources information.
Delete Server(s)	Select the server(s) from the list, and click **Delete** to remove the selected server(s).
Search Server(s)	Enter a keyword in the search box on the upper right corner of the page to quickly search the target server(s).

9.28 Add DeepinMind Server

When you know the related parameters such as IP address and port No. of the DeepinMind server, you can add it to the platform for intelligent functions, such as facial recognition, behavior analysis, and intrusion detection.

Before You Start

Make sure the DeepinMind server you are going to use is 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 HikCentral Professional via network.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Device and Server** → **DeepinMind Server** on the left.
3. Click **Add** to enter the Add DeepinMind Server page.
4. Set the required basic information such as device address, device port number, and WAN access.

   Address

   IP address of the DeepinMind server.

   Port No.

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

   Enable WAN Access

   Enable the DeepinMind 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 DeepinMind server for WAN access.
5. Enter the name, user name, and password of the DeepinMind 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.
6. Finish adding the DeepinMind server.
   - Click **Add** to finish adding the server.
   - Click **Add and Continue** to add the current server and continue to add more.
7. **Optional:** Perform the following operations after adding the server.

Edit Server	Click **Name** field of the server, and you can edit the information of the server.
Delete Server	Select the server(s) from the list, and click **Delete** to delete the selected server(s).
Configure Server	Click , and the login interface of the server displays. You can log in and configure the server.

Search Server(s) Enter a keyword in the search box on the upper right corner of the page to quickly search the target server(s).

9.29 Manage Scanning Device

Scanning devices are used for scanning barcodes, such as those on parcels. You can add scanning devices to the platform for management one by one or batch add scanning devices via a predefined template.

9.29.1 Add a Single Scanning Device

You can add a scanning device to the platform for management by specifying the IP address of the device.

Before You Start

Make sure the device you are going to add is 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 device to HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. On the left navigation pane, select **Device and Server** → **Scanning Device** .
3. Click **Add** to enter the device adding page.
4. Select an access protocol from the drop-down list.
5. Select **IP Address / Domain** as the adding mode.
6. Enter the information required for adding the scanning device.

   Device Address

   Enter the IP address of the device.

   Serial No.

   Enter the serial No. of the device.

   Note

   This field is displayed only if you select **Platform Integration Protocol** as the access protocol.

   Device Name

   Create a descriptive name for the device. For example, you can use an alias that can show the location or feature of the device.
7. **Optional:** Switch **Add Resource to Area** to on to add the resources of the device to an area.

Note

You can choose from creating a new area by the name of the device and selecting one from existing areas.

8. Click **Add** to finish adding the device or click **Add and Continue** to add another scanning device.
9. **Optional:** Perform the following operations.

Edit Device Information	Click the name of a device to enter its details page and edit its basic information.
Delete Device(s)	Select one or multiple devices and click **Delete** to delete the selected device(s).
Search for Devices	Enter a keyword in the search box to search for matching devices by device name. Supports fuzzy search.

9.29.2 Batch Add Scanning Devices

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

Before You Start

Make sure the devices you are going to add 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 HikCentral Professional via network.

Steps

1. On the top navigation bar, select → **Basic Management** → **Device** .
2. On the left navigation pane, select **Device and Server** → **Scanning Device** .
3. Click **Add** to enter the device adding page.
4. Select an access protocol from the drop-down list.
5. Select **Batch Import** as the adding mode.
6. Click **Download Template** to download the template to the local PC.

Note

The content in the template is predefined and will vary depending on the access protocol you select.

7. Open the predefined template file and enter the required information.
8. Click to select the edited template file.
9. Click **Add** to finish adding the devices listed in the template or click **Add and Continue** to add another batch of scanning devices.
10. **Optional:** Perform the following operations.

Edit Device Information	Click the name of a device to enter its details page and edit its basic information.

Delete Device(s)	Select one or multiple devices and click **Delete** to delete the selected device(s).
Search for Devices	Enter a keyword in the search box to search for matching devices by device name. Supports fuzzy search.

9.30 Manage Remote Site

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.

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.

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.

Central System

If the HikCentral Professional has RSM module (based on the License you purchased), you can add other Remote Sites to this system. This system and the added Remote Sites are called Central System.

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.

9.30.1 Add Remote Site by IP Address or Domain Name

If you know the IP address or domain name of the Remote Site to be added, you can add the site to the Central System by specifying the IP address (or domain name), user name, password, and other related parameters.

Steps

Note

- When adding Remote Site, the site's cameras and area information are imported to the Central System by default.
- When you perform the following steps, the progress of the whole task will be displayed on the upper right side.

1. On the top navigation bar, select → **Security Monitoring** → **Video** .

2. On the left pane, click **Remote Site Management**.
3. Enter the Add Remote Site page.
   - If no Remote Site is added, click **Add Site** to enter the Add Remote Site page.
   - If you have already added Remote Site, click + on the left to enter the Add Remote Site page.

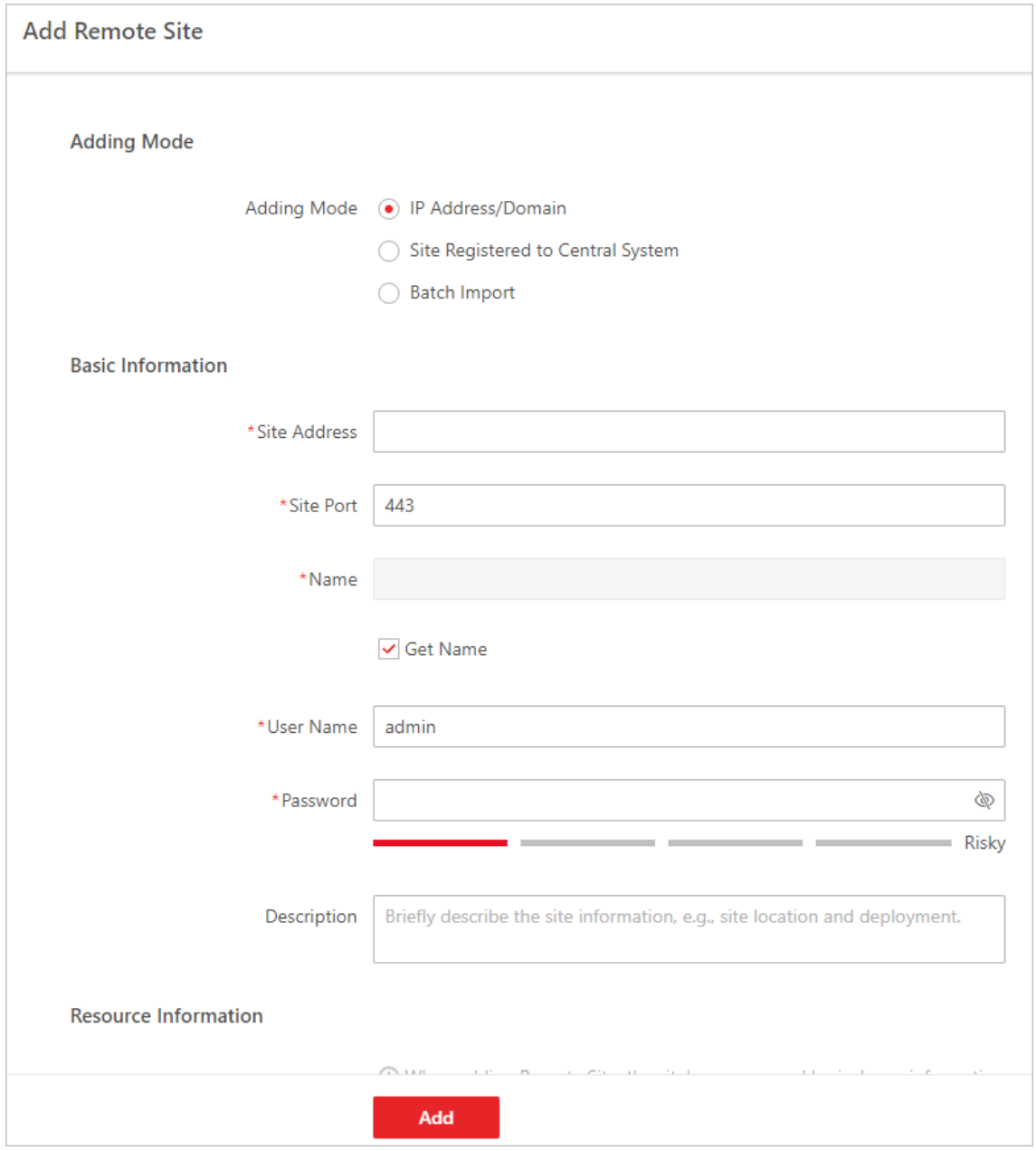


Figure 9-32 Add Remote Site

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.

4. Select **IP Address/Domain** as the adding mode.
5. Enter the required information.

Site Address

The IP address or domain name of the Remote Site.

Site Port

Enter the port No. of the Remote Site.

Name

Edit a name for the Remote Site as desired. You can check **Get Name** to synchronize the Remote Site's name automatically.

User Name

The user name for the Remote Site, such as admin user and normal user.

Password

The password required to access the Remote Site.

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.

Description

Optionally, you can enter the descriptive information for the Remote Site, such as location and deployment.

6. **Optional:** Enable receiving the alarms configured on the Remote Site.
   1) Switch on **Select Configured Alarms to Be Received by Central System** to display all the configured alarms on a Remote Site.
   2) **Optional:** Click to filter the configured alarms by the alarm source, area, triggering event, etc.
   3) Select the configured alarm(s).

Note

- 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.
- You can view and edit alarms in Event and Alarm module. For details about setting the event and alarm, refer to ***Event and Alarm*** .

7. Back up the Remote Sites' database in the Central System and you can set the maximum number of backups and view the database saving path in the Central System.
   Max. Number of Backups
   Define the maximum number of backup files available on the platform.
8. **Optional:** Enable backing up the Remote Site's database in schedule.
   1) Switch on **Scheduled Database Backup**.
   2) Select how often to back up the database.

   Note
   If you select **Weekly** or **Monthly** for running the backup task, select which day to run.

   3) Select what time of a day to start backup.
9. Click **Add** to add the remote site.

9.30.2 Add Remote Site Registered to Central System

If the Remote Sites have been registered to the Central System and the Central System also enabled the receiving site registration function, the registered Remote Sites will display in the site list. You can add them to the Central System by entering user names and passwords.

Before You Start

- The Remote Site must be registered to the Central System by entering the Central System's network parameters (see ***Set Network Parameters*** for details).
- Make sure the receiving site registration function has been enabled on the Central System. (see ***Set Network Parameters*** for details).

Perform this task when you need to add the site which has registered to the Central System.

Steps

Note

- When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.
- When you perform the following steps, the progress of the whole task will be displayed on the upper right side.

1. On the top navigation bar, select → **Security Monitoring** → **Video** .
2. On the left pane, click **Remote Site Management**.

3. Enter the Add Remote Site page.
   - If no Remote Site added, click **Add Site** to enter the Add Remote Site page.
   - If you have already added Remote Site, click + on the left to enter the Add Remote Site page.

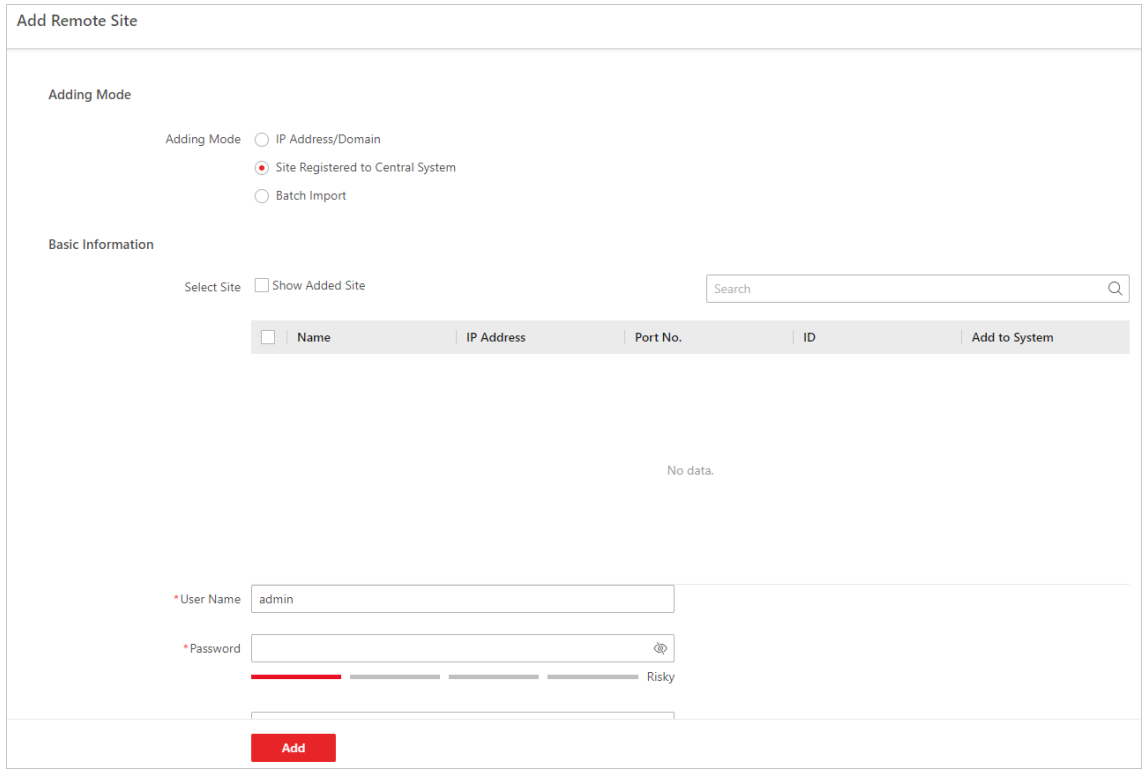


Figure 9-33 Add Remote Site Page

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.

4. Select **Site Registered to Central System** as the adding mode.

   The sites which have already registered to the Central System will display in the list.
5. Select the Remote Site(s) and enter the user name and password of the Remote Site(s).

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.

6. Back up the Remote Sites' database in the Central System and you can set the maximum number of backups and view the database saving path in the Central System.
   Max. Number of Backups
   Define the maximum number of backup files available on the system.

   Note
   The value of maximum number of backups ranges from 1 to 5.
7. **Optional:** Back up the Remote Site's database in schedule.
   1) Set the **Scheduled Database Backup** switch to **ON** to enable the scheduled backup.
   2) Select how often to back up the database.

      Note
      If you select **Weekly** or **Monthly** for running the backup task, select which day to run.
   3) Select what time of the day to start backup.
8. Click **Add** to add the Remote Site and go back to the Remote Site list page.

9.30.3 Add Remote Sites in a Batch

When you want to add multiple Remotes Sites at a time for convenience, you can edit the predefined template by entering the sites' parameters and import the template to the Central System to add them.

Steps

Note

- When adding Remote Site, the site's cameras and logical area information are imported to the Central System by default.
- When you perform the following steps, the progress of the whole task will be displayed on the upper right side.

1. On the top navigation bar, select → **Security Monitoring** → **Video** .
2. On the left pane, click **Remote Site Management**.
3. Enter the Add Remote Site page.
   - If no Remote Site added, click **Add Site** to enter the Add Remote Site page.
   - If you have already added Remote Site, click + on the left to enter the Add Remote Site page.

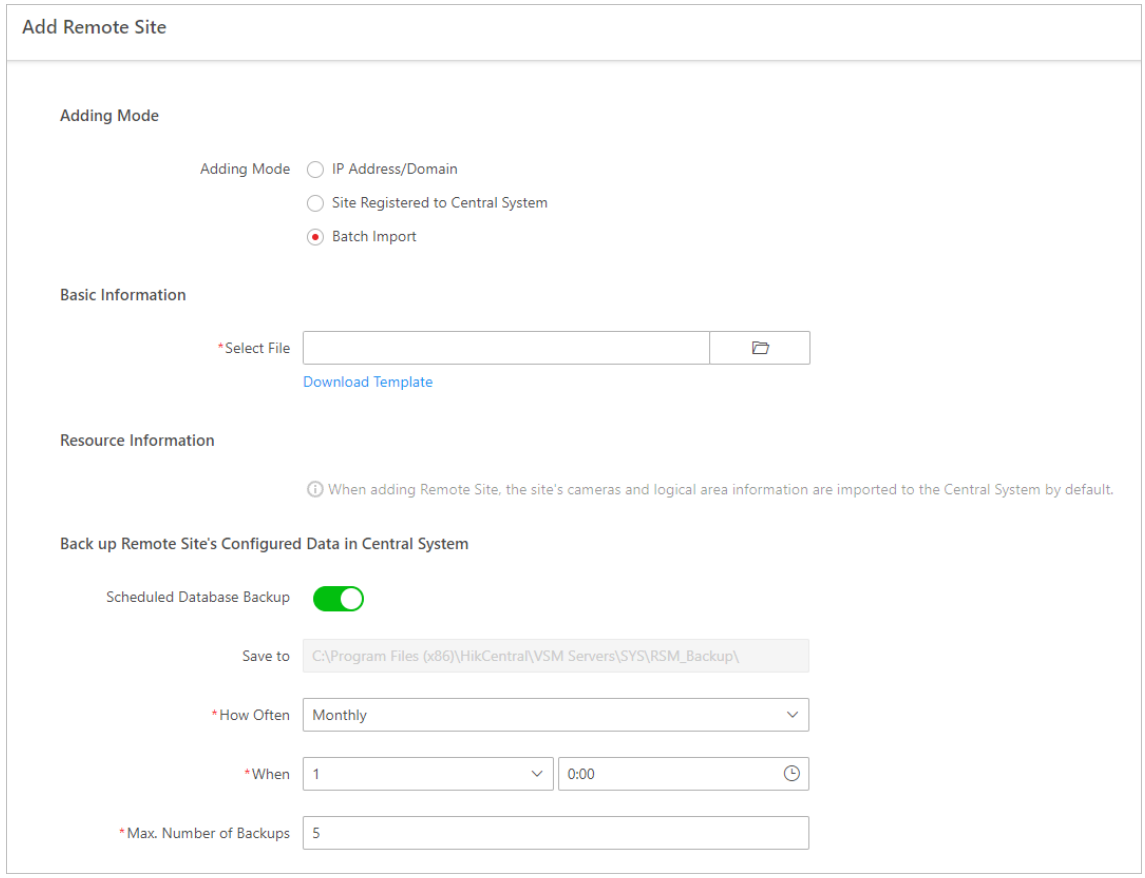


Figure 9-34 Add Remote Site

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.

4. Select **Batch Import** as the adding mode.
5. Click **Download Template** and save the predefined template on your PC.
6. Open the exported template file and input the required information of the Remote Sites to be added on the corresponding column.
7. Click and select the template file.
8. Back up the Remote Sites' database in the Central System and you can set the maximum number of backups and view the database saving path in the Central System.

   Max. Number of Backups

   Define the maximum number of backup files available on the system.
9. **Optional:** Back up the Remote Site's database in schedule.
   1) Set the **Scheduled Database Backup** switch to **ON** to enable the scheduled backup.
   2) Select how often to back up the database.

Note

If you select **Weekly** or **Monthly** for running the backup task, select which day to run.

3) Select what time of the day to start backup.

10. Click **Add** to add the Remote Site and go back to the Remote Site list page.

9.30.4 Back Up Remote Site's Database to Central System

After adding the Remote Site, you can back up the database of the Remote Site to the Central System. The database backup can be performed according to the configured schedule or immediately. In case of the data deletion or corruption following a natural or human-induced disaster, you can recover the data to ensure the business continuity.

Steps

1. On the top navigation bar, select → **Security Monitoring** → **Video** .
2. On the left pane, click **Remote Site Management**.
3. In the site list on the left, click the Remote Site name to view its details.

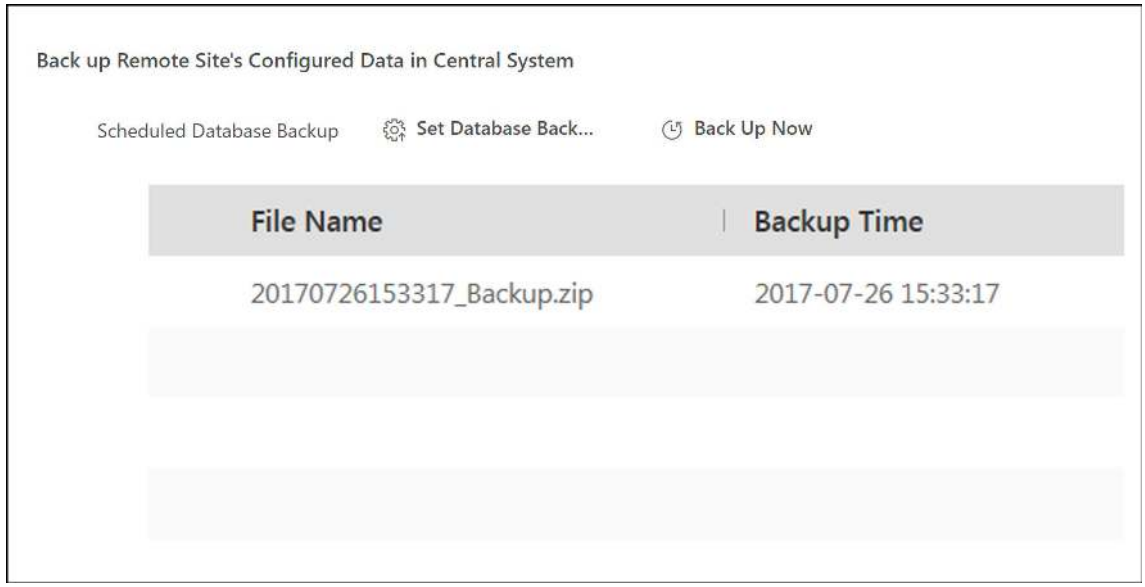


Figure 9-35 Back Up Remote Site Database in Central System

4. Click **Back Up Now** to back up the Remote Site's database manually.
5. **Optional:** Set the backup parameters and enable scheduled database backup if needed to back up the Remote Site's database regularly.
   1) Click **Set Database Backup** to open the Set Database Backup dialog.

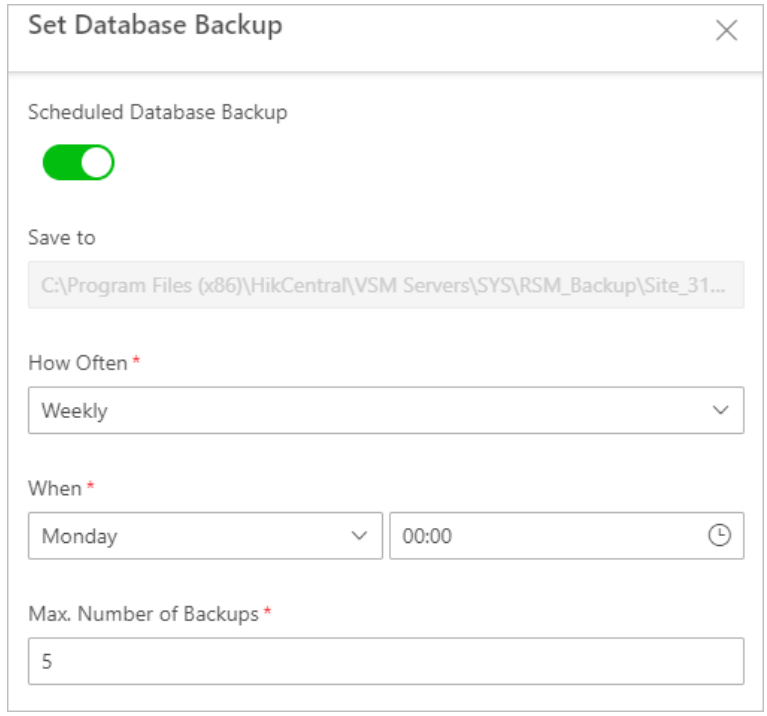


Figure 9-36 Set Database Backup

2) Switch on the **Scheduled Database Backup** to enable the scheduled backup.
3) Select how often to back up the database.

Note

If you select **Weekly** or **Monthly** for running the backup task, select which day to run.

4) Select what time of the day to start backup.
5) Set the **Max. Number of Backups** to define the maximum number of backup files available on the system.

Note

The maximum number of the backups should be between 1 to 5.

6) Click **Save**.

Result

The backup file (including manual backup and scheduled backup) will display in the list, showing the file name and backup time.

9.30.5 Edit Remote Site

After adding the Remote Site, you can view and edit the added Remote Site's information and set its GPS location.

Steps

1. On the top navigation bar, select → **Security Monitoring** → **Video** .
2. On the left pane, click **Remote Site Management**.
3. In the site list on the left, click the Remote Site name to view its details.
4. View and edit the basic information of the Remote Site, including IP address, port, alias, etc.

   Note

   You cannot edit the address and port of the site registered to the Central System.
5. In the original information field, view the Remote Site's site name, system ID, system version, and GPS location.

   Note

   If the GPS location is not configured, click **Configuration** to set its location in Map module. See ***Map Management*** for details.
6. **Optional:** Click **Configuration on Site** to open the Web Client of the Remote Site and log in for further configuration.

   Note

   The site must be online if you need to enter its Web Client.
7. Click **Save**.

9.30.6 View Remote Site's Changes

When there are changed resources on the Remote Site, such as newly added cameras, deleted cameras, and name changed cameras, you can view the changed resources and synchronize the resources in Central System with the Remote Site.

Steps

Note

The site should be online if you need to view the changed resources.

1. On the top navigation bar, select → **Security Monitoring** → **Video** .
2. On the left pane, click **Remote Site Management**.
3. Click in the site list on the left to get the latest status of the Remote Sites.
4. Click the site name whose resources are changed to enter its details page.
5. Click **Changes of Remote Site** to view the changes.

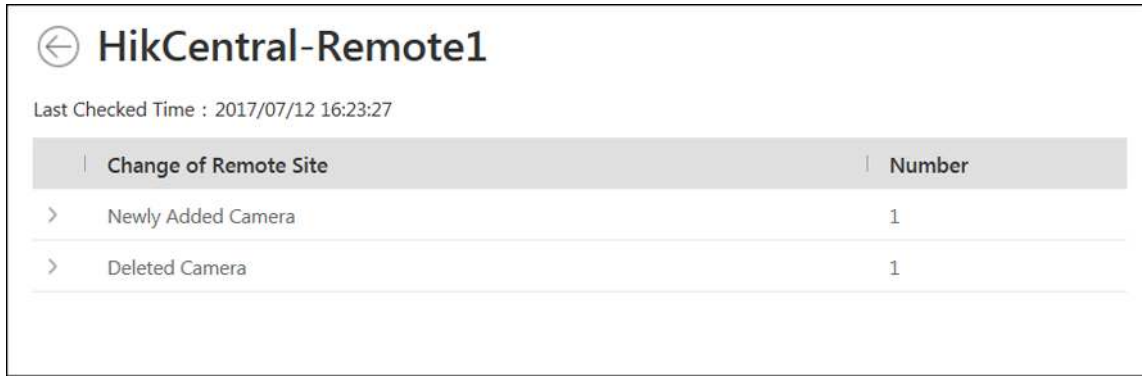


Figure 9-37 Remote Site Management

6. **Optional:** When there are newly added cameras on the site, you can view the added cameras and add them to the area in Central System.
   1) If there are some newly added cameras on Remote Site, click **Newly Added Camera** to expand the newly added camera list.

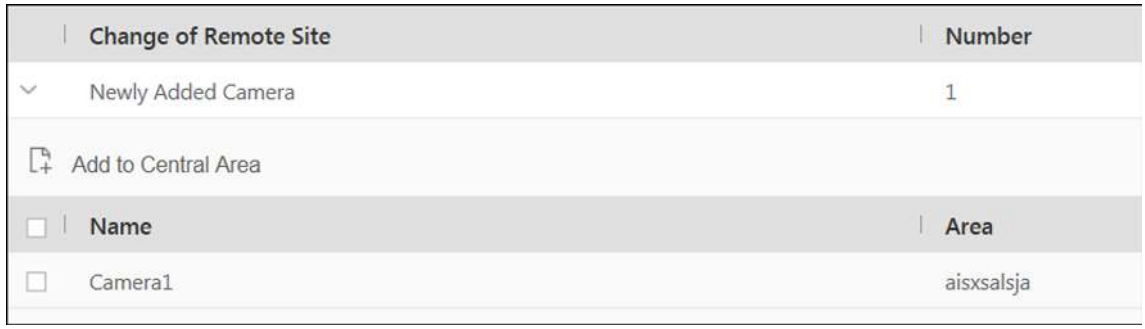


Figure 9-38 Changes of Remote Site

   You can view the camera name and area name on the Remote Site.
   2) Select the camera(s) and click **Add to Central Area** to synchronize the newly added cameras to the Central System.
   3) Select the area in the Central System.
   4) Click **Save**.
7. **Optional:** When there are some cameras deleted from the site, you can view the deleted cameras and remove them from Central System.
   1) If there are some cameras deleted from Remote Site, click **Deleted Camera** to expand the deleted camera list.

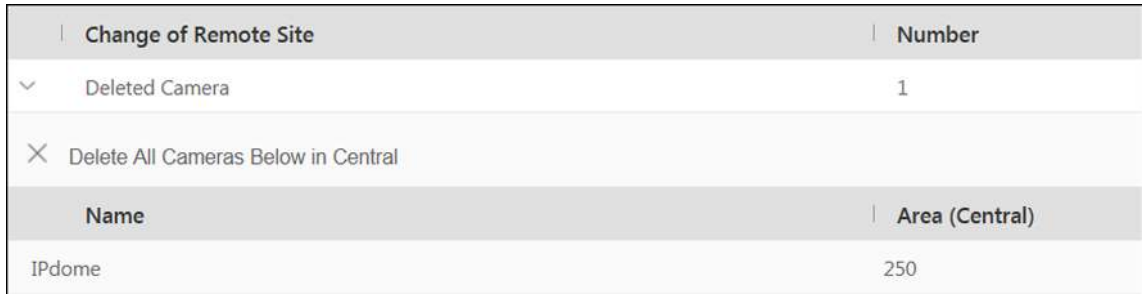


Figure 9-39 Change of Remote Site

You can view the camera name and its area in Central System.

2) Click **Delete All Cameras Below in Central** to delete the deleted cameras in Central System.

8. **Optional:** When there are some cameras whose names are changed on the site, you can view the name changed cameras and synchronize them to Central System.

1) If the name of camera of Remote Site is changed, click **Name Changed Camera** to expand the name changed camera list.

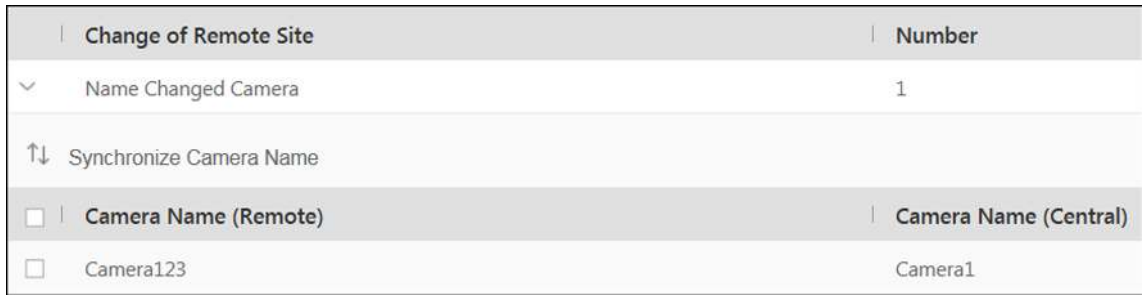


Figure 9-40 Name Changed Camera

You can view the camera names in Remote Site and Central System.

2) Select the cameras and click **Synchronize Camera Name** to synchronize the camera name in Central System.

Chapter 10 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. For example, on the 1st floor, there mounted 64 cameras, 16 access points, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one area (named 1st Floor) for convenient management. You can get the live view, play back the video files, 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.

10.1 Add Area

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

10.1.1 Add an Area for Current Site

You can add an area for the current site to manage the devices.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select the parent area in the area list panel to add a sub area.

   Note

   - For a Central System with a Remote Site Management module, you can select the current site from the drop-down site list to show its areas.
   - The icon indicates that the site is the current site.
5. Click + on the area list panel to open the Add Area panel.

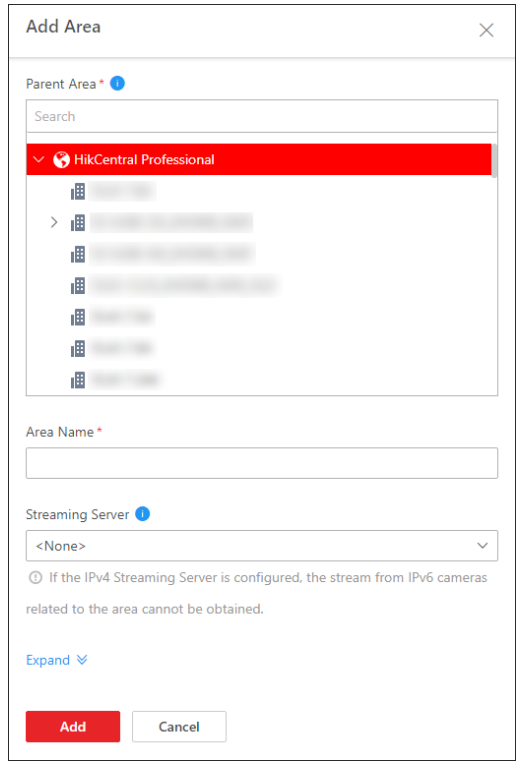


Figure 10-1 Add Area for Current Site

6. Select the parent area to add a sub area.
7. Create a name for the area.
8. **Optional:** Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server.

   All cameras belonging to this area via the server are listed in the Related Cameras area. If the camera is online, you can click its name to view its basic information, recording settings, and picture storage settings.
9. **Optional:** If you select a Streaming Server for the area, check **Wall Display via Streaming Server** to display the area's resources on the smart wall via this Streaming Server.
10. **Optional:** Click **Expand** to expand and set the additional area information as needed.

    Note

    For details about customizing fields of the additional area information, refer to ***Customize Additional Information*** .
11. Click **Add**.
12. **Optional:** After adding the area, you can do one or more of the following:

Edit Area	Hover the cursor on a specific area and click ··· → **Edit** to edit the area.
Delete Area	Select an area and click 🗑 or hover the cursor on an area 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.

Note

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.

Search Area	Enter a keyword in the search field of the area list panel to search for the area.
Move Area	Drag the added area to another parent area as the sub area.
Stick on Top	Hover the cursor on a specific area and click ··· → **Stick on Top** → to stick the area to the top.

Note

The order of the parent area will not be changed.

Remove from Top	Hover the cursor on a specific area and click ··· → **Remove from Top** to restore the area order to the default (name order).

10.1.2 Add Area for Remote Site

You can add an area for the remote site to manage the devices in the Central System.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select an added remote site from the drop-down site list to show its areas.

Note

The icon indicates that the site is a remote site.

4. Click + on the area list panel to open the Add Area panel.

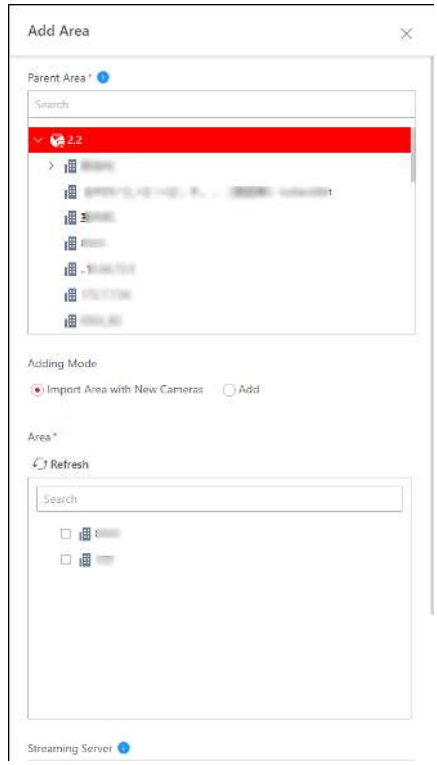


Figure 10-2 Add Area for Remote Site

5. Select a parent area to add a sub-area.
6. Set the adding mode for adding the area.

   Import Area with New Cameras

   If there are some cameras newly added to the areas on a remote site, you can import the areas as well as those newly added cameras. The areas with newly added cameras will be displayed and you can select the areas to add.

   Add

   Add a new area to the parent area.
7. **Optional:** Select a Streaming Server for the area to get the video stream of the cameras belonging to this area via the server.
8. **Optional:** If you select a Streaming Server for the area, check **Wall Display via Streaming Server** if you want to display the area's resources on the smart wall via this Streaming Server.
9. **Optional:** Click **Expand** to expand and set the additional area information as needed.

   Note

   For details about customizing the additional area information, refer to ***Customize Additional Information*** .
10. Click **Add**.
11. **Optional:** After adding the area, you can do one or more of the following:

Edit Area	Hover the cursor on a specific area and click ··· → **Edit** to edit the area.
Delete Area	Select an area and click 🗑 or hover the cursor on an area 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.
	Note After deleting the area, the cameras will be removed from the area, as well as the corresponding recording settings and event settings.
Search Area	Enter a keyword in the search field of the area list panel to search for the area.
Move Area	Drag the added area to another parent area as the sub area.
Stick on Top	Hover the cursor on a specific area and click ··· → **Stick on Top** → to stick the area to the top.
	Note The order of the parent area will not be changed.
Remove from Top	Hover the cursor on a specific area and click ··· → **Remove from Top** to restore the area order to the default (name order).

10.1.3 Customize Additional Information

You can customize the area information which is not included in the basic information according to actual needs, e.g., description. After customizing, you can enter the additional area information to make the area information complete when adding or editing an area.

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

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.

You can also click ✎ to edit the additional information or click 🗑 to delete it.

10.2 Add Element to Area

You can add elements to areas for management, including cameras, doors, elevators, vehicles, security radars, alarm inputs, alarm outputs, Under Vehicle Surveillance Systems (UVSSs), digital signage terminals, and interactive flat panels.

10.2.1 Add Camera to Area for Current Site

You can add cameras to areas for the current site to get the live view, play the video files, and so on.

Before You Start

The cameras need to be added to HikCentral Professional for area management. Refer to ***Manage Encoding Device*** for details.

Steps

Note

One camera can only belong to one area. You cannot add a camera to multiple areas.

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding cameras to.
5. Select the **Camera** tab.
6. Click + on the element page to enter the Add Camera page.
7. Select the device type.
8. Select the camera(s) to be added.
9. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
10. **Optional:** 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.

    Note

    If the recording schedule configured on the device is not continuous recording, it will be changed to event recording on the local device.
11. Click **Add**.

    The added camera(s) will be displayed in the list.
12. **Optional:** After adding the camera(s), you can do one or more of the followings:

Configure Camera	Click in the Operation column to configure the camera.
Export Information of All Cameras	Click to export the information of all cameras added to the area to an Excel file.

Synchronize Camera Name	Select the cameras and click ↑↓ to get the cameras' names from the devices in a batch. **Note** You can only synchronize the camera name of the online HIKVISION device.
Apply Camera Name	Select the cameras and click to apply the cameras' names to the devices in a batch.
Get Recording Schedule	Select the cameras and click to get the recording schedules from the devices in a batch.
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 is 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.
Move Camera(s) to Another Area	Select the cameras, click , select a target area, and click **Move** to move the selected cameras to the target area.
Set Geographic Location	Click to enter the Map Settings page and drag the camera to the map. For details, refer to ***Add Hot Spot on Map*** .
Display Cameras of Sub Areas	Check **Include Sub-Area** to display the cameras of sub areas.
Filter Cameras by Device Type	Select the device type(s) to be displayed in the list from the drop-down list to the left of the search box.
Mark Camera	Select the cameras, click and check **Two-Way Audio Supported** to mark the cameras which support two-way audio.

10.2.2 Add Camera to Area for Remote Site

If the current system is a Central System with a Remote Site Management module, you can also add cameras from the Remote Site to areas in the Central System for management.

Before You Start

Encoding devices need to be added to HikCentral Professional for area management. Refer to ***Manage Encoding Device*** for details about adding devices.

Steps

Note

Cameras can only belong to one area. You cannot add a camera to multiple areas.

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added Remote Site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is a Remote Site.
4. **Optional:** Select an area for adding cameras to in the area list panel.
5. Select the **Camera** tab.
6. Click + on the element page to enter the Add Camera page.

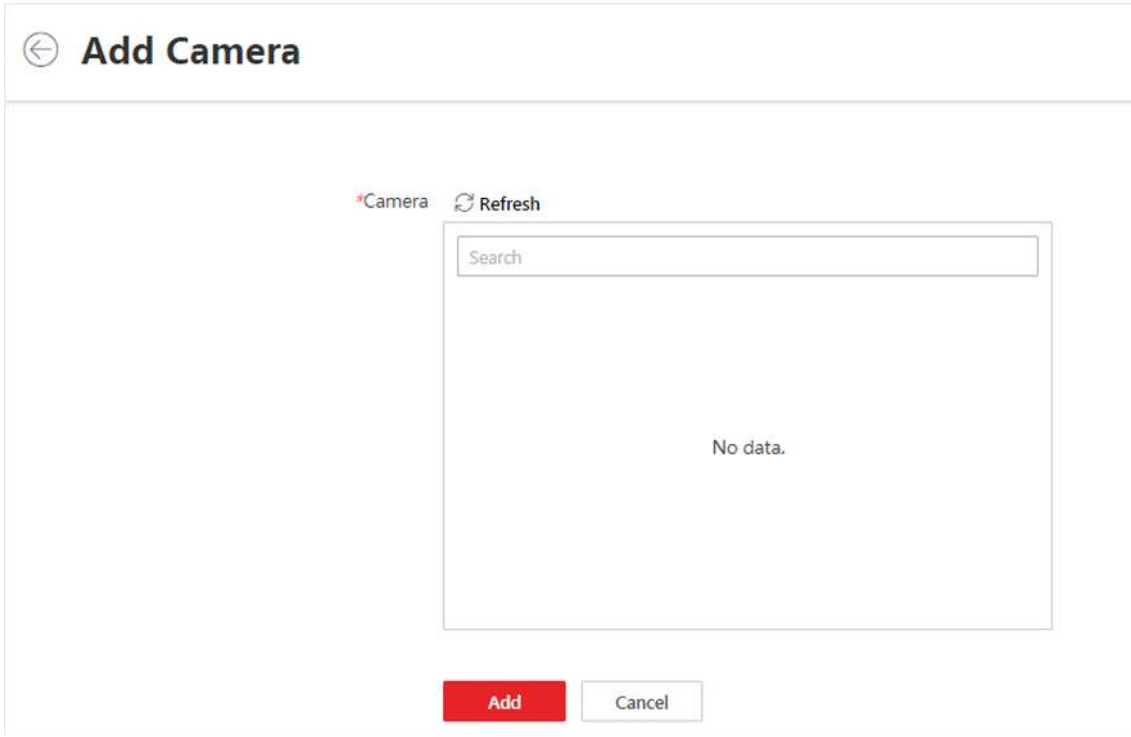


Figure 10-3 Add Camera to Area for Remote Site

7. Select the camera(s) to be added.

   Note

   Up to 64 cameras can be added to one area.
8. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.

   The added camera(s) will be displayed in the list.

10. **Optional:** After adding the camera(s), you can do one or more of the followings:

Export Information of All Cameras	Click to export the information of all cameras added to the area to an Excel file.
Synchronize Camera Name	Select the cameras and click to get the cameras' names from the devices in a batch.
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.
Move Camera(s) to Another Area	Select the cameras, click , select a target area, and click **Move** to move the selected cameras to the target area.
Display Cameras of Sub Areas	Check **Include Sub-Area** to display the cameras of sub areas.
Filter Cameras by Device Type	Select the device type(s) to be displayed in the list from the drop-down list to the left of the search box.
Mark Camera	Select the cameras, click and check **Two-Way Audio Supported** to mark the cameras which support two-way audio.

10.2.3 Add Door to Area for Current Site

You can add doors to areas for the current site for management.

Before You Start

The access control devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Access Control Device*** for details.

Steps

Note

One door can only belong to one area. You cannot add one door to multiple areas.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding doors to the area list panel.
5. Select the **Door** tab.
6. Click + on the element page to enter the Add Door page.
7. Select the device type.
8. Select the door(s) to be added.
9. **Optional:** Select the area.

   Note

   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
10. Click **Add**.

    The added door(s) will be displayed in the list.
11. **Optional:** After adding the doors, you can do one or more of the following.

Synchronize Door Name	Select the doors and click ↑↓ to synchronize the doors' names from the device in a batch. **Note** You can only synchronize the door name of online HIKVISION device.
Apply Door Name	Select the doors and click to apply the doors' names to the device in a batch.
Move to Other Area	Select the doors and click . Then select the target area to move the selected doors to and click **Move**.
Set Geographic Location	Click to enter Map Settings page and drag the door to the map. See ***Add Hot Spot on Map*** for details.
Display Doors of Sub Areas	Check **Include Sub-area** to display the doors in sub areas.
Filter by Device Type	Click and check the device type in the drop-down list to filter the doors.

Search for Doors	Enter the keywords in the Search field to search for doors.

10.2.4 Add Elevator to Area for Current Site

You should add elevator to areas for further management.

Before You Start
The elevator control devices need to be added to the HikCentral Professional for area management. Refer to ***Manage Elevator Control Device*** for details.

Steps

Note
One elevator can only belong to one area. You cannot add an elevator to multiple areas.

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note
   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding elevators to in the area list panel.
5. Select the **Elevator** tab.
6. Click + to enter the Add Elevator page.
7. In the **Elevator Control Device** field, all the added elevator control devices are displayed. Select the device to add the elevator to.
8. 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.

   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.
9. **Optional:** Select the area.

   Note
   - You can click **Add** in the Area field to add new areas.
   - If you have not selected area in previous step, selecting area in this step will be required.
10. Click **Add**.
11. **Optional:** After adding the elevator, you can do one or more of the followings.

Get Floor Name	Select the elevator and click ↑↓ to get the floors' names of the elevator from the device in a batch.
Apply Floor Name	Select the elevator and click to apply the elevator's floors names to the device in a batch.

Move to Other Area	Select the elevators and click . Then select the target area to move the selected elevators to and click **Move**.
Set Geographic Location	Click to enter the Map Settings page and drag the elevator to the map. See ***Add Hot Spot on Map*** for details.
Display Elevators of Sub Areas	Check **Include Sub-Area** to display the elevators of sub areas.
Search for Elevators	Enter the keywords in the Search field to search for elevators.

10.2.5 Add Vehicle to Area for Current Site

You can add vehicles to areas for the current site for management. Only vehicles linked with on-board devices can be added to areas and one vehicle can only be added to one area.

Before You Start

The on-board devices need to be added to HikCentral Professional for area management. Refer to ***Manage On-Board Devices*** for details.

Steps

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding vehicles to in the area list panel.
5. Select the **Vehicle** tab.
6. Click **Add** on the element page to enter the Add Vehicle page.

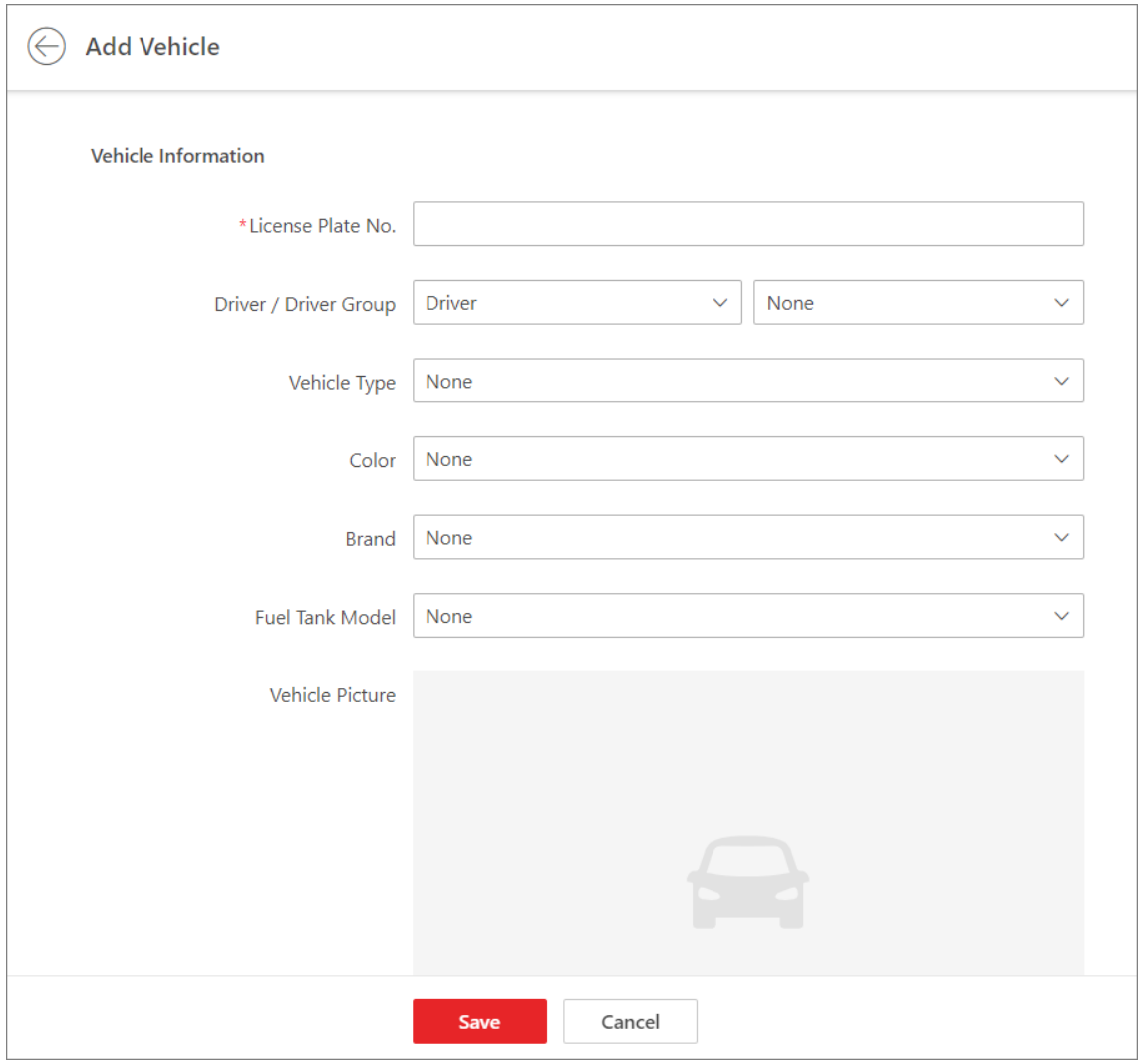


Figure 10-4 Add Vehicle to Area

7. Set the vehicle information, including the license plate No., driver / driver group, vehicle type, color, brand, fuel tank model, and vehicle picture.
8. Select the on-board device linked with the vehicle from the Linkage Device drop-down list.
9. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

10. Click **Save**.

    The added vehicle will be displayed in the list.
11. **Optional:** After adding the vehicle(s), you can do one or more of the followings:

Delete Vehicle	Select the vehicle(s) and click **Delete**.

Set Speed Threshold	Select the vehicle(s), click **Speed Threshold Settings**, and drag the slider or enter an integer in the text field.
Move to Other Area	Select the vehicle(s) and click **Move to Other Area**. Then select the target area to move the selected vehicle(s) to and click **Move**.
Display Vehicles of Sub Areas	Check **Include Sub-Area** to display the vehicles in sub areas.
Remotely Configure Linkage Device	Click in the Operation column of a vehicle to go to the remote configuration page of the on-board device. **Note** This function is supported when the transfer protocol between the Web Client and the SYS server is HTTPS.
Search for Vehicles	Enter the keywords in the Search field to search for vehicles.

10.2.6 Add Security Radar to Area for Current Site

You can add security radars to different areas of the current site according to their locations, so that you will be informed when an alarm/event is triggered if you have configured an alarm/event.

Before You Start

The devices need to be added to the HikCentral Professional for area management. Refer to ***Device and Server Management*** for details.

Steps

Note

You cannot add a security radar to multiple areas.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site in the drop-down site list to show its areas.

   Note

   The icon indicates that the site is current site.
4. **Optional:** Select an area for adding security radars to.
5. Select the **Security Radar** tab.
6. Click + .
7. Select a security radar in the **Security Radar** field.
8. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.

   The added security radar will be displayed in the list.

10. **Optional:** After adding the security radars, you can do one or more of the followings:

Arm/Disarm Security Radar	Select the security radar(s) and click / to arm/disarm the selected security radar(s). **Note** An event will be triggered if any person or object enters an armed security radar's detection area.
Move to Other Area	Select the security radars and click . Then select the target area to move the selected security radars to and click **Move**.
Add Security Radar to Map	Click to enter the Map Settings page and drag the security radar to the map. See ***Add Hot Spot on Map*** for details.
Display Security Radars of Sub Areas	Check **Include Sub-Area** to display the security radars of sub areas.
Search for Security Radars	Enter the keywords in the Search field to search for security radars.

10.2.7 Add Alarm Input to Area for Current Site

You can add alarm inputs to areas for the current site for management.

Before You Start

The devices need to be added to the HikCentral Professional for area management. Refer to ***Device and Server Management*** for details.

Steps

Note

One alarm input can only belong to one area. You cannot add an alarm input to multiple areas.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.

4. **Optional:** Select an area for adding alarm inputs to.
5. Select the **Alarm Input** tab.
6. Click + to enter the Add Alarm Input page.
7. Select the device type.
8. Select the alarm inputs to add.

Note

For the security control device, you need to select its zones as alarm inputs to add to the area.

9. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

10. Click **Add**.
11. **Optional:** After adding the alarm inputs, you can do one or more of the followings.

Delete Alarm Input	Select the alarm input(s) and click **Delete**.
Move to Other Area	Select the alarm input(s) and click . Then select the target area to move the selected alarm inputs to and click **Move**.
Add Alarm Input to Map	Click to enter Map Settings page and drag the alarm input to the map. See ***Add Hot Spot on Map*** for details.
Display Alarm Inputs of Sub Areas	Check **Include Sub-Area** to display the alarm inputs of sub areas.
Filter Alarm Inputs by Device Type	Select the device type(s) to be displayed in the list from the drop-down list to the left of the search box.
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.

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.
Search for Alarm Inputs	Enter the keywords in the Search field to search for alarm inputs.

10.2.8 Add Alarm Output to Area for Current Site

You can add alarm outputs to areas for the current site for management. 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.

Before You Start

The devices need to be added to the HikCentral Professional for area management. Refer to ***Device and Server Management*** for details.

Steps

Note

One alarm output can only belong to one area. You cannot add an alarm output to multiple areas.

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is the current site.
4. **Optional:** Select an area for adding alarm outputs to.
5. Select the **Alarm Output** tab.
6. Click + to enter the Add Alarm Output page.
7. Select the device type.
8. Select the alarm outputs to add.
9. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

10. Click **Add**.
11. **Optional:** After adding the alarm outputs, you can do one or more of the followings.

Delete Alarm Output	Select the alarm output(s) and click **Delete**.
Move to Other Area	Select the alarm outputs and click . Then select the target area to move the selected alarm outputs to and click **Move**.
Set Geographic Location	Click **Set Geographic Location** to enter the Map Settings page and drag the alarm output to the map. See ***Add Hot Spot on Map*** for details.
Display Alarm Outputs of Sub Areas	Check **Include Sub-Area** to display the alarm outputs of sub areas.
Search for Alarm Outputs	Enter the keywords in the Search field to search for alarm outputs.

10.2.9 Add UVSS to Area for Current Site

You can add Under Vehicle Surveillance Systems (UVSSs) to areas for the current site for management.

Before You Start

The UVSS devices need to be added to the HikCentral Professional for area management. Refer to ***Add Under Vehicle Surveillance System*** for details.

Steps

Note

One UVSS can only belong to one area. You cannot add a UVSS to multiple areas.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area for adding UVSSs to.
5. Select the **UVSS** tab.
6. Click + to enter the Add UVSS page.
7. Select the UVSSs to add.
8. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.
10. **Optional:** After adding the UVSSs, you can do one or more of the followings.

Delete UVSS	Select the UVSSs and click **Delete**.
Move to Other Area	Select the UVSSs and click . Then select the target area to move the selected UVSSs to and click **Move**.
Set Geographic Location	Click **Set Geographic Location** to enter the Map Settings page and drag the UVSS to the map. See ***Add Hot Spot on Map*** for details.
Display UVSSs of Sub Areas	Check **Include Sub-Area** to display the UVSSs of sub areas.
Search for UVSSs	Enter the keywords in the Search field to search for UVSSs.

10.2.10 Add Digital Signage Screen to Area for Current Site

You can add digital signage screens to areas for the current site for management.

Before You Start

The digital signage screens need to be added to HikCentral Professional for area management. Refer to ***Manage Digital Signage Terminals*** for details.

Steps

Note

One digital signage screen can only belong to one area. You cannot add one digital signage screen to multiple areas.

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area for adding digital signage screens to.
5. Click **Digital Signage Screen** tab.
6. Click **Add** to enter the Add Digital Signage Screen page.
7. Select the digital signage screens to add them.
8. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.
10. **Optional:** After adding the digital signage screens, you can do one or more of the followings:

Delete Digital Signage Screen(s)	Select the digital signage screen(s) in the list and click **Delete**.
Move to Other Area	Select the digital signage screens and click **Move to Other Area**. Then select the target area to move the selected digital signage screens to and click **Move**.
Display Digital Signage Screens of Sub Areas	Check **Include Sub-Area** to display the digital signage screens of sub areas.
Search for Digital Signage Screens	Enter the keywords in the Search field to search for digital signage screens.

10.2.11 Add Interactive Flat Panel to Area for Current Site

You can add interactive flat panels to areas for convenient management.

Before You Start

- Make sure you have switched to the Interactive Flat Panel mode. See details in ***Switch Application Mode*** .
- The interactive flat panels need to be added to the HikCentral Professional for area management. Refer to ***Manage Interactive Flat Panel*** for details.

Steps

Note

One interactive flat panel can only be added to one area.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Select **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area from the area list on the left side.
5. Select the **Interactive Flat Panel** tab.
6. Click **Add** to enter the Add Interactive Flat Panel page.

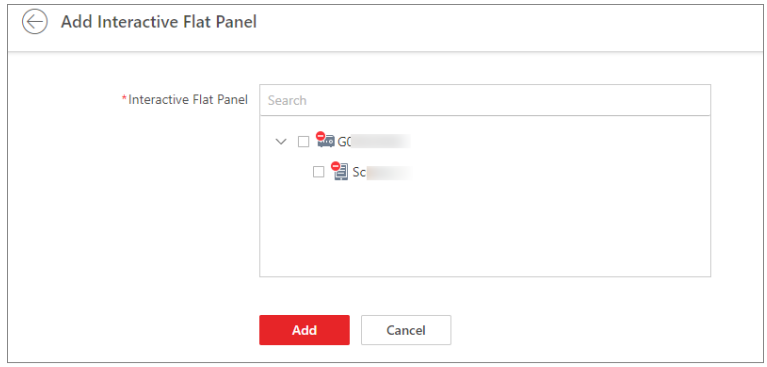


Figure 10-5 Add Interactive Flat Panel

7. Select interactive flat panel(s) to be added.
8. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.
10. **Optional:** After adding the interactive flat panels, perform the following operations.

Delete	Select the interactive flat panel(s), and then click **Delete** to delete the selected interactive flat panel(s) from this area.
Search	Enter keywords in the upper right corner to search for the target interactive flat panel(s).
Edit Name	Click the name of a interactive flat panel to edit its name.

10.2.12 Add Speaker Unit to Area for Current Site

You can add speaker units to areas for the current site for management.

Before You Start

The speaker units need to be added to HikCentral Professional for area management. Refer to ***Group Speaker Units*** for details.

Steps

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area for adding speaker units to.

5. Select the **Speaker Unit** tab.
6. Click **Add** on the element page to enter the Add Speaker Unit page.

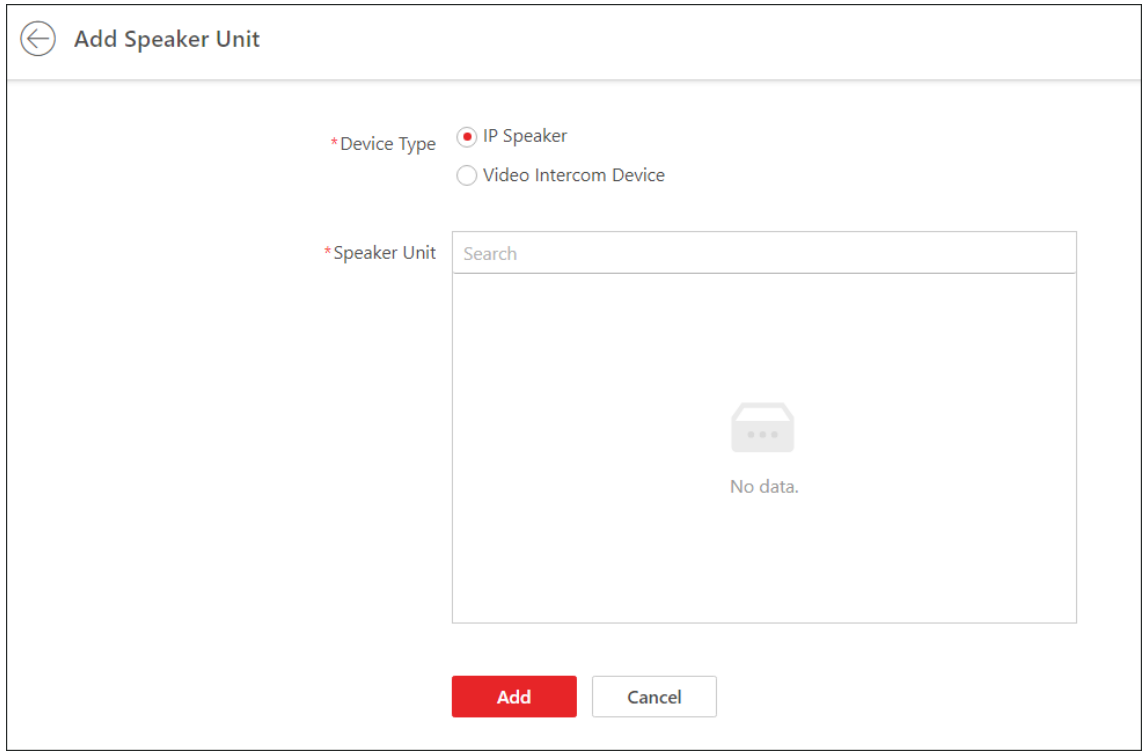


Figure 10-6 Add Speaker Unit

7. Select the device type.
8. Select the speaker unit(s) to be added.
9. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

10. Click **Add**.

    The added speaker unit(s) will be displayed in the list.
11. **Optional:** After adding speaker unit(s), you can do one or more of the followings:

Move to Other Area	Select the speaker unit(s) and click **Move to Other Area**. Then select the target area to move the selected speaker unit(s) to and click **Move**.
Adjust Volume	Select speaker unit(s) and click **Volume** to adjust the alarm volume and/or volume.
Set Geographic Location	Click **Set Geographic Location** to enter the Map Settings page. You can search for the speaker unit(s) to be added to the map and drag

	the speaker unit to the map. For details, refer to ***Add Hot Spot on Map*** .
Display Speaker Unit of Sub Areas	Check **Include Sub-Area** to display the speaker units in sub areas.
Search Speaker Units	Enter the name of speaker unit(s) and click to search for the speaker unit(s).
Delete Speaker Unit	Select the speaker unit(s) and click **Delete** to delete the speaker unit(s).

10.2.13 Add Fire Detector to Area for Current Site

You can add fire detectors to areas for the current site for management.

Before You Start

The fire protection devices need to be added to HikCentral Professional for area management. Refer to ***Manage Fire Protection Device*** for details.

Steps

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area for adding fire detectors to.
5. Select the **Fire Detector** tab.
6. Click **Add** on the element page to enter the Add Fire Detector page.
7. Select the fire detector(s) to be added.
8. **Optional:** Select the area.

Note

- You can click **Add** in the Area field to add new areas.
- If you have not selected area in previous step, selecting area in this step will be required.

9. Click **Add**.

   The added fire detector(s) will be displayed in the list.
10. **Optional:** Perform the following operations.

Remote Configurations	Click in the operation column to configure the device remotely.

	Note For details about remote configuration, see the user manual of the device.
Move to Other Area	Select the fire detector(s) and click **Move to Other Area**. Then select the target area to move the selected fire detector(s) to and click **Move**.
Set Geographic Location	Click **Set Geographic Location** to enter the Map Settings page. You can search for the fire detector(s) to be added to the map and drag the fire detectors to the map. For details, refer to ***Add Hot Spot on Map*** .
Display Fire Detector of Sub Areas	Check **Include Sub-Area** to display the fire detectors in sub areas.
Search Fire Detectors	Enter the name of fire detector(s) and click to search for the fire detector(s).
Delete Fire Detector	Select the fire detector(s) and click **Delete** to delete the fire detector(s).

10.3 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.

10.3.1 Edit Camera for Current Site

You can edit the basic information, recording settings, and picture storage settings of a camera for the current site.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

   Note

   The icon indicates that the site is current site.
4. **Optional:** Select an area.
5. Select the **Camera** tab to show the added cameras.
6. Click a camera's name in the **Name** column to enter the camera editing page.
7. Edit the camera's basic information, including camera name and protocol type.

Note

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

8. **Optional:** Click **Live View** to view the live view of the camera and click again to switch to playback.

Note

- If the device supports PTRZ, you can long press / to rotate by clockwise/anticlockwise during live view.
- You can click to set rotating speed, and click to refresh the live view.

9. Edit the recording settings of the camera. See ***Configure Storage and Recording*** for details.

Note

- If no recording settings have been configured for the camera, you can click **Configure** to set the parameters.
- You can also select multiple cameras and click **Get Device's Recording Settings** in the added cameras list page to get recording schedules of the devices in a batch.

10. **Optional:** Enable **Water Level Device**, and then enter the address of the telemetry station.
11. **Optional:** Set the **Picture Storage** switch to ON and select the storage location from the drop-down list for storing the pictures uploaded from the camera to the specified location.

Note

- Refer to ***Configure Storage for Uploaded Pictures*** for details.
- For cameras added by ISUP protocol, this function is not available. You should click **Configure** to edit the picture storage configurations.

12. **Optional:** Click **Configuration on Device** in the top right corner of the camera editing panel or click in the **Operation** column of the added camera list page to set the remote configurations of the corresponding device if needed.

Note

For details about the remote configuration, refer to the user manual of the device.

13. **Optional:** In the top right corner of the camera editing panel, click **Copy To** to select configuration item(s) and copy the settings of this camera to other cameras.
14. Click **Save**.

10.3.2 Edit Door for Current Site

You can edit the basic information, related cameras, picture storage settings, card reader settings, and face recognition terminal settings of a door on the current site.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .

2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas and select one area.

Note

The icon indicates that the site is current site.

4. Select the **Door** tab to show the added doors in this area.
5. Click a door's name in the **Name** column to enter the door editing page.
6. Edit the door's 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 the door is unlocked and locked 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.

7. 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.

8. **Optional:** Switch on **Picture Storage** and select a storage location from the drop-down list.

Note

For details, refer to ***Configure Storage for Uploaded Pictures*** . If an error occurs during picture storage configuration, ⓘ appears on the right of the door name.

9. **Optional:** On the Card Reader panel, switch on **Card Reader 1** or **Card Reader 2** and set the card reader related parameters.

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.

Note

The parameters displayed vary according to the different models of the access control devices. For details about the parameters, refer to the user manual of the device.

10. **Optional:** 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.
    1) Click **Add** to enter the Add Face Recognition Terminal page.
    2) Select **IP Address**, **Online Devices**, or **Device ID** as the adding mode, and set the required parameters, which may vary according to different terminals.
    3) Click **Add** to link the terminal to the turnstile or access controller.
    4) **Optional:** Click ⚙ in the Operation column to configure parameters for the terminal. For details, refer to ***Configure Other Parameters*** .

    Electrostatic Discharge Testing Settings

    Electrostatic Discharge Testing

    When enabled, electrostatic discharge testing is required.

    Communication Timeout Threshold with Turnstile

    Configure the communication timeout threshold between the turnstile and the electrostatic discharge detector. If the detection time exceeds the threshold, the related event will be uploaded to the platform.
11. **Optional:** Click **Copy To** in the upper right corner to apply the current settings of the door to other door(s).
12. Click **Save**.

10.3.3 Edit Elevator for Current Site

You can edit basic information, floor information, related cameras, card reader settings of the elevator on current site.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .

2. Click **Area** on the left.
3. In the left panel, select the current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area.
5. Select the **Elevator** tab to show the added elevators in this area.
6. Click an elevator's name in the **Name** column to enter the elevator editing page.
7. Edit the elevator's basic information.

Name

Edit the name for the elevator.

Note

If you changes the name, you can click in the elevator list page to apply the new name to the device.

Open Duration

The time interval between the elevator door is open and closed again.

Extended Open Duration

The time interval between the elevator door is open and closed again for the person whose extended access function is enabled.

Elevator Door Open Timeout Alarm

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

Max. Open Duration

The time interval between the elevator door is unlocked and locked again if the person has enabled Extended Access function.

Duress Code

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

8. In the Floor panel, all the imported floors will be displayed in the list. You can edit the floor's name or reset the imported floor No.

Edit Floor Name

You can edit the floor name if needed.

Note

If you changes the name, you can click **Apply Floor Name** in the elevator list page to apply the new name to the device.

Reset Imported Floor No.

You can click **Reset Imported Floor No.** and enter the range of the floor No. to reset the settings of the floors, such as schedule settings, name, access level settings, etc.

9. Relate cameras (such as the cameras mounted inside the elevator) to the elevator, and you can view its live view, recorded video, captured pictures via the Control Client.

Note

- Up to two cameras can be related to one elevator.
- You can select the door and click ↑ or ↓ to adjust the displaying priority of its auto capture.
- You can switch on **Auto Capture** to realize the function of capturing automatically.

10. In the Card Reader panel, switch on **Card Reader 1** or **Card Reader 2** and set the card reader related parameters.

Min. Card Swipe Interval

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

Reset Entry on Keypad after

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 enabled, if the door has 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 enabled, if the door has 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.

Buzzer Polarity

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

Fingerprint Security Level

Select the fingerprint security level. The higher is the security level, the lower is the face acceptance rate (FAR). The higher is the security level, the higher is the false rejection rate (FRR).

Note

The parameters displayed vary according to the model of the access control device. For details about the parameters, refer to the user manual of the device.

11. **Optional:** Click **Copy to** in the upper right corner to apply the current settings of the elevator to other elevator(s).
12. Click **Save**.

10.3.4 Edit Vehicle for Current Site

After adding vehicles to areas of the current site, you can edit the basic vehicle information (e.g., license plate No., driver / driver group, vehicle type, color, brand, fuel tank model, and vehicle picture) for the current site as needed.

Steps

1. In the top left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the area list panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area.
5. Select the **Vehicle** tab to show the added vehicles.
6. Click a vehicle's license plate number in the License Plate No. column.
7. Edit the vehicle information (e.g., license plate No., driver / driver group, vehicle type, color, brand, fuel tank model, vehicle picture).
8. Click **Save**.

10.3.5 Edit Security Radar for Current Site

After adding a security radar to an area of the current site, you can edit the security radar's name, view the drawn zones or trigger lines, and view the related calibrated cameras.

Steps

1. In the top left corner of the Home page, select → **Basic Management** → **Device** .

2. Click **Area** on the left.
3. In the area list panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area.
5. Select the **Security Radar** tab to show the added security radars.
6. Click a security radar's name in the **Name** column to enter the security radar editing page.
7. Edit the security radar's name.
8. **Optional:** In the **Zone** field, view the drawn zones of the security radar.

Note

If there is no zone drawn for the security radar, you should go to the Map Settings module to draw. Refer to ***Draw Zone or Trigger Line for Radar*** for details.

9. **Optional:** In the **Relate Calibrated Camera** field, view the calibrated cameras related to the security radar.

Note

If there is no calibrated camera related to the security radar, you should go to the Map Settings module to configure. Refer to ***Relate Calibrated Camera to Radar*** for details.

10. Click **Save** to save the settings for the security radar.

10.3.6 Edit Alarm Input for Current Site

You can edit the basic information of alarm input and relate detector to the security control panel's alarm input for current site.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the area list panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area.
5. Select the **Alarm Input** tab to show the added alarm inputs.
6. Click an alarm input name in the **Name** column to enter the Edit Alarm Input page.
7. Edit the alarm input name.
8. **Optional:** For the alarm input of security control panel, set the **Related Detector** switch to ON to configure related detector for the alarm input.

1) Click **Add** to add a detector.
2) Enter the detector name.
3) Click to save the detector type.

Note

- Only the alarm input of a security control panel supports this function. Make sure you have added a security control device to the system, and have added its zone to area as an alarm input. See ***Add Alarm Input to Area for Current Site*** for details.
- On Map Settings page, the detectors related to the alarm input of a security control panel will be displayed in the resource list of alarm input on the right panel. When selecting the alarm input and dragging it to the map, the related detectors will also be added to the map, and the relations among them will be marked with lines. If you only drag the alarm input to the map without selecting it, the related detectors will not be added to the map.
- You cannot edit the detector type here. If you want to edit it, go to the Remote Configuration page of security control panel, and click **Input Settings → Zone** .

9. Click **Save**.

10.3.7 Edit Alarm Output for Current Site

You can edit the alarm output name for current site.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area.
5. Select the **Alarm Output** tab to show the added alarm outputs.
6. Click an alarm output name in the **Name** column.
7. Edit the alarm output name in the pop-up window.
8. Click **Save**.

10.3.8 Edit UVSS for Current Site

You can edit name of the Under Vehicle Surveillance System (UVSS) and relate cameras to the UVSS for current site.

Steps

1. In the top left corner of Home page, select → **Basic Management → Device** .
2. Click **Area** on the left.

3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area.
5. Select the **UVSS** tab to show the added UVSSs.
6. Click an UVSS name in the **Name** column.
7. Edit the name of UVSS.
8. **Optional:** Relate cameras to the UVSS.
   1) Set the **Relate Camera** switch to ON.
   2) Select the camera(s).
9. Click **Save**.

10.3.9 Edit Digital Signage Screen for Current Site

You can edit the name of a digital signage screen for the current site.

Steps

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area.
5. Select the **Digital Signage Screen** tab to show the added digital signage screens.
6. Click a digital signage screen's name in the **Name** column.
7. Edit the name in the pop-up window.
8. Click **Save**.

10.3.10 Edit Interactive Flat Panel for Current Site

You can edit the name of a interactive flat panel for the current site.

Before You Start

Make sure you are in the Interactive Flat Panel mode. See details in ***Switch Application Mode*** .

Steps

1. In the top-left corner of the Client, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is the current site.

4. **Optional:** Select an area.
5. Select the **Interactive Flat Panel** tab to show the added interactive flat panels.
6. Click a interactive flat panel's name in the **Name** column.
7. Edit the name in the pop-up window.
8. Click **Save**.

10.3.11 Edit Speaker Unit for Current Site

You can edit basic information, related cameras settings of the speaker unit on current site.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area.
5. Select the **Speaker Unit** tab to show the added speaker unit(s) in this area.
6. Click speaker unit's name in the Name column to enter the speaker unit editing page.
7. Edit the name for the speaker unit.
8. **Optional:** Relate camera(s) to the broadcast.
   - Up to 4 related cameras are allowed.
   - Click ↑ or ↓ to adjust the displaying sequence of the cameras.
9. Click **Save**.

10.3.12 Edit Third-Party Integrated Resource for Current Site

After integrating the resources on third-party system to the HikCentral Professional via Optimus, the third-party resources are added to the areas.

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. Optional: Select an area.
5. Select the **Third-Party Integrated Resource** tab to show the added third-party resources.
6. Click the name of third-party resource to enter the details page.

7. You can view the basic information of the resource, such as name, device type, and manufacturer.
8. You can also add the resource on the map so that when an event/alarm is triggered on the resource, you can view the notification and details on the map.

Note

- For details about locating resource on map, refer to ***Add Hot Spot on Map*** .
- The **Third-Party Integrated Resource** tab is available only when the **Integrate via Optiums** switch in System Configuration module is set to ON. For details, refer to ***Set Third-Party Integration*** .

10.3.13 Edit Fire Detector for Current Site

You can edit the basic information of the fire detector on current site.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area.
5. Select the **Fire Detector** tab to show the added fire detector(s) in this area.
6. Click fire detector's name in the **Name** column to enter the fire detector editing page.
7. Edit the name for the fire detector.
8. Click **Save**.

10.3.14 Edit Element for Remote Site

If the current system is a Central System with a Remote Site Management module, you can edit the cameras added from the Remote Site.

Steps

1. In the top-left corner of the Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the leftt panel, select the added Remote Site from the drop-down site list to show its areas.

Note

The icon indicates that the site is a Remote Site.

4. **Optional:** Select an area to show its cameras.
5. Click a camera's name in the Name column to enter the camera editing page.

6. Edit the camera's basic information, including camera name and protocol type.

Note

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

7. **Optional:** Click **Live View** to 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 ***System Security Settings*** .

8. Edit the recording settings of the camera.

Note

For recording settings, if no recording settings have been configured for the camera, click **Configuration on Site** to set the parameters (for details, refer to ***Configure Recording for Cameras on Remote Site***).

9. **Optional:** Click **Configuration on Device** in the top-right corner of the camera editing panel or click in the **Operation** column of the added camera list page to set the remote configurations of the corresponding device if needed.

Note

For details about the remote configuration, refer to the user manual of the device.

10. **Optional:** Click **Copy to** to copy the current camera's specified configuration parameters to other cameras of the Remote Site.
11. Click **Save**.

10.4 Remove Element from Area

You can remove the added cameras, doors, elevators, vehicles, security radars, alarm inputs, alarm outputs, Under Vehicle Surveillance Systems (UVSSs), digital signage screens, interactive flat panels, speaker units, and fire detectors from the area.

10.4.1 Remove Element from Area for Current Site

You can remove the added cameras, doors, elevators, security radars, alarm inputs, alarm outputs, UVSSs, digital signage terminals, interactive flat panels, speaker units, and fire detectors from the area for current site.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.

3. In the left panel, select the added current site from the drop-down site list to show its areas.

Note

The icon indicates that the site is current site.

4. **Optional:** Select an area in the area list panel to show its added elements.
5. Select the **Camera**, **Door**, **Elevator**, **Vehicle**, **Security Radar**, **Alarm Input**, **Alarm Output**, **UVSS**, **Digital Signage Screen Speaker Unit** or **Fire Detector** tab to show the added elements.
6. Select the elements.
7. Click to remove the elements from the area for current site.

10.4.2 Remove Element from Area for Remote Site

If the current system is a Central System with a Remote Site Management module, you can remove the added cameras from its area.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **Device** .
2. Click **Area** on the left.
3. In the left panel, select the added Remote Site from the drop-down site list to show its areas.

Note

The icon indicates that the site is a Remote Site.

4. **Optional:** Select an area to show its added cameras.
5. Select the cameras.
6. Click to remove the cameras from the area for remote site.
7. **Optional:** 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 11 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 comparison (adding a person to a face comparison group), time and attendance (assign a schedule to a person), etc. After adding the persons, you can edit and delete the person information if needed.

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

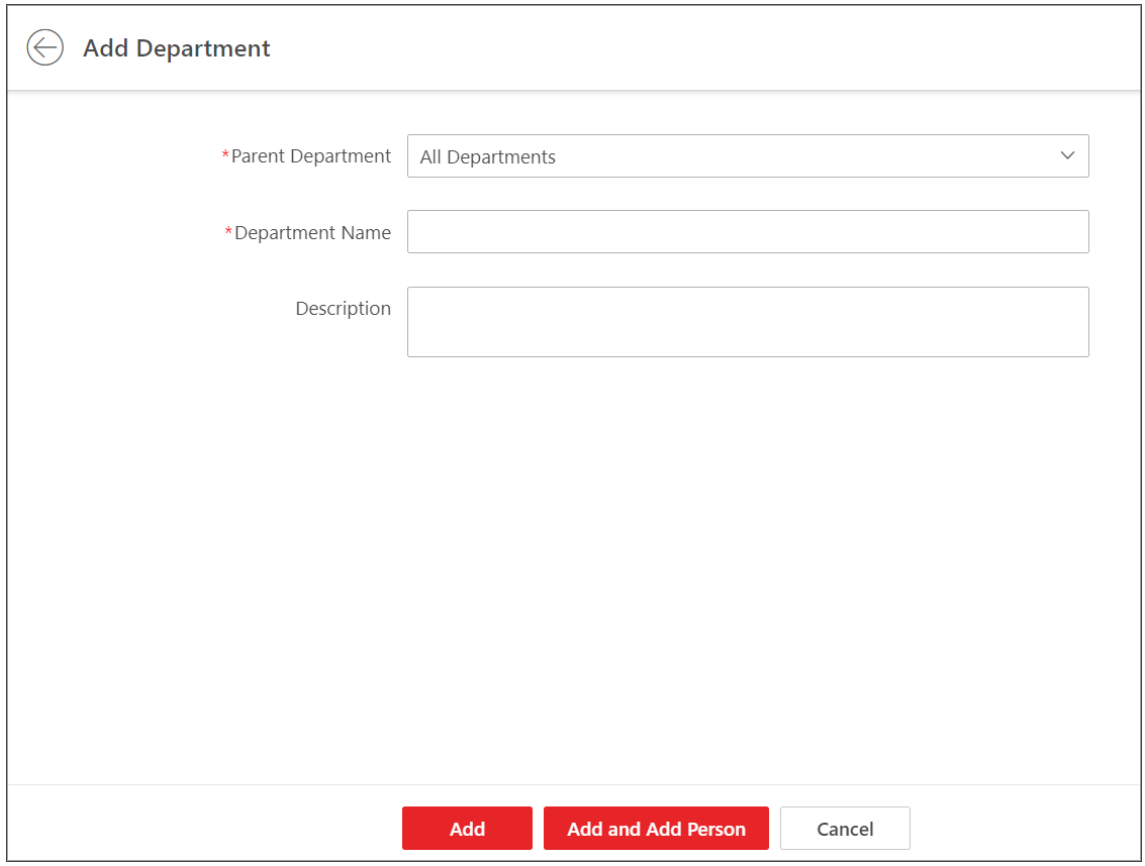


Figure 11-1 Add Department

5. 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.
6. **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*** .

   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.

7. **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 group, group name, or remarks.
Delete a Department	Select a department and click at the top of the department list to delete the selected one.
	Note The root department cannot be deleted.
Delete All Departments	Click beside at the top of the department list to delete all added departments.

11.2 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 access control devices / video intercom devices / enrollment stations. In addition, you can batch add profile pictures for persons, and import domain persons.

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 ***Set Person ID Rule*** .

You can perform the following operations for adding persons.

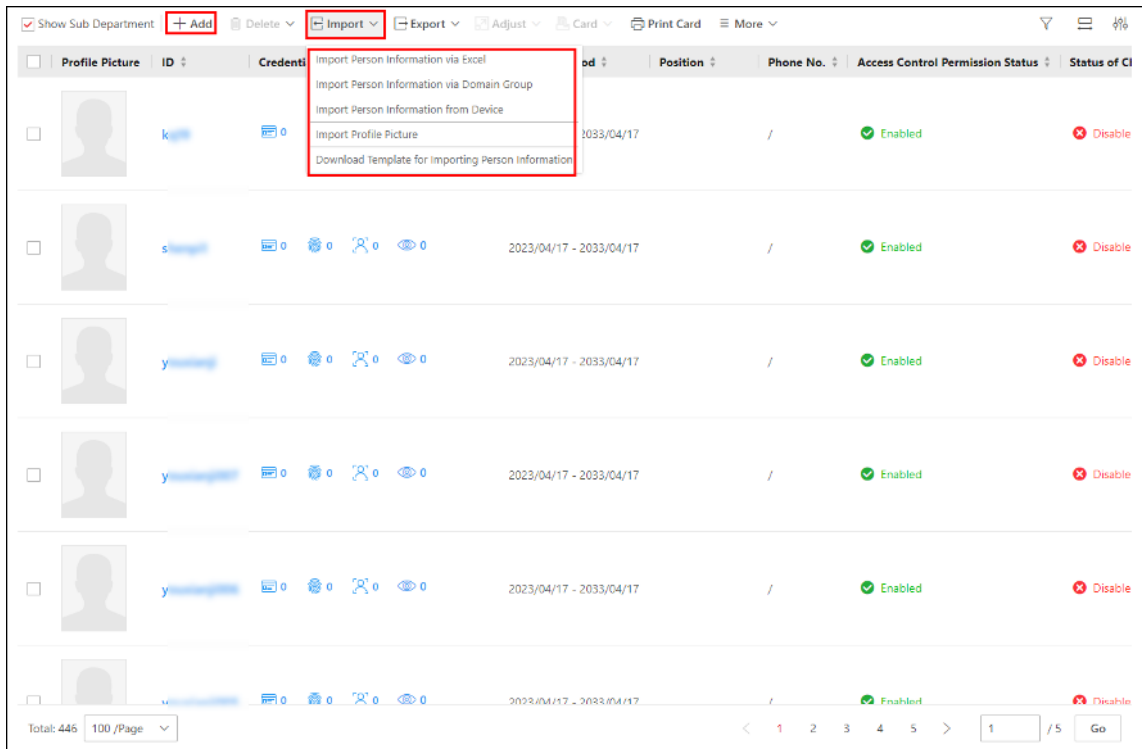


Figure 11-2 Introduction to Adding Persons

1. You can click + to add a single person. For details, refer to ***Add a Single Person*** .
2. You can click to perform the following operations.
   - Batch import persons by template. For details, refer to ***Batch Add Persons by Template***
   - Import users in the AD (Active Directory) domain to the platform as persons. For details, refer to ***Import Domain Persons*** .
   - Import person pictures. For details, refer to ***Import Profile Pictures*** .
   - Import persons information to the platform from devices, including access control devices, video intercom devices, or enrollment station. For details, refer to ***Import Persons from Access Control Devices or Video Intercom Devices*** or ***Import Persons from Enrollment Station*** .
3. 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.

11.2.1 Add a Single Person

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.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. Select a department from the department list on the left.

   All persons in the selected department will be displayed on the right. You can check **Show Sub Department** to display the persons in sub departments (if any).
4. Click + at the top of person list to enter the Add Person page.

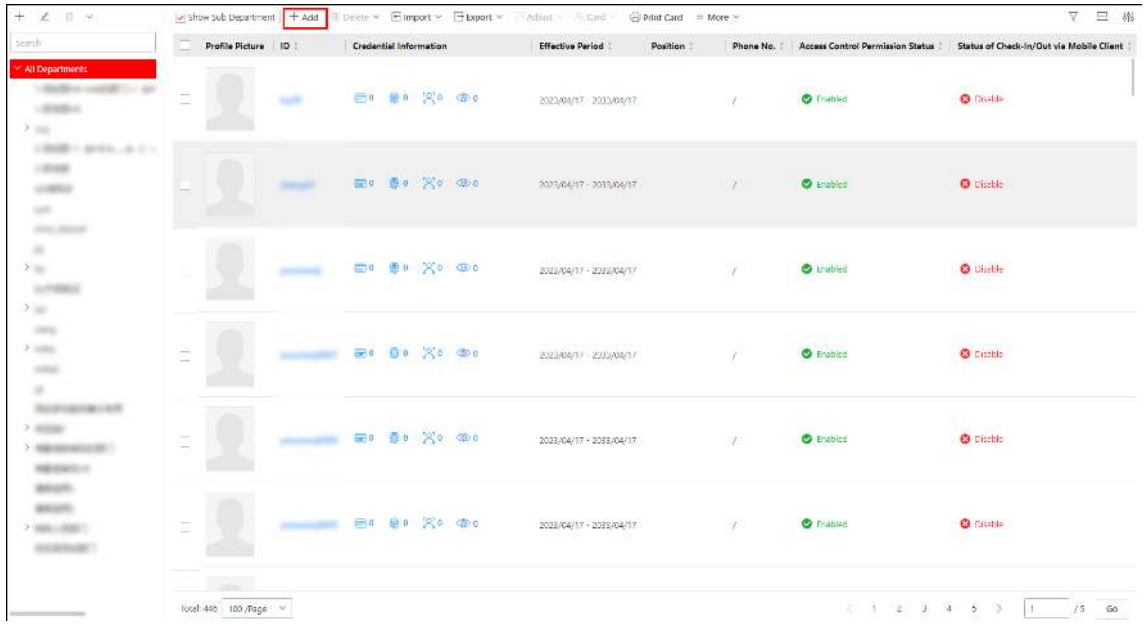


Figure 11-3 The Entry for Adding a Person

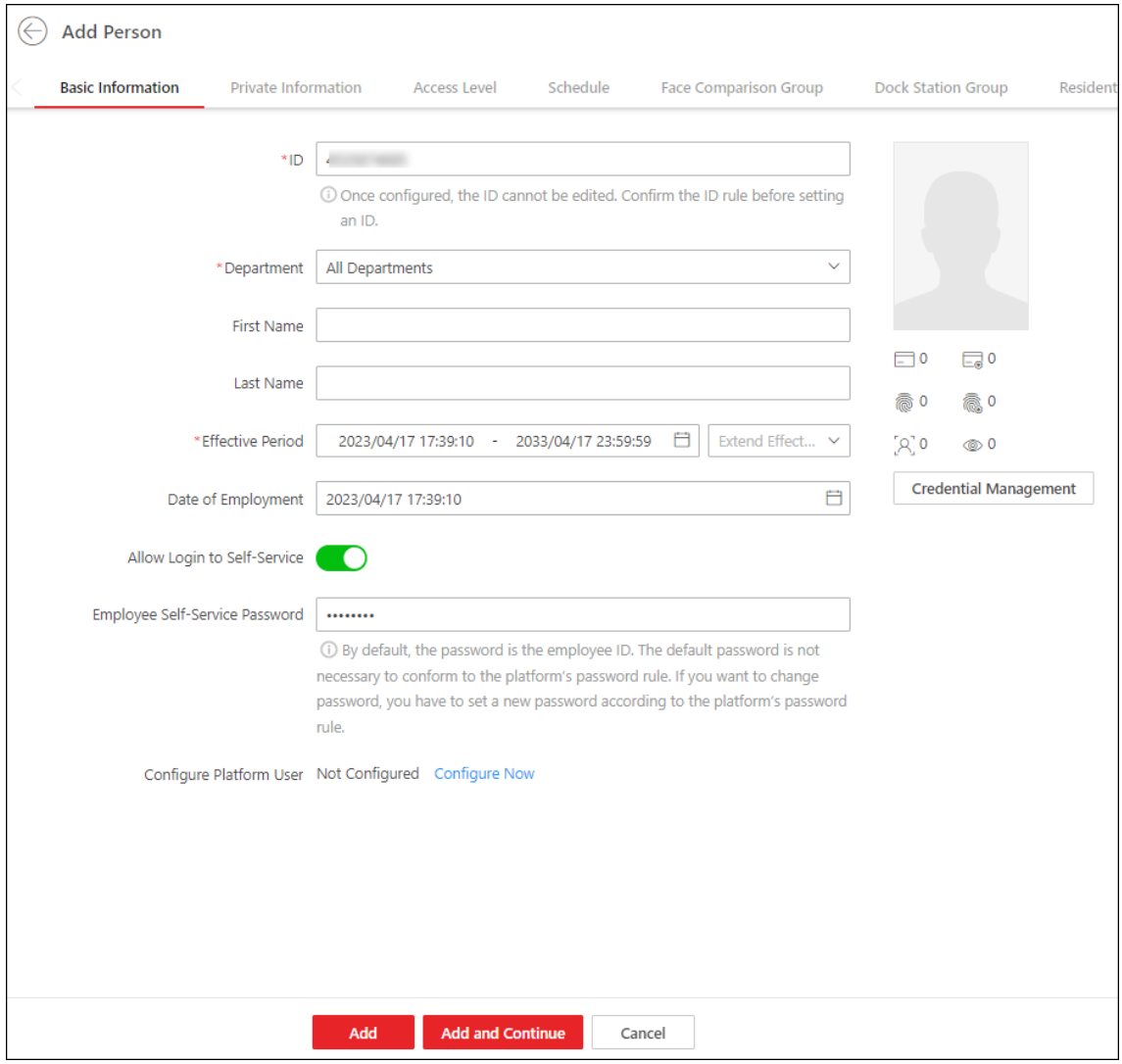


Figure 11-4 Add Person Page

5. 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.

Note

The ID cannot be edited after finishing adding a person, so you should ensure its correctness at the beginning.

Department (Required)

Select a department for the person.

Note

See ***Add Departments*** for details about how to add a department.

Profile Picture

Hover the cursor onto , and you can select from three modes to add a picture.

From Device

You can select **Access Control Device**, **Video Intercom Device**, or **Enrollment Station** and set parameters (if required) to connect the device to the platform, and then collect the face picture via the device. This mode is suitable for non-face-to-face scenario when the person and the system administrator are on different locations.

Note

- For access control devices, only specific models of face recognition terminals are supported.
- 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.

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.
- You can switch on **Check Face Picture Quality via Device** and select a device to check the quality of the profile picture. Click **Save** to start checking. You will be informed if the picture is not qualified.

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

You can set the start date of employment for the person.

Allow Login to Self-Service

Switch on **Allow Login to Self-Service** to allow employees to log in to self-service on the platform. For details, refer to ***Login via Web Client (Employee)*** .

Employee Self-Service Password

After enabling **Allow Login to Self-Service** for the employee self-service, set the password.

Note

By default, the password is the employee ID if the password has not been set. Once the password is modified, the new password should be set according to the password verification rule.

Configure Platform User

Click **Configure Now** to configure a platform user for the person to link the person to a platform user.

Note

No more than one person can be linked to a platform user.

Add New User

Create a new user to link the user with the person by setting the user name, password, user status, and role.

Select Existing User

Select an existing user from the drop-down list to link the user with the person, or click **Add User** to add a user first. For details about adding a user, see ***Add Normal User*** .

Credential Management

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

6. **Optional:** Set the person's private information, such as email, and phone No.
7. **Optional:** Assign access levels to the person to define the access points where the person can access during the authorized period.

Superuser

If the person is set as a superuser, the person will be exempted from remaining locked (credential failed) restrictions, all anti-passback rules, and first person authorization.

Electrostatic Discharge Testing Mode

You can select **Detection Not Required**, **Detect Hand**, **Detect Foot**, **Detect Hand and Foot** as the detection mode for the person.

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.

Open Door via Bluetooth on Mobile Client

Check the box to open enable opening door via bluetooth on the Mobile Client.

PIN Code

Set the PIN code for access authentication. 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**.

Note

- 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

a. Click **Assign**.
b. Select one or more access levels for the person.
c. Click **Assign** to add the person to the selected access level(s).

Note

You can click to view information on access points and access schedules.

8. **Optional:** View and edit the schedule of the person in the table.

Allow Check-In/Out via Mobile Client

Note

Make sure you have purchased the license for this function.

Switch on it to allow the person to check in/out via the Mobile Client. For details, refer to ***Configure Check-In/Check-Out via Mobile Client*** .

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*** .

9. **Optional:** Select a face comparison group and a dock station group for the person.
10. **Optional:** Set resident information to link the person with the indoor station and room number.

Note

- 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.
- Make sure you have added indoor stations to the platform.
- 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.

11. **Optional:** In Vehicle Information area, add the vehicle information for the person.
12. **Optional:** 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.

Note

When the platform is in emergency status, it is not allowed to add a person to an emergency counting group.

13. **Optional:** 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.
14. **Optional:** In Additional Information area, enter additional information to be applied.

Note

Make sure you have set the additional information. See ***Object Missing*** for details.

15. Finish adding the person.
    - Click **Add**.
    - Click **Add and Continue** to finish adding the person and continue to add other persons.

    The person will be displayed in the person list and you can view the details.
16. **Optional:** After adding persons, you can perform the following operation(s).

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

Note

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 to delete the selected person(s).

Delete All Persons

Hover the cursor onto beside , and then click **Delete All** to delete all persons.

Clear Profile Pictures

Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.

Export Person Information

Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.

Export Profile Pictures

Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to **General → System Configuration → Security → Export Profile Pictures** page to check the **Export Profile Pictures**.

Adjust Person

- Move the persons to another department. Once moved, the access levels and schedules of the selected persons will be changed.
  a. Select one or more persons, click → **Adjust Department** .
  b. Select the target department to which the persons are about to be moved.
  c. Click **Move**.
- Adjust the effective period for the person in applications.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Select the effective period from the drop-down list.
  c. Click **OK**.
- Adjust the person's status as resigned.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Set the departure date, type, and reason..
  c. Click **OK**.

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. For details, refer to ***Link Persons to an Indoor Station*** . **Note** • 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). • Make sure you have added indoor stations to the platform. • Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations. • Make sure the room number is consistent with the actual location information of the indoor station.
Clear Access Levels	Select one or more persons, click **More → Clear Access Levels of Person** to clear the access levels of the selected persons. **Note** The access levels of these persons cannot be restored once they are cleared.
Disable Access Levels	Select one or more persons, and click **More → Disable Access Levels of Person** to disable the access levels of the selected persons temporarily. **Note** The access level settings of the selected persons will not be cleared, and will be restored after restoring the persons access levels.
Restore Access Levels	Select one or more persons, and click **More → Restore Access Levels of Person** to restore the disabled access levels.
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.

Enable/Disable Check-In/Out via Mobile Client	Select one or more persons, click **More → Enable/Disable Check-In/Out via Mobile Client** .
Filter Displayed Persons	Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.
	Note When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .
View/Edit Credential Information	In **Credential Information** column, you can view/edit a person's card, fingerprint, face picture, and iris information, and view and download the person's QR code.

Manage Credentials

When adding a person, you can add the required credential information for the person. The supported credentials include normal cards, faces, fingerprints, and irises. These credentials can be used for the access authentication in applications such as access control and elevator control.

Steps

1. On the top navigation bar, select → **Basic Management → Person** .
2. Select **Person Management → Person** on the left.
3. On the adding or editing person page, click **Credential Management** under the profile picture to open the Add Credential pane.
4. 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.

Note

- 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*** .

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.

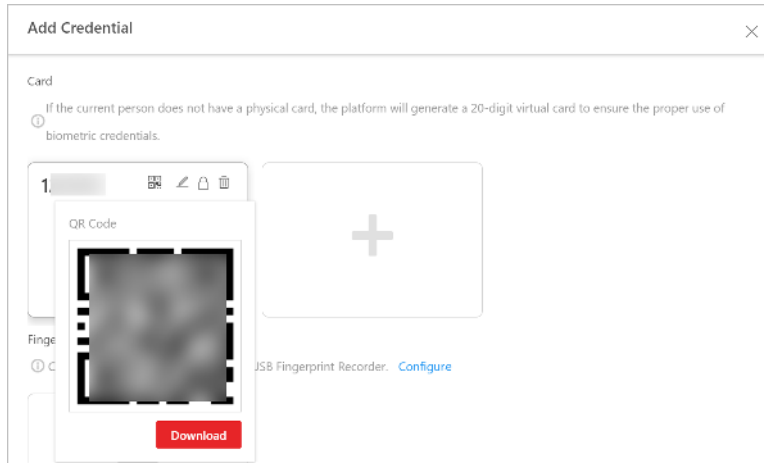


Figure 11-5 View QR Code of Card

5. 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.

6. **Optional:** In the Iris area, collect irises of the person.
   1) Click **Configure** to select a device used for collecting the person's irises.
   2) Click + and then start collecting irises.
7. **Optional:** Switch on **Special Credential** and then add special cards and corresponding fingerprint information.
8. **Optional:** Perform the following operation(s).

Edit Card / Fingerprint / Iris Information	Hover the cursor onto an added card, fingerprint, or iris, and then click .
View and Download QR Code of Card	Hover the cursor onto an added card, and then click .

Delete Card / Fingerprint / Iris	Hover the cursor onto an added card, fingerprint, or iris, and then click .

9. Click **Save**.

11.2.2 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. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. Click → **Import Person Information via Excel** .

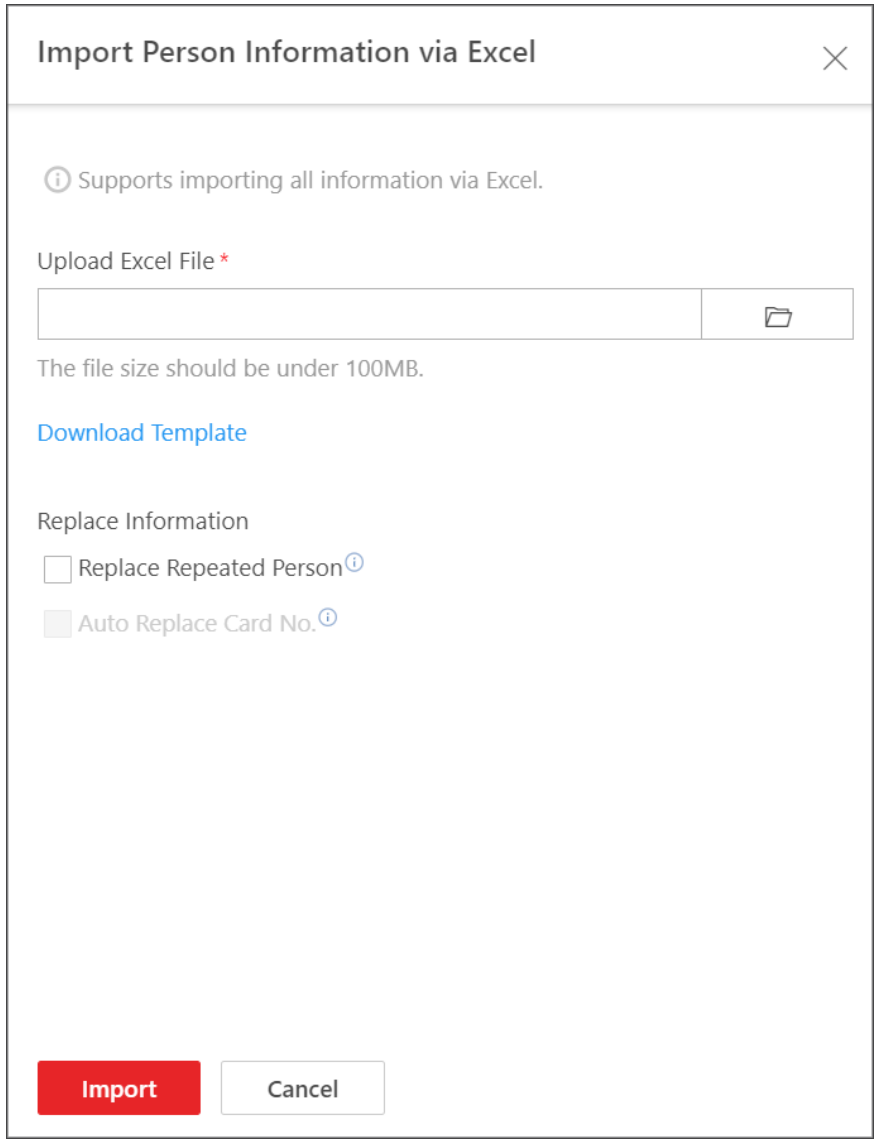


Figure 11-6 Batch Add Persons by Template

4. In the pop-up window, click **Download Template**.
5. 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. See ***Object Missing*** for how to add custom additional information for persons.
6. Click **Download** to save the template to your PC.
7. In the downloaded template, enter the person information following the rules shown in the template.

Note

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.

8. Click , and then select the template (with person information) from your PC.
9. **Optional:** Check **Replace Repeated Person** to replace the person information if the imported ID information is the same with that of the existing persons in the list.
10. **Optional:** Check **Auto Replace Card No.** to replace the card No. automatically if it already exists in the platform.
11. 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.

12. **Optional:** After adding persons, perform the following operation(s).

Edit Person	Click the person name to edit the person details. **Note** 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 to delete the selected person(s).
Delete All Persons	Hover the cursor onto beside , and then click **Delete All** to delete all persons.
Clear Profile Pictures	Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.
Export Person Information	Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file. **Note** You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.

Export Profile Pictures

Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to **General → System Configuration → Security → Export Profile Pictures** page to check the **Export Profile Pictures**.

Adjust Person

- Move the persons to another department. Once moved, the access levels and schedules of the selected persons will be changed.
  a. Select one or more persons, click → **Adjust Department** .
  b. Select the target department to which the persons are about to be moved.
  c. Click **Move**.
- Adjust the effective period for the person in applications.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Select the effective period from the drop-down list.
  c. Click **OK**.
- Adjust the person's status as resigned.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Set the departure date, type, and reason..
  c. Click **OK**.

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. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- 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).
- Make sure you have added indoor stations to the platform.
- Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations.
- Make sure the room number is consistent with the actual location information of the indoor station.

Clear Access Levels	Select one or more persons, click **More → Clear Access Levels of Person** to clear the access levels of the selected persons. **Note** The access levels of these persons cannot be restored once they are cleared.
Disable Access Levels	Select one or more persons, and click **More → Disable Access Levels of Person** to disable the access levels of the selected persons temporarily. **Note** The access level settings of the selected persons will not be cleared, and will be restored after restoring the persons access levels.
Restore Access Levels	Select one or more persons, and click **More → Restore Access Levels of Person** to restore the disabled access levels.
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.
Enable/Disable Check-In/Out via Mobile Client	Select one or more persons, click **More → Enable/Disable Check-In/Out via Mobile Client** .
Filter Displayed Persons	Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required. **Note** When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .
View/Edit Credential Information	In **Credential Information** column, you can view/edit a person's card, fingerprint, face picture, and iris information, and view and download the person's QR code.

11.2.3 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 top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. Click → **Import Person Information via Domain Group** to enter the Import Person Information via Domain Group page.
4. 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.

   Person in Security Group

   Import the selected security groups in the AD domain.
5. 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.
6. Set the effective period for the persons as needed.
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*** .

8. **Optional:** After adding persons, perform the following operation(s).

Edit Person	Click the person name to edit the person details. **Note** 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 to delete the selected person(s).
Delete All Persons	Hover the cursor onto beside , and then click **Delete All** to delete all persons.
Clear Profile Pictures	Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.
Export Person Information	Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file. **Note** You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.
Export Profile Pictures	Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file. **Note** To activate this function, you should go to **General → System Configuration → Security → Export Profile Pictures** page to check the **Export Profile Pictures**.
Adjust Person	• Move the persons to another department. Once moved, the access levels and schedules of the selected persons will be changed. a. Select one or more persons, click → **Adjust Department** . b. Select the target department to which the persons are about to be moved. c. Click **Move**. • Adjust the effective period for the person in applications. a. Select one or more persons, click → **Adjust Effective Period** . b. Select the effective period from the drop-down list. c. Click **OK**. • Adjust the person's status as resigned.

a. Select one or more persons, click → **Adjust Effective Period** .
b. Set the departure date, type, and reason..
c. Click **OK**.

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. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- 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).
- Make sure you have added indoor stations to the platform.
- Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations.
- Make sure the room number is consistent with the actual location information of the indoor station.

Clear Access Levels

Select one or more persons, click **More → Clear Access Levels of Person** to clear the access levels of the selected persons.

Note

The access levels of these persons cannot be restored once they are cleared.

Disable Access Levels

Select one or more persons, and click **More → Disable Access Levels of Person** to disable the access levels of the selected persons temporarily.

Note

The access level settings of the selected persons will not be cleared, and will be restored after restoring the persons access levels.

Restore Access Levels

Select one or more persons, and click **More → Restore Access Levels of Person** to restore the disabled access levels.

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.
Enable/Disable Check-In/Out via Mobile Client	Select one or more persons, click **More → Enable/Disable Check-In/Out via Mobile Client** .
Filter Displayed Persons	Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required. **Note** When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .
View/Edit Credential Information	In **Credential Information** column, you can view/edit a person's card, fingerprint, face picture, and iris information, and view and download the person's QR code.

11.2.4 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.

11.2.5 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.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. Click → **Import Person Information from Device** .
4. Select **Access Control Device** or **Video Intercom Device** as the device type.
5. Select one or more devices from the device list.

Note

You can enter a key word (fuzzy search supported) in the search box to search the target device(s) quickly.

6. Select the importing mode.

   All

   Import all the persons stored in the selected devices.

   Specified Employee No.

   Specify the employee No. of up to five persons and import the persons to the platform.

7. Select a department to which the persons will be imported.
8. **Optional:** Check **Replace Profile Picture** to replace the existed person profile pictures with the new ones from the devices.
9. Click **Import** to start importing.

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.

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

Note

If not, skip this step.

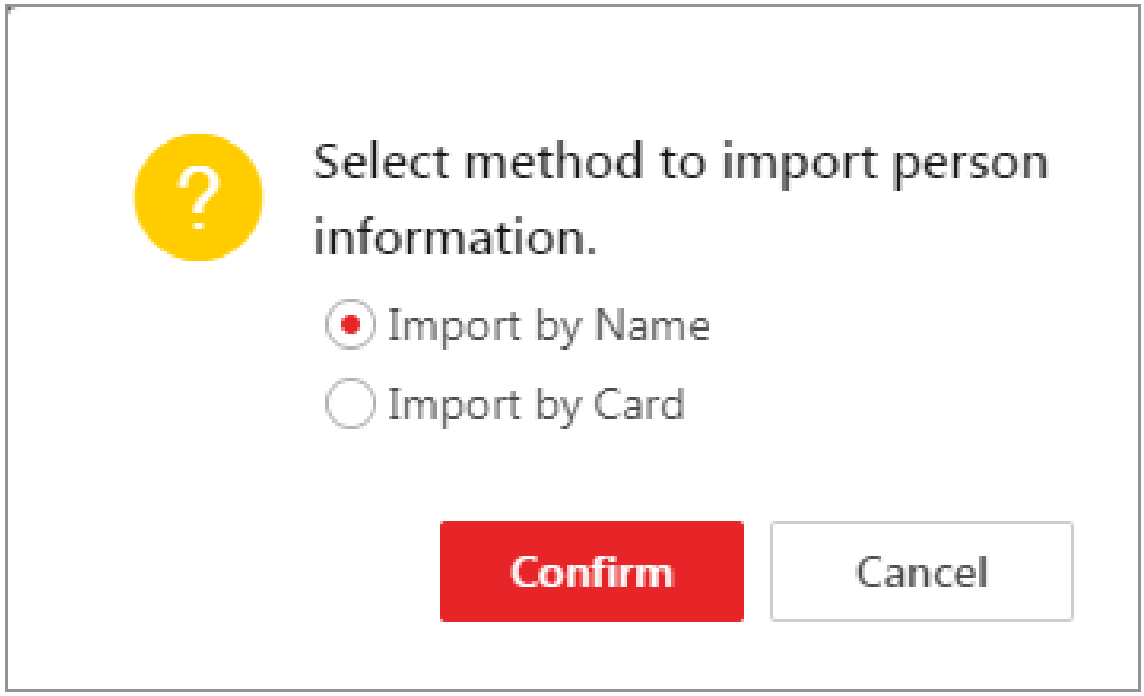


Figure 11-7 Select an Import Method

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.

11. **Optional:** Perform the following operation(s).

Edit Person	Click the person name to edit the person details. **Note** 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 to delete the selected person(s).

Delete All Persons	Hover the cursor onto beside , and then click **Delete All** to delete all persons.
Clear Profile Pictures	Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.
Export Person Information	Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file. **Note** You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.
Export Profile Pictures	Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file. **Note** To activate this function, you should go to **General → System Configuration → Security → Export Profile Pictures** page to check the **Export Profile Pictures**.
Adjust Person	• Move the persons to another department. Once moved, the access levels and schedules of the selected persons will be changed. a. Select one or more persons, click → **Adjust Department** . b. Select the target department to which the persons are about to be moved. c. Click **Move**. • Adjust the effective period for the person in applications. a. Select one or more persons, click → **Adjust Effective Period** . b. Select the effective period from the drop-down list. c. Click **OK**. • Adjust the person's status as resigned. a. Select one or more persons, click → **Adjust Effective Period** . b. Set the departure date, type, and reason.. c. Click **OK**.
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. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- 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).
- Make sure you have added indoor stations to the platform.
- Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations.
- Make sure the room number is consistent with the actual location information of the indoor station.

Clear Access Levels

Select one or more persons, click **More → Clear Access Levels of Person** to clear the access levels of the selected persons.

Note

The access levels of these persons cannot be restored once they are cleared.

Disable Access Levels

Select one or more persons, and click **More → Disable Access Levels of Person** to disable the access levels of the selected persons temporarily.

Note

The access level settings of the selected persons will not be cleared, and will be restored after restoring the persons access levels.

Restore Access Levels

Select one or more persons, and click **More → Restore Access Levels of Person** to restore the disabled access levels.

Enable/Disable Check-In/Out via Mobile Client

Select one or more persons, click **More → Enable/Disable Check-In/Out via Mobile Client** .

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.

Filter Displayed Persons

Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.

Note

When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

View/Edit Credential Information

In **Credential Information** column, you can view/edit a person's card, fingerprint, face picture, and iris information, and view and download the person's QR code.

11.2.6 Import Persons from Enrollment Station

HikCentral Professional allows you to 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 You Start

Make sure you have enroll the persons' credentials via the enrollment station. For details, see ***Manage Credentials*** .

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Click → **Import Person Information from Device** .
3. Select **Enrollment Station** as the device type.
4. Set other parameters, such as access mode, device address, device port, and stage.

   Device Address

   Enter the IP address of the enrollment station from which the person information needs to be imported.

   Device Port

   Enter the port No. of the enrollment station from which the person information needs to be imported.

   User Name

   Enter the user name of the enrollment station from which the person information needs to be imported.

   Password

   Enter the password of the enrollment station from the person information needs to be imported.
5. Set importing stage and method.

   Apply Person Information

The persons whose credentials need to be enrolled will be applied to the enrollment station.

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.

Copy Back Person and Credential Information

When the persons' credentials are enrolled, select the department to which the person and credential information will be imported to.

6. Click **Import** to start importing.
7. **Optional:** Perform the following operation(s).

Edit Person	Click the person name to edit the person details. **Note** 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 to delete the selected person(s).
Delete All Persons	Hover the cursor onto beside , and then click **Delete All** to delete all persons.
Clear Profile Pictures	Hover the cursor onto beside , and then click **Delete Profile Picture Only** to clear all the uploaded profile pictures.
Export Person Information	Click → **Export Person Information** to export all the added person information as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file. **Note** You can check **Access Level Information** or **Schedule Information** to export the additional information at the same time.
Export Profile Pictures	Click → **Export Profile Picture** to export the profile pictures of the added persons as a ZIP file to your PC. For information security, you need to set a password for decompressing the ZIP file.

Note

To activate this function, you should go to **General → System Configuration → Security → Export Profile Pictures** page to check the **Export Profile Pictures**.

Adjust Person

- Move the persons to another department. Once moved, the access levels and schedules of the selected persons will be changed.
  a. Select one or more persons, click → **Adjust Department** .
  b. Select the target department to which the persons are about to be moved.
  c. Click **Move**.
- Adjust the effective period for the person in applications.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Select the effective period from the drop-down list.
  c. Click **OK**.
- Adjust the person's status as resigned.
  a. Select one or more persons, click → **Adjust Effective Period** .
  b. Set the departure date, type, and reason..
  c. Click **OK**.

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, click **More → Link to Indoor Station** and then select an indoor station for each person to apply the person information to the indoor station. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- Make sure you have added indoor stations to the platform.
- Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations.
- Make sure the room number is consistent with the actual location information of the indoor station.

Clear Access Levels

Select one or more persons, click **More → Clear Access Levels to Person** to clear the access levels of the selected persons.

Note

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.

Link Persons to Indoor Stations
Select one or more persons, click **More → Link to Indoor Station** and then select an indoor station for each person to apply the person information to the indoor station. For details, refer to ***Link Persons to an Indoor Station*** .

Note

- Make sure you have added indoor stations to the platform.
- Up to 10 persons can be linked to one indoor station. And one person can only be linked to one indoor stations.
- Make sure the room number is consistent with the actual location information of the indoor station.

Filter Displayed Persons
Enter a person's full name, ID, or card No. and click **Filter** to filter persons as required.

Note

When entering the card No., you can select **Read Card Number by Device** to select a device to read the card No. For details, refer to ***Set Card Issuing Parameters*** .

11.3 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 are 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.
- The self-registration function is available when you purchase and activate any License.

11.3.1 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.

On the top navigation bar, select → **Basic Management** → **Person** . Then select **Basic Configuration** → **Self-Registration Settings** on the left panel to enter the Self-Registration Settings page.

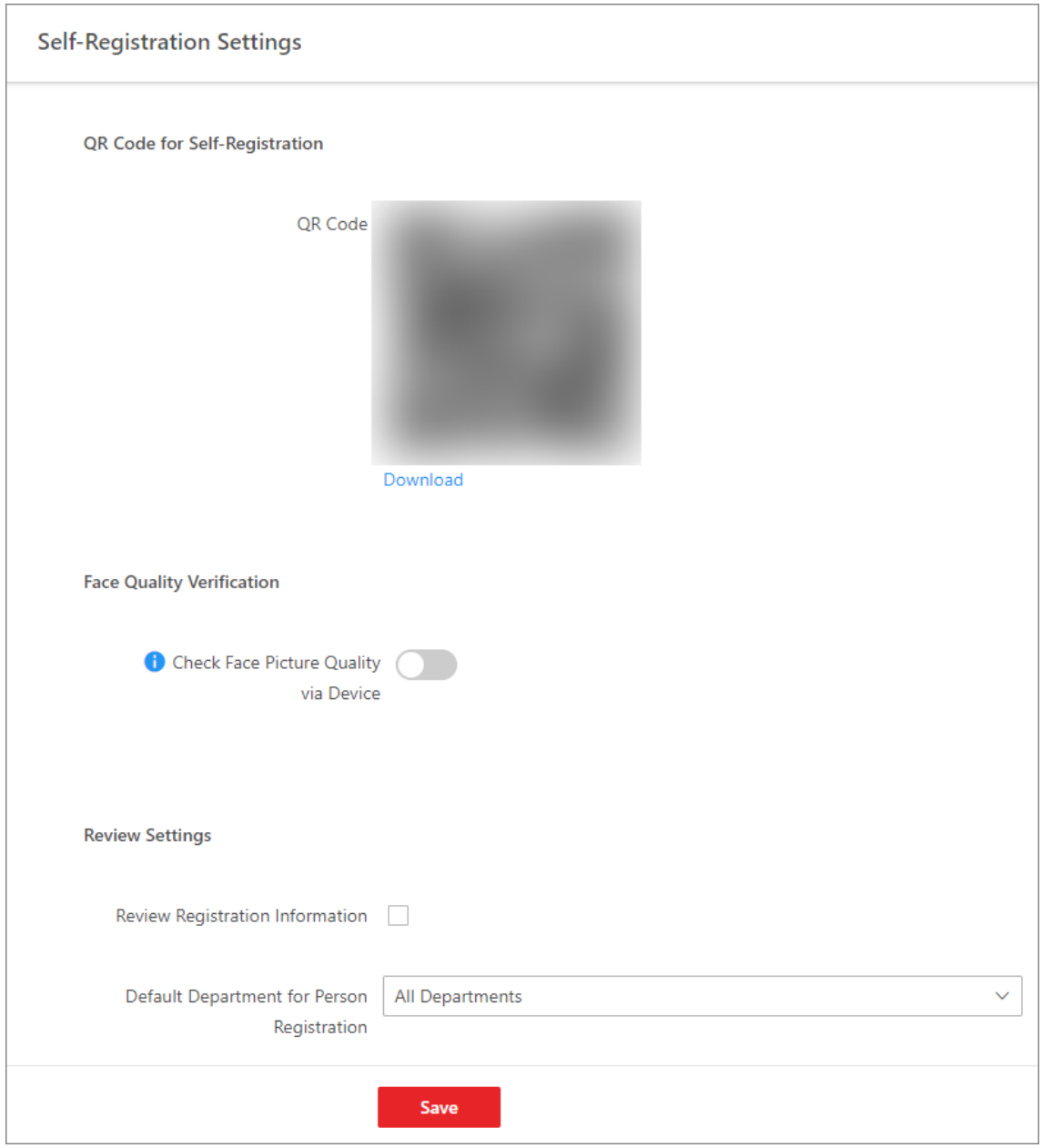


Figure 11-8 Self-Registration Settings

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.

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.

11.3.2 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.

11.3.3 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.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Then select **Person Management** → **To Be Reviewed** on the left panel to enter the Persons to Be Reviewed page.
3. **Optional:** Click to filter registered persons by name, ID, or status to quickly find your wanted persons.
4. Review the displayed person information and verify them.

Operations	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. • Select a registered person, and click to approve the person. • 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. • Select a registered person, and click to reject the person. • 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. • Check multiple registered persons, and click **Delete** to delete them all from the Persons to be Reviewed list.
Self-Registration Settings	Click **Self-Registration Settings**, jumping to enter the Self-Registration Settings page to set self-registration parameters. **Note** For details, refer to ***Set Self-Registration Parameters*** .

Note

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.

11.4 Set Person ID Rule

Before adding persons, you should configure a rule to define the prefix No., total length, and whether using random digits for the person ID.

Steps

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.

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Basic Configuration** → **Person ID Rule** on the left.
3. Enter a prefix No. and set the total length.
4. **Optional:** Check **Random ID** to generate the ID (excepts the fixed prefix No.) with random digits.

   Example

   If you enter ***10*** as the prefix No. and set the total length to 8, all the person IDs will start from "10", such as "10125454" (when **Random ID** is checked) and "10000001" (when **Random ID** is unchecked).
5. Click **Save**.

11.5 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.

11.5.1 Add a Position

You can manually add a position to the platform by entering the position name and specifying its upper-level position.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Position Management** on the left.
3. Click + above the left position tree to open the Add Position pane.
4. Enter the name of the position.
5. From the drop-down list, select the upper-level position to which the position to be added is subordinate.

Note

If you select **<None>**, the position has no upper-level position.

6. **Optional:** Click to select the persons that have been assigned to this position.
7. Click **Add**.
8. **Optional:** Perform the following operations.

Edit Position	• Select the position from the tree on the left and click at the top to edit its information. • Click in the Operation column of a position to edit its information.
Delete Position(s)	• Select a position from the tree on the left and click at the top to delete the selected position. • Click in the Operation column of a position to delete it. • Select one or multiple positions on the right pane and click **Delete** at the top to delete the selected position(s). • To delete all positions, click → **Delete All** either above the left tree or on the top of the right pane.
Search for Position	Enter the position name in the search box above the left tree to search in all added positions, and in the search box on the top right to search under the selected upper-level position. Supports fuzzy search.

11.5.2 Import Positions

You can import multiple positions at once by entering the names of the positions and their corresponding upper-level positions in a predefined template.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Position Management** on the left.
3. Click above the left position tree to open the Batch Import Positions pane.
4. Click **Download Template** to download the template to the local PC.
5. Open the downloaded template file and fill in the required information, including the names of the positions and their upper-level positions.
6. Click to select the edited template file from the local PC.
7. **Optional:** 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.

8. Click **Import**.
9. **Optional:** Perform the following operations.

Edit Position	• Select the position from the tree on the left and click at the top to edit its information. • Click in the Operation column of a position to edit its information.
Delete Position(s)	• Select a position from the tree on the left and click at the top to delete the selected position. • Click in the Operation column of a position to delete it. • Select one or multiple positions on the right pane and click **Delete** at the top to delete the selected position(s). • To delete all positions, click → **Delete All** either above the left tree or on the top of the right pane.
Search for Position	Enter the position name in the search box above the left tree to search in all added positions, and in the search box on the top right to search under the selected upper-level position. Supports fuzzy search.

11.6 Object Missing

This object is not available in the repository.

11.7 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. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. Select persons to whom the cards will be issued.
4. Move the cursor onto , and then click **Batch Issue Cards to Persons**.
5. 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*** .
6. 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.

7. Click **Start** to start issuing cards.
8. 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.

9. Click **Save**.

11.7.1 Set Card Issuing Parameters

HikCentral Professional provides multiple modes for issuing cards, including reading card numbers via devices (card enrollment stations, enrollment stations, or card readers)(card enrollment stations or enrollment stations) and manually entering card numbers.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. 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.
4. 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 Format

   If the card is Wiegand card, select **Wiegand**. If not, select **Normal**.

   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 format, 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**. If not, select **Normal**.

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.

Note

- 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

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

11.8 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. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. **Optional:** Set conditions to search for the target persons.
4. Select the persons for whom you need to print cards.
5. Click to open the Print Card window.

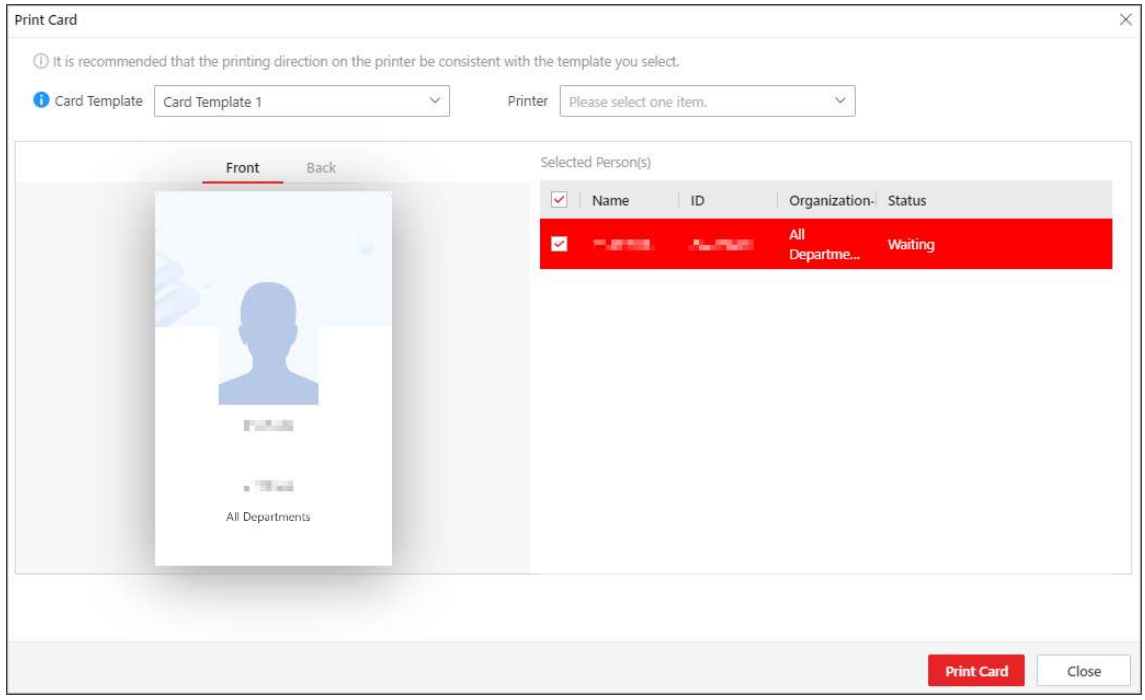


Figure 11-10 Print Card Window

6. Select a card template from **Card Template**.
7. Select a printer from **Printer**.
8. Select person(s) from the Selected Person list.
9. Click **Front** and **Back** to preview the information to be printed on the front and back of the physical cards.
10. 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.

Related Information Add a Single Person

11.9 Report 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.

11.9.1 Report Card Loss

If a person cannot find her/his card, you can report card loss via the platform to freeze the access levels related to the card.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. **Optional:** On the Filter pane, click and set more conditions to search for persons for whom you want to report card loss.
4. 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.

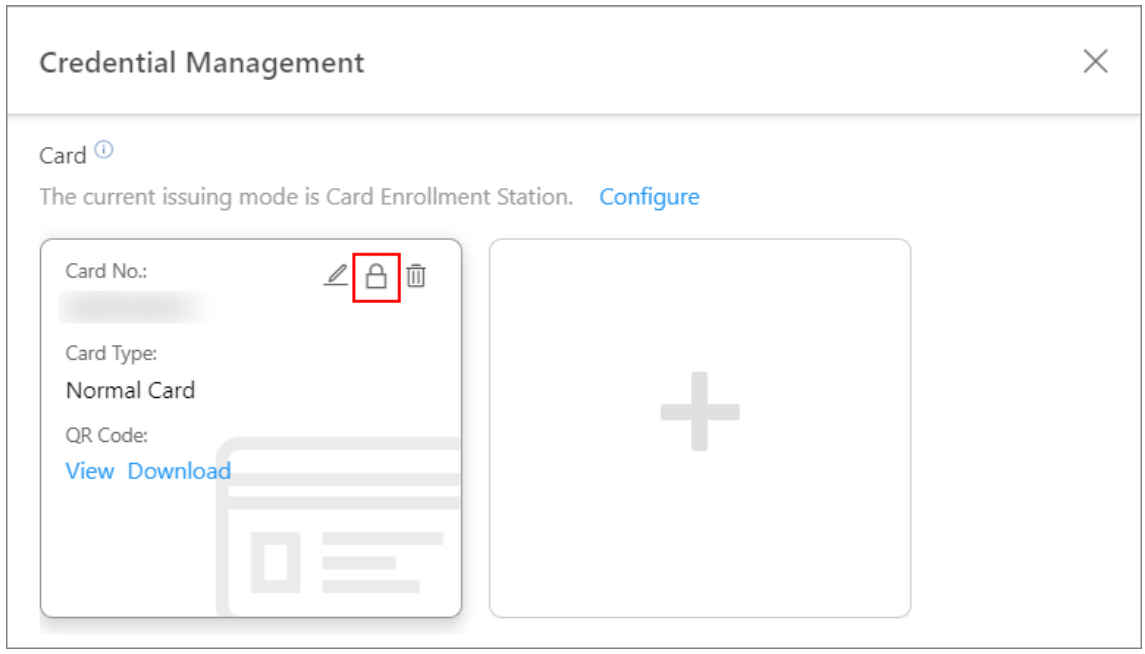


Figure 11-11 Add Credential Panel

5. In the Card area, move the cursor onto the lost card and then click .
6. Click **OK** to confirm the operation.
7. Click **Save**.

   After you report card loss, the access levels of the lost card will be inactive.
8. **Optional:** Move the cursor onto the lost card and then click to cancel the card loss report.

Note

You need to delete all the temporary cards before you can cancel the card loss report.

The card's access level will be active and the original biometric credentials (such as fingerprints and face information) will be linked to this card again.

9. **Optional:** Select the persons in the person list, move the cursor onto on the top, and then click **Report Loss** on the top to batch report loss of multiple cards.

11.9.2 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.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. **Optional:** On the Filter pane, click and set more conditions to search for the person to whom you want to issue the temporary card.
4. Click the name of the person in the person list to enter the basic information page.
5. Click **Credential Management** to open the Credential Management pane.
6. In the Card area, click .
7. Click **OK** to confirm the operation.
8. Enter the card number.
9. Set the expiry date to define the time when the temporary card becomes invalid.

Note

The expiry date of the 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*** .

10. Click **Save**.

Note

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.

11. Perform the following operation(s) if needed.

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 .

11.9.3 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.

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Person** on the left.
3. **Optional:** On the Filter pane, click and set more conditions to search for the persons for whom you want to cancel card loss reports.
4. Select the persons in the person list.
5. Move the cursor onto , and then click **Cancel Card Loss**.

   The persons' temporary cards will be deleted.

11.10 Set Authentication via PIN Code

You can enable this function for allowing persons to access via PIN code.

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

Then select **Basic Configuration** → **Authentication via PIN Code** on the left.

Switch on **Person Authentication 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*** .

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.

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.

Click **Save**.

11.11 Manage Resigned Persons

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

11.11.1 Add Resigned Persons

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

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Resigned** on the left.
3. Click **Add** to open the Add Resigned Person pane.
4. 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.

5. 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*** .

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

Note

You can also adjust the person's status as resigned in Person Management module. See details in ***Add a Single Person*** 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.

9. 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.

11.11.2 Reinstate Persons

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

Steps

1. On the top navigation bar, select → **Basic Management** → **Person** .
2. Select **Person Management** → **Resigned** on the left.
3. Select one or multiple persons and click **Reinstate**.
4. 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 permissions and attendance schedule will be accordance to that of their departments.

11.11.3 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.

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.

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 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.

12.1.1 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.

Access Control

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.

Vehicle

Vehicle Attribute

Events occurred during the vehicle recognition process, such as license plate number matched events, vehicle type matched events, and license plate number 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

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.

Intelligent Analysis Group

Events occurred during the regional people counting process and 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, UVSSs, dock stations, recording servers) added to the platform, such as the camera offline, server exception, and so on.

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.

Security Inspection

Events occurred on walk-through metal detectors.

On-Board Monitoring

Events detected by driving devices and occurring during the vehicle driving process.

12.1.2 Add Normal Event and Alarm

The platform has provided multiple triggering event types for you to configure rules for detection or triggering alarms.

In the top left corner of the Home page, select → **Security Monitoring** → **Event and Alarm** .

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 cameras, devices, servers, etc.) which can trigger this event and alarm.

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.
- The Triggering Event and Source fields support fuzzy search.

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, area name, triggering event name, or site name, so that you can quickly know the location where the event/alarm occurs.

Face Comparison Group

If the triggering event you select is **Face**, you need to select the face comparison group so that the platform can compare the detected face pictures with face pictures in the group.

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.

Frequency

If the source type you selected is **Parking Lot** and the triggering event is **Frequently Appeared Vehicle**, 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.

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.

- 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).

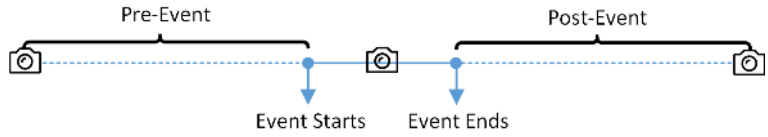


Figure 12-1 Capture Pictures

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 emergency operation groups as the linkage targets. When the event occurs, the platform will trigger these doors, floors, or 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.

Close Alarm Output: The added alarm output(s) can be closed manually, or you can set the time period (unit: s) after which the alarm output(s) will be closed automatically.

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 Third-Party Integrated Resource

Click **Add** to select the resources integrated from a third-party platform 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 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 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.

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.

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.

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).

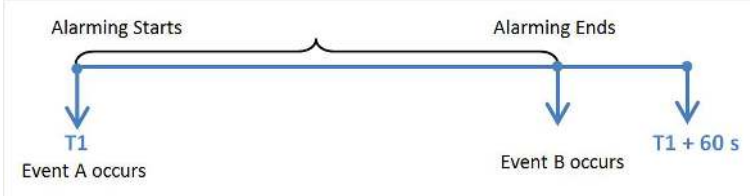


Figure 12-2 Event Receiving Schedule 1

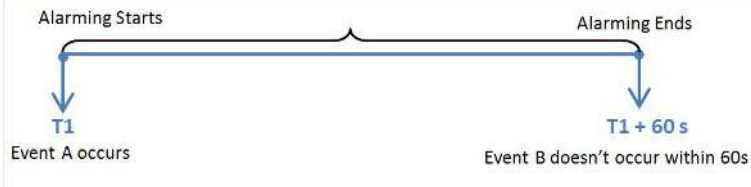


Figure 12-3 Event Receiving Schedule 2

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.

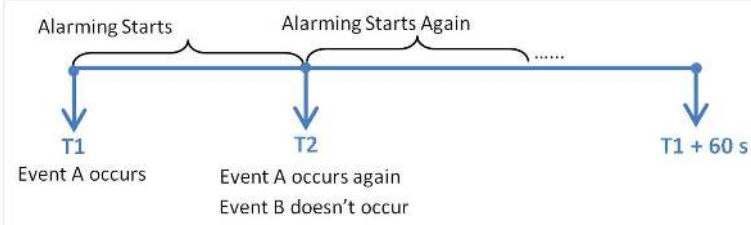


Figure 12-4 Event Receiving Schedule 3

Alarm Settings

Switch on **Trigger Alarm** to trigger the configured event as an alarm.

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 group(s) or user(s) to send the alarm information to and the recipient(s) can receive the alarm information when he/she logs in to HikCentral Professional via the Mobile Client.

Note

By default, users configured as the default recipients on the Alarm Receiving Configuration page will be automatically selected and cannot be deselected. For how to configure default recipients and recipient groups, refer to ***Add Call Recipients*** .

Trigger 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

When the alarm is triggered by an emergency (such as a fire), the platform automatically switches to the **Trigger Emergency** mode or **Turn Off Emergency** mode.

Link Map

Select a map to show the alarm information and you should add the camera to the map as a hot spot (refer to).

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.

Trigger Audible 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 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. 2. Click **Copy To** in the top right corner of the page. 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. 4. Specify the settings of the source and select the target(s). 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** . 2. Set the time when the event(s) start being disabled and the duration of how long the event(s) will be disabled for. 3. (Optional) Enter the reason for disabling the event(s).

Operation	Description
	4. (Optional) Check **Disable Device Alarm** to change the alarm status of the device(s) displayed in the event list. 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.

12.1.3 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. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** .
2. Select **Event and Alarm Configuration** → **Combined Alarm** on the left.
3. Click **Add Combined Alarm** to open the Add Combined Alarm pane.

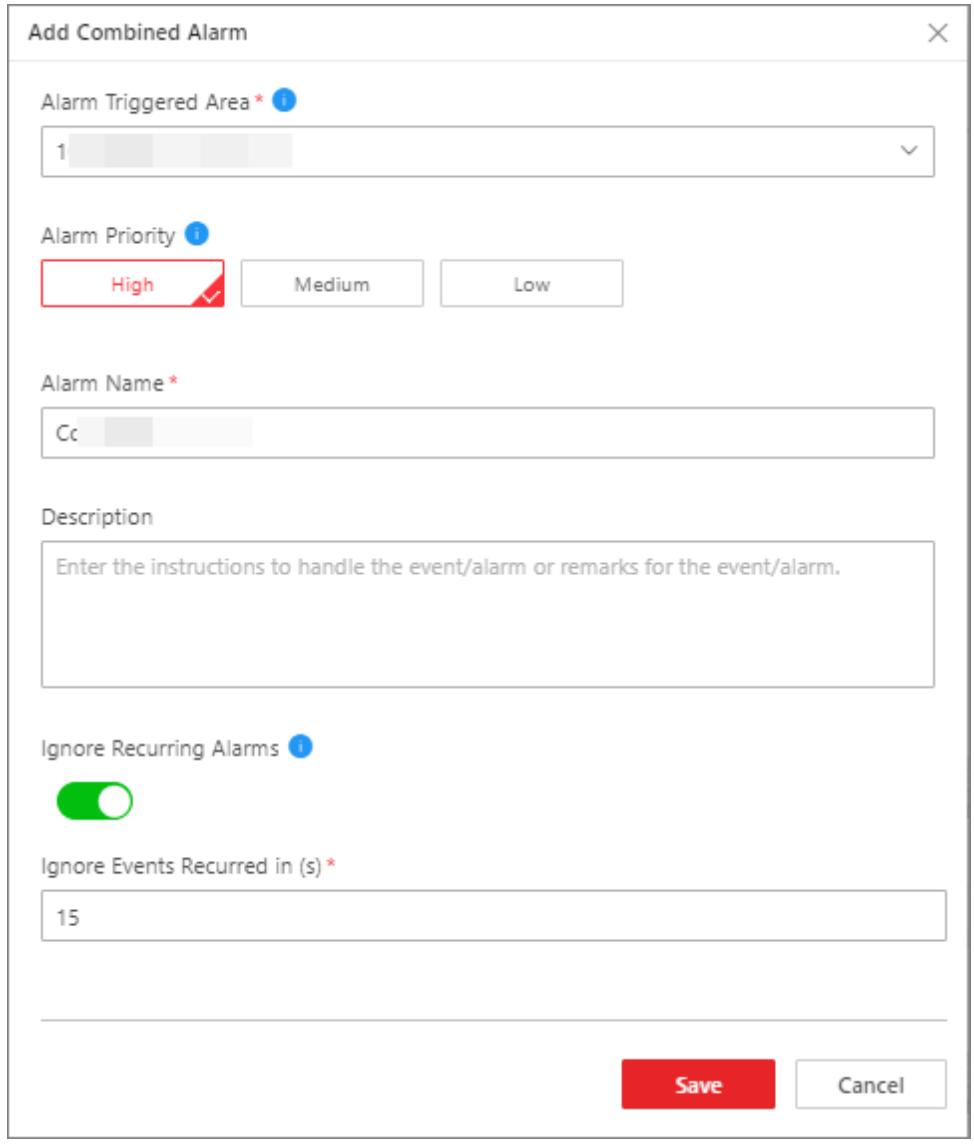


Figure 12-5 Add Combined Alarm

4. 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.

5. Click **Save** to enter the configuration page.
6. 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**.

   A Receiving Schedule card will appear on the page.

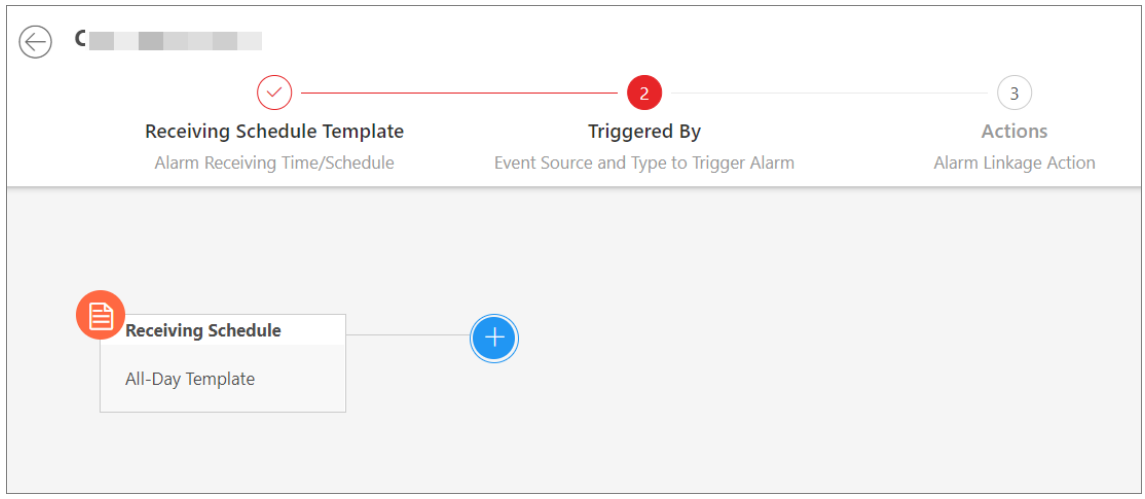


Figure 12-6 Receiving Schedule Card

7. Configure conditions for triggering the combined alarm.
   1) Click at the right of the Receiving Schedule card to open the Select Alarm Triggering Logic pane.
   2) Select a triggering logic and click **Save**.

   The condition card will appear.

   3) Click on the condition card to open the Select Event Source and Event Type pane.
   4) Select a triggering event and a source, and click **Save**.

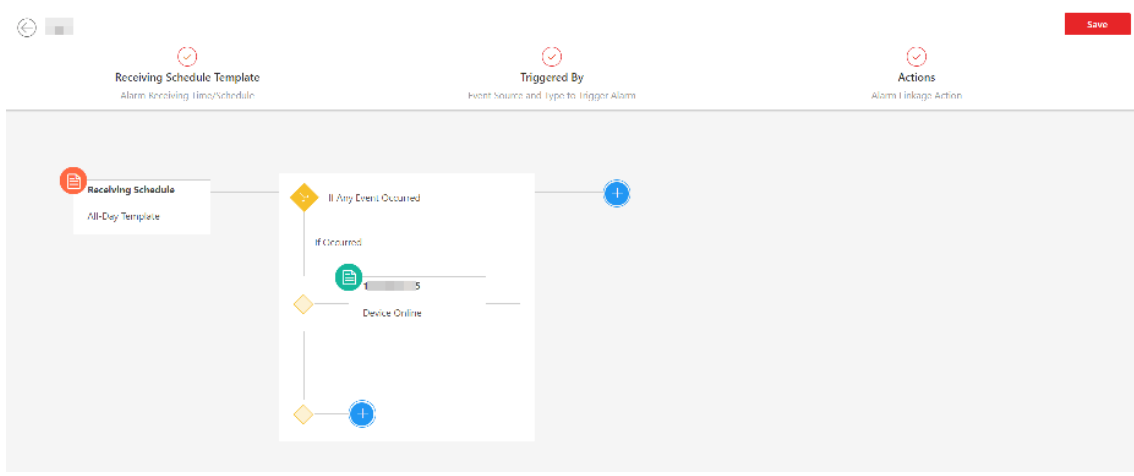


Figure 12-7 Condition Card

5) **Optional:** Click below the newly added event source and type card to select more event sources and types.

6) **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.

8. 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 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. For details, refer to ***Add Normal Event and Alarm*** .

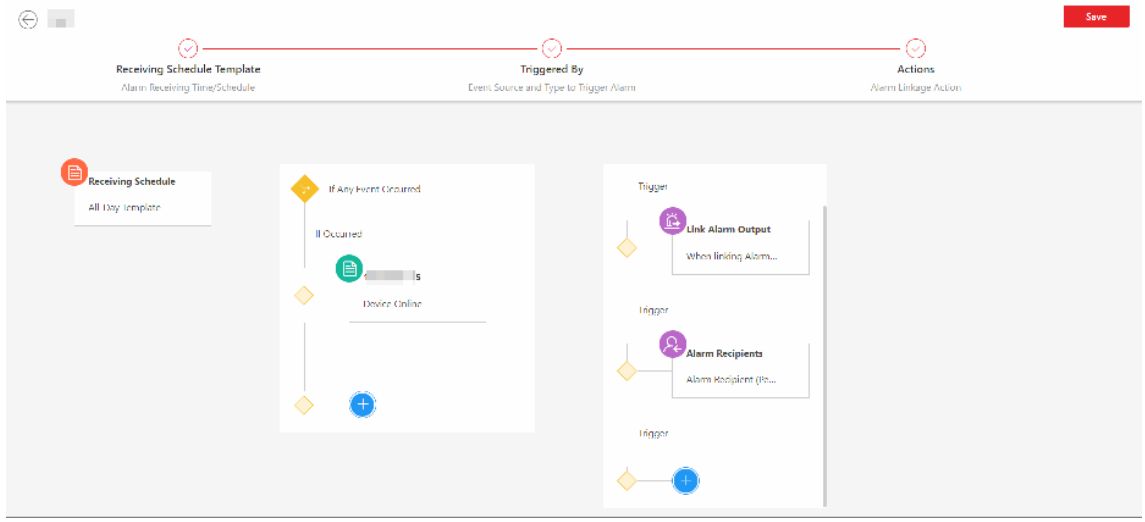


Figure 12-8 Action Card

5) **Optional:** Click ⊕ below the Alarm Recipients card to add more linkage actions.

9. **Optional:** Click the icon on the top left of each card to reselect the content.
10. **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.

11. 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.

12. **Optional:** Perform the following operations according to your requirements.

Add to Map	Click **Add to Map** to add this alarm to the map. After that, the alarm will be marked on the map when the alarm is triggered.
Copy Parameters to Existing Alarm	Click **Copy**, and then select the items (such as basic information, actions, receiving schedule, receiving mode), and select the target alarm to copy to.
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.

12.1.4 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. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** .
2. Select **Custom Event** → **Generic Event** on the left.
3. Click **Add** to enter the Add Generic Event page.

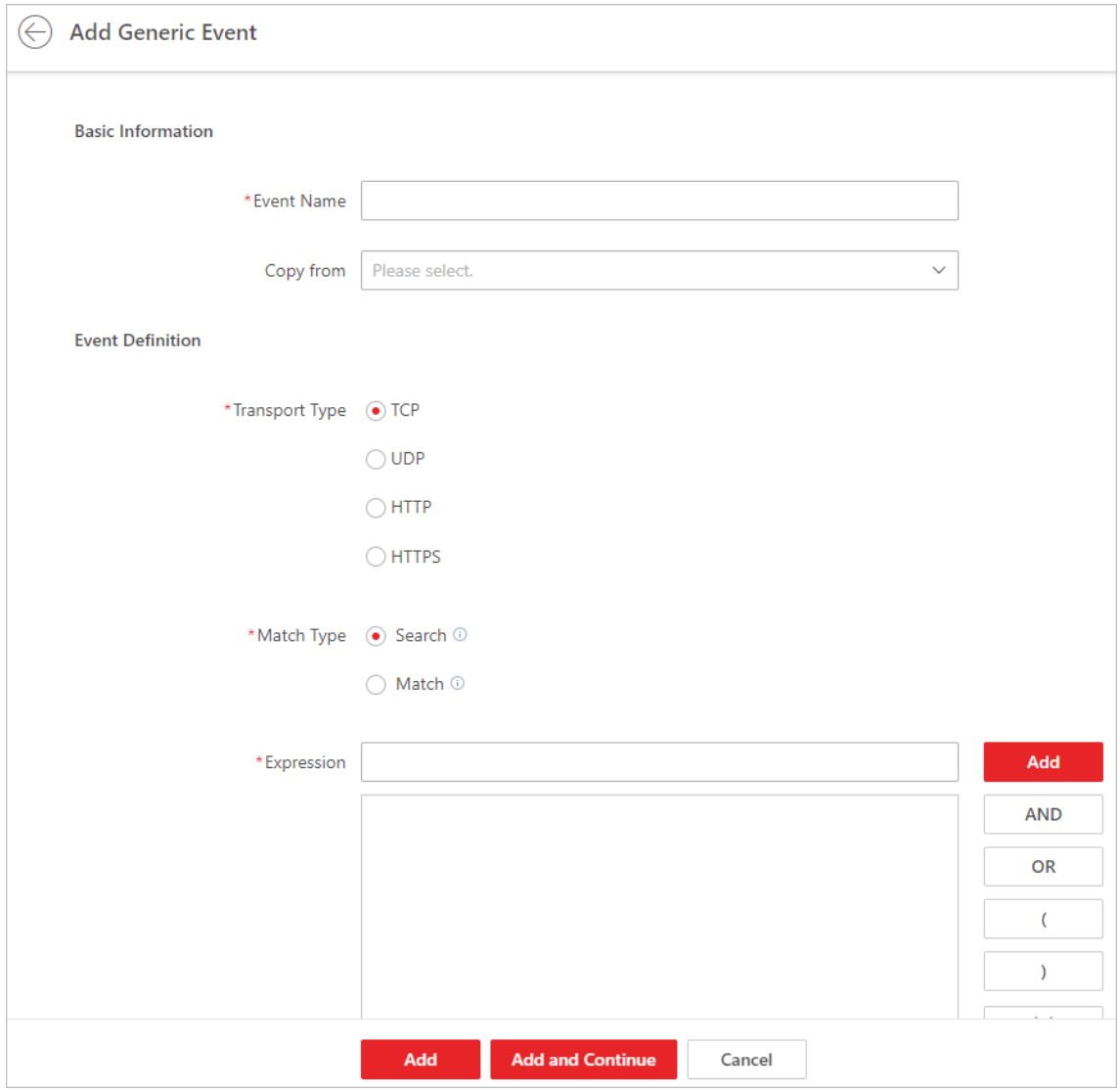


Figure 12-9 Add Generic Event Page

4. Set a name for the event.
5. **Optional:** Copy the settings from other generic events in the **Copy from** field.
6. Select **TCP**, **UDP**, **HTTP**, or **HTTPS** as the transport protocol.
7. Select the match type which indicates how particular your system should be when analyzing the received data packages:

   Search

   The received package must contain a part of text defined in the expression.

   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

The text contained in the received package must be exactly the same as that defined in the expression.

8. 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.

9. 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.
10. **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.
Delete Event Settings	Select the event(s) and click **Delete** to delete the selected event settings.
Delete All Event Settings	Check the checkbox in the heading row, and click **Delete** to delete all the event settings.
Receive Generic Event	Select the event(s), click **Receive Generic Event** to open the settings pane, and check the checkbox(es) to enable receiving the generic event(s) via different protocols.

12.1.5 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. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** .
2. Select **Custom Event** → **User-Defined Event** on the left.
3. Click **Add**.

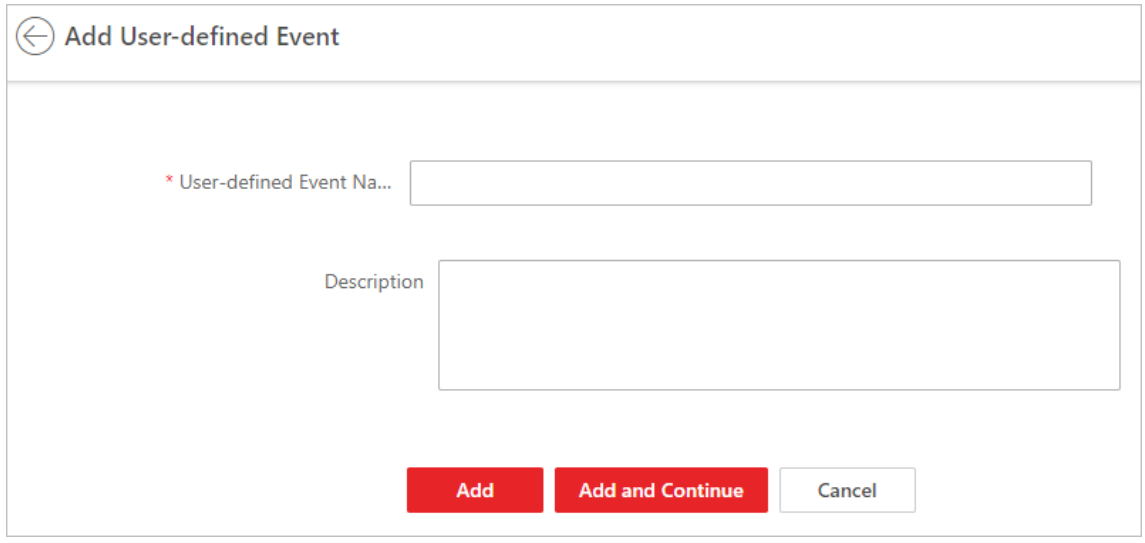


Figure 12-10 Add User-Defined Event

4. Create a name for the event.

5. **Optional:** Enter the information to describe the event.
6. 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.

12.2 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.

12.2.1 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. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** .
2. Select **Basic Configuration** → **Receiving Schedule Template** on the left.
3. Click + to enter the Add Receiving Schedule Template page.

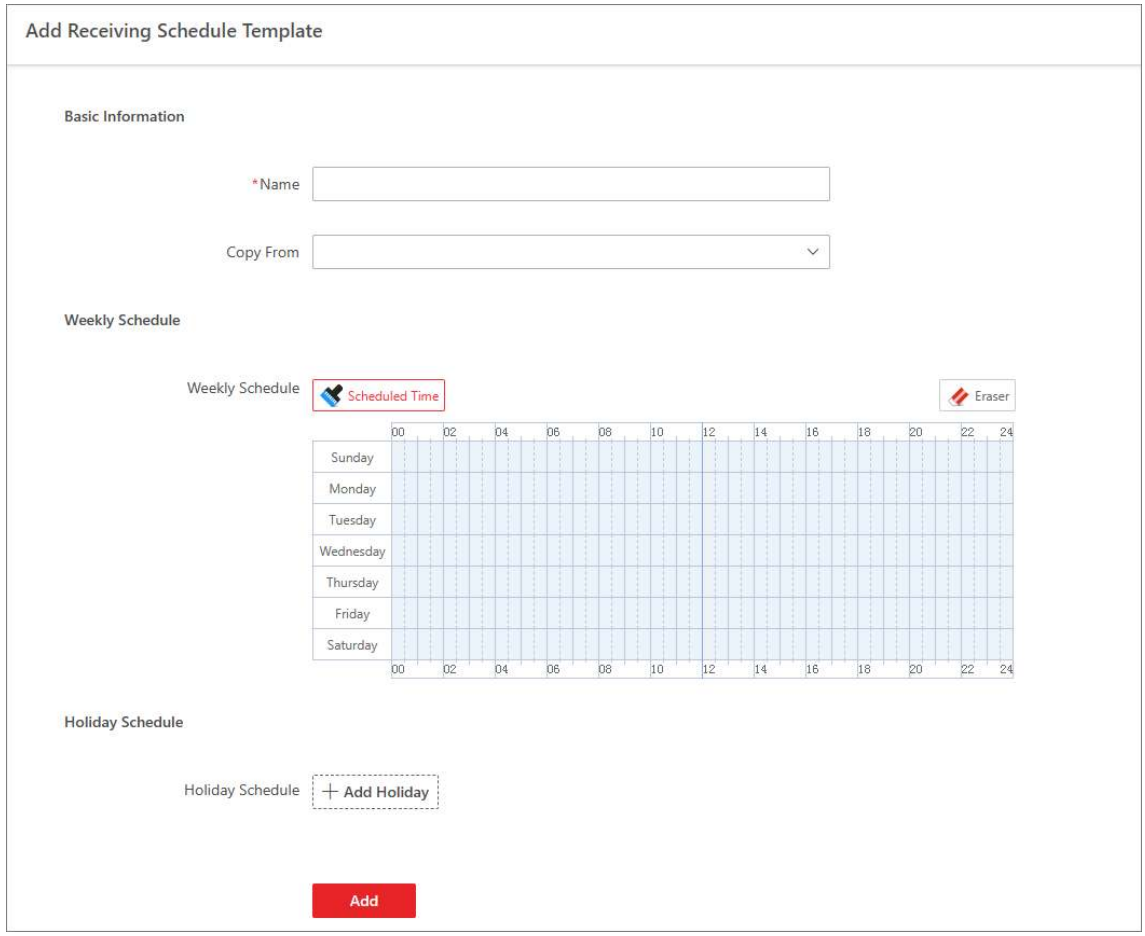


Figure 12-11 Add Receiving Schedule Template

4. Enter a name for the template.
5. **Optional:** Select another defined template to copy the settings to the current template.
6. 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.

7. **Optional:** Click **Erase** and click on the drawn time period to clear the corresponding time period.
8. **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.

9. Click **Add** to add the template.

The receiving schedule template will be displayed on the receiving schedule template list.

10. **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. **Note** The predefined templates cannot be edited.
Delete Template	Select a template and click to delete the template. **Note** • The predefined templates cannot be edited. • 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.

12.2.2 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. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** .

2. Select **Basic Configuration → Alarm Custom Settings** on the left.
3. Customize alarm priorities according to actual needs. By default, three kinds of alarm priority exist.

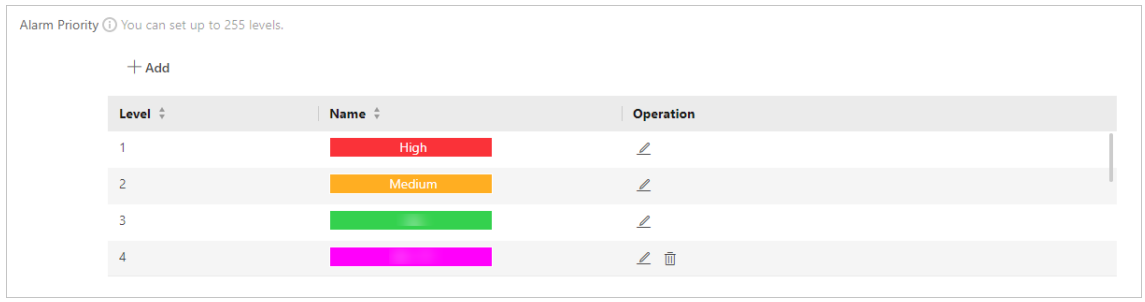


Figure 12-12 Alarm Priority

1) Click **Add** to open the adding alarm priority pane.

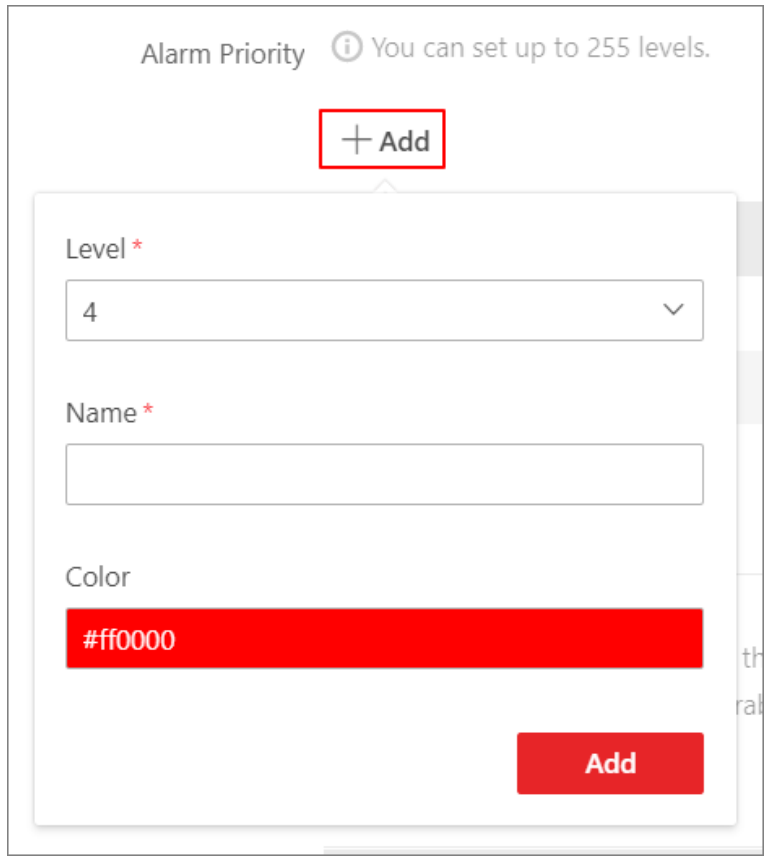


Figure 12-13 Add Alarm Priority

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.

4. Customize alarm categories according to actual needs. By default, four alarm categories exist.

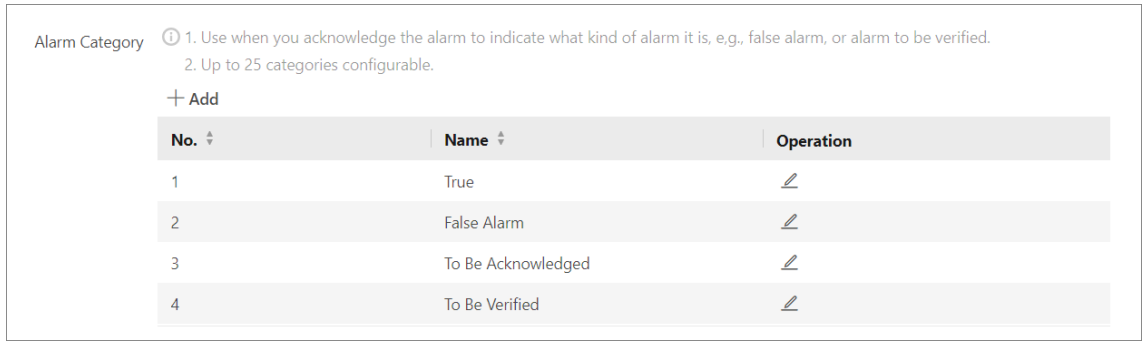


Figure 12-14 Alarm Category

1) Click **Add** to open the adding alarm category pane.

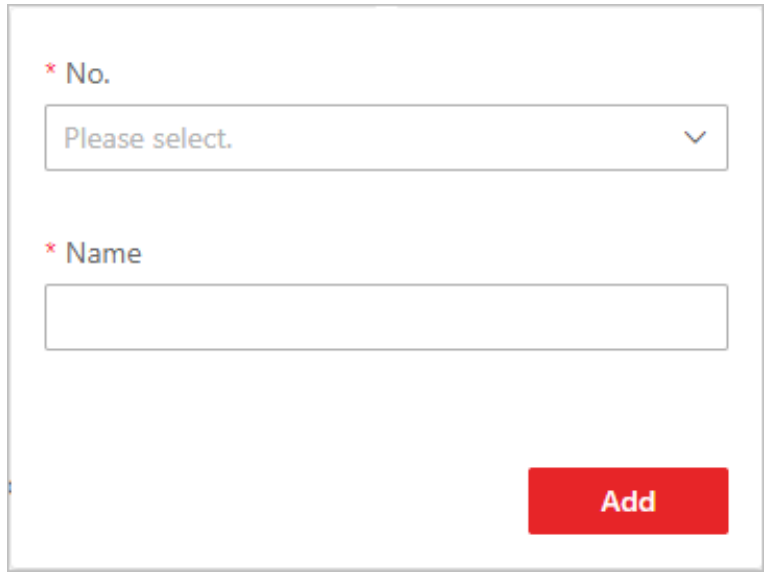


Figure 12-15 Add Alarm Category

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.

5. Customize color template according to actual needs. By default, three alarm categories exist.

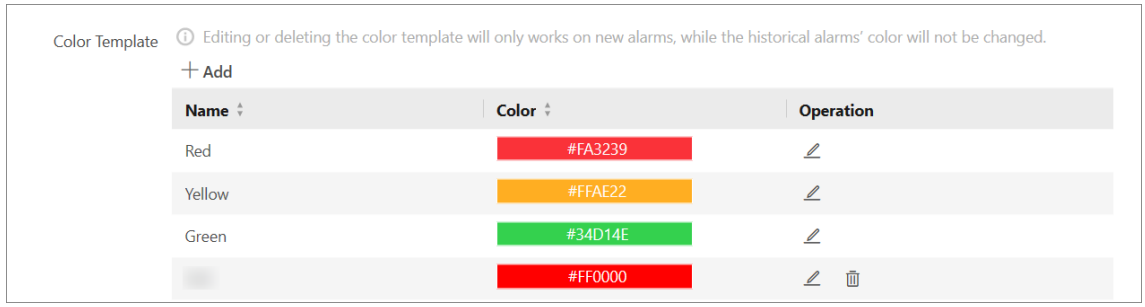


Figure 12-16 Color Template

1) Click **Add** to open the adding color template pane.

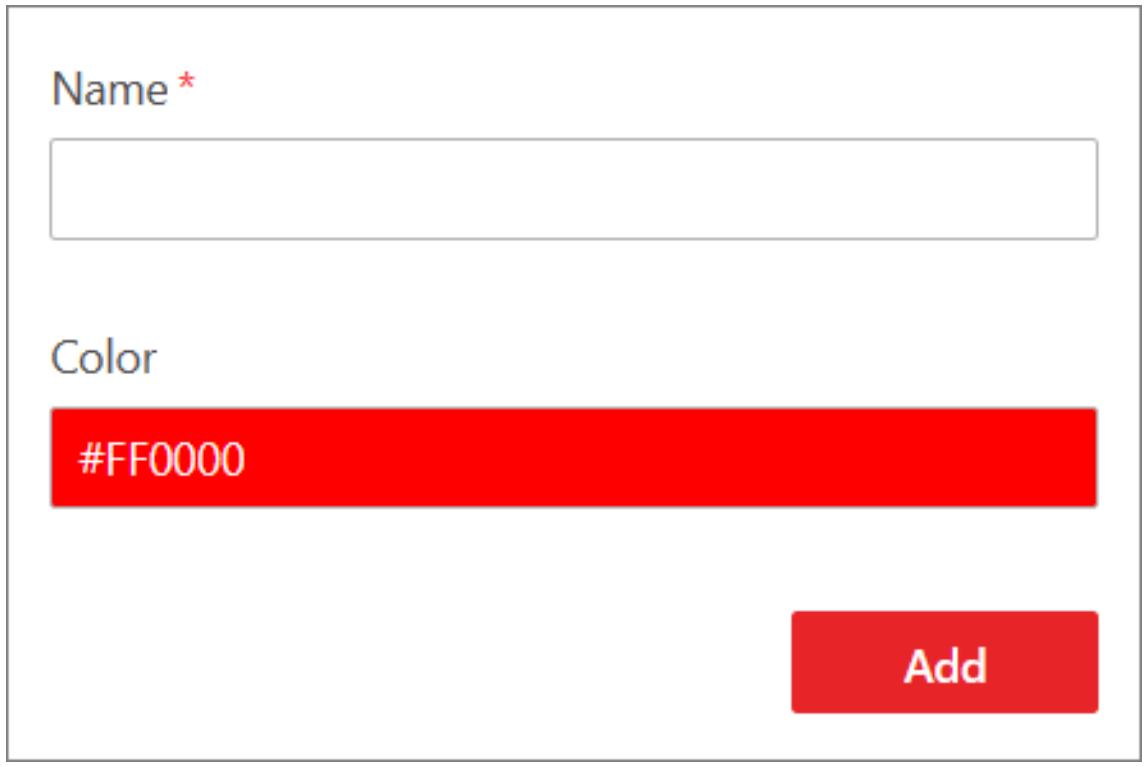


Figure 12-17 Add Color Template

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.

6. 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.

7. **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.

12.2.3 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. In the top left corner of the Client, select → **Security Monitoring** → **Event and Alarm** .
2. Select **Basic Configuration** → **Alarm Receiving Configuration** on the left.
3. In the Alarm Recipient Group field, click + above the group list to open the adding alarm recipient group pane.
4. Enter a name for the group and click **Add**.

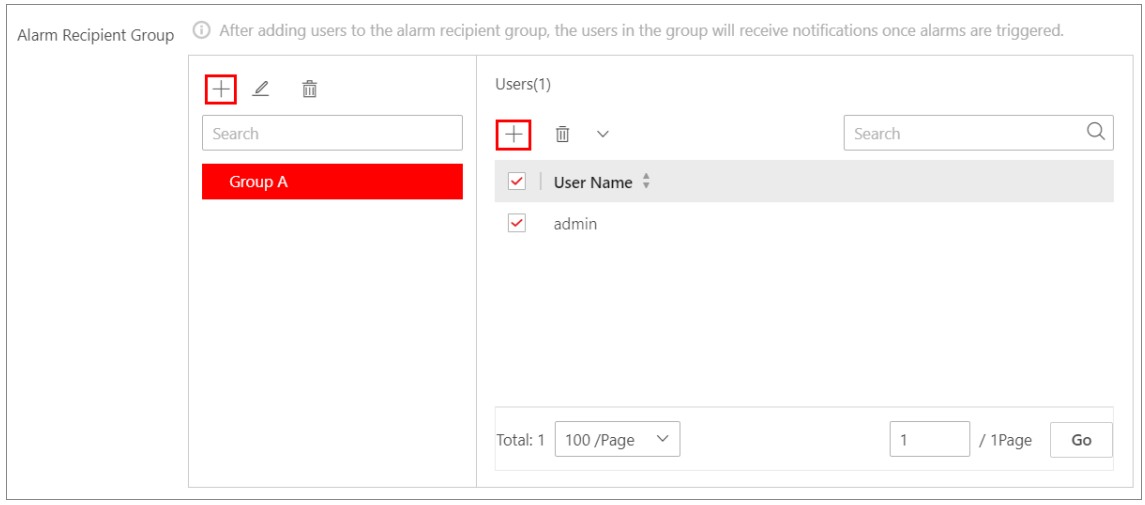


Figure 12-18 Alarm Recipient Group Field

5. Select an alarm recipient group and click + in the Users field to add user(s) to the group.

6. **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.
7. 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.
8. **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.
9. **Optional:** Check **Upload Historical Alarm** to enable uploading the historical alarms to the Control Client.
10. 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.

12.2.4 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 ***Set Email Template*** .
- 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. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** .
2. Select **Basic Configuration** → **Scheduled Report** on the left.
3. Click **Add** if there is no scheduled report rule or click + above the rule list to enter the Create Report page.
4. 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.

5. In the Report Target field, click **Add** to select events or alarms to be contained in the report.

Note

Up to 32 events and alarms can be added in one report.

6. 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.

7. Set advanced parameters.

Send Report 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 ***Set Email Template*** .

Upload to SETP

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 Evidence Management Center

If it is enabled, the platform will automatically upload and save reports to the Evidence Management Center. You can select evidence type and evidence tag(s) for the scheduled reports. For details, refer to ***Evidence Management Center*** .

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.

8. Click **Save** to add the report rule.

12.3 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.

12.3.1 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 12-19 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. • 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.

12.3.2 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. In the top left corner of Home page, select → **Security Monitoring** → **Event and Alarm** → **Search** → **Event and Alarm Search** .
2. Set the time range for search.
   - Select a predefined time period for search.
   - Select **Custom Time Interval** 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 **Triggered By** 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:** 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.

12.3.3 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.

In the top left corner of the Client, select → **Security Monitoring** → **Event and Alarm** .

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 Role and User Management

The system allows you to add users and assign user's permissions for accessing and managing the system. Before adding users to the system, you should create roles to define the user's access rights to system resources and then assign the role to the user for granting the permissions to the user. A user can have many different roles.

13.1 Add 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. You can click the role name to view details. The two default roles 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 on the Web Client.

1. On the top, select **System**.
2. Select **Account and Security → Roles** on the left.
3. Click **Add** to enter Add Role page.

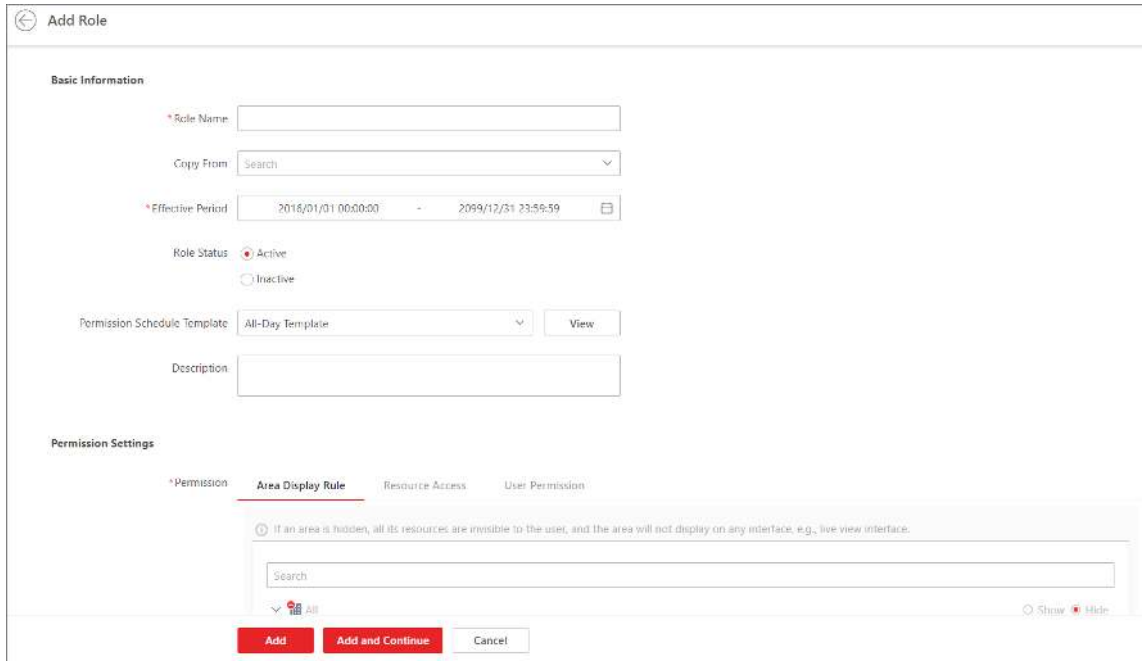


Figure 13-1 Add Role Page

4. 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.

Effective Period

Set the time range within which the role takes effect. The role is inactive outside the effective period.

Role Status

Active is selected by default. If you select **Inactive**, the user account will be inactivated until you activate it.

Permission Schedule Template

Set the authorized time period when the role's permission is valid. Select **All-day Template**/ **Weekday Template**/**Weekend Template** as the permission schedule of the role, or click **Add** to customize a new permission schedule template.

Note

- When 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.

5. 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.

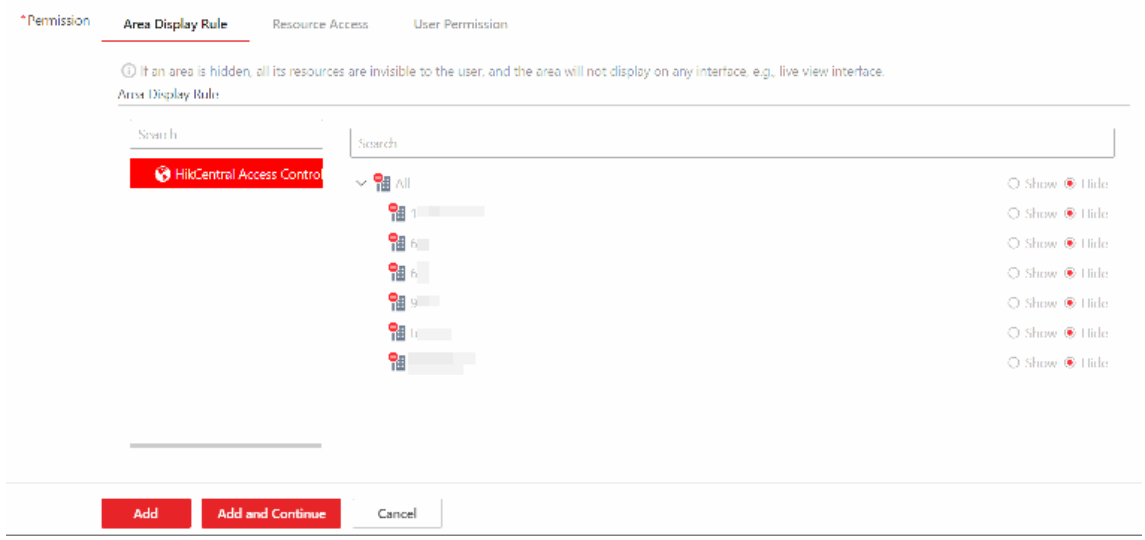


Figure 13-2 Area Display Rule

Resource Access

Select the functions from the left panel and select resources from right panel to assign the selected resources' permission to the role.

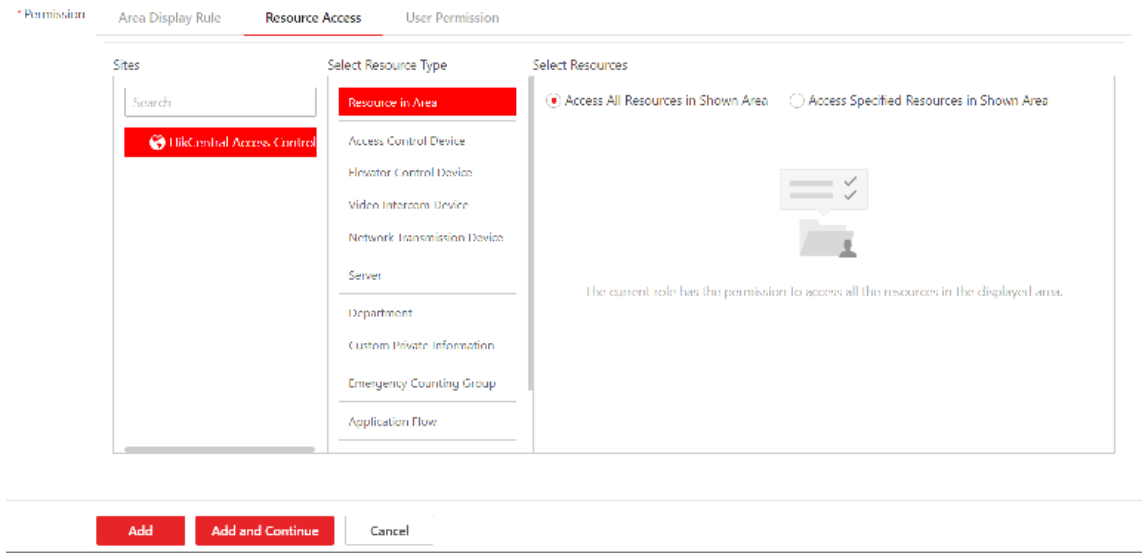


Figure 13-3 Resource Access

Note

If you do not check the resources, the resource permission cannot be applied to the role.

User Permission

Assign resource permissions, configuration permissions, and operation permissions to the role.

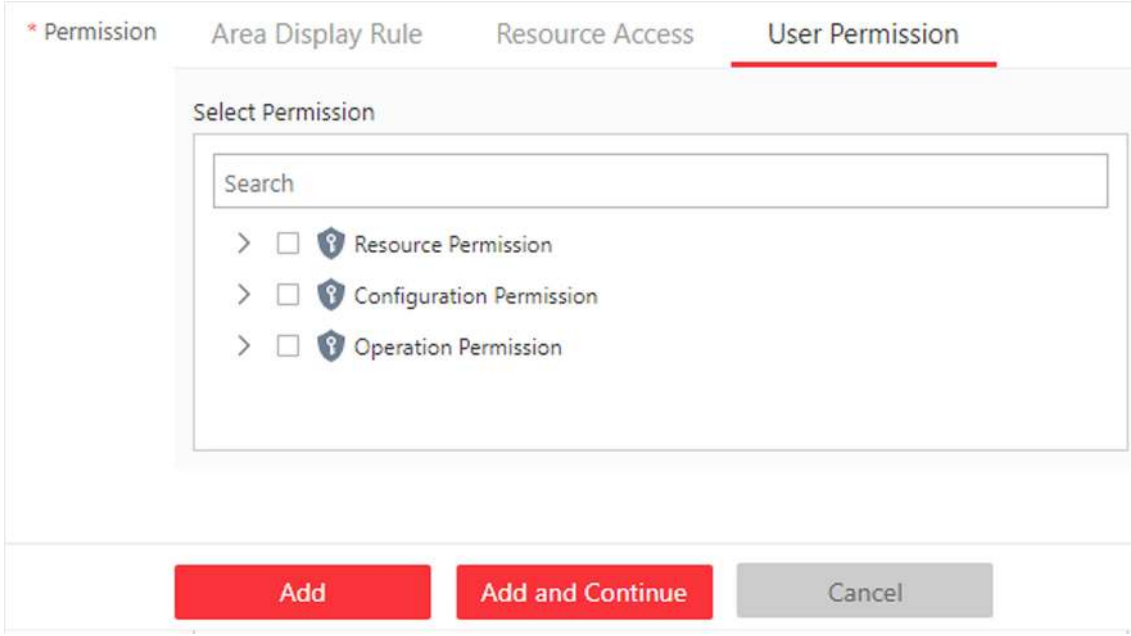


Figure 13-4 User Permission

6. Complete adding the role.
   - Click **Add** to add the role and return to the role management page.
   - Click **Add and Continue** to save the settings and continue to add another role.
7. **Optional:** Perform further operations on added roles.

Edit Role	Click a role name to view and edit role settings. **Note** The two default roles cannot be edited.
Delete Role	Check a role and click **Delete** to delete the role. **Note** The two default roles cannot be deleted.
Inactivate Role	Check a role and click **Inactivate** to set the role status to **Inactive**.
Activate Role	Check an inactive role and click **Activate** to set the role status to **Active**.

Refresh Role	Click **Refresh All** to get the latest status of the roles.
Filter Role	Click to expand the filter conditions. Set the conditions and click **Filter** to filter the roles according to the set conditions.

13.2 Add 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 top left corner of Home page, select → **All Modules** → **General** → **Account and Security** .
2. Click **Users** on the left.
3. Click **Add**.
4. Set basic information for the user.

User Name

Only letters (a-z, A-Z), digits (0-9), and "-" are allowed.

Password

Create an initial password for the user. The user will be asked to change the password when logging in for first time. See ***First Time Login for Normal User*** for details.

Note

We highly recommend you to create a strong 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.

Expiry Date

The date when the user account becomes invalid.

Email

The system can notify user by sending an email to the email address. The user can also reset the password via email.

Note

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 **Inactive**, the user account will be inactivated until you activate it.

Restrict Concurrent Logins

To limit the maximum IP addresses logged in to the system using the user account, switch on **Restrict Concurrent Logins** and set the maximum number of concurrent logins.

5. Configure permission settings for the user.

PTZ Control Permission

Set the permission level (1-100) for PTZ control. 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 of a camera.

Assign Role

Select the roles that you want to assign to the user.

Note

If you want to add new roles, click **Add**. See ***Add 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.

6. Do one of the following to complete adding the user.
   - Click **Add** to add the user and return to the user management page.
   - Click **Add and Continue** to save the settings and continue to add another user.
7. **Optional:** Perform further operations on the added normal users.

Edit User	Click user name to view and edit user settings.
Reset Password	Click user name and click **Reset** to set a new password for the user. Enter a new password and click **Reset**. **Note** The admin user can reset the passwords of all the other users (except domain user). Other users with Security permission (in Configuration and Control Permission) can reset the passwords of the users without Security permission. When the normal user's password is reset by admin user, he/she should change the initial password and set a new password when logging into HikCentral Professional via the Web Client.
Delete User	Select a users and click **Delete** to delete the selected user.
Force Logout	Select an online user and click **Force Logout** to log out the online user.
Inactivate/ Activate User	• The admin user or user with administrator permission can inactivate or activate a user. • Select an active users and click **Inactivate/Activate** to inactivate/activate the user.
Refresh User	Click **Refresh All** to get the latest status of all users.

Filter User Click to set conditions and filter the users.

13.3 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.

Before You Start

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

Steps

1. On the top left corner of Home page, select → **All Modules** → **General** → **Account and Security** .
2. Click **Users** on the left.
3. Click **Import Domain Users**.

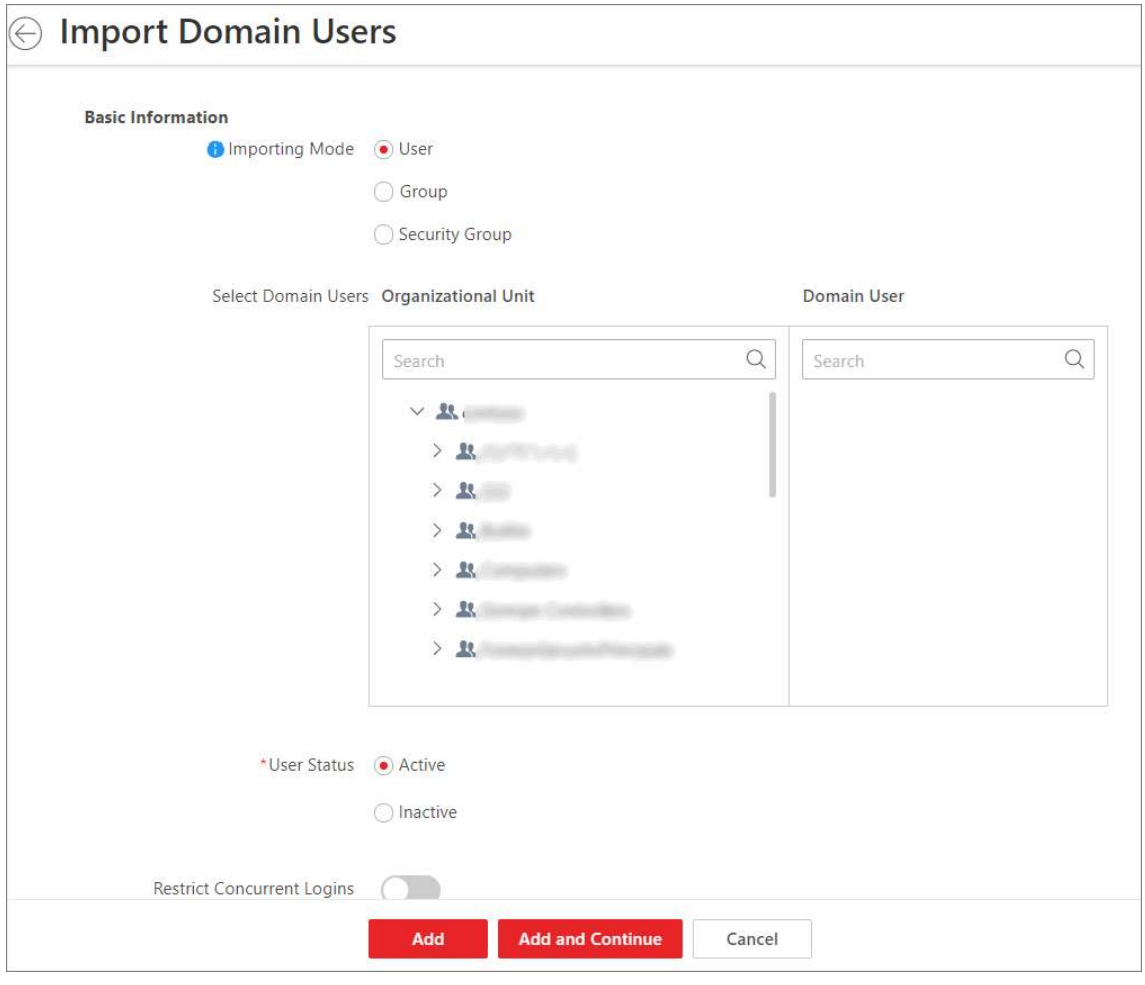


Figure 13-5 Import Domain Users

4. Select an importing mode.

   User

   Import individual users. Select an organization unit and select one or more domain users in this organization unit.

   Group

   Select an organization unit to import all the domain users in this organization unit.

   Security Group

   Import all the domain users in the security group(s). Select an organization unit and select one or more security groups in this organization unit.
5. Select domain users from active directory.
6. Select the user status as **Active** or **Inactive**.
7. **Optional:** 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.
8. Set the permission level (1-100) for PTZ control in PTZ Control Permission.

   Note

   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.

   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.
9. Select the roles that you want to assign to the domain users.

   Note

   - If no role has been added, two default roles are selectable: administrator and operator.

     Administrator

     The role that has all permissions of the HikCentral Professional.

     Operator

     The role that has all permissions of the HikCentral Professional Control Client.
   - If you want to add new roles, you can click **Add New Role**. See ***Add 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.
10. Complete importing the domain users.
    - Click **Add** to import the domain users and return to the user management page.
    - Click **Add and Continue** to save the settings and continue to import other domain users.
11. **Optional:** 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 latest user information from the domain group (including added users, deleted users, edited users, etc., in the group).

Result

After successfully adding the domain users, the users can log in to the HikCentral Professional via the Web Client and Mobile Client with their domain accounts and passwords.

13.4 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.

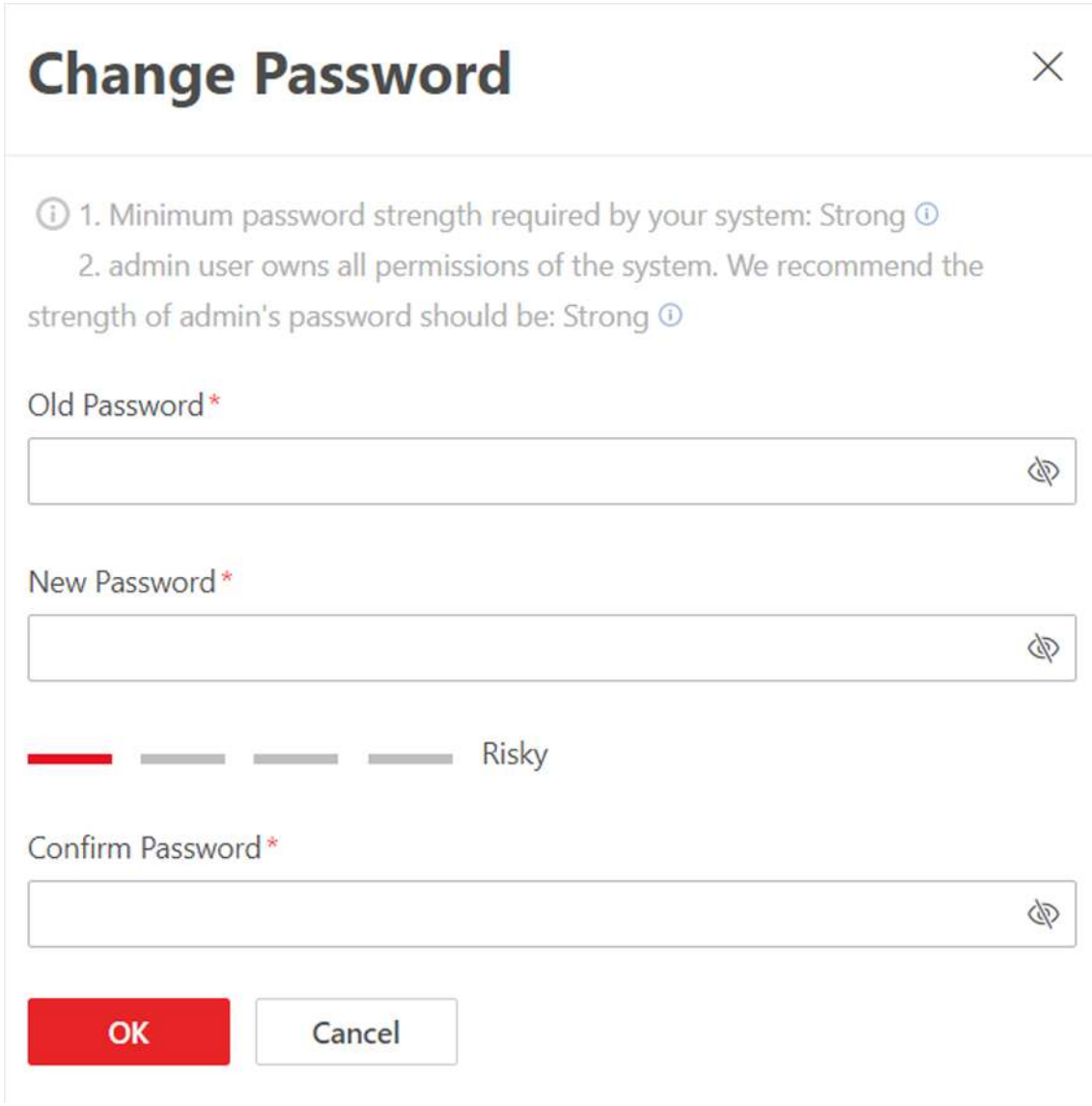


Figure 13-6 Change Password Panel

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.

13.5 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, Weekday Template, and Weekend Template. You can add new templates according to actual needs.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Account and Security** .
2. Click **Permission Schedule Template** on the left.
3. Click + .
4. Set basic information.

   Name

   Create a name for the template.

   Copy From

   Select the template from the drop-down list to copy the settings from another existing template.
5. In the **Weekly Schedule** area, set the weekly schedule as needed.
   1) Click **Authorize**, and select or draw in the box to define the authorized time periods.
   2) **Optional:** Click **Erase**, and select or draw on the authorized time periods to clear the selection.

   Note

   You can set up to 6 separate time periods for each day.
6. **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 New** to create a new holiday template (see ***Set Holiday*** for details).
   3) Click **Add**.
   4) Set the schedule for holidays.

   Note

   The holiday schedule has a higher priority than the weekly schedule.
7. Click **Add** to add the permission schedule template.
8. **Optional:** Perform further operations for the added templates.

View and Edit Template Details	Click the template to view and edit its configuration.

Note

Default templates cannot be edited.

Delete Template Click a template, and click to delete it.

Note

Default templates cannot be deleted.

What to do next

Set permission schedules for roles to define in which period the permissions for the roles are valid. For details, refer to ***Add Role*** .

Chapter 14 System Security Settings

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.

Steps

1. In the top left corner, select → **All Modules** → **General** → **Account and Security** .
2. Select **Security Settings** → **Basic Parameter** on the left.

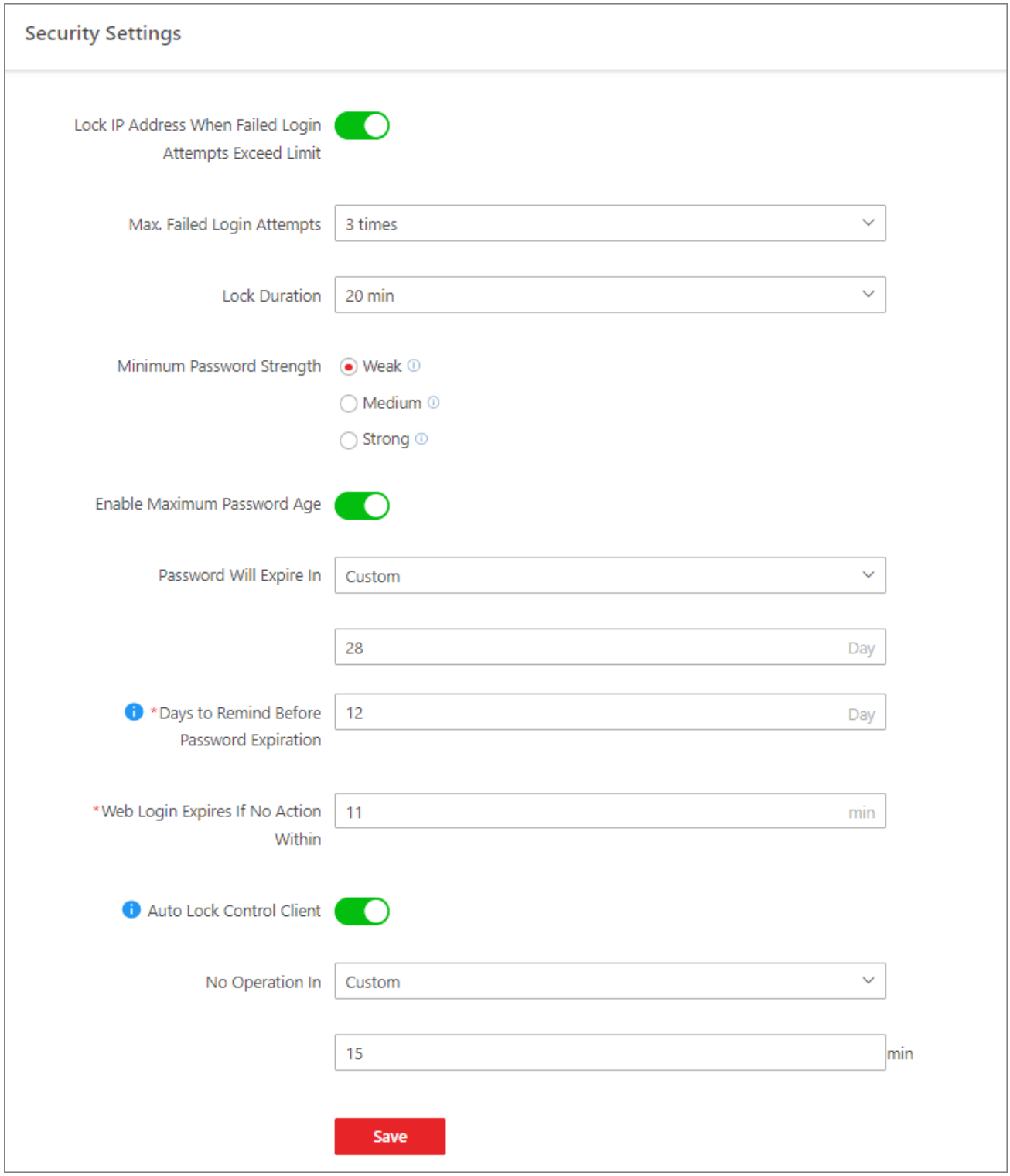


Figure 14-1 Security Settings Page

3. Switch on **Lock IP Address When Failed Login Attempts Exceeds Limits** to limit the number of failed login attempts.
   1) Select the maximum allowable login attempts for accessing HikCentral Professional.

   Note

   Failed login attempts include failed password attempt and failed verification code attempt.

   2) Set the locking duration for this IP address. During the locking duration, the login attempt via this IP address is not allowed.

   The number of login attempts is limited.
4. Select the **Minimum Password Strength** to define the minimum complexity requirements that the password should meet.
5. Set the maximum password age.
   1) Switch on **Enable Maximum Password Age** to force user to change the password when the password expires.
   2) Set the maximum number of days that the password is valid.

   Note

   After the maximum number of days, you should change the password. You can select the predefined time length or customize the time length.

   3) 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.
6. Set minutes after which the Web login will expire if there is no actions during the set minutes.
7. Configure the settings to automatically lock the Control Client after a time period of inactivity on the Control Client.
   1) Switch on **Auto Lock Control Client**.
   2) Select time period for user inactivity.

   Note

   You can select the predefined time period or customize the time period.
8. Configure double authentications by selecting the authenticator and the users who need authentication.

   Note

   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.

   1) Switch on **Double Authentications**.
   2) Click **Add** to enter the Add Authenticator panel.
   3) Select a user from the drop-down list, configure the authenticatable resource(s) and permission(s), and click **Add** to add the authenticator.
   4) Select the user(s) who need authentication.

9. Click **Save** to save the above settings.

Chapter 15 System Configuration

The System page allows you to set basic parameters for the system, such as defining a customized name for your site, setting the WAN IP address for allowing to access your system via WAN (Wide Area Network), and configuring NTP (Network Time Protocol) settings to synchronizing the time between the system and the NTP server.

- For the system with Remote Site Management module, you can enable it to receive the registration from Remote Site.
- For the system without Remote Site Management module, you can set to register it to the Central System as a Remote Site.

15.1 Set User Preference

For different nations, regions, cultures and enterprise backgrounds, the user preference might be different. You can set the user preference according to the actual scene, including the first day of a week and the temperature unit.

On the top, select **System**.

Select **Normal → User Preference** on the left.

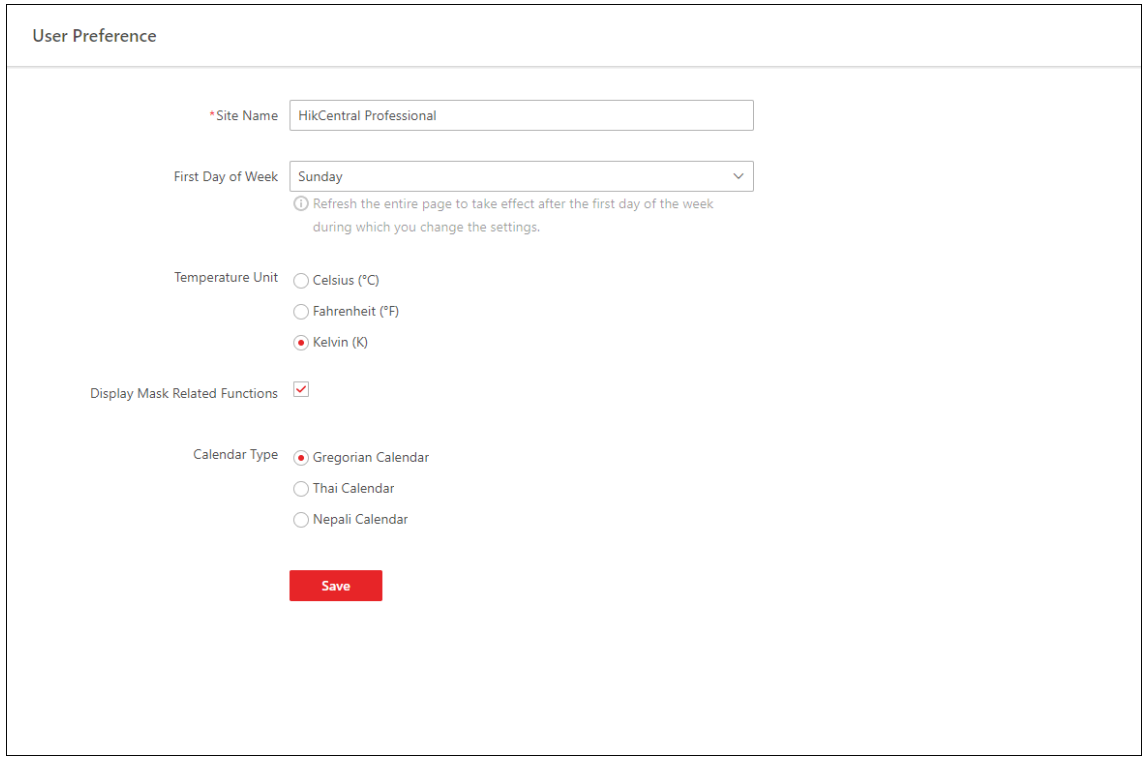


Figure 15-1 User Preference

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 intelligent analysis report generation, live view and playback, attendance settings, etc.

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.

15.2 Set Printer

You can set printer(s) for the system, which can be used to print the stranded person list in some urgent evacuation scenario, such as fire hazard.

Note

Make sure the printer(s) are installed in the same network with the SYS server.

On the top, select **System**.

Select **Normal → Printer Settings** on the left.

Click **Add** to select the printer(s) detected by the HikCentral Professional.

Note

After setting printer(s) for the system, you can link the printer when configuring alarm/event whose source type is alarm input. For details, refer to ***Add Normal Event and Alarm*** .

You can click in the Operation column to delete the printer.

You can also click **Delete All** to delete all printers.

15.3 Set NTP

You can set the NTP server for synchronizing the time between the resources (devices managed in the platform, recording servers, sites, SYS, etc.) and the NTP server.

Steps

Note

For devices added via Open Network Video Interface protocol, time synchronization will fail. Please configure the time on the device locally and make sure the device's NTP settings are the same as the platform's.

1. On the top, select **System**.
2. Select **Network → NTP** on the left.
3. Switch on **Time Synchronization** to enable the NTP function.
4. Set the NTP server address and NTP port.

   Note

   If the local NTP service has been configured, you can click **Detect Local NTP** to fill in the NTP server address and NTP port automatically.
5. Enter the interval for the automatic time synchronization.
6. **Optional:** Click **Test** to test the communication between the resources and the NTP server.
7. **Optional:** Switch on **Configure WAN Mapping** and enter the IP address and port 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.
8. Click **Save**.

15.4 Set Active Directory

If you have the 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 HikCentral Professional conveniently.

Steps

1. On the top, select **System**.
2. Select **Network → Active Directory** on the left.
3. Configure the basic information parameters to connect to the AD domain controller.

Domain Name

The domain name of the AD domain controller.

Note

- HikCentral Professional only supports the NetBIOS format, e.g., TEST\user, instead of the DNS Domain name format.
- To get the NetBIOS domain name, open the CMD window and enter ***nbtstat – n***. The NetBIOS domain name is the one in **GROUP** type.

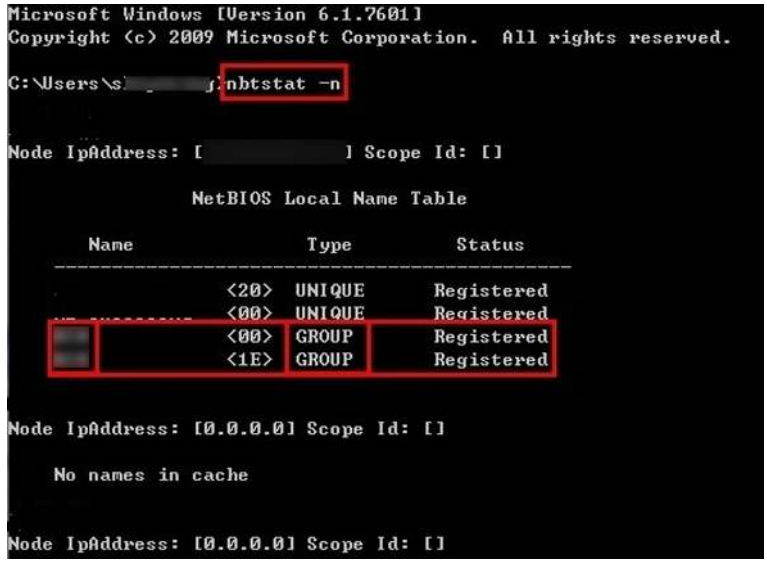


Figure 15-2 How to Get NetBIOS Domain Name

Host Name

The DNS server's IP address. You can get it in Network Connection Details.



Figure 15-3 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

The user name of the AD domain controller. The user should be the domain administrator.

Password

The password of the AD domain controller.

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. Click **Fetch DN** to have the filter condition entered automatically.
- 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.

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 in the system.
   1) Switch on **Linked Person Information**.

   The default and custom additional information items (see ***Object Missing***) are displayed in the Person Information area 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 new person information item is also displayed on the Custom Additional Information page, where you can edit or delete the items. Refer to ***Object Missing*** for details.
- The person information item is case-sensitive.

3) **Optional:** Click + to show the person information items stored in the domain.
4) Check the checkbox in the domain to link it to the added person information item when importing the domain's persons.
5) **Optional:** Hover over the linked person information in the domain and click × to remove the relationship. You can also change the relationship between each other by clicking and dragging one item to another.

6. Click **Save**.

After the configuration, the organization unit and domain user information will be displayed when you click **Import Domain User** on the User Management page.

If the Linked Person Information function is enabled, the corresponding person information in the system will match the linked person information in the domain and cannot be edited.

15.5 Device Access Protocol

Before adding devices supporting ISUP 2.6/4.0 to the system, you need to set the related configuration to allow these devices to access the system.

On the top, select **System**.

Select **Network → Device Access Protocol** on the left.

Switch on **Allow ISUP Registration**.

Check **Allow ISUP of Earlier Version**.

Note

The device may be attacked when accessing the system via ISUP of earlier versions.

Click **Save**.

15.6 Set Hik-Partner Pro Site Access

After setting Hik-Partner Pro Site access, you can add devices on the site of to the platform, and you can also add devices to the site of Hik-Partner Pro via the platform.

Steps

1. In the top-left corner of the Home page, select → **Basic Management → System → Network** .

2. Select Hik-Partner Pro **Access** on the left.

3. Switch on **Access on**Hik-Partner Pro to set required parameters.
4. Select the access mode.
   - Select **Key Access**, and enter the Hik-Partner Pro key.
   - Select **AccessKey/SecretKey Access**, and enter the access key and secret key of Hik-Partner Pro.
5. Enter the domain name where the account locates.
6. **Optional:** Switch on **Receive Event From Hik-Partner Pro** as needed.
7. **Optional:** Switch on **Synchronize Device with DDNS Configured** as needed.
8. Click **Save**.

15.7 Set WAN Access

In some complicated network environments, you need to set a static IP address or a domain name and ports for HikCentral Professional to enable it to access the SYS via WAN (Wide Area Network). For example, if the SYS is in a local area network, and you need to visit the platform via the Web Client or Control Client running in WAN, you should enable WAN access and set a static IP address or a domain name and ports for HikCentral Professional.

Steps

1. On the top, select **System**.
2. Select **Network → WAN Access** on the left.
3. Switch on **Access WAN** to enable the WAN access function.
4. Enter the IP address of the server for WAN access.
5. Enter a static IP address or a domain name of the server for WAN access.
6. Set the client communication port.

   HTTP

   Used for the Web Client and Control Client to access the platform via HTTP. By default, it is 80.

   HTTPS

   Used for the Web Client and Control Client to access the platform via HTTPS. By default, it is 443.

   Cluster Port Segment

   Used for translating the network address and mapping the platform to access via WAN. By default, the internal network port is 18020, and you should specify the port of WAN.

   Note

   If the port is conflicted, you can view the exception on **System → Maintenance** .
7. If you adopt generic events to integrate HikCentral Professional with external sources, you need to set the TCP port, UDP port, HTTP port, and HTTPS port for receiving the TCP, UDP, HTTP, and/or HTTPS data packages.

Note

For setting the generic event, refer to ***Add Generic Event*** .

8. **Optional:** For the platform with a Remote Site Management module, you can set the port to receive the registration from the Remote Site.

Note

This configuration item is only available for the Central System with a Remote Site Management module based on the License you purchased.

9. If you need to manage devices accessed via ISUP, you can set the ports for these ISUP devices, such as the registration port, alarm receiving port, and so on.

Port for Downloading Files from ISUP Devices

Used for downloading files from ISUP devices. By default, it is 8555.

ISUP Registration Port

Used for the ISUP devices registering to the platform. By default, it is 7660.

ISUP Alarm Receiving Port (TCP)

Used for receiving alarms from ISUP devices via TCP. By default, it is 7332.

ISUP Alarm Receiving Port (UCP)

Used for receiving alarms from ISUP devices via UCP. By default, it is 7334.

ISUP Streaming Port (via VAG)

Used for getting the stream from ISUP devices via the VAG server. By default, it is 7661.

ISUP Streaming Port (via Plugin)

Used for getting the stream from ISUP devices via the Plugin. By default, it is 16000.

ISUP Port for Two-Way Audio

Used for two-way audio between the platform and ISUP devices. By default, it is 16001.

Note

If the ISUP ports are disabled on the SYS, the ISUP related ports will not be displayed on the WAN Access page.

10. Set other ports.

Real Time Streaming Port

Used for getting the stream for live view via the Control Client. By default, it is 554.

ISUP Registration Port

Used for the ISUP devices registering to the platform. By default, it is 7660.

Local Picture Storage Port on Server(TCP)

Used for storing local pictures on the server. By default, it is 6123.

Local File Picture Storage Port on Server(TCP)

Used for storing local files on the server. By default, it is 6203.

11. Click **Save**.

15.8 Set IP Address for Receiving Device Information

You can select the NIC of the current SYS so that the platform can receive the alarm information of the device connected via ISUP account, and to perform live view and playback for the devices connected via ISUP account.

Before You Start
Make sure the server's ports ranging from 8087 to 8097 are available.

Steps
1. In the top left corner of Home page, select → **All Modules → General → System Configuration → Network → Address for Receiving Device Info** .
2. Select **Get from NIC** or **Enter Manually**.

   Get from NIC

   Usually, you can select **Get from NIC** to get IP address from the NIC of SYS.

   Select the currently used NIC name of SYS in the drop-down list. The NIC information including description, MAC address, and IP address will display.

   Enter Manually

   If you have configured hot spare for the SYS. Manually enter the IP address for receiving device information.
3. Click **Save**.

15.9 Set Records Storage Information

The data retention period specifies how long you can keep the events, logs, and some records in the SYS server, such as recording tags and vehicle entering/exiting records.

Steps
1. On the top, select **System**.
2. Select **Storage → Records Storage** on the left.
3. Set the data retention period from the drop-down list for the required data types.

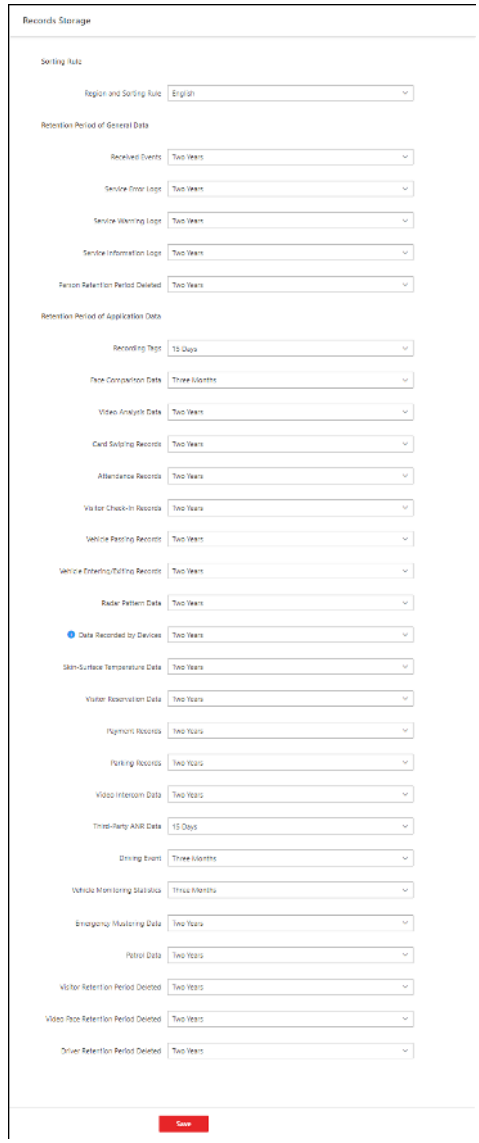


Figure 15-4 Set Data Retention Period

4. Click **Save**.

15.10 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.

On the top, select **System**.

Select **Normal → Holiday Settings** on the left.

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.
Click **Add** to open the adding holiday dialog.
Enter the holiday name and select **Regular Holiday** as the holiday type.
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 system will generate the date of the holiday according to the date of the VSM server.

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.
Click **Add** to open the adding holiday dialog.
Enter the holiday name and select **Irregular Holiday** as the holiday type.
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 the SYS server.

Note

If you check **Repeat Annually**, the specified date of this holiday will be generated automatically according to the current year of the SYS server.
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**.

15.11 Set Card Template

You can set the styles for card templates. After settings, the card will be applied in the format of the template.

Steps

1. On the top, select → **Basic Management** → **System** .
2. Select **Normal** → **Card Template** on the left.
3. Click **Add**.
4. Create a name for the template.
5. **Optional:** Select the shape of the template.
6. 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. You can set the font and the font size for the text after clicking the text field.
Content	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	Set the text style as needed. You can set the text to bold, align content,etc.

Note

- You can drag any edge or corner to adjust the size of the picture and text box.
- You can select one or multiple text boxes on the template and click , , or to adjust the alignment of the text in the box.
- You can select multiple elements on the template and click , , or to adjust these elements.
- You can right-click on the element (except the background picture) and click **Stick on Top**, **Stick at Bottom**, **Move Up**, or **Move Down** to adjust the layer of the element displayed on the template.

7. **Optional:** Set the back style of the template.

Note

You can set the back style according to step 5.

8. Click **Add** to add the template and go back to the card template list page.

   The email template will be displayed on the card template list.
9. **Optional:** Perform the following operation(s).

View Template	Click to view the template.

Edit Template	Click in the Operation column to edit template details.
Delete Template	Click in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

Note

On the card template list page, there are two default templates. You can view default templates but cannot edit or delete them.

15.12 Set Email Template

Before sending report or sending event message to the designate email account(s) as email linkage, you should set the email template properly. The email templates include template for sending report and template for sending event message as linkage action when the event is triggered. The email template specifies the recipient, email subject, and content.

15.12.1 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. In the top-left corner of the Home page, select → **All Modules** → **General** → **System Configuration** → **Email** → **Email Settings** .

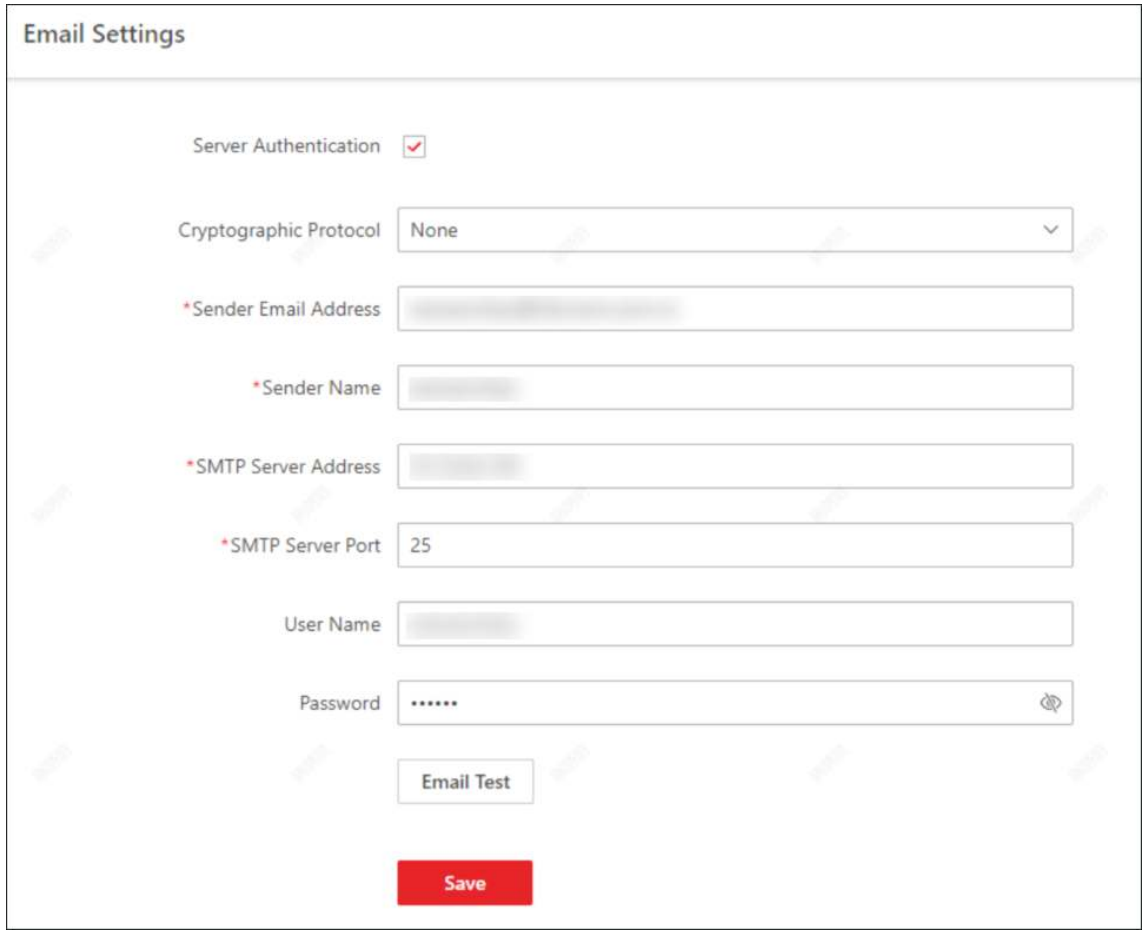


Figure 15-5 Email Settings

2. Configure the parameters according to actual needs.

Server Authentication (Optional)

If your mail server requires authentication, check this checkbox to use authentication to log in to this server.

Cryptographic Protocol

Select the cryptographic protocol of the email to protect the email content if required by the SMTP server.

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 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.

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.

3. Click **Email Test** to test whether the email settings work or not.

   The corresponding attention message box will pop up.
4. Click **Save**.

15.12.2 Add Email Template for Sending Report Regularly

You can set email templates (including specifying the recipient, email subject, and content) for sending the report regularly, so that the platform can send the report as an email attachment to the designated recipient regularly according to the predefined email template.

Before You Start

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. In the top-left corner of the Web Client, select → **Basic Management** → **System** .
2. On the left navigation pane, click **Email** → **Scheduled Report Email Template** .
3. Click **Add** to enter the Add Email Template page.

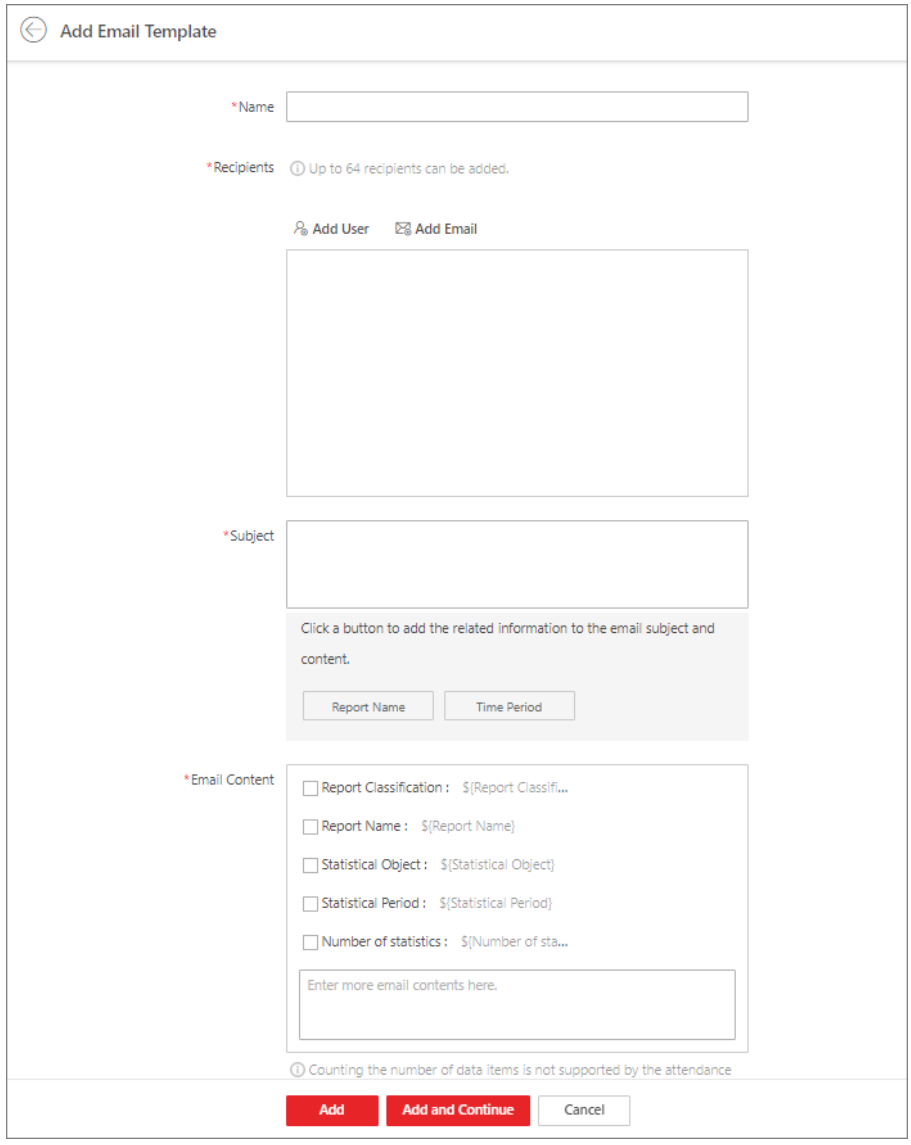


Figure 15-6 Add Email Template for Sending Reports Regularly

4. Enter the required parameters.

Name

Create a name for the template.

Recipients

- Click **Add User** and select the person's email, which is configured when adding the person.
- Click **Add Email** and enter the recipient email address to send the email to.

Note

You can enter multiple recipients and separate them by ";".

Subject

Enter the email subject as desired. You can also click buttons below to add the related information to the subject.

Email Content

Define report contents to be sent. In the Email Content field, check the content type(s) (i.e., Report Classification, Report Name, Statistical Object, Statistical Period, and Number of Statistics) to add the related information to the content and enter more detailed contents in the text box to complete the design of report contents.

Note

If you add the time period to the email subject or add the statistical period to the email content, and the email application (such as Outlook) and the platform are in different time zones, the displayed period may have some deviations.

5. Finish adding the email 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.
6. **Optional:** Perform the following operation(s) after adding the email template.

Edit Template	Click in the Operation column to edit template details.
Delete Template	Click in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

15.12.3 Add Email Template for Event and Alarm Linkage

You can set email templates (including specifying the recipient, email subject, and content) for event and alarm linkage. 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.

Before You Start

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. In the top of top left corner of Home page, select → **All Modules** → **General** → **System Configuration** → **Email** → **Event and Alarm Email Template** .
2. Click **Add** to enter the Add Email Template page.
3. Enter the required parameters.

   Name

   Create a name for the template.

   Recipients

   Click **Add User** and select the person's email as the recipient, which is configured when adding the person.

Click **Add Email** and enter the recipient(s) email address to send the email to.

Note

You can enter multiple recipients and separate them by ";".

Subject

Enter the email subject as desired. You can also click the button in the lower part of the window to add the related information to the subject.

Email Content

Define the event or alarm information to be sent. You can also click buttons below the **Email Content** parameter to add the related information to the content.

Note

If you add the event time to the email subject or content, and the email application (such as Outlook) and the platform are in different time zones, the displayed event time may have some deviations.

4. **Optional:** Check **Attach Captured Picture** to send email with image attachment.
5. Select a content language to define the language of the sent content.
6. Finish adding the email 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 on the email template list.
7. Perform the following operation(s) after adding the email template:

Edit Template	Click in the Operation column to edit template details.
Delete Template	Click in the Operation column to delete the template.
Delete All Templates	Click **Delete All** to delete all the added templates.

15.13 Set Transfer Protocol

You can set the SYS server's transfer protocol to define the access mode for the SYS (via Web Client, Control Client, or Mobile Client) as HTTP or HTTPS. The HTTPS protocol provides higher data security.

Steps

1. In the top left corner of Home page, select → **All Modules** → **General** → **System Configuration** → **Security** → **Transfer Protocol** .
2. In the **Clients and SYS Transfer** field, select **HTTP** or **HTTPS** as the transfer protocol between the clients (Web Client, Control Client, and Mobile Client) and the SYS servers

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.

3. If you select **HTTPS**, you are required to set the certificate. You can use the system provided certificate, or select **New Certificate** and click to select a new certificate file.

Note

- The new certificate should be in PEM format.
- The public key and private key should be in the same certificate file.

4. **Optional:** You can add the upper-level certificate as needed.
   1) Click **Add**.
   2) Click to select the file.
   3) Click **Confirm**.
   4) **Optional:** Select the added certificate(s) and click **Delete** to delete.
   5) **Optional:** In the Operation column, click to download the certificate.
5. Click **Save**.
   - The SYS server will reboot automatically after changing the clients and SYS server transmission settings.
   - All the users logged in will be forced to log out during reboot. The reboot takes about one minute and after that, the users can log in again.

15.14 Export Service Component Certificate

For data security, before adding the Streaming Server or Cloud Storage Server to the system, you should generate the service component certificate stored in the SYS server and input the certificate information to the Streaming Server you want to add, or export the service component certificate stored in the SYS and import the certificate to the Cloud Storage Server, so that the certificates of the Streaming Server, Cloud Storage Server and SYS server are the same.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **System** .
2. Select **Security** → **Service Component Certificate** on the left.
3. Click **Generate Again** beside **Certificate between Services in System** 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. For the following operations, see ***Add Streaming Server*** for details.

4. Click **Export** to export the service component certificate in XML format and save it in the local PC.

Note

On the Cloud Storage Server you want to add, import the service component certificate you export. For more details, see ***Manage Cloud Storage Server*** .

15.15 Set Database Password

You can set the database password of the system on the Web Client running on the SYS server.

Note

Setting database password is only available when you access the Web Client on the SYS server locally.

In the top left corner of Home page, select → **All Modules** → **General** → **System Configuration** → **Security** → **Database Password** .

Enter the password and then click **Verify** to generate the verification code and enter the verification code.

15.16 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 the SYS service, you can enable the hot spare function and configure the hot spare property of the current SYS server as host server or spare server. When the host server fails, the spare server switches into operation, thus ensuring the stability of the system.

Steps

1. In the top left corner of Home page, select → **Basic Management** → **System** → **Advanced** → **Hot Spare** .
2. Set the **Hot Spare Configuration** switch to ON to enable the hot spare function.

   The current SYS server's server name and available IP address will be displayed.
3. Set the server as host server or spare server in Hot Spare Property.
4. Click **Save**.

15.17 Set Third-Party Integration

HikCentral Professional supports integrating third-party resources (such as camera, door, etc.) via Optimus. Also, the system provides open platform to integrate the third-party system. By the Open APIs (application programming interface) provided on the open platform, the third-party system can obtain some functions (such live view, playback, alarm, etc.) of HikCentral Professional, to develop more customized features.

In the top left corner of Home page, select → **Basic Management** → **System** .

Select **Third-Party Integration** on the left.

Note

- Setting open platform is only available when you access the Web Client on the SYS server locally.
- Only admin/administrator users have the permission to perform this function.

Integrate via Optimus

Select **Integrate via Optimus** on the left panel, and switch on the **Integrate via Optimus**.
Configure related parameters in the Optimus software. For details, refer to the *User Manual of Optimus*.
The default icons of resources integrated from the third-party will be displayed. Hover the cursor over the default icon and click Click to change the resource icons according to your need.

Open Platform

Note

Setting open platform is only available when you access the Web Client on the SYS server locally.

Select **Open API** on the left panel, switch on **Open API**, and set the IP address of the open platform, management port of the open platform, and the partner user.

Note

- The open platform should be deployed in the same network with the SYS server.
- The third-party system integrates the HikCentral Professional by the partner user(s) you select, which defines the permission(s) of resources and operations in the HikCentral Professional.

Click **Test** to test the service availability of the open platform.
Click **Save** to save the settings.

15.18 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.

15.18.1 Synchronize Card Swiping Records to Third-Party Database

You can enable synchronization function to apply the card swiping records of specified resources from HikCentral Professional to the third-party database automatically.

Steps

1. In the top left corner of Home page, select → **All Modules → General → System Configuration → Third-Party Integration → Data Interchange** .
2. Switch on **Data Interchange** to enable data interchange function.
3. Click **Add** and select the resource(s) for card swiping records synchronization.

Note

You can click in the Operation column to delete the resource or click **Delete All** to delete all added resources.

4. Select the encoding format of data interchange.
5. **Optional:** Check **Do Not Push Failed Records**.

   The failed records will not be pushed to the third-party system.
6. Select **Database Synchronization**.
7. **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.
8. **Optional:** Select **Database Type** from the drop-down list to set the database type.
9. Set the required parameters of the third-party database, including server IP address or domain name, server port, database name, user name, and password.
10. Click **Test Connection** to test whether database can be connected.
11. 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.
12. Click **Save**.

    The data will be written to the third-party database.

15.18.2 Dump Access Records to Third-Party Database

The access records of specified resources can be dumped as a CSV file or TXT file and the third-party system will read the dumped file (instead of accessing the database and mapping the table fields) for further applications, such as attendance calculation and pay 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. In the top-left corner of the Home page, select → **All Modules → General → System Configuration → Third-Party Integration → Data Interchange** .

2. Switch on **Data Interchange** to enable the data interchange function.
3. Click **Add** and select the resource(s) for card swiping records synchronization.

Note

You can click in the Operation column to delete the resource or click **Delete All** to delete all added resources.

4. Select the encoding format of data interchange.
5. **Optional:** Check **Do Not Push Failed Records**.

The failed records will not be pushed to the third-party system.

6. Select **Access Record Dump**.
7. 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 server. 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 server 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 card swiping records.

Dump Time

The time when dumping card swiping records is started.

8. Click **Add**.

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.

9. Click **Save**.

15.19 Diagnose Remote Fault

When faults occur in HikCentral Professional, you can get the system information using the authentication code generated by HikCentral Professional to help diagnose the system faults.

On the top, select **System**.

Select **Advanced → Diagnosis & Maintenance** on the left.

Switch on **Remote Fault Diagnosis** to generate an authentication code for remote diagnosis. It will be canceled automatically after 60 minutes.

Note

The authentication code will be refreshed every time you switch on **Remote Fault Diagnosis**.

Launch Postman, create a new request, set the HTTP method to POST, and enter the request URL (format: ***http://<host>[:port]/ISAPI/Bumblebee/Platform/V1/TranckTaskInfo?&MT=GET***).

Then in the Body area, enter the request message in JSON format (set the **trackModuleNmae** to the module name and set the **AccessKey** to the authentication code generated on HikCentral Professional), and click **Send**.

The response message is returned in the Body area of Response and it shows the system running information. You can perform fault diagnosis remotely according to the information.

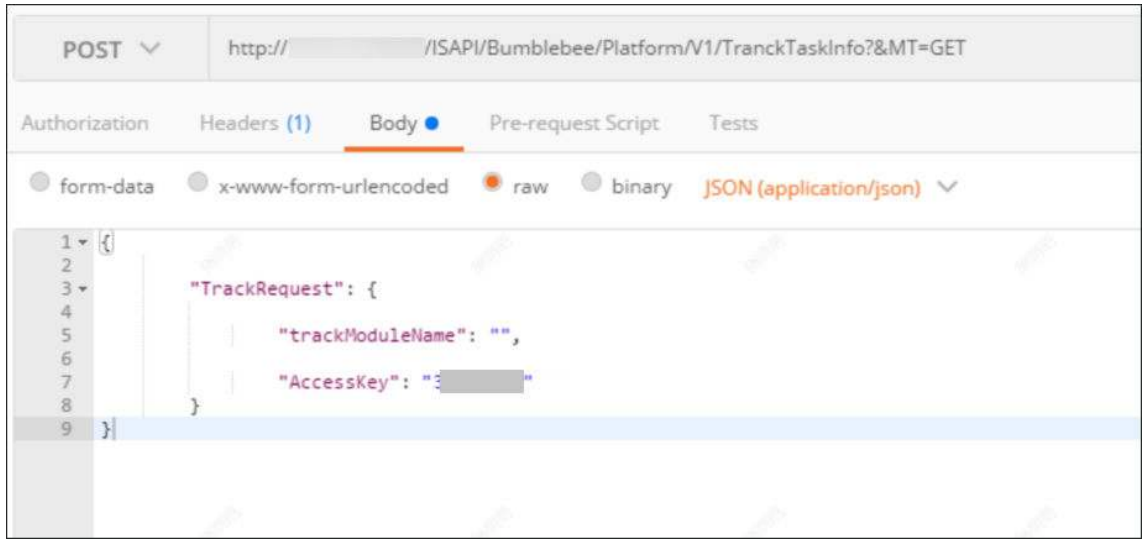


Figure 15-7 Get System Running Information Using Postman

15.20 Reset Device Network Information

When system network domain changes (such as server migration), you must reset the network information of the added device to adapt to the new network environment. Otherwise the device live view, playback and other functions will be affected.

Perform this task when you need to reset the network information of the added device.

Steps

1. In the top left corner of Home page, select → **All Modules** → **General** → **System Configuration** → **Advanced** → **Reset Network Information** .
2. Click **Reset** to one-touch reset the device network information.

15.21 Set Company Information

You can configure and show the company information on the Web Client for customization requirements.

In the top left corner of Home page, select → **All Modules** → **General** → **System Configuration** → **Company Information** to enter the Company Information Settings page.

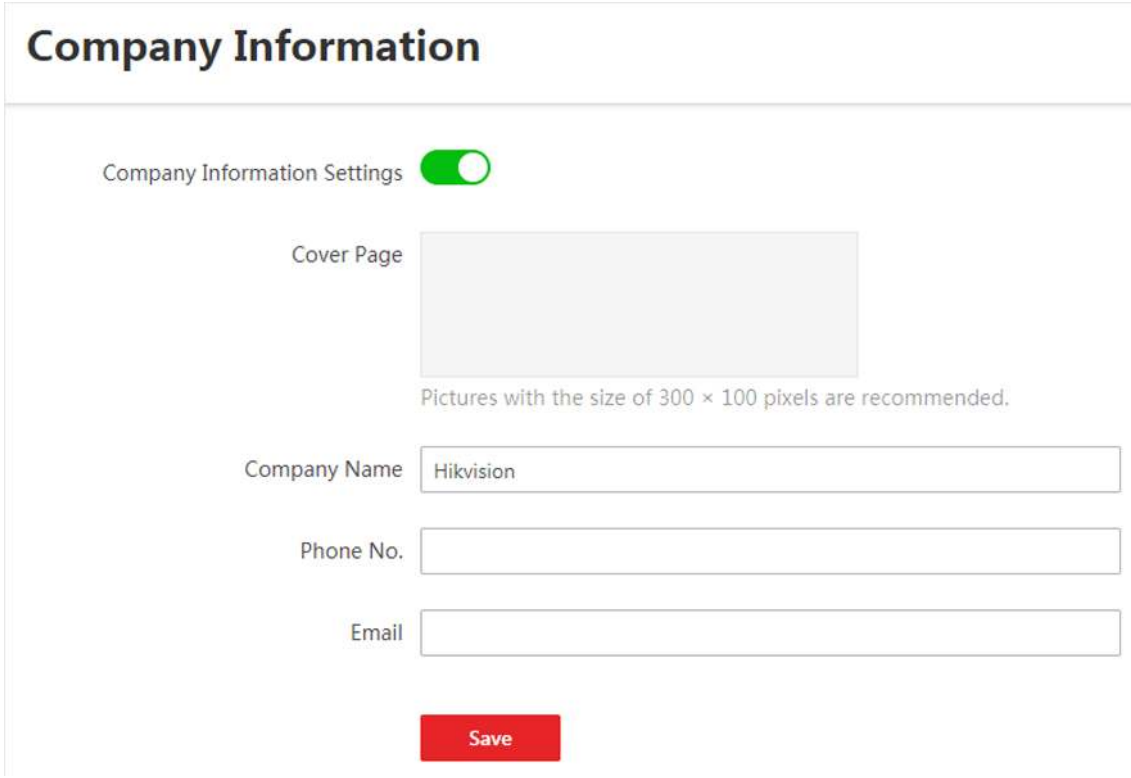


Figure 15-8 Company Information Settings

Switch on **Company Information Settings** to enable displaying company information on the Web Client. And 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.

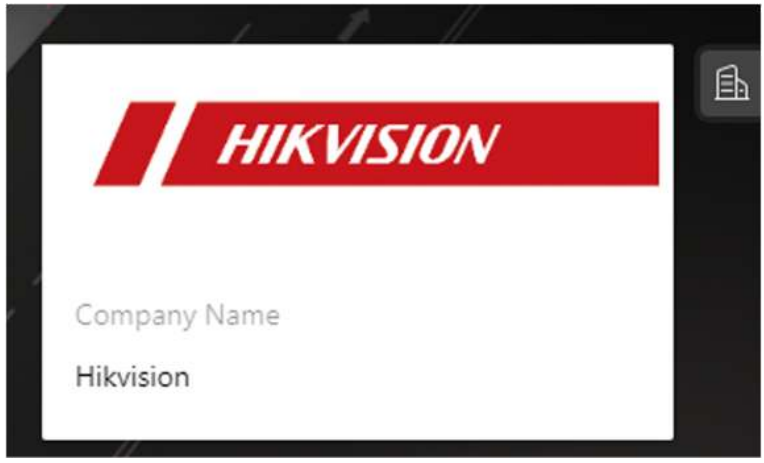


Figure 15-9 Company Information Displayed on Web Client

Chapter 16 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 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 (e.g., camera, alarm input) placed on the map are called hot spots) geographic locations in the real world. GIS map lets you view and access cameras 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 (e.g., camera, alarm input) 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.

16.1 Configure Map

You need to configure GIS maps and e-maps before using them. You can add hot spots, hot regions, labels, resource groups, entrance and exit, combined alarms, and remote sites to the maps.

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 navigation bar, select → **Security Monitoring → Visual Map** .
2. Select **Map** on the left panel.
3. Click **Map Settings** on the top right to enter the map settings page.
4. 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 provides 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**.

5. Click **Icon Settings** to set the customized icons.
1) Click **Hot Region** or the following device types 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 path.

   Note

   The icon picture format can only be PNG, JPG, or JPEG.
4) **Optional:** Click to constrain the aspect ratio.
5) Click **Save**.

Result

You can view the GIS map on Map Monitoring page and perform the following operations in the map area.

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	Hover over a resource, and you can view its latitude and longitude on the GIS map.

16.1.2 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.

Before You Start

Make sure you have disabled the GIS Map function. See ***Set GIS Map and Icons*** for details.

Steps

1. In the top left corner of Home page, select → **Visual Monitoring → Map → Map Settings** to enter the map settings page.
2. Select an area on the left.
3. 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.
4. Select an adding mode.
5. 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.
6. Click **Add**.
7. **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 **Calibrate** 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.
8. **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.

9. **Optional:** Perform the following operations after adding map in the map area.

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	Drag the map or the red window in the lower part to adjust the map area for view.

16.1.3 Add Hot Spot on 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. Refer to ***Add E-Map for Area*** for details about adding e-map.

Steps
1. In the top left corner of Home page, select → **All Modules** → **Map** → **Map Settings** 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. Refer to ***Add Security Radar to Area for Current Site*** and ***Add Hot Spot on Map*** for details.

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** .
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.

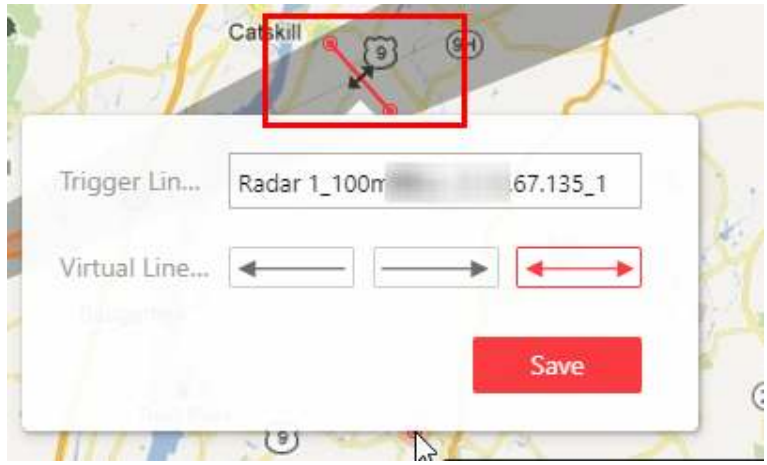


Figure 16-2 Trigger Line in the Detection Area

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.

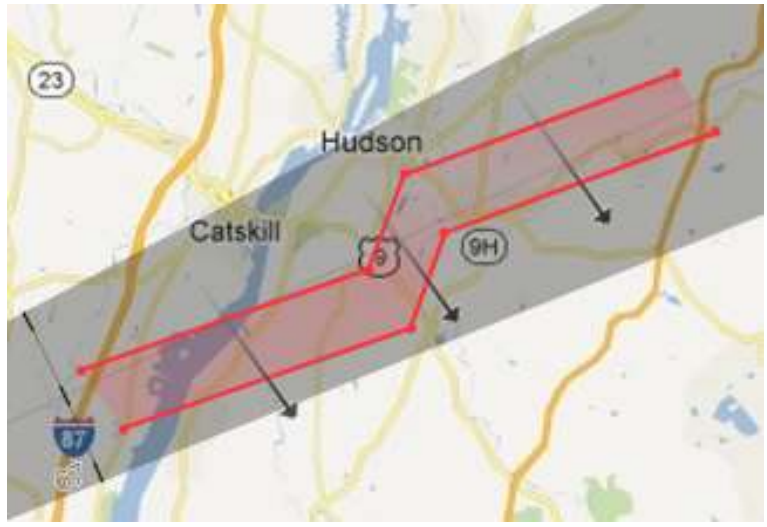


Figure 16-3 Dual-Trigger Line in the Detection Area

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.

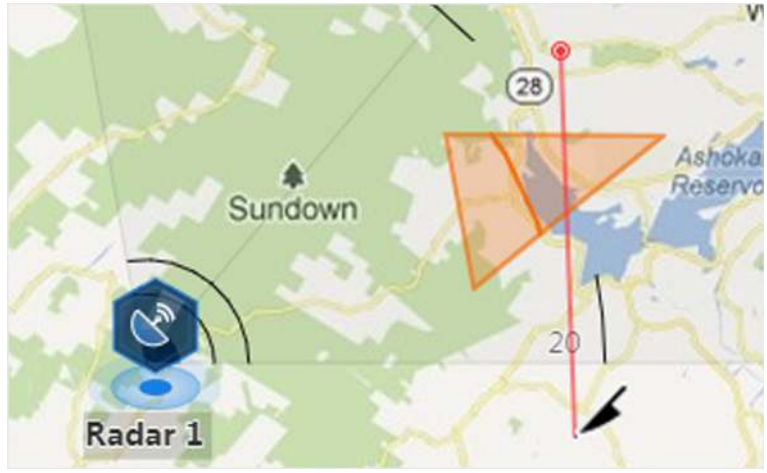


Figure 16-4 Zone Segmentation

Distance Segmentation

Split a zone into two smaller zone by an arc.

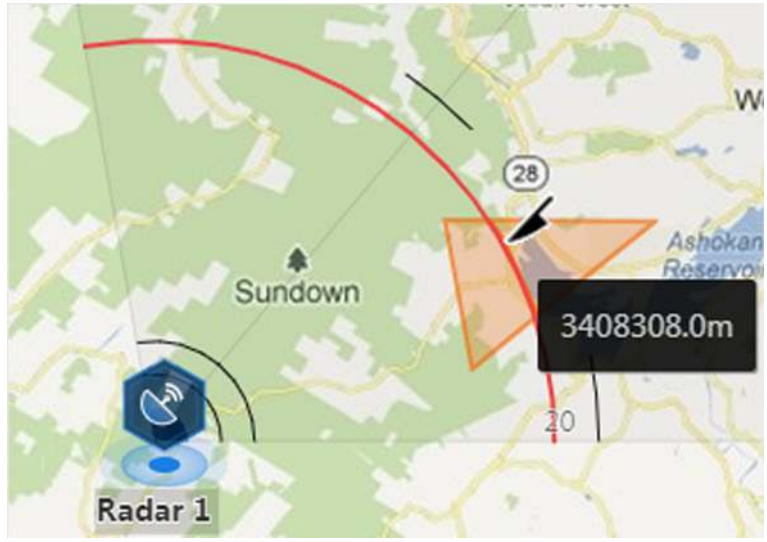


Figure 16-5 Distance Segmentation

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. Refer to ***Add Security Radar to Area for Current Site*** and ***Add Hot Spot on Map*** for details.

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** .
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.

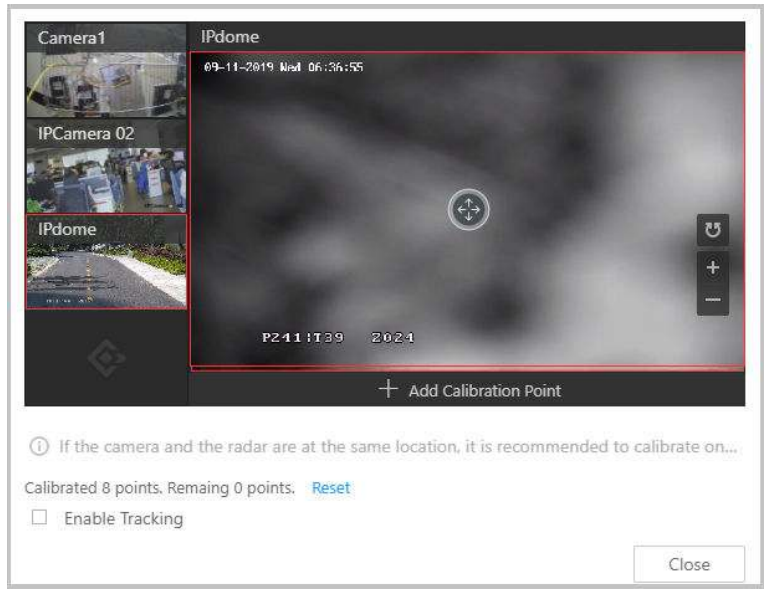


Figure 16-6 Add Calibration Point

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.

16.1.4 Add Hot Region on 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. Refer to ***Add E-Map for Area*** or ***Set GIS Map and Icons*** for details about adding maps.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Map** → **Map Settings** 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, and refer to for details), 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.

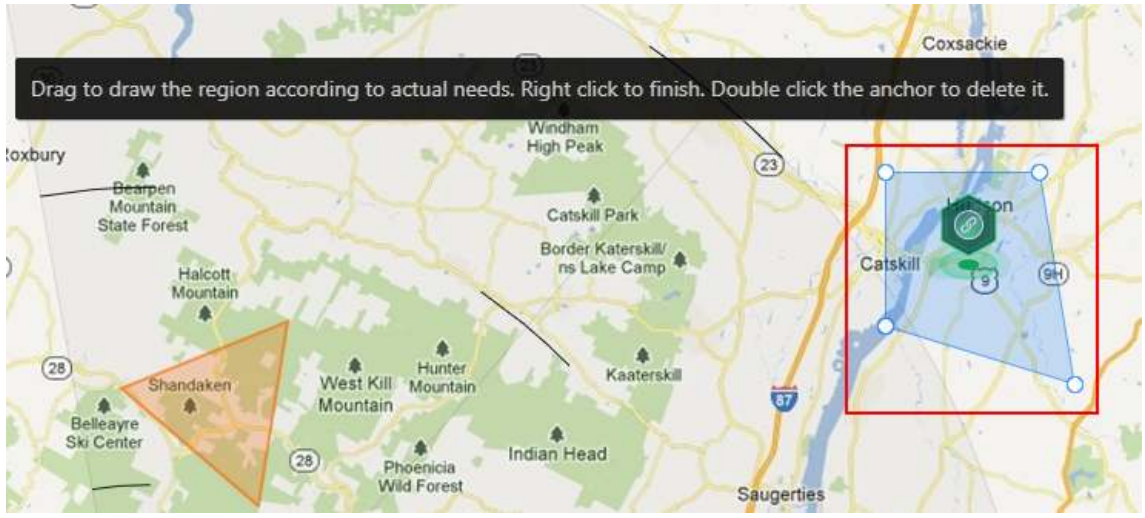


Figure 16-7 Edit Hot Region Area

16.1.5 Add Label on Map

You can add labels with description on the map.

Before You Start

At least one map should have been added. Refer to ***Add E-Map for Area*** or ***Set GIS Map and Icons*** for details about adding e-maps or GIS maps.

Steps

1. In the top left corner of Home page, select → **All Modules → Map → Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a static map.
4. Click **+** on the **Label** icon on the right.
5. Click on the map where you want to place the label.
6. Customize a name for the label, and you can input content for the label as desired.
7. Click **Save**.

   The added label icon will be displayed on the map.
8. **Optional:** Perform the following operation(s) after adding the label.

Adjust Label Location	Drag the added label on the map to the desired locations.
Edit Label	Click the added label icon on the map to view and edit the detailed information, including name and content on the appearing dialog.
Delete Label	Click the label icon on the map and click **Delete** on the appearing dialog to delete the label.

16.1.6 Add Resource Group on Map

You can also add the resource groups on the map by locating the resources in the group on the map and setting the border of the region for detection.

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.

For details about how to add a people counting group on the map, refer to ***Add People Counting Group*** .

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.

For details about adding a heat analysis group, refer to ***Add Heat Analysis Group*** .

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.

For details about how to add a pathway analysis group, refer to ***Add Pathway Analysis Group*** .

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.

For details about adding a person feature analysis group, refer to ***Add Person Feature Analysis 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 Area Anti-Passback Rules*** .

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***

Entry & Exit 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 Entry and Exit Counting Group*** .

Emergency Operation 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 Emergency Operation Group*** .

Security Control Partition (Area)

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*** .

16.1.7 Add Parking Lot on 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. Refer to ***Add E-Map for Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** 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.

16.1.8 Add Combined Alarm on Map

You can add the combined alarms on map to locate the alarm for a visualized monitoring.

Before You Start

Make sure you have added a map. Refer to ***Add E-Map for Area*** or ***Set GIS Map and Icons*** for details about adding e-map or GIS map.

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** to enter the map settings page.
2. Select an area on the left.
3. **Optional:** Select a map.
4. Click **Combined Alarm** on the right.
5. Drag a combined alarm to the map.

   The combined alarm is displayed on the map.
6. **Optional:** Perform the following operations after adding the combined alarm.

Adjust Combined Alarm Location	Drag the added combined alarm on the map to the desired locations.
Edit Combined Alarm	Click the added combined alarm 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 Combined Alarm	Click the combined alarm icon on the map and click **Delete** to remove the combined alarm from the map.

16.1.9 Add Remote Site on 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. See ***Set GIS Map and Icons*** for details.

Steps
1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Settings** 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.

16.2 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.

16.2.1 View and Operate Hot Spot

You can view locations of hot spots including cameras, alarm inputs, alarm outputs, access points, elevators, radars, sites, Under Vehicle Surveillance Systems (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. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Monitoring** .
2. 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.
3. Select a map to enter the map.
4. **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. **2D/3D**: Switch the displaying dimension of the map. Search : Search hot spot or location on the map.

5. Click the 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.

6. 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 Control Client can receive the triggered alarm information from the hot spot. 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.
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 to play the audio file immediately if it is a local file.



Figure 16-8 Arm Hot Spot / View History Alarm



Figure 16-9 Broadcast via Hot Spot

16.2.2 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 **Select Map** 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 to enter the map of the hot region.

16.2.3 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*** .

In the top left corner of Home page, select → **Visual Map → Map → Map Monitoring** .

- 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 Control Client.
- Pathway Analysis Group: You can view the real-time number of people walking by in the Monitoring module on the Control 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 Control 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 Control 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 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.

16.2.4 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. See ***Add Remote Site on GIS Map*** for details.

Steps

1. In the top left corner of Home page, select → **Visual Map** → **Map** → **Map Monitoring** 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.

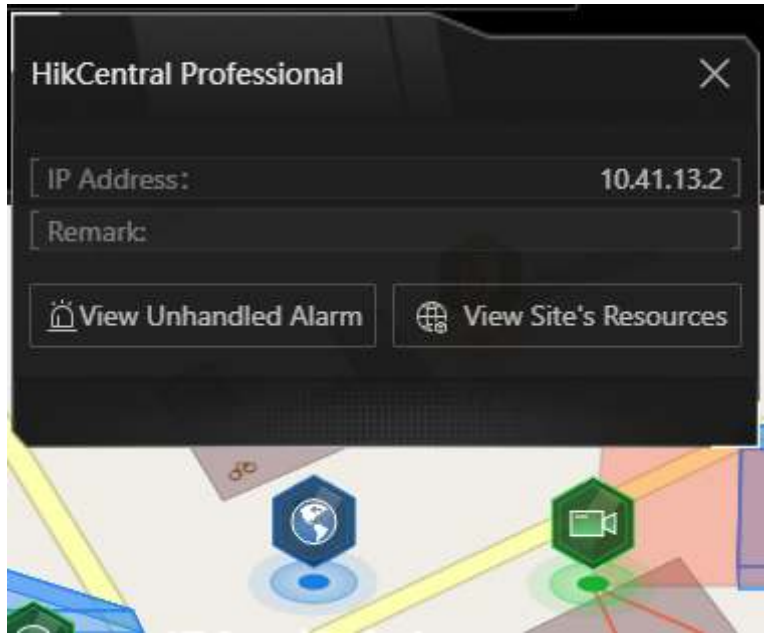


Figure 16-10 Site Details

The color of site icon will turn blue.

4. Click **View Unhandled Alarm** to open the Unhandled Alarm window.

   Alarm information including alarm name, alarm priority, triggering time, alarm source, etc. is displayed.
5. **Optional:** Perform the following operation(s).

Filter Alarm by Priority	Click on the Alarm Priority column to filter alarms by alarm priority.
Filter Alarm by Status	Click on the Alarm Status column to filter alarms by alarm status.

16.2.5 Operate Map

After opening map, you can perform one or more operations of the followings, such as zooming in or out map, adding label, displaying map in full screen mode, and so on.

Zoom in/Zoom out Map

Use the mouse wheel or click + or − to zoom in or zoom out on the map.

Filter

Click and select the resource type you want to show on the map.

Add Label

Click to add a label with description to the map.

Search Location

With the search bar on the top of the map, you can search for locations on GIS map and hot spot / hot region on the e-map by entering keyword(s).

On the top left of the map, enter a location name you want to search in the field. The related locations will display in the search field.

Click to select the location you want to locate from the related locations, and the location will be located on the map.

Chapter 17 AR Management

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.

17.1 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** .

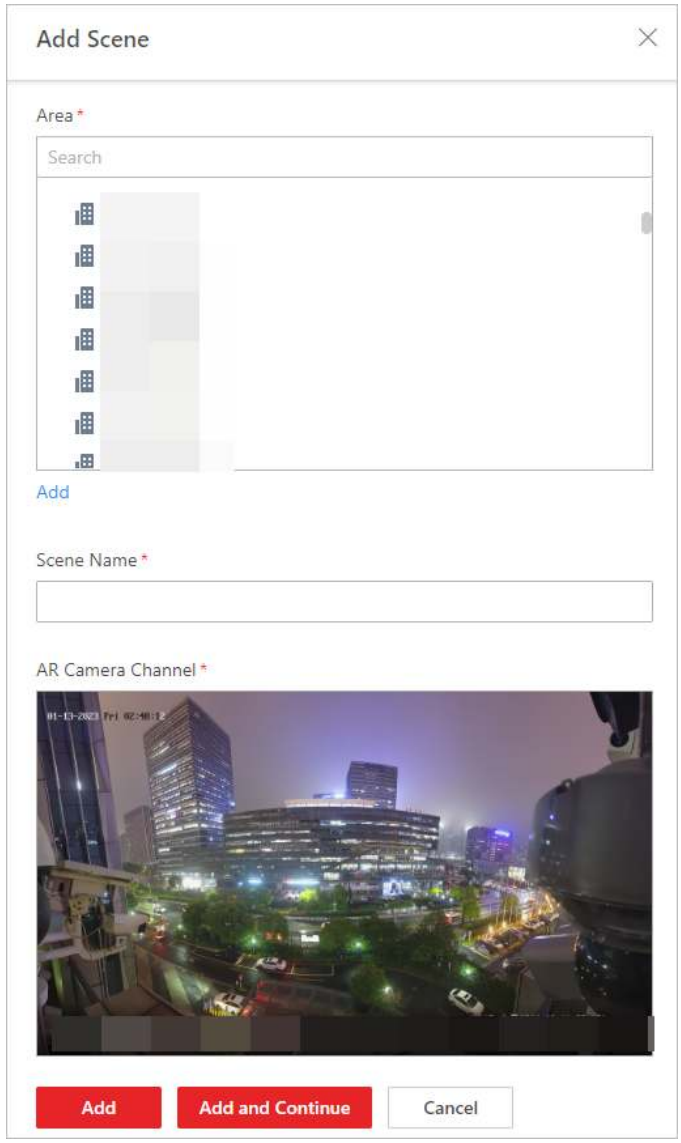


Figure 17-1 Add Scene

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*** .

17.2 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.

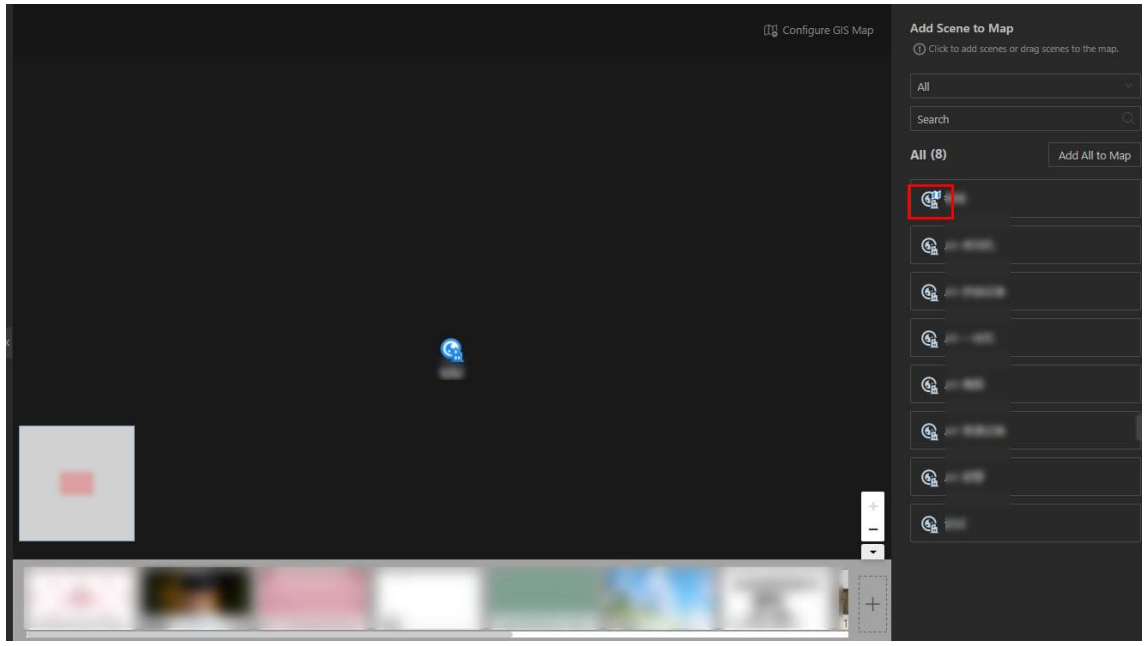


Figure 17-2 Icon of Added Scene

4. Click **Finish**.

Chapter 18 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.

18.1 Health Monitoring

Health monitoring 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.

18.1.1 Real-Time Health Status Overview

In the Health Monitoring 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.

In the top left corner of the client, select → **All Modules → Maintenance → Health Monitoring → Real-Time Overview** .

Click **Real-Time Overview** tab at the top to enter the Real-Time Overview page.

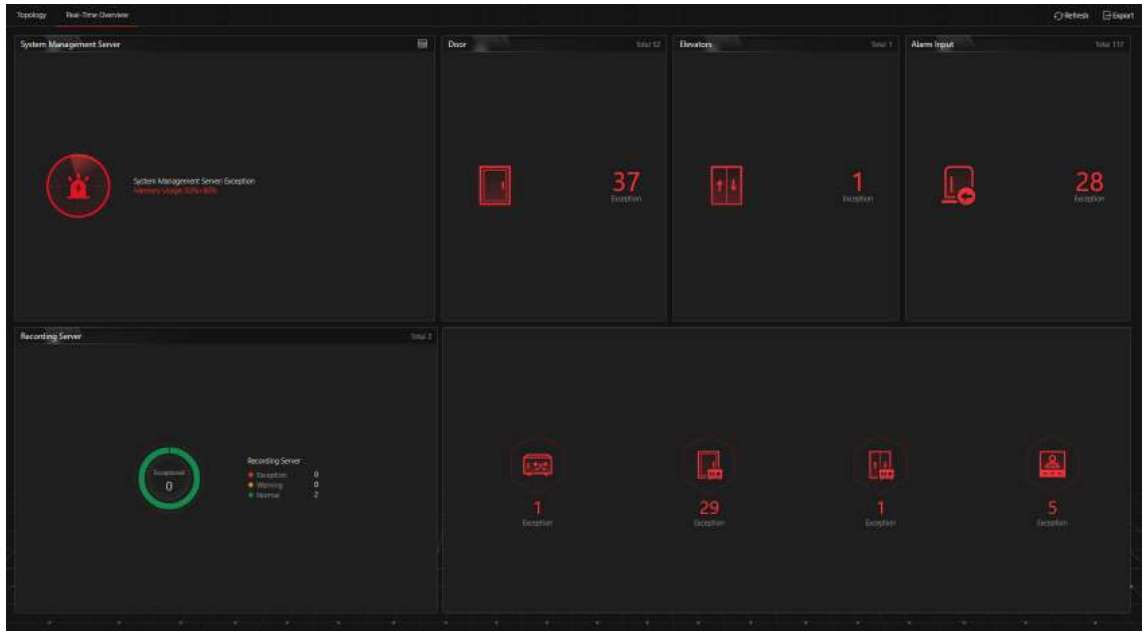
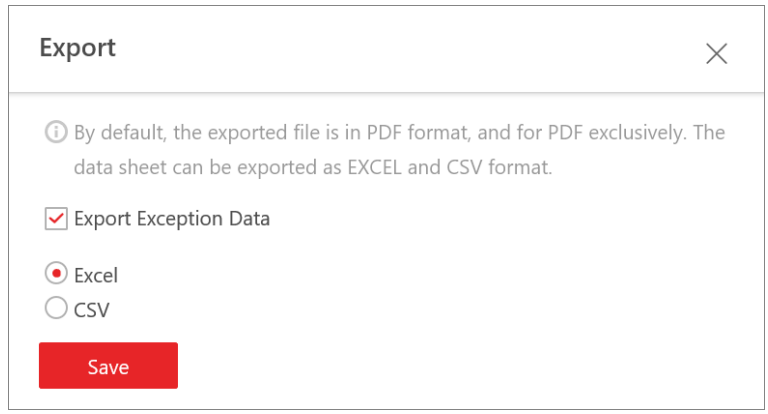


Figure 18-1 Real-Time Health Status Overview

Table 18-1 Real-Time Health Status Page

Section	Description
Resource Status	View the abnormal data of different resources (e.g., cameras, doors, elevators, or alarm inputs) added to the areas of Central System in the graphical way. You can click the numbers and status types on the chart to view the real-time status details of resources or Remote Sites. **Note** The Remote Site status is only available for the Central System with Remote Site Management module (based on the License you purchased).
System Management Server Status	View the network health status and server running status. Click in the upper right corner of System Management Server panel to view the running status details of the server, including CPU usage, RAM usage, etc.

Section	Description
	 **Figure 18-2 System Management Server Status Details**
Server Status	View the status (i.e., exception, warning, normal) of servers added on Central System. You can click the numbers and status types on the chart to view the real-time status details of servers.
Device Status	View the abnormal data of different devices added on Central System. You can click the numbers on the chart to view the real-time status details of devices. 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*** .
Select Sites	Select one or multiple Sites (including Remote Sites) from the drop-down list in the upper left corner of Real-Time Overview page to display the status of resources on the selected Site(s).
Refresh	• Manually Refresh: Click **Refresh** in the upper right corner of Real-Time Overview page to manually refresh the resource status on the page. • 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 Health 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.  **Figure 18-3 Export Overview Page or Exception Data**

18.1.2 Real-Time Health Status Overview (Topology)

In the Health Monitoring 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 top left corner of the client, select → **All Modules** → **Maintenance** → **Health Monitoring** → **Real-Time Overview** .

Click **Topology** tab at the top to enter the Topology page.

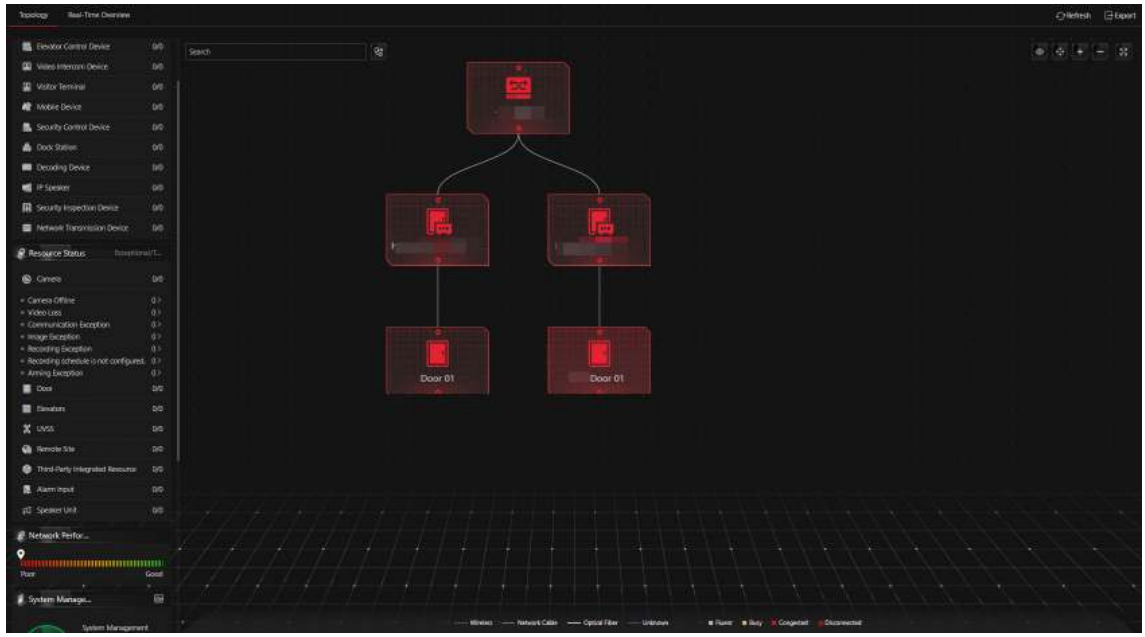
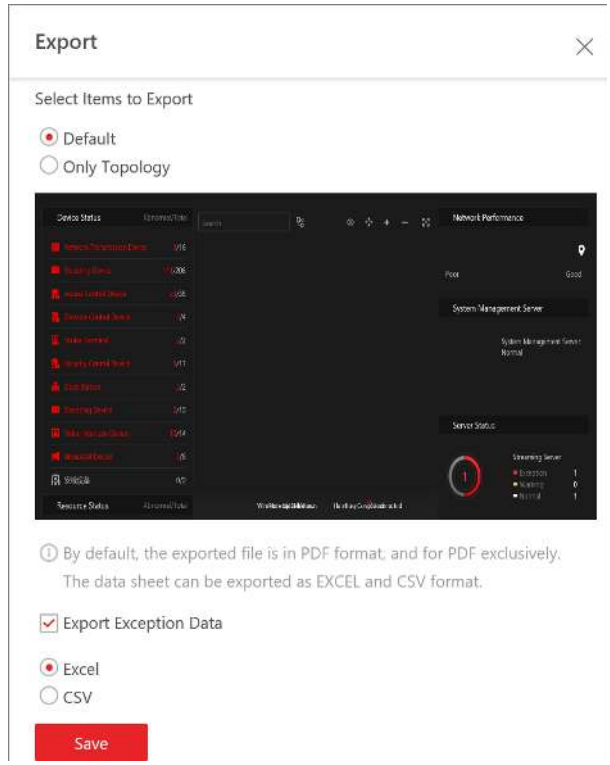


Figure 18-4 Topology Overview

Table 18-2 Topology Page

Section	Description
Device Status	View the abnormal data of different devices (e.g., encoding devices and decoding device) added on the Central System. You can click the number to locate the abnormal device in the topology or view the devices' real-time status. 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 (e.g., cameras, doors, elevators, or alarm inputs) added to the areas of the Central System. You can click the number to view the real-time status details of resources or Remote Sites. **Note** The Remote Site status is only available for the Central System with the Remote Site Management module (based on the License you purchased).
Topology Details	View the relationships among devices, device information, link status, alarm information, etc. See details in ***Topology Details*** .

Section	Description
Network Performance	View the current network performance (i.e., poor or good) of the System Management Server.
System Management Server Status	View the network health status and server running status. Click in the upper right corner of the System Management Server panel to view the running status details of the server, including its CPU usage, RAM usage, etc.  **Figure 18-5 System Management Server Status Details**
Server Status	View the status (i.e., exception, warning, normal) of servers added on the Central System.
Generate Topology Again	Click **Refresh → Generate Topology Again** to draw the network topology again.
Refresh	• Manual Refresh: Click **Refresh** in the upper right corner of the Real-Time Overview page to manually refresh the resource status on the page. • 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 Health Check Frequency*** .
Export Topology or Exception Data	Click **Export** in the upper right corner of Topology page and select the export type as **Default** or **Only Topology** to export the topology in PDF format or the exception data in Excel/CSV format.

Section	Description
	Note • If the export type is selected as **Default**, the whole displayed information (topology and exception data) on the Health Monitoring page will be exported. • If the export type is selected as **Only Topology**, only the topology will be exported in PDF format.  **Figure 18-6 Export Topology**

Topology Details

The topology of devices will display the hierarchical relationships among the devices, device information, link status, alarm information, etc.

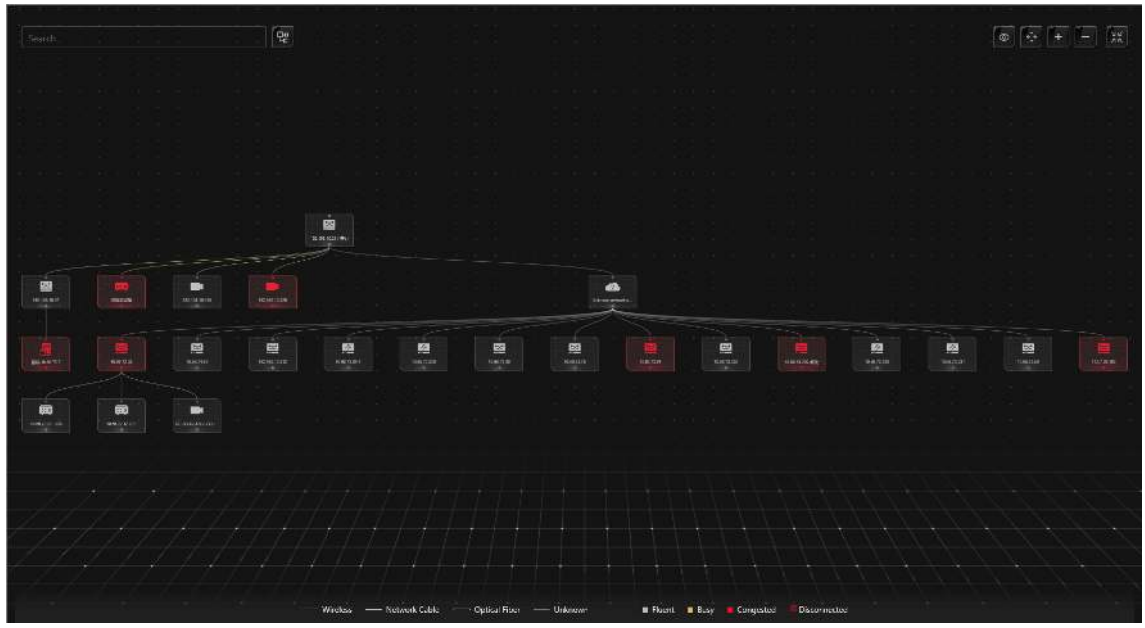


Figure 18-7 Topology Details

Device Node

The device nodes are displayed by icons, including the System Management Server, Recording Server, network transmission device, encoding device, access control device, video intercom device, network bridge, fiber converter, etc. Each device node displays the device name and IP address.

Note

- When the device information (device name, IP address, online/offline status) changes, you should manually refresh to generate the topology again or set auto-refresh.
- When the device hierarchy or physical connection changes, you should manually refresh to generate the topology again.
- If the node icon is displayed in red, it indicates that the device is abnormal or alarms are triggered. You can view the reason for device exception or alarm details.
- For the added online devices, the displayed device alias is the same as the device IP address.

View Device Details

Click the device node in the topology and click **Details** in the drop-down list. You can view the 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).

Note

The device details vary with different device models.

Link

The color of link indicates the utilization rate of network bandwidth (red: congested, yellow: busy, gray: fluent). And the shape of link indicates the link type (wireless, network link, optical fiber).

View Link Details

Move the cursor to the link between nodes to display the link details. You can view the upstream rate and downstream rate to determine whether the network status is normal or not. You can also view the connected device type, IP address, port name, and port status.

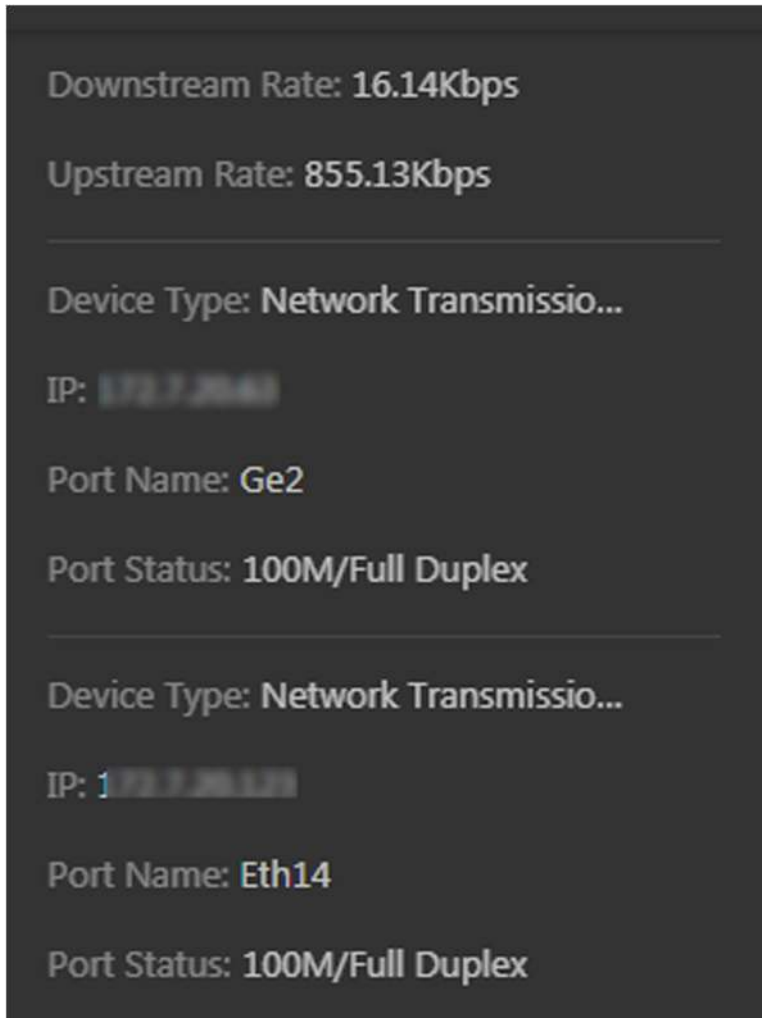


Figure 18-8 View Link Details

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, so as to restore the link as quickly as possible. Click the device node and in the topology and click **Show Connection Path** in the drop-down list. 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.

Remote Configuration

Click the device node in the topology and click **Remote Configuration** in the drop-down list to configure the 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.

Note

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. Click the device node in the topology and click **View Device Logs** in the drop-down list to enter the Device Logs page, and you can set the conditions to search the device logs.

Note

This function should be supported by the device.

Set as Root Node

When you need to adjust the topology structure, you can click the device node in the topology and click **Set as Root Node** in the drop-down list to set the node as the root node.

Note

Only the switch, wireless network bridge, and fiber converter can be set as root node.

Zoom In/Zoom Out

Click + or − to zoom in or zoom out the device node(s) and the subsidiary device node(s). You can scroll the mouse wheel to zoom in or zoom out the topology.

Adjust Topology

Click the background of the topology to move the topology in up, down, right, or left direction.

Full Screen

Click on the upper-right corner of the topology to display the topology in full-screen mode.

Adaptive View

Click on the upper-right corner of the topology to adapt the topology to the current window, to help you know the whole topology hierarchy quickly.

Search

By entering the device name or IP address in the search box, you can quickly locate the device on the topology.

18.1.3 Historical Health Data Overview

You can view the historical online rate of resources and devices, or the recording integrity rate.

On the top, select → **Basic Management** → **Maintenance** .

Select **Health Monitoring** → **History Overview** on the left.

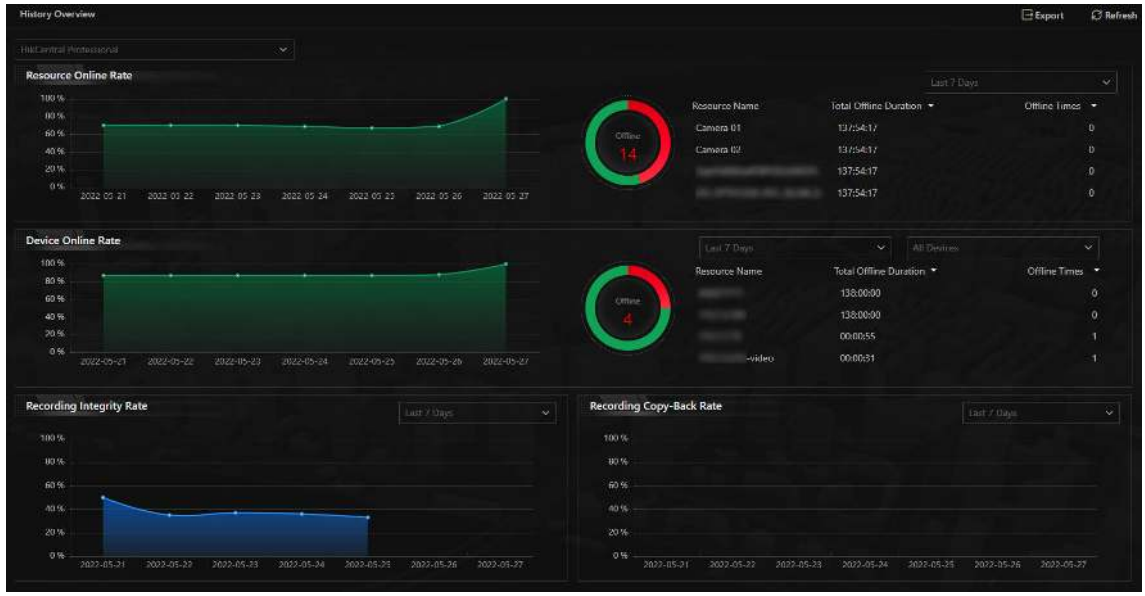
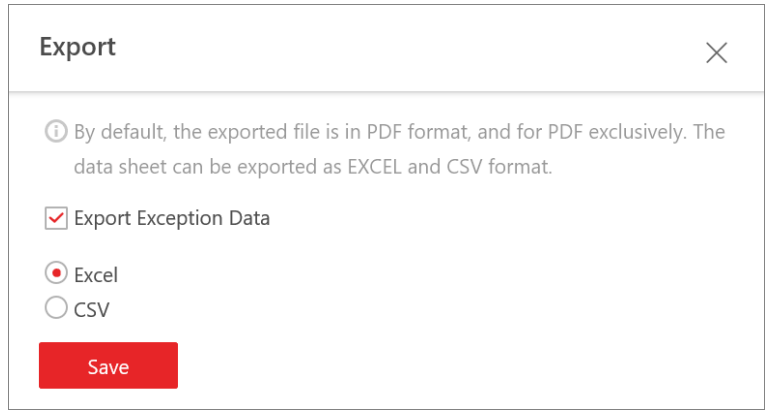


Figure 18-9 Historical Health Data Overview

Table 18-3 Historical Health Data Page

Section	Description
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. ◦ 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. • On the doughnut chart, you can perform the following operations: ◦ 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. ◦ 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. • On the table, you can do one of the followings: ◦ Click **Total Offline Duration** to rank the cameras in terms of total offline duration within the time period you select. ◦ 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. ◦ Move the cursor on the line chart to view the device online rate and the number of offline devices at specific time points. ◦ 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. • On the doughnut chart, you can perform the following operations. ◦ 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. ◦ 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. • On the table, you can do one of the followings. ◦ Click **Total Offline Duration** to rank the devices in terms of total offline duration within the time period you select. ◦ Click **Offline Times** to rank the devices in terms of offline times within the time period you select.

Section	Description
Recording Integrity Rate	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.
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.
Refresh	• Manually Refresh: Click **Refresh** in the upper right corner of History Overview page to manually refresh the data on the page. • 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 Health 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.  **Figure 18-10 Export Overview Page or Exception Data**

18.2 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.

18.2.1 Send Log Report Regularly

You can configure parameters to send device and resource log reports to specified users regularly via email. Device log reports contain information on the online/offline status of device, and resource log reports contain the online/offline status of resources as well as the recording status.

Send Resource Log Report Regularly

You can set report sending rules for camera resources, and the platform can send emails with resource log reports to specified users daily, weekly, or monthly.

Before You Start

- Make sure you have set an email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Make sure you have configured 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 records in total.
- The report is an Excel file.

1. On the top, select → **Basic Management** → **Maintenance** .
2. Select **Basic Configuration** → **Scheduled Report** on the left.
3. Click + to create a new report rule.

   Note

   If there is no report rule added before, you should click **Add** to add a new one.
4. In **Report Category**, select **Resource Logs**.
5. Edit the report rule.

   Report Target

   Specify the resources that you want to add into the report.

   Statistical Cycle

Select the generation frequency of the report.

By Day

The report shows data on a daily basis. 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 **Send On**, 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 **Send At**, 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 **Recent 7 Days**.

Report Time

Set the time period during which the logs will be recorded.

Send On

Set the report sending date(s) if you have set **Statistical Type** as **By Day**.

Send At

Set a report sending time.

Effective Period

Set the effective period for the report rule.

Send Report via Email

Switch on to send the report via email.

Email Template

Select an email template to define the recipient information and content if you have switched on **Send Report via Email**.

Note

You can click **Add** to add a new email template. For setting email templates, refer to ***Set Email Template*** .

Upload to SFTP

Switch on to upload the report to SFTP.

Note

You can click **Configure** to set the SFTP.

Save to Local Storage

Switch on to save the report to the local PC.

Note

You can click **Configure** to set the saving path.

6. Click **Add** to save the report rule.

Send Device Log Report Regularly

You can set report sending rules for encoding devices, and the platform can send emails with device log reports to specified users daily, weekly, or monthly.

Before You Start

- Make sure you have set an email template with recipient information, subject, and content. For details, refer to ***Set Email Template*** .
- Make sure you have configured 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 records in total.
- The report is an Excel file.

1. On the top, select → **Basic Management** → **Maintenance** .
2. Select **Basic Configuration** → **Scheduled Report** on the left.
3. Click + to create a new report rule.

Note

If there is no report rule added before, you should click **Add** to add a new one.

4. In **Report Category**, select **Device Logs**.
5. Edit the report rule.

Report Target

Specify the devices that you want to add into the report.

Statistical Cycle

Select the generation frequency of the report.

By Day

The report shows data on a daily basis. 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 **Send On**, 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 **Send At**, 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 **Recent 7 Days**.

Report Time

Set the time period during which the logs will be recorded.

Send On

Set the report sending date(s) if you have set **Statistical Type** as **By Day**.

Send At

Set a report sending time.

Effective Period

Set the effective period for the report rule.

Send Report via Email

Switch on to send the report via email.

Email Template

Select an email template to define the recipient information and content if you have switched on **Send Report via Email**.

Note

You can click **Add** to add a new email template. For setting email templates, refer to ***Set Email Template*** .

Upload to SFTP

Switch on to upload the report to SFTP.

Note

You can click **Configure** to set the SFTP.

Save to Local Storage

Switch on to save the report to the local PC.

Note

You can click **Configure** to set the saving path.

6. Click **Add** to save the report rule.

18.2.2 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.

In the top left corner of Home page, select → **All Modules → General → Maintenance → Basic Settings → Server Usage Thresholds** .

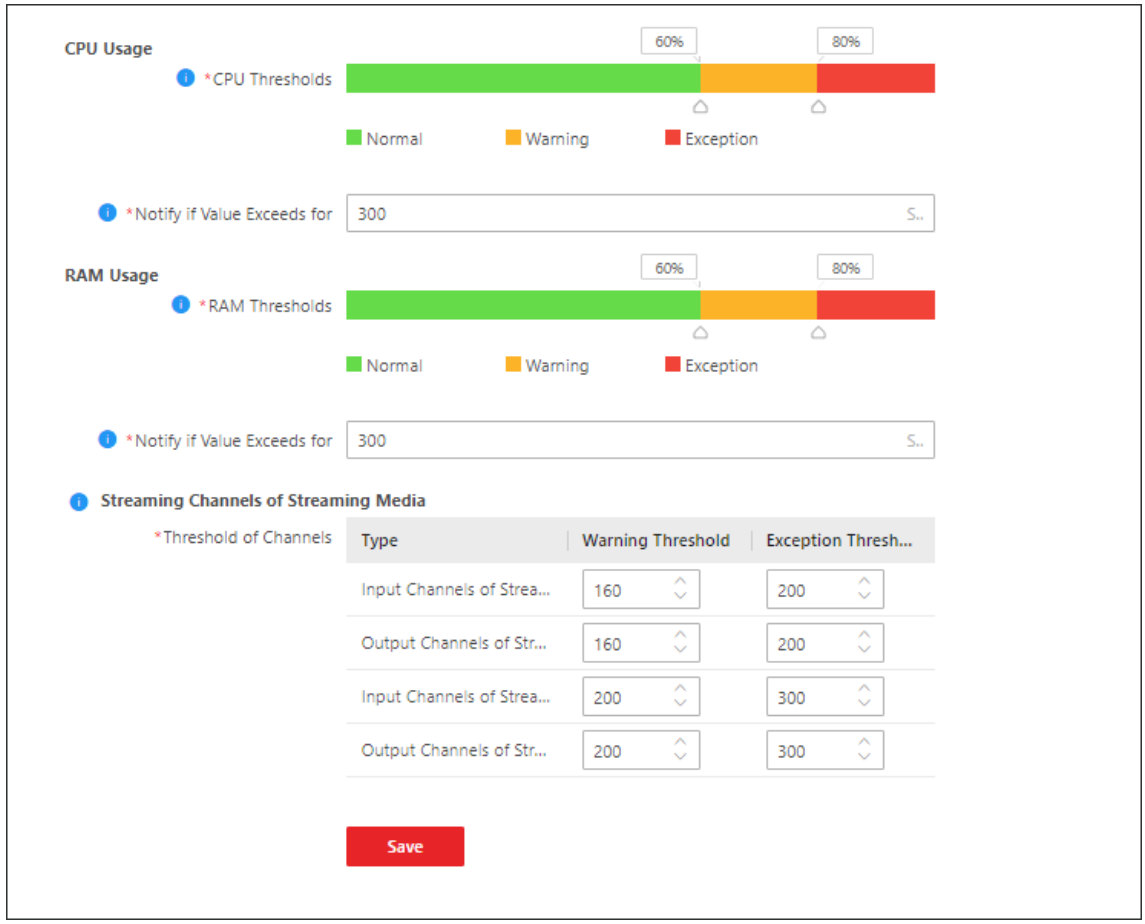


Figure 18-11 Set Server Usage Threshold

CPU/RAM Usage

Drag the ⌂ 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.

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.

18.2.3 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.

In top left corner of Home page, select → **All Modules** → **Maintenance** → **Basic Settings** → **Network Timeout** .

Select the network timeout and click **Save**.

Table 18-4 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.

18.2.4 Set Health 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.

Select **Maintenance → Health Check Frequency** on the left.

In the top left corner of Home page, select → **All Modules → Maintenance → Basic Settings → Health 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.

18.2.5 Set Topology Show Parameters

You can set parameters in the topology of Health Monitoring module, including topology hierarchy and bandwidth threshold.

Note

For details about health monitoring, see ***Health Monitoring*** .

In the top left corner of Home page, select → **All Modules** → **Maintenance** → **Basic Settings** → **Topology Show**



Figure 18-12 Topology Show Settings

Topology Hierarchy

If the devices connection hierarchy is complicated, you can set the topology hierarchy to display the primary devices.

Note

After setting the topology hierarchy, the topology will be generated again.

Bandwidth Threshold

When the bandwidth usage exceeds the threshold, the link on the topology will turns to the corresponding color.

18.3 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.

You can perform the following operations for different resource types.

- 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.
- Click **Export** to export the status data as CSV or Excel to the local PC.
- 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.

Note

The resource status will be automatically refreshed in a specified interval (see details in ***Set Health Check Frequency***).

18.3.1 Camera Status

On the camera status page, you can view camera status, such as network status, arming status, and recording status.

You can also perform the following operations.

- Select a Remote Site from the drop-down list in the camera list panel to display the status of cameras on the Remote Site.
- Click the camera name to view its status and basic information.
- Click the IP address to view the status of the device to which the camera is related.
- Click in the Operation column to go to the Area page to configure the parameters of the specified camera. See details in ***Edit Camera for Current Site*** or ***Edit Element for Remote Site*** .
- 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*** .

Note

This operation is not available for the cameras added on Remote Sites.

- Click in the Operation column to view the recording status of the camera. For details, see ***Search for Recording Status of Resource*** .

Note

This operation is not available for the cameras added on Remote Sites.

- 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.
- Select the device type(s) from the first drop-down list on the top to filter the camera status by device type.
- Check the check box and select the exception type from the drop-down list on the top to filter the door status by exception type.

Note

Contact the admin user to edit the abnormal configurations of camera's event or alarm via the Web Client if an icon appears near the camera name.

18.3.2 Door Status

On the door status page, you can view the information such as the network status of related devices and door status.

Note

For the door linked to the video intercom device, the door status is not available to be displayed.

You can also perform the following operations.

- Click the door name to view the status details and basic information of the door, and view the live video of the related access control device (if the device is with a camera).
- Click the device name to view the status of the device to which the door is related.
- Click in the Operation column to go to the Area page to configure the parameters of the specified door. See details in ***Edit Door for Current Site*** .
- Click in the Operation column and select a control type from the drop-down list to control the door status.
  - **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.
  - **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.
  - **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).

    Note

    For the door linked to video intercom device, setting its status to remain unlocked is not available.
  - **Remain Locked**: The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.
- Check the check box and select the exception type from the drop-down list on the top to filter the door status by exception type.

18.3.3 Floor Status

On the floor status page, you can view information, such as the network status of elevator control devices and the card reader status.

You can also perform the following operations.

- Click the name to view the status details and basic information.
- Click the device name to view the status of the device to which the floor is related.

- Click in the Operation column to go to the Area page to configure the parameters of the specified floor. See details in ***Edit Elevator for Current Site*** .
- Check the check box and select the exception type from the drop-down list on the top to filter the floor status by exception type.

18.3.4 Alarm Input Status

You can view the alarm input status including resource usage status (online or offline), arming status, bypass status, fault status, alarm status, detector connection status, battery status, and so on.

You can also perform the following operations.

- Click the device name to view the status of the device to which the alarm input is related.
- Select the device type(s) from the first drop-down list on the top to filter the alarm input status by device type.
- Check the check box and select the exception type from the second drop-down list on the top to filter the alarm input status by exception type.

18.3.5 UVSS Status

On the UVSS status page, you can view the information such as line scan camera status and capture camera status.

You can also perform the following operations.

- Click the UVSS name to view the status details and basic information.
- Select a Remote Site from the drop-down list at the top of UVSS status page to display the status of UVSSs on the Remote Site.
- Click in the Operation column to go to the Area page to configure the parameters of the specified UVSS. See details in ***Edit UVSS for Current Site*** .

Note

This operation is not available for the UVSSs added on Remote Sites.

18.3.6 Speaker Unit Status

On the speaker unit status page, you can view the status and information of speaker units, such as the network status and health check time.

You can also perform the following operations.

- Click the speaker unit name to view the status details and basic information.
- Click the device name to view the status of the device to which the speaker unit is related.

- Click in the Operation column to go to the Area page to configure the parameters of the specified speaker unit. See details in ***Edit Speaker Unit for Current Site*** .
- Check the check box and select the exception type from the drop-down list on the top to filter the speaker unit status by exception type.

18.3.7 Third-Party Integrated Resource Status

You can view status and information of the third-party integrated resource, such as the resource type, manufacturer, and network status.

You can also perform the following operations.

Note

The actual interface may vary with the kind of third-party resource.

- Click the resource name to view the status details and basic information.
- In the Operation column, click to control the door status.

18.3.8 Remote Site Status

You can view the Remote Site status such as the network status and health check time, and click the Remote Site name to view the status details and basic information.

18.3.9 Streaming Server Status

You can view the streams via each added Streaming Server (including incoming streams and outgoing streams), and view the hardware status such as network status, CPU usage, and RAM usage.

You can click the Streaming Server name to view the status details and basic information.

Click in the Operation column to go to the Resource Management Module to configure the parameters of the server.

18.3.10 Recording Server Status

You can view the status and information of Recording Server, such as the recording status, CPU usage, RAM usage, HDD status, and so on.

You can also perform the following operations.

- Click the Recording Server name to view the status details and basic information.
- Click the status in Recording Status column to view the recording status of the channels configured to store the video files in this Recording Server.

- Click the status in Hardware Status or HDD Status column to view the hardware status and HDD exception details if the status is exceptional.
- Check the check box and select the exception type from the drop-down list on the top to filter the Recording Server status by exception type.

18.3.11 DeepinMind Server Status

You can view the network status, CPU usage, and RAM usage, etc., of the DeepinMind Servers.

You can perform the following operations.

- Click the server name to view the status details and basic information.
- Click in the Operation column to go to the Resource Management Module to configure the parameters of the specified server.

18.3.12 Encoding Device Status

You can view the encoding device status including the recording status, HDD usage, arming status, etc.

You can perform the following operations.

- Select a Remote Site from the drop-down list at the top to display the status of encoding devices on the Remote Site.
- Click the device name to view the status and basic information of the encoding device and the related cameras.
- Click the status in **Recording Status** column to view the recording status of channels configured to store the video files on this encoding device.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified encoding device.
- Click to wake up the encoding device if it is in sleep mode.
- 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*** .

18.3.13 Access Control Device Status

You can view the status and information such as network status and battery status of the added access control devices. If the device is turnstile, you can view the status of master lane controller, slave lane controller, and component.

You can perform the following operations.

- Click the device name to view the status and basic information of the access control device, and the related doors and live videos (if the access control device is with a camera).
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified access control device.
- Check the check box and select the exception type from the drop-down list on the top to filter the Access Control Device status by exception type.

18.3.14 Elevator Control Device Status

You can view the information such as network status, arming status, and distributed elevator controller status.

- Click the device name to view the status and basic information of the elevator control device and the related floors.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified elevator control device.
- Check the check box and select the exception type from the drop-down list on the top to filter the elevator control device status by exception type.

18.3.15 Video Intercom Device Status

You can view the status information of the video intercom device such as network status, arming status, and the status of calling center from device (whether the device is able to call the security center of the platform).

You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Click the device name to view the status and basic information of the video intercom device and the related doors.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified video intercom device.
- Select the device type(s) from the first drop-down list on the top to filter the video intercom device status by device type.
- Check the check box and select the exception type from the second drop-down list on the top to filter the video intercom device status by exception type.

18.3.16 Visitor Terminal Status

On the visitor terminal status page, you can view the status and information of visitor terminals, such as the network status and arming status.

You can also perform the following operations.

- Click the visitor terminal name to view the status details and basic information.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified visitor terminal.

18.3.17 On-Board Device Status

On the on-board device status page, you can view the status and information of on-board devices, such as the license plate No., mobile signal, and disk status.

You can also perform the following operations.

- Click the on-board device name to view the status details and basic information.
- Click in the Operation column to view the online/offline records of the specified device. For details, see ***Search for Online/Offline Logs of Resource*** .
- Click in the Operation column to go to the Resource Management page to configure the parameters of the device.

18.3.18 Entrance/Exit Control Device Status

On the entrance/exit control device status page, you can view the status and information of entrance/exit control devices, such as the network status, arming status, and checking time.

You can also perform the following operations.

- Click the entrance/exit control device name to view the status details and basic information.
- Click in the Operation column to go to the Resource Management page to configure the parameters of the device.

18.3.19 Guidance Terminal Status

On the guidance terminal status page, you can view the status and information of guidance terminals, such as the network status, arming status, and checking time.

You can also perform the following operations.

- Click the guidance terminal name to view the status details and basic information.
- Click in the Operation column to go to the Resource Management page to configure the parameters of the device.

18.3.20 Security Control Device Status

You can view the managed devices' network status, battery status, and so on.

You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Click the device name to view the status and basic information of the security control device, and the related alarm inputs and cameras.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified security control device.

18.3.21 Fire Protection Device Status

On the fire protection device status page, you can view the status and information of fire protection devices, such as network status, arming status, and checking time.

You can also perform the following operations.

- Click the fire protection device name to view the status details and basic information.
- Click in the Operation column to go to the Resource Management page to configure the parameters of the device.

18.3.22 Dock Station Status

You can view the network status, HDD status, file backup status, and so on, of the added dock station.

You can perform the following operations.

- Select a Remote Site from the drop-down list at the top to display the status of dock stations on the Remote Site.
- Click the device name to view the status and basic information of the dock station.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified dock station.

18.3.23 Decoding Device Status

You can view the status information such network status, first added time, and checking time.

You can perform the following operations.

- Select a Remote Site from the drop-down list at the top to display the status of decoding devices on the Remote Site.
- Click the device name to view the status and basic information of the decoding device.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified decoding device.
  Click in the Operation column to view the status of distributed decoding device when exceptions occur. The status includes CPU usage, memory usage, network bandwidth, temperature, network status, etc.

18.3.24 IP Speaker Status

You can view the IP speakers' network status, serial No., address, and so on.

You can perform the following operations.

- Click the device name to view the status and basic information of the IP speaker.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified IP speaker.

18.3.25 Security Inspection Device

You can view the security inspection devices' network status, IP address, serial No., and so on.

You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Click the device name to view the status and basic information of the security inspection device.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified security inspection device.
- Click in the Operation column to view the online/offline records of the security inspection device. For details, see ***Search for Online/Offline Logs of Device*** .

18.3.26 Network Transmission Device

You can view the network transmission devices' CPU usgae, RAM usage, PoE usage, occupied ports, and so on.

You can perform the following operations.

- Click **All Devices** and then select a device type to display the device status of selected type only.
- Check the check box and select the exception type from the drop-down list on the top to filter the network transmission device status by exception type.
- Click the device name to view the basic information, device usage, and port information of the network transmission device.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified network transmission device.

18.3.27 Digital Signage Terminal Status

You can view the status and information of digital signage terminals, for example, network status.

You can perform the following operations.

- Click the device name to view the status and basic information of the digital signage terminal.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified digital signage terminal.

18.3.28 Interactive Flat Panel Status

You can view the status and information of interactive flat panels, for example, network status.

You can perform the following operations.

- Click the device name to view the status and basic information of the interactive flat panel.
- Click in the Operation column to go to the Device and Server page to configure the parameters of the specified interactive flat panels.

18.4 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.

18.4.1 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 top navigation bar, select → **Basic Management** → **Maintenance** . Then select **System Log** → **Server Logs** on the left.

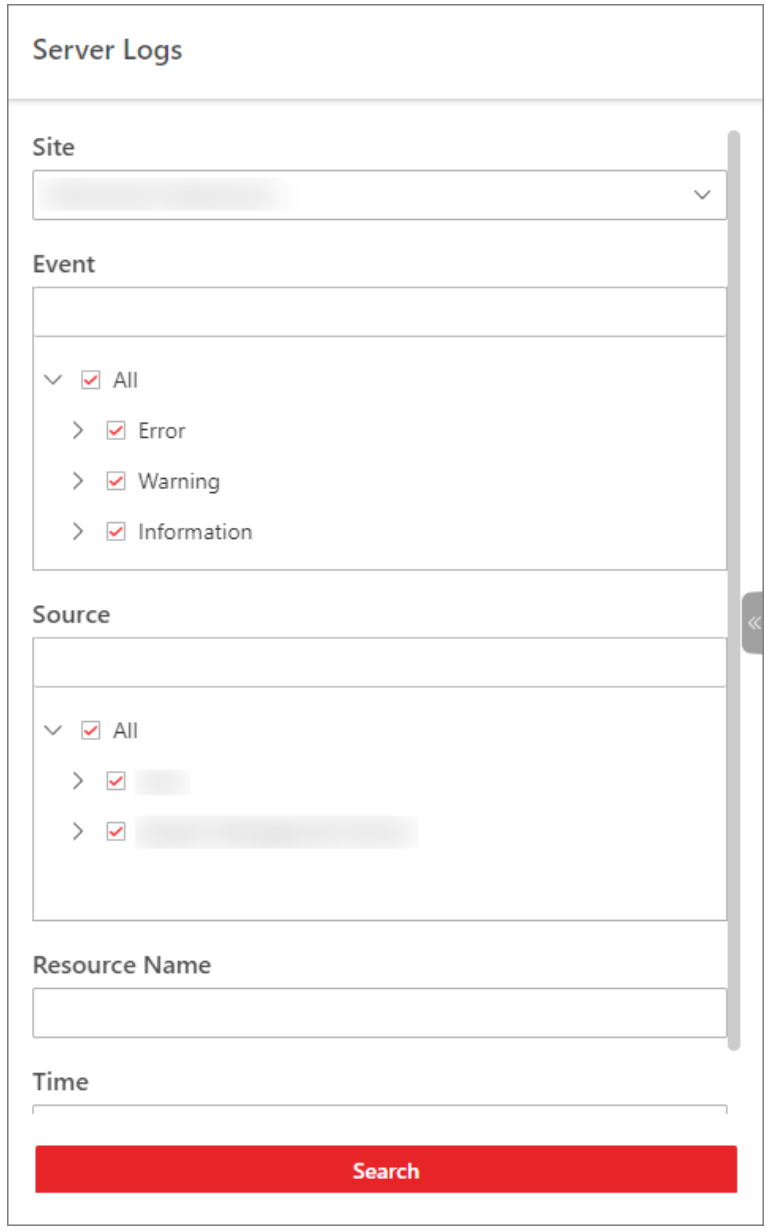


Figure 18-13 Search for Server Logs

2. In **Site**, select the current site or a Remote Site.
3. In **Event**, 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 **Source**, select user and server to set the source of the logs that you want to search for.
5. **Optional:** In **Resource Name**, enter the name of a resource to search the logs of the resource.
6. In **Time**, select the time range of this search.

Note

You can select **Custom Time Interval** 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.

18.4.2 Search for Online/Offline Logs of Device

You can search for the online/offline logs of encoding devices, security inspection devices, and on-board 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 top, select → **Basic Management** → **Maintenance** → **System Log** .
2. Select **Device Logs** on the left.

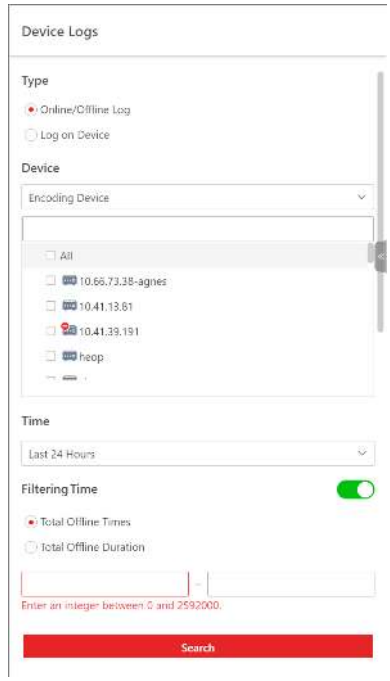


Figure 18-14 Search for Device Online/Offline Logs

3. In **Type**, select **Online/Offline Log** as the log type.
4. Select a device type and check the devices you want to search.
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 devices, switch on **Filtering Time** 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 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.
8. **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. You can perform the following operations. • Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter the data. • 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.

18.4.3 Search for Logs Stored on Device

You can search for the logs stored on encoding devices, security control devices, decoding device, access control devices, elevator control devices, network transmission devices, on-board device, and fire protection device.

Steps

1. In the top left corner, select → **All Modules** → **Maintenance** → **System Log** → **Device Logs** .
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. You can perform the following operations. • Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter the data. • 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.

18.4.4 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 top, select → **Basic Management** → **Maintenance** → **System Log** .
2. Select **Resource Logs** on the left.

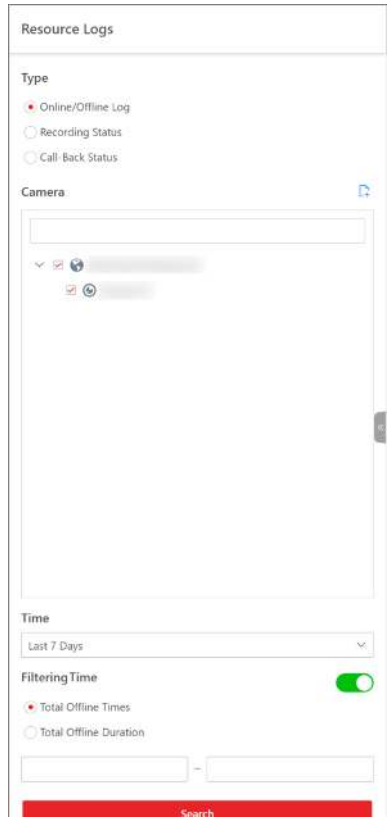


Figure 18-15 Search for Resource Online/Offline Logs

3. In **Type**, select **Online/Offline Log**.
4. Click to show the area list on the current site and then select the cameras whose logs are to be searched for.
5. **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.
6. 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.

7. **Optional:** If there are a large number of devices, switch on **Filtering Time** 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.
8. 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.
9. **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. You can perform the following operations. • Filter Data: Select a time period and a status (online, offline or all) from the drop-down lists respectively to filter data. • 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.

18.4.5 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 top, select → **Basic Management** → **Maintenance** .
2. Select **System Log** → **Resource Logs** on the left.

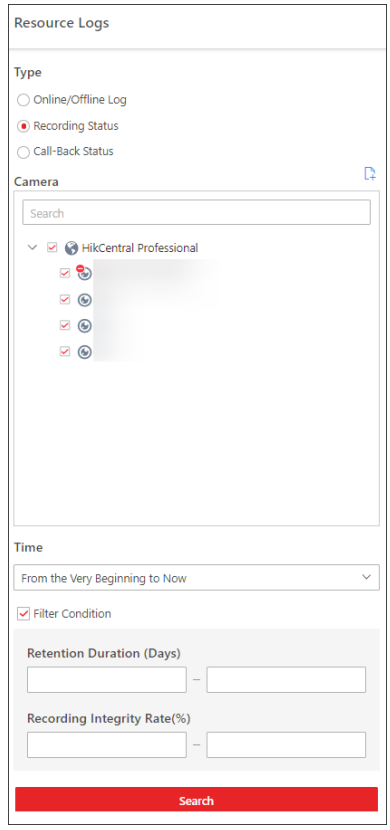


Figure 18-16 Search for Resource Recording Status

3. In **Type**, select **Recording Status**.
4. Click to show the area list of the current site and then select the cameras whose logs are to be searched for.
5. **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.
6. 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.

7. **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

For details about recording schedule, refer to ***Configure Recording Schedule Template*** .

8. 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.

9. **Optional:** Check historical recording status.

1) **Optional:** Click **Rule** in the top right corner to view the analytical rules for history videos.

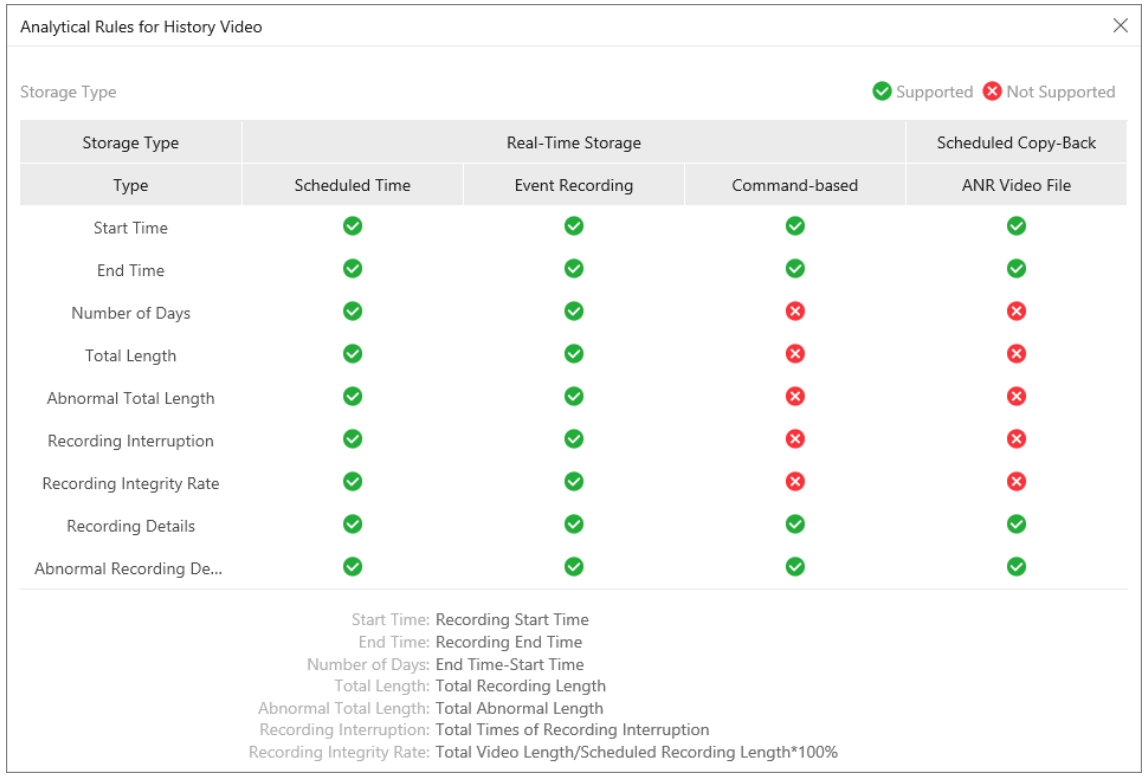


Figure 18-17 Analytical Rules for History Video

2) Click a camera name to open the History Recording Status panel.

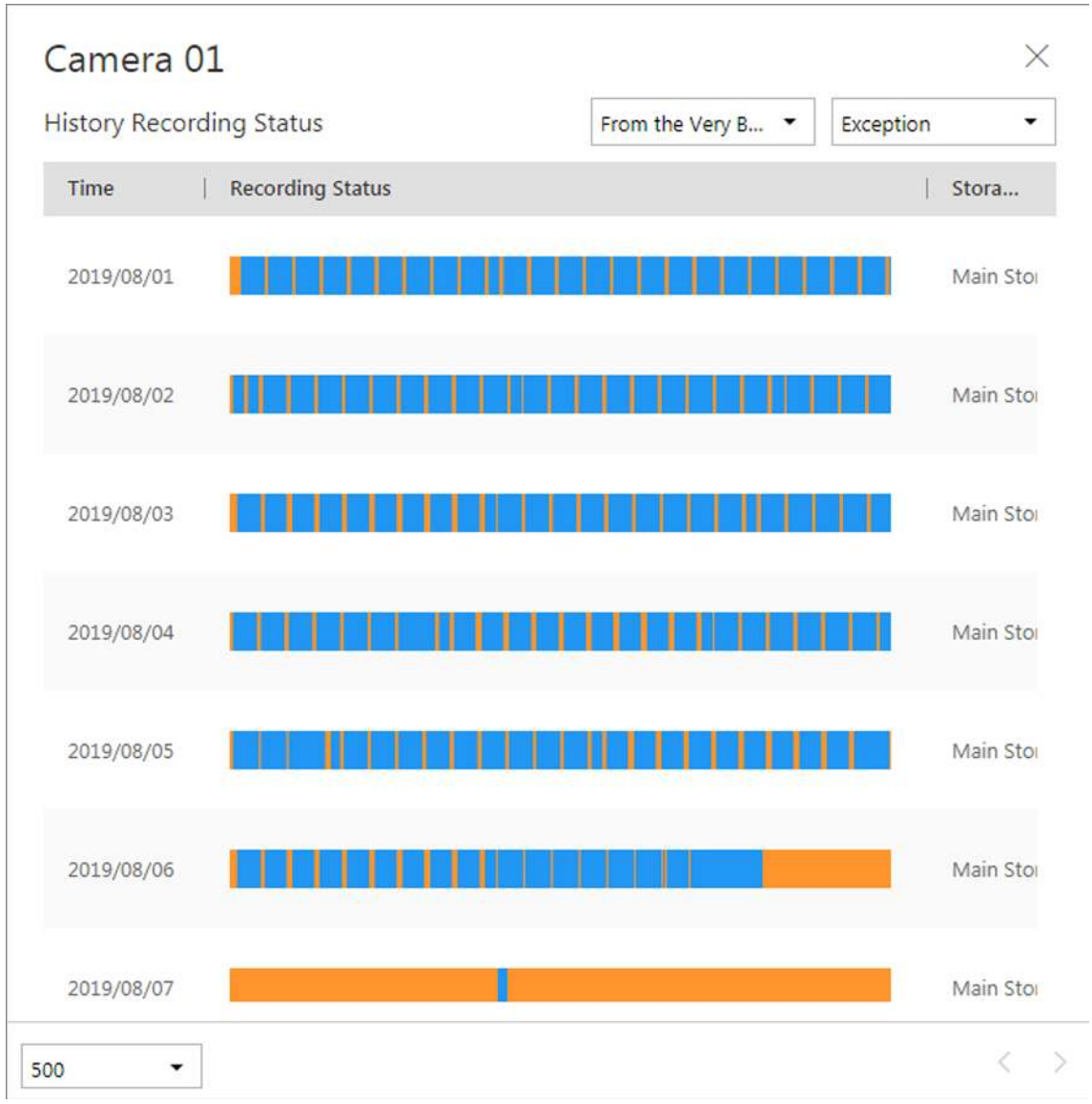


Figure 18-18 History Recording Status

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.

10. **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.

18.4.6 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 top, select → **Basic Management** → **Maintenance** .
2. Select **System Log** → **Resource Logs** on the left.

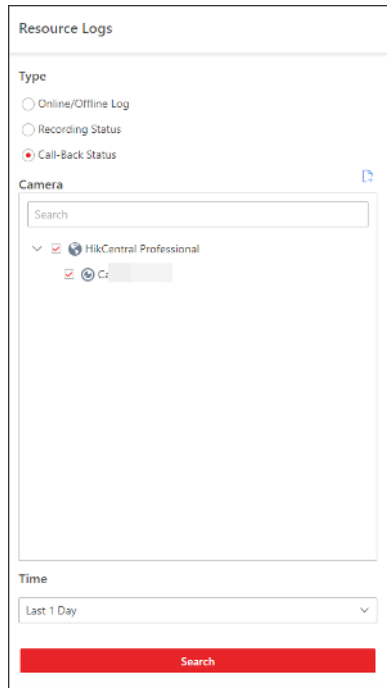


Figure 18-19 Search for Resource Call-Back Status

3. In **Type**, select **Call-Back Status**.
4. Click to show the area list of the current site and then select the cameras whose logs are to be searched for.
5. **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.

6. 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.

7. Click **Search**.

Call-back status of each camera are listed on the right.

8. **Optional:** Click **Export** and then select a file format (i.e., Excel or CSV) to download the call-back status to your local PC.

18.5 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.

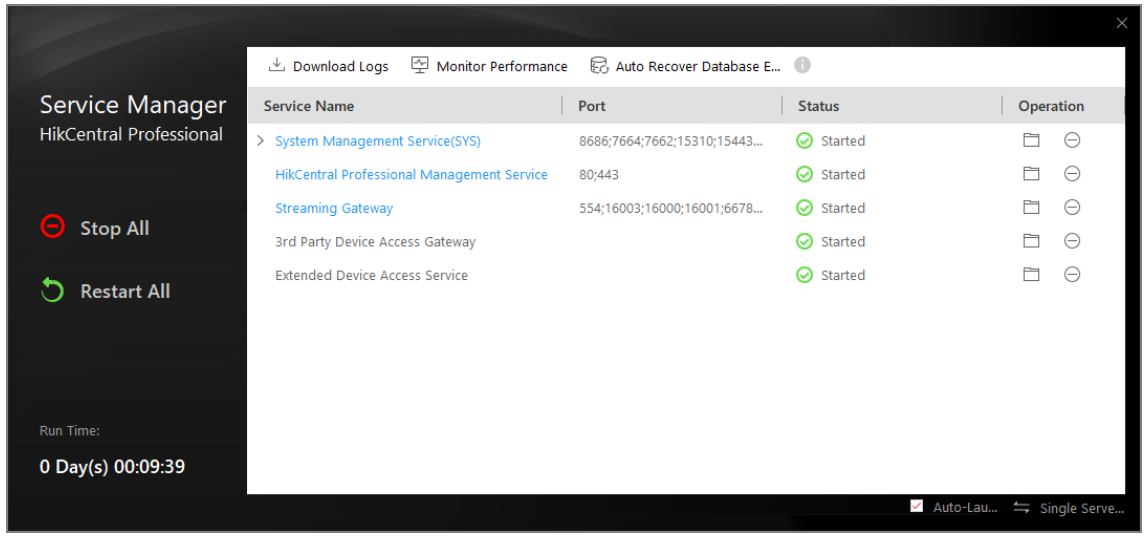


Figure 18-20 Service Manager Main Page

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.

Note

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.

18.6 Set System Data Backup

For purpose of restoring the original system data after a data loss event or recovering data from an earlier time, you can manually back up system data, or configure a schedule to back up regularly. System data includes data configured in the system, pictures, received events and alarms, face comparison data, card swiping data, maintenance data, etc.

Steps

Note

The backups are stored in the SYS server. You can edit the saving path only on the Web Client running on the SYS server.

1. In the top right of the client, click **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Back Up** tab.
3. In **Type**, select the system data that you want to back up.
4. Set a backup schedule to run backup regularly.
   1) In **How Often**, select the frequency to back up the system data.

2) In **Which Day** and **When**, specify which time to back up.
3) In **Max. Number of Backups**, set the maximum number of backup files. Old backup files will be automatically deleted.

Note

The value ranges from 1 to 5.

5. Save the settings.
   - Click **Save** to save the backup schedule.
   - Click **Save and Back Up Now** if you need to back up the system data immediately.

18.7 Restore System Data

When an exception occurs, you can restore the system data if you have backed up system data before.

Before You Start

Make sure you have backed up system data. Refer to ***Set System Data Backup*** for details.

Steps

Note

System data recovery will restore the system to an earlier state, and thus the data added after backup date will be lost.

1. In the top right of the Home Page, click **Maintenance and Management → Back Up and Restore System Data** .
2. Select the **Restore** tab.
3. Select a backup file to be restored.

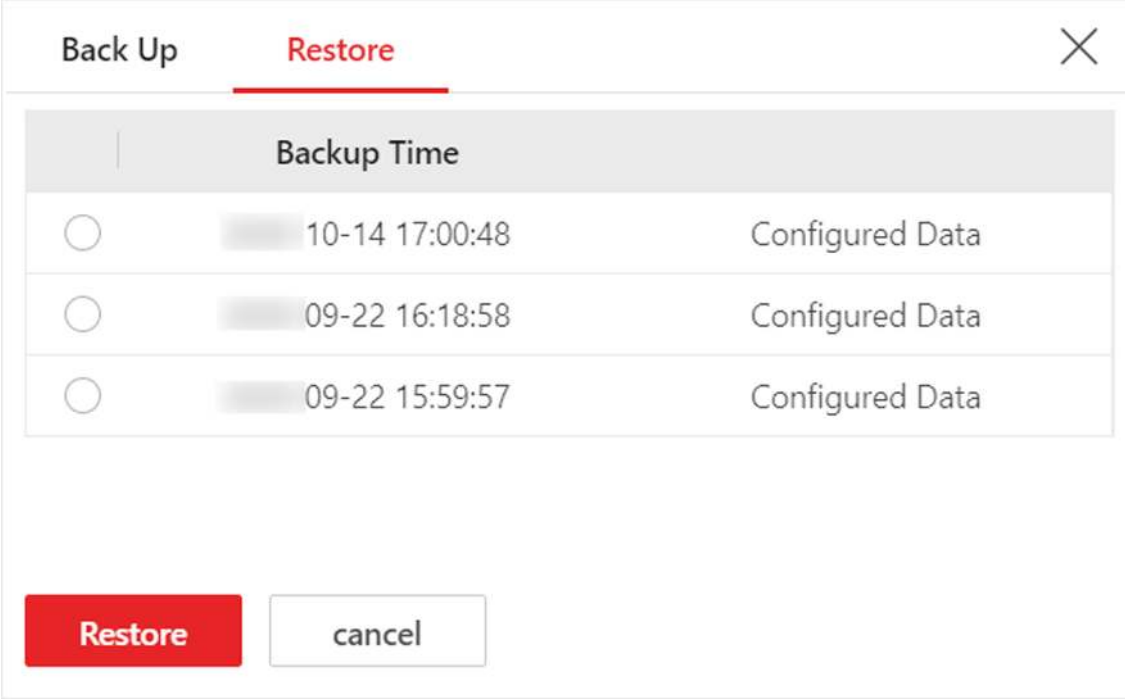


Figure 18-21 Restore System Data

4. Click **Restore** to confirm the system data recovery.

What to do next

After restoring the system data, you must reboot the SYS service via Service Manager and log in to Web Client again.

18.8 Export Configuration File

You can export and save configuration data to local disk, including remote site configurations, 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.
3. Click **Export** to download the data to the local PC.

Note

The configuration data file is in CSV format.

Chapter 19 Evidence Management Center

In the Evidence Management Center, you can manage evidence and the unlinked files (including pictures, videos, audios and other files), which contain important information about incidents such as traffic accidents and violent crimes in case of the need for settling disputes or legal cases.

19.1 Basic Settings

You can set the storage location for evidence and set custom items to define the evidence type, on-site organization, and result/conclusion, all of which containing the information about evidence. This configuration will affect the functionality of evidence management on the Client.

On the top left, select → **Security Monitoring** → **Evidence Management Center** . Then select **Basic Settings** on the left.

Storage Location

Set the storage location to **Local Storage** or **SFTP**.

Note

- If **SFTP** is selected as the storage location, the following fields are required: address, port, user name, and password.
- If **Local Storage** is selected as the storage location, you can select the local resource pool.

Evidence Type

You can add or delete the type of accident or suspect incident recorded in the evidence, such as theft, robbery, attack, and missing person.

On-Site Organization

You can add or delete the organization or personnel on the site, which is responsible for collecting the evidence of the accident or suspect incident, such as police, ambulance, and fire department.

Result/Conclusion

You can add or delete the result/conclusion of incidents based on the evidence collected from the on-site organization, such as arrested, warned, and injured.

19.2 Add Evidence

You can add evidence about incidents such as traffic accidents and violent crimes in case of the need for settling disputes or legal cases. You can set detailed information for the added evidence, including the evidence 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 evidence content from cameras or local PC.

Before You Start

Make sure you have configured basic settings. For details, refer to ***Basic Settings*** .

Steps

1. On the top left, select → **Security Monitoring** → **Evidence Management Center** .
2. Select **Evidence** → **Evidence Management** on the left.
3. Click **Add** to enter the Add Evidence page.

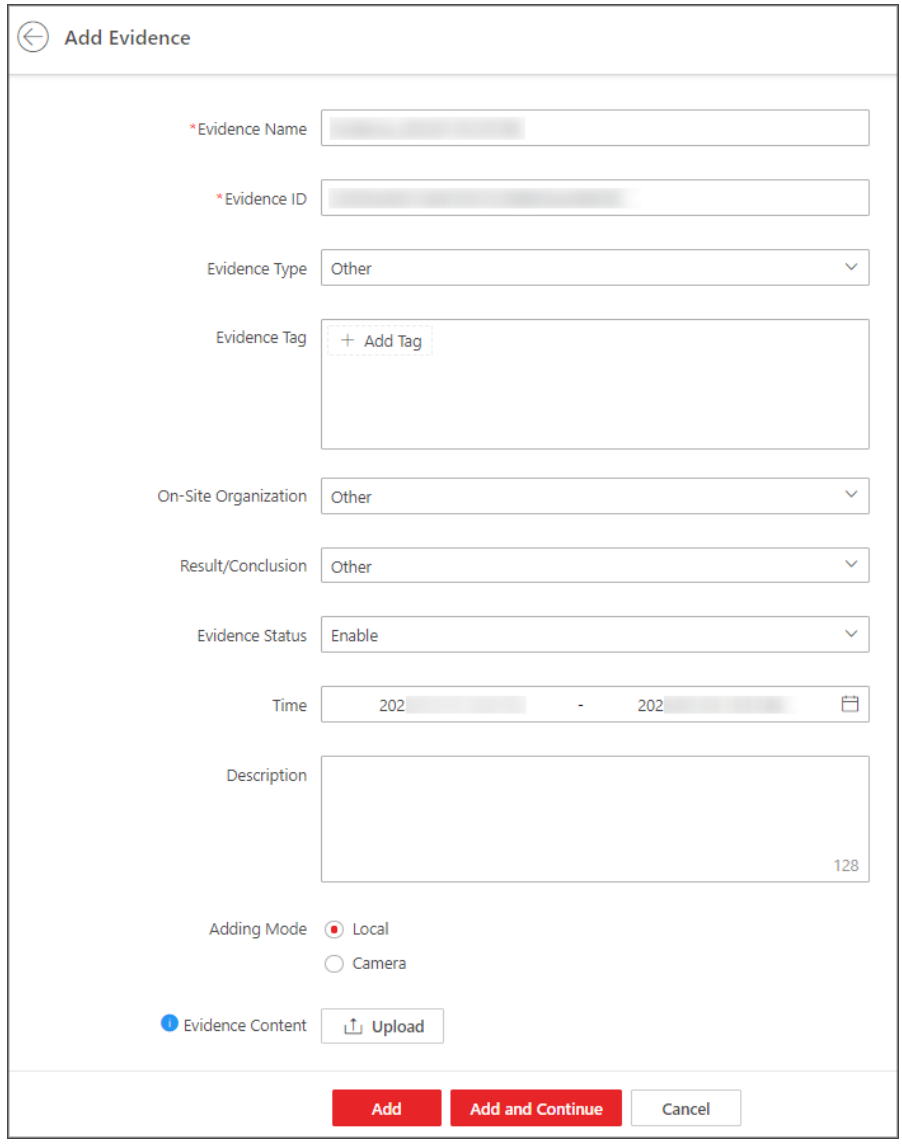


Figure 19-1 Add Evidence

4. Create a name for the evidence.

The evidence ID will be generated automatically on the Client. You can edit the evidence ID which should be 1 to 64 letters or digits.

5. Set the type, tag, on-site organization, result/conclusion, status, time (start time and end time of the evidence event), or description for the evidence.
6. **Optional:** Set the mode of adding files as the evidence.
   - Select **Local** and click **Upload** to upload files (such as pictures, audios, and videos) from the local PC for the evidence content.
   - Select **Camera**, check cameras in the Linked Camera list, select the uploading mode, and set the corresponding parameters for the selected uploading mode. If you select **Upload at Specified Time**, you should specify the start time and end time of file uploading and recording. If you select **Upload when Wi-Fi Detected**, the files will be automatically uploaded once the Wi-Fi is detected and connected, so you are only required to specify the start time and end time of file recording.

   Note

   If the uploading mode is **Upload when Wi-Fi Detected**, the Client only supports uploading evidence from cameras linked to the same device.
7. Finish adding the evidence.
   - Click **Add** to add the evidence and back to the Evidence Management page.
   - Click **Add and Continue** to save the settings and continue to add other evidence.
8. **Optional:** Perform further operations after adding evidence(s) if needed.

Refresh Evidence	Click **Refresh** to refresh the latest view of evidence information.
Switch Display Mode	Click or to display the added evidence in card mode or list mode.
Delete Evidence	Select the evidence(s) and click **Delete** to delete the evidence(s).
Filter Evidence	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 evidence(s).
Enable/ Disable Evidence	Click **Disable Evidence** to disable the evidence if the related case is settled, or click **Enable Evidence** to enable the selected evidence if the related-case is pending.
Export Evidence Record	Click **Export** to export the selected evidence record(s) in Excel, CSV, or PDF format. **Note** You can check **Include Evidence File** to export the attached evidence file.

View Evidence Details and Edit Evidence

In card mode or list mode, you can click the evidence name to view the evidence's content, basic information, and operation records.

You can edit the evidence's basic information, such as the evidence type, time, and tag.

You can also upload related files from local PC for the evidence content.

Note

- If you have added a picture for evidence content, you can click or to zoom in or delete the picture.
- If you have added the file for evidence content and exported the evidence, you can hover your cursor on the added file, then click → to copy the evidence's original sha256 value. You can compare it with the sha256 value of the evidence collected by other persons so as to verify the content integrity of collected evidence.

19.3 Manage Unlinked Files

The unlinked files refer to the files about incidents such as traffic accidents and violent crimes in case of the need for settling disputes or legal cases, but have not been linked with any evidence. You can manage the unlinked files, such as adding and viewing the files by category (pictures, videos, audios, and others). You can also link the added files with the specific evidence.

19.3.1 Add and View Unlinked Files

You can add the files which are unlinked with evidence(s). For the added unlinked file(s), you can perform more operations such as viewing the added files by category, filtering and exporting the unlinked files.

Steps

1. On the top left, select → **Security Monitoring** → **Evidence Management Center** .
2. Select **Evidence** → **File Management** on the left.

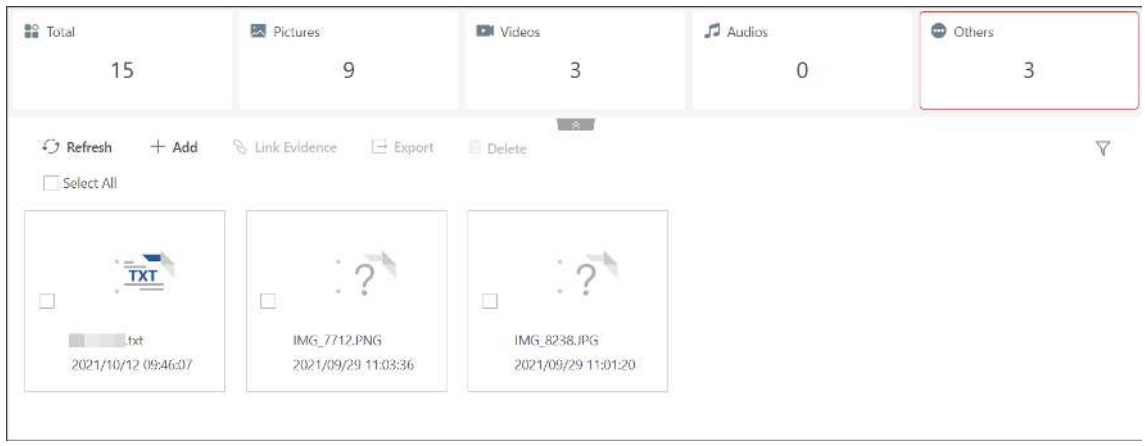


Figure 19-2 File Management Page

3. Click **Add**.
4. Select the pictures, videos, audios, or other files from local PC to add.
5. **Optional:** Perform further operations if needed.

View the Unlinked Files by Category	At the top of File Management page, you can view the total number of unlinked files or the number of categorized files, including pictures, videos, audios, and others. You can also click each category to view all of the corresponding files information, including the file name and uploading time.
Filter the Unlinked Files	Click in the upper right corner to unfold the filter pane, enter the evidence name in the search box or select the creation time, and then click **Filter** to filter the target evidence.
Refresh the Unlinked Files	You can click **Refresh** to refresh the file list.
Floating Window Display	Hover your cursor on the added picture to view the enlarged picture in a floating window.
Link the Unlinked Files to Evidence	For details, refer to ***Link Files with Evidence*** .
Export the Unlinked Files	Select the unlinked file(s) and click **Export** to export the file(s). **Note** For viewing the file exporting records, refer to ***Manage Operation Records*** .
Delete the Unlinked Files	Select the unlinked file(s) and click **Delete** to delete the selected file(s).

19.3.2 Link Files with Evidence

You can link the added file with the existing evidence or newly added evidence. The linked files recorded in the evidence can be used as materials in case of the need for settling disputes or legal cases.

Before You Start

Make sure you have added the file(s). For details, refer to ***Add and View Unlinked Files*** .

Steps

1. On the top left, select → **Security Monitoring** → **Evidence Management Center** .
2. Select **Evidence** → **File Management** on the left.
3. Select the unlinked file(s) in the list.
4. Click **Link Evidence** to enter the Link Evidence pane.

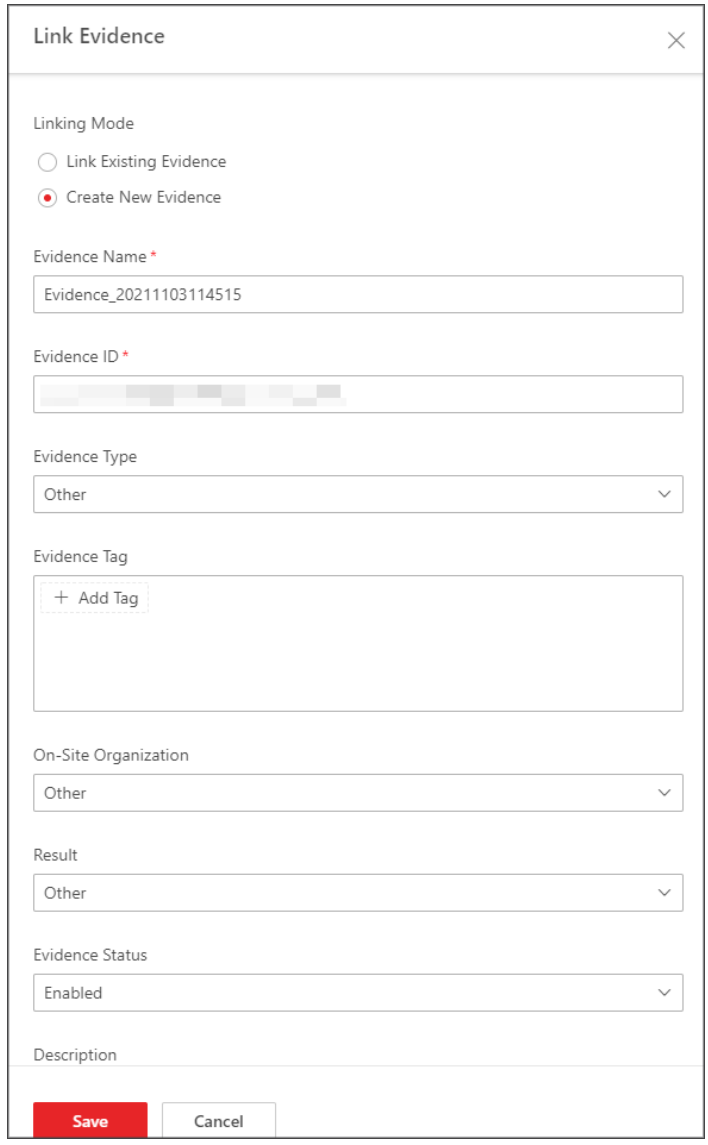


Figure 19-3 Link Files with Evidence

5. Select the linking mode.
   - Select **Link Existing Evidence** and enter the evidence name/ID/tag/description in the Select Evidence box to select the existing evidence for linking.
   - Select **Create New Evidence** and create a new evidence for linking.

   Note

   For details about adding evidence, refer to ***Add Evidence*** .
6. Click **Save**.

   The linked files will not be displayed in the list.

19.4 Manage Operation Records

You can manage the evidence operation records, including viewing or deleting the upload/download records of evidence or files from the local PC or cameras.

On the top left, select → **Security Monitoring** → **Evidence Management Center** . Then select **Operation Record** on the left.

Upload Record

On the Upload Record page, you can view the records (including evidence or file size and upload status) of the evidence or files uploaded from local PC or related cameras.
You can also search for records by name, check a record and click / / in the Operation column to pause/start/retry the upload task. Or you can check record(s) and click **Delete** to delete the selected record(s).

Download Record

On the Download Record page, you can view the records (including evidence or file size and download status) of exporting evidence or files on the platform.
You can also search for records by name, check a record and click / / in the Operation column to pause/start/retry the download task. Or you can check record(s) and click **Delete** to delete the selected record(s).

Chapter 20 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.

20.1 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** .

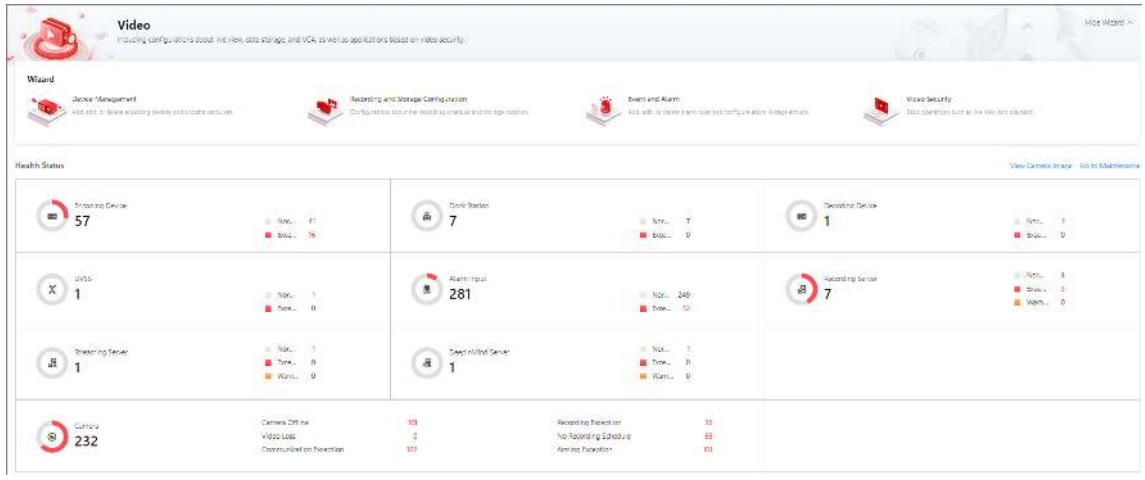


Figure 20-1 Video Overview

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. • 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. For further operations, refer 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.

20.2 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.

20.2.1 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, and so on.

Start Live View in Area Mode

You can start the live view of cameras grouped in an area.

Before You Start

Make sure you have grouped cameras into areas. Refer to the ***Add Camera to Area for Current Site*** or ***Add Camera to Area for Remote Site*** for details.

Steps

1. In the top left corner of the Client, select → **Video** → **Video Security** .

   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.

   Note

   For setting the user permission, refer to ***Role and User Management*** .

2. **Optional:** Click in the upper-right corner to change live view window division.

   Average

   All the divided windows are distributed in average.

   Highlighted

   The highlighted window is used to display the live video of the critical camera.

   Horizontal

   The divided windows are distributed horizontally in the window.

   Vertical

   The divided windows are distributed vertically in the window.

   Others

   Other types of window division besides the types above.

3. Start live view.

For One Camera	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.
For All Cameras in The Same Area	Drag an area to a display window, and click **Batch Play**, or double-click the area to start the live view of all camera in the area. **Note** The display windows automatically adapt to the number of cameras in the area.

4. **Optional:** When an alarm is triggered on a resource, the title bar of the resource's live view window will turn red. Click the red title bar to view the alarm information and acknowledge the alarm.

Start Live View in View Mode

You can quickly start the live view of the cameras managed in a view.

Before You Start

Make sure you have added at least a view. Refer to ***Manage View*** for details.

Steps

1. In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Security** .
2. Select **View** on the top of left navigation bar.
3. Start the live view of the cameras related to the view.
   - Double click a view.
   - Move the mouse cursor to a view, and click → **Play** beside the view name.

Note

You can switch the added views from the drop-down list above the live view window.

4. **Optional:** Perform further operations after starting live view.

Operations on Live View Toolbar	Move the mouse cursor to the lower edge of the live view window and perform more operations. **Note** For details about the functions of different icons, refer to ***Customize Icons on Live View Window*** .
View Alarm Information	When an alarm is triggered on a resource, the title bar of the resource's live view window will turn red. Click the red title bar to view the alarm information and acknowledge alarm.
Adjust Windows' Sequence	Drag the windows to adjust the sequences. **Note** The changed sequence will be restored after restarting live view in view mode.
Stop Live View	Click that appears in the upper-right corner when the mouse pointer is over the display window. You can also click above the display window to stop the live view of all the display windows.

Auto-Switch Cameras in an Area

You can play the live view of all cameras in an area in turn in one window and perform further operations after auto-switch starts.

Steps

1. In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Security** .

The areas which the current user has permission to access are listed and cameras which the user has permission to access are shown in each area.

Note

For setting the user permission, refer to ***Role and User Management*** .

2. Start auto-switch in the area.
   - Drag an area to the live view window and select **Single-Screen 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.
3. **Optional:** Move the cursor to the live view window and perform further operations after auto-switch starts.

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.

4. **Optional:** Move the cursor to the display window to access the icons for further operations.

Note

For details about these icons, refer to ***Customize Icons on Live View Window*** .

20.2.2 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.

Note

For details, refer to ***Start Live View in Area Mode*** and ***Start Live View in View Mode*** .

2. On the toolbar of display window, click to enter the fisheye dewarping mode and view live view.



Figure 20-2 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. **Note** Setting pattern is not supported by fisheye cameras.

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 20-3 Manual Panorama Tracking

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. b. Press and move the cursor on the picture to draw. For example, you can mark the suspicious persons in the picture. c. Click **Save As** and specify the path to save the edited picture.

Operation	Description
	Note The picture cannot be saved if the free space on your disk is less than 512 MB.

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 20-1 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. **Note** After capturing a picture, a thumbnail will pop up on the upper-right corner. You can click **Search by Picture** 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 Control 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.
	Switch Stream Type	Switch the live view stream to main stream, sub-stream (if supported), or smooth stream (if supported). **Note** 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.
	Video 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.

Note

The icons on the toolbar in the live view window vary with the device's capabilities.

5. Click **Save**.

20.2.3 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 panel.

Note

The PTZ control function should be supported by the camera.

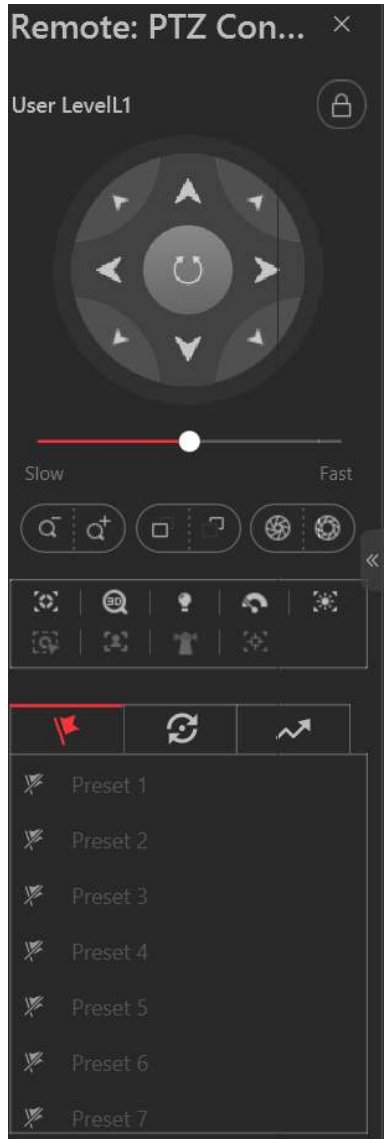


Figure 20-4 PTZ Control Panel

The following buttons are available on the PTZ control panel:

	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.

	Note 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 **Focus +** move the focal point forward, and click **Focus -** to move the focal point backward.
	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.

- In the live video display window, you can click the icon to enable window PTZ control. Move the cursor to the direction you desired and click on the image to pan or tilt.
- You can click and drag the cursor with a white arrows to the direction you desired for a quick direction control.
- You can 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.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Video** → **Video Application** → **Video Application** .
2. Start live view of the PTZ camera.
3. Click to enter the PTZ Control mode.
4. Click to enter the PTZ preset configuration panel.
5. Use the direction buttons and other buttons to control the PTZ movement.
6. Select a PTZ preset number from the preset list and click .
7. Create a name for the preset in the pop-up window.
8. Click **OK** to save the settings.

Note

- Up to 256 presets can be added.
- The unconfigured preset is gray.
- The configured preset is highlighted.

9. **Optional:** After adding the preset, you can do one or more of the followings:

Call Preset	Double-click the preset, or select the preset and click .
Edit Preset	Select the preset from the list and click .
Delete Preset	Select the preset from the list and click .
Get Device PTZ Configuration	You can click to get device PTZ configuration.

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

Two or more presets for one PTZ camera need to be added. Refer to ***Configure Preset*** for details about adding a preset.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Video** → **Video Application** → **Video Application** .
2. Start live view of the PTZ camera.
3. Click to enter the PTZ Control mode.
4. **Optional:** You can click to get device PTZ configuration.
5. Click to enter the PTZ patrol configuration panel.
6. Add presets to the patrol.
   1) Click on the right side of a patrol.
   2) Select **Device Preset** or **Virtual Preset** as the preset type.
   3) Click to add a configured preset, and set the dwell time and patrol speed.

   Note

   - The preset dwell time ranges from 15 to 30s.
   - The patrol speed ranges from 1 to 40.
   - The unconfigured patrol is gray.
   - The configured patrol is highlighted.

   4) Repeat the above steps to add other presets to the patrol.

   Note

   By default, the first preset is added to the patrol list. Double-click the preset, speed, and dwell time to access a drop-down configuration list.

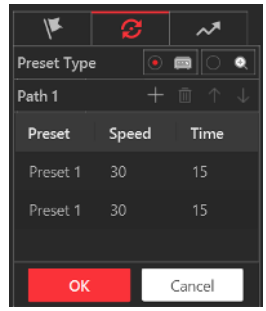


Figure 20-5 Configure Patrol

7. **Optional:** Perform the following operations after you add the preset.

Edit Added Preset	Double-click the corresponding field of the preset to edit the settings.
Remove Preset from Patrol	Click to remove the preset from the patrol.
Adjust Preset Sequence	Click or to adjust the presets sequence.

8. Click **OK** to save the patrol settings.

Note

Up to 8 patrols can be configured.

9. **Optional:** After setting the patrol, you can do one or more of the followings:

Call Patrol	Click to start the patrol.
	Note When the patrol is working, it will stop if you start performing PTZ control including direction button control, zoom in/out, focus +/-, iris +/-, etc. The patrol will continue working after you have stopped PTZ control for 15 seconds.
Stop Calling Patrol	Click to stop the patrol.

Configure Pattern

Patterns can be set to record the movement of the PTZ.

Steps

1. In the top left corner of the Client, select → **All Modules** → **Video** → **Video Application** → **Video Application** .
2. Start live view of the PTZ camera.
3. Click to enter the PTZ Control mode.
4. Click to enter the PTZ pattern configuration panel.
5. Click to start recording the movement path of the pattern.
6. Use the direction buttons and other buttons to control the PTZ movement.
7. Click to stop and save the pattern recording.

Note

Only one pattern can be configured, and the newly-defined pattern will overwrite the previous one.

8. **Optional:** After setting the pattern, you can do one or more of the followings:

Call Pattern	Click to call the pattern.
	Note When the pattern is working, it will stop if you perform PTZ control including direction button control, zoom in/out, focus +/-, iris +/-, etc. The pattern will continue working after you have stopped PTZ control for 15 seconds.
Stop Calling Pattern	Click to stop calling the pattern.

Delete Pattern Click to clear the recorded pattern.

20.2.4 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.

Normal Playback

You can search video files by area or camera for the Normal Playback and download found video files to local PC. You can also add a tag to mark important video footage, and so on.

Note

- You can search video files by the time of the time zone where the device locates in, or by the time of the time zone where the PC running the Control Client locates in.
- Automatically converting daylight saving time to standard time is supported, or vice versa.
- Synchronous playback or asynchronous playback of devices in different time zones are supported.

Search Video File

You can search video files by camera, by area, or by time for normal playback. And you can also filter the searched video files by recording type, tag type, target type and storage location.

Steps

1. In the top left corner of the Client, select → **Video** → **Video Security** .
2. Click **Playback** to enter the playback page.
3. Drag the camera or area to the display window, or double-click the camera or area to play the recording of the specified camera(s) in selected window.

   Note

   The playback window supports up to 16 channels.

   Today's recorded video files of the selected camera will be played.
4. Click on the toolbar to set the date and time.

   Note

   In the calendar, the date with video files will be marked with a triangle.

   After selecting the date and time, the matched video files will start playing in the display window.
5. **Optional:** Click on the toolbar to select recording type, tag type, target type and storage location for playback.

Note

To set the storage location for recording, refer to ***Configure Storage and Recording*** .

Play Video File

After searching the video files for the normal playback, you can play the video via timeline or thumbnails.

Steps

1. In the top left corner of the Client, select → **All Modules → Video → Video Security** .
2. Click the **Playback** tab to enter the playback page.
3. Select a date with videos to start playing video and show the timeline after searching the video files.

Note

The video files of different types are displayed in different colors on the timeline.

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

Note

- Click / on the right of the timeline bar, or use the mouse wheel to zoom in or zoom out the timeline.
- Click / to show or hide the thumbnail bar.
- Move the cursor to the top border of the thumbnail bar and drag to adjust the height of the thumbnails when the cursor changes into . You can also click to lock the thumbnail bar above the playback timeline, and click to hide the thumbnail bar automatically.

Start Playback in View Mode

You can quickly access the playback of the cameras managed in a view.

Before You Start

Make sure you have added a view. For details, refer to ***Manage View*** .

Steps

1. In the top left corner of the platform, select → **Security Monitoring → Video → Video Security** .
2. Click **View** on the top of left navigation bar.
3. Click the **Playback** tab to enter the playback page.
4. Click a view to quickly start the playback of all the cameras related to the view.

Note

You can also quickly switch the added view from the drop-down view list above the display windows.

Synchronous Playback

You can play the video files of different cameras synchronously. Synchronous playback allows you to synchronize the display of video from multiple cameras.

Steps

Note

Video files from up to 16 cameras can be played simultaneously.

1. In the top left corner of the Client, select → **Video** → **Video Security** .
2. Click the **Playback** tab to enter the playback page.
3. Start normal playback of at least two cameras.

   Note

   For detailed configuration about normal playback and playback control, refer to ***Normal Playback*** . Some icons may not be available for synchronous playback.
4. Click **Synchronous Playback** on the playback toolbar to enable the synchronous playback.

   The cameras displayed in Playback will start synchronous playback.
5. **Optional:** Click **Asynchronous Playback** on the playback toolbar to disable synchronous playback.
6. **Optional:** Click and to perform normal and reverse playback.
7. **Optional:** Click and to perform single-frame normal and reverse playback.

   Note

   - No more than 16 cameras are allowed in single-frame normal and reverse playback.
   - If you pause one camera, others will be paused in the synchronous playback mode.
8. **Optional:** Move the cursor to the lower edge of the playback window to access the icons for further operations.

   Note

   For details, refer to ***Customize Icons on Playback Window*** .

Fisheye Playback

Fisheye playback function allows you to play the fisheye camera's video in fisheye dewarping mode. Fisheye dewarping mode refers to the process of perspective correction of an image, to

reverse the effects of geometric distortions caused by the fisheye camera lens. Dewarping allows you to cover a wide area with a single device and have a normal view of an otherwise distorted or reversed image.

Steps

1. In the top left corner of the Client, select → **Video** → **Video Security** .
2. Click the **Playback** tab to enter the playback page.
3. Select a fisheye camera from the camera list to start playback.

Note

For detailed configuration about playback and playback control, refer to ***Normal Playback*** .

4. Move the cursor to the display window, and click on the appearing toolbar to enter the fisheye dewarping mode.
5. Drag on the video to adjust the view angle.
6. Scroll the mouse wheel to zoom in or zoom out the view.

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 20-2 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.

		Note After capturing a picture, a thumbnail will pop up on the upper-right corner. You can click **Search by Picture** 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. For details aboutsaving video files as evidence and setting saving path, see ***Manual Recording and Capture*** .
	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. **Note** 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. **Note** When in software decoding mode, you can also capture the zoomed in picture after enabling digital zoom function.
	Fisheye Expansion	Available for fisheye camera for entering the fisheye dewarping mode. See ***Fisheye Playback*** .
	Camera Status	Show the camera's recording status, signal status, connection number, etc.
	Stream Switch	Switch the stream to main stream, sub-stream (if supported), or smooth stream (if supported). If the device supports transcoding playback, start transcoding and you need to set the resolution, frame rate and bitrate for transcoding.

		Note • The smooth stream will show if device supports. You can switch to smooth stream when in low bandwidth situation to make playback more fluent. • Only video files stored in DVR and I-series NVR support transcoding playback.
	Video 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.

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.

20.2.5 Manage Favorites

You can add and manage Favorites on the client. For camera(s) added to the Favorites, you can quickly view the live view or start the playback.

Before You Start

Make sure you have added camera(s) to area(s). Refer to the ***Add Camera to Area for Current Site*** or ***Add Camera to Area for Remote Site*** for details.

Steps

1. In the top left corner of the Client, select → **Video** → **Video Security** .
2. Click **Favorites** on the left navigation bar.

Note

In the Favorites list, two default root Favorites (**Favorites** and **Favorites Shared by Others**) are displayed. You can click to view the sub Favorites and cameras added in these two root Favorites.

3. Select a parent Favorites.

Note

You can either select the root Favorites or the sub Favorites added under the root one.

4. Add a Favorites under the parent Favorites.
   1) Click .

2) Enter the name for Favorites.
3) **Optional:** Select a parent node from the drop-down list.
4) **Optional:** Check **Online Resource Only** to display online resources only on the list.
5) Select the camera(s) to be added to Favorites.
6) Click **Save**.

Note

Up to 5 levels of Favorites can be added.

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

Edit Favorites	Select a Favorites, and click ··· → **Edit** on the right side of Favorites' name to edit its name and add more camera(s) to it if needed.
Share Favorites	Select a Favorites, and click ··· → **Share** on the right side of Favorites' name to share it with others. **Note** For details about adding user(s), refer to the *User Manual of HikCentral Professional Web Client*.
Delete Favorites	Select a Favorites, and there are two methods to delete it. • Click 🗑 on the top of the Favorites list, and click **OK**. • Click ··· → **Delete** on the right side of Favorites' name.
View Live View/Playback of All Cameras	• 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. • When in Playback window, select a Favorites, and click ··· → **Play All** to start viewing the playback of all the camera(s) added in Favorites.
Search Camera in Favorites	Enter keywords in the search box above the Favorites list to search for the target camera(s) or Favorites.
Delete Camera in Favorites	Select a camera in Favorites, and click 🗑 to delete it.

20.2.6 Manage View

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.

Perform this task when you need to get quick access to a certain set of channels for live view or playback.

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.

Steps

1. In the top left corner of the platform, select → **Security Monitoring → Video → Video Security** .
2. Click **View** on the top of left navigation bar.
3. **Optional:** Add a custom view group.
   1) 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.

   2) Click .
   3) Create a name for the group or use the default name.
   4) Click **OK** to add this view group.
4. Add a view.
   1) Select a view group.
   2) Click .
   3) Create a name for the view or use the default name.
   4) Click **Add** to select cameras.
   5) Select a stream type for each camera in the Stream Type column, or you can click **Set Stream Type** to select a stream type.
   6) Select a preset you want to switch to for each camera.
   7) **Optional:** Click **Up** or **Down** to adjust the camera order.
   8) **Optional:** Select camera(s) and click **Delete** to delete them.
   9) Select a layout for the view.
   10) Select a switching interval or click **Custom Time Interval** to set the switching interval among the selected cameras.
   11) Click **Add** to add this view.
5. **Optional:** You can also Drag the channels to the window or double-click the channels to start live view or playback. Save the view with the displayed view division and channels.
   - Click → **Save View** to save the current window division mode and displayed channels and (or) map as the selected view.
   - Click → **Save as View** to save the current window division mode and displayed channels and (or) map as a new view by creating view name (optional) and selecting the view saving path.

Note

If the added view is not selected before, you can also save the current window division and displayed channels as a new view.

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

Edit View	Click to edit the view settings, such as the view name and camera's stream type.
Add Camera/Map to the Existing View	a. Go to **Monitoring**. b. Select camera(s) or map. **Note** You can press Ctrl on the keyboard to select multiple cameras. c. Click → **Save View** to save the camera(s) or map to an existing view.
Delete Camera/Map from View	a. Move the cursor to a camera or a map in a view. b. Click to close the current camera or map window. c. Click → **Save View** to save the current view.
Live View/ Playback in View Mode	Select a view, and click → **Play** to start live view or playback in view mode. See ***Start Live View in View Mode*** and ***Start Playback in View Mode*** for details.
Delete View or View Group	Click to delete the custom view or view group.
Reset View	Click to restore the view to its initial settings.
Search View	Click , and enter keywords in the search box to search for target view(s).

20.2.7 Set Video Parameters

You can set network parameters, picture file format, display parameters, etc.

In the top left corner of the platform, select → **Security Monitoring** → **Video** → **Video Security** → .

Table 20-3 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.

Area	Parameters	Description
	Window Divisions for Main Stream	When the number of divided windows is smaller than the number you set, the live video 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. 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	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 set as 4:3 or 16:9.
	Display Window No.	Display the No. of each window 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.
	Overlay Temperature Information	When On, displays the temperature information on the live view and playback image.

Area	Parameters	Description
	GPU Hardware Decoding	When On, enables the GPU decoding for live view and playback to save CPU resources.
	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.	

20.3 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.

20.3.1 Search for Scheduled Captures

You can search for captures by specify a capture schedule, camera(s), and time.

Before You Start
Make sure you add a capture schedule. For details, see ***Configure Capture Schedule*** .

Steps
1. In the top left corner of Control Client, select → **Video** → **Picture Center** → **Scheduled Capture Search** .
2. Select a capture schedule, resources for capturing, and time.
3. Click **Search**.

   The results will be displayed on the right pane.
4. **Optional:** You can perform the following operations.

Operation	Description
Real-Time Capture	Click **Real-Time Capture** to capture pictures of the selected resources in real time.
Send Email	Select pictures, click **Send Email**, select an email template, enter remark, and click **OK** to send the selected pictures via email.

Export	Choose file contents and file format, and click **OK**.

20.3.2 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.

Steps

1. In the top left corner of the platform, select → **Security Monitoring → 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. Set the search time period of a day.
6. Select the video length to be generated.

   The time-lapse videos based on searched pictures are generated and displayed.
7. **Optional:** Move your cursor to a video and click **Download** to download the video.

   The download task is in the task center.

20.4 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.

20.4.1 Manage Face Comparison Group

HikCentral Professional 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.

On the Web Client, after adding the persons to the person group, the administrator should create a face comparison group, and then add persons (selected from the person list) to the group before you can perform face comparison. Finally, the administrator should apply the face comparison group with person information to the face recognition device to take effect.

When a person's face is detected and it matches or mismatches the person information in the face comparison group, an event/alarm (if configured) will be triggered to notify the security personnel and you can view the face comparison information during live view on the Control Client.

Add a Face Comparison Group

You need to add a face comparison group and add persons to the group for face comparison for further configurations such as intelligent recognition task settings.

Steps

Note

For details about intelligent recognition task settings, see ***Manage Intelligent Recognition Task*** .

1. In the top left corner of the Home page, select → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Click + to open the Add Face Comparison Group pane.
3. Create a name for the face comparison group.
4. **Optional:** Enter a description about the face comparison group.
5. Click **Add**.

   The face comparison group will be displayed in the group list.
6. **Optional:** Perform further operations.

Edit Face Comparison Group	Select a group from the group list and then click to edit its name and description.

Delete Face Comparison Group	Select a face comparison group and click to delete it.
Add Persons to Face Comparison Group	Select a face comparison group and click **Add** to add new or existing persons on the platform to the group. See details in ***Add Persons to a Face Comparison Group*** .
Import Persons to Face Comparison Group	Select a face comparison group and click **Import** to batch import persons to the group. Choose the method of importing persons. See details in ***Import Persons or Profile Pictures*** .
Delete Persons from Face Comparison Group	Select persons in the group and click **Delete** to delete them from the group. Or click → **Delete All** to delete all persons in the group.
Delete Profile Pictures	Select persons in the group and click → **Delete Profile Picture Only** to delete the profile pictures of selected persons.
Export All Face Information in a Group	a. Click **Export**. b. Create a password for decompressing the exported file, and then confirm it.

Import Face Comparison Group from Device

You can import face picture libraries from an encoding device or a facial recognition server to the platform as face comparison groups. After you importing the face picture libraries, the face information contained in them will also be imported.

Steps

1. In the top left corner of the Home page, select → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Click to open the Import Face Comparison Group from Device pane.
3. Select **Encoding Device** or **Facial Recognition Server** from the Device Type field.

   All available devices will be displayed.

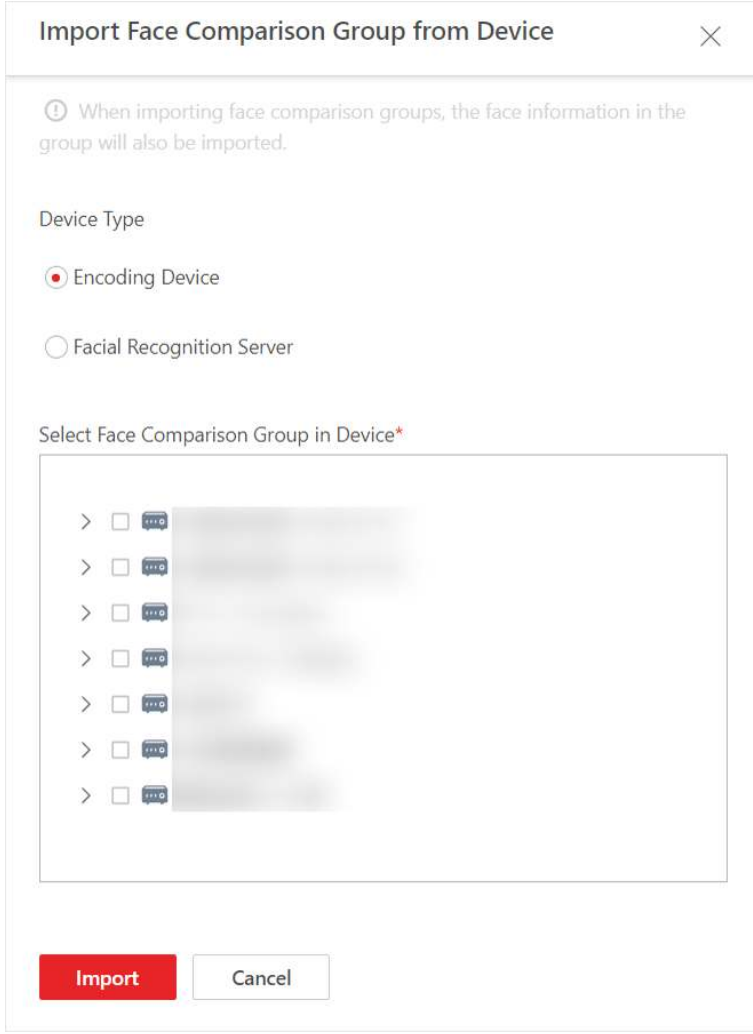


Figure 20-6 Import Face Comparison Group from Device

4. Click › to show the face comparison group(s) of a device.
5. Select face comparison group(s), and the click **Import**.

   The Import Face Comparison Group window pops up, displaying the import results.

Note

If a face picture library fails to be imported, you can view the failure details such as library name, device name, and the failure reason.

Add Persons to a Face Comparison Group

You can add new persons manually to a face comparison group, or add existing persons on the platform to the group.

Steps

1. In the top left corner of the Home page, select → **Video** → **Intelligent Recognition** → **Face Comparison Group** .
2. Select a group from the group list.
3. Click **Add** → **Add New Person** or **Add Existing Person** to add persons to the group.

Add New Person	Enter the required person information including ID, first name, and last name, and then click **Add** or **Add and Continue** to add the person to the group.
Add Existing Person	Select persons from the person list, and then click **Add**. **Note** You can check **Include Sub-Group** to include the persons in the sub-groups.

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. **Optional:** Perform further operations.

Delete Persons from Face Comparison Group	Select persons in the group and click **Delete** to delete them from the group. Or click → **Delete All** to delete all persons in the group.
Delete Profile Pictures	Select persons in the group and click → **Delete Profile Picture Only** to delete the profile pictures of selected persons.

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. In the top left corner of the Home page, select → **Video** → **Intelligent Recognition** → **Face Comparison Group**
2. Select a face comparison group.
3. Click **Import**, and click one among **Import by Template**, **Import Zipped Profile Pictures**, and **Import from Enrollment Station**.

Table 20-4 Import Profile Pictures

Method	Description
Import by Template	a. Click **Download Template** on the pane to download the template. b. Fill required information into the template, and then click to select the filled-in template from the local PC. c. Check **Replace Repeated Person** to allow the system to overwrite the person information already exists in the face comparison group when you import the information. 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. **Apply Face Information** Import specific face information from the enrollment station to the face comparison group. **Copy Back Face Information** Copy back all the face information acquired by the enrollment station to the selected face comparison group. **Select File** 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 comparison group.

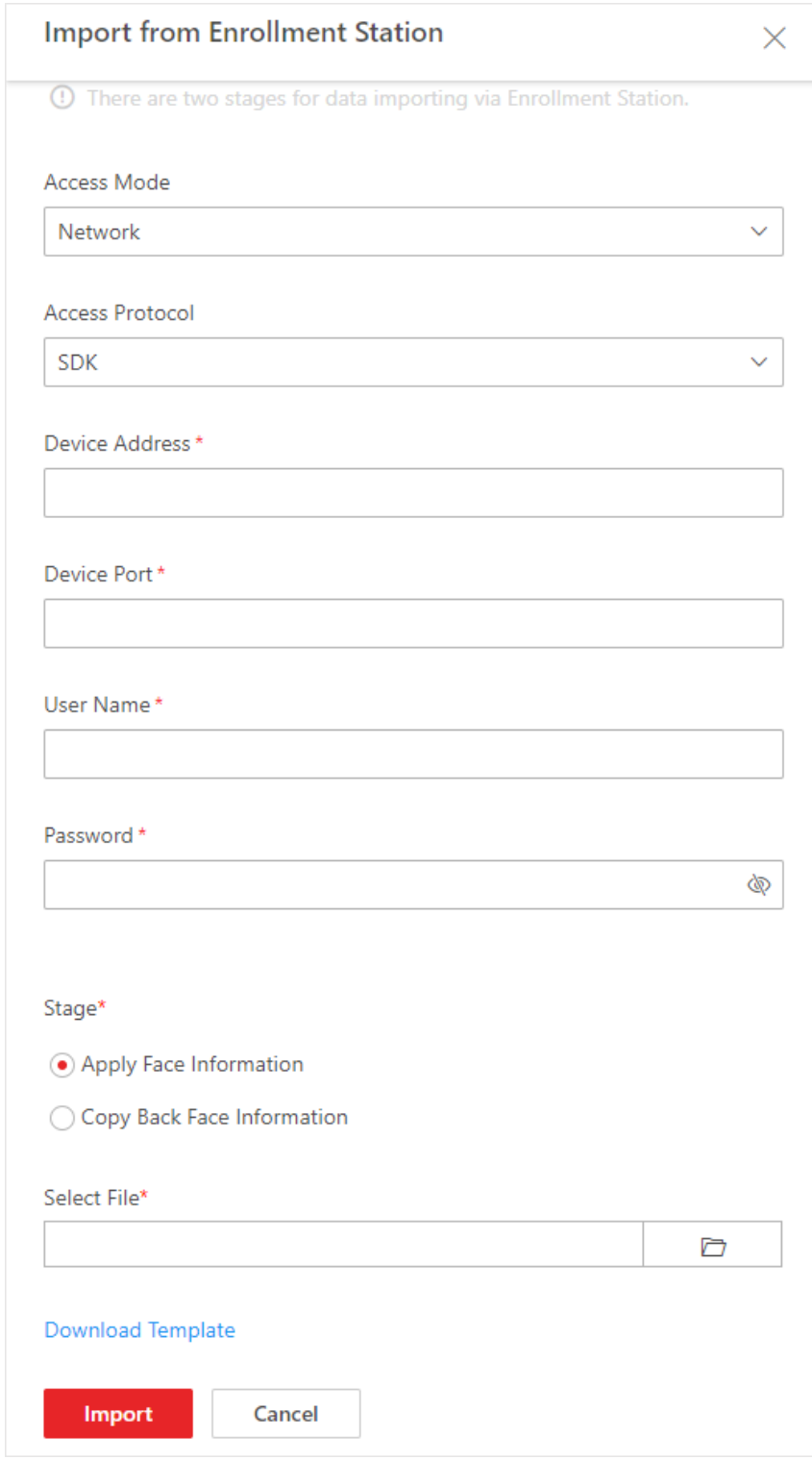


Figure 20-7 Import from Enrollment Station

Apply Face Comparison Group to Device

After setting the face comparison group and adding person(s) to the group, you need to apply the group settings to the device which supports face comparison so that the camera can compare the detected faces with the face pictures in the face comparison group and trigger alarms (if configured). After applying the face comparison group 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 comparison groups 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 → Intelligent Recognition → 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 camera(s) to apply the selected face comparison group(s) to.
6. Click **Apply** to start applying.

20.4.2 Manage Intelligent Recognition Task

You can add an intelligent recognition task to define the conditions such as the device and time for intelligent recognition. The task types include face comparison, people feature analysis, frequently appeared person analysis, rarely appeared person analysis, archive analysis, and behavior analysis.

Add Face Comparison Task

You can add face comparison task to define the time, device, face comparison group, similarity threshold, and so on, for face comparison. Once a face comparison task is added, the security personnel can view real-time matched face information during live view and search face comparison records via the Control Client and Mobile Client.

Before You Start

Make sure you have set face comparison groups. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Face Comparison** .
2. Click **Add** to enter the Add Face Comparison Task page.
3. Set parameters, such as task name, description, and task schedule template.

Note

The parameter marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when the face comparison functionality is activated.

You can click **View** to view the details of the scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select a type of face comparison device.

Camera

Select camera(s) from the Available list, and then click › to add selected one(s) to the Selected list.

Face Comparison Group

Select face comparison group(s). The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).

Similarity

Drag the slider to adjust the similarity threshold based on your face comparison requirements. The higher the threshold, the preciser the comparison will be. The lower the threshold, the higher comparison rate will be.

Once the similarity between a detected face and a face picture in the selected face comparison group(s) reaches the threshold, the detected face will be recognized and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.

   The face information in the selected face comparison group(s) will be applied to the selected camera(s).
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click next to **Delete**, and then click **Delete All**.
Filter Tasks	Click and set filter conditions such as task name, and then click **Filter**.

Add People Feature Analysis Task

You can add a people feature analysis task to define conditions such as time, device(s), and detection area, for people feature analysis, which recognizes and records body features of the people appeared in the fields of view of the cameras linked to the people feature analysis device. Once a people feature analysis task is added, the security personnel can search and view people feature analysis records via the Control Client and Mobile Client.

Steps

1. In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **People Feature Analysis** .
2. Click **Add** to enter the Add People Feature Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

Note

The parameter marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when the people feature analysis functionality is activated.

You can click **View** to view details of the scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select a type of people feature analysis device for the execution of people feature analysis.

Camera

Select cameras for detecting persons.

Detection Area

Click **Draw Area** and the drag the cursor on the image to draw an area for detecting persons.

4. Complete adding the task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click next to **Delete**, and then click **Delete All**.
Filter Tasks	Click and set filter conditions such as task name, and then click **Filter**.

Add Frequently Appeared Person Analysis Task

You can add a frequently appeared person analysis task to define the time, device(s), appeared times threshold, and so on, for frequently appeared person analysis, which searches 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.

Before You Start

Make sure you have set facial comparison groups. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Frequently Appeared Person Analysis** .
2. Click **Add** to enter the Add Frequently Appeared Person Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

Note

The parameter marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when frequently appeared person analysis is activated.

You can click **View** to view detailed scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select the device type for frequently appeared person analysis.

Camera

Select camera(s) for detecting persons.

Face Comparison Group

Select face comparison group(s). The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).

Time Period

Set a time period for counting the appearance times of a detected person.

Appeared Times

Set threshold times for regarding a detected person as a frequently appeared person.

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.

Counting Interval

Set a time interval for filtering out invalid counting.

If a person is detected for multiple times within the time interval, the system will regard he/she only appeared for one time.

Similarity

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.

Once the similarity between a detected face and a face picture in the selected face comparison group(s) reaches the threshold, the detected face will be recognized and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click next to **Delete**, and then click **Delete All**.
Filter Tasks	Click and set filter conditions such as task name, and then click **Filter**.

Add Rarely Appeared Person Analysis Task

You can add a rarely appeared person analysis task to define the time, device(s), appeared times threshold, and so on, for searching 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.

Before You Start

Make sure you have set facial comparison groups. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Rarely Appeared Person Analysis**
2. Click **Add**to enter the Rarely Appeared Person Analysis Task page.
3. Set related information, such as task name, description, and task schedule template.

Note

The information marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when rarely appeared person analysis is activated.

You can click **View** to view detailed scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select the device type for rarely appeared person analysis.

Camera

Select camera(s) for detecting persons.

Face Comparison Group

Select face comparison group(s). The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).

Time Period

Set a time period for counting the appearance times of a detected person.

Reporting Time

The time when the results of rarely appeared person analysis is reported to system each day.

Appeared Times

Set threshold times for regarding a detected person as a frequently appeared person.

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.

Counting Interval

Set a time interval for filtering out invalid counting.

If a person is detected for multiple times within the time interval, the system will regard he/she only appeared for one time.

Similarity

Drag the slider to adjust the similarity threshold based on your facial recognition requirements. The higher the threshold, the preciser the recognition will be.

Once the similarity between a detected face and a face picture in the selected face comparison group(s) reaches the threshold, the detected face will be recognized and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click next to **Delete**, and then click **Delete All**.
Filter Tasks	Click and set filter conditions such as task name, and then click **Filter**.

Add Archive Analysis Task

You can add an archive analysis task to define conditions such as time, device, and face comparison group for archive analysis. 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.

Before You Start

Make sure you have set face comparison group. For details, see ***Manage Face Comparison Group*** .

Steps

1. In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Archive Analysis** .
2. Click **Add** to enter the Add Archive Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

Note

The parameter marked with a red asterisk is required.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when rarely appeared person analysis is activated.

You can click **View** to view detailed scheduled time.

Note

For details about adding task schedule template, see ***Add Task Schedule Template*** .

Device for Analysis

Select the device type for archive analysis.

Camera

Select camera(s) for detecting persons.

Face Comparison Group

Select face comparison group(s). The faces detected by the specified camera(s) will be compared with the face pictures in the selected group(s).

Similarity

Drag the slider to adjust the similarity threshold based on your face comparison requirements. The higher the threshold, the preciser the comparison will be.

Once the similarity between a detected face and a face picture in the selected face comparison group(s) reaches the threshold, the detected face will be compared and a face comparison record will be generated.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click next to **Delete**, and then click **Delete All**.
Filter Tasks	Click and set filter conditions such as task name, and then click **Filter**.

Add Abnormal Event Detection 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 (e.g., 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.

Before You Start

Make sure you have added abnormal event analysis server to the system. For details, see ***Add DeepinMind Server*** for details.

Steps

1. In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Abnormal Event Analysis** .
2. Click **Add** to enter the Add Abnormal Event Detection Analysis Task page.
3. Set parameters, such as task name, description, and task schedule template.

Note

- The parameter marked with a red asterisk is required.
- The parameters vary with different abnormal event types. Here we only introduce part of the parameters. For details about the settings of each type of abnormal event analysis, see the user manual of the device.

Abnormal Event Type

Select an abnormal event type.

The abnormal event types are categorized into different groups based on their usage scenarios, including people density analysis, perimeter protection, prison abnormal event, and street abnormal event.

Task Schedule Template

Select a task schedule template from the drop-down list to define the time when abnormal event analysis 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 analysis.

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.

4. Complete adding this task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more.
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click next to **Delete**, and then click **Delete All**.
Filter Tasks	Click and set filter conditions such as task name, and then click **Filter**.

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.

Before You Start

Make sure you have added DeepinMind server to the platform. For details, see ***Add DeepinMind Server*** .

Steps

1. In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Vehicle Analysis** .
2. Click **Add** to enter the Add Vehicle Analysis Task page.
3. Set the related parameters.

   Note

   The parameter marked with a red asterisk is required.

   Task Schedule Template

   Select a task schedule template from the drop-down list to define the time when the vehicle analysis functionality is activated.

   You can click **View** to view the details of the scheduled time.

   Note

   For details about adding a new task schedule template, see ***Add Task Schedule Template*** .

   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.
4. Adding the task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more task(s).
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.

Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ , set filter conditions such as task name and device for analysis, and then click **Filter**.
View Exception Details	If the device for vehicle analysis or the camera is abnormal, a red icon will appear beside the corresponding device, hover the mouse cursor on the icon to view the exception details.

Add Customer Traffic Task Excluding Staff

A customer traffic task excluding staff 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, you can add a customer traffic task excluding staff, so only actual customers will be counted instead of all people captured by cameras.

Steps

1. In the top left of the Home page, select ▦ → **Video** → **Intelligent Recognition** → **Intelligent Recognition Task** → **Customer Traffic Task Excluding Staff** .
2. Click **Add** to enter the Add Customer Traffic Task Excluding Staff page.
3. Set the related parameters.

Note

The parameter marked with a red asterisk is required.

Camera

Select camera(s) from the Available list, and then click › to add selected one(s) to the Selected list.

Face Comparison Group

You can choose face comparison group(s), and set a similarity threshold, so when people whose similarity with the people in the comparison group is above the threshold, they will not be counted.

4. Add the task.
   - Click **Add** to complete adding this task.
   - Click **Add and Continue** to complete adding this task and continue adding more task(s).
5. **Optional:** Perform the following operations after adding task(s).

Delete a Task	Select a task from the task list, and then click **Delete**.
Delete All Tasks	Click ⌄ next to **Delete**, and then click **Delete All**.
Filter Tasks	Click ▽ , set filter conditions such as task name and device for analysis, and then click **Filter**.

View Exception Details	If the device for vehicle analysis or the camera is abnormal, a red icon will appear beside the corresponding device, and hover the cursor on the icon to view the exception details.

20.4.3 Applying Center

In Applying Center, you can apply the face comparison group settings to the face recognition cameras to make the these settings take effect on the cameras. You can also view the cameras that fail to receive the settings and the face information that fails to be applied to the cameras, and then apply the face information again.

View Applying Status

You can view the status of the applying of face comparison groups from different perspectives, including the cameras failed to receive face comparison group, the cameras to which certain face comparison groups need to be applied, the person information failed to be applied, and the person information to be applied.

In the top left of the Home page, select → **All Modules** → **Video** → **Intelligent Recognition** → **Applying Center** .

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 comparison group, analysis device, and exception details (e.g., the device reaches its maximum face comparison group capacity, the face comparison group 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 comparison groups: the applying status of each face comparison group 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 comparison group 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 comparison group 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.

Steps

1. In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Applying Center** .
2. 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 comparison group 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 comparison group 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.

20.4.4 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.

Perform the following operations to add a custom template.

Steps

1. In the top left of the Home page, select → **Video** → **Intelligent Recognition** → **Task Schedule Template** .
2. Click + to add a schedule template.
3. Create a name for the template.
4. **Optional:** Select an existing template from the **Copy to** drop-down list.
5. Edit weekly schedule.

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.

6. Click **Add**.
7. **Optional:** Select a task from the task list, and then click to delete it.

20.5 Video Application

This section introduces advanced features including self-learning library, visual tracking, and person/vehicle arming and panorama tracking.

20.5.1 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.

Operation	Description
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.

20.5.2 Configure Visual Tracking

Visual tracking allows you to track an individual (such as a suspect) across different areas without losing sight of her/him. 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. More the cursor to one of the thumbnail, and then click the appeared **Set Visual Tracking** to open visual tracking settings page.
5. **Optional:** Click **Refresh** to get the latest view of the camera.
6. Click **Add Related Camera** to open the camera list panel, and select a camera from the camera list or search for a specific camera by keywords, and then click **OK**.

   The icon representing the related camera will be displayed on the view of the current camera. And the thumbnail of the view of the related camera will be listed on the right side.
7. Drag the icon to a proper position on the view according to its actual mounting position.
8. **Optional:** Hover the cursor over the thumbnail list on the right side, and then click **Set Visual Tracking** to set visual tracking for the related camera.

Note

You can repeat this step to set visual tracking for more cameras. After that, you can view the visual tracking route of different cameras. You can click one camera to view its corresponding visual tracking image.

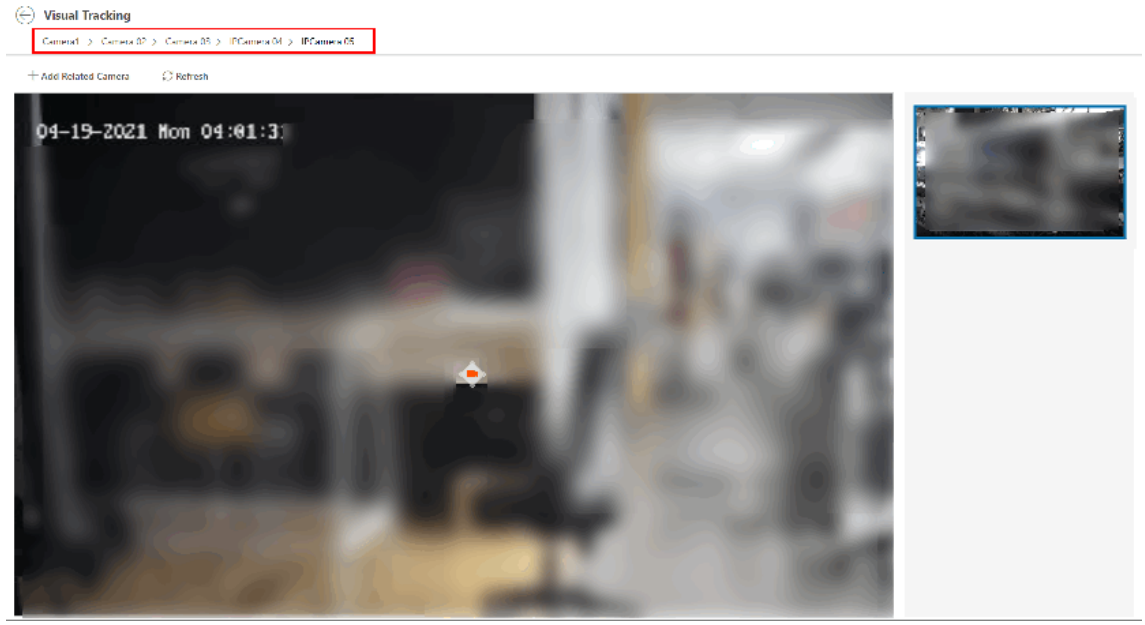


Figure 20-8 Set Visual Tracking

9. **Optional:** Hover the cursor over the thumbnail list on the right side, and then click **Delete** to cancel the association between the current camera and its related camera.
10. Click in the upper-left corner to save the above settings and back to the visual tracking page.

    The security personnel will be able to use the video tracking function on the Control Client.

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 20-9 Monitoring Image of Camera A

20.5.3 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 → Configure Person/Vehicle Arming** .

Person/Vehicle arming groups are groups containing multiple cameras. The cameras are added to a 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**.

20.5.4 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 Applications** → **Configure 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. 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.

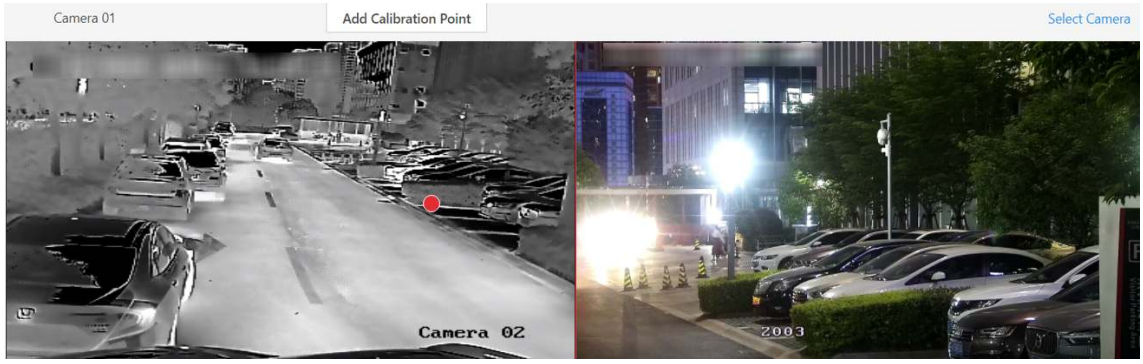


Figure 20-10 Manual Calibrating

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 20-11 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.

20.6 Video Settings

In Video Settings, you can set recording templates, capture schedule, scheduled report and network parameters.

20.6.1 Configure Storage and Recording

Before you can play back video files recorded by cameras, you need to set the time periods for video recording and the location for storing video files and pictures first. Also, before you can import pictures (e.g., static e-map picture) and view pictures (e.g., alarm-related pictures) uploaded from devices, you need to set storage locations for these pictures and set related parameters.

HikCentral Professional provides four storage locations (encoding devices, Hybrid Storage Area Network, Cloud Storage Server, and pStor) for storing the recorded video files of the cameras.

Encoding Device

Store video files on the encoding devices (i.e., DVR, NVR, and network camera) locally. Take NVR for an example, the video files recorded by the cameras linked to it will be stored in its storage medium (e.g., HDDs, Net HDDs, and SD/SDHC cards) if you select **Encoding Device** as the storage location.

To store video files in this way, you need to make sure the encoding device is equipped with a storage medium and the storage medium should have been formatted.

Perform the following operations to format storage medium if required:

Go to the remote configuration page of the encoding device (→ **All Modules → General → Resource Management → Encoding Device →**), and then click **Storage → Storage Management → HDD Management → Format** to initialize the selected storage device.

Hybrid Storage Area Network

Store the video files in the added Hybrid Storage Area Network. For details about adding Hybrid Storage Area Network, refer to ***Add Hybrid Storage Area Network*** .

Cloud Storage Server

Store the video files in the added Cloud Storage Server. For details about adding Cloud Storage Server, refer to ***Add Cluster Storage Server*** .

pStor

Store the video files in the added pStor, which is the storage access service used for managing local HDDs and logical disks. For details about adding pStor, refer to ***Add pStor*** .

pStor Cluster Service

pStor Cluster Service is a service that can manage multiple pStors. When there are multiple pStors storing a large number of video files, use pStor Cluster Service to manage these pStors. For details about adding pStor Cluster Service, refer to ***Add pStor Cluster Service*** .

Configure Recording Schedule Template

Recording schedule is time arrangement for video recording. You can configure the recording schedules to record video in a certain period. Two default recording schedules are available: All-day Time-based Template and All-day Event-based Template. All-day Time-based Template can be used for recording videos for all day continuously, and All-day Event-based Template is for recording videos when alarm is triggered. You can also customize the recording schedule.

Perform this task when you need to customize the schedule to record the video files.

Steps

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.

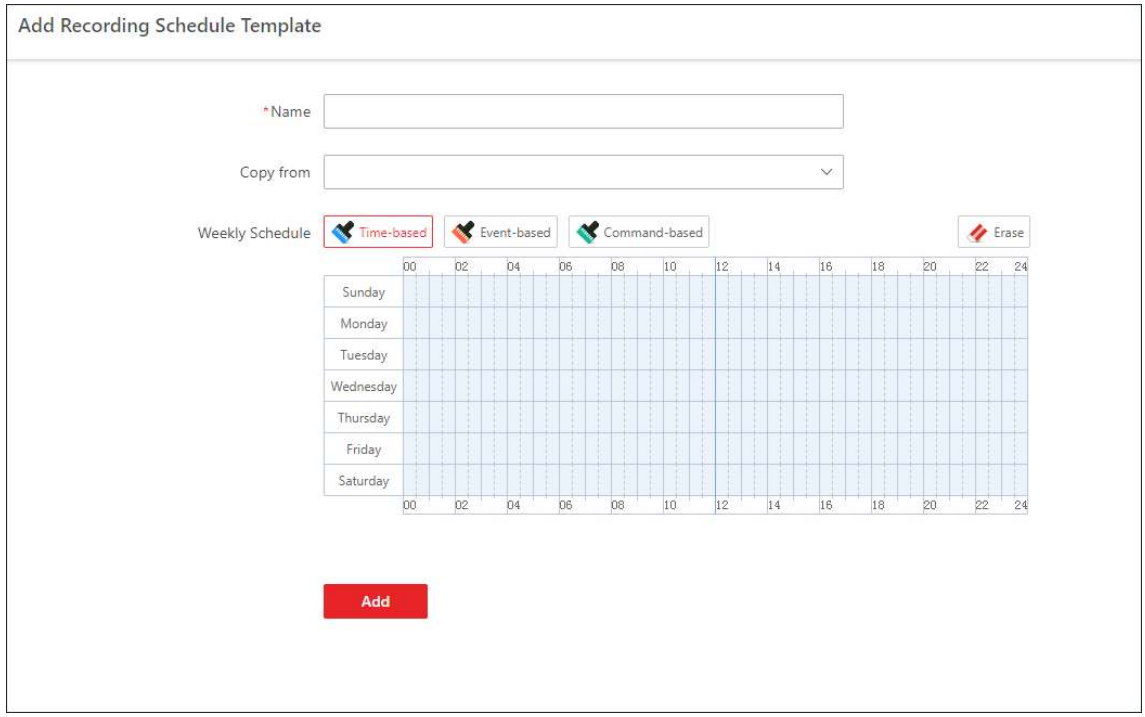


Figure 20-12 Adding Recording Schedule Template Page

3. Set the required information.

Name

Set a name for the template.

Copy from

Optionally, you can select to copy the settings from other defined templates.

4. Select a recording type and drag on the time bar to draw a time period.

Note

By default, the Time-based is selected.

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.

Note

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

5. **Optional:** Click **Erase** and click on the time bar to clear the drawn time period.
6. Click **Add** to add the template and back to the recording schedule template list page.
7. **Optional:** Perform the following operations on the recording schedule template list page.

View Template Details	Click the template to check the detailed settings.
Delete Template	Click to delete a template.

Configure Capture Schedule

You can add a capture schedule to determine when and which camera will capture pictures.

Steps

1. In the top left corner of Control Client, select → **Video** → **Video Settings** → **Capture Schedule** .
2. Click + to add a capture schedule.

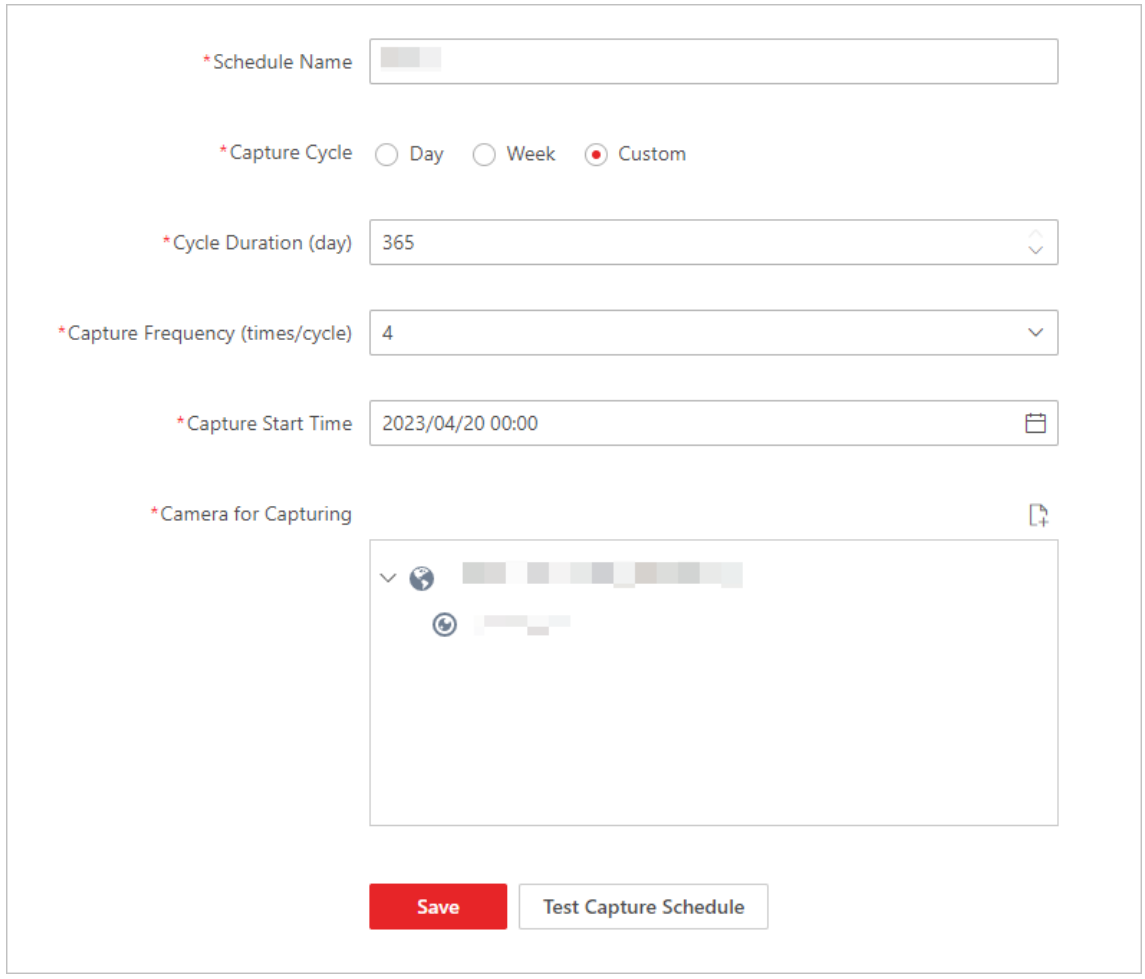


Figure 20-13 Configure Capture Schedule

3. Set a schedule name.
4. Set the capture cycle as **Day**, **Week**, or **Custom**.
5. Set a value for capture frequency.
6. Set a time of starting the task.
7. Select camera(s) and/or preset(s) for capturing.
8. Click **Add**.

   The added schedule will be displayed on the left pane.
9. **Optional:** Click **Test Capture Schedule** to see if the selected resource(s) function properly.

Configure Scheduled Report

You can add a scheduled report so that captured pictures will be sent regularly via email.

Before You Start

Make sure you have added a capture schedule. For details, see ***Configure Capture Schedule*** .

Steps

1. In the top left corner of Control Client, select → **Video** → **Video Settings** → **Scheduled Report** .
2. Click + to add a scheduled report.

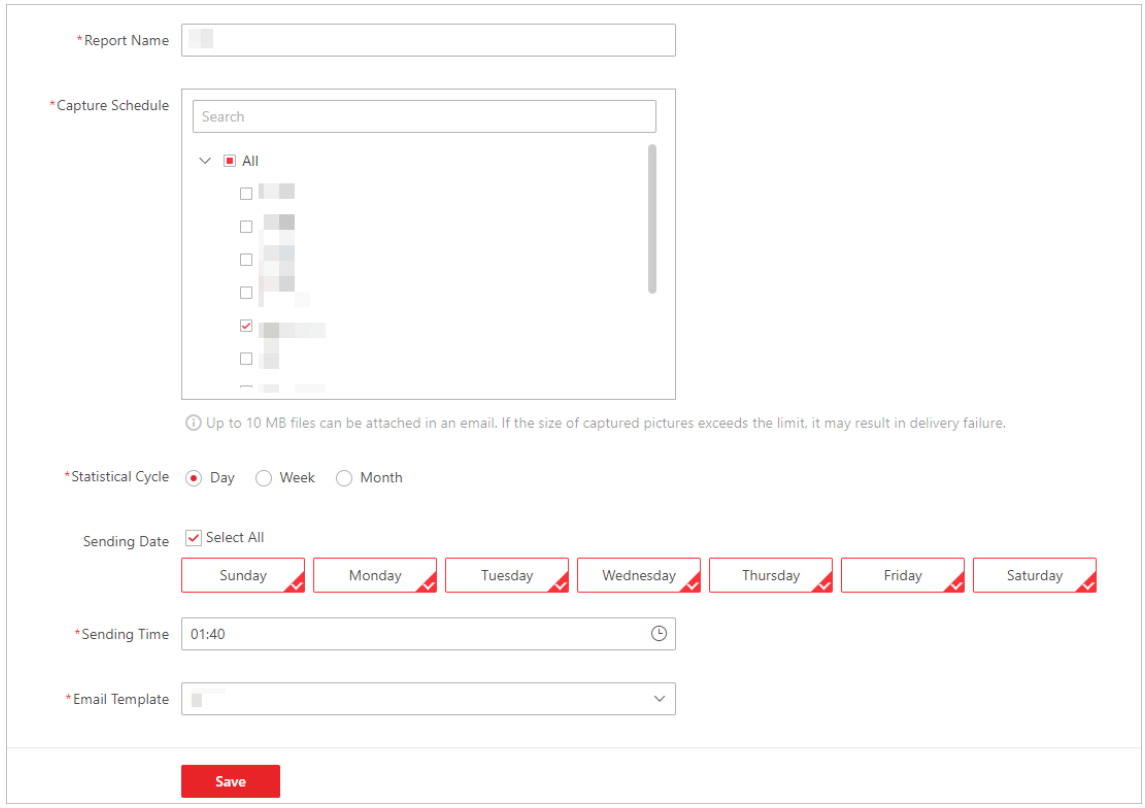


Figure 20-14 Add a Scheduled Report

3. Set the report name, capture schedule, statistical cycle, sending time, email template, and report language.

Note

You can click **Add** to add a new email template. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

4. Select the language as **Report Language**.

Note

By default, the language is the same with the selected language when you log in on the Web Client.

5. Click **Save**.

The added report will be displayed on the left pane.

Configure Recording for Cameras on Current Site

For cameras on the current site, HikCentral Professional provides five storage methods (storing on encoding devices, Hybrid Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service) for storing the video files of the cameras according to the configured recording schedule. You can get device's recording settings when adding camera to an area.

Before You Start

Encoding devices need to be added to the HikCentral Professional for area management. Refer to ***Device and Server Management*** for detailed configuration about adding devices.

Steps

1. Enter the **Recording Setting** tab.
   1) In the top left corner of the Home page, select → **Basic Management** → **Device** → **Area** .
   2) Select an area to show its cameras.

   Note

   For Central System with Remote Site Management module, you can select the current site (marked with icon) from the drop-down site list to show its cameras.
   3) Select a camera and click its name to enter camera settings page.
   4) Select the **Recording Settings** tab.
2. Turn on **Main Storage**.
3. Select the storage location for storing the recorded video file.
4. Select the storage type and configure other required parameters.
   - 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 Storage Area Network**, **Cloud Storage Server**, **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. For details about setting customized template, refer to ***Configure Recording Schedule Template*** .

View

View the template details.

Note

The event-based recording schedule can not be configured for the **Cloud Storage Server**, and the command-based recording schedule can not be configured for the **Cloud Storage Server** and **pStor**.

Stream Type

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

Note

For storing on Hybrid Storage Area Network, Cloud Storage Server, 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, Cloud Storage Server, 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 Storage Area Network. It is available for the camera that is configured with event-based recording.

Video Expiration

If you select **Encoding Device** as the storage location , set **Video Expiration** switch to on 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 Storage Area Network** 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

- Make sure you have configured recording schedule stored in the device local storage or pStor for auxiliary storage first. Otherwise, the scheduled copy-back is not configurable.
- The recordings can be copied only from the encoding device to Hybrid Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service, or from pStor to another pStor.

Copy in

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.

5. **Optional:** Set the **Auxiliary Storage** switch to ON and configure another storage location for the video files.

Note

- If Cloud Storage Server, Hybrid Storage Area Network, 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 Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service, or from pStor to another pStor.

6. Click **Save**.

Configure Recording for Cameras on Remote Site

You can set recording schedule to record the video of cameras on Remote Sites and stores in the Central System's Recording Servers (Hybrid Storage Area Network, Cloud Storage Server, pStor or pStor Cluster Service).

Steps

1. Go to the **Recording Settings** tab.
   1) In the top left corner of the Home page, select → **Basic Management** → **Device** → **Area** .
   2) Select the added Remote Site form the drop-down list.

   Note

   The icon indicates that the site is Remote Site.

   3) Select an area to show the cameras added to it.

4) Select a camera and click its name to enter the camera settings page.
5) Select **Recording Settings** tab.

2. In the Recording Settings area, turn on **Storage in Central System**.
3. Select the storage location for storing the recorded video file.
4. Select the storage type and configure the required parameters.
   - Select **Real-Time Storage** as the storage type to store the recorded video files in the specified storage location at the real time.

Note

You can select **Hybrid Storage Area Network**, **Cloud Storage Server**, **pStor**, or **pStor Cluster Service**, specify a server and (optional) select a Streaming Server to get the video stream of the camera via it.

Recording Schedule Template

Set the template which defines when 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. For details about setting customized template, refer to ***Configure Recording Schedule Template*** .

View

View the template details.

Stream Type

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

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 Cloud Storage Server, pStor, or pStor Cluster Service, and it is available for the camera that is configured with event-based recording.

Post-Record

Start recording the video from periods following detected events.

This field displays when the storage location is set as Hybrid Storage Area Network, and it is available for the camera that is configured with event-based recording.

Streaming Server

Optionally, select a **Streaming Server** to get the video stream of the camera via it.

Enable ANR

If you select the Storage Location as Hybrid Storage Area Network, check **Enable ANR** to turn the automatic network replenishment on to temporarily store the video in the camera when network disconnects and transport the video to Hybrid Storage Area Network when network recovers.

- Select **Scheduled Copy-Back** as the storage type and specify period, main/auxiliary storage, recording type and uploading speed to upload the recorded video files from the device local storage or pStor on the Remote Site to the specified storage location according to scheduled period.

Note

Make sure you have configured recording schedule stored on encoding device or pStor for the camera on the remote site.

5. Click **Save**.

Configure Storage for Imported Pictures and Files

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 the HDD of SYS server. You can configure the storage locations and the corresponding quotas for them.

Steps

Note

You can configure the storage only when the current Web Client is running on SYS server.

1. In the top left corner of the Home page, select → **Basic Management** → **System** .
2. Select **Storage** → **Storage on SYS Server** on the left.

   The disks of the SYS server are displayed with current free space and total capacity.
3. Switch on **Enable Local Storage**.
4. 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.
5. 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.

6. Click **Save**.

Configure Storage for Uploaded Pictures

The pictures uploaded from the devices, such as alarm triggered pictures, captured face pictures, and captured plate license pictures, can be stored on the HDD of SYS server, Hybrid Storage Area Network, Cloud Storage Server, pStor, or NVR (Network Video Recorder).

Steps

1. Enter the picture storage setting page.
   1) In the top left corner of the Home page, select → **Basic Management** → **Device** → **Area** → **Camera** .
   2) Select an area to show its cameras.

   Note

   For Central System with Remote Site Management module, you can select the current site (marked with icon) from the drop-down site list to show its cameras.

   3) Select a camera and click its name to enter the camera settings page.
2. Select the **Picture Storage Settings** tab.
3. Switch on **Picture Storage**.
4. Select the storage location from the drop-down list.

   Note

   - If you select System Management Server, the pictures will be stored on the SYS server. Click **Configuration** 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 ***Configure Storage for Imported Pictures and Files*** for details.
   - You cannot configure the storage location for the captured undercarriage pictures, which are stored on the UVSS device.

5. Click **Save** to save the uploaded pictures to the specified location.

20.6.2 Set Network Parameters

You can set parameters for registering the platform without Remote Site Management module (or Remote Site) to the Central System, and set access mode for encoding and decoding devices.

Steps

1. In the top left corner of the Home page, select → **Video** → **Video Settings** → **Network** .

2. Set network parameters.

Register to Central System

Switch on **Register to Central System** and enter the IP address and port No. of Central System to allow the system without Remote Site Management module (as we called Remote Site) to be registered to the Central System. Central System is the system that has Remote Site Management module and can group multiple Remote Sites together to form a larger-scale union. The purpose of grouping Central System and Remote Sites is to allow Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same system.

Note

- Before registering to the Central System, make sure you have enabled the Central System to receive the site registration. Refer to the parameter **Receive Site Registration** for details.
- Registering to Central System is only available for the system without Remote Site Management module.
- Open Service Manager (installed on the PC running central system's SYS service), and click **System Management Service** if you need to view or edit the Central System's port.

Receive Site Registration

Check the **Receive Site Registration** to allow the system with Remote Site Management module (or Central System) to receive the registration from Remote Sites. Remote Site is the system that does not have Remote Site Management module and can register to Central System to form a larger-scale union. The purpose of joining Central System and Remote Sites is to allow Central System's users to view and manage resources belonging to multiple Remote Sites simultaneously as if they were on the same system.

Note

- If a remote site needs to register to the Central System, it should open the Remote Site's Web Client and enter **Register to Central System** to configure the Central System's parameters. See ***Set Network Parameters*** for details.
- Allowing remote site registration is only available for the system with Remote Site Management module.

Device Access Mode

Set the device access mode to **Automatically Judge** or **Proxy** mode to define how the system accesses all the added encoding devices and decoding devices.

Automatically Judge

The system will automatically judge the condition of network connection and then set the device access mode accordingly as accessing directly or accessing via Streaming Gateway and Management Service.

Proxy

The system will access the device via Streaming Gateway and Management Service. It is less effective and less efficient than accessing directly.

Note

The two parameters **Register to Central System** and **Receive Site Registration** are not available at the same time.

3. Click **Save**.

Chapter 21 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.

21.1 Configure Scenario

There are two scenarios available: public scenario and 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 and then cleared.

21.2 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.

21.2.1 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.

Steps

1. In the top left corner of the Client, select → **Operation Analytics** → **Intelligent Analysis** → **Dashboard** .
2. Select a store or multiple stores.

3. **Optional:** You can perform the following operations.

Operation	Description
Set Report Time	Click **Day**, **Week**, **Month**, **Year**, **Promotion Day** or **Custom** to select the report time.
View Parameter Meaning	Hover your cursor over the top right corner of a certain parameter, and you will see the explanations of the parameter.
Export Report	• Click **Export** to display the Export panel. • Select Excel, CSV, or PDF as the format of the exported report(s). • Click **Export**.
Expand Dashboard/Report	Click ⤢ to view the dashboard or report more clearly.

21.2.2 Manage 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.

Add a Single Store

You should add a store before generating reports of stores.

Steps

Note

Make sure you have switched the scenario to Retail/Supermarket scenario. For details, refer to ***Configure Scenario*** .

1. In the top left corner of Home page, select → **Operation Analytics** → **Intelligent Analysis** → **Store Management** → **Configure Store** .
2. Open the Add Store panel.
   - If you have not added any store yet, you can click **Add Store** on the page to open the Add Store panel.
   - If you have added stores, you can click + in the top left corner to open the Add Store panel.
3. Set store parameters.
   1) Set store name.

2) Select an area for the store.
3) Set business hours for the store.
4) Set the store location on the map, and its coordinates will be automatically generated.
5) Select **Single Floor** or **Multiple Floors** for the store.
6) **Optional:** (Optional) Set names for each floor if you select **Multiple Floors**.
7) Click **Save**.

4. Add resources to the store.

1) 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.

2) Click **Add** to add entries & exits in the Configure People Counting section.
3) (Optional) Switch on **Regularly Clear All**, and set a time when all data will be cleared.
4) (Optional) Select entries and exits of the store.
5) (Optional) 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.
6) (Optional) Click **Configure Actual People Counting Task** to configure who will be excluded when counting people.

Note

For details, refer to ***Add Customer Traffic Task Excluding Staff*** .

7) (Optional) Switch on **Staff-Excluded People Count** to count people excluding those such as store staff to get more accurate people counting statistics. After enabling the function, you can sync the deduplication interval from device, and you can also batch configure the deduplication interval and apply it to devices.

Note

The same face of people (excluding staff) will be counted once even if it appears many times during the deduplication interval.

8) Click **Save and Continue**.

5. Add resources to floor.

1) Select a floor under the Resource tab on the right pane.
2) Drag the resources to the left map.
3) Click **Finish**.

You will see a dashboard displaying resource status.

6. **Optional:** Perform the following operations for managing added stores.

Edit the Store Information	Select a store and click **Edit** on the right top corner to edit the store information.
Delete Store(s)	• Delete a single store:

	Select a store from the store list panel and click to delete it. • Batch delete multiple stores: Check multiple stores of a site and click **Delete** to delete selected stores.
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**. • 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**. **Note** The opening hours of store(s) should be within one day.
Search Store	Enter a keyword in the search field on the upper-right corner of the page to search for the store.
View Resource Capability Status	After you add a store, click the store, and click **Resource Capability** to view resource status, including the online status and data uploading status.

Batch Add Stores

You can batch add stores by template before generating reports of stores.

Steps

Note

Make sure you have switched the scenario to Retail/Supermarket scenario. For details, refer to ***Configure Scenario*** .

1. In the top left corner of Home page, select → **Operation Analytics** → **Intelligent Analysis** → **Store Management** → **Configure Store** .
2. Open the Batch Import panel.
   - If you have not added any store yet, you can click **Batch Import** on the page to open the Batch Import panel.
   - If you have added stores, you can click in the top left corner to open the Batch Import panel.
3. Click **Download Template** to download the store template and save it to your PC.
4. In the downloaded template, enter the store information (such as store name, site, and area) following the rules shown in the template.
5. Click , and then select the template from your PC.
6. Click **OK**.

The importing progress shows and you can check the results.

7. **Optional:** Perform the following operations for managing added stores.

Edit the Store Information	Select a store and click **Edit** on the right top corner to edit the store information.
Delete Store(s)	• Delete a single store: Select a store from the store list panel and click to delete it. • Batch delete multiple stores: Check multiple stores of a site and click **Delete** to delete selected stores.
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**. • 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**. **Note** The opening hours of store(s) should be within one day.
Search Store	Enter a keyword in the search field on the upper-right corner of the page to search for the store.
View Resource Capability Status	After you add a store, click the store, and click **Resource Capability** to view resource status.

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 → **All Modules** → **Intelligent Analysis** → **Store Management** → **Configure Promotion Day** .
2. Click **Add** to open the promotion day configuration page.



Figure 21-1 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 page, 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.

Send Store Analysis Report Regularly

You can set scheduled reports to designated recipients.

Steps

1. In the top left corner of Home page, select → **Operation Analytics** → **Intelligent Analysis** → **Store Management** → **Scheduled Report** .
2. Open the Create Report panel.
   - If you have not added any scheduled report yet, you can click **Add** on the page to open the Create Report panel.
   - If you have added stores, you can click + in the top left corner to open the Create Report panel.
3. Set basic information such as report name, report type, report language.
4. 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.
5. Set the report contents.

   Statistics Target

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.

Configure 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.

Configure 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.

6. In the Advanced Settings section, perform the following operations as you need.
   1) Switch on **Send Report 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. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .
   2) 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 in the top left corner to edit SFTP settings. For details, refer to the table below.
   3) 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 in the top left corner to edit the saving path of local storage. For details, refer to the table below.
7. Click **Add**.
8. 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. • Click **SFTP Settings** to configure the SFTP settings, including SFTP address, port number, user name, password, and saving path. • Click **Configure Local Storage** to set the local saving path.

21.2.3 View Store Report

If you choose the Retail/Supermarket scenario, you can view store reports of a single store, two stores, and multiple stores.

View Single Store Report

You can view reports of a single store.

In the top left corner of the Client, select → **Intelligent Analysis** → **Store Report** → **Single Store Report** .

Set Parameters

Operation	Description
Set Report Time	Click **Day/Week/Month/Year/Custom** to select the report time.
View Parameter Meaning	Hover your cursor on the top right corner of a certain parameter, and you will see the explanations of the parameter.
Set Report Contents	Click **Set Report Contents** to open the Set Report Contents pane.

Operation	Description
	• Switch on **Stick Statistics on Top**, and check the items so that they will be displayed on the top of the report. • 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. For details, refer to ***Send Store Analysis Report Regularly*** .

View Reports

On the top of the page, the set contents are displayed. Hover your cursor on the top right corner of a certain parameter, and you will see the explanations of the parameters.
In the People Counting Trend section, you can see the daily and hourly trend of people counting (in), people counting (in + passby), and walk-in rate.
In the People Counting Details section, you can see data collected from each floor and their rankings.
Click **Export** to display the Export panel. Select Excel, CSV, or PDF as the format of the exported report(s). Select By Day, By Hour, or By Month as the report dimension. Finally click **Export**.

View Multiple-Store Reports

You can view reports of multiple stores.

In the top left corner of the Client, select → **Intelligent Analysis → Store Report → Multiple-Store Report** .

Click to select multiple stores.

You can perform the following operations.

Operation	Description
Set Report Time	Click **Day/Week/Month/Year/Custom** to select the report time.
View Parameter Meaning	Hover your cursor on the top right corner of a certain parameter, and you will see the explanations of the parameter.

Operation	Description
Set as Scheduled Report	Click **Set as Scheduled Report** to set the current report as a scheduled report. For details, refer to ***Send Store Analysis Report Regularly*** .
Export Report	• Click **Export** to display the Export panel. • Select Excel, CSV, or PDF as the format of the exported report(s). • Select By Day, By Hour, or By Month as the report dimension. • Click **Export**.

Comparison Report

You can view comparison reports of two stores.

In the top left corner of the Client, select → **Intelligent Analysis → Store Report → Comparison Report** .

Click to select two stores.

You can perform the following operations.

Operation	Description
Set Report Time	Click **Day/Week/Month/Year/Custom** to select the report time.
View Parameter Meaning	Hover your cursor on the top right corner of a certain parameter, and you will see the explanations of the parameter.
Set as Scheduled Report	Click **Set as Scheduled Report** to set the current report as a scheduled report. For details, refer to ***Send Store Analysis Report Regularly*** .
Export Report	• Click **Export** to display the Export panel. • Select Excel, CSV, or PDF as the format of the exported report(s). • Select By Day, By Hour, or By Month as the report dimension. • Click **Export**.

View Store Promotion Day Report

You can 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).

1. In the top left corner of the platform, select → **Intelligent Analysis → Store Report → Store Promotion Day Report** .
2. Check stores in the drop-down list. You can also enter the store name in the search field to search for the store.
3. Select a promotion day for generating a report of store(s) on that day.
   The corresponding report of selected store(s) on the promotion day is displayed.
4. (Optional) Export the report.
   - Click **Export** to display the Export panel.
   - Select Excel, CSV, or PDF as the format of the exported report(s).
   - Select By Day, By Hour, or By Month as the report dimension.
   - Click **Export**.

21.2.4 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.

View 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.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis → Analysis Center → People Counting** .
2. Select Store / Entry & Exit / Camera as the report target.
3. **Optional:** Perform the following operation(s).

Set Report Time	Click **Day/Week/Month/Year/Promotion Day/Custom** to select the report time.
Export Report	a. Click **Export**. b. Set the format of the exported file as Excel, CSV, or PDF. c. Select the time dimension as **By Hour**, **By Day**, or **By Month**. d. Click **Export**.

View 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.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Analysis Center** → **Person Feature Analysis** .
2. Select Store/Camera as the report target.
3. **Optional:** Perform the following operation(s).

Set Report Time	Click **Day/Week/Month/Year/Promotion Day/Custom** to select the report time.
Export Report	a. Click **Export**. b. Set the format of the exported file as Excel, CSV, or PDF. c. Select the time dimension as **By Hour**, **By Day**, or **By Month**. d. Click **Export**.

View Store Heat Analysis Report

You can generate a heat analysis report to track consumer movements and analyze the visit times and dwell time in a configured area.

Before You Start

- Add 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.
- Add 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*.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Analysis Center** → **Heat Analysis** .
2. Select Store/Camera as the report target.
3. Switch the report type (daily, weekly, monthly, annual, and custom) by setting the statistical cycle as **Day**, **Week**, **Month**, **Year**, **Promotion Day**, or **Custom**.

   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.

   Weekly Report, Monthly Report, and Annual Report

As compared to daily report, weekly report, monthly, and annual 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, every month, or every year, which contains analysis results on the last 7 days, last month, or last year before the sending date.

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

You 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. 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.

5. **Optional:** Perform the following operation(s).

Switch Statistical Dimension	Select **Heat map represents people count** or **Heat map represents dwell duration**.
Filter Data	• You can set the dwell duration to get statistics within the configured range. 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. • You can 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.
Export Report	a. Click **Export**. b. Set the format of the exported file as Excel, CSV, or PDF. c. Select the time dimension as **By Hour**, **By Day**, or **By Month**. d. Click **Export**.

Generate 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.

Before You Start

- Properly add 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 Pathway Analysis Group*** .

Steps

Note

This function is only supported by the second generation of fisheye cameras.

1. In the top left corner of the platform, select → **Intelligent Analysis → Analysis Center → Pathway Analysis** .
2. Select a store.

   The static map with the cameras and pathways color coded on the map will be displayed. The red color block (255, 0, 0) indicates the most welcome pathway (most persons detected or longest dwell time), and blue color block (0, 0, 255) indicates the less-popular pathway (least persons detected or shortest dwell time).
3. Select the report type as daily report, weekly report, monthly report, annual report, promotion day report, or customize the time interval for a report.

   Daily Report

   Daily report shows data on a daily basis. The platform will calculate the number of people or people dwell time 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 reports show 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 in the Time field for statistics.

Note

For custom time interval report, you need to set the start time and end time to specify the time period.

5. Move the cursor to the camera hot spot to view the line chart or heat map of the people amount and people dwell time in the pathways during this time period.
6. **Optional:** Export the report to the local PC.
   1) Click **Export**.

      The Export panel will display with camera selected and time configured according to the range you defined previously.
   2) Set the format of the exported file as Excel, CSV, or PDF.
   3) Select shorter time period to view more detailed data of each camera.

      Example

      For example, if you select Daily Report, you can select **By Day** or **By Hour**, and it will export 1, 24 records respectively for each camera.
   4) Click **Export**.

Generate 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.

Before You Start

Add 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.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Analysis Center** → **Queue Analysis** .
2. Select a store/camera to search for queue data.

   A queue analysis report of the selected camera/store is 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).

Edit Statistic Range	a. Click **Set Queue Statistics**. b. Set the statistic range of waiting time and number of queuing people. For example, if you set the queue duration as Range1 < 300 < Range 2 <600 < Range 3. The platform will calculate the distribution of three ranges (shorter than 300 seconds, from 300 to 600 seconds, and longer than 600 seconds). c. Click **Save**.
Export Report	a. Click **Export** to export the report to the local PC. b. Set the format of the exported file as Excel, CSV, or PDF. c. Select the time dimension as **By Hour**, **By Day**, or **By Month**. d. Click **Export**.

21.3 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.

21.3.1 Customize 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.

Steps

1. In the top left corner of the Client, select → **Operation Analytics** → **Intelligent Analysis** → **Dashboard** .
2. **Optional:** On the top left corner, click **New Dashboard** → **Add Dashboard** on the report dashboard page and create a name to add a new dashboard.

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:** Edit dashboard(s).
   1) Click to expand the added dashboard(s).
   2) Click to edit the dashboard name or click to delete the dashboard.
4. Add report(s) to a dashboard and edit the report(s).
   1) Click **Add Report**.
   2) Select a report type and generate the report.
   3) Click **Add** on the report page to add the report to dashboard.

      The report appears on the selected dashboard.
   4) Perform the following operations.
      - Add More Reports: Click **Add Report** to add more reports to the dashboard.
      - View Report in Larger Window: Click to view the report in larger window.
      - Edit Report Name: Click and then click **Edit**.
      - Delete Report from Dashboard: Click and then click **Delete**.
5. Switch time to view report data.
   1) Select a dashboard and then click **Switch Time to View** to set the report type and time.

      Report Type

      Select the time basis for the reports. For example, daily report shows data on a daily basis.

      Time

      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.
   2) 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. **Optional:** Export report(s) on the dashboard to the local PC.
   1) Click **Export** to display the Export panel.
   2) Select report(s) from the report list.
   3) Select **Excel**, **CSV**, or **PDF** as the format of the exported report(s).
   4) Click **Export**.

21.3.2 View Intelligent Analysis Report

In the public scenario, to view intelligent analysis reports including people counting analysis, person feature, heat analysis, pathway analysis, queue analysis, people density analysis, and temperature analysis, you should configure corresponding analysis groups / camera(s) in advance.

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.

Before generating a people counting report, you can add people counting group(s) to group the doors and people counting cameras of a certain region so as to define region border. After that, you can set a regular report rule for the specified cameras which support people counting or people counting groups, and the platform will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a people counting report at any time to view the data if required.

For details about adding a people counting group, refer to ***Add People Counting Group*** .

Add 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 border. 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.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis → Analysis Group → People Counting Group** .
2. Click **Add**.
3. Set basic configurations.
   1) Create a name for the group.
   2) Select a site.
   3) (Optional) Switch on the **Maximum Number of Persons** and enter the maximum number of persons that can enter the area monitored by this group.
   4) (Optional) Switch on the **Regularly Clear All** and set a time for clearing all data regularly.
   5) (Optional) Switch on the **Staff-Excluded People Count** to count people excluding those such as store staff to get more accurate people counting statistics.

Note

You can click **Configure** to go to Customer Traffic Excluding Staff page.

6) Click **Save and Continue**.

4. Configure resources for counting people.

1) In the **Resource for Counting People** part, click **Add** to select the resources (including doors and people counting cameras) for calculating the number of people stayed in this region.
2) Click **Edit** to select statistics type, and In/Out Direction, and click **Save**.

Note

- You can set **Statistics Type** as **Total Entries**, **Total People Passed By**, and **Total People Entered/Passed By**. The reports will display and only display the data concerning the statistics type that you select.
- For doors, the access records on the entry reader will be calculated as person entered this region while the access records on the exit one will be calculated as person exited this region.
- For cameras, the people crossing along the entry direction will be calculated as person entered this region while the people crossing along the exit one will be calculated as person exited this region.

3) Click **Save and Continue**.

5. Add the people counting group to a map.

1) Drag the people counting group from the Resource Group list on the right to the map.

The region as well as the doors and cameras in the group will be added on the map.

2) Drag to draw the region according to actual needs.
3) Drag the icons of the doors and cameras onto the map to set the their locations on the map.
4) Right click to finish.

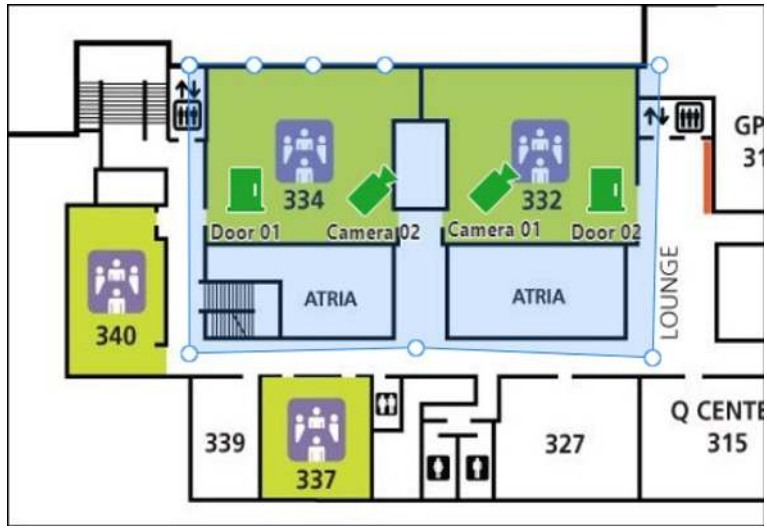


Figure 21-2 Draw People Counting Group on Map

5) Click **Finish**.

The people counting group is displayed on the list.

Generate 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.

Before You Start

Make sure you have properly configured the camera with a people counting rule for the required area. To configure the people counting rule, refer to the user manual of people counting camera.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis → Report → 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 People Counting 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.

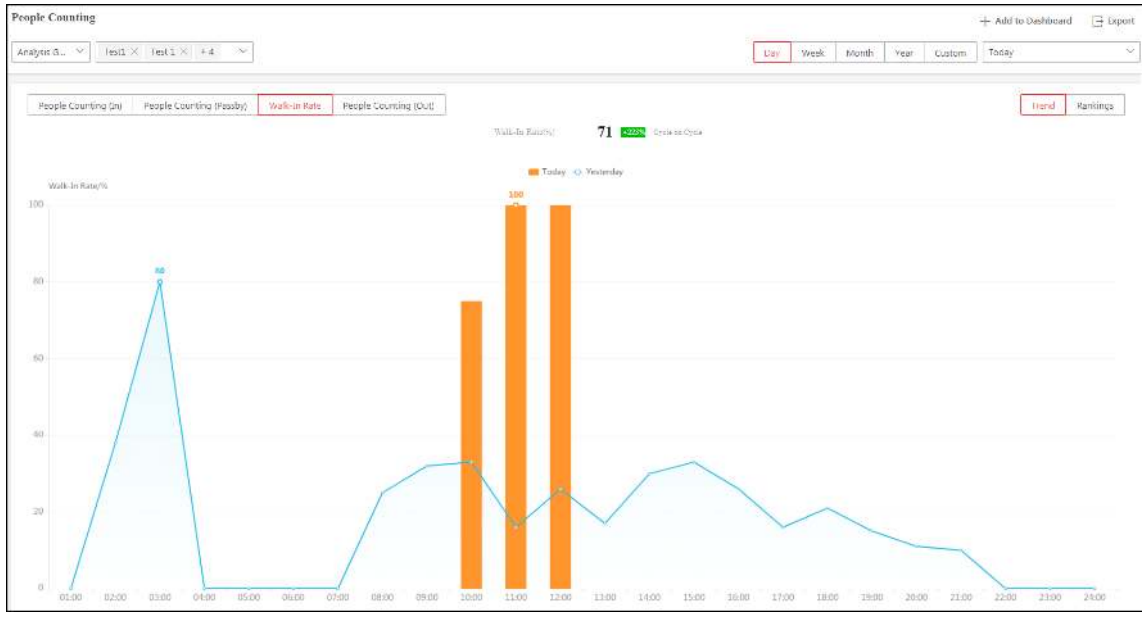


Figure 21-3 People Counting Report

The corresponding report of selected camera(s)/group(s) is displayed.

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. **Optional:** Perform the following operation(s) after generating the people counting report.

Switch Between Trend Report and Rankings Report	**Note** It is invalid when you select only one camera/group. Click **Trend** or **Rankings** on the upper-right corner to switch between trend report (displaying the trend of people counting statistics at different time)

	and rankings report (displaying the statistics of different cameras/groups for comparison).
Add to Dashboard	a. Click **Add to Dashboard** in the upper-right corner of the page. b. Create a report name. c. Select a dashboard. Or click **New** to create a new board and then select it. d. Click **OK** or **Add and Go to Dashboard**.
Export Report	a. Click **Export**. b. Set the format of the exported file as Excel, CSV, or PDF. c. Select the time dimension as **By Hour**, **By Day**, or **By Month**. d. Click **Export**.

Send People Counting Report Regularly

You can set a regular report rule for specified people counting cameras or specified people counting groups, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the number of people entered or exited detected by people counting cameras, or the number of people stayed calculated by the people counting cameras and doors in the same region.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email settings such as the sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Analysis Group** → **Scheduled Report** .
2. Click **Add** or + in the upper-left corner to open the Create Report page.
3. Create a name for the report.
4. Select the report category as **People Counting Analysis**.
5. Select the 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 the analysis type.

People Counting for One Region

The report contains the number of people stayed in one region, which is calculated by the detected people from the people counting camera(s) and the statistic people from the doors in the region. You need to select the people counting group(s) as the Report Target.

People Counting for One Camera

The report contains the number of people entered and exited detected by the people counting camera(s). You need to select the camera(s) as the Report Target.

For example, if you select the people counting type as **People Counting for One Camera** and select two people counting cameras as the **Report Target**, the platform will generate two reports of the cameras respectively, including the number of people entered and exited detected by the two cameras.

7. Select the people counting camera(s) or groups contained in the report.

Note

If you select **People Counting for One Camera** as the analysis type, you should select camera(s). If you select **People Counting for One Region**, you should select people counting group(s).

8. 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.

9. Set how the report will present the results analyzed in the specified time period.

Example

For example, if you select the report type as **By Day**, 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 analysis results in each hour or each minute for one camera.

10. Set the report time and sending time according to the report type.
11. **Optional:** Set the effective period (start time and end time) in which the reports will be regularly sent.
12. **Optional:** Switch on **Send Report 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. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

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 ⚙ at the top of report list and click **SFTP Settings** from the drop-down list to enter the configuration pane.

14. **Optional:** Switch on **Local Storage**, and click **Configure** beside **Saving Path** to configure the saving path of local storage.

Note

You can also hover the cursor on ⚙ at the top of report list and click **Configure Local Storage** from the drop-down list 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.

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.

Before using heat analysis report, you can add a heat analysis group to define the region for heat analysis. After that, you can set a regular report rule for the specified cameras or the specified heat analysis groups, and the system will send emails with heat analysis reports attached to the target

recipients daily, weekly, or monthly. You can also manually generate a heat analysis report at any time to view the data if required.

For details about adding a heat analysis group, refer to ***Add Heat Analysis Group*** .

Add 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.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis → Analysis Group → Heat Analysis Group** .
2. Click **Add**.
3. Set basic configurations such as name, site, and store.
4. Add resources for calculating dwell time, resources for people counting, and analysis groups.
   1) Click **Edit** in the **Draw Count Area** column.
   2) Click to draw the count area for analyzing dwell rate, or you can click **Sync with Device** to sync with the count area on device.
   3) Name the drawn area.
   4) Click **Save**.
5. **Optional:** Add the group to the map by setting the locations of the resources in the group and setting the border of the region for detection.
   1) Drag the heat analysis group from the Resource Group list on the right to the map.

      The region as well as the doors and cameras in the group will be added on the map.
   2) Drag to draw the region according to the actual needs.
   3) Click **Set Camera Position**, and drag the icons of the doors and cameras to set the their locations on the map.
   4) Click **Save**.

   After adding the heat analysis group on the map, you can know the dwell time of the people stayed in the region, the number of persons stayed in the region, and average dwell time of each people.
6. Click **Finish**.

   The heat analysis group is added in the table and you can view the resources in the group.

Generate Heat Analysis Report

You can generate a heat analysis report to track consumer movements and analyze the visit times and dwell time in a configured area.

Before You Start

- Add 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.
- Add 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*.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis → Report → Heat Analysis** .
2. Select the report data resource type.

   Camera

   A heat analysis report based on the data from the camera you select will be generated.

   Analysis Group

   A heat analysis report based on the data from the heat analysis group you select will be generated.

   Note

   You should have added heat analysis group(s). For details, see ***Add Heat Analysis Group*** .
3. Select a camera or a heat analysis group based on the data resource type you set in the previous step.

   The corresponding report of the selected camera/group is displayed.
4. Switch the report type (daily, weekly, monthly, annual, and custom) by setting the statistical cycle as **Day**, **Week**, **Month**, **Year**, or **Custom**.

   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.

   Weekly Report, Monthly Report, and Annual 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.
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. **Optional:** Perform the following operation(s) after generating the heat analysis report.

Switch Statistical Dimension	Select **Heat map represents people count** or **Heat map represents dwell duration**.
Filter Data	• You can set the dwell duration to get statistics within the configured range. 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. • You can 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.
Highlight Ranking Data of Heat Area	The ranking of heat areas is based on the number of dwell people. Click a heat area on the map to highlight the row of the heat area in the ranking table.
Add to Dashboard	Click **Add to Dashboard** to add the current report to a dashboard.
Export Report	a. Click **Export**. b. Set the format of the exported file as Excel, CSV, or PDF. c. Select the time dimension as **By Hour**, **By Day**, or **By Month**. d. Click **Export**.

Send Heat Analysis Report Regularly

You can set a regular report rule for specified heat map cameras, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the heat map data (people dwell time at each location and number of people detected) during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Analysis Group** → **Scheduled Report** .

2. Click **Add** or + in the upper-left corner to open the Create Report page.
3. Create a name for the report.
4. Select **Heat Analysis** as the report category.
5. Select the 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.

Store Heat Analysis

A heat analysis report based on the data from the store will be generated.

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 Heat Analysis Group*** .

7. Select the stores, heat analysis camera(s) or groups contained in the report.

Note

If you select **Store Heat Analysis** as the analysis type, you should select store(s). 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. 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 Report 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. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .
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 **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.
14. **Optional:** Switch on **Local Storage**, and click **Configure** beside **Saving Path** to configure the saving path of local storage.

    Note

    You can also hover the cursor on , then click **Configure Local Storage** from the drop-down list 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.

Person Feature Analysis Report

Person feature analysis report shows the proportion of persons with different features detected by cameras which support facial recognition.

You can add a person feature 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. After that, you can set a regular report rule for the specified cameras or specified person feature analysis groups, and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a person feature analysis report at any time to view the data if required.

For details about adding a person feature analysis group, refer to ***Add Person Feature Analysis Group*** .

Add Person Feature Analysis Group

Person feature analysis is a group of cameras which support facial 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.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis → Analysis Group → Person Feature Analysis Group** .
2. Click **Add**.
3. Create a name for the group.
4. Select a site.
5. Select the cameras for analyzing the detected persons' features.
6. Click **Add**.

   The feature group is added in the table and you can view the cameras in the group.
7. **Optional:** Locate the person feature analysis group on the map by setting the locations of the cameras in the group and setting the border of the region for detection.
   1) Click **Set Geographic Location** to enter the Map Settings page.
   2) 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.
   3) Drag to draw the region according to the actual needs.
   4) Drag the icons of the cameras to set the their locations on the map.
   5) Right click to finish.

   After adding the person feature analysis group on the map, you can view the features of the persons appeared on the Control Client.

Generate 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.

Before You Start

Make sure you have added a person feature analysis group if you want to perform feature analysis in one region. See ***Add Person Feature Analysis Group*** for details about adding a person feature analysis group.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis → Report → Person Feature Analysis** .
2. Select camera(s) / analysis group(s).

Note

- Only online cameras will be displayed.
- Up to 20 cameras/groups can be selected for statistics at the same time.
- Both remote site and current site are supported.

The corresponding report of selected camera(s)/group (s) is displayed.

3. Set the statistical cycle as **Day**, **Week**, **Month**, **Year**, or **Custom**.
4. 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.

5. **Optional:** Click **Add to Dashboard** to display the report on the Dashboard.
6. **Optional:** Export the report to the local PC.
   1) Click **Export**.
   2) Set the format of the exported file as Excel, CSV, or PDF.
   3) Select the time dimension as **By Hour**, **By Day**, or **By Month**.
   4) Click **Export**.

Send Person Feature Analysis Report Regularly

You can set a regular report rule for specified cameras of person feature analysis, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the percentage and number of people of different features during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of the platform, select → **Intelligent Analysis → Analysis Group → Scheduled Report** .

2. Click **Add** or + in the upper-left corner to open the Create Report page.
3. Create a name for the report.
4. Select **Person Feature Analysis** as the report category.
5. Select the 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 analysis type.

Feature Analysis in One Region

Compare percentage and number of people of different features detected by the cameras in specified person feature analysis group(s) of multiple regions.

Feature Analysis for One Camera

Compare percentage and number of people of different features detected by specified camera(s).

7. Select the camera(s) or person feature analysis groups contained in the report.

Note

If you select **Feature Analysis for One Camera** as person feature type, you should select camera(s). If you select **Feature Analysis in One Region**, you should select feature analysis group(s).

8. 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.

9. Set the report time and sending time according to the report type.
10. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
11. **Optional:** Switch on **Send Report 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. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .
12. **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 click ⌄ on the right of ⚙ , then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.
13. **Optional:** Switch on **Local Storage**, and click **Configure** beside **Saving Path** to configure the saving path of local storage.

    Note

    You can also click ⌄ on the right of ⚙ , then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.
14. Click **Add**.
15. **Optional:** Click **Export** to export the report of this schedule for verifying the report sending schedule settings.

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.

You can set a regular report rule for the specified cameras, and the system will send emails with queue analysis reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a queue analysis report at any time to view the data if required.

Generate 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.

Before You Start

Add 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.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Report** → **Queue Analysis** .
2. Select a camera to search for queue data.
   1) Click to open the resource list.
   2) **Optional:** Click **Include Sub-Area** to allow the display of camera(s) in sub-areas.
   3) Select a site (current site / remote site) or an area to show cameras under the site/area.

   Note

   - Only the online cameras which support queue management will be displayed here.
   - You can also enter keywords of the camera name to search for cameras.

   4) Select a camera .

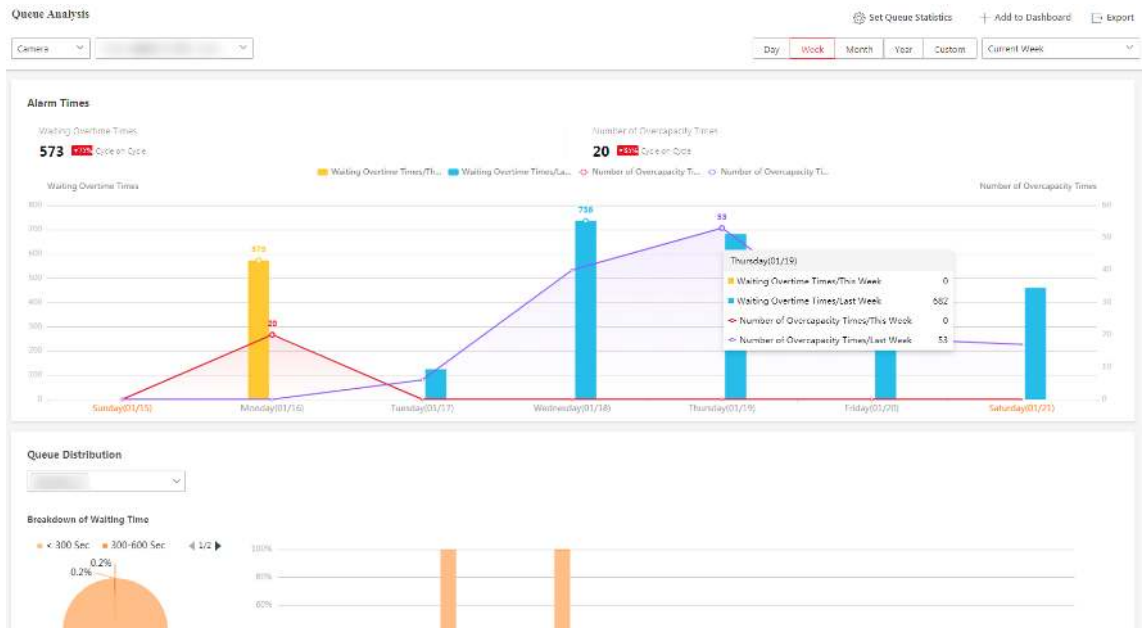


Figure 21-4 Queue Analysis Report

A queue analysis report of the selected camera is displayed.

3. **Optional:** Set the statistical cycle as **Day**, **Week**, **Month**, **Year**, 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, Annual Report

   As compared to daily report, weekly report, monthly report, and annual report can be less time-consuming, since they are not to be submitted every day. The system will calculate the queue data detected in each day of one week, in each day of one month, and in each month of one year.

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) after generating the report.

Add Report to Dashboard	a. Click **Add to Dashboard** in the upper-right corner of the page. b. Create a report name. c. Select a dashboard. Or click **New** to create a new board and then select it. d. Click **OK** or **Add and Go to Dashboard**.
Edit Statistic Range	a. Click **Set Queue Statistics**. b. Set the statistic range of waiting time and number of queuing people. For example, if you set the queue duration as Range1 < 300 < Range 2 <600 < Range 3. The platform will calculate the distribution of three ranges (shorter than 300 seconds, from 300 to 600 seconds, and longer than 600 seconds). c. Click **Save**.
Show/Hide Certain Data	Click the legend to show or hide the data of certain element.
Filter Queue Distribution Data by Queue	Click ⌄ under **Queue Distribution** to display configured queue(s), and filter the data of queue duration and number of queuing people by queue.
Export Report	a. Click **Export** to export the report to the local PC. b. Set the format of the exported file as Excel, CSV, or PDF. c. Select the time dimension as **By Hour**, **By Day**, or **By Month**. d. Click **Export**.

Send Queue Analysis Report Regularly

You can set a regular report rule for specified cameras which support queue management, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing queue exceptions, number of persons in the queue, and queue status including waiting duration and queue length, detected by these cameras during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of Home page, select → **Intelligent Analysis** → **Analysis Group** → **Scheduled Report** .
2. Click **Add** or + in the upper-left corner to open the Create Report page.
3. Create a name for the report.
4. Select the report category as **Queue Analysis**.
5. Select the 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 the camera(s) which support queue management contained in the report.

   Note

   Only cameras which support queue management will be displayed here.

   The report will show the data of all the queues configured on the cameras.

   Note

   For configuring the queue, refer to the user manual of the camera.
7. Set the statistic range of waiting time and number of queuing people.
8. 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.

9. Set the report time and sending time according to the report type.
10. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
11. **Optional:** Switch on **Send Report 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. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

12. **Optional:** Switch on **Upload to SFTP**.

Note

You can also hover the cursor on and click **SFTP Settings** to enter the panel to configure the corresponding information.

13. **Optional:** Switch on **Local Storage**.

Note

You can also hover the cursor on and click **Configure Local Storage** to enter the panel to configure the corresponding information.

14. Click **Add**.
15. **Optional:** Click **Export** to export the report of this schedule for verifying the report sending schedule settings.

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.

Before using pathway analysis, you should add pathway analysis groups first, which define the region for pathway analysis. After that, you can set a regular report rule for the specified pathway analysis group, and the system will send emails with pathway analysis reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a pathway analysis report at any time to view the data if required.

For details about adding a pathway analysis group, refer to ***Add Pathway Analysis Group*** .

Add 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.

Steps

Note

This function is only supported by the second generation of fisheye cameras. You should have configured intersection analysis rule for the fisheye camera. If not, click **Configuration** to set that on the remote configuration page of the device.

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Analysis Group** → **Pathway Analysis Group** .
2. Click **Add**.
3. Create a name for the group.
4. Select the fisheye cameras for calculating the number of people on different directions in specific pathway.
5. Click **Add**.

   The pathway analysis group is added in the table and you can view the cameras in the group.
6. **Optional:** Locate the pathway analysis group on the map by setting the locations of the fisheye cameras in the group and setting the directions for camera's exits.

   Note

   To define the camera's exits, refer to the user manual of the camera.

   1) Click **Set Geographic Location** to enter the Map Settings page.
   2) Drag the pathway 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.
   3) Drag the icons of the cameras to set the their locations on the map.
   4) Click an exit of the fisheye camera as starting point and then draw a line, indicating the direction of the pathway.
   5) Enter the pathway name and select an exit for this pathway.
   6) Click **Save** to save the pathway.
   7) Perform the above sub-steps to draw other pathways.

Note

You can also draw a line to link the exits of two fisheye cameras if there are two cameras in the pathway.

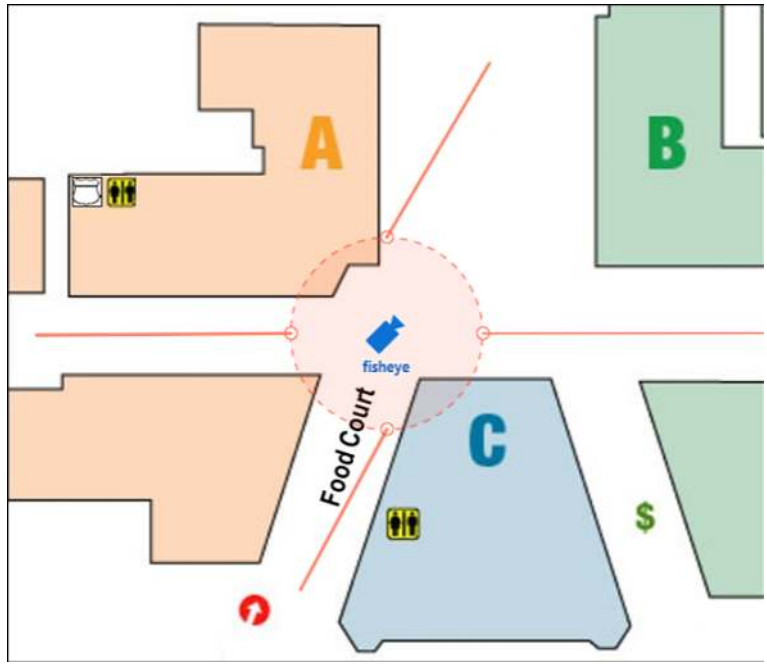


Figure 21-5 Add Pathway Analysis Group

8) **Optional:** Click the camera icon and select **Edit Direction Area** to set radius, view angle and direction.
9) Right click to finish.

After adding the pathway analysis group on the map, you can view the real-time number of people walking by on the Control Client.

Generate 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) 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.

Before You Start

- Properly add 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 Pathway Analysis Group*** .

Steps

Note

This function is only supported by the second generation of fisheye cameras.

1. In the top left corner of the platform, select → **Intelligent Analysis → Report → Pathway Analysis** .
2. Select a path analysis group for statistics.

   The remote site is not supported.

   The static map with the cameras and pathways color coded on the map will be displayed. The red color block (255, 0, 0) indicates the most welcome pathway (most persons detected or longest dwell time), and blue color block (0, 0, 255) indicates the less-popular pathway (least persons detected or shortest dwell time).
3. Select the report type as daily report, weekly report, monthly report, annual report, or customize the time interval for a report.

   Daily Report

   Daily report shows data on a daily basis. The platform will calculate the number of people or people dwell time in each hour of one day.

   Weekly Report, Monthly Report, 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.

   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 in the Time field for statistics.

   Note

   For custom time interval report, you need to set the start time and end time to specify the time period.
5. Move the cursor to the camera hot spot to view the line chart or heat map of the people amount and people dwell time in the pathways during this time period.
6. **Optional:** Export the report to the local PC.

   1) Click **Export**.

The Export panel will display with camera selected and time configured according to the range you defined previously.

2) Set the format of the exported file as Excel, CSV, or PDF.
3) Select shorter time period to view more detailed data of each camera.

Example

For example, if you select Daily Report, you can select **By Day** or **By Hour**, and it will export 1, 24 records respectively for each camera.

4) Click **Export**.

Send Pathway Report Regularly

You can set a regular report rule for specified fisheye cameras which support pathway analysis, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the people counting data (people dwell time at each location and number of people) on the configured pathways, detected by these fisheye cameras, during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 10,000 records in total.
- The report will be an Excel file.

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Analysis Group** → **Scheduled Report** .
2. Click **Add** or + in the upper-left corner to open the Create Report page.
3. Create a name for the report.
4. Select the report category as **Pathway Analysis**.
5. Select the 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 the pathway analysis group(s) contained in the report.
7. 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.

8. Set how the report will present results analyzed in the specified time period.

Example

For example, if you select the report type as **By Week**, you can select **Calculate by Day** or **Calculate by Hour**. There will be 7 or 7×24 records for each camera respectively in the report, showing analysis results on each day or each hour for one camera.

9. Set the report time and sending time according to the report type.
10. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
11. **Optional:** Switch on **Send Report 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. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

12. **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 click ∨ on the right of ⚙, then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.

13. **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 click ∨ on the right of ⚙, then click **Configure Local Storage** from the drop-down list to enter the panel to configure the corresponding information.

14. Click **Add**.
15. **Optional:** Click **Export** to export the report of this schedule for verifying the report sending schedule settings.

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.

Generate People Density Analysis Report

You can manually generate a people density report to view the people density data of two adjacent time period. You can also export the report to the local PC.

Before You Start

- Make sure you have purchased the License that supports people density analysis, or the function will be unavailable.
- Make sure you have added the behavior analysis server to the HikCentral Professional and linked cameras to the server.
- Make sure you have configured people density analysis on the behavior analysis server. For details, see the user manual of the server.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis → Report → People Density Analysis** .
2. Select a camera to search for people density data.
   1) Click to open the resource list.
   2) **Optional:** Click **Include Sub-Area** to allow the display of camera(s) in sub-areas.
   3) Select a site (current site / remote site) or an area to show cameras under the site/area.

      Note

      - Only the online cameras will be displayed.
      - You can also enter keywords of the camera name to search for cameras.

   4) Select a camera.



Figure 21-6 People Density Analysis Report

A people density report of the selected camera is displayed.

3. Switch the report type (daily, weekly, monthly, annual, and custom) by setting the statistical cycle as **Day**, **Week**, **Month**, **Year**, or **Custom**.

   Daily Report

   Daily report shows data on a daily basis. The system will calculate the peak amount of people appeared in the images of the camera in each hour of one day.

   Weekly Report, Monthly Report, Annual Report

   Compared to generating daily report, generating weekly report, monthly report, and annual report can be less time-consuming. The system will calculate the peak amount of people in each day of one week, in each day of one month, and in each month of one year respectively.

   Custom Time Interval

   Users can customize the days in the report to analyze the peak amount of people in each day or month of the custom time interval.

4. Select a pre-defined time period or customize a time period for statistics.
5. **Optional:** Perform the following operations if required.

Add Report to Dashboard	a. Click **Add to Dashboard** in the upper-right corner of the page. b. Create a report name. c. Select a dashboard. Or click **New** to create a new board and then select it. d. Click **OK** or **Add and Go to Dashboard**.
Show/Hide Certain Data	Click the legend to show or hide the data of certain element, such as certain camera.

View Detailed Data in Each Time Segment

Hover the cursor onto the line chart to view the detailed data.

View Linked Video

Hover the cursor on the statistics of a time period and click **Click to View**on a pop-up floating window to view the video of the time period.

Note

Viewing linked videos is not supported by annual report.

View Detailed Data in Each Minute

Note

Viewing detailed data in each minute is only supported by daily report.

a. Generate a daily report.
b. Select a camera at the bottom of the line chart to display its statistics only.
c. Hover the cursor onto the report and then click **Details** on the pop-up floating window.
   A report that shows statistics in each minute will be displayed.

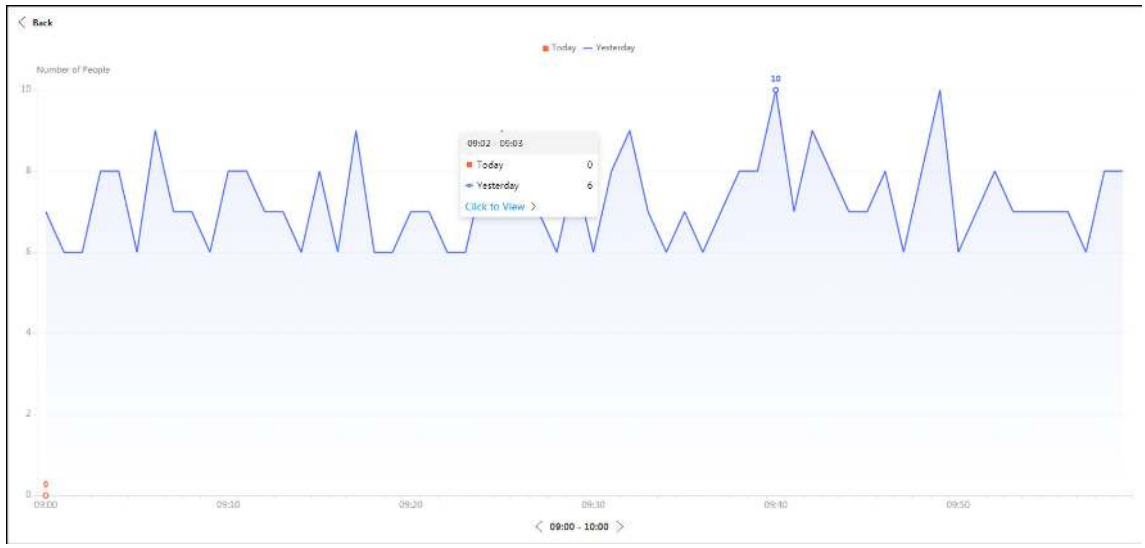


Figure 21-7 View Detailed Data In Each Minute

6. **Optional:** Export the report to the local PC.
   1) Click **Export**.
   2) Set the format of the exported file as Excel, CSV, or PDF.
   3) Select the time dimension as **By Hour**, **By Day**, or **By Month**.
   4) Click **Export**.

Send People Density Analysis Report Regularly

You can set a regular people density analysis report rule for specified cameras, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing the variation trend of people density data in line chart, which is calculated by behavior server.

Before You Start

- Add behavior analysis server to the platform, and configure people density analysis task for specified camera(s). For details, refer to ***Add DeepinMind Server*** .
- Set the email template with recipient information, subject, and content. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Analysis Group** → **Scheduled Report** .
2. Click **Add** or + in the upper-left corner to open the Create Report page.
3. Create a name for the report.
4. Select the report category as **People Density Analysis**.
5. Select the 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. Set the camera(s) contained in the report.

   Note

   Make sure you have configured people density analysis for the camera(s). For details, refer to ***Add DeepinMind Server*** .
7. 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.

8. Set how the report will present the results analyzed in the specified time period.

Example

For example, if you select the report type as **By Day**, 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 analysis results in each hour or each minute for one camera.

9. Set the report time and sending time according to the report type.
10. **Optional:** Set the effective period (start time and end time) of sending the report regularly.
11. **Optional:** Switch on **Send Report 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. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

12. **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 and click **SFTP Settings** to enter the panel to configure the corresponding information.

13. **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.

14. Click **Add**.
15. **Optional:** Click **Export** to export the report of this schedule for verifying the report sending schedule settings.

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.

You can set a regular report rule for the specified thermal cameras and the system will send emails with reports attached to the target recipients daily, weekly, or monthly. You can also manually generate a temperature analysis report at any time to view the data if required.

Generate Temperature Analysis Report

For thermal cameras, you can generate a report to show the number of exceptions (temperature too high or too low) and maximum/minimum temperature of different thermometry points on different presets.

Steps

1. In the top left corner of the platform, select → **Intelligent Analysis → Report → Temperature Analysis** .
2. Select the preset(s) configured on the thermal camera(s) for statistics.
   1) Select a current site or remote site from the drop-down site list to show its thermal cameras.

   Note

   Only the online thermal cameras will be displayed here.

   2) Select the thermal camera(s) for statistics.
   3) Check the preset(s) configured on the camera.

   Note

   For configuring the thermometry point with temperature measurement rules, refer to the user manual of the thermal camera.

   The corresponding report of selected preset(s) is displayed.
3. Set the statistical cycle as **Day**, **Week**, **Month**, **Year**, or **Custom**.

   Daily Report

   Daily report shows data on a daily basis. The platform will calculate the temperature data detected in each hour of one day.

   Weekly Report, Monthly Report, 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 temperature data detected in each day of way week, in each day of one month, and in each month of one year.

   Custom Time Interval

   Users can customize the days in the report to analyze temperature data detected in each day or month of the custom time interval.

4. 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.

5. **Optional:** Perform the following operation(s) after generating the temperature report.

View Temperature Report of Single Preset	Click the preset name on the report to view the detailed report of the preset.
View Temperature Report of Single Thermometry Point	a. Click the preset name on the report to view the detailed report of the preset. b. In the **Item for Comparison** field, select one thermometry point. c. In the **Item for Comparison** field, select the indicator you want to view in the chart. **High/Low Temperature** Shows the number of exceptions that the temperature at this thermometry point is higher or lower than the pre-defined temperature. **Max. Temperature** Shows the maximum temperature at this thermometry point during the set time period. The temperature is displayed in line chart, indicating the trend. **Min. Temperature** Shows the minimum temperature at this thermometry point during the set time period. The temperature is displayed in line chart, indicating the trend.

6. Click **Add to Dashboard** to display the report on the Dashboard.
7. **Optional:** Export the report to the local PC.
   1) Click **Export**.

      The Export panel will display with camera selected and time configured according to the range you defined previously.
   2) Set the format of the exported file as Excel, CSV, or PDF.
   3) Select shorter time period to view more detailed data of each camera.

      Example

      For example, if you select Daily Report, you can select **By Day** or **By Hour**, or **By Minute** and it will export 1, 24, or 24×60 records respectively for each thermometry point.
   4) Select the content to export.

      Abnormal Temperature

Export the number of exceptions on temperature (temperature too high or too low) of each thermometry point.

Skin-Surface Temperature Status

Export the maximum temperature and minimum temperature of each thermometry point.

5) Click **Export**.

Send Temperature Analysis Report Regularly

You can set a regular report rule for specified thermal cameras, and the platform can send an email with a report attached to the target recipients daily, weekly, or monthly, showing temperature exceptions or min./max. temperature, detected by these thermal cameras during the specified time periods.

Before You Start

- Set the email template with recipient information, subject, and content. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email settings such as sender address, SMTP server address and port. For details, refer to ***Configure Email Account*** .

Steps

Note

- One report can contain up to 32,000 records in total.
- The report will be an Excel file.

1. In the top left corner of the platform, select → **Intelligent Analysis** → **Analysis Group** → **Scheduled Report** .
2. Click **Add** or + in the upper-left corner to open the Create Report page.
3. Create a name for the report.
4. Select the report category as **Temperature Analysis**.
5. Select the 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 the thermal camera(s) and presets contained in the report.

   The report will show the temperature exceptions (including temperature too high or too low) or maximum and minimum temperature of different thermometry points on these presets.
7. Set the content in the report.

   Temperature Exception

   The number of exceptions on temperature (temperature too high or too low) of each thermometry point.

Temperature Status

The maximum temperature and minimum temperature of each thermometry point.

8. 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.

9. Set how the report will present results analyzed in the specified time period.

Example

For example, if you select the **Statistical Cycle** as **By Day**, you can select **Calculate by Hour** or **Calculate by Minute**. There will be 24 or 24×60 records for each thermometry point respectively in the report, showing the temperature exceptions or min./max. temperature detected in each hour or each minute.

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 Report 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. For setting the email template, refer to ***Add Email Template for Sending Report Regularly*** .

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 click ⌄ on the right of ⚙, then click **SFTP Settings** from the drop-down list to enter the panel to configure the corresponding information.

14. **Optional:** Switch on **Local Storage**, and click **Configure** beside **Saving Path** to configure the saving path of local storage.

Note

You can also click ⌄ on the right of ⚙, then click **Configure Local Storage** from the drop-down list 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 22 On-Board Monitoring

The On-Board Monitoring module is for users to 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.

22.1 Flow Chart of On-Board Monitoring

The flow chart introduces the process of on-board monitoring configuration.

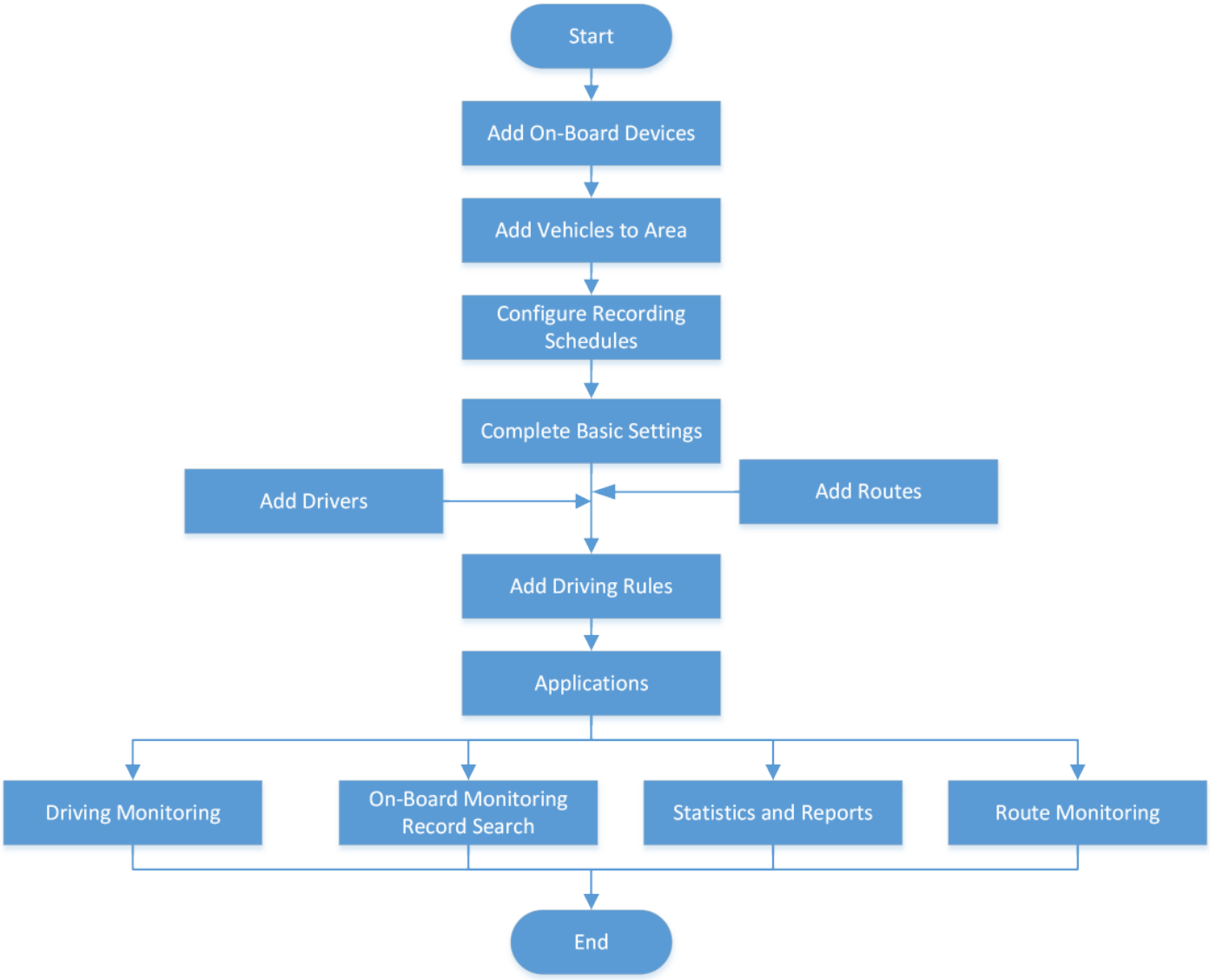


Figure 22-1 Flow Chart of On-Board Monitoring Configuration

22.2 On-Board Monitoring Overview

The Overview page displays the major steps of On-Board Monitoring configuration and presents brief information such as the health status of devices and real-time driving events.

On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → On-Board Monitoring Overview** .

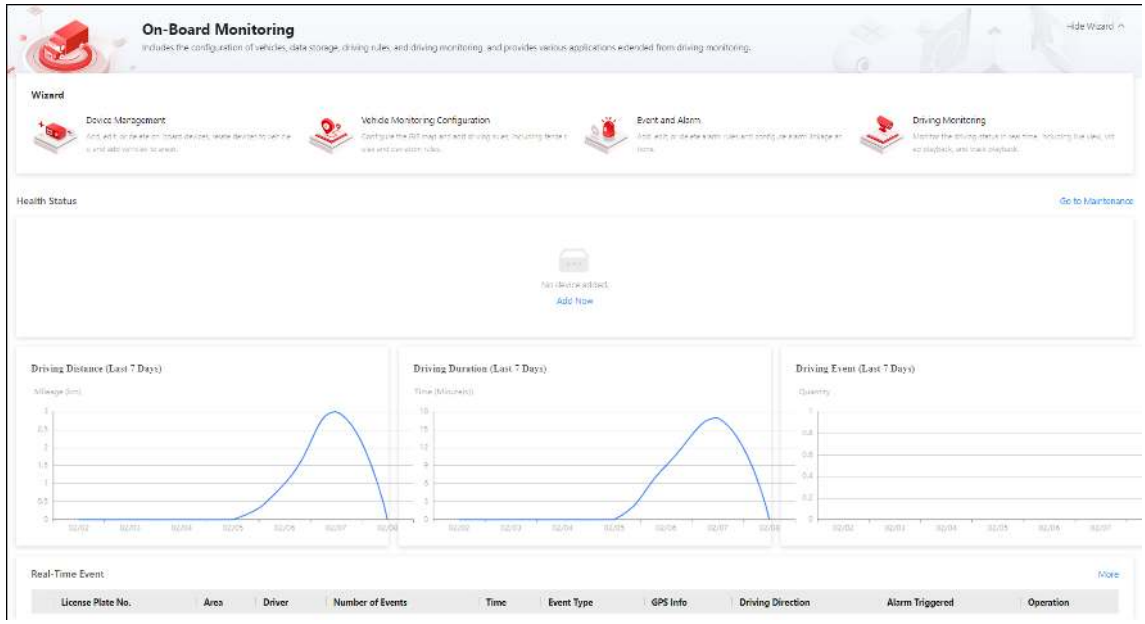


Figure 22-2 On-Board Monitoring Overview

Content	Description
Wizard	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. 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 on-board devices, cameras, and alarm inputs. You can click **Go to Maintenance** to view more details. For more information, refer to ***Maintenance*** .
Statistics and Reports	You can view some of the on-board monitoring statistics generated in the last 7 days, including the driving distance, driving duration, and driving event. See ***Statistics and Reports*** for how to view more details and reports.
Real-Time Events	You can view the events triggered by monitored vehicles. Detailed information of each record is also provided, including the vehicle's license plate number, the area where an event was triggered, driver information, etc.

22.3 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.

22.3.1 Configure Basic Parameters

You can configure the basic parameters including the distance unit, GIS map, and retention period of GPS data.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Basic Configuration** → **Basic Parameters** .

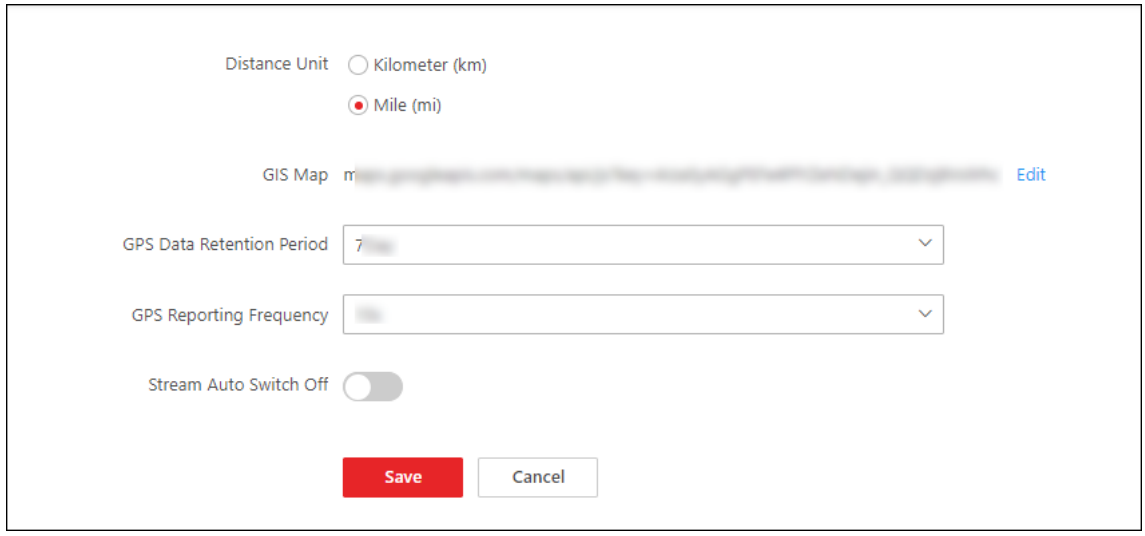


Figure 22-3 Basic Parameter Configuration

2. Select a distance unit.
3. 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. See ***Set GIS Map and Icons*** for details.

4. Select the retention period of GPS data.

Note

GPS data can be retained for one year at most.

5. Set the frequency at which the GPS information is reported to the platform.
6. **Optional:** Switch on **Stream Auto Switch Off** and set a duration.

Note

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 save network traffic.

22.3.2 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.

22.3.3 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.

Steps

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. Select the **Fuel Quantity Unit** for fuel consumption calculation.
4. Add a fuel tank model.
   1) Click **Add**.
   2) Enter the fuel tank name, capacity, fuel height, and threshold of fuel consumption.

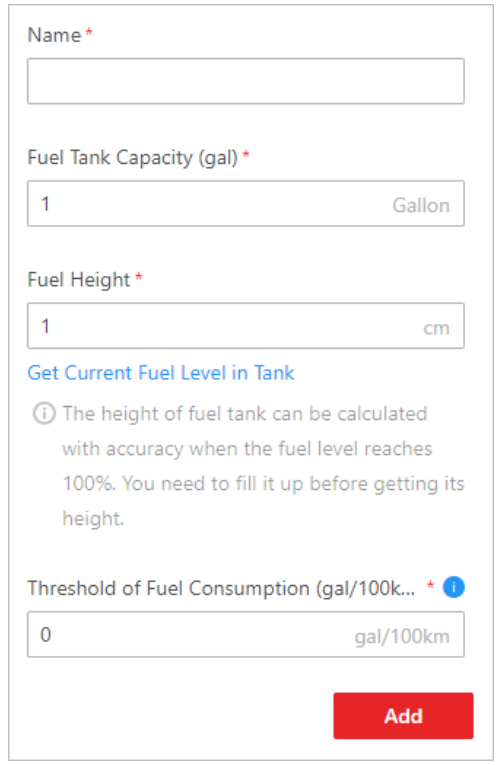


Figure 22-4 Window of Adding Fuel Tank Model

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.

3) (Optional) Click **Get Current Fuel Level In Tank**, and then select a vehicle to get the current fuel level of the vehicle's tank.
4) Click **Add**.

5. Enter the **Fuel Tolerance in Tank**.
6. Click **Save**.

22.3.4 Configure Scheduled Reports

You can set parameters for sending scheduled reports including driver analysis reports, fuel level analysis reports, and stop traffic analysis reports.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Basic Configuration** → **Scheduled Report** .

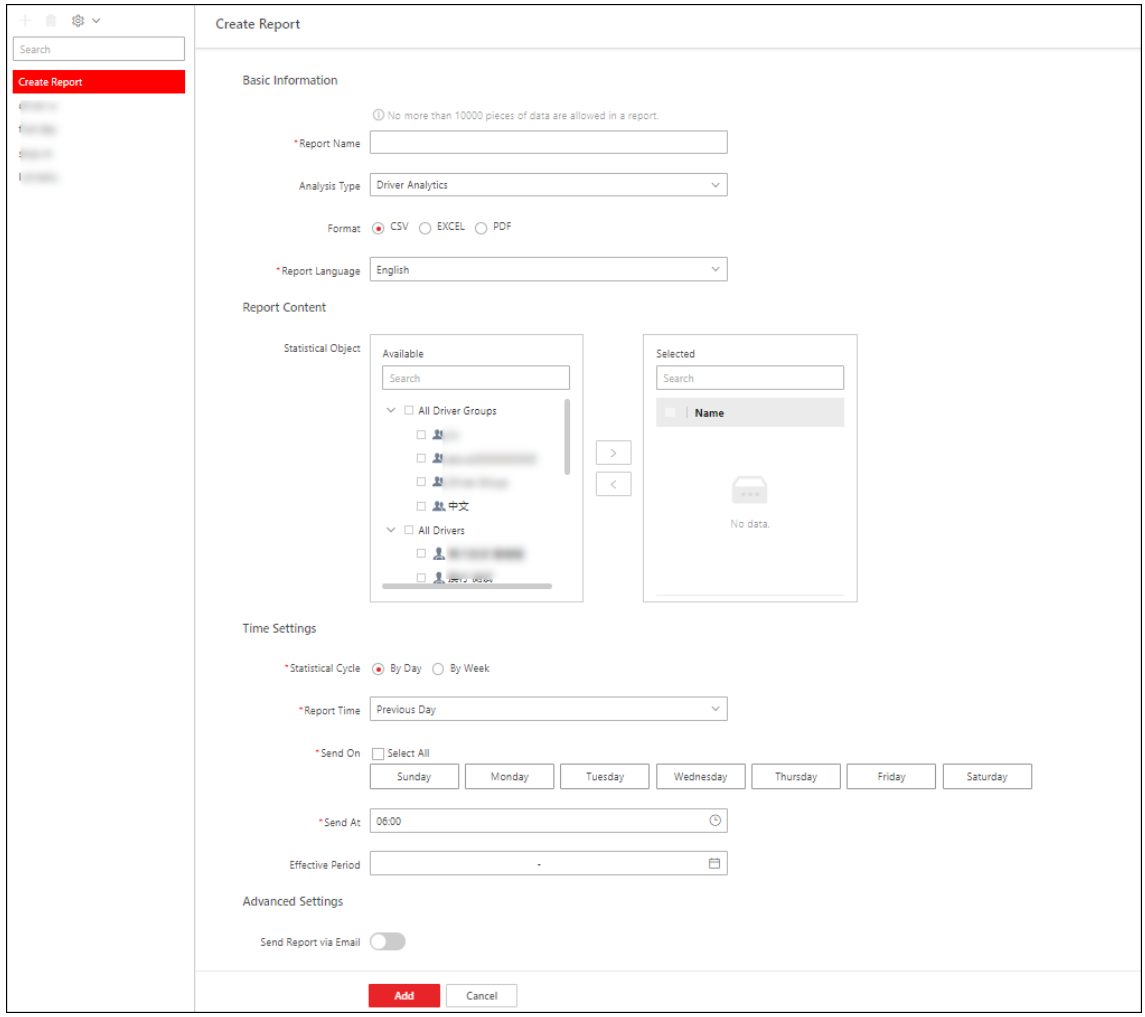


Figure 22-5 Create Report Page

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.
   1) 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.

2) Select the report time, which means the statistical range of the report.

Note

The options change according to the statistical cycle you select.

3) Select a day and/or time of sending the report at the **Send At** / **Send On** field.
4) (Optional) Select an effective period for the settings.

6. **Optional:** Complete the advanced settings.
   1) Enable **Send Report via Email**, and then select an email template.

   Note

   You can click **Add** to add a new email template. For setting the email template, refer to ***Set Email Template*** .

   2) 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**.

22.4 Driver Management

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.

22.4.1 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. In addition, you can batch add driver information by importing a template with driver information or importing ZIP files containing driver's profile photos.

Add a Single Driver

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driver Management** → **Driver** .
2. Hover the mouse cursor over **Add** and click **Add Driver** to enter the Add Driver page.

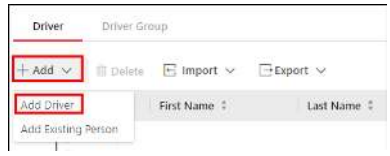


Figure 22-6 Add Driver

3. Set the driver's basic information, such as the ID, driver group, first name, last name.

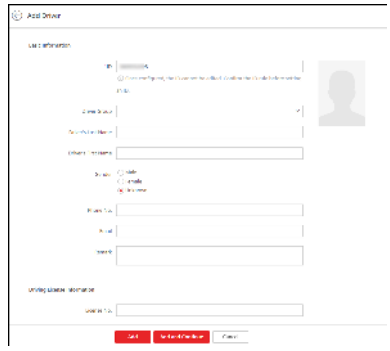


Figure 22-7 Add Driver Page

ID (Required)

The default ID is generated by the platform. You can edit it if needed. Once the driver is added successfully, the ID cannot be edited any more.

Driver Group

See details about how to add a driver group in ***Add a Driver Group*** .

Driver's Last/First Name (Required)

Either the last name or the first name is required.

Profile Photo

Hover over , and then take or upload a profile photo of the driver.

4. **Optional:** Set the driver's driving license information, including the driving license No. and picture.
5. Finish adding the driver.
   - Click **Add**.
   - Click **Add and Continue** to finish adding the driver and continue to add other drivers.
6. **Optional:** Perform the following operations.

Edit a Driver	Click the driver name to edit the driver details.
Delete Drivers	Select one or multiple drivers and click **Delete** to delete the drivers.
Filter Drivers	Click to filter drivers by name, ID, phone No., driver group or/and driving license No.

Add from Existing Persons

If you have added persons to the platform, you can add them as drivers.

Before You Start

Make sure you have added persons to the platform. See ***Person Management*** for details.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driver Management** → **Driver** .
2. Hover the mouse cursor over **Add** and click **Add Existing Driver**.

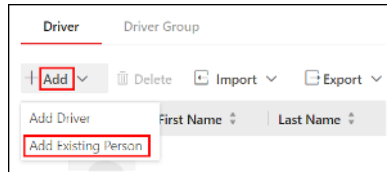


Figure 22-8 Add Existing Driver

3. Select one or multiple persons from the list and click **Add**.

Note

You can search for target persons by keywords.

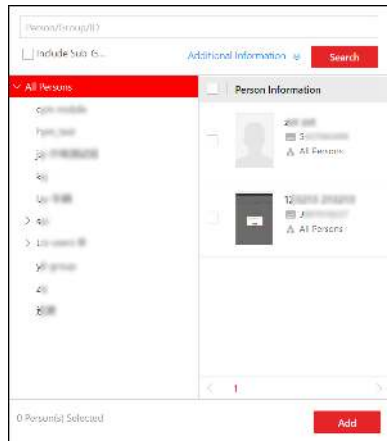


Figure 22-9 Add Existing Person Page

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

Edit a Driver	Click the driver name to edit the driver details.
Delete Drivers	Select one or multiple drivers and click **Delete** to delete the drivers.
Filter Drivers	Click to filter drivers by name, ID, phone No., driver group or/and driving license No.

Import Drivers via the Template

You can batch add drivers to the platform by importing a template which contains driver information including name, driver group.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driver Management** → **Driver** .
2. Hover the mouse cursor over **Import** and click **Import Driver via Template**.



Figure 22-10 Import Drivers via the Template

3. In the pop-up window, click **Download Template** to save the template to the local PC.

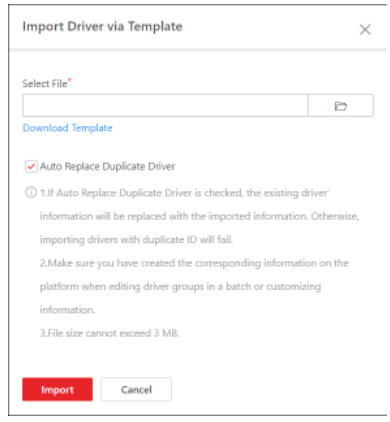


Figure 22-11 Import Drivers via the Template Page

4. In the downloaded template, enter the driver information by following the rules shown in the template.
5. Click and select the template with driver information from the local PC.
6. **Optional:** Check **Auto Replace Duplicate Driver** to replace the existing driver information if the imported ID is the same as that of the existing driver.
7. Click **Import** to start importing driver information.
8. **Optional:** Perform the following operations.

Edit a Driver	Click the driver name to edit the driver details.
Delete Drivers	Select one or multiple drivers and click **Delete** to delete the drivers.
Filter Drivers	Click to filter drivers by name, ID, phone No., driver group or/and driving license No.

Import Drivers via Profile Photos

You can batch add driver information to the platform by importing ZIP files containing JPG, JPEG, or PNG profile photos.

Steps

1. Name the profile photos as required, move these photos into one folder, and then compress the folder in ZIP format.

Note

- Naming rule of profile photos: First Name+Last Name_ID. Either first name or last name is required, and the ID is optional. For example, Kate+Smith_123.jpg; Kate_123.jpg; Smith_123.jpg; Kate+Smith.jpg; Smith.jpg
- If the ID in the profile photo name is the same as that of an existing driver on the platform, the existing driver's information will be modified.
- If the ID in the profile photo name does not exist on the platform or the existing driver with the same name does not have an ID, a new driver with the profile photo, name, and ID will be created.
- If the profile photo name contains ID only, the existing driver with the same ID will be modified.

2. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driver Management** → **Driver** .
3. Hover the mouse cursor over **Import** and click **Import Driver via Profile Photo**.

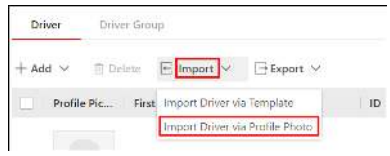


Figure 22-12 Import Drivers via Profile Photos

4. Click and select the ZIP files from the local PC.

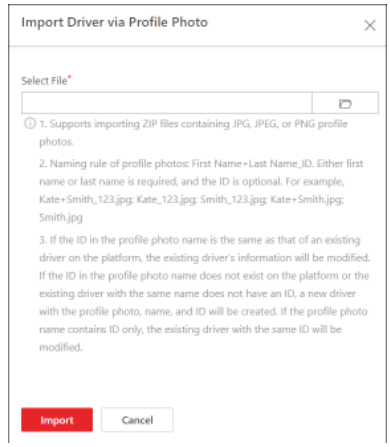


Figure 22-13 Import Drivers via Profile Photos Page

5. Click **Import**.
6. **Optional:** Perform the following operations.

Edit a Driver	Click the driver name to edit the driver details.
Delete Drivers	Select one or multiple drivers and click **Delete** to delete the drivers.
Filter Drivers	Click to filter drivers by name, ID, phone No., driver group or/and driving license No.

22.4.2 Export Drivers

You can batch export driver detailed information and driver's profile photos.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driver Management** → **Driver** .
2. Hover the mouse cursor over **Export** and click **Export Driver Information** or **Export Driver Profile Photo** as required.
3. Set a password and confirm the password for decompressing the exported ZIP file.

Note

For exporting driver profile photos, the user name and password are also required.

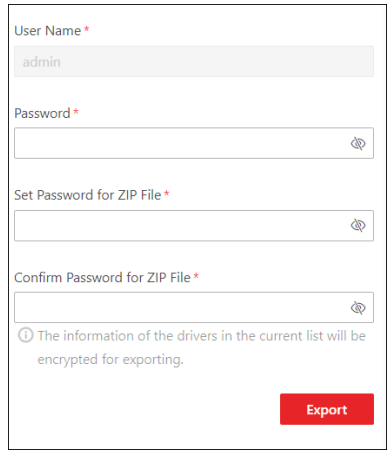


Figure 22-14 Export Driver Profile Photos

4. Click **Export**.

Note

You can use the password you set previously to decompress the exported ZIP file.

22.4.3 Add a Driver Group

You can add driver group(s) to categorize different drivers for convenient management.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driver Management** → **Driver Group** .
2. Click + and enter the driver group name.
3. Click **OK**.

   In the driver group list, the added driver group will be displayed with the number of people.
4. **Optional:** Perform the following operations.

Edit Driver Group	Select a driver group, click to edit the driver group name and then click **OK**.
Delete Driver Group	Select a driver group, click to delete the driver group.
Search for Driver Group	Enter a key word in the search box, and click to search for the target driver group.

22.4.4 Add Drivers to a Driver Group

After adding a driver group, you can add drivers to the driver group for management.

Before You Start

Make sure you have added drivers and driver group(s) on the Client. For details, refer to ***Add Drivers*** and ***Add a Driver Group*** .

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Driver Management → Driver Group** .
2. Select the added driver group in the left list.
3. Click **Add**.

   The Add Driver pane will pop up.
4. Select driver(s) and click **Add**.

   Note

   You can search the target driver by name or ID.
5. **Optional:** Perform the following operations.

Filter Drivers	Select a driver group, click and set filter conditions such as name, and then click **Filter**.
Delete Drivers	Select a driver group in the driver list on the left, then select one or multiple drivers on the right and click **Delete** to delete the drivers.

22.5 Driving Rule

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.

22.5.1 Configure a Fence Rule

You can add a fence rule to specify the area where vehicles are allowed or not allowed to drive.

Before You Start

Make sure you have set the GIS map. For details, refer to ***Configure Basic Parameters*** .

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Driving Rule Configuration → Fence Rule** .
2. Click **Add** to enter the Add Rule page.

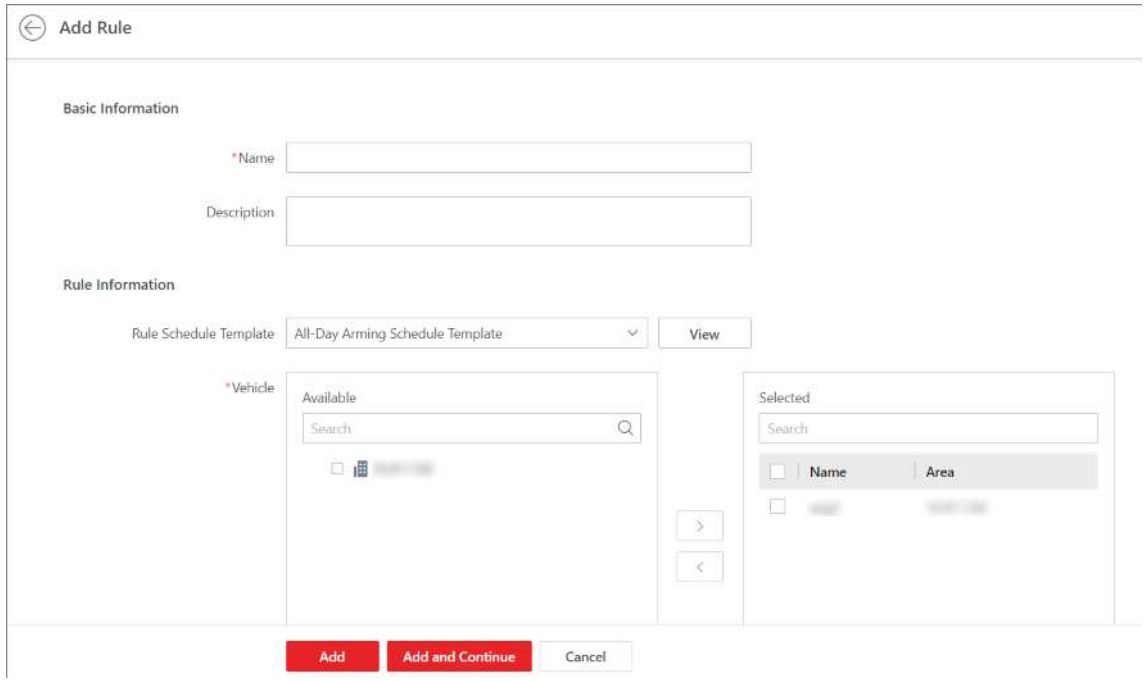


Figure 22-15 Add a Fence Rule

3. Set the basic information for the fence rule, including the name and description.
4. Set rule information.
   1) 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, you can see ***Configure a Rule Schedule Template*** for how to configure one.

   2) Select vehicle(s) that the fence rule will be applied to.
   3) 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.

   4) In the Fence Area area, click to draw a fence area on the map.
5. Click **Add** to finish or click **Add and Continue** to add another fence rule.
6. **Optional:** Perform further operations.

Edit Fence Rule	On the rule list, click the name of a fence rule to edit it.
Filter Fence Rule	On the fence rule page, click in the upper-right corner, set filtering conditions, and click **Filter** to filter fence rules.

Delete Fence Rule	On the rule list, select one or multiple fence rules and click **Delete** to delete them.

22.5.2 Configure a Deviation Rule

You can add a deviation rule to specify the route that vehicles should drive along.

Before You Start

Make sure you have set the GIS map. For details, refer to ***Configure Basic Parameters*** .

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driving Rule Configuration** → **Deviation Rule** .
2. Click **Add** to enter the Ad Rule page.

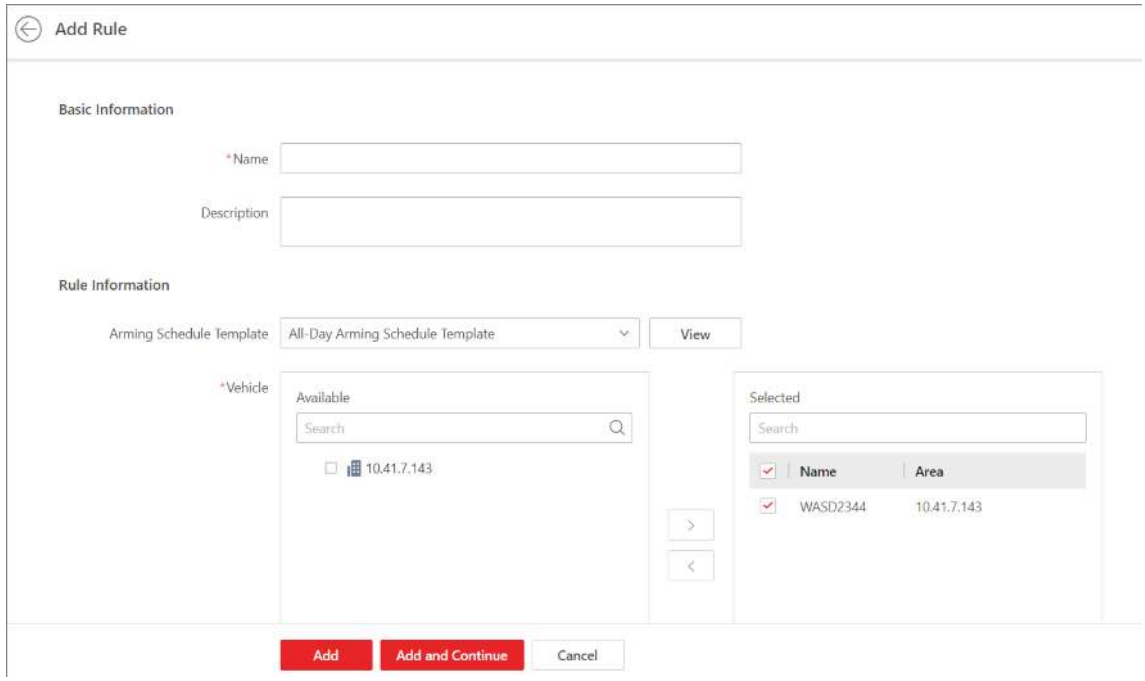


Figure 22-16 Add a Deviation Rule

3. Set the basic information for the fence rule, including the name and description.
4. Set rule information.
   1) 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, you can see ***Configure a Rule Schedule Template*** for how to configure one.

   2) Select vehicle(s) that the deviation rule will be applied to.

3) Set the deviation threshold.

Note

An event will be triggered if a selected vehicle deviates from the route beyond the threshold.

4) In the Driving Route area, click to draw a route on the map.

5. Click **Add** to finish or click **Add and Continue** to add another deviation rule.
6. **Optional:** Perform further operations.

Edit Deviation Rule	On the rule list, click the name of a deviation rule to edit it.
Filter Deviation Rule	On the deviation rule page, click in the upper-right corner, set filtering conditions, and click **Filter** to filter deviation rules.
Delete Deviation Rule	On the rule list, select one or multiple deviation rules and click **Delete** to delete them.

22.5.3 Configure a Rule Schedule Template

You can add a rule schedule template to define the time when the related driving rules are effective in a week.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Driving Rule Configuration** → **Rule Schedule Template** .
2. Click + to enter the Add Rule Schedule Template page.

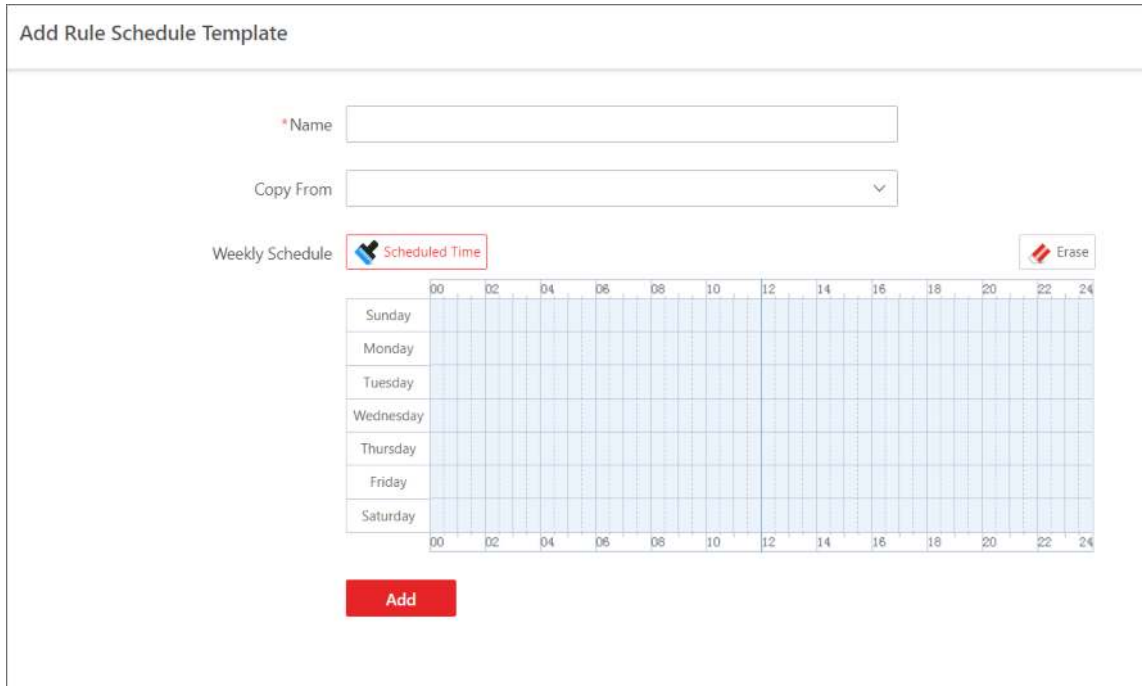


Figure 22-17 Add Rule Schedule Template

3. Create a name for the rule schedule template.
4. **Optional:** In the **Copy from** field, select an existing template to copy its weekly schedule to the current one.
5. Click **Scheduled Time** and click or drag on the timetable to define the period.

Note

- A rectangle represents half an hour.
- You can click a selected rectangle to set a more accurate time.
- You can click **Erase** and drag on the formerly selected rectangle(s) to remove them from the scheduled time.

6. Click **Add**.
7. **Optional:** Perform further operations.

Edit Rule Schedule Template	On the template list, click a rule schedule template to edit it.
Delete Rule Schedule Template	On the template list, select a rule schedule template and click **Delete** to delete it.

22.6 Route Management

HikCentral Professional supports managing driving stops, routes, and stop event rules. 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.

22.6.1 Manage 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 Group

You can add a stop group to categorize different stops for convenient management.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Management** → **Stop** .
2. Click in the top left coner, enter the stop group name, and click **Add**.

   The added stop group will be displayed in the stop group list.

What to do next
Add a single stop or import stops via the template to the stop group. See details in ***Add a Stop*** and ***Import Stops via the Template*** .

Add a Stop

After adding a stop group, you can add a single stop to the group.

Before You Start
Make sure you have set the GIS map. For details, refer to ***Configure Basic Parameters*** .

Steps
1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Management** → **Stop** .
2. Select a stop group in the stop group list.
3. Click + .
4. Move your mouse cursor to the target location on the map and click .

   Note
   You can search for the target geographic location by entering keywords in the search box in the top left corner of the map.
5. Select **Circle** or **Polygon** as the stop shape, move your mouse cursor to adjust the size, and click to confirm.
6. Enter a name and description for the stop and switch on/off **People Counting for Stops**.

   Note
   For more information about the results of people counting for stops, refer to ***People Counting Report*** .
7. Click **Save**.
8. **Optional:** Perform the following operations.

Edit a Stop	Select a stop, click to edit the information of the stop.
Delete a Stop	Select a stop, click to delete the stop.
Filter Stops	Check **Stops with People Counting Enabled Only** to filter stops.

Import Stops via the Template

You can fill the predefined template with the stop information to add multiple stops to the group at a time.

Before You Start
Make sure you have set the GIS map. For details, refer to ***Configure Basic Parameters*** .

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Management** → **Stop** .
2. Click .
3. Click **Download Template** and save the predefined template (EXCEL file) in your PC.
4. Open the downloaded template file and edit the required information of the stops to be added in the corresponding column.
5. Click and select the template file.
6. Click **Import**.
7. **Optional:** Perform the following operations.

Edit a Stop	Select a stop, click to edit the information of the stop.
Delete a Stop	Select a stop, click to delete the stop.
Filter Stops	Check **Stops with People Counting Enabled Only** to filter stops.

22.6.2 Configure Driving Routes and Shift Schedules

You can configure the driving route manually or generate it automatically, and manage stops of the route. After configuring routes, you can configure shift schedules which can repeat by week, and can also configure schedules which are effective only at a fixed date or during a specific time period for temporary use.

Before You Start

Make sure you have added stops on the platform. For details, refer to ***Manage Stops*** .

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Management** → **Route** .
2. 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.
3. Select at least two stops on the map.
   - Click **Switch to List Mode** and select stops in the list.
   - Click the stop icon on the map to select the stop.

     Note

     Click the stop icon again on the map to deselect it.

Note

- In the top left corner of the map, you can search for a specific location on the map.
- You can click **Reverse** to reverse the order of the selected stops.
- You can hover the cursor over the stop name on the left and click to delete the stop.

The selected stops are displayed on the left.

4. In the top right corner of the page, click **Next** and configure the driving route.
   - 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.

     Note

     To generate the driving route automatically, you need to enable the Google map charging service.
5. Click **Next** to configure shift schedules.

   Note

   You can also click **Finish** to finish adding the route without configuring shift schedules.
6. Configure a single schedule or batch configure schedules for the route.
   1) Click **Add Schedule** or **Batch Add Schedules**.
   2) Set the schedule information.

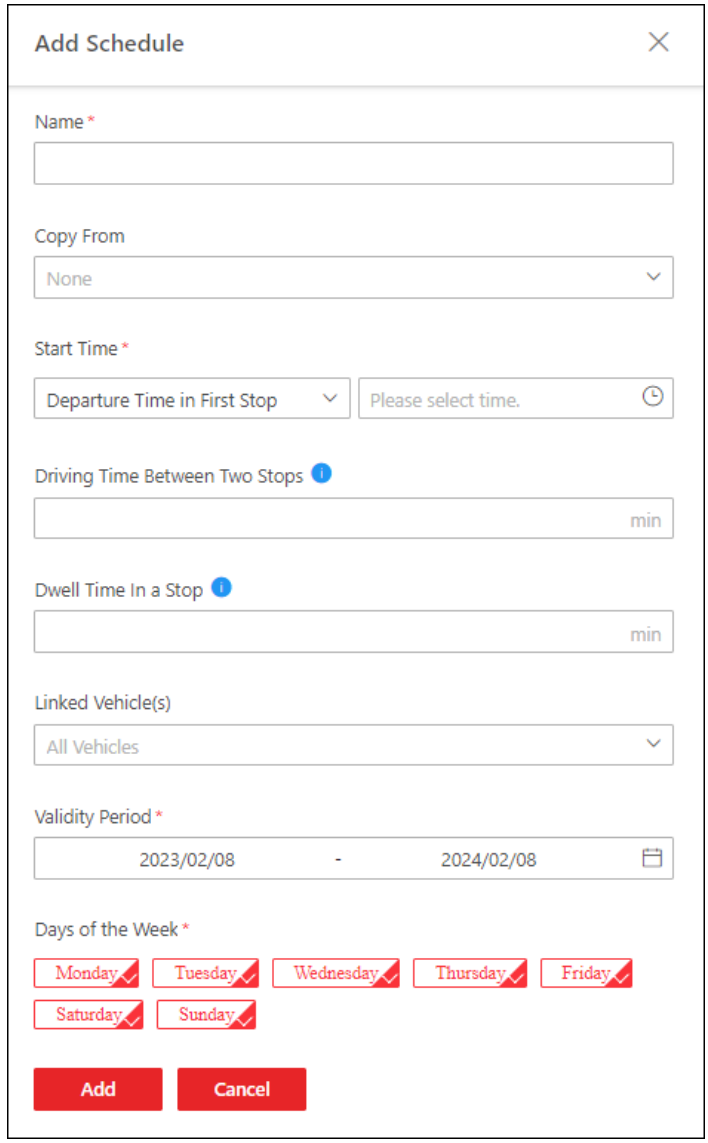


Figure 22-18 Add a Single Schedule

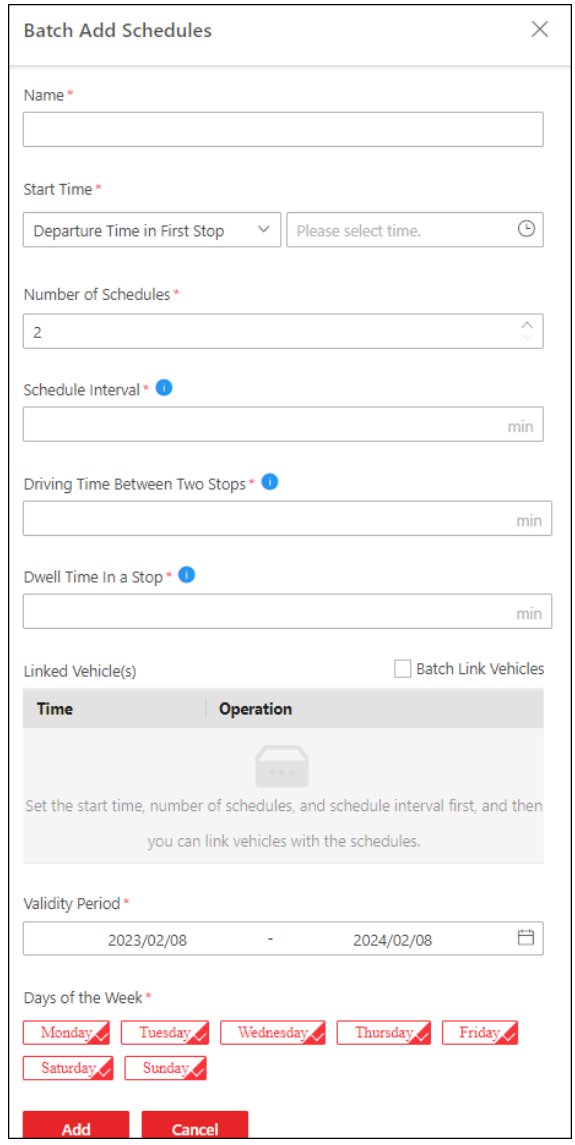


Figure 22-19 Batch Add Schedules

3) Click **Add**.

Note

You can set route parameters to define late arrivals/departures for the schedules. For details, refer to ***Configure Route Parameters*** .

7. Click **Finish** in the top right corner.
8. **Optional:** Perform the following operations.

Delete Route	Select the route and click to delete.
Filter Routes	Click to set filtering conditions to search for matched routes.

View Route Details	Click the route name to view details of the route. On the details page, you can click **Edit Route** to edit the route and click **Edit Schedule** to edit the shift schedule(s) of the route.
Enable/ Disable Route	Click ⊘ / ⊖ to enable/disable the route.
Switch Display Mode	• At the top of the route list, click **Week** or **Day** to display the timetable of routes on a weekly or daily basis. You can click ‹ / › to adjust the time period. • Click the route name displayed on the timetable, you can view the route's shift schedule details, including the departure time, arrival time and vehicle. You can also click ⊘ / ⊖ to enable/disable the route.

22.6.3 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.

Before You Start

- Make sure you have added devices on the platform and alarm inputs to areas. For details, refer to ***Device and Server Management*** and ***Add Alarm Input to Area for Current Site*** .
- Make sure you have added stops on the platform. For details, refer to ***Manage Stops*** .

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Route Management** → **Stop Event Rule** .
2. Click **Add** to add a stop event rule.
3. Set rule basic information.
   1) Create a rule name.
   2) **Optional:** Enter the rule description.
4. Select the rule type.

   Stops Allowing Triggering Alarm Inputs

   Alarm inputs triggered outside the selected stops will be recorded as unintended alarm inputs.

   Stops Forbidding Triggering Alarm Inputs

   Alarm inputs triggered within the selected stops will be recorded as unintended alarm inputs.
5. Select the alarm input(s).
6. Select the stop(s) by stop or route.
7. Click **Add** to finish or click **Add and Continue** to add another rule.
8. **Optional:** On the rule list page, perform the following operations.

Delete Rule	Select the rule(s) and click **Delete**.

Edit Rule On the rule list, click the name of a rule to edit the rule.

Filter Rules Click ▽ in the upper-right corner, set filtering conditions, and click **Filter**.

22.7 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** .

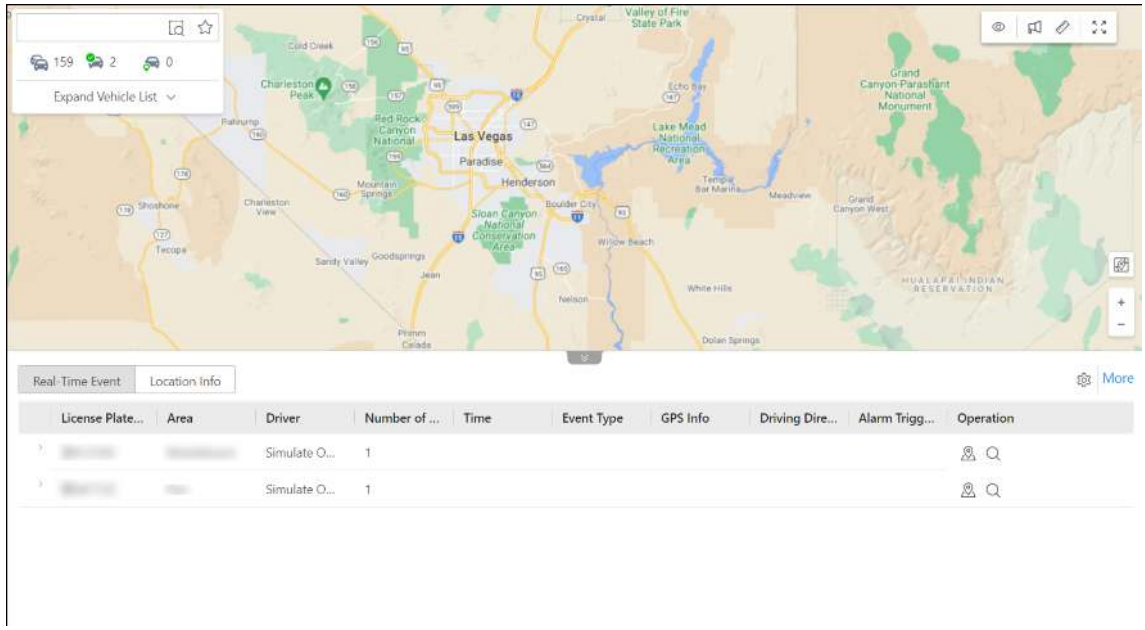


Figure 22-20 Driving Monitoring Page

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. • Click ⊡ to specify an area for vehicle search.

Operation	Step
	• Click / / to view all/online/located vehicles. • 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 your mouse cursor over the drawn circle and click **Locate** or **Broadcast** to locate or broadcast to all vehicles in the circle.
View Vehicle Details	On the vehicle list, hover the mouse cursor over a vehicle to view its real-time information, including its location, speed, etc.
Locate Vehicle	On the vehicle list, hover the mouse cursor 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 the mouse cursor 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 the mouse cursor over a vehicle and click ··· to display the operation menu and 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.

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:

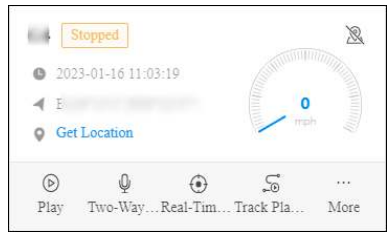


Figure 22-21 Driving Monitoring Pane

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 in the vehicle.
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.

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:

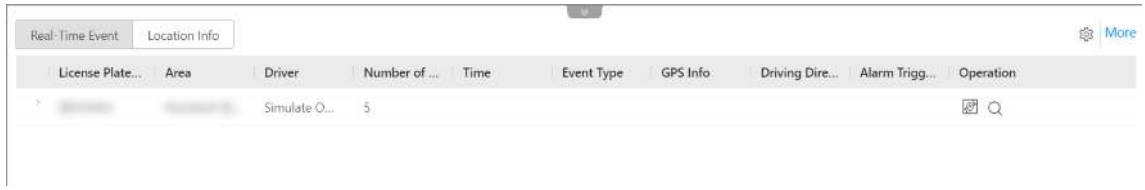


Figure 22-22 Real-Time Event Table

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:

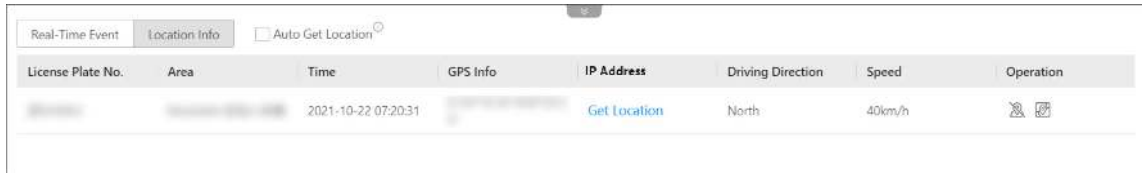


Figure 22-23 Location Info Table

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.

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. For configuring fence rules and deviation rules, see details in ***Driving Rule*** .
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.

22.8 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

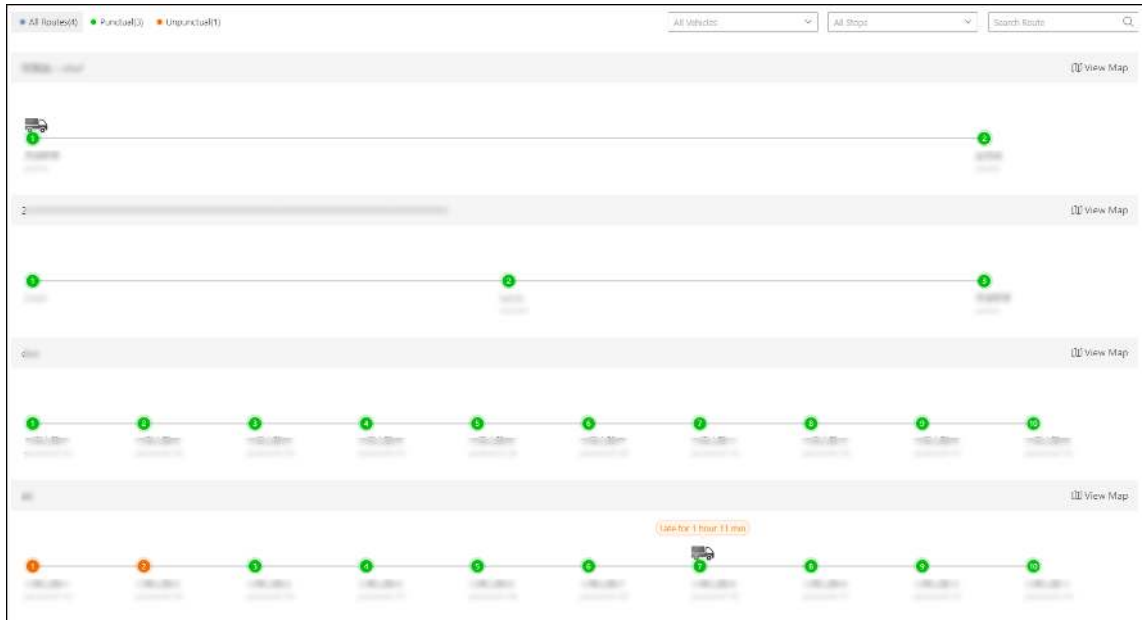


Figure 22-24 Route List

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. • 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. • 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 22-25 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. • 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). • 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.

22.9 On-Board Monitoring Record

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.

22.9.1 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.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Search** → **Vehicle Track Search** .
2. Set search conditions.
   1) Specify the period you want to search for vehicle tracks in.
   2) Select vehicle(s).
   3) **Optional:** Switch on **Speed Range** and set a speed range.
   4) **Optional:** Switch on **Triggered By** and click to select event type(s).

   Note

   All event types have been selected by default.
3. Click **Search**.

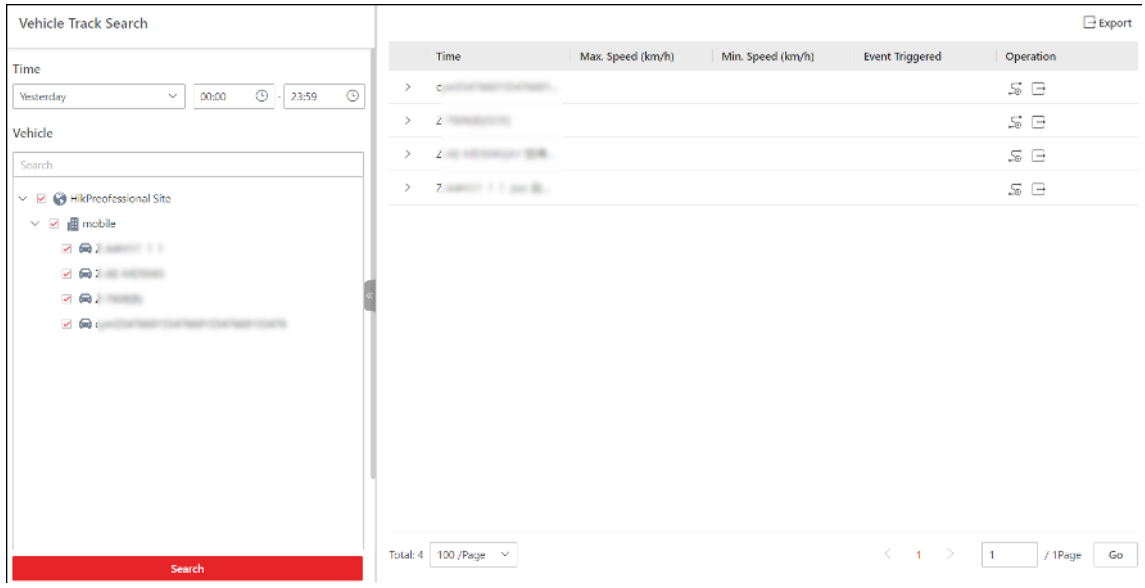


Figure 22-26 Vehicle Track Search

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

Play Back Track	Click to play back a track.
Export Record	Click to export a single record to the PC. Click **Export** in the upper-right corner to export all records to the PC.
Other	Click and more records generated in the specified period will be displayed. You can also click to play back a track and click to export a record to the PC.

22.9.2 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.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Search** → **Driving Event Search** .
2. Set search conditions.

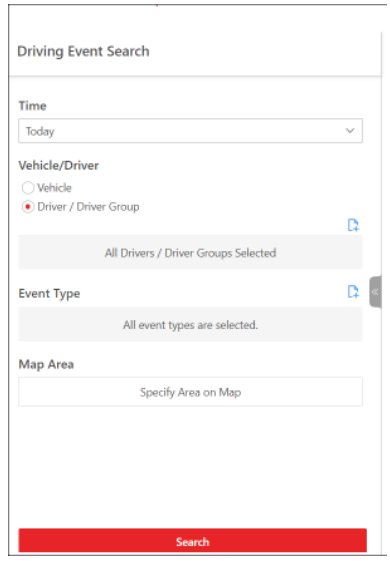


Figure 22-27 Search for Driving Events

1) Specify the period you want to search for driving events in.
2) Select **Vehicle** or **Driver / Driver Group** as the type.
3) Click to select vehicle(s), driver(s), or driver group(s).

Note

All vehicles / drivers / driver groups have been selected by default.

4) In the Event Type area, click to select event type(s).

Note

All event types have been selected by default.

5) In the Map Area area, click **Specify Area on Map** and draw an area on the map.

The platform will search for events triggered in the specified area.

3. Click **Search**.
4. **Optional:** Perform the following operations.

Play Back Track	Click to play back a track.
Export Record	Click to export a single record to the PC. Check record(s) and click **Export** in the upper-right corner to export them to the PC.

22.9.3 Search for Routes

You can search for routes, view detailed information of each route, and export route information to the local PC.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Search** → **Route Search** .
2. Set search conditions.

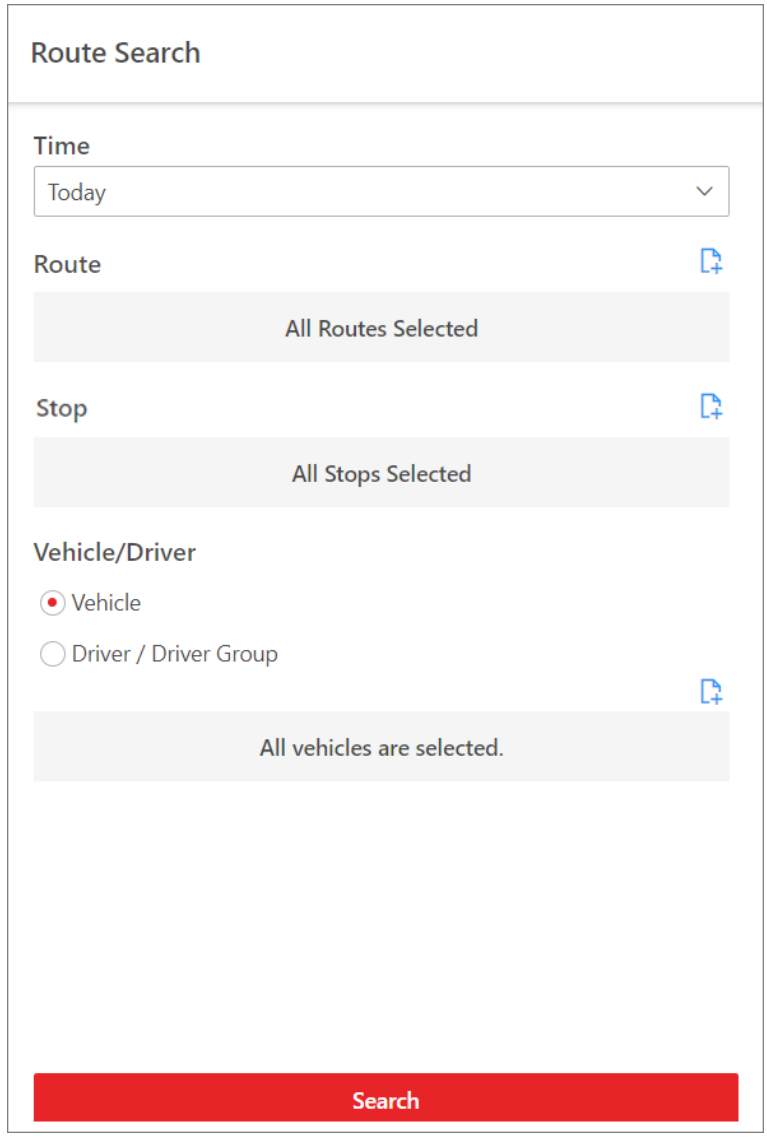


Figure 22-28 Search Conditions

1) Specify the period you want to search for routes in.
2) Click to select route(s).

Note

All routes have been selected by default.

3) Click to select stop(s).

Note

All stops have been selected by default.

4) Select **Vehicle** or **Driver / Driver Group** as the type.

5) Click to select vehicle(s), driver(s), or driver group(s).

Note

All vehicles / drivers /driver groups have been selected by default.

3. Click **Search**.

The needed routes will be displayed in the list.

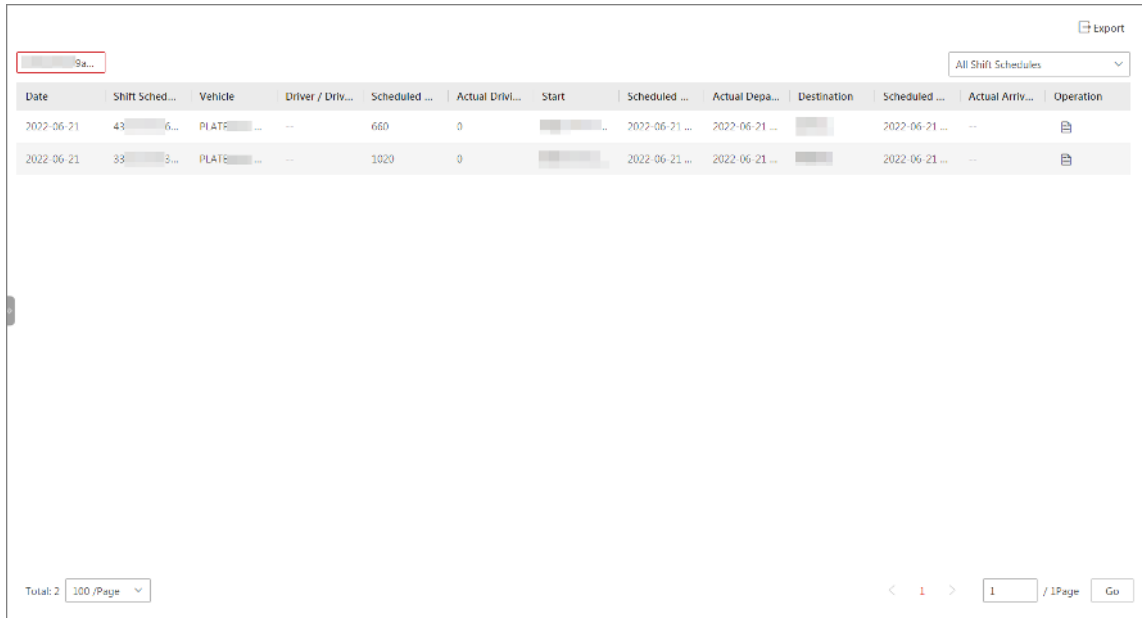


Figure 22-29 Search for Routes

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

Play Back Track	In the Operation column, click to play back a track.
Export Record	Click to export a single record to the PC. Check records and click **Export** in the upper-right corner to export them to the PC.

22.9.4 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.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Search** → **Fuel Level Record Search** .
2. Set search conditions.
   1) Specify the period you want to search for fuel level records in.
   2) Select **Vehicle** or **Driver / Driver Group**, and all vehicles or all drivers / driver groups are selected by default.

   Note

   Click to specify certain vehicles or driver / driver groups.
3. Click **Search** to get the list of fuel level monitoring records.

Note

You can click **Export** in the upper-right corner to export the records to your local PC.

22.10 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.

22.10.1 Overview

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.

On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** → **Overview** .

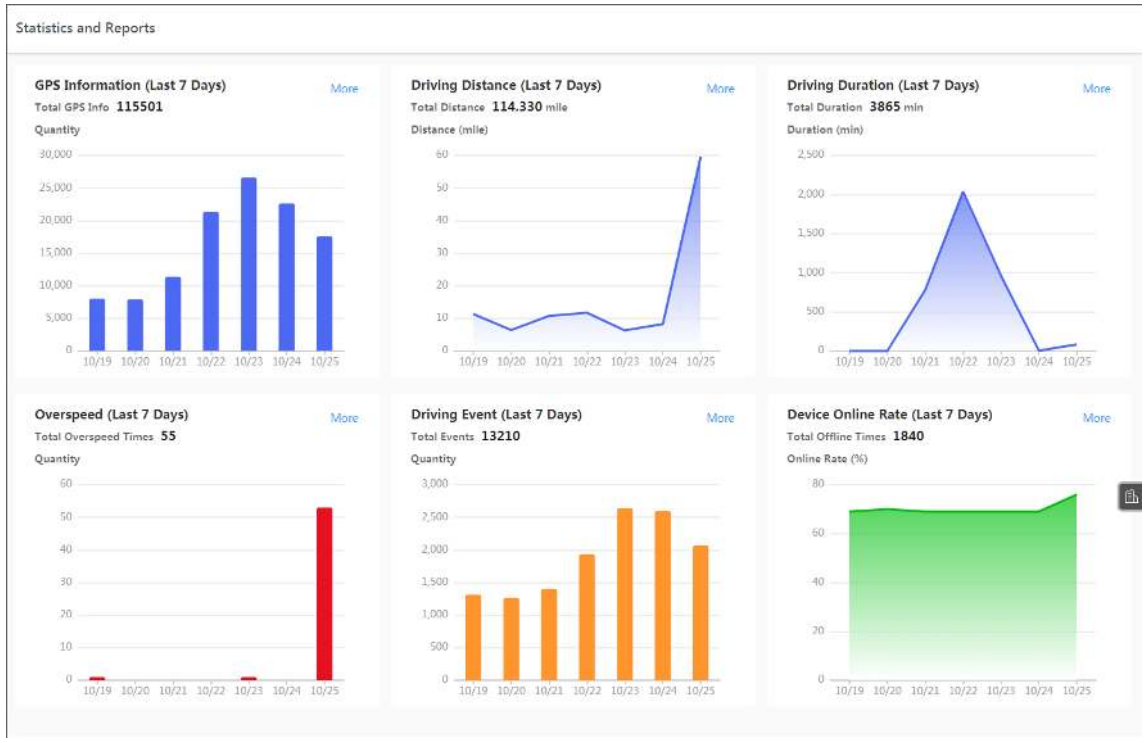


Figure 22-30 Statistics Overview

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.

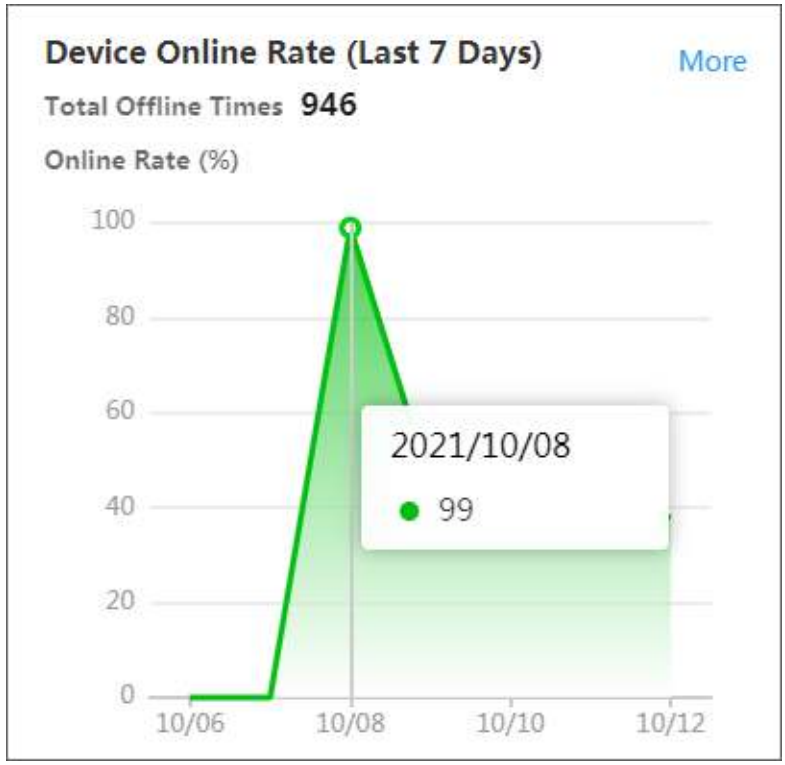


Figure 22-31 Example

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.

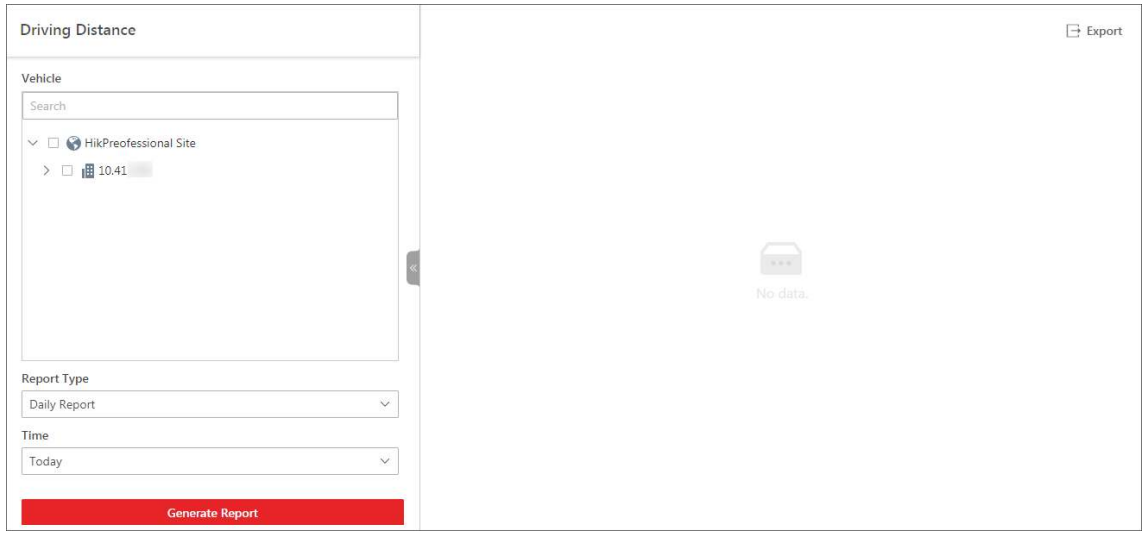


Figure 22-32 Generate Report

22.10.2 Generate a Driver Analytics Report

You can generate 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.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** → **Driver Analytics** .

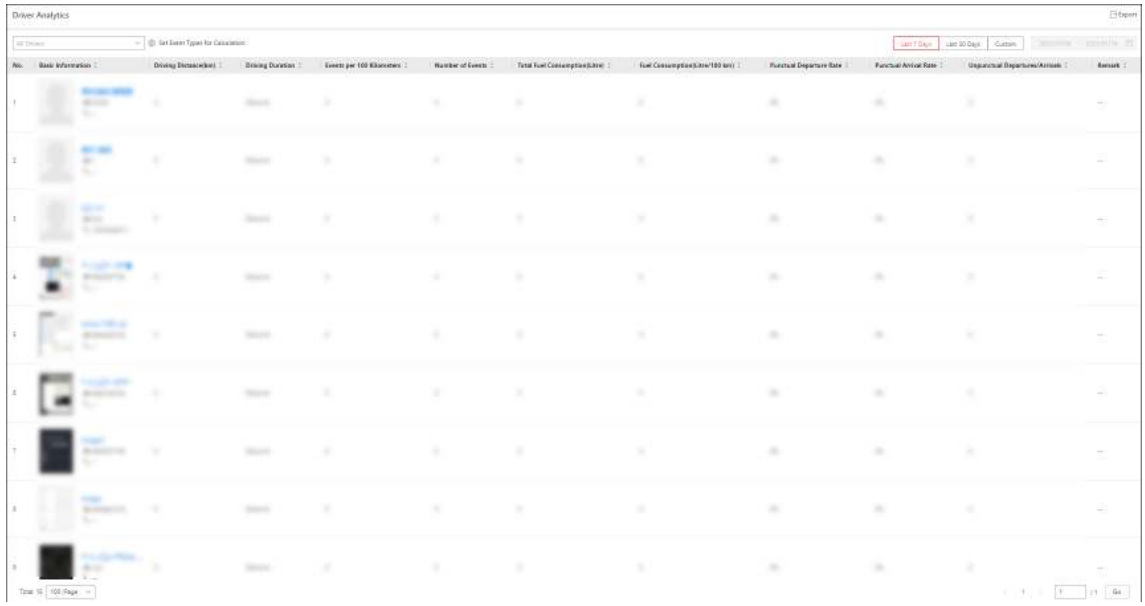


Figure 22-33 Generate a Driver Analytics Report

2. Select drivers from the drop-down list.
3. Click **Set Event Types for Calculation** to select event(s).
4. Set the time period within which driver's statistics will be shown in the report.

   The filtered records will be displayed automatically.
5. Click **Export** in the top right corner. Select **All Drivers** or **Filtered Drivers** and click **Export** to export the corresponding statistics report to the local PC.

22.10.3 Generate a GPS Information Report

You can generate 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.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → GPS Information Report** .
2. Set search conditions.

   Vehicle

   Select vehicles from the areas listed below.

   Note

   Up to 20 vehicles can be selected.

   Report Type

Select a report type.

Daily Report

The report to be generated will show the data of the selected vehicles in one calendar day.

Weekly Report

The report to be generated will show the data of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

By default, the data will be shown in a line chart, on which the Y-axis represents the number of locations and the X-axis the time.

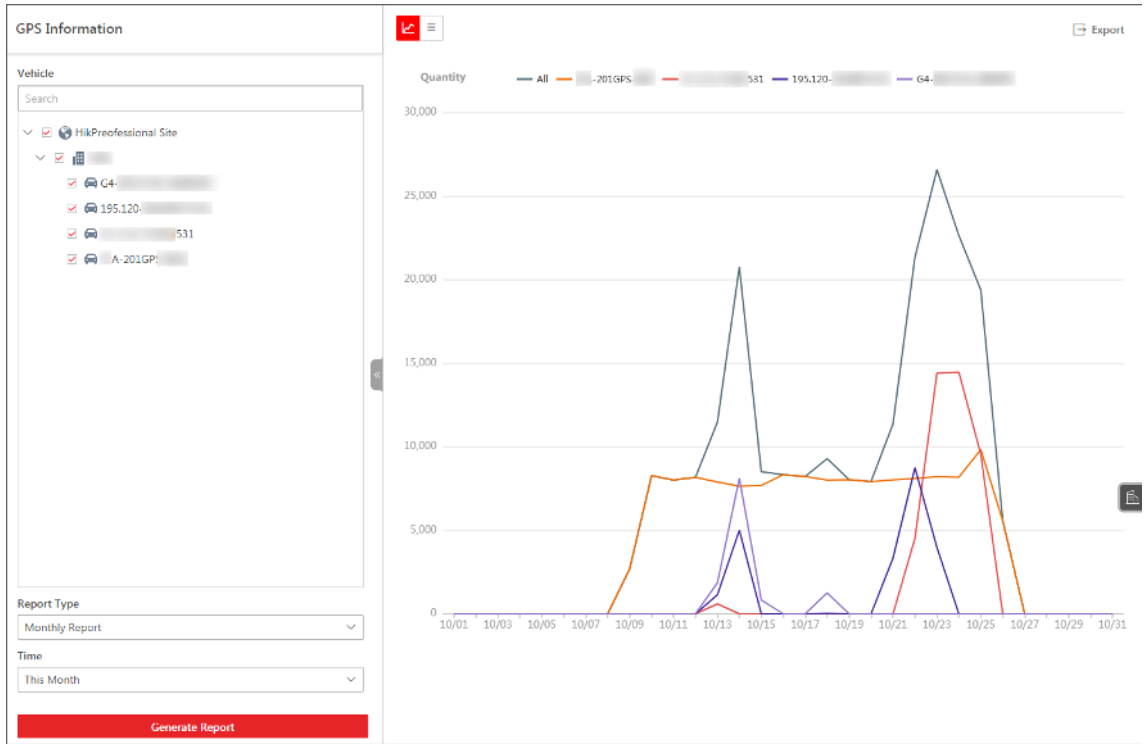


Figure 22-34 View Data in Line Chart

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

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide it.
View Data in Table	Click ≡ to view the data in a table that shows the license plate number, area, time, GPS information, direction, and speed. You can select a vehicle from the drop-down list and set a period to further filter the data.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles, time, content, and file format to export the report.

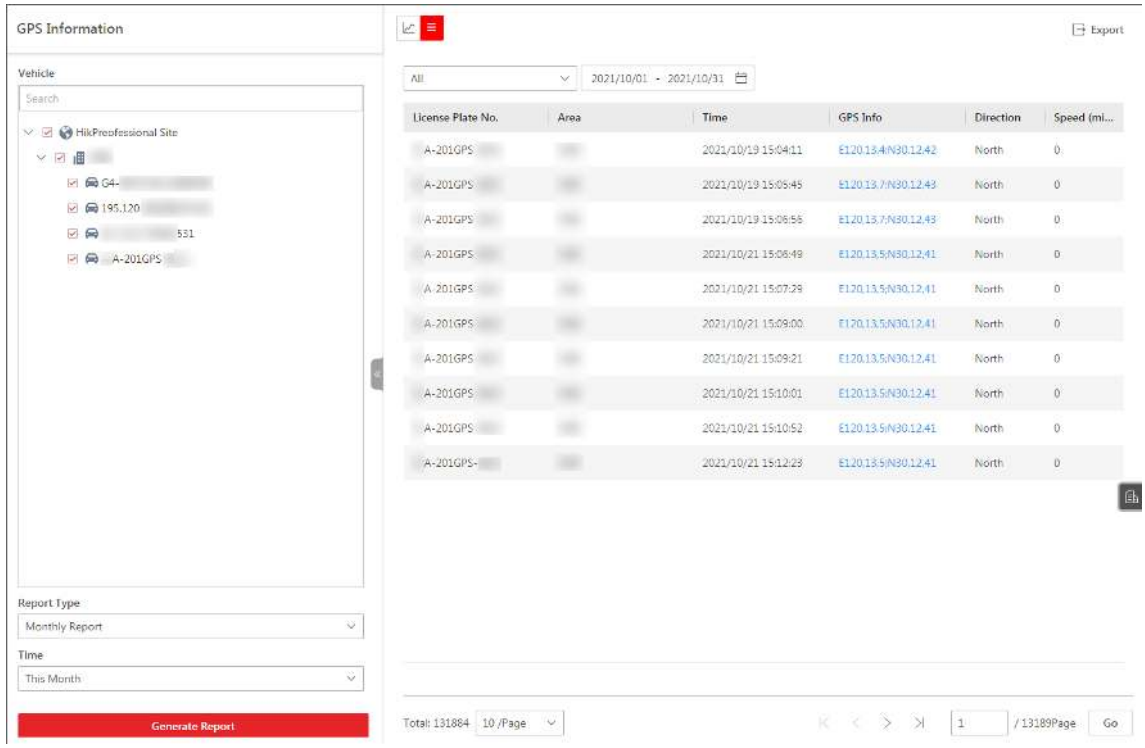


Figure 22-35 View Data in Table

22.10.4 Generate a Driving Distance Report

You can generate a driving distance report to view the driving distance of specific vehicles or drivers in a certain period.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → Driving Distance Report** .
2. Set search conditions.

   Analysis Type

   Select vehicle or driver as the analysis type and select vehicles/drivers from the list accordingly.

   Report Type

   Select a report type.

   Daily Report

   The report to be generated will show the driving distance of the selected vehicles in one calendar day.

   Weekly Report

The report to be generated will show the driving distance of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the driving distance of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the driving distance of the selected vehicles in a custom period of no more than 31 days.

Time

The driving distance in the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

By default, the data will be shown in a line chart, on which the Y-axis represents the driving distance and the X-axis the time.



Figure 22-36 Generate Report

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

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles/drivers at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide the corresponding data.
View Data in Table	Click ≡ to view the data in table.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles/drivers, time, and file format to export the report.

22.10.5 Generate a Driving Duration Report

You can generate a driving duration report to view the driving duration of specific vehicles or drivers at a certain speed in a certain period.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → Driving Duration Report** .
2. Set search conditions.

Analysis Type

Select vehicle or driver as the analysis type and select vehicles/drivers from the list accordingly.

Report Type

Select a report type.

Daily Report

The report to be generated will show the data of the selected vehicles in one calendar day.

Weekly Report

The report to be generated will show the data of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

Driving Speed Exceeds

Determine the threshold for calculating the driving duration. For example, if you select **40 mile/h**, the duration when the selected vehicles drove faster than 40 mile/h will be calculated.

3. Click **Generate Report**.

By default, data will be shown in a line chart, on which the Y-axis shows the driving duration (unit: second) and the X-axis the time.

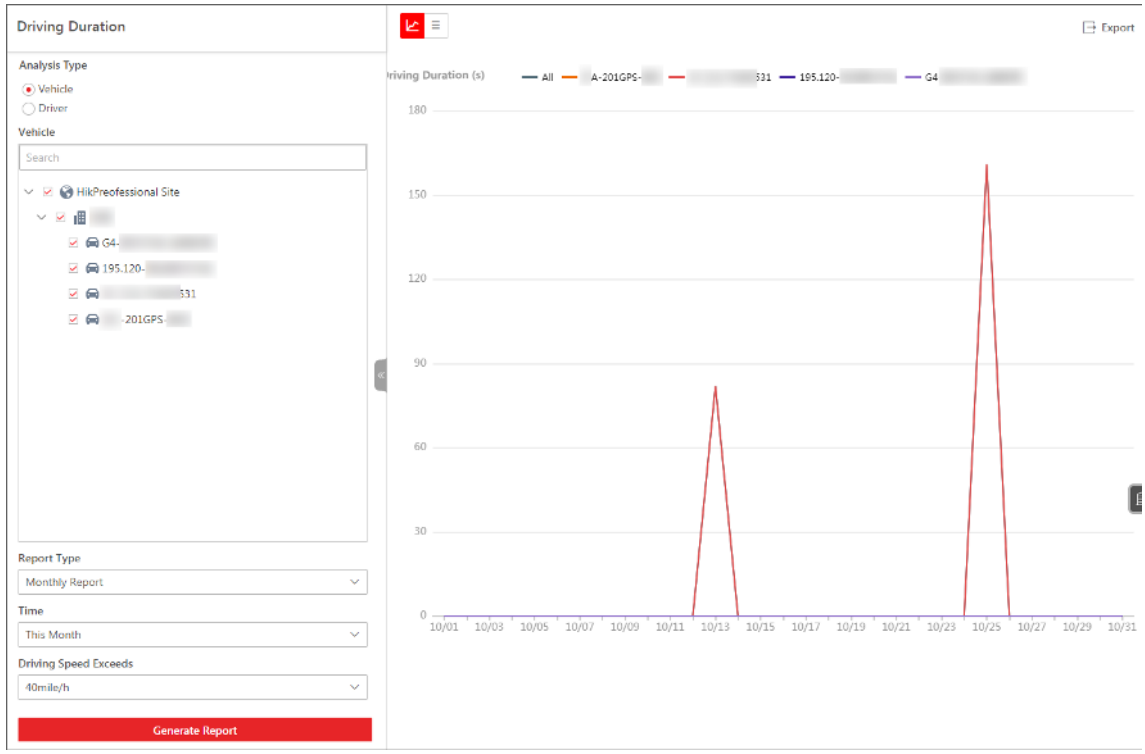


Figure 22-37 Monthly Report Example

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

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles/drivers at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide it.

View Data in Table	Click ≡ to view the data in a table.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles/drivers, time, and file format.

22.10.6 Generate a Speeding Report

You can generate a speeding report to view the vehicles' speeding records in a specific period.

Steps

Note

You can set the speed threshold for vehicles in a specific area. For details, see ***Add Vehicle to Area for Current Site*** .

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** → **Speeding Report** .
2. Set search conditions.

Vehicle

Select vehicles from the areas listed below.

Note

Up to 20 vehicles can be selected.

Report Type

Select a report type.

Daily Report

The report to be generated will show the data of the selected vehicles in one calendar day.

Weekly Report

The report to be generated will show the data of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

   By default, the data will be shown in a line chart, on which the Y-axis represents the speeding times and the X-axis the time.

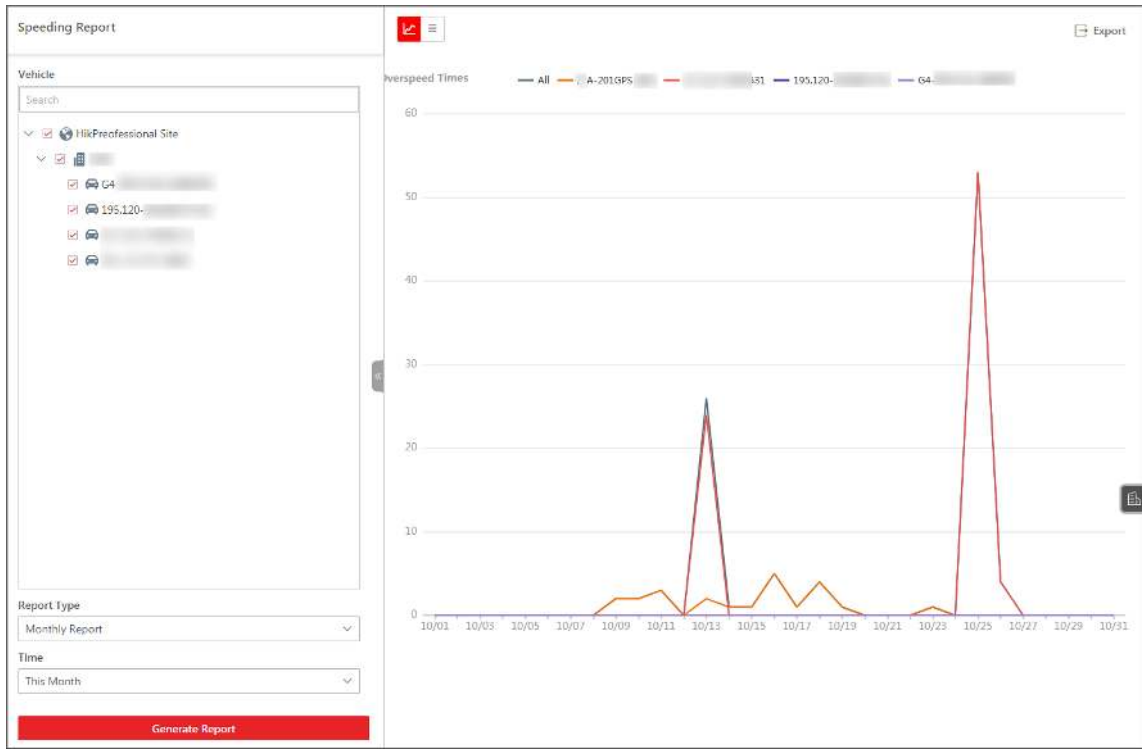


Figure 22-38 View Data in Line Chart

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

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide it.
View Data in Table	Click ≡ to view the data in a table that shows the license plate number, area, time, data, direction, and speed.

You can select a vehicle from the drop-down list and set a period to further filter the data.

Export Report Click **Export** to open the Export pane, and then set parameters including vehicles, time, content, and file format to export the report.

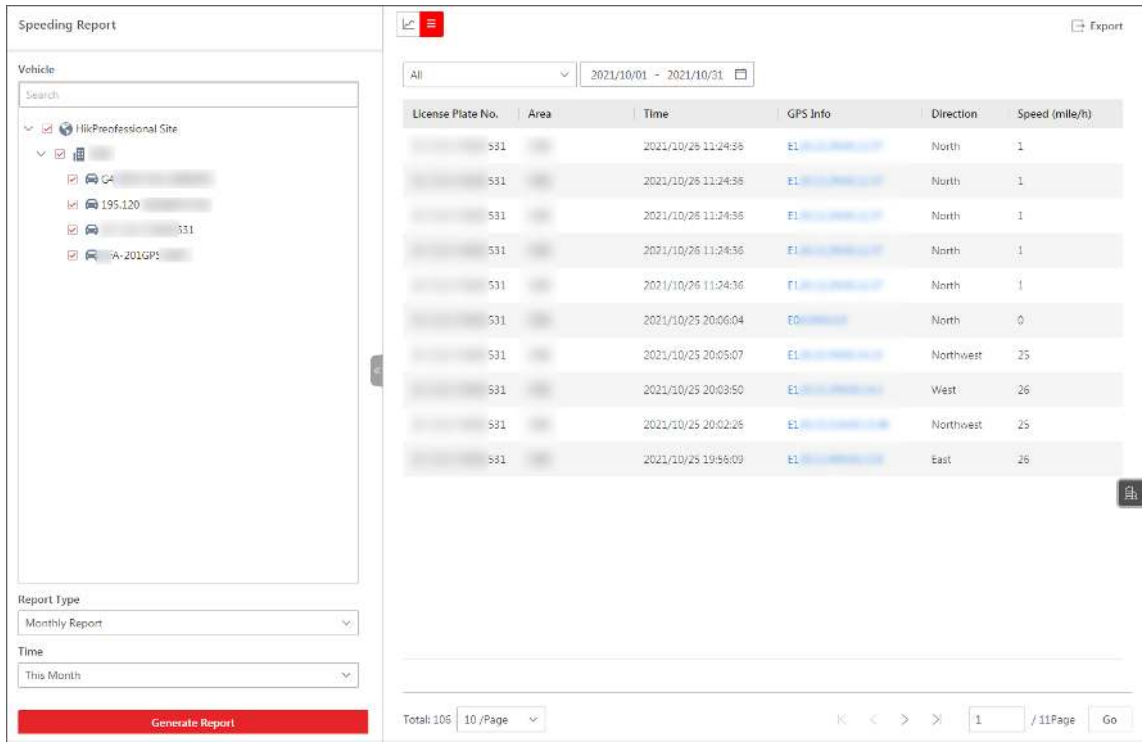


Figure 22-39 View Data in Table

22.10.7 Generate a Stop Analytics Report

You can generate 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.

Steps

1. On the top navigation bar, go to → **On-Board Service → On-Board Monitoring → Statistics and Reports → Stop Analytics** .
2. Select route(s) and stop(s) accordingly from the drop-down lists.
3. Select a time period for the report from **Today**, **Last 7 Days**, and **Custom**.

Note

The custom time period should be within 7 days.

The stop analytics report of the selected time period will be displayed on the page.

22.10.8 Generate a Driving Event Report

You can generate a driving event report to view the times of event detection related to specific vehicles in a specific period.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** → **Driving Event Report** .
2. Set search conditions.

Analysis Type

Select **Vehicle** or **Driver** as the analysis type and select vehicles/drivers from the list.

Statistics Type

Select **Total Events** or **Events per 100 Kilometers** as the statistics type.

Report Type

Select a report type.

Daily Report

The report to be generated will show the data of the selected vehicles in one calendar day.

Weekly Report

The report to be generated will show the data of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).

- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

Event Type

By default, all event types are selected.

You can click to select the events whose detection times will be calculated.

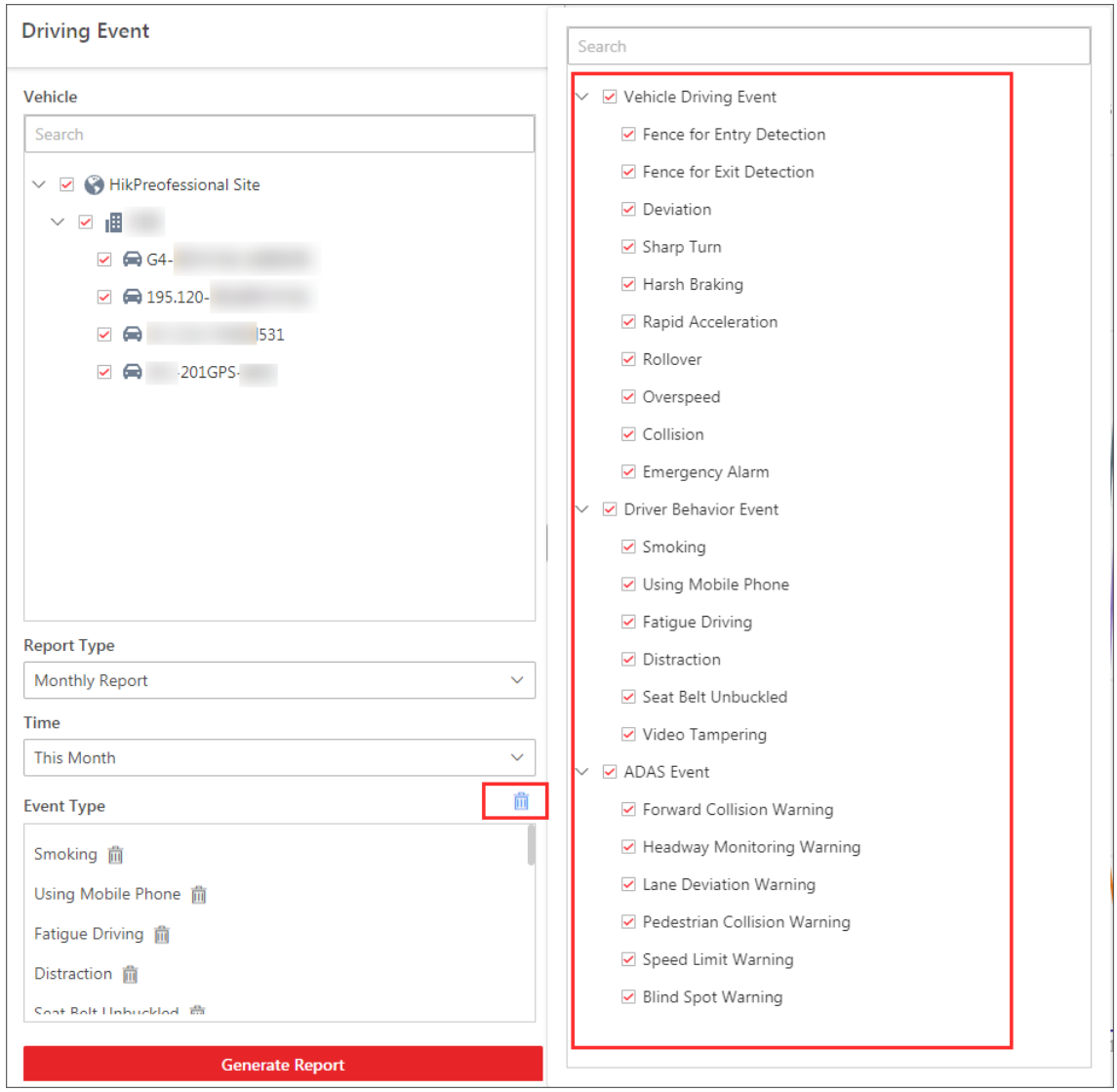


Figure 22-40 Select Events

3. Click **Generate Report**.

The data will be shown in a line chart on which the Y-axis represents the number of events and the X-axis the time.

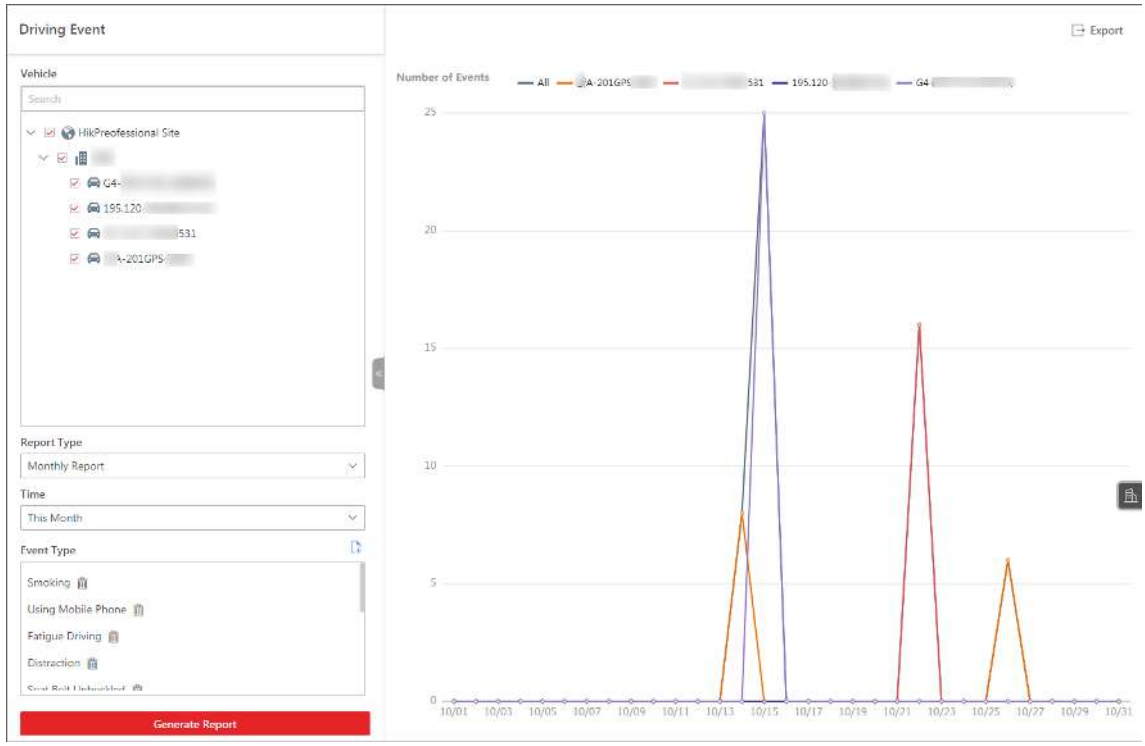


Figure 22-41 View Data in Line Chart

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

View Detailed Data	Hover the cursor onto the line chart to view detailed data of the selected vehicles at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide it.
Export Report	Click **Export** to open the Export pane, and then set parameters to export the report to your local PC.

22.10.9 Generate a Fuel Consumption Analytics Report

You can generate a fuel consumption analytics report to view the fuel consumption of specific vehicles or drivers in a certain period.

Steps

Note

Fuel consumption analytics reports can only be generated with fuel level monitoring enabled and the related parameters configured. For details, see ***Configure Fuel Level Monitoring Parameters*** .

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** → **Fuel Consumption Report** .

2. Set search conditions.

Analysis Type

Select vehicle or driver as the analysis type and select vehicles/drivers from the list accordingly.

Report Type

Select a report type.

Daily Report

The report to be generated will show the fuel consumption of the selected vehicles/drivers in one calendar day.

Weekly Report

The report to be generated will show the fuel consumption of the selected vehicles/drivers in one calendar week.

Monthly Report

The report to be generated will show the fuel consumption of the selected vehicles/drivers in one calendar month.

Custom Time Interval

The report to be generated will show the fuel consumption of the selected vehicles/drivers in a custom period of no more than 31 days.

Time

Fuel consumption in the selected time period will be shown in the report.

- For **Daily Report**, you can select from **Today**, **Yesterday**, and **Custom Time Interval** (any calendar day).
- For **Weekly Report**, you can select from **Current Week**, **Last Week**, and **Custom Time Interval** (any calendar week).
- For **Monthly Report**, you can select from **Current Month**, **Last Month**, and **Custom Time Interval** (any calendar month).
- For reports of a custom time interval, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

The report will be shown on the right side of the page.

Note

By default, data will be shown in a line chart, of which the y-axis is the overall fuel consumption value of all selected vehicles/drivers and the x-axis is the time. A table listing the statistics for each vehicle/driver is shown below the line chart.

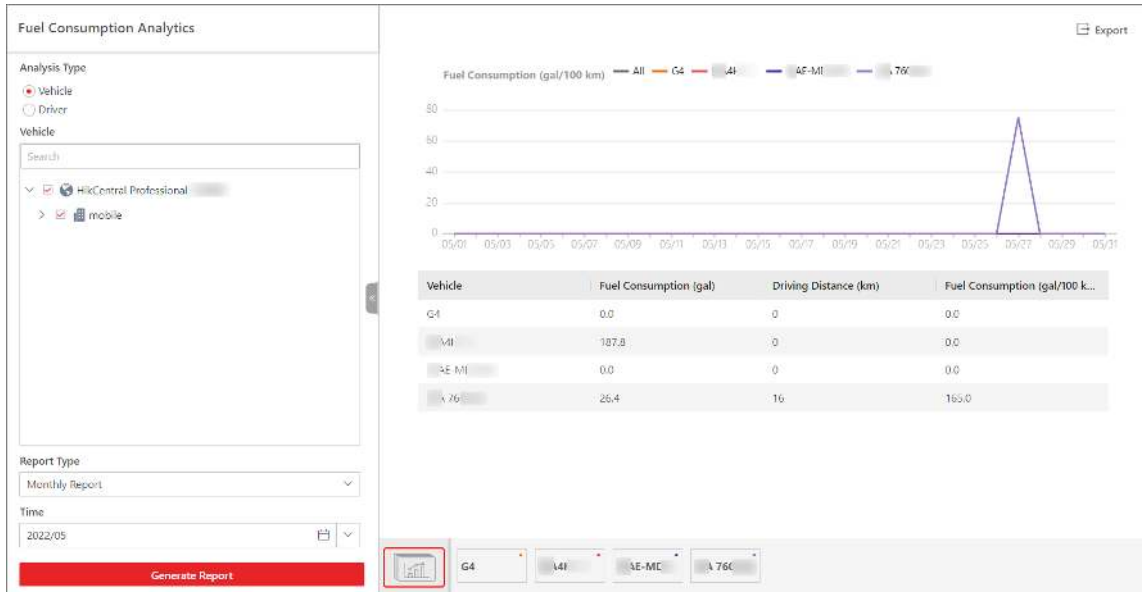


Figure 22-42 Monthly Report Example

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

View Fuel Consumption of a Specific Vehicle/ Driver	Click the name of a specific vehicle/driver at the bottom and select the **Fuel Consumption** tab on top. Hover the cursor over the line chart to view the fuel consumption value of specific time points and the average consumption value of the selected time period. Data such as total fuel consumption, total driving distance, and fuel consumption per 100 kilometers are shown above the chart.
View Fuel Level Change of a Specific Vehicle	Click the name of a specific vehicle at the bottom and select the **Fuel Level Change** tab on top. Hover the cursor over the line chart to view detailed information of specific time points, including the specific report time, license plate number, driver, fuel level, fuel quantity, and GPS information. Click a point on the chart to pinpoint the vehicle's report location on the map above.
Show/Hide Legend	Click a legend on the top of the line chart to show/hide it.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles/drivers, time, report content, and file format.

22.10.10 Generate a Passenger Counting Report

You can generate a passenger counting report to view the number of passengers who got on/off in a specific period.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** → **Passenger Counting Report** .
2. Set search conditions.

   Analysis Type

   Select vehicle or stop as the analysis type and select vehicles/stops from the list accordingly.

   Report Type

   Select a report type.

   Daily Report

   The report to be generated will show the data of the selected vehicles in one calendar day.

   Weekly Report

   The report to be generated will show the data of the selected vehicles in one calendar week.

   Monthly Report

   The report to be generated will show the data of the selected vehicles in one calendar month.

   Custom Time Interval

   The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

   Time

   The data of the selected period will be shown in the report.

   - For **Daily Report**, you can set the time to today, yesterday, or custom time interval (any calendar day).
   - For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
   - For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
   - For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.
3. Click **Generate Report**.

   By default, the data will be shown in a line chart on which the Y-axis represents the number of passengers and the X-axis the time.

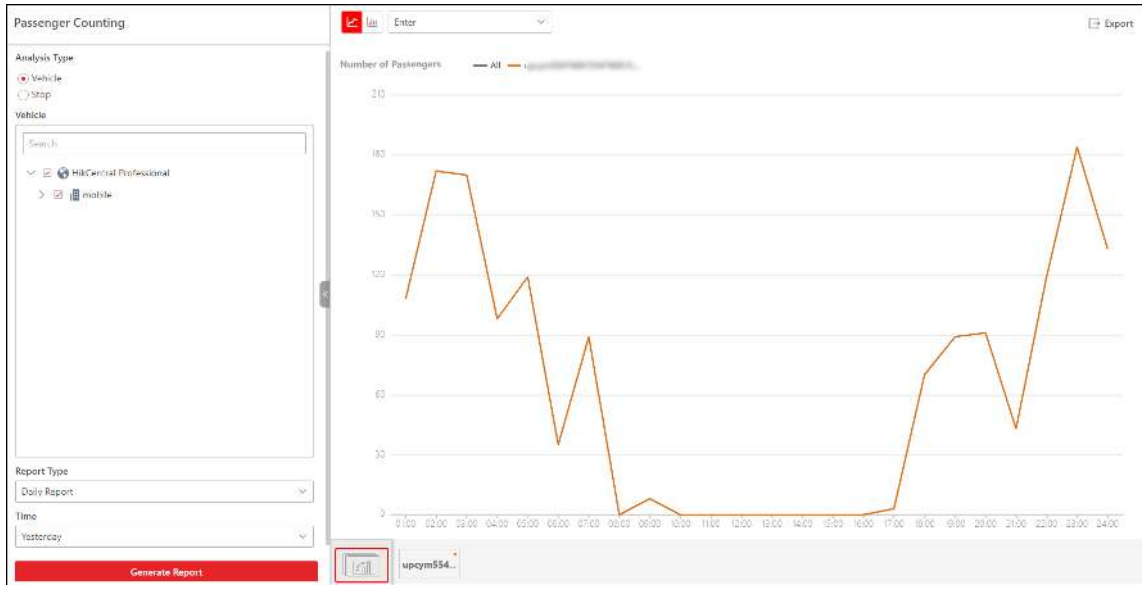


Figure 22-43 Generate a Passenger Counting Report

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

Switch Chart Mode	Click to switch the chart mode to histogram.
View Detailed Data	Hover the cursor onto the chart to view detailed data of the selected vehicles/stops at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the chart to show/hide it.
Filter by Passenger Movement Direction	Click the drop-down list on the top of the chart to select a passenger movement direction (Enter, Exit, Enter and Exit) to filter the data.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles/stops, time, and file format.

22.10.11 Generate a Device Online Rate Report

You can generate a report to view the online rate of the on-board devices mounted on the selected vehicles in a specific period.

Steps

1. On the top navigation bar, go to → **On-Board Service** → **On-Board Monitoring** → **Statistics and Reports** → **Device Online Rate Report** .
2. Set search conditions.

Vehicle

Select vehicles from the areas listed below.

Note

Up to 20 vehicles can be selected.

Report Type

Select a report type.

Weekly Report

The report to be generated will show the data of the selected vehicles in one calendar week.

Monthly Report

The report to be generated will show the data of the selected vehicles in one calendar month.

Custom Time Interval

The report to be generated will show the data of the selected vehicles in a custom period of no more than 31 days.

Time

The data of the selected period will be shown in the report.

- For **Weekly Report**, you can set the time to the current week, last week, or custom time interval (any calendar week).
- For **Monthly Report**, you can set the time to the current month, last month, or custom time interval (any calendar month).
- For setting **Custom Time Interval** as **Report Type**, you can only set the time to a period of no more than 31 days.

3. Click **Generate Report**.

The data will be shown in a line chart on which the Y-axis represents the devices' online rate and the X-axis the time.

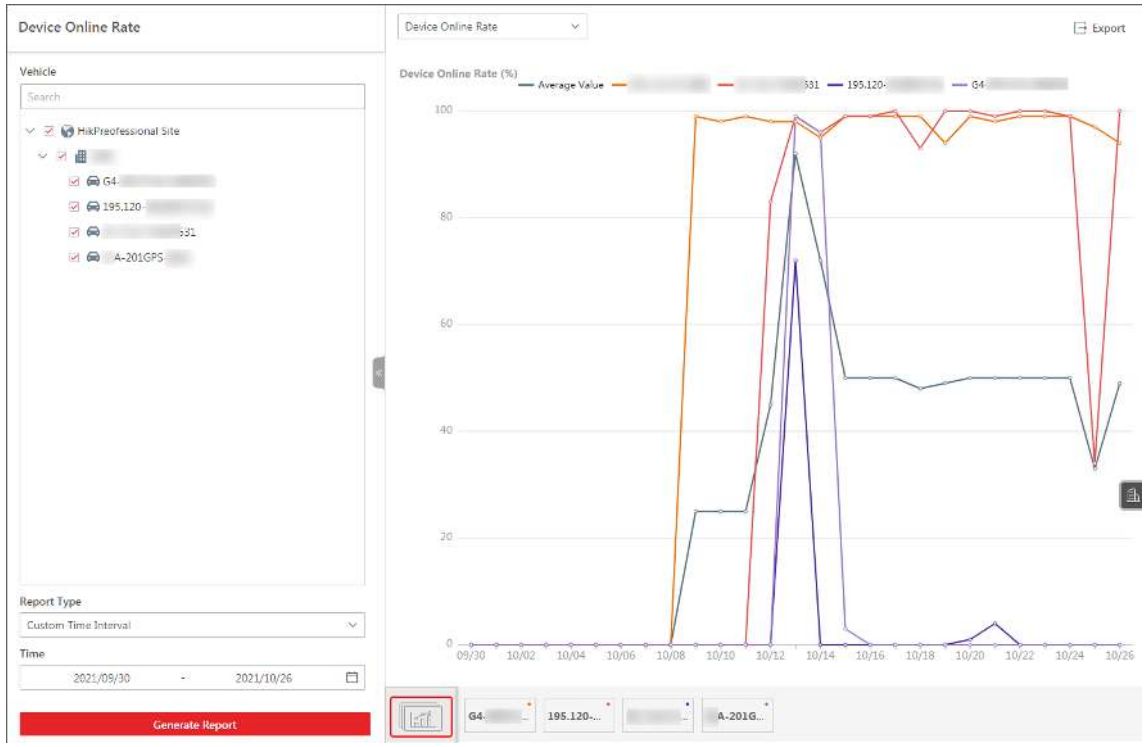


Figure 22-44 View Data in Line Chart

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

Switch Data Type	Select a data type (device online rate, online duration, or offline times) from the drop-down list on the top of the chart to display the selected type of data.
View Detailed Data	Hover the cursor onto the chart to view detailed data of the selected vehicles at the corresponding time point.
Show/Hide Legend	Click a legend on the top of the chart to show/hide it.
Filter by Vehicle	Click a vehicle at the bottom of the chart to view the data of the vehicle in the selected period.
Export Report	Click **Export** to open the Export pane, and then set parameters including vehicles, time, and file format.

Chapter 23 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.

23.1 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.

23.1.1 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 top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.
2. On the left navigation pane, click **Vehicle Management** → **Registered Vehicle** → **Vehicle** .
3. In the top left corner of the Vehicle page, click **Add** to enter the Add Vehicle page.

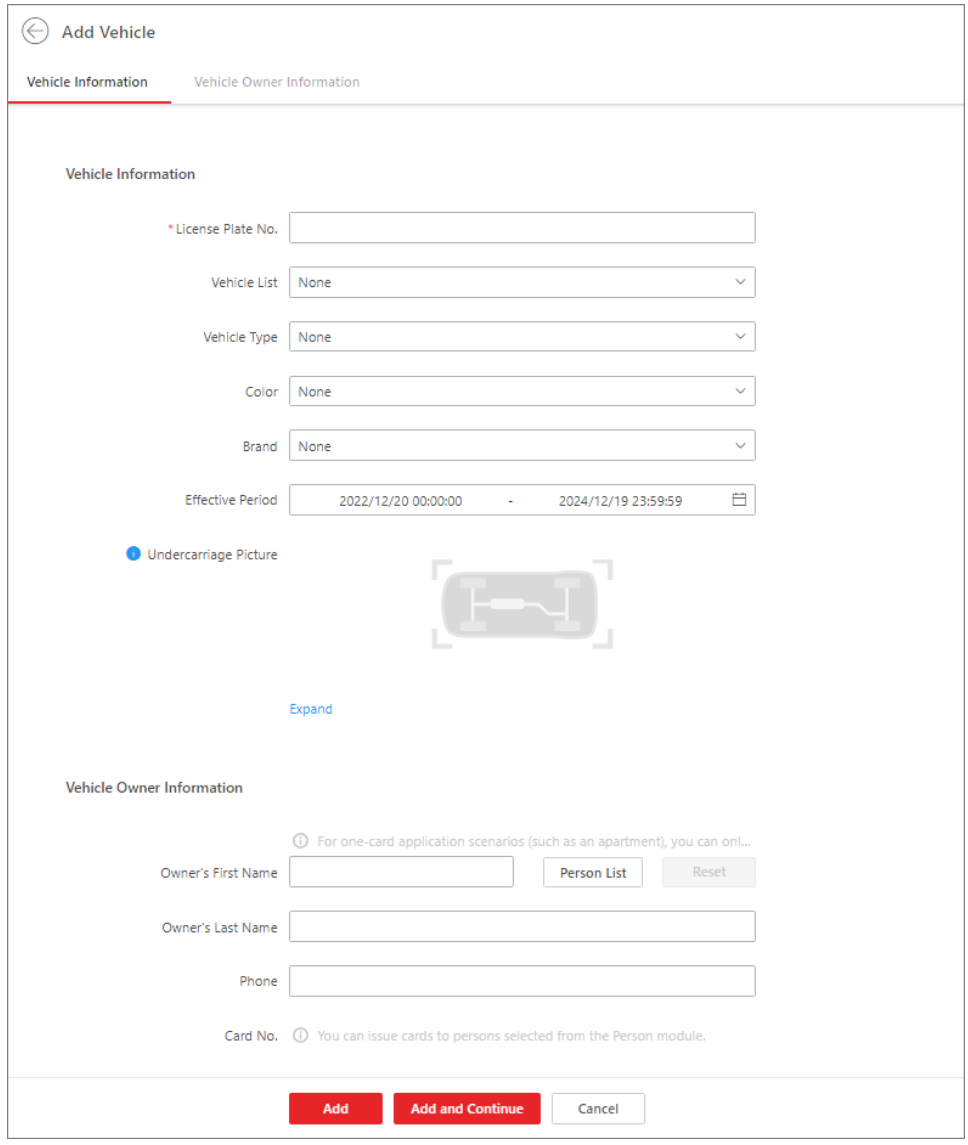


Figure 23-1 Add a Registered Vehicle

4. Set the vehicle information, such as the license plate number, vehicle list, type, color, brand, and so on.

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.

Custom Vehicle Information

If you have customized some fields for vehicles, click **Expand** to show the custom fields and fill in the corresponding information.

5. 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.

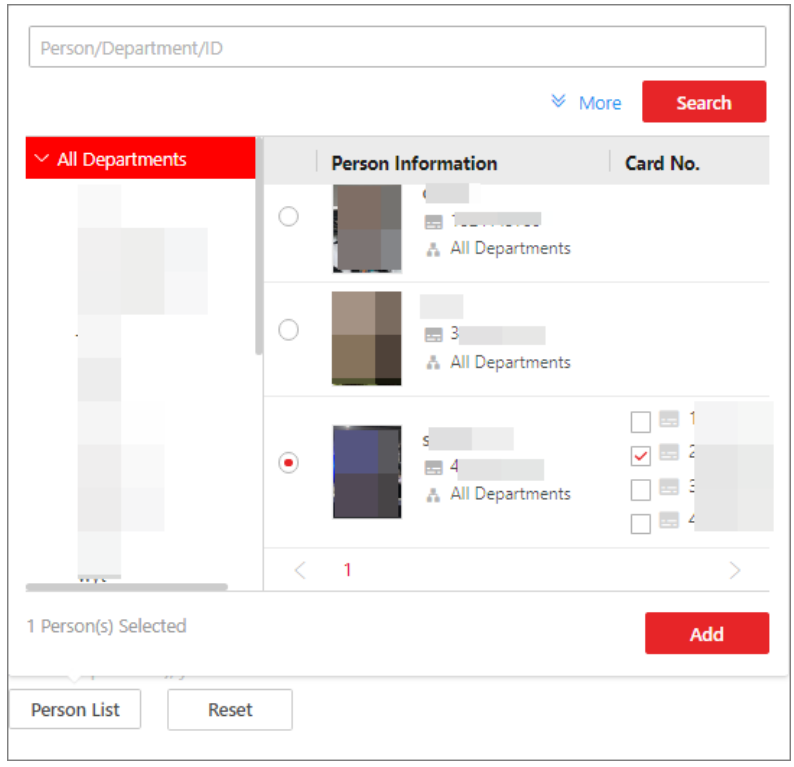


Figure 23-2 Select an Existing Person as Vehicle Owner

Note

- You can also select a person who has been linked to another vehicle.
- On the person list pane, you can enter the person's name, department, or ID to search for a specific person. Or you can click **More** to display persons' additional information fields,

enable the field(s), and enter the corresponding keywords to make the search result more accurate.

- For how to add persons and how to issue cards to persons, refer to ***Add a Single Person*** and ***Batch Issue Cards to Persons*** .

6. Click **Add** to add the registered vehicle or click **Add and Continue** to continue adding anther registered vehicle.

Note

If the license plate number already exists (in the current vehicle list or other vehicle lists), a prompt box will be displayed and you can select whether to replace the existing vehicle with the new one.

As only the vehicle with a parking pass can enter and exit the parking lot as a registered vehicle, after adding a registered vehicle, a window will pop up to remind you of topping up a parking pass for the vehicle by clicking **Parking Pass Top-Up**. Or you can click **Return to Vehicle List** and top up a parking pass for the vehicle in the Top-Up Management module later. See ***Top Up Parking Pass*** for more details.

7. **Optional:** Perform the following operation(s) after adding registered vehicles.

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). • 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.
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.

23.1.2 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 top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.
2. On the left navigation pane, click **Vehicle Management** → **Registered Vehicle** → **Vehicle** .
3. In the top left corner of the Vehicle page, click **Import**.

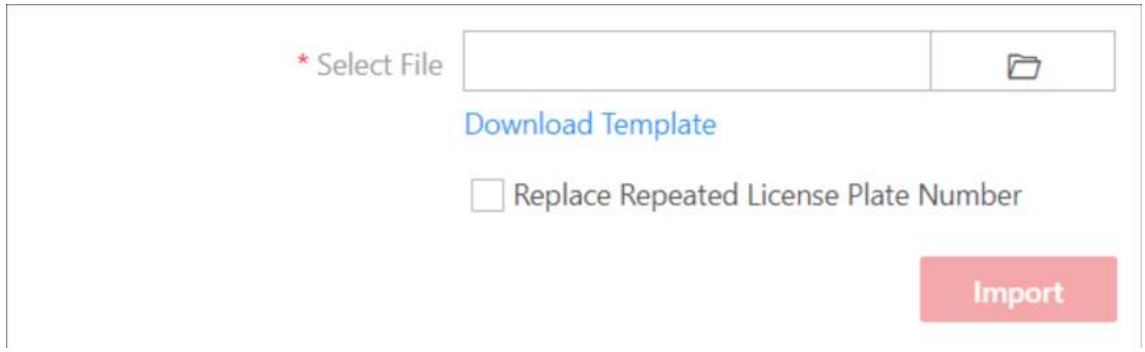


Figure 23-3 Import File

4. Click **Download Template** to download and save the template file to your PC.
5. Open the downloaded template file and enter the required information.
6. Click and select the file.
7. **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.
8. Click **Import**.
9. **Optional:** Perform the following operation(s) after importing registered vehicles.

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). • Click beside **Delete** and click **Delete All** 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.
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.

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. See ***Top Up Parking Pass*** for more details.

23.2 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 Role*** for details on permission settings.

Steps

Note

Up to 100 vehicle lists can be added.

1. On the top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.
2. On the left navigation pane, click **Vehicle Management** → **Registered Vehicle** → **List Management** .
3. At the top of the left pane, click + to open the Add Vehicle List pane.

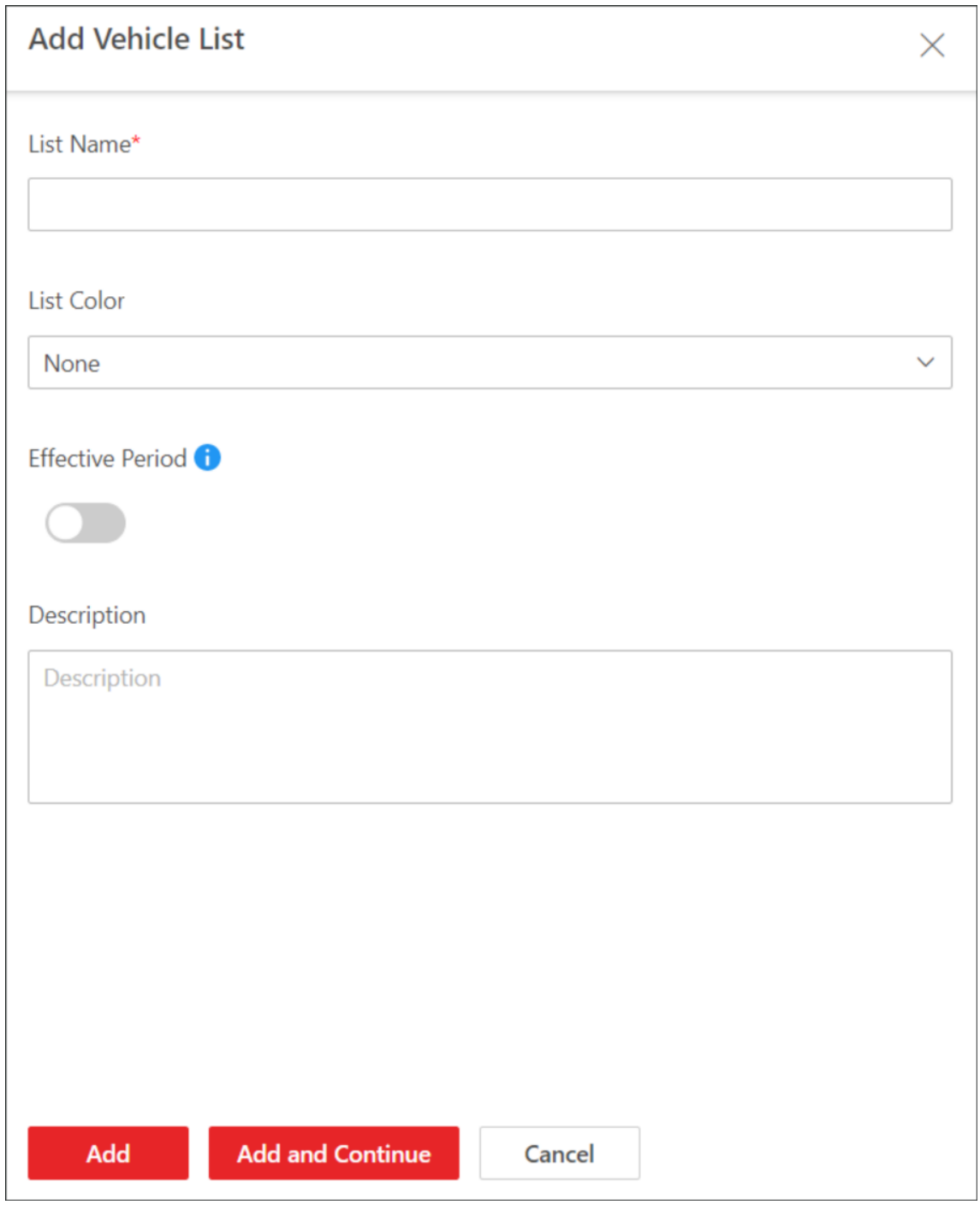


Figure 23-4 Add Vehicle List Page

4. 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, vehicles in the list will not be allowed to enter the parking lot 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.

5. Click **Add** to add the vehicle list or click **Add and Continue** to continue adding another vehicle list.
6. **Optional:** Select the added list and click **Add** to search for vehicles to be added to the list.

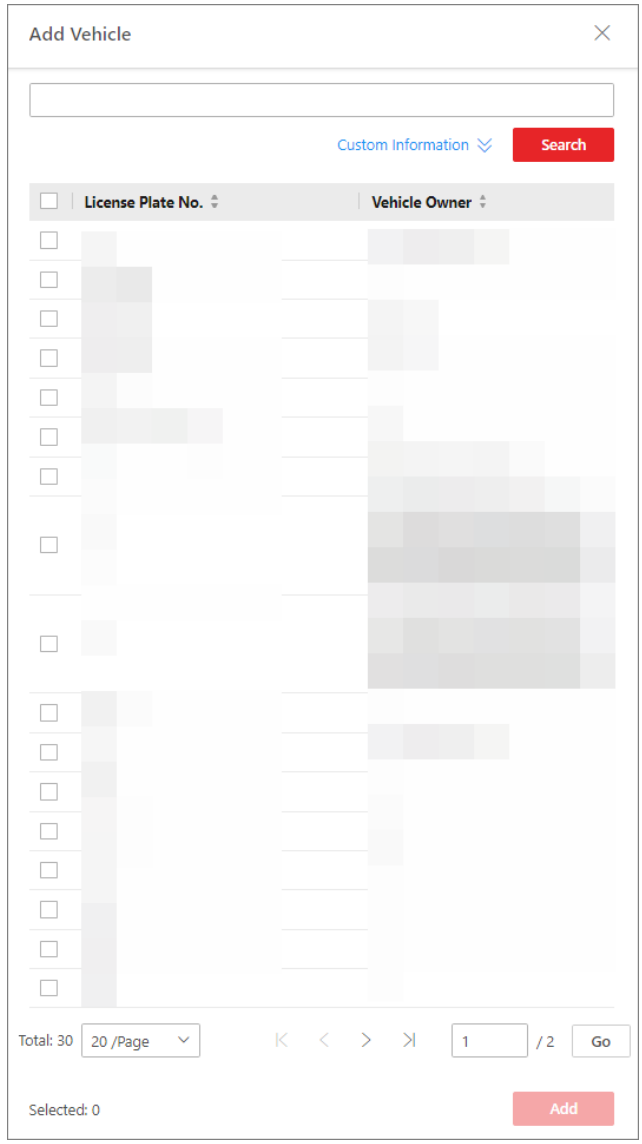


Figure 23-5 Add Vehicles to List

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*** .

7. **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.
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. • 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.

23.3 Filter and Export 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, so you can 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.

Steps

1. On the top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.
2. On the left navigation pane, click **Vehicle Management** → **Visitor Vehicle** .
3. Click in the top right corner to display the filter pane.

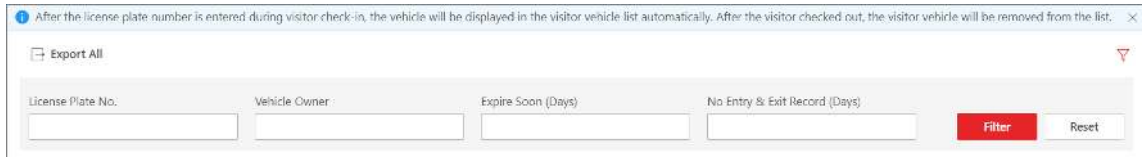


Figure 23-6 Search Visitor Vehicle Page

4. Set the filter condition(s), including license plate number, vehicle owner, expire soon (days), and no entry & exit record (days).

   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.
5. Click **Filter**.

   The matched result(s) will be displayed.
6. 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.

23.4 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.

23.4.1 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 top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.
2. On the left navigation pane, click **Vehicle Management** → **Blocklist** .
3. Click **Add** to enter the Add Vehicle to Blocklist page.

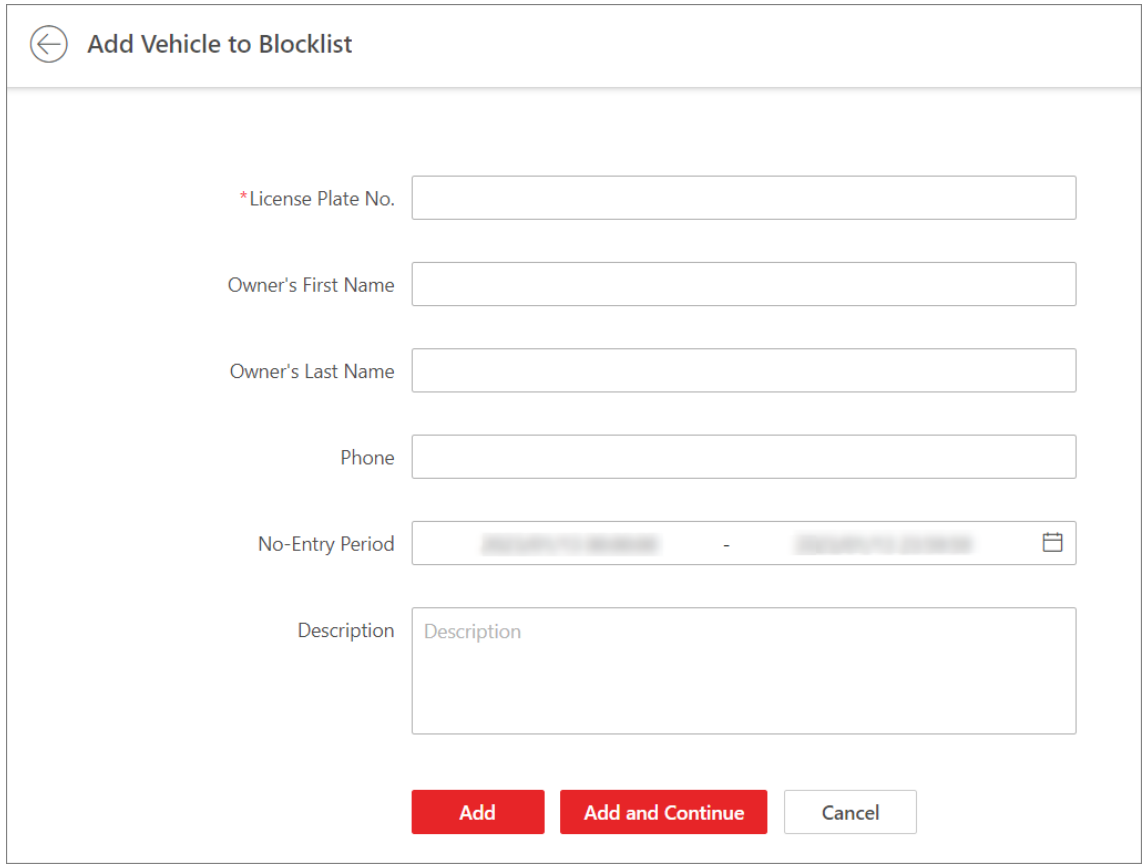


Figure 23-7 Add Vehicle to Blocklist

4. Enter the vehicle's license plate number.
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.
9. **Optional:** Perform the following operations if needed.

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. • 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.

23.4.2 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 top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.
2. On the left navigation pane, click **Vehicle Management** → **Blocklist** .
3. Click **Import**.

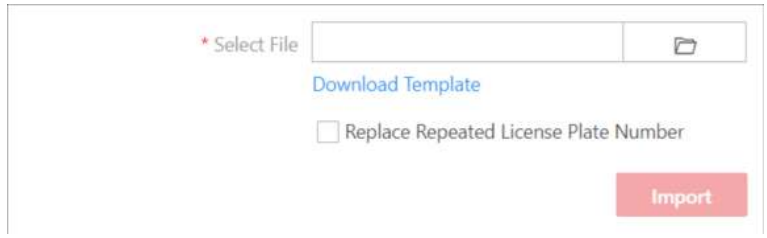


Figure 23-8 Import File

4. Click **Download Template** to download and save the template file to your PC.
5. Open the downloaded template file and enter the required information.
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 blocklist. Otherwise, the original vehicle information will be reserved.
7. Click **Import**.
8. **Optional:** Perform the following operations if needed.

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. • 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.

23.5 Customize Vehicle Information

You can customize different items of vehicle information (such as vehicle model) which are not predefined in the basic information. The customized vehicle information can help to recognize vehicles or search for vehicles more accurately.

Steps

1. On the top navigation bar, select → **Basic Management** → **Vehicle** or click **Vehicle** to enter the vehicle management page.
2. On the left navigation pane, click **Vehicle Information**.
3. Add vehicle types.
   1) Click **Add** in the Vehicle Type area to open the Add Vehicle Type pane.

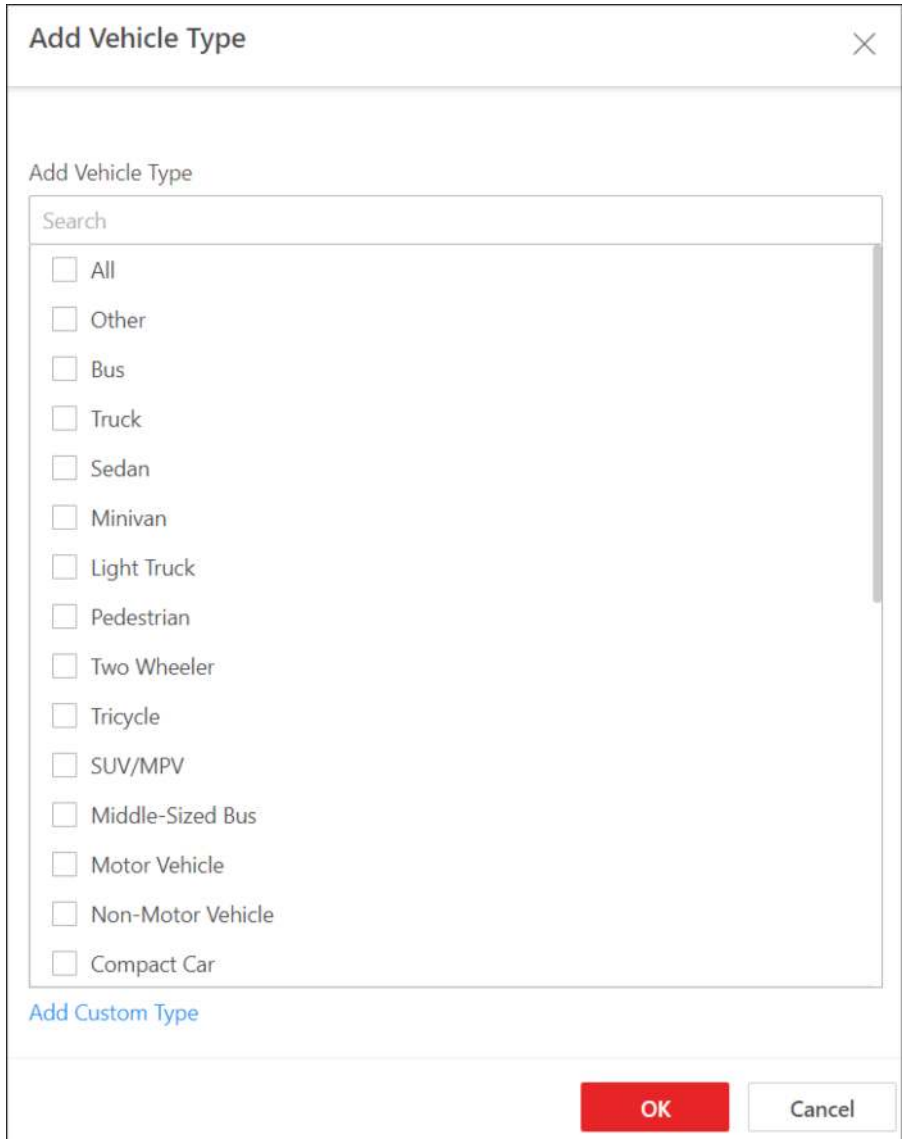


Figure 23-9 Add Vehicle Type

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**.

4. 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.

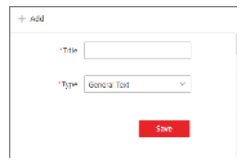


Figure 23-10 Customize Additional Information

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**.

5. **Optional:** Perform the following operation(s) after adding vehicle types or custom items.

Delete a Vehicle Type	Click in the Operation column of a vehicle type to delete it.
Edit a Custom Item	Click in the Operation column of a custom item to edit it.
Delete a Custom Item	Click in the Operation column of a custom item to delete it.

23.6 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 top navigation bar, select → **Basic Management** → **Vehicle** to enter the vehicle management page.
2. On the left navigation pane, click **Plate Fuzzy Search**.
3. Click **Add**.



Figure 23-11 Add Fuzzy Matching Rule

4. 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.

5. Click **Save**.
6. **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 24 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.

24.1 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 top navigation bar, select → **Passing Management** → **ANPR** → **Passing Vehicle Search** .

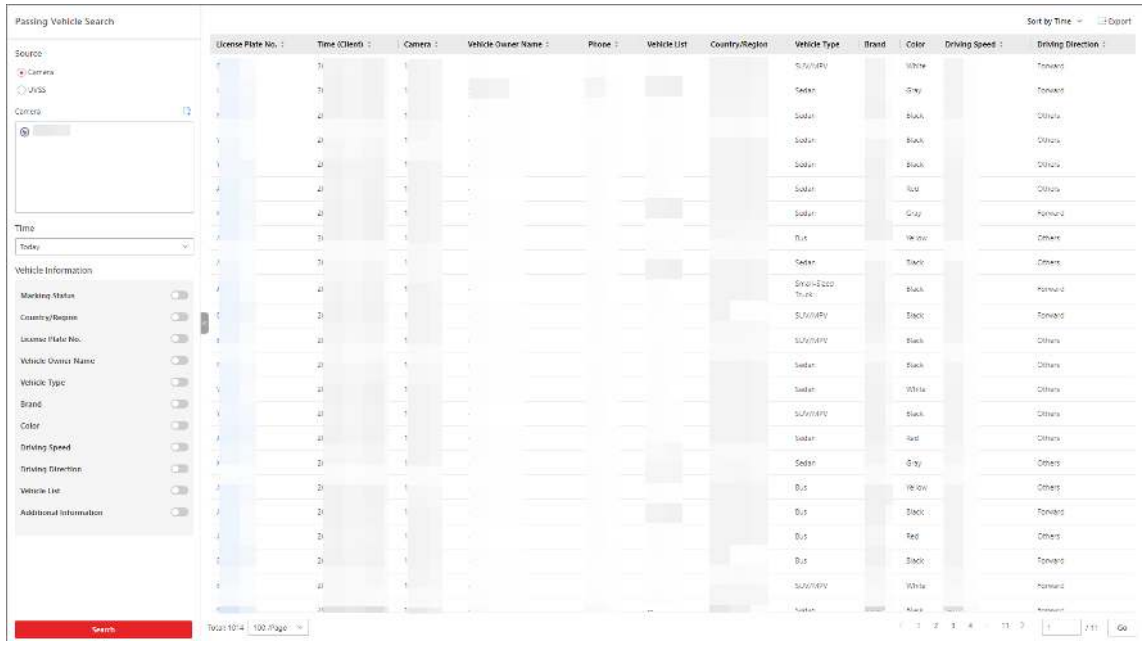


Figure 24-1 Passing Vehicle Search Page

2. Select a 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. 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.
5. Switch on and set the search condition(s) according to your needs. Here we only introduce some conditions that you may confuse.

   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

   A 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 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. 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.

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 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.
- No more than 100,000 passing vehicles without captured pictures can be exported at one time.

Sort Search Results

Sort by Time

Sort search results by the time when vehicles are passing through the camera or UVSS.

Sort by Vehicle Passing Times

Sort search results by times that vehicles passed through the camera or UVSS.

24.2 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 top navigation bar, select → **Passing Management → ANPR → Vehicle Analysis** .
2. Select the camera(s) for this report.
   1) Click in the Camera field to open the Select Camera pane.
   2) On the pane, select a site from the drop-down list to show its areas.
   3) Click an area to show its cameras which support the ANPR function.

   Note

   Only the online ANPN cameras will be displayed here.

   4) Check the camera(s) for analysis.

   Note

   No more than 20 ANPR cameras can be selected for one time analysis.

   5) Click anywhere outside the Select Camera pane to finish selecting the camera(s).
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 to 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 will calculate the number of vehicles in each day of way week, in 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 in each day or month of the custom time interval.

4. Set the time or a time period for analysis.

Note

- For the daily/weekly/monthly/annual report, you can select the current day/week/month/year, the last day/week/month/year, or specify a day/week/month/year in which the number of vehicles will be calculated.
- For the custom time interval report, you need to set the start time and end time to specify the time period in which the number of vehicles will be calculated.

5. Click **Generate Report**.

The statistics of passing vehicles detected by all the selected camera(s) are displayed on the right pane.

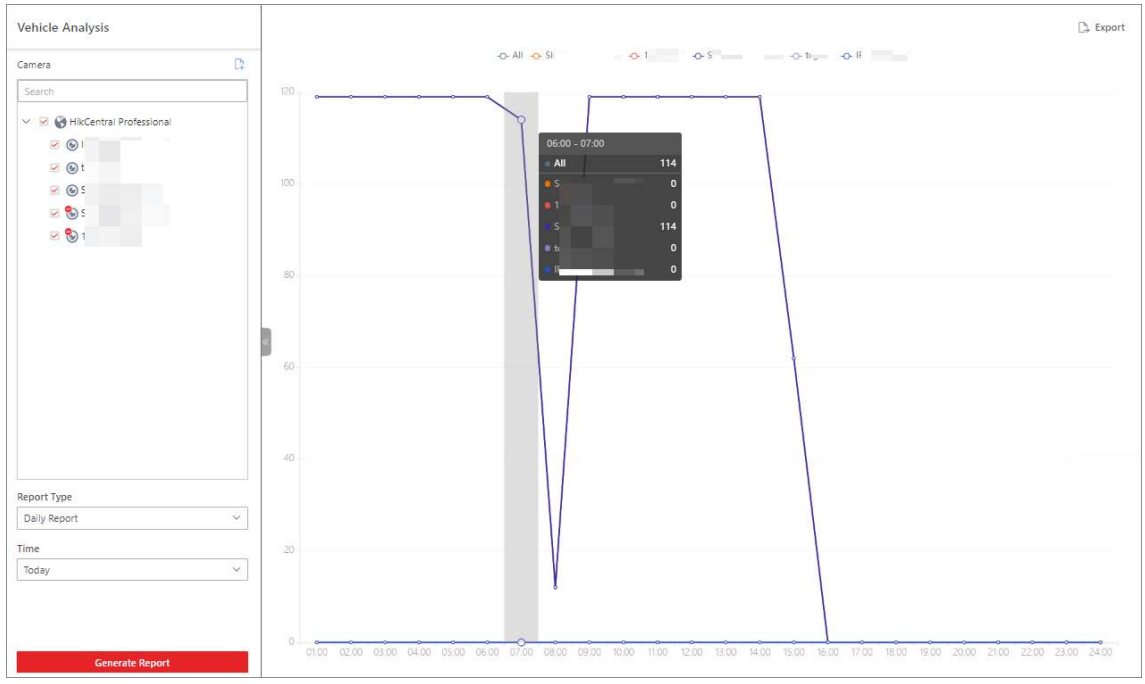


Figure 24-2 Vehicle Analysis Report

6. **Optional:** Export the generated report to the local PC.

1) Click **Export** in the top right corner of the report pane.

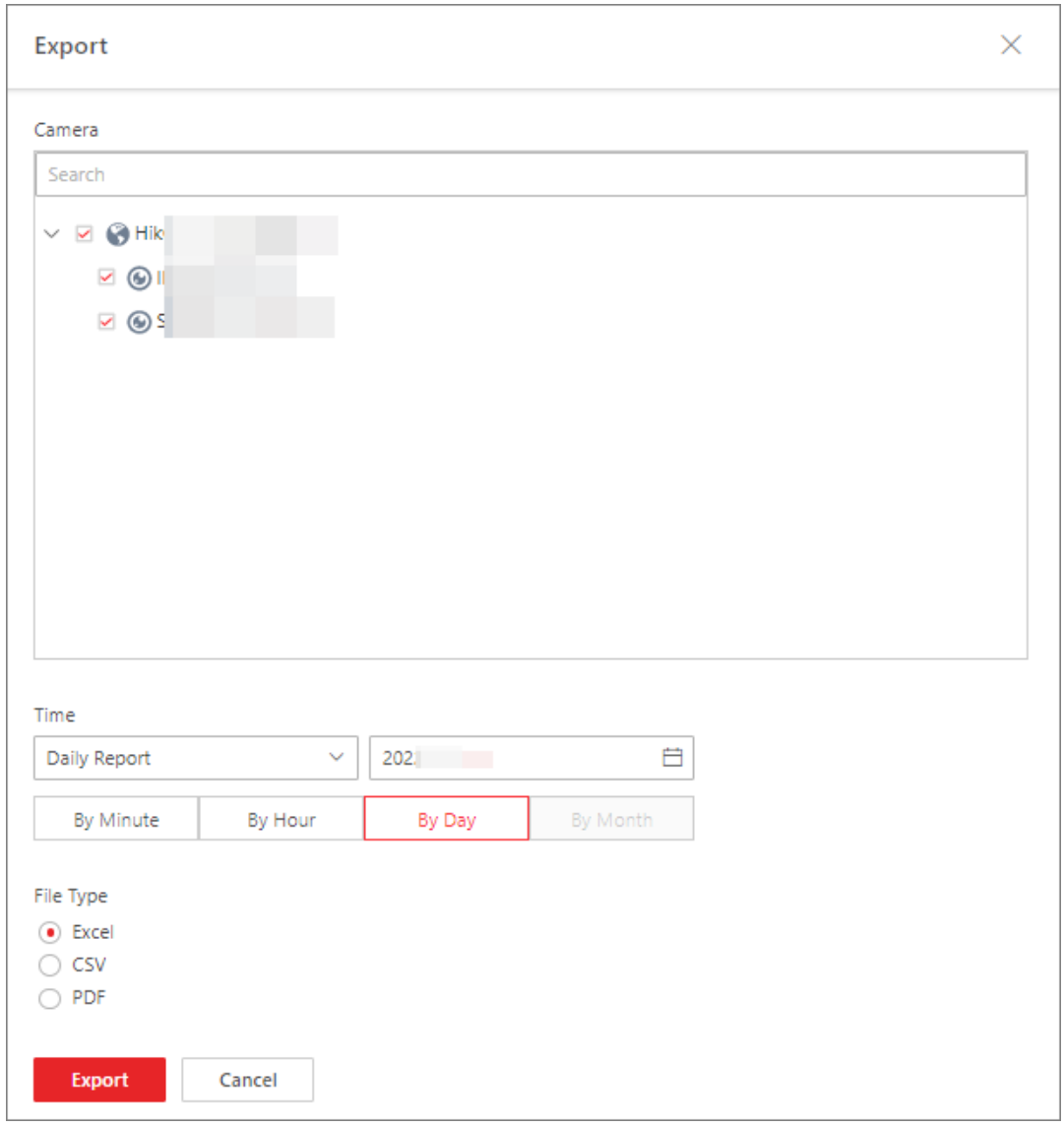


Figure 24-3 Export Vehicle Analysis Report

2) **Optional:** Select the camera(s) contained in the report 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 period is only available for the daily report.

By Hour

The exported report shows the detailed data of each hour for each camera. This period is available for the daily / weekly / monthly / custom time interval report.

By Day

The exported report shows the detailed data of each day for each camera. This period is available for all types of reports.

By Month

The exported report shows the detailed data of each month for each camera. This period 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.

24.3 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. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email settings such as sender address, SMTP server address, and port No. For details, refer to ***Configure Email Account*** .

Steps

Note

No more than 32,000 records can be contained in one report.

1. On the top navigation bar, select → **Passing Management → ANPR → 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.

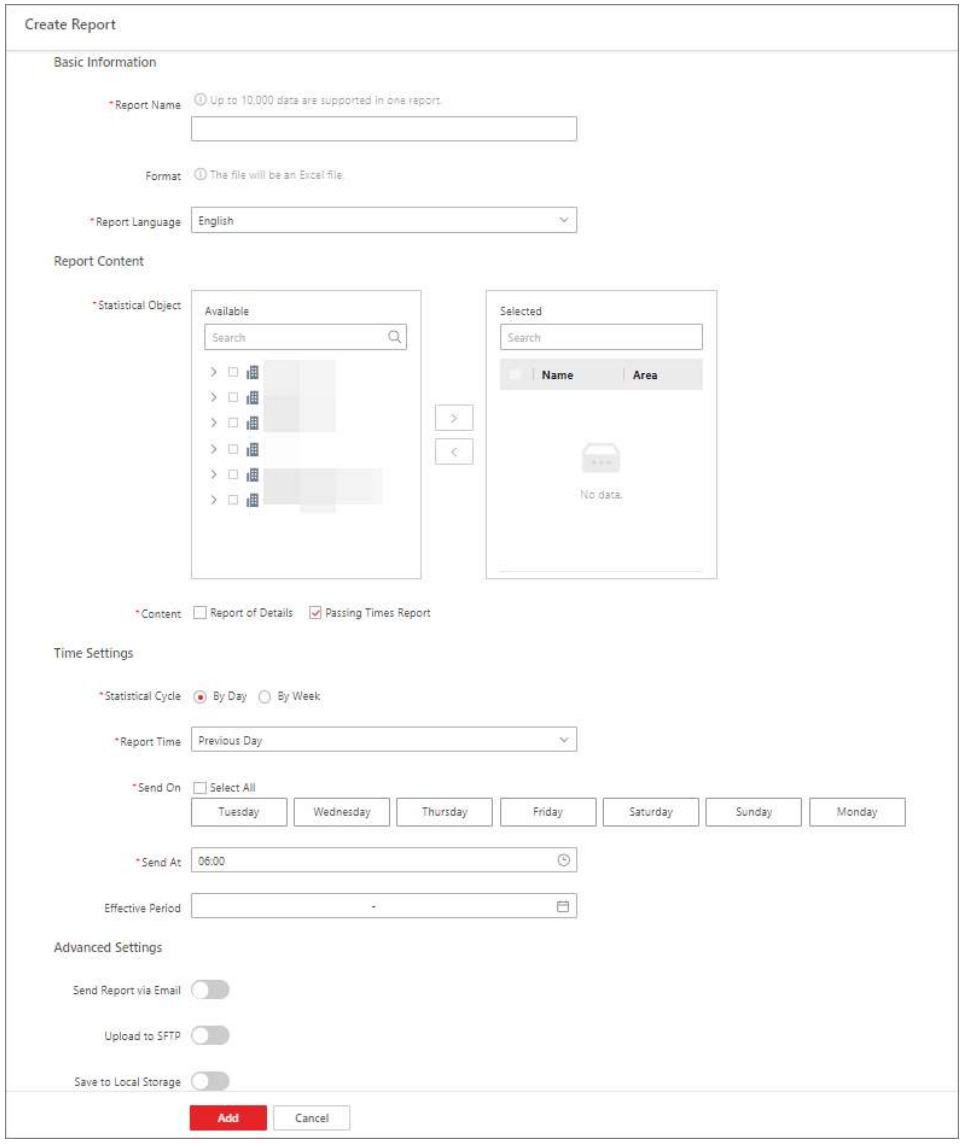


Figure 24-4 Create Report Page

3. Create a name for the report and select a report language from the drop-down list.

Note

By default, the language matches with the one you selected when logging in to the Web Client.

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.

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 On / Send At

- When the statistical cycle is set to **By Day**, the Send On 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 On field, and set the Send At 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 At 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. For setting an email template, refer to ***Add Email Template for Sending Report Regularly*** .

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 open the Configure Local Storage pane to configure the corresponding parameter.

7. Click **Add** to finish setting the scheduled report rule.

Chapter 25 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.

25.1 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.

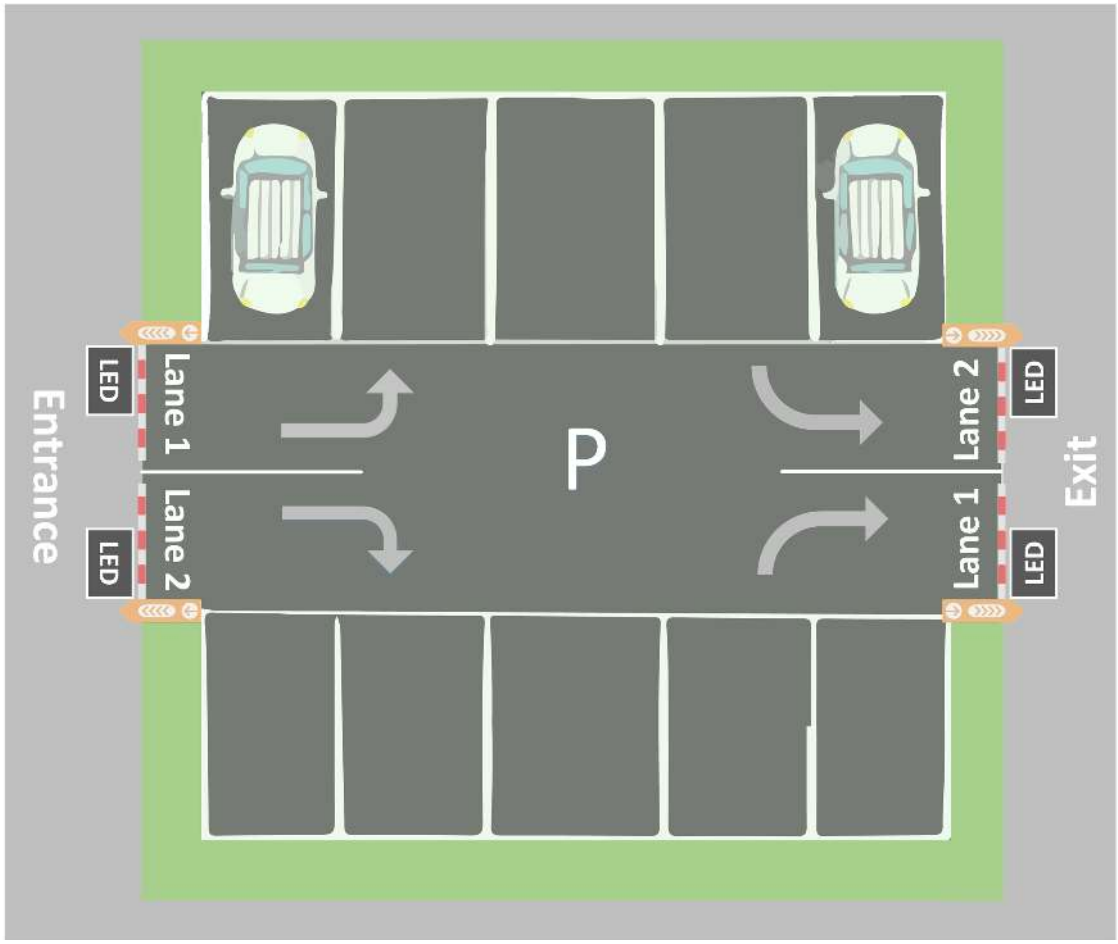
Entrance & Exit

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.


Entrance
LED
Lane 1
Lane 2
LED
P
Lane 2
Lane 1
LED
LED
Exit

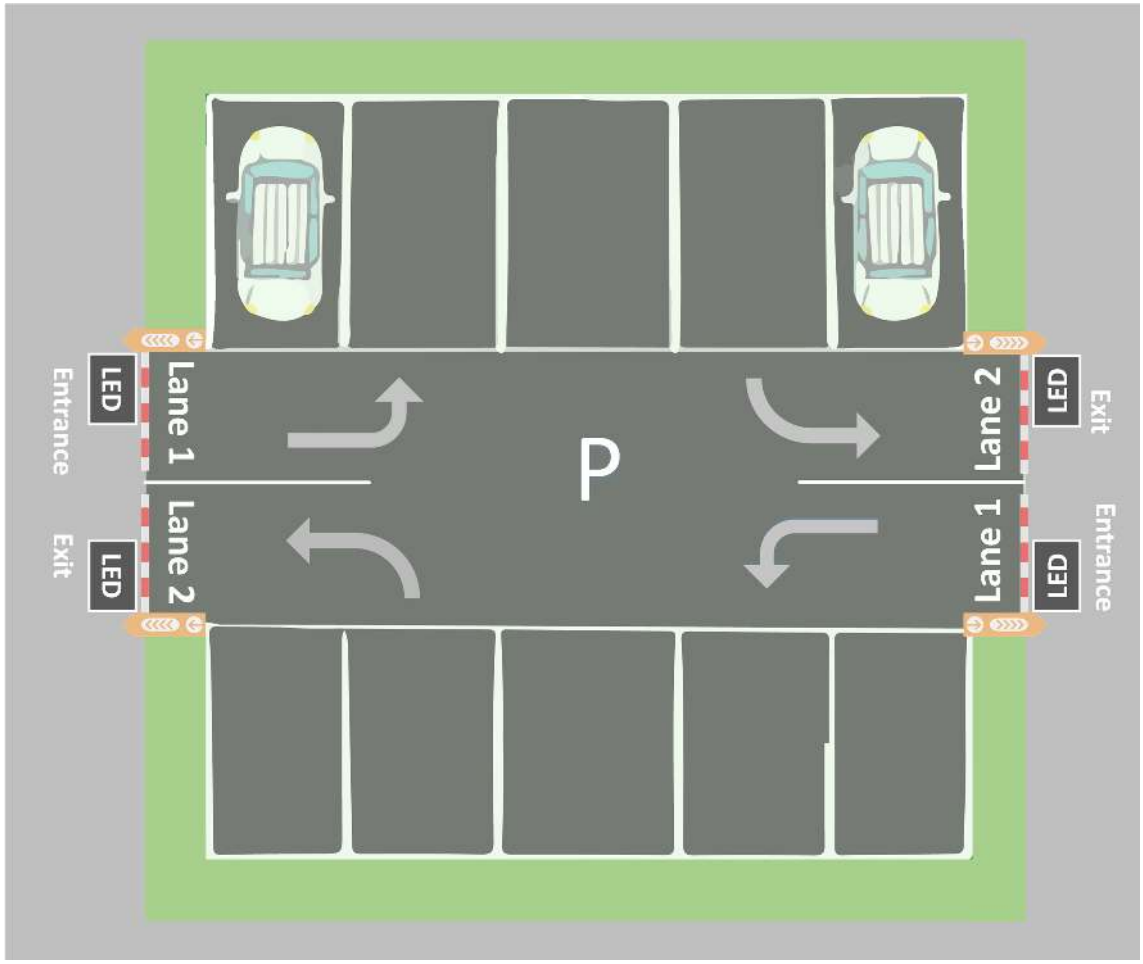


Figure 25-1 Parking Lot

25.1.1 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.

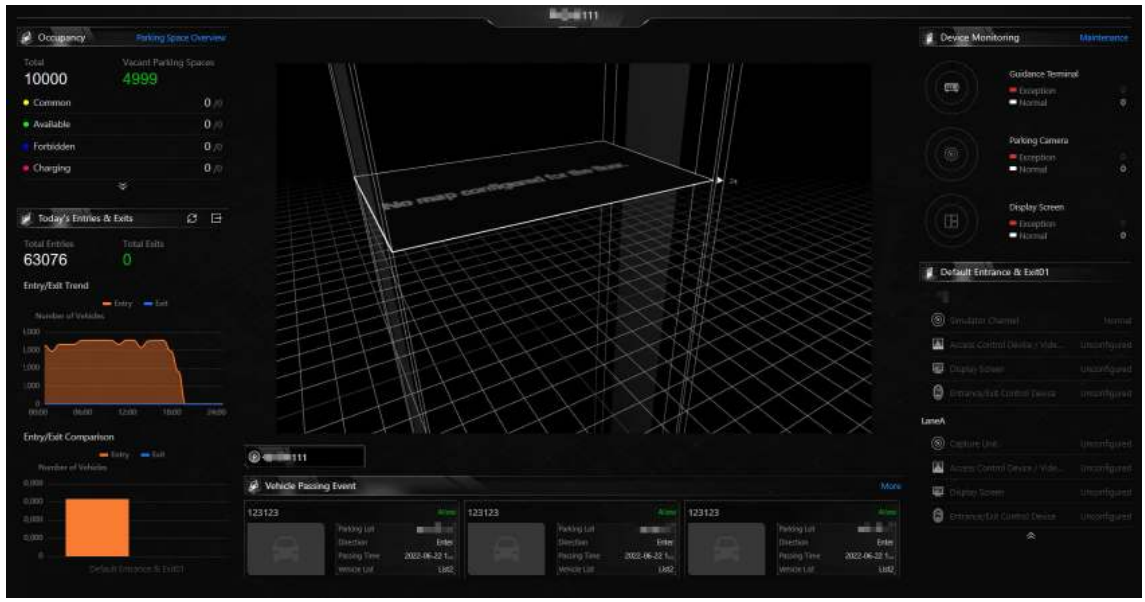


Figure 25-2 Parking Lot Overview Page

25.1.2 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 top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Parking Lot Management**.
3. In the top right corner of the page, click **Add Parking Lot** to open the Add Parking Lot pane.

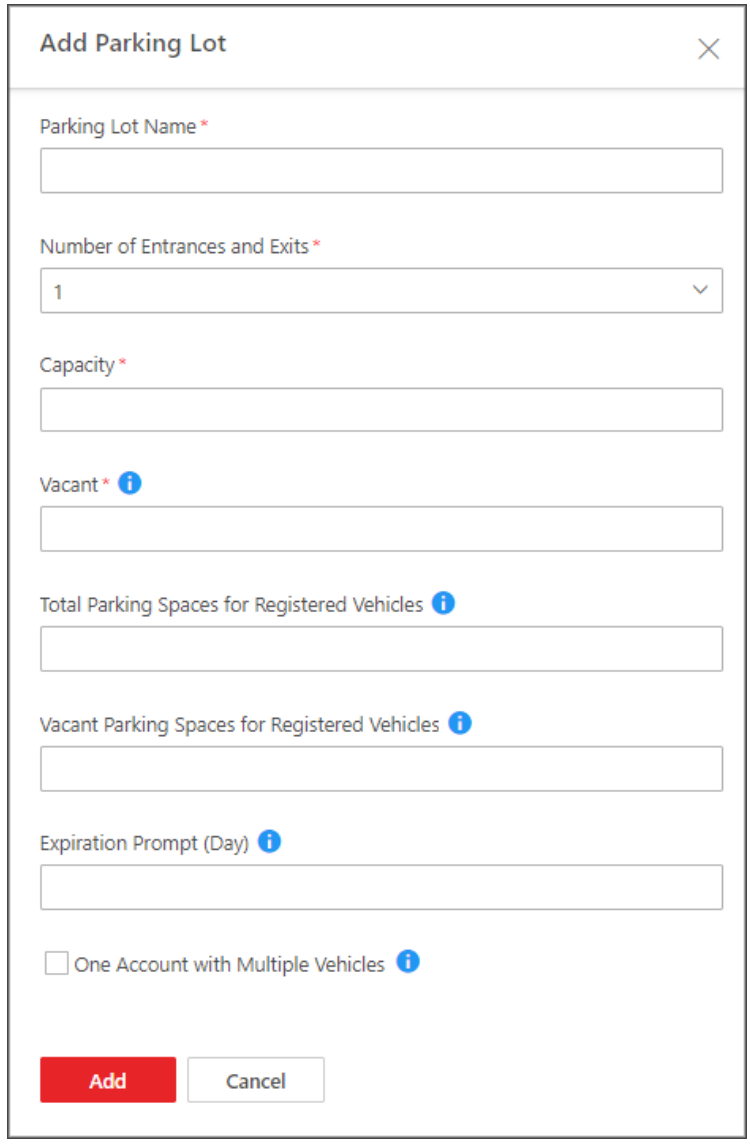


Figure 25-3 Add Parking Lot

4. Set the name, number of entrances and exits, the total parking capacity, and the number of vacant parking spaces for the parking lot, and set other related parameters as needed, such as the number of total/vacant parking spaces for registered vehicles, the number of days for displaying expiration prompts in advance, 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.

One Account with Multiple Vehicles

If checked, owners who have multiple vehicles but fewer valid parking spaces will be charged according to the parking fee rule selected for multiple vehicles under one account. For details, refer to ***Set Additional Parking Fee Rule*** .

5. Click **Add** to create the parking lot.
6. **Optional:** Edit the parking lot as needed.

Delete a Parking Lot	In a parking lot area, click **Delete** to delete it.
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** to enter the page of this parking lot. 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** to enter the page of this parking lot. b. On the right side of **Allowed Parking Duration**, click **Add**. c. In the pop-up window, select a vehicle type from Vehicle List. d. Enter the maximum parking duration allowed for the selected vehicle 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** to enter the page of this parking lot.

- 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.

25.1.3 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 top navigation bar, select → **Passing Management** → **Parking Lot** → **Parking Lot Management** .
2. Click **Settings** of an added parking lot to enter the configuration page of this parking lot.
3. On the top of the left list, select a parking lot and click .

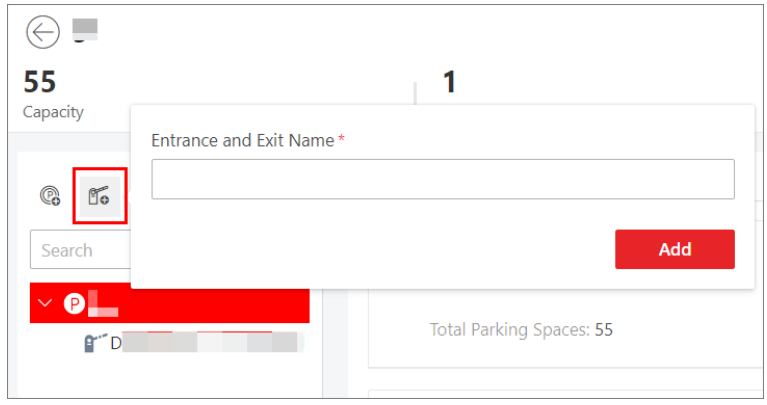


Figure 25-4 Add Entrance and Exit

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.

25.1.4 Add Lane

A lane is used to link different devices to realize different functions. For example, a lane linked with an entrance/exit control device is used for managing the entrance or exit of a parking lot, 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 (i.e., access control device and video intercom device) is used for controlling the barrier, a lane linked with a camera is used for capturing pictures, and a lane linked with a display screen is used for displaying information such as the number of vacant parking spaces.

Before You Start

Make sure you have added at least an entrance/exit for the parking lot. See ***Add Entrance and Exit*** for details.

Steps

1. On the top navigation bar, select → **Passing Management** → **Parking Lot** → **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.

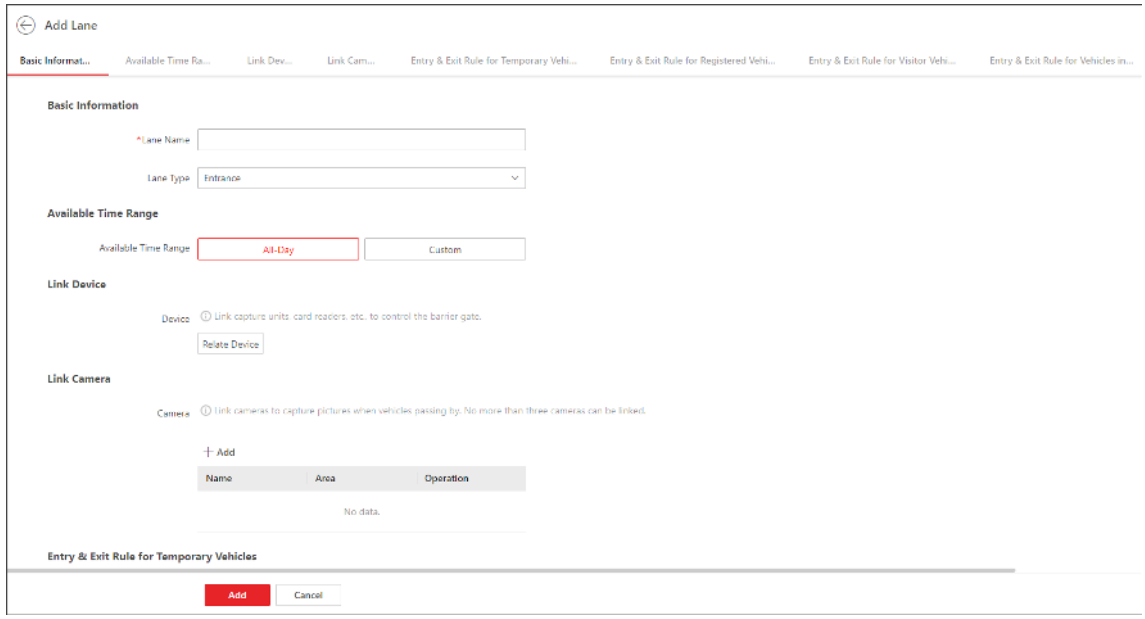


Figure 25-5 Add Lane Page

5. Set the lane.
   1) In the Basic Information area, create a name for the lane, and select a lane type from the drop-down list.

2) In the Available Time Range area, set the period during which the lane is available. Select **All-Day**, or select **Custom** to customize a period.
3) **Optional:** In the Link Device area, click **Relate Device** to select device(s) to be linked to the lane, and set one device as the barrier control unit according to actual needs.

Entrance/Exit Control Device

An entrance/exit control device is used for managing the entrance or exit of a parking lot, especially that of an unattended parking lot. After a vehicle gets a ticket or card from an entrance/exit control device, the device will control the barrier gate to open and let the vehicle enter; after the vehicle returns the ticket or card, the device will allow the vehicle to exit. Besides, if an entrance/exit device assigns cards instead of tickets, its guidance screen is configurable. See ***Link Display Screen and Set Displayed Content*** for details.

Capture Unit

A capture unit is used for capturing and recognizing license plate number. For example, the capture unit will open the barrier to allow the vehicle to enter the parking lot when recognizing a license plate number in the vehicle list, and will not open the barrier to prevent the vehicle from entering the parking lot when recognizing a license plate number 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 so, you need to set the **Matching Time**. Hence, when two capture units capture two pictures within the matching time, the picture captured by the capture unit with the higher confidence value will be kept.

Access Control Device

If the administrator selects a card (already issued to the owner for card authentication) for the owner when adding the owner's vehicle, the administrator actually binds the card with the vehicle's license plate number. So the barrier will open when the owner swipes the card on an access control device at the lane. In this circumstance, a capture unit is not needed.

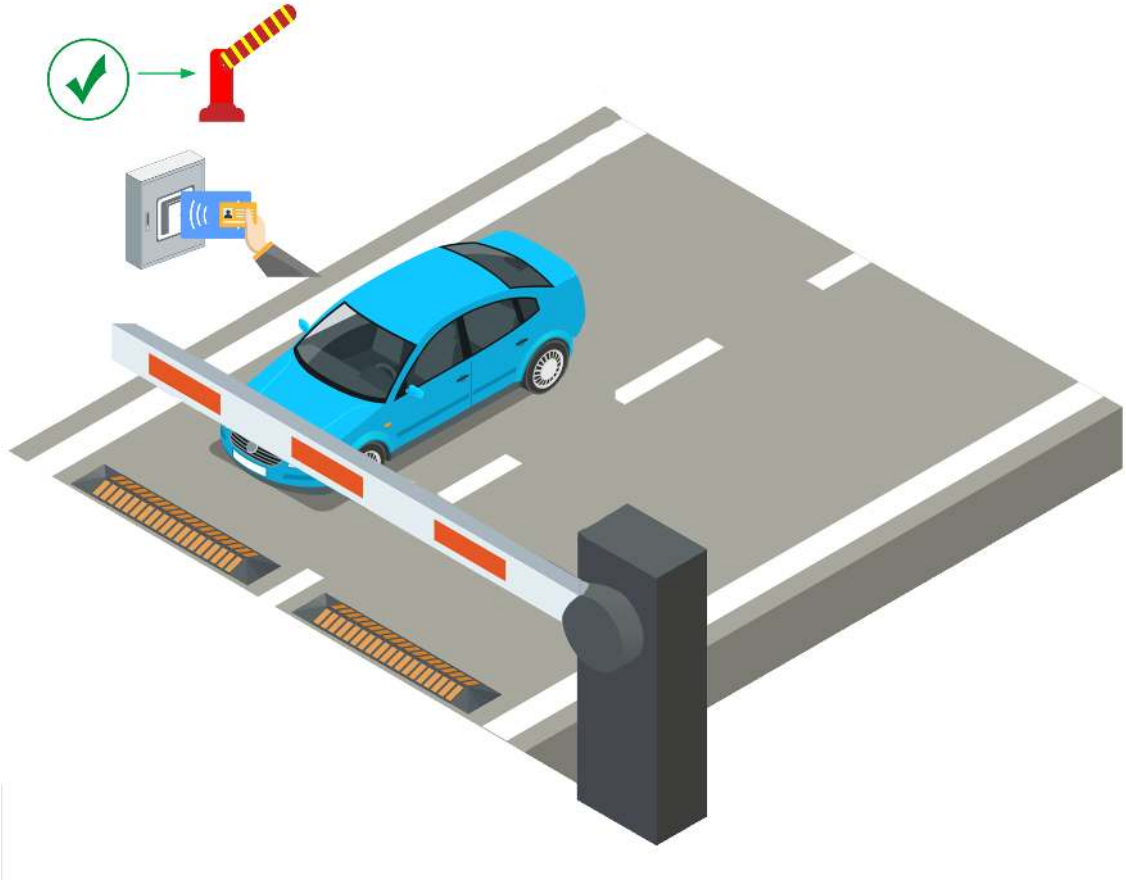


Figure 25-6 Opening Barrier by Card Swiping

Video Intercom Device

a. The vehicle owner calls the security guard by the video intercom device (some access control devices can also be used for video intercom).
b. The security guard verifies the owner's identity by viewing her/him by the video intercom device or the license plate number captured by a capture unit.
c. The security guard opens the barrier manually if the vehicle owner is authenticated.



Figure 25-7 Opening Barrier by Video Intercom

Display Screen

A display screen is used for displaying information such as the number of vacant parking spaces, vehicle expiration date. See ***Link Display Screen and Set Displayed Content*** for details.

4) In the Link Camera area, select camera(s) to be linked to the lane.

Note

- Make sure you have enabled picture storage for the camera. Otherwise, you cannot see the captured pictures. See ***Area Management*** for details about how to enable picture storage for a camera.
- Up to three different cameras can be linked to the lane.
- One camera can be linked to multiple lanes.
- You can view the pictures captured by the linked camera when viewing the vehicle-passing information.

5) Set the entry & exit rule for temporary vehicles, registered vehicles, and visitor vehicles, and vehicles in list. You can switch on **Same Rule as Parking lot** to use the rule for the parking lot, or switch it off to set a new rule.

Note

For how to configure entry & exit rules, refer to ***Configure Entry & Exit Rules*** .

6. Click **Add**.

25.1.5 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. See ***Add Display Screen*** for details about how to add a display screen.

1. On the top navigation bar, select → **Passing Management** → **Parking Lot** → **Parking Lot Management** .
2. Click **Settings** of an added parking lot to enter the configuration page.
3. Select an entrance or exit from the left list.
4. Select a display screen to link it to the parking lot and click **Display Screen Configuration** beside the name of the display screen to open the Screen Configuration pane.

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.

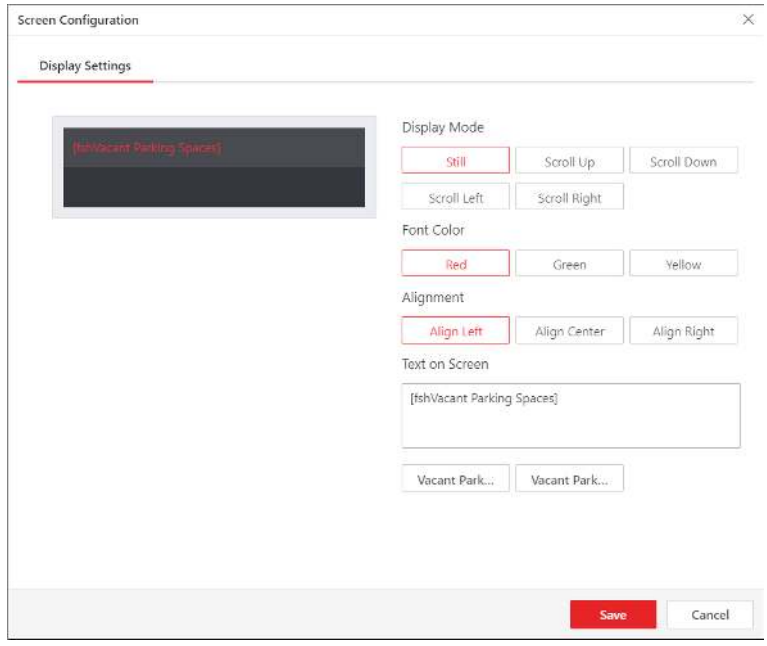


Figure 25-8 Configure the Entrance and Exit Display Screen Not Linked with a Lane

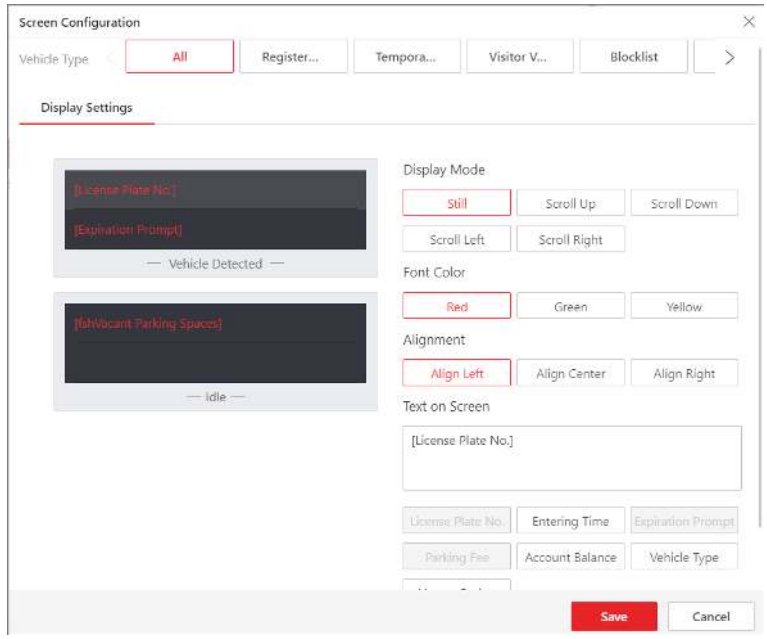


Figure 25-9 Configure the Entrance and Exit Display Screen Linked with a Lane

1. Select a vehicle type.

Note

Vehicle type is not configurable for the entrance and exit display screen not 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 Type

Display the vehicle type 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.

c. 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.

Note

The Vacant Parking Spaces in Vehicle List refers to 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.

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.

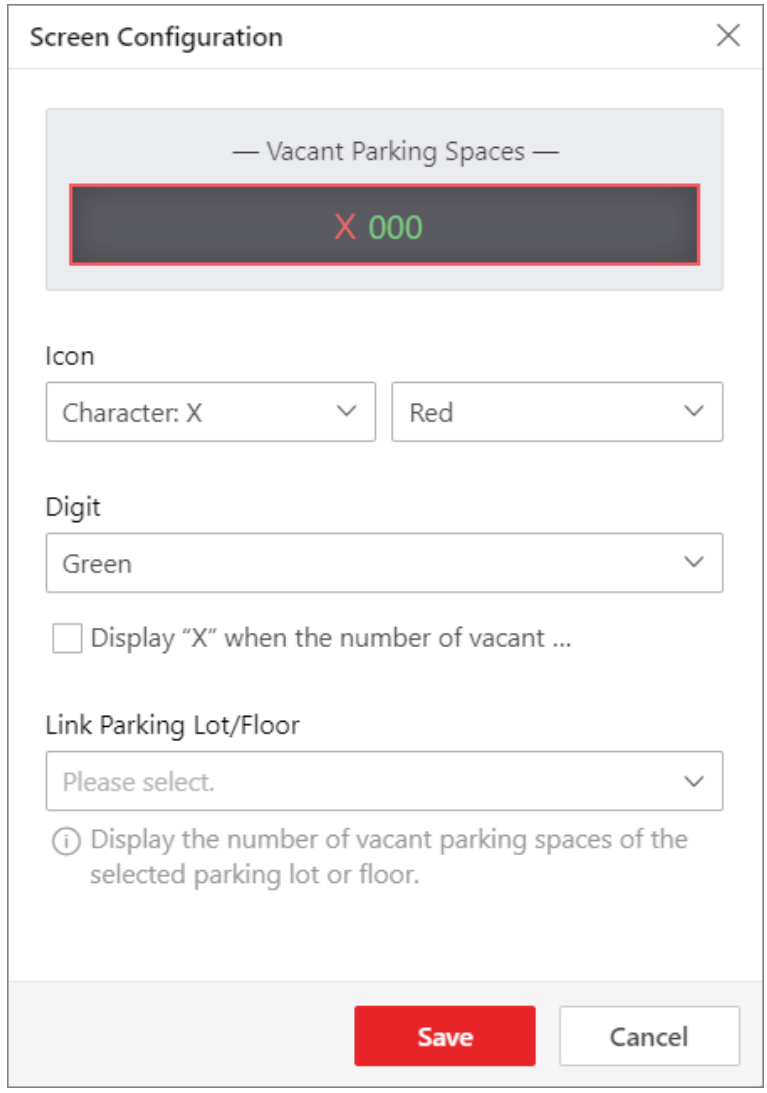


Figure 25-10 Configure Indoor Guidance Screen

1. Click a sub screen and select a icon type and color to be displayed.
2. Select a color for the digits displayed on the screen.

Note

If the current number of vacant parking spaces is 0, you can check the checkbox below the Digit field to display "X".

3. Select a parking lot or a floor to be linked with the indoor guidance screen.
4. 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.

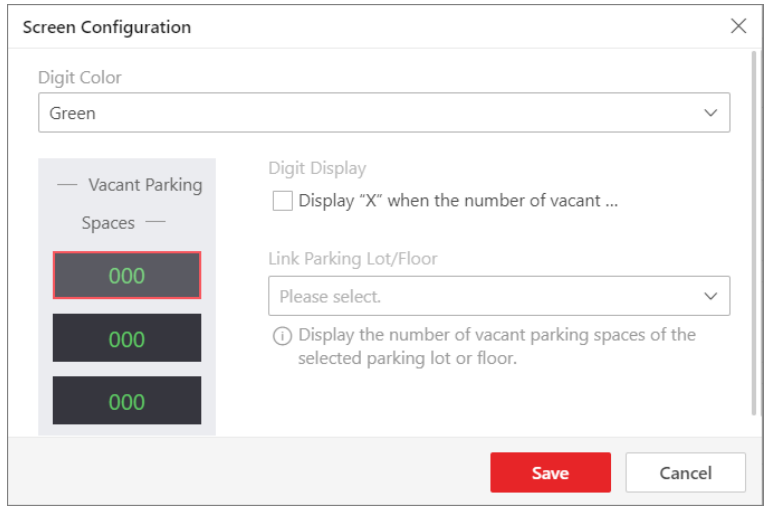


Figure 25-11 Configure Entrance Guidance Screen

1. Click a sub screen and select a color for the digits displayed on the screen.

   Note

   If the current number of vacant parking spaces is 0, you can check the checkbox below the Digit field to display "X".
2. Select a parking lot or a floor to be linked with the entrance guidance screen.
3. Click **Save**.

25.1.6 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 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 Entry & Exit Mode

You can set the entry & exit mode for a parking lot, which can help you manage the entry and exit of vehicles more easily.

Steps

1. On the top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Parking Lot Management**.
3. Click **Settings** to enter the settings page of a parking lot.
4. Click **Entry & Exit Rule**.
5. Click **Edit** beside **Entry & Exit Mode**.

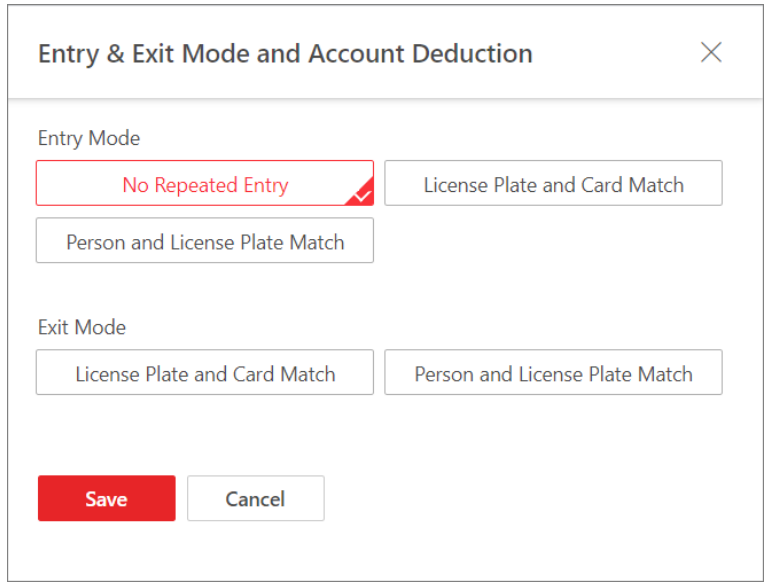


Figure 25-12 Set Entry & Exit Mode

6. Select the entry mode and exit mode accordingly.

   Entry Mode

   The condition in which a vehicle is allowed to enter.

   No Repeated Entry

   Repeated entry for an 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.

   Note

   The **License Plate and Card Match** mode and **Person and License Plate Match** mode cannot be selected at the same time.

   Exit Mode

   The condition in which a vehicle is allowed to exit.

7. 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 top navigation bar, select → **Passing Management** → **Parking Lot** → **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.

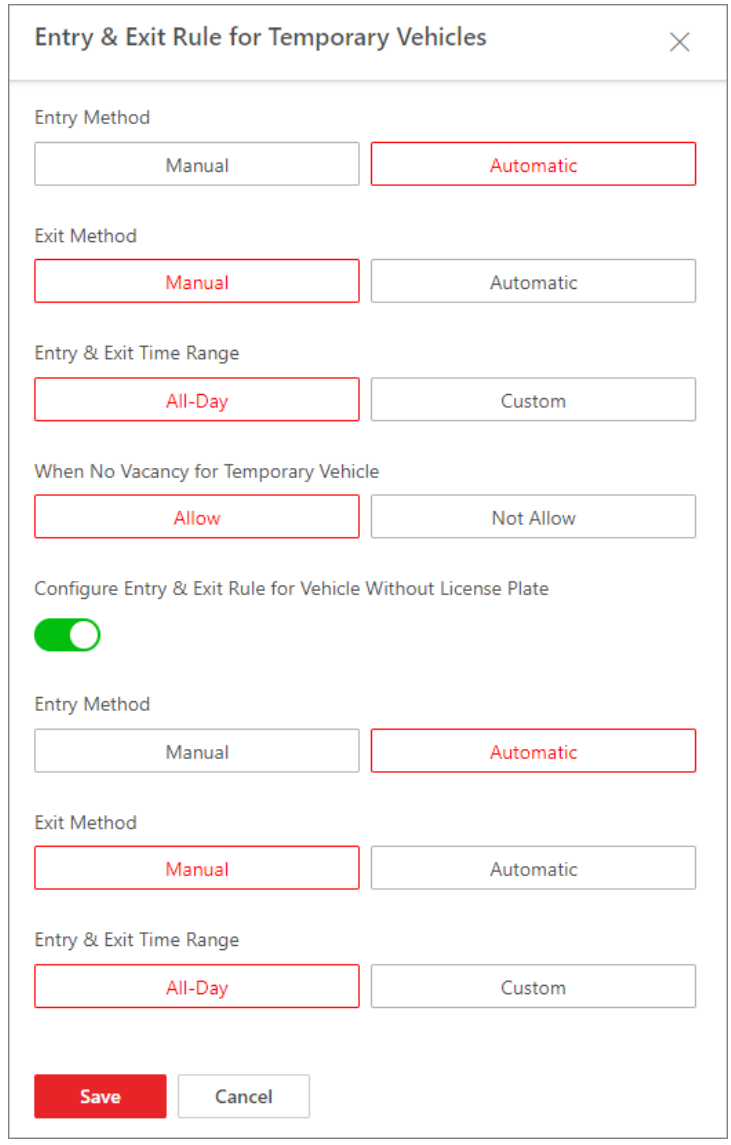


Figure 25-13 Entry & Exit Rule for Temporary Vehicles

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 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. See ***Add a Registered Vehicle*** or ***Batch Import Registered Vehicles*** for details.

Steps

1. On the top navigation bar, select → **Passing Management** → **Parking Lot** → **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.

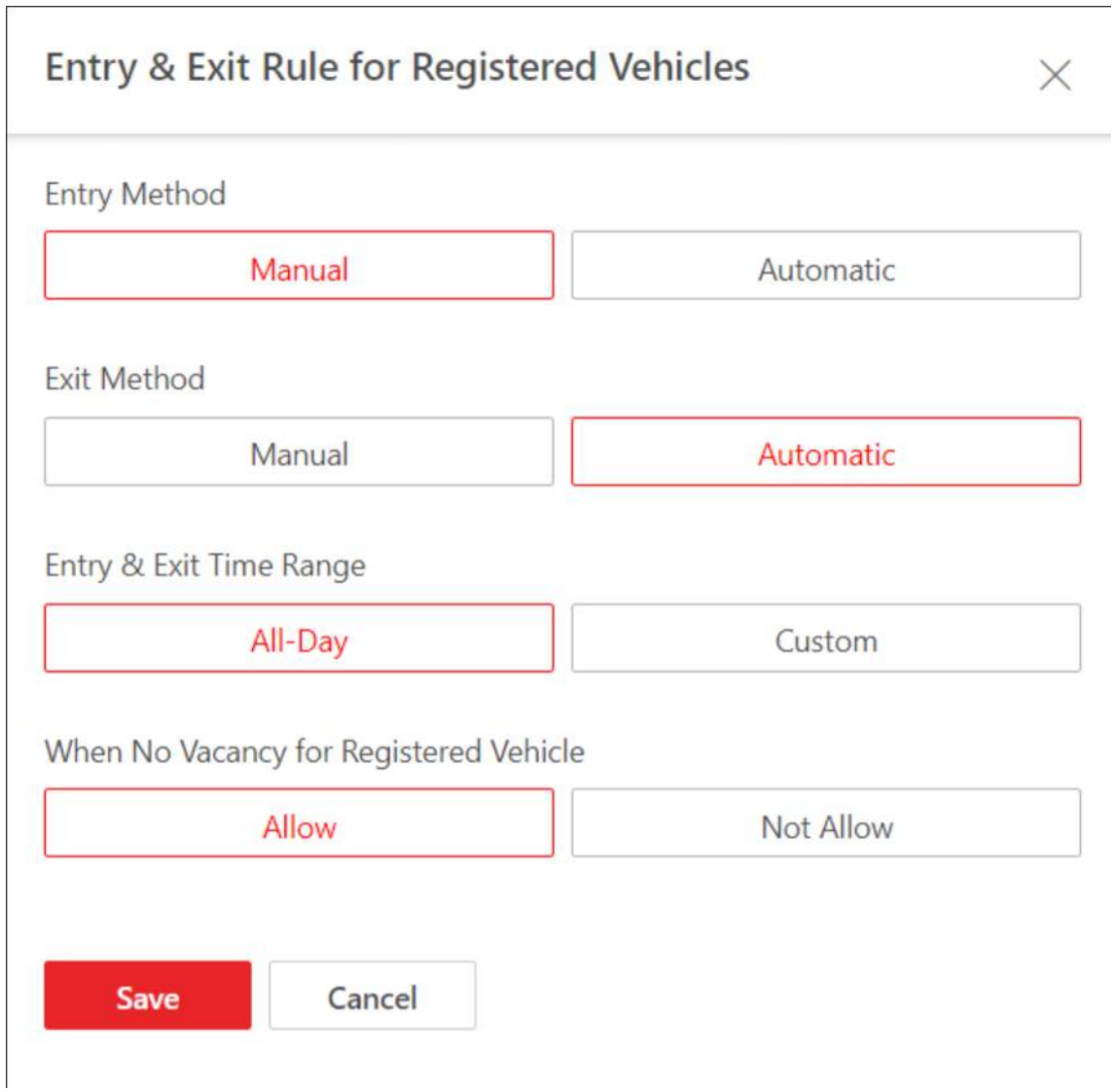


Figure 25-14 Entry & Exit Rule for Registered Vehicles

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 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**.

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 top navigation bar, select → **Passing Management** → **Parking Lot** → **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.

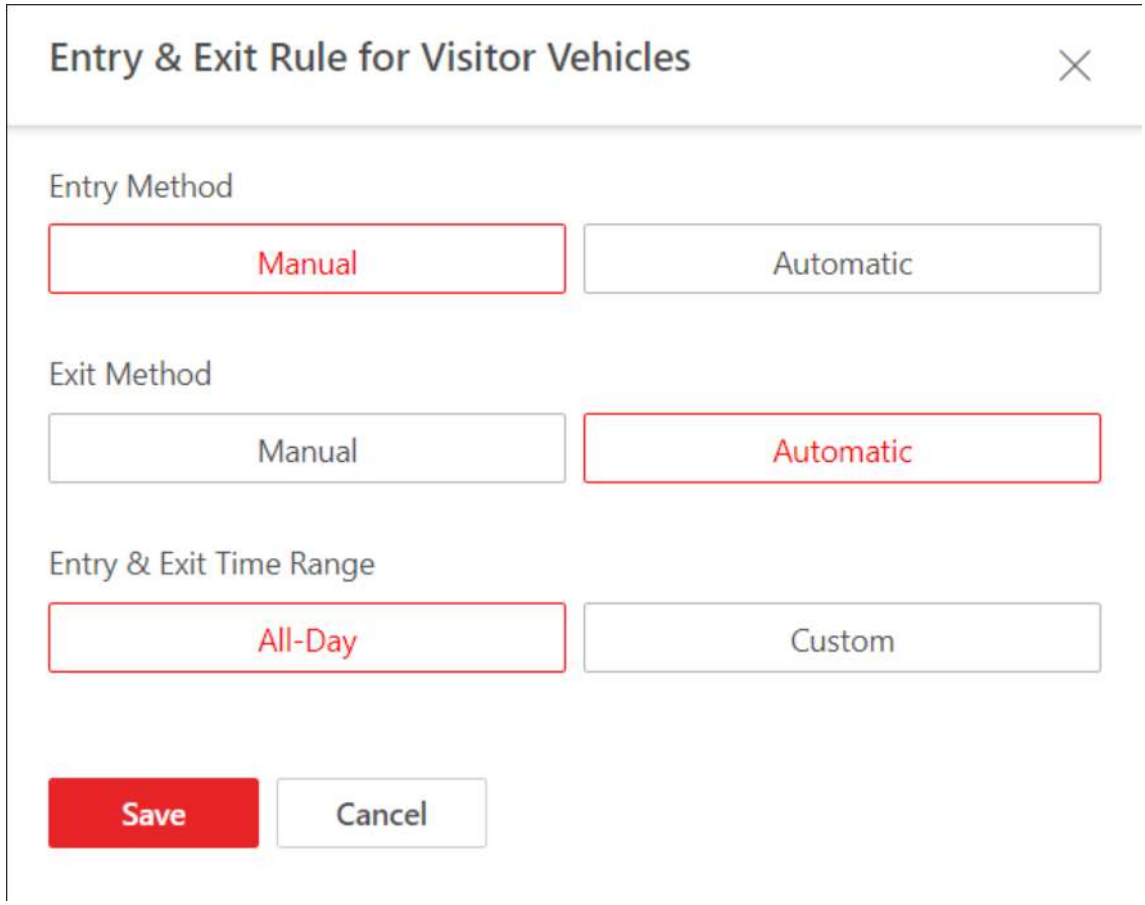


Figure 25-15 Entry & Exit Rule for Visitor Vehicles

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. See ***Manage Vehicle Lists*** for details.

Steps

1. On the top navigation bar, select → **Passing Management → Parking Lot → 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.

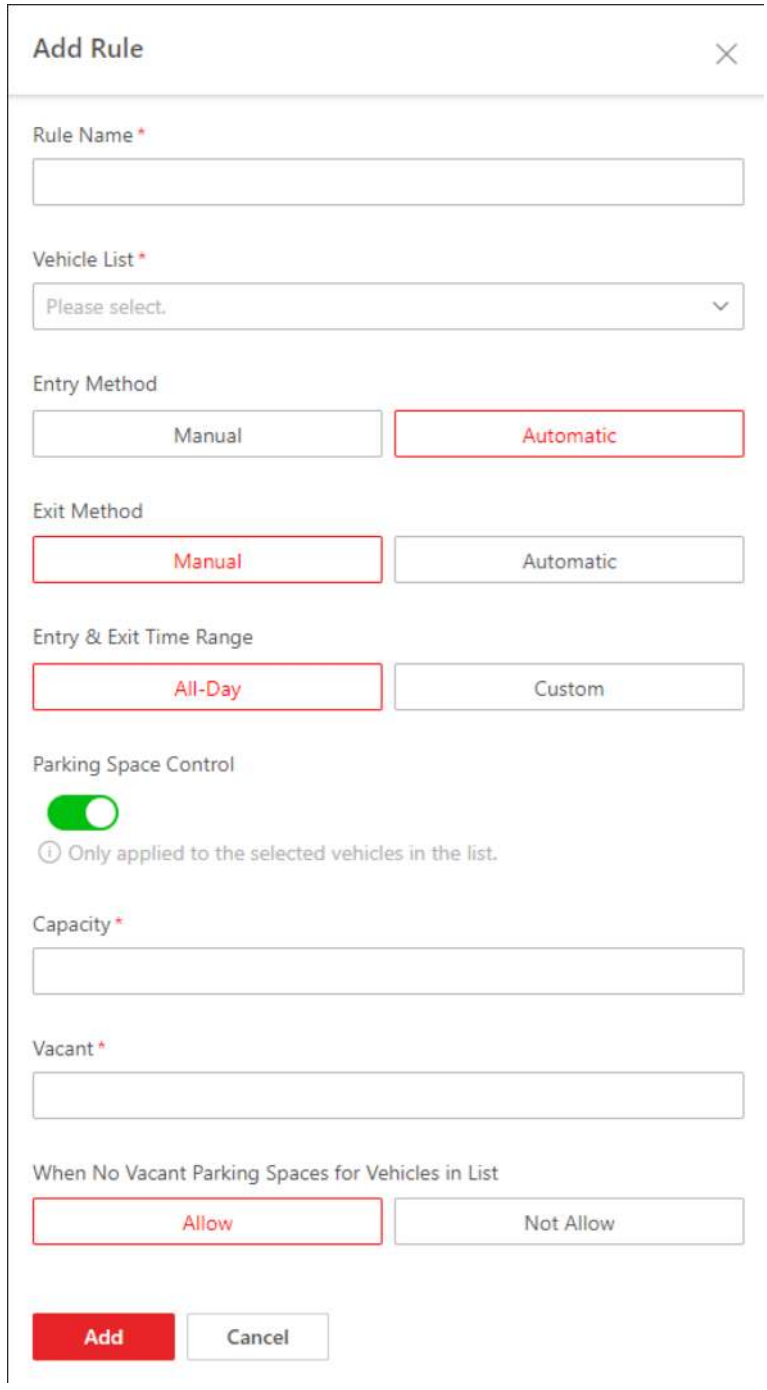


Figure 25-16 Add Rule

5. Set the rule.

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

Note

If you switch on **Parking Space Control**, you need to configure the following parameters.

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:** Perform the following operations if needed.

Edit a Rule	Click to edit a rule.
Delete a Rule	Click to delete a rule.

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 top navigation bar, select → **Passing Management** → **Parking Lot** → **Parking Lot Management** .
2. Click **Settings** to enter the settings page of a parking lot.
3. Click **Entry & Exit Rule**.
4. Click **Add** beside **Free Entry & Exit on Holidays** to open the Add Holiday pane.

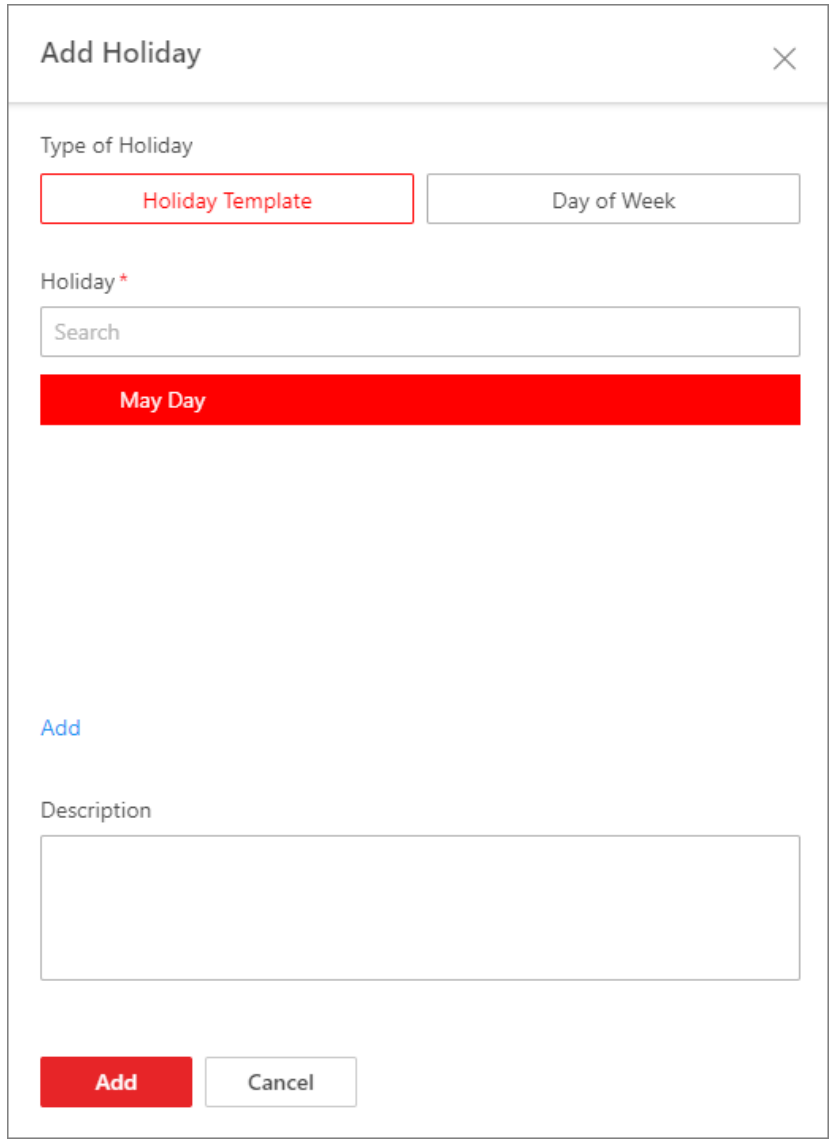


Figure 25-17 Holiday Template

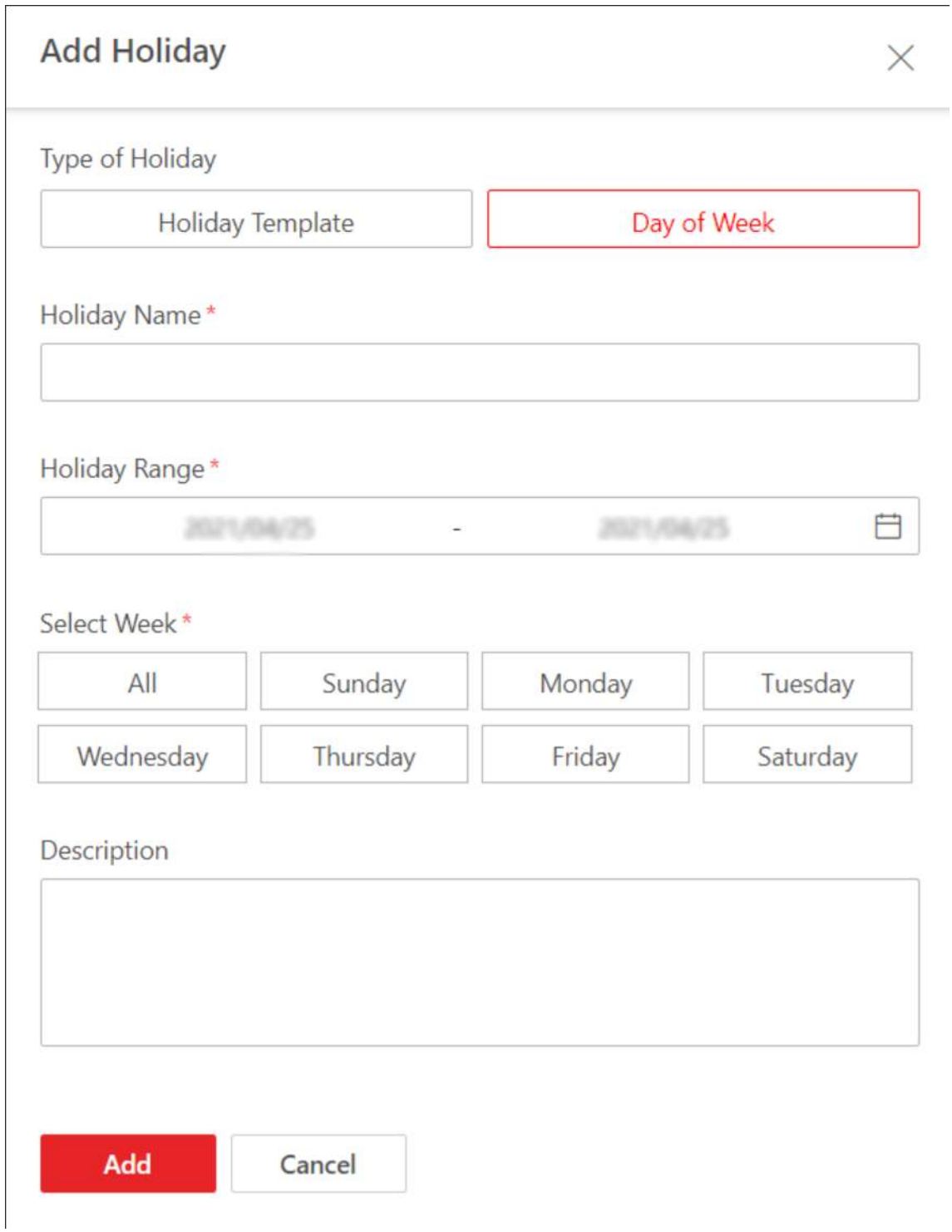


Figure 25-18 Day of Week

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.
b. (Optional) Enter remarks in the Description field if needed.
c. Click **Add**.

Day of Week
a. Create a name for the holiday.
b. Click to set a time range for the holiday.
c. Select the day(s) of a week that the rule is applied to.
d. (Optional) Enter remarks in the Description field if needed.
e. Click **Add**.

6. **Optional:** Perform the following operation(s) if needed.

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 top navigation bar, select → **Passing Management → Parking Lot → Basic Configuration → Call Recipient Settings** .

Click **Add** to select user(s) to receive entrance & exit calls on the Control Client.

25.1.7 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 top navigation bar, select → **Passing Management** → **Parking Lot** → **Basic Configuration** → **Parking Fee Mode** .

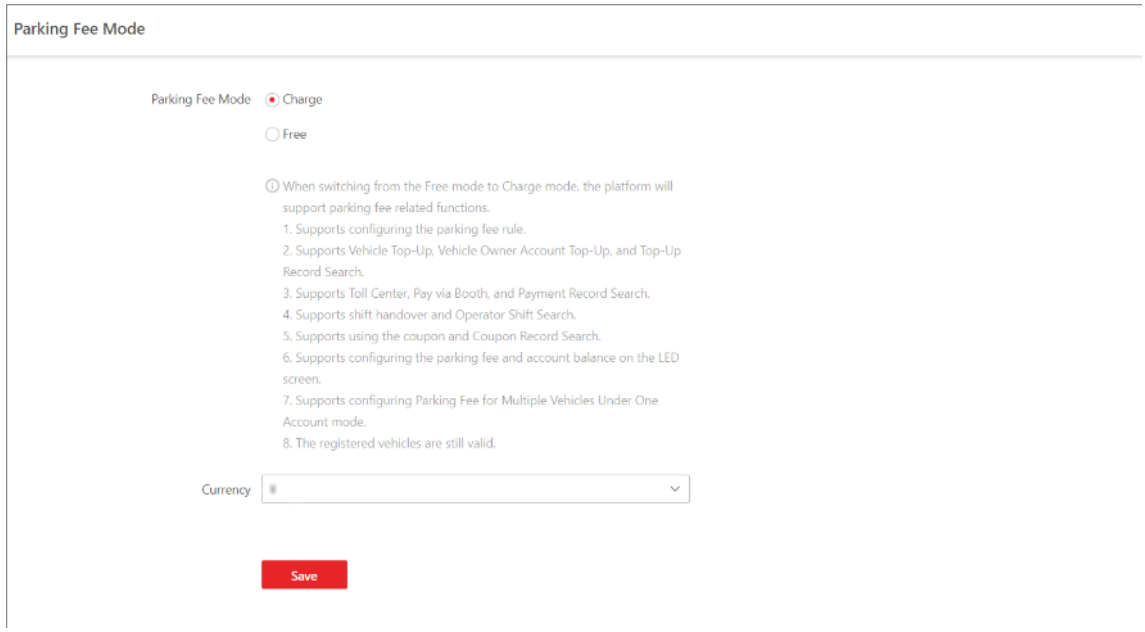


Figure 25-19 Parking Fee Mode Settings Page

2. Select **Charge** or **Free** as the parking fee mode.

Note

If you select **Free**, the settings related to parking fee will not be able to configure.

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 top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Parking Lot Management**.

3. Click **Settings** to enter the settings page of a parking lot.
4. Click **Entry & Exit Rule**.
5. Click **Edit** beside **Entry & Exit Mode and Account Deduction**.

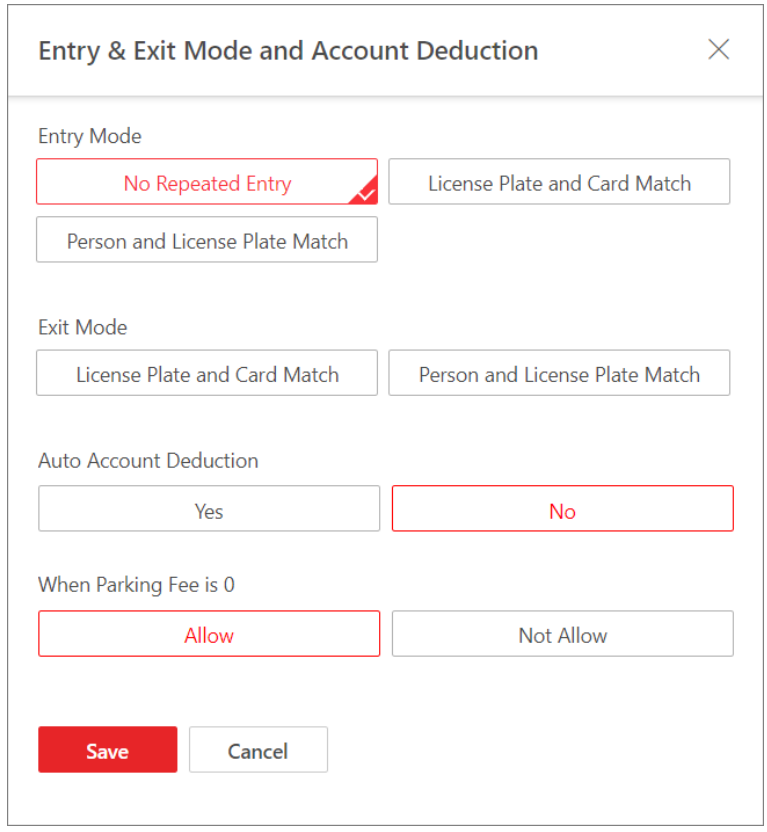


Figure 25-20 Entry & Exit Mode and Account Deduction

6. Set the modes.

Entry/Exit Mode

The condition in which a vehicle is allowed to enter/exit the parking lot. Refer to ***Set Entry & Exit 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.

7. 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 top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Parking Lot Management**.
3. Click **Settings** to enter the settings page of a parking lot.
4. Click **Parking Fee Rule**.
5. Click **Add** beside **Parking Fee Rule for Temporary Vehicles** to enter the Add Parking Fee Rule pane.

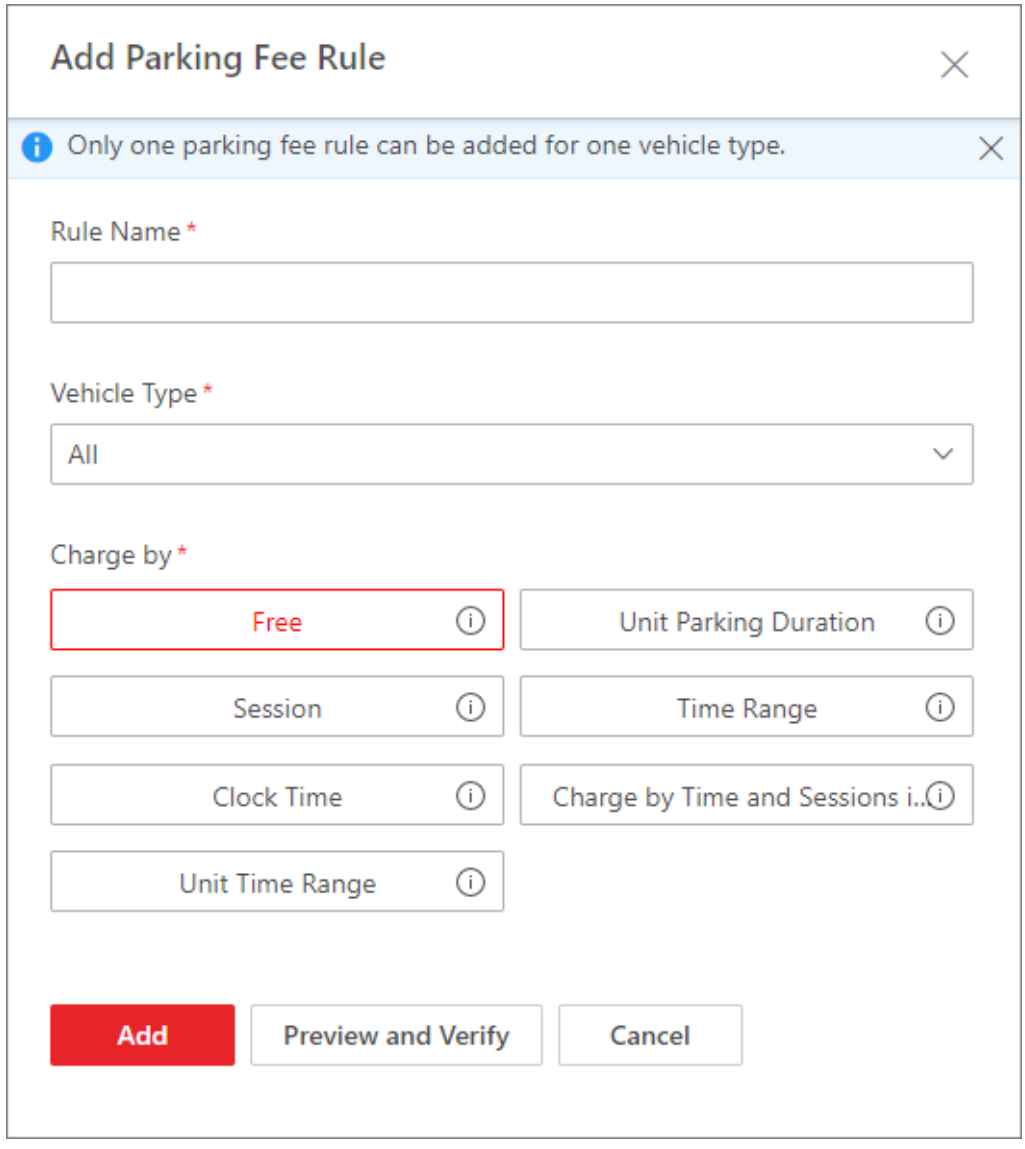


Figure 25-21 Add Parking Fee Rule for Temporary Vehicles

6. Create a name for the rule.
7. Select the type of vehicle to which the rule applies.

Note

No more than one rule can be added for each vehicle type.

8. 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
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.

and Nighttime

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.

9. **Optional:** Click **Preview and Verify** to preview and verify the rule.
10. 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).

11. **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 top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Parking Lot Management**.
3. Click **Settings** to enter the settings page of a parking lot.
4. Click **Parking Fee Rule**.
5. Click **Add** beside **Parking Fee Rule for Registered Vehicle** to enter the Add Parking Pass Rule pane.

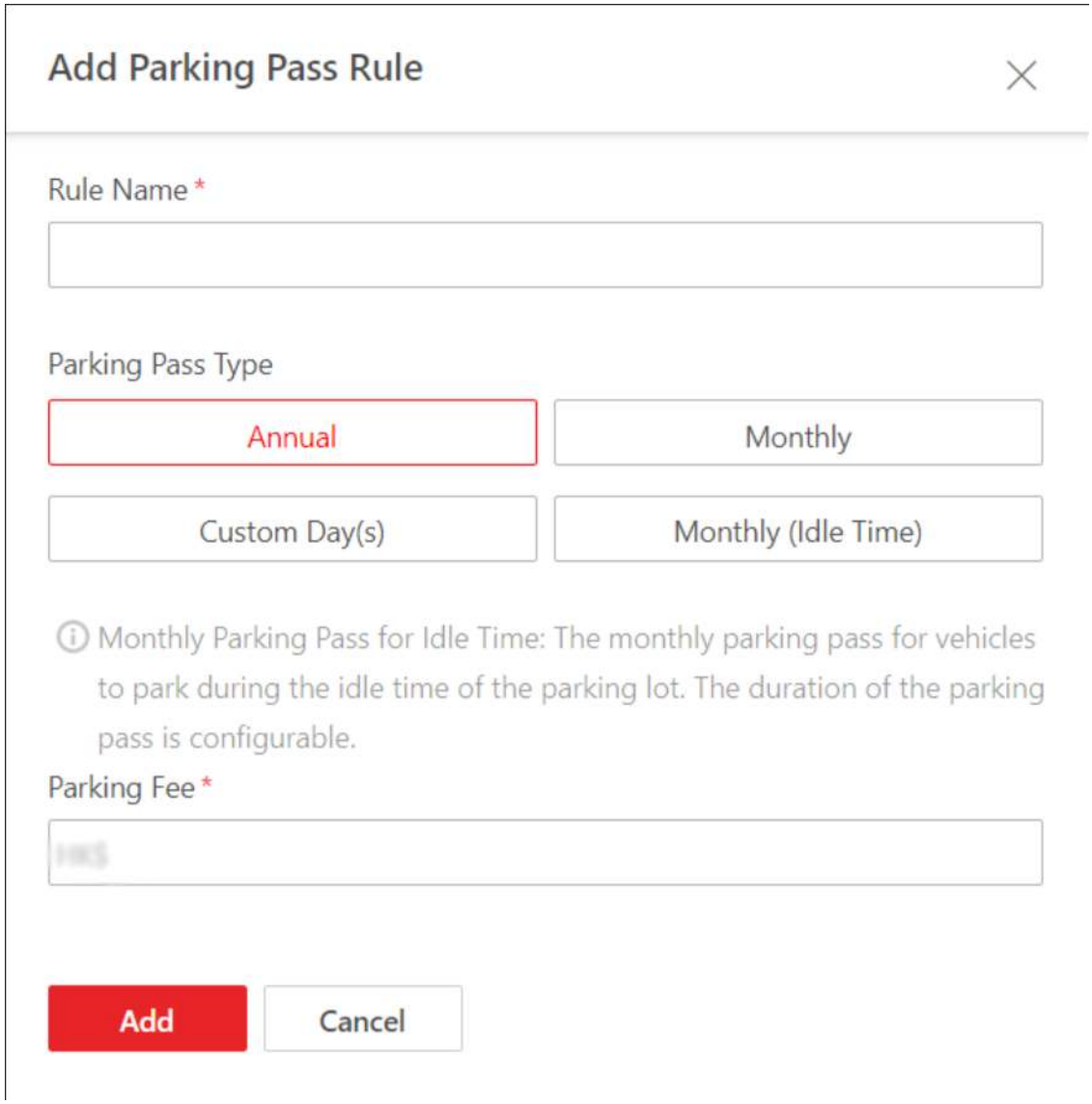


Figure 25-22 Add Parking Pass Rule Pane

6. Create a name for the rule.
7. 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 (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.

8. Click **Add**.

Note

Vehicle owners can top up their parking passes as needed. Refer to ***Top Up Parking Pass*** for details.

9. **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. See ***Manage Vehicle Lists*** for details.

Steps

1. On the top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Parking Lot Management**.
3. Click **Settings** to enter the settings page of a parking lot.
4. Click **Parking Fee Rule**.
5. Click **Add** beside **Parking Fee Rule for Vehicles in List** to enter the Add Parking Fee Rule pane.
6. Create a name for the rule.
7. Select a vehicle list from the drop-down list.

Note

No more than one rule can be added for each vehicle list.

8. 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.

9. **Optional:** Click **Preview and Verify** to preview and verify the rule.
10. 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).

11. **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**.

Steps

1. On the top navigation bar, select → **Passing Management** → **Parking Lot** → **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

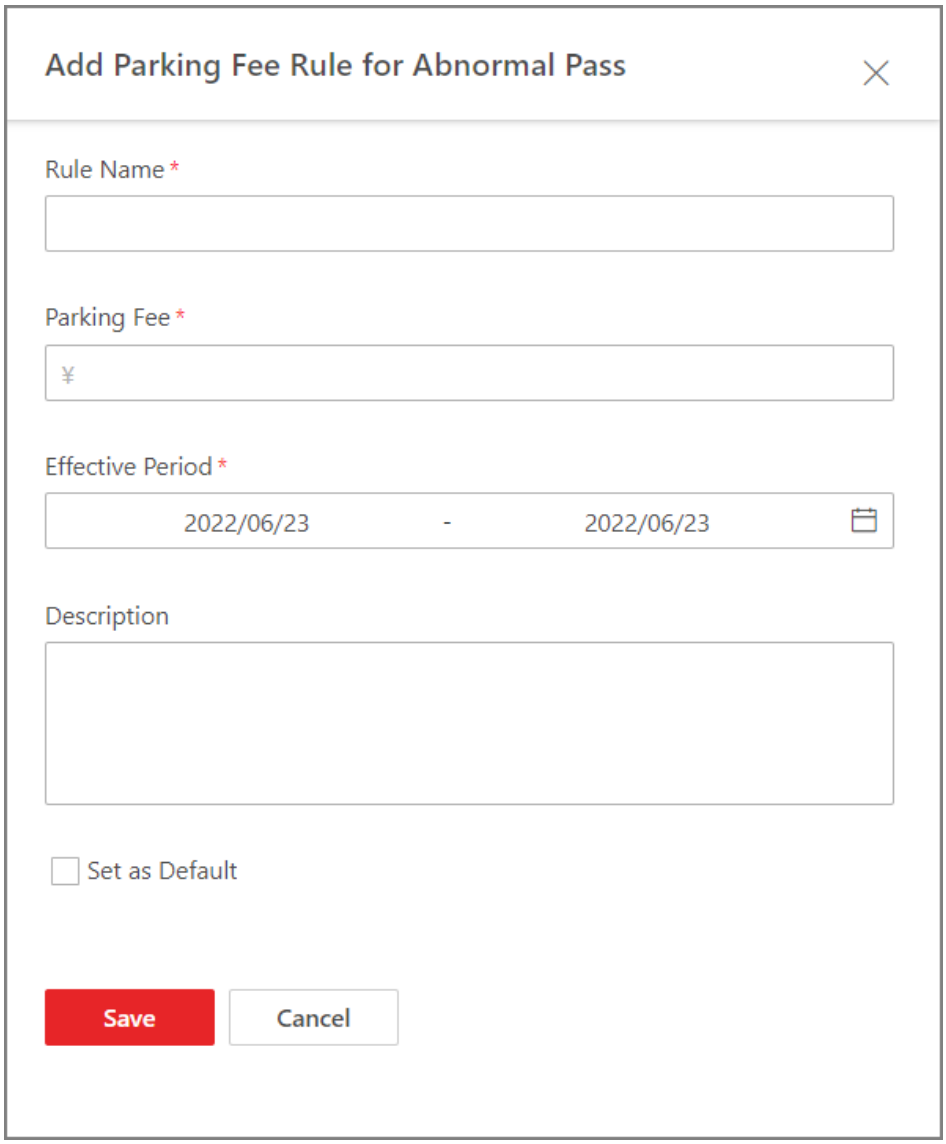
You can add parking fee rule for abnormal pass (e.g., a vehicle with an entry record but without an exit record), which can help you manage abnormal entries and exits more easily.

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 top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Parking Lot Management**.
3. Click **Settings** to enter the settings page of a parking lot.
4. Click **Parking Fee Rule**.
5. Click **Add** beside **Parking Fee Rule for Abnormal Pass**.



6. Create a name for the rule.
7. Enter the parking fee for abnormal pass.
8. Set a validity period for the rule.
9. **Optional:** Enter remarks in the Description field as needed.
10. **Optional:** Check **Set as Default** to set the rule as the default rule for abnormal entry & exit.
11. 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.

12. **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.

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**.

Steps
1. On the top navigation bar, select → **Passing Management** → **Parking Lot** → **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 enter the Additional Configuration pane.

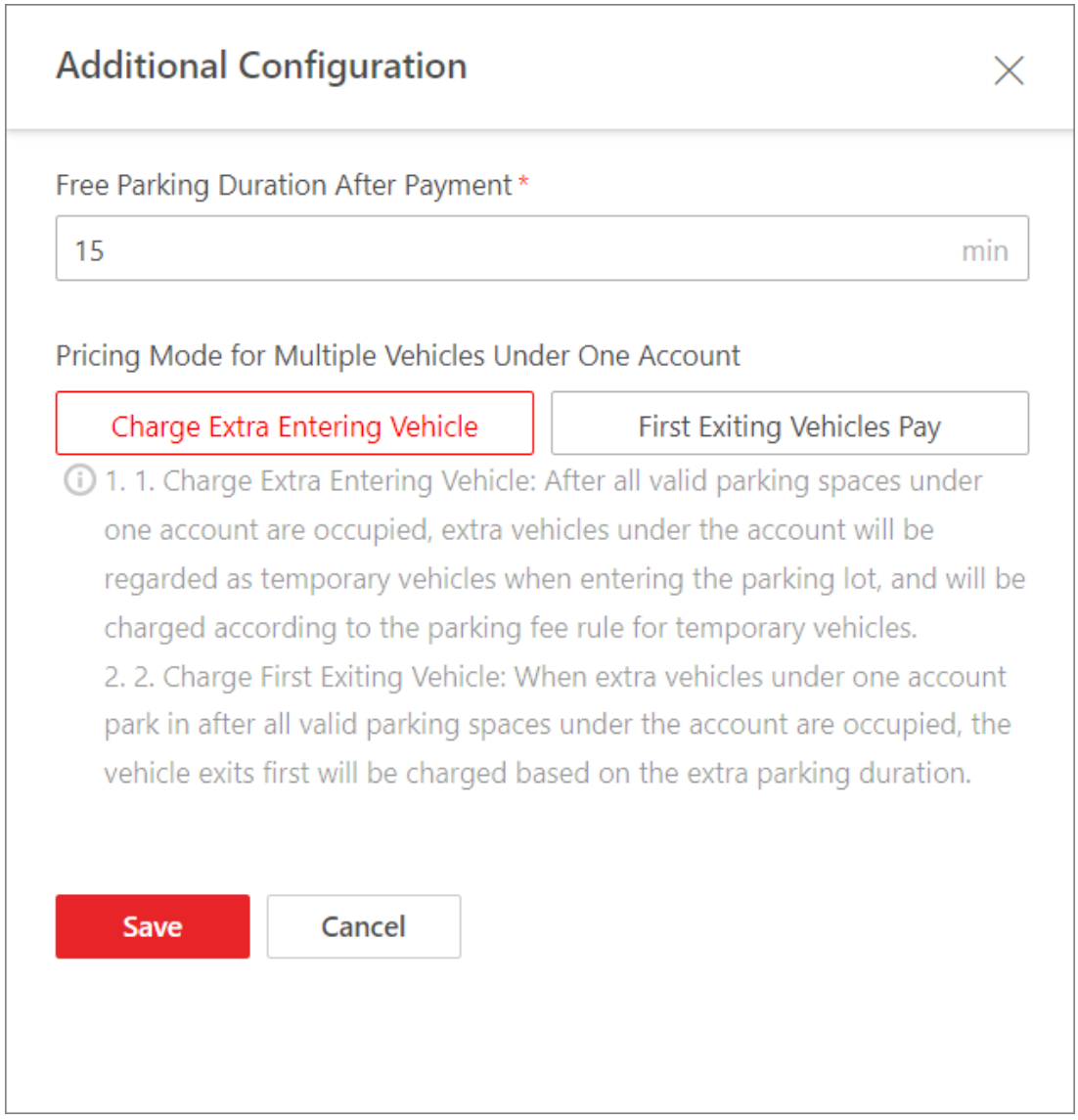


Figure 25-24 Additional Configuration

5. Enter the parking duration that is free of charge after paying the parking fee.
6. **Optional:** Switch on **Parking Fee Rule for Multiple Vehicles Under One Account**, and select **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. 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 top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Temporary Card**.

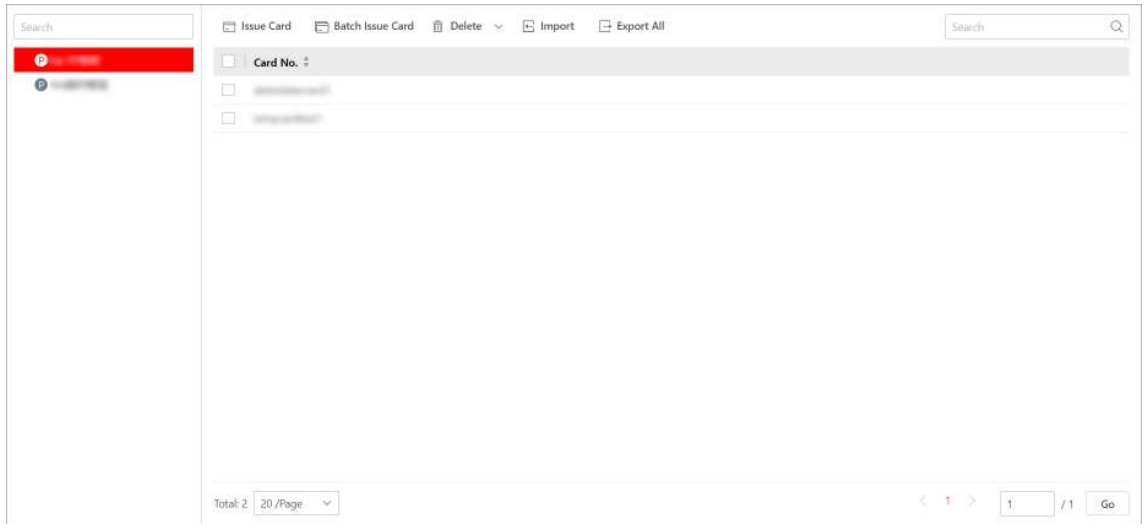


Figure 25-25 Issue Temporary Card Page

3. Select a parking lot from the left list.
4. Click **Issue Card**.

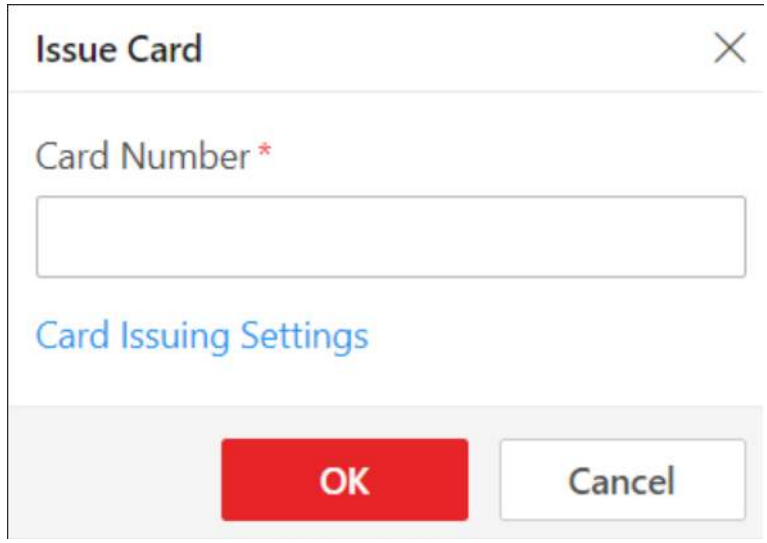


Figure 25-26 Issue Card Window

5. Enter the card number.
6. **Optional:** Click **Card Issuing Settings** to set card issuing parameters. See ***Set Card Issuing Parameters*** for more details.
7. Click **OK**.

   The card will be added to the selected parking lot.
8. **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**. **Note** • You can click **Download Template** and save the predefined template (in XLSX format) to the local PC. • 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.

25.2 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 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.

25.2.1 Top Up Parking Pass

A parking pass costs a certain amount of money and is valid for a specific time period. If a vehicle is topped up with a parking pass, it can enter and exit a specific parking lot as a registered vehicle and park in that parking lot without paying any fees. You can top up parking passes for one or multiple vehicles at the same time via Top-Up Management.

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 top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Top-Up Management**.
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.

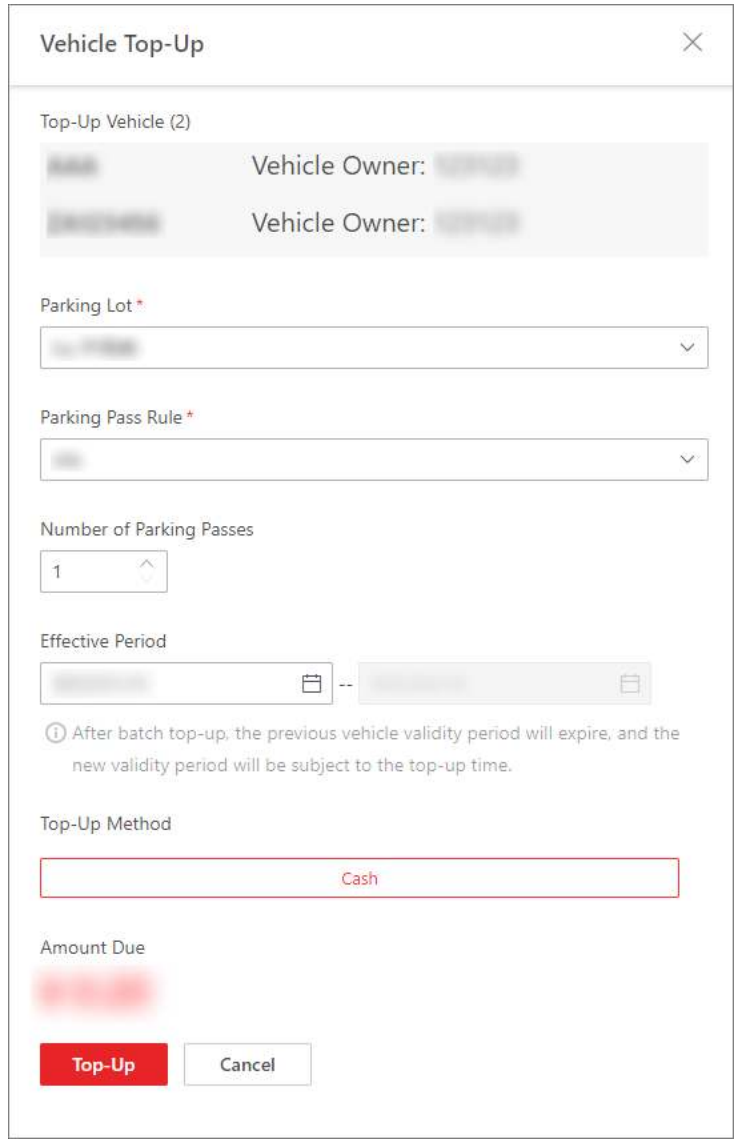


Figure 25-27 Vehicle Top-Up Pane

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.

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**.

25.2.2 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 top navigation bar, select → **Passing Management** → **Parking Lot** .
2. On the left navigation pane, click **Toll Center**.

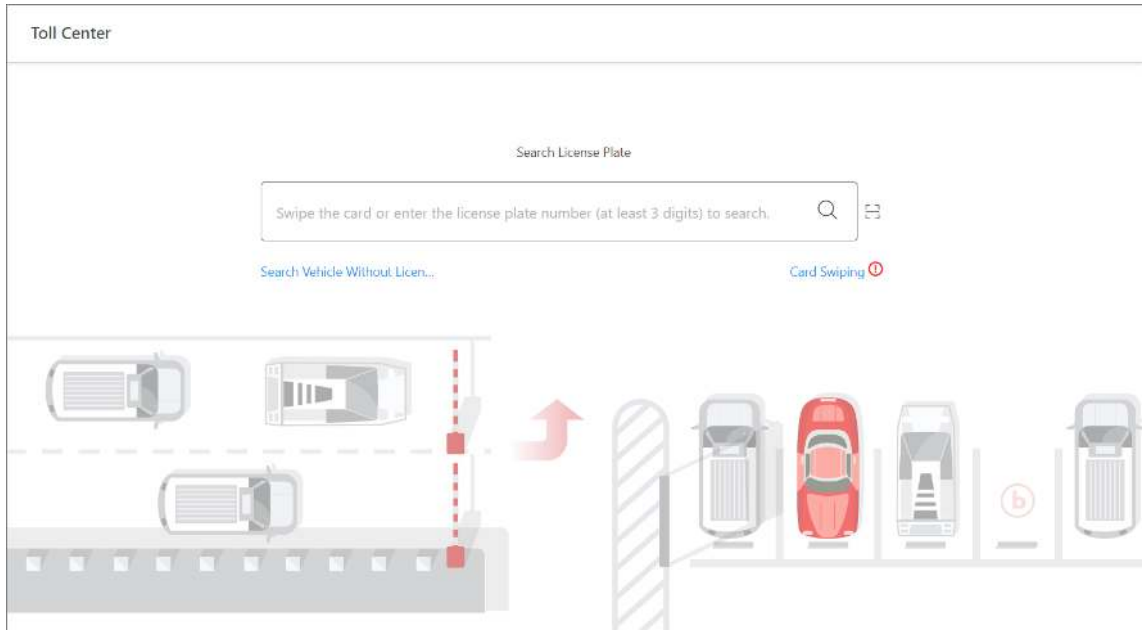


Figure 25-28 Toll Center Page

3. Search for a specific vehicle to get its parking information.

- Search by license plate number: Enter at least three digits of a license plate number to search for the vehicle.
- Search by 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).
- 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** to switch on/off the card encryption and turn on/off the audio.
- Scan parking receipt: Click next to the search box. After scanning the code on a parking receipt, the parking details will be displayed for the vehicle.

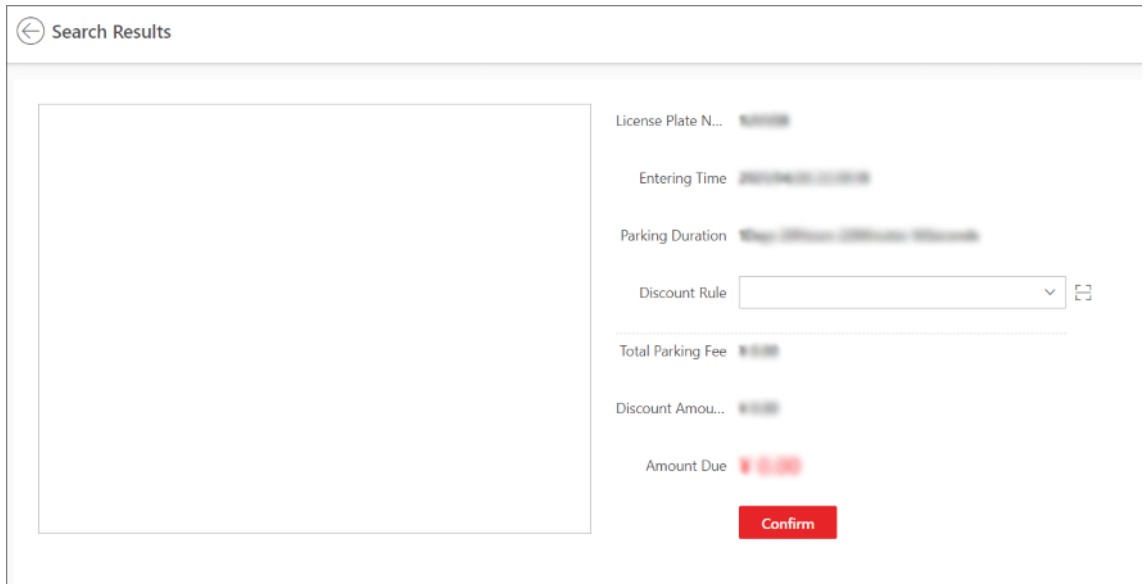


Figure 25-29 Search Result Page

4. **Optional:** Set the discount rule on the Search Results pane.
   - Select a coupon from the drop-down list.
   - Click to add a coupon.
5. Check the information and click **Confirm**.
6. **Optional:** On the pop-up window, click **Print Receipt** to print the receipt or save the receipt to the local PC in PDF format.

25.3 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 top navigation bar, select → **Passing Management → Parking Lot → Parking Guidance Configuration** , and then select a parking lot to enter the corresponding configuration page.

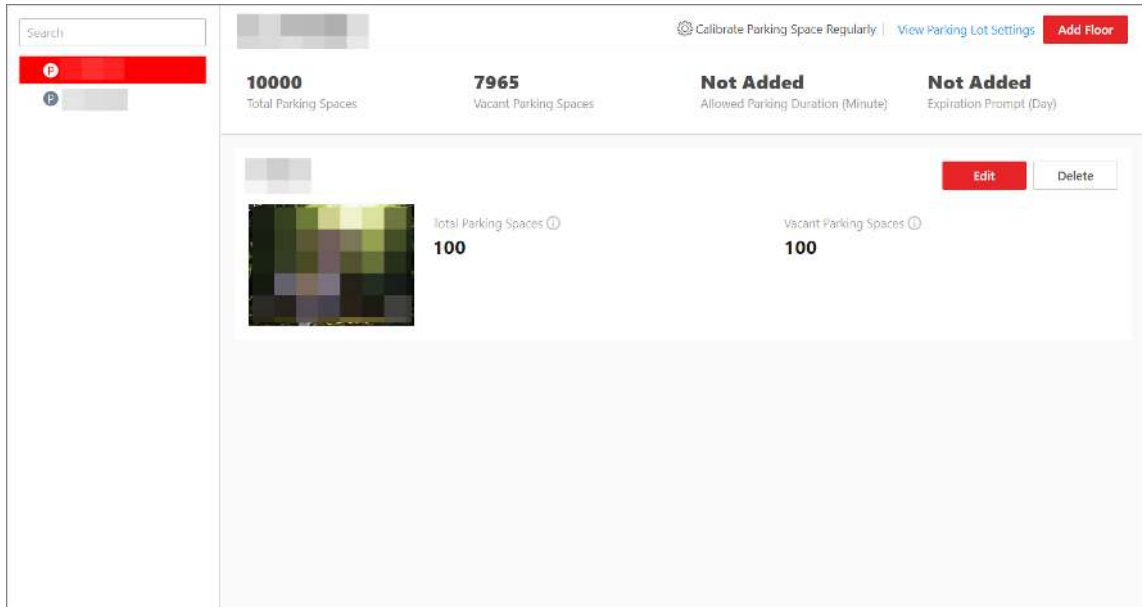


Figure 25-30 Parking Guidance Configuration Page

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***

25.3.1 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**.

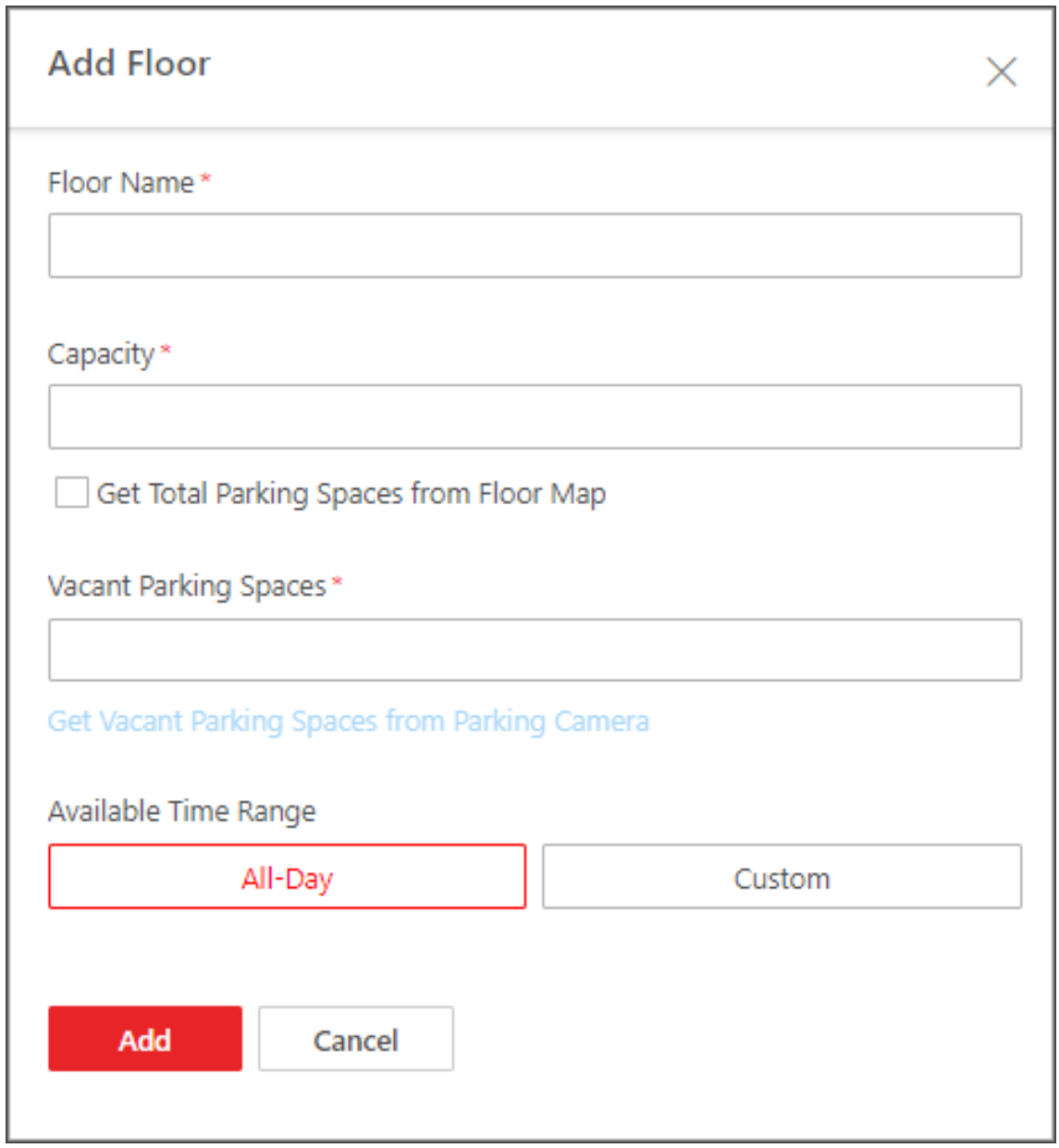


Figure 25-31 Add Floor Pane

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.

25.3.2 (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 which will be used to count the number of vacant and occupied parking spaces.

Steps

1. Enter the following page after adding a floor.

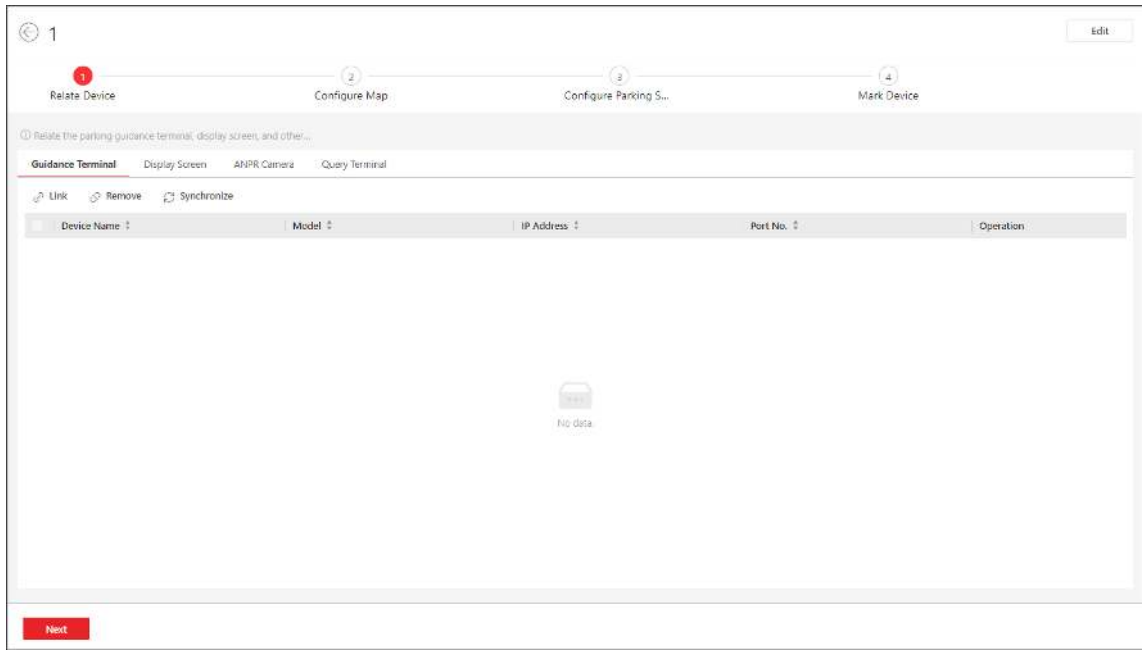


Figure 25-32 Link Device

2. Click **Link 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 the 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.

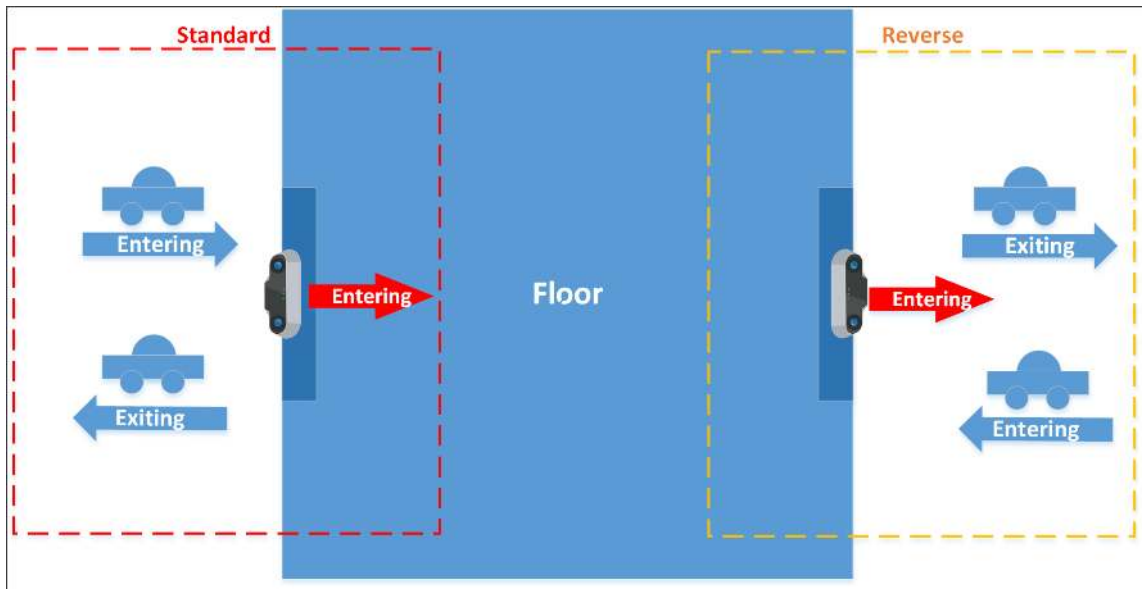


Figure 25-33 Schematic Diagram of Calculation Mode

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.

25.3.3 (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.

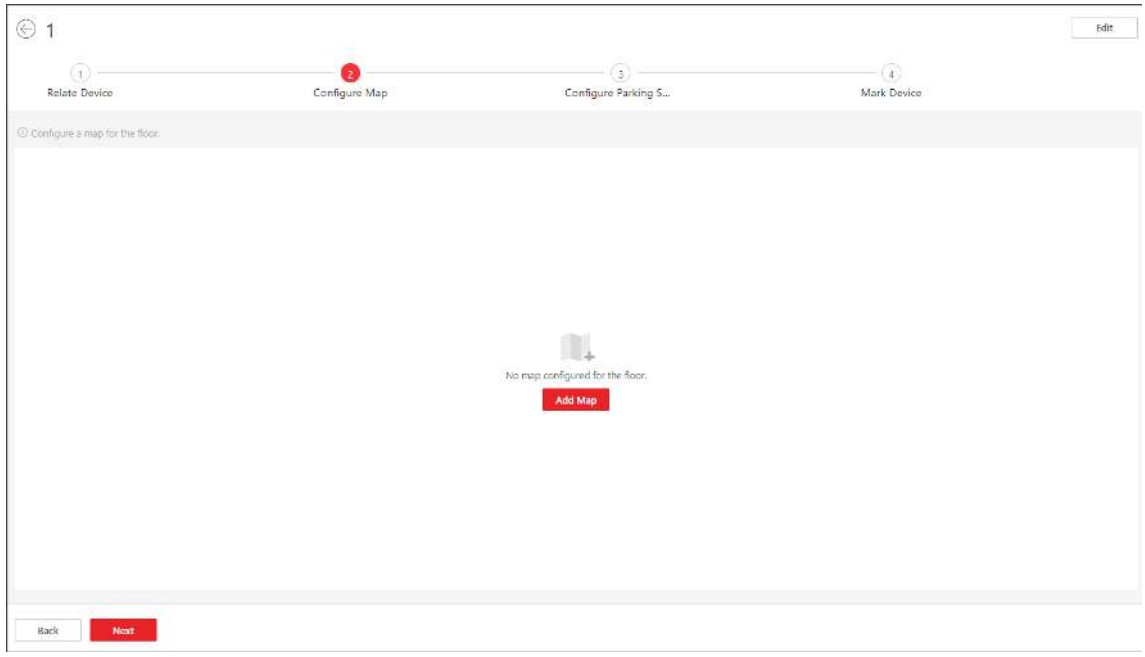


Figure 25-34 Add a Map

2. Click **Add Map**.
3. Select a map from your PC and add it to the floor.

Note

You can click + or − to adjust the size of the map.

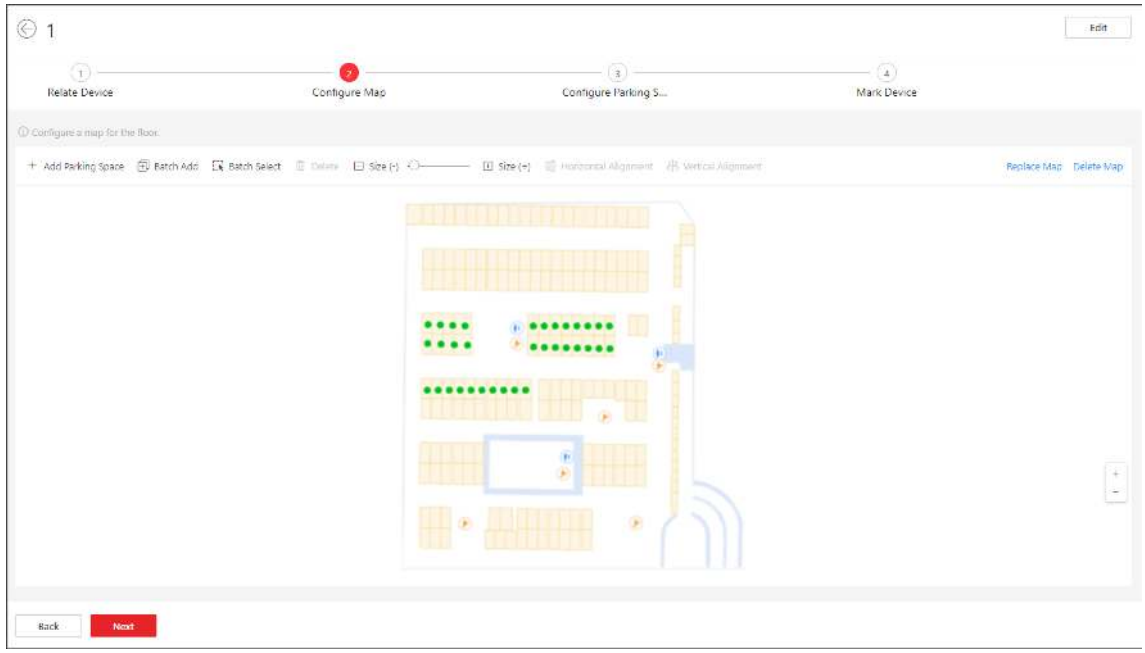


Figure 25-35 Configure the Map

4. Add parking space(s).
   - Add parking spaces one by one.
     a. Click **Add Parking Space** 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 **Batch Add**.
     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**.
5. **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 **Delete** to delete it. • Click **Batch Select**, drag you cursor to select multiple parking spaces, and click **Delete** to batch delete them.

Adjust the Size of the View of Parking Space(s)	• Click one parking space and click **Size (+)** or **Size (-)** to make it bigger or smaller. • Click **Batch Select**, drag you cursor to select multiple parking spaces, and click **Size (+)** or **Size (-)** to make them bigger or smaller.
Align Parking Spaces Horizontally	Click **Batch Select**, drag you cursor to select multiple parking spaces, and click **Horizontal Alignment** to align them in a horizontal line.
Align Parking Spaces Vertically	Click **Batch Select**, drag you cursor to select multiple parking spaces, and click **Vertical Alignment** to align them in a vertical line.
Replace Map	Click **Replace Map** to change the map.
Delete Map	Click **Delete Map** to delete the map.

6. **Optional:** Click **Back** to edit former configuration.

What to do next

Click **Next** to set types for parking spaces on the map. See ***Set Types for Parking Spaces on the Map*** .

25.3.4 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.

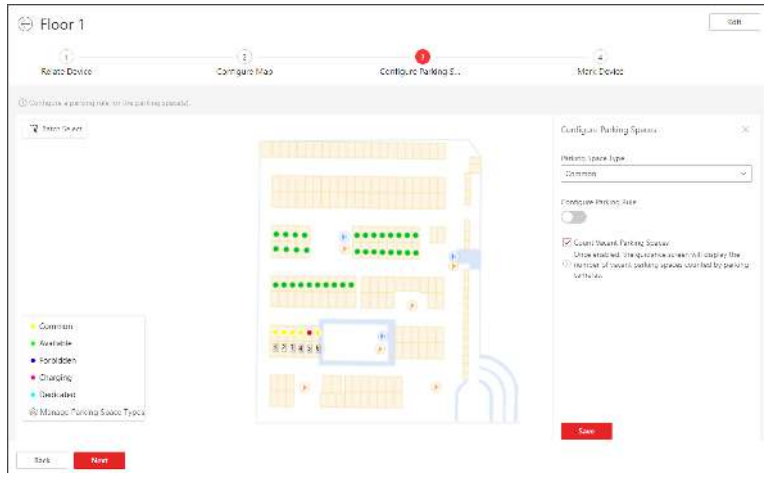


Figure 25-36 Set Types for Parking Spaces

2. Click a parking space to open the Configure Parking Spaces pane.

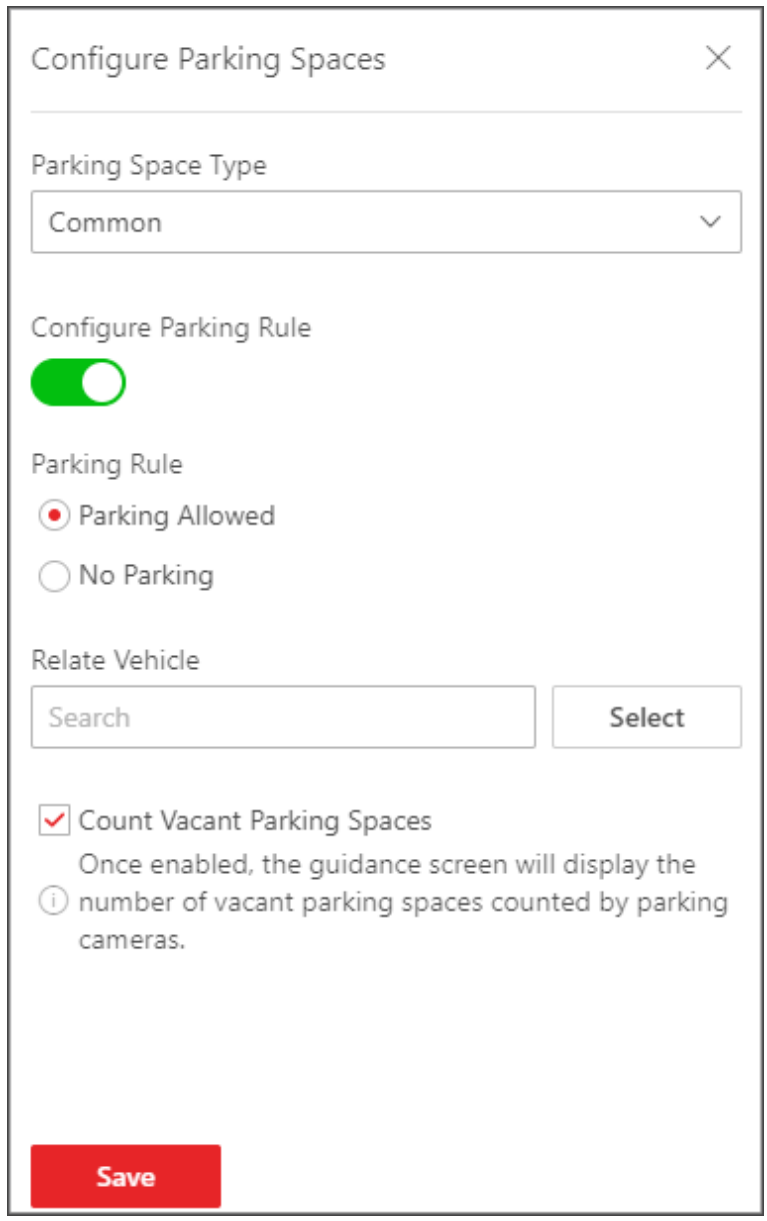


Figure 25-37 Configure Parking Spaces Pane

3. Select a type for the parking space from the drop-down list.
4. Switch on **Configure Parking Rule** to check **Parking Allowed** or **No Parking**.
5. Link vehicle(s) or vehicle list(s) to the parking space.
6. **Optional:** Check **Count Vacant Parking Spaces** to display the number of vacant parking spaces on the guidance screen.
7. **Optional:** Click **Manage Parking Space Types** and perform the following operations if needed.

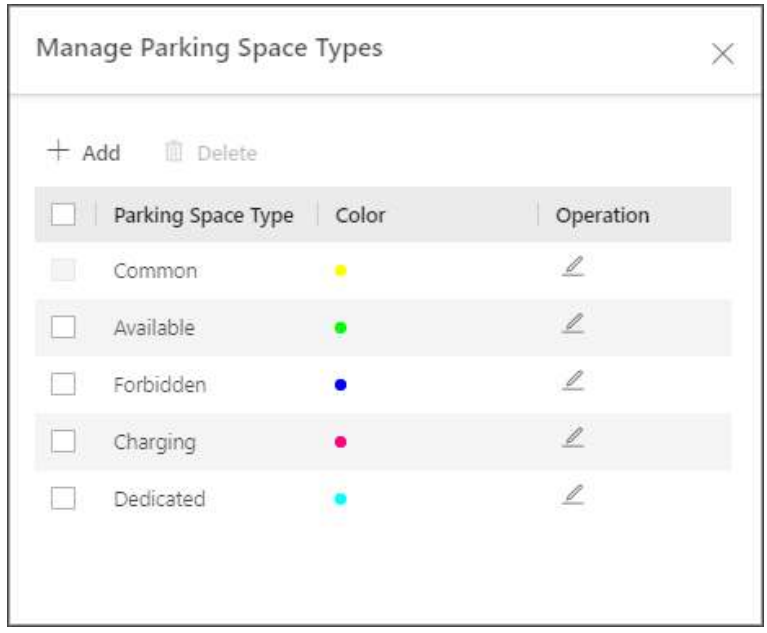


Figure 25-38 Manage Parking Space Types

Add a Parking Space Type

a. Click **Add**.
b. Create a name for the type.
c. Set a color for the type.

Note

The color will be applied to the indicator light of the parking cameras monitoring this type of parking spaces.

d. 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.

8. Click **Next**.

9. Optional: Click **Back** to edit former configuration.

What to do next

Click **Next** to mark device(s) on the map. See ***Mark Devices on the Map*** .

25.3.5 Mark Devices on the Map

You can link guidance screens to parking spaces at a specific direction in the parking lot. Once linked, the guidance screen can display the number of vacant parking spaces and guide vehicles to them.

Steps

1. Enter the following page after configuring the parking space type.

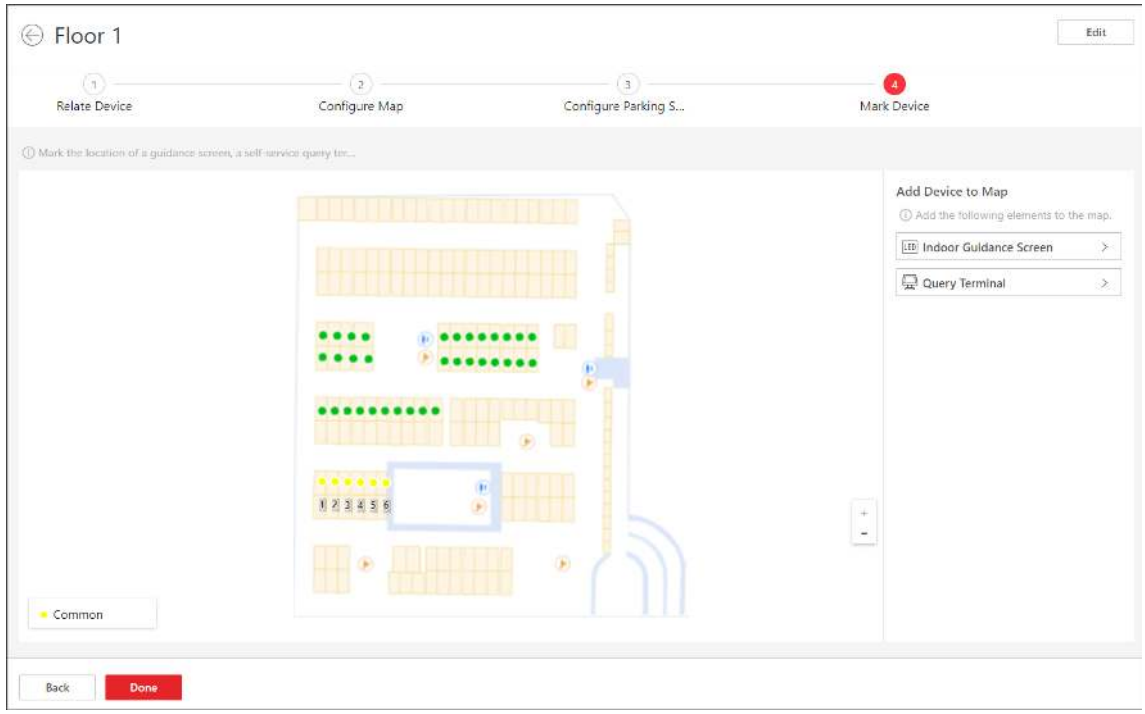


Figure 25-39 Mark Device

2. Add a device (indoor guidance screen or query terminal) to the map by dragging the device from the device list to the map.

Note

Only the indoor guidance screen can be marked. The entrance guidance screens or entrance and exit display screens will not be displayed in the list.

3. Click **Link Parking Space** on the pop-up menu to enter the marking window.
4. Select the parking space(s) and click **OK** to link the selected parking space(s) with the device.

Note

- When you select the parking space(s), you can click a parking space icon to select one, or click **Batch Select** to select multiple parking spaces at a time, or check **Select All Parking Spaces** to select all parking spaces on the map.
- If the current floor has linked with multiple maps, you can click **Switch Map** to switch to another map for marking.

5. **Optional:** Perform the following operations after marking devices on the map.

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. For details about configuring guidance screens, refer to ***Link Display Screen and Set Displayed Content*** .
Check Information Currently Displayed on Guidance 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. 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 at the moment. **Note** This function is only supported by some guidance screens.
Remove Device	Click the device icon on the map and click **Delete** on the pop-up menu to remove the device from the map.

6. **Optional:** Click **Back** to configure the parking space types again.
7. Click **Done** to finish the parking guidance configuration.

25.3.6 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.

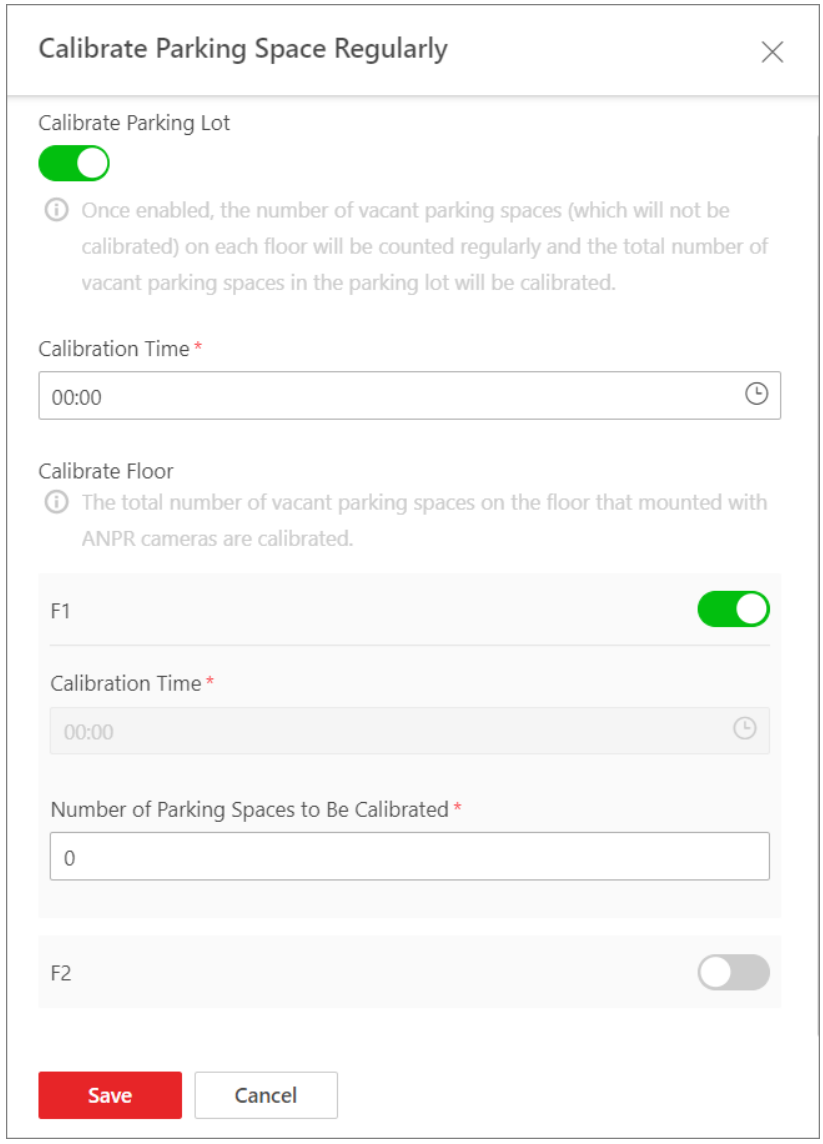


Figure 25-40 Calibrate Parking Spaces Regularly

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**.

25.3.7 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 various kinds of statistics of parking spaces, including the occupancy rate of the parking spaces in a parking lot, the number of vacant parking spaces, occupied parking spaces, parking spaces with unknown status, and the number of overtime parking and parking violations.

Note

- If there is no map added for the parking lot, parking space information will be overlaid directly on the monitoring video.
- An icon will be displayed on a parking space for overtime parking. Click the icon to view the parking space details and check the type of the vehicle that parked overtime.
- By selecting → **Export Unknown Parking Space Information** next to the number of parking spaces with the unknown status under **Violation**, you can export details such as the related parking space numbers and the corresponding parking lot and floor information to the local PC as an XLSX file.

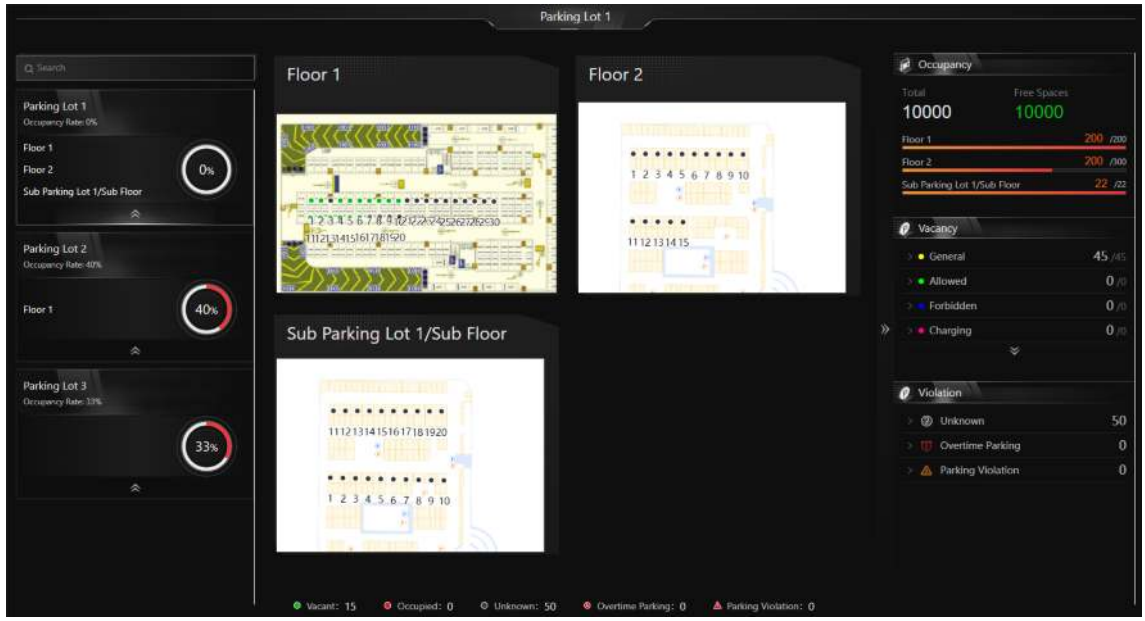


Figure 25-41 Parking Space Overview

You can click a floor name to view the statistics of the parking spaces of this floor. On the following page, you can move to a specific parking space to view its detailed information, and can click a parking space to view its real-time status and search for parking records. Moreover, you can click **Occupancy Status Overview** or **Parking Duration Overview** to view these two types of statistics respectively.

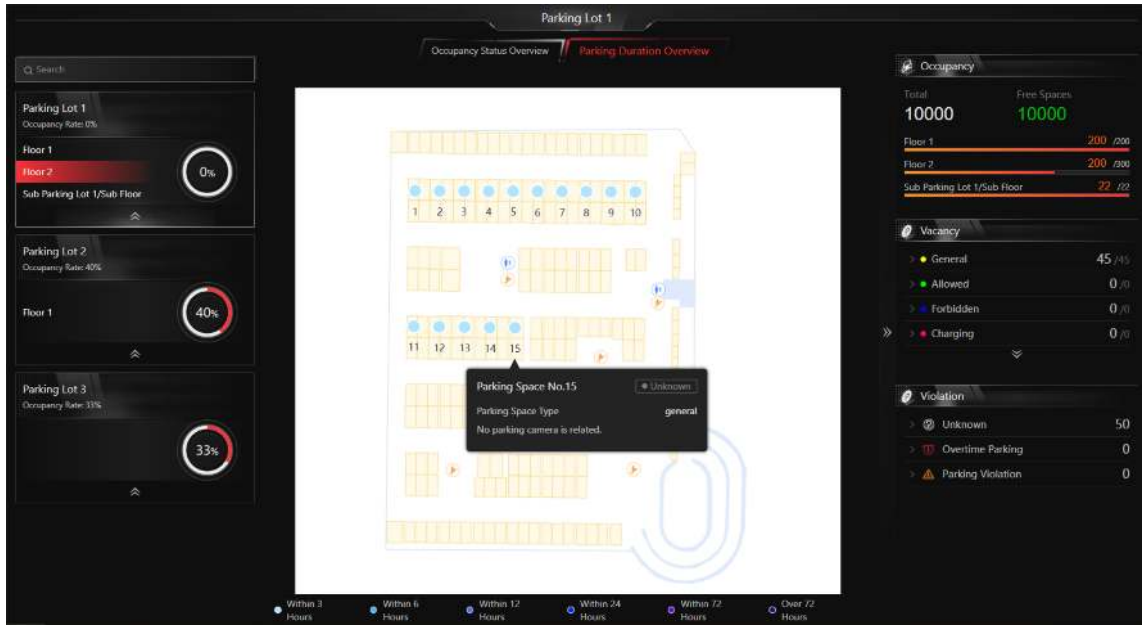


Figure 25-42 Floor Parking Space Overview

25.4 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.

25.4.1 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 top navigation bar, select → **Passing Management** → **Parking Lot** → **Search** → **Passing Vehicle Search** .

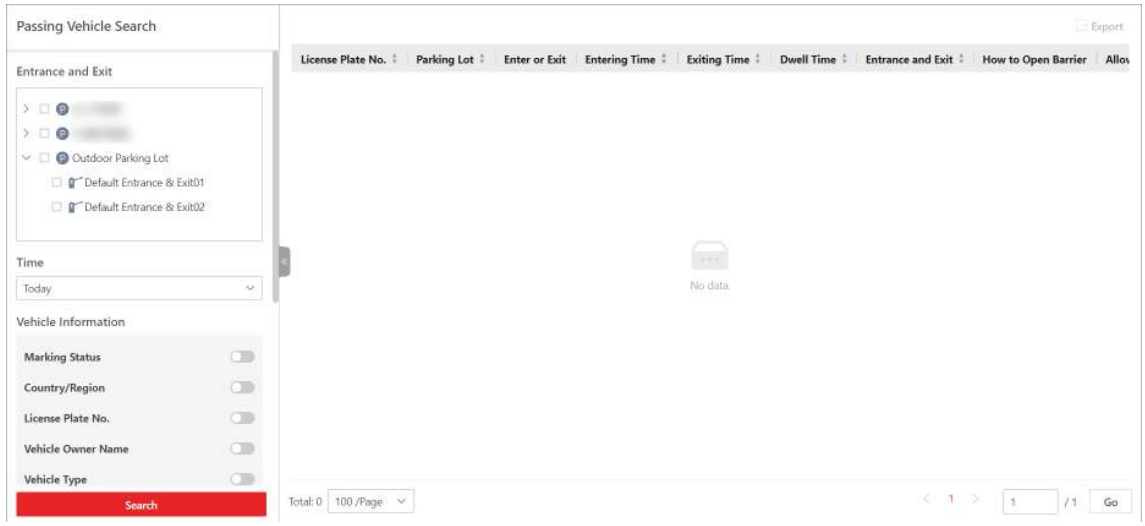


Figure 25-43 Passing Vehicle Search Page

2. Select one or multiple entrances and exits where you want to search for the vehicle passing records.
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. Switch on and set the search condition(s) according to your needs. Here we only introduce conditions that may confuse you.

   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. For how to customize vehicle information, refer to ***Customize Vehicle Information*** .

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. 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 is set to **Person and License Plate Match**. For details about setting the entry/exit modes, refer to ***Set Entry & Exit 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.
- 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.

25.4.2 Search for Parking Records

On the platform, you can search for the parking records generated in a specific parking lot or the record 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 top navigation bar, select → **Passing Management → Parking Lot → Search → Parking 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.

   Parking Space No.

   Enter a 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. 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 is set to **Person and License Plate Match**. For details about setting the entry/exit modes, refer to ***Set Entry & Exit 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.

25.4.3 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 top navigation bar, select → **Passing Management → Parking Lot → Search → Parked Vehicle Search** .

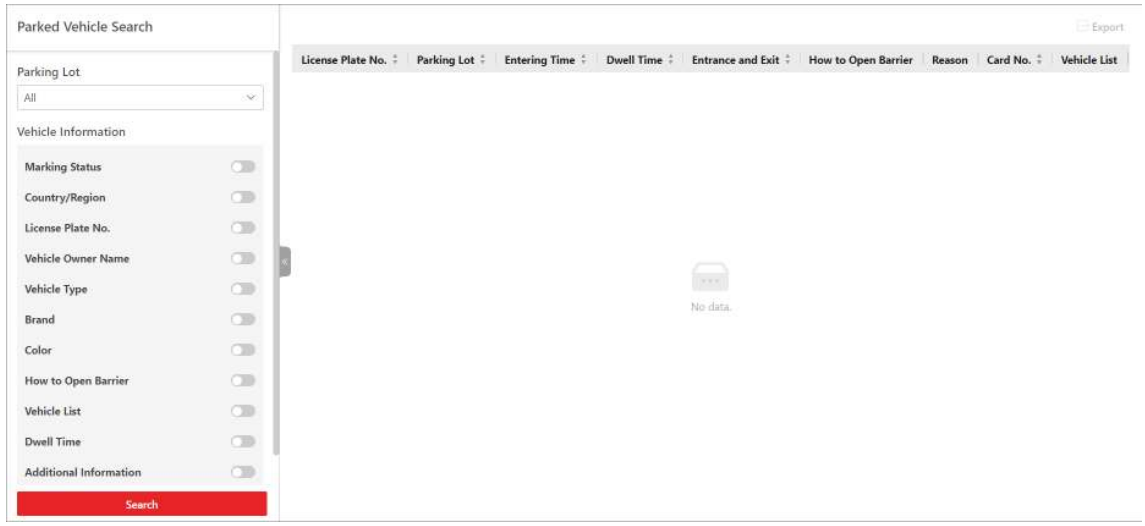


Figure 25-44 Search for Parked Vehicles in Parking Lot

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.

   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. For how to customize vehicle information, refer to ***Customize Vehicle Information*** .
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. 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 is set to **Person and License Plate Match**. For details about setting the entry/exit modes, refer to ***Set Entry & Exit Mode*** .
Export All 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 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 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.

25.4.4 Search for Payment Records

If a vehicle pays the parking fee and exits the parking lot, its payment information, such as the payment source and operation time, will be recorded in the platform. On the platform, you can search for the payment records generated in a specific parking lot or the records of a specific vehicle by setting search conditions according to actual needs. You can also export the records to your PC. With the statistics, you can monitor some of the transactions done in the parking lots, which can help you manage the parking lots better.

Steps

1. On the top navigation bar, select → **Passing Management** → **Parking Lot** → **Search** → **Payment 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.

   Operator

   Select the person responsible for collecting the fee from the drop-down list.

   Payment Method

   Select how the parking fee is paid. **Cash** indicates the fee is paid in cash; **Vehicle Owner Account** indicates the fee is deducted from the owner's account balance.

   Payment Source

   Select where the parking fee is paid. **Booth** indicates the parking fee is paid at the booth; **Toll Center** indicates the parking fee is paid in the toll center.
4. Click **Search**.

   The matched record(s) will be displayed on the right.

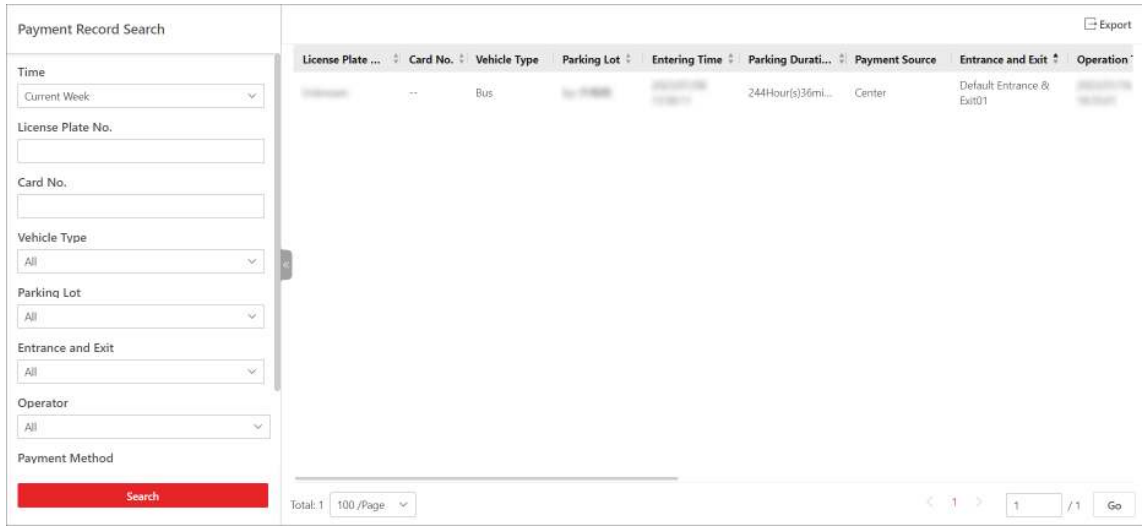


Figure 25-45 Payment Record Search Results

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.

25.4.5 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 top navigation bar, select → **Passing Management** → **Parking Lot** → **Search** → **Top-Up and Refund Record Search** .

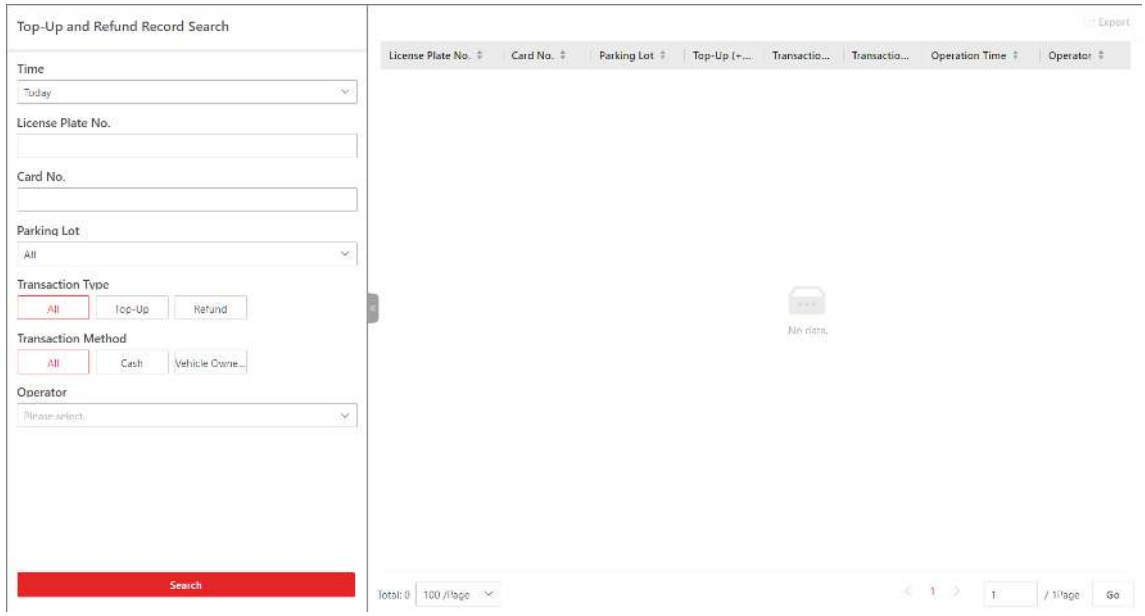


Figure 25-46 Top-Up and Refund Record Search Page

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).

   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.
4. Click **Search**.

   The matched record(s) will be displayed on the right.
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.

25.4.6 Search for Transaction Records of Vehicle Owner Account

In the Search module, 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 top navigation bar, select → **Passing Management** → **Parking Lot** → **Search** → **Account Transaction Record Search** .

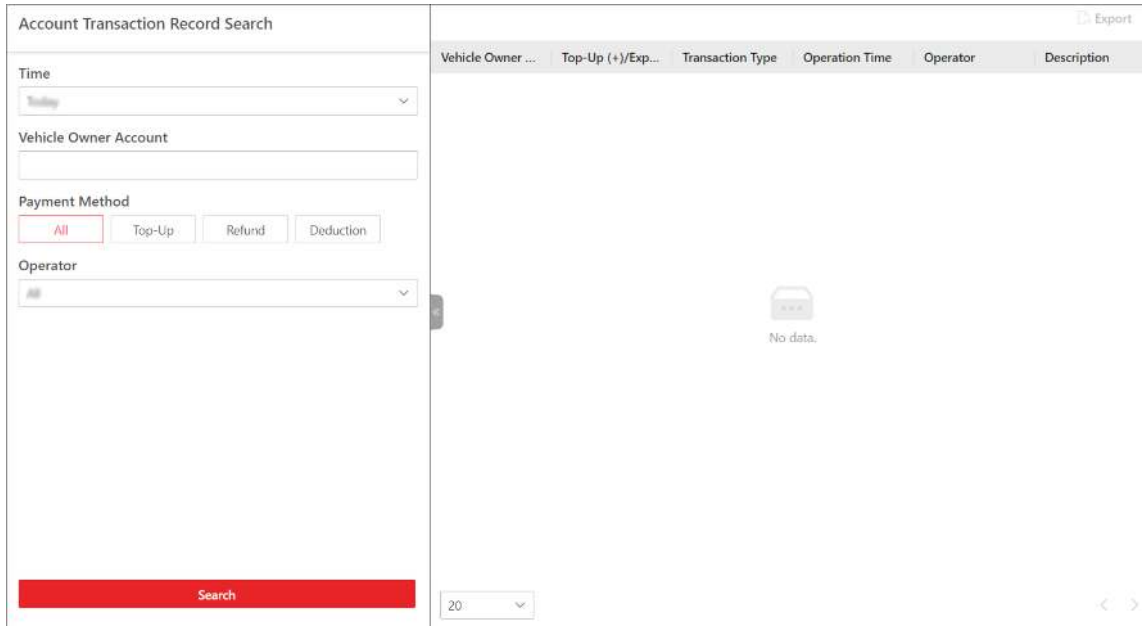


Figure 25-47 Account Transaction Record Search Page

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**.

   The matched record(s) will be displayed on the right.
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.

25.4.7 Search for Work Records of Operators

In the Search module, you can search for the work records of operators (i.e., the persons responsible for payment management). You can view 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 top navigation bar, select → **Passing Management** → **Parking Lot** → **Search** → **Operator Shift Search** .

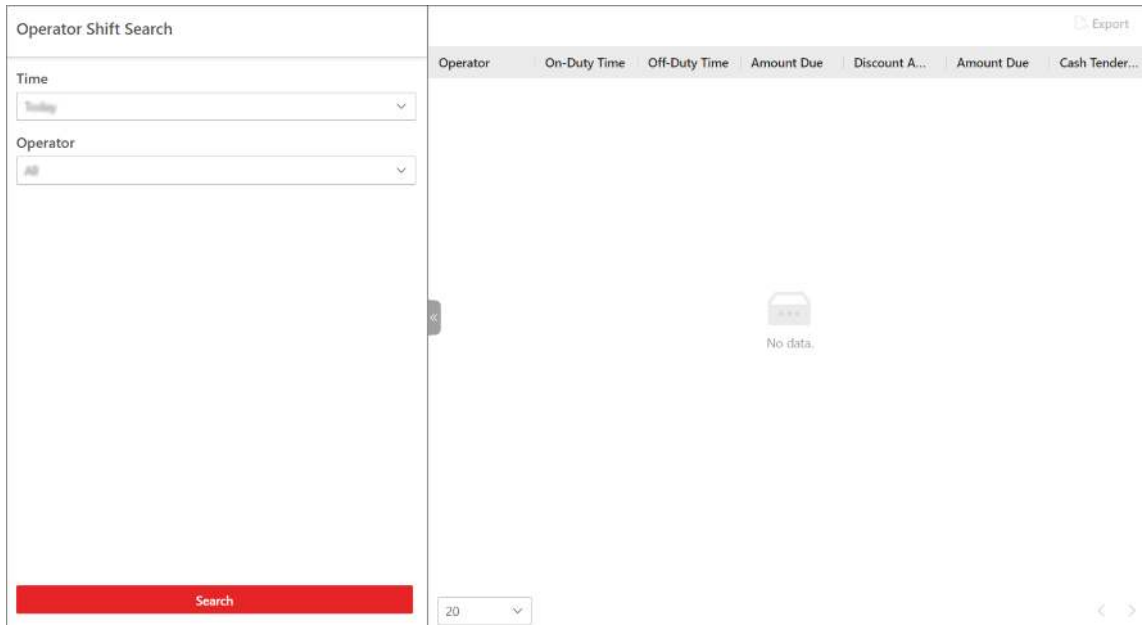


Figure 25-48 Operator Shift Search Page

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**.

   The matched record(s) will be displayed on the right.
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.

25.4.8 Search for Coupon Records

In the Search module, 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 top navigation bar, select → **Passing Management** → **Parking Lot** → **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**.

   The matched record(s) will be displayed on the right.

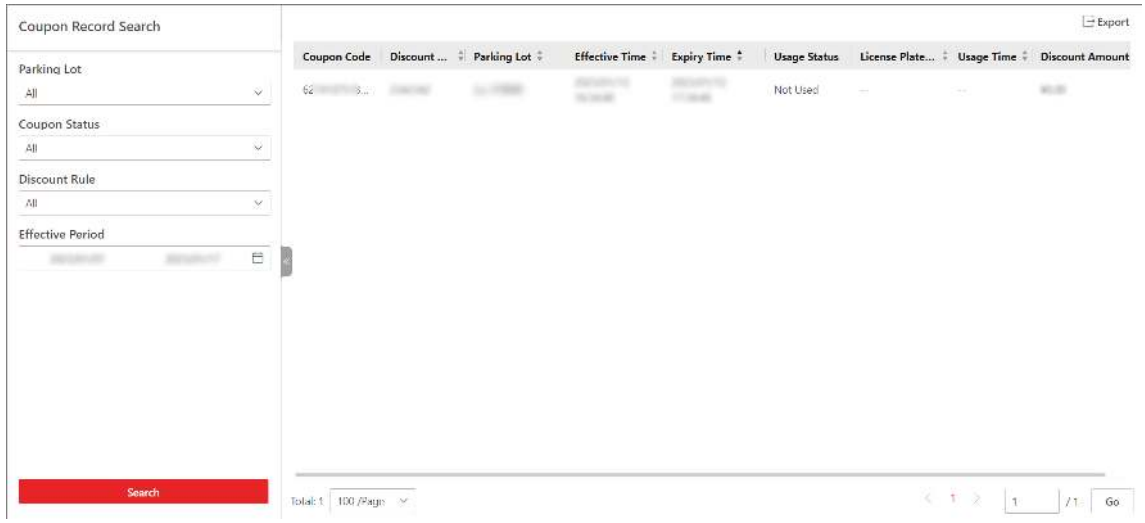


Figure 25-49 Coupon Record Search Results

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.

25.5 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.

25.5.1 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 top navigation bar, select → **Passing Management → Parking Lot → Statistics and Reports → Operation Report** .
2. In the top right corner of the Operation Report page, click **Set Statistics Type** and select the types of statistics to be displayed below for the parking lot(s).

   Note

   - Any user with the permission to view the parking lot operation is able to set which types of statistics 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 a specific parking lot.

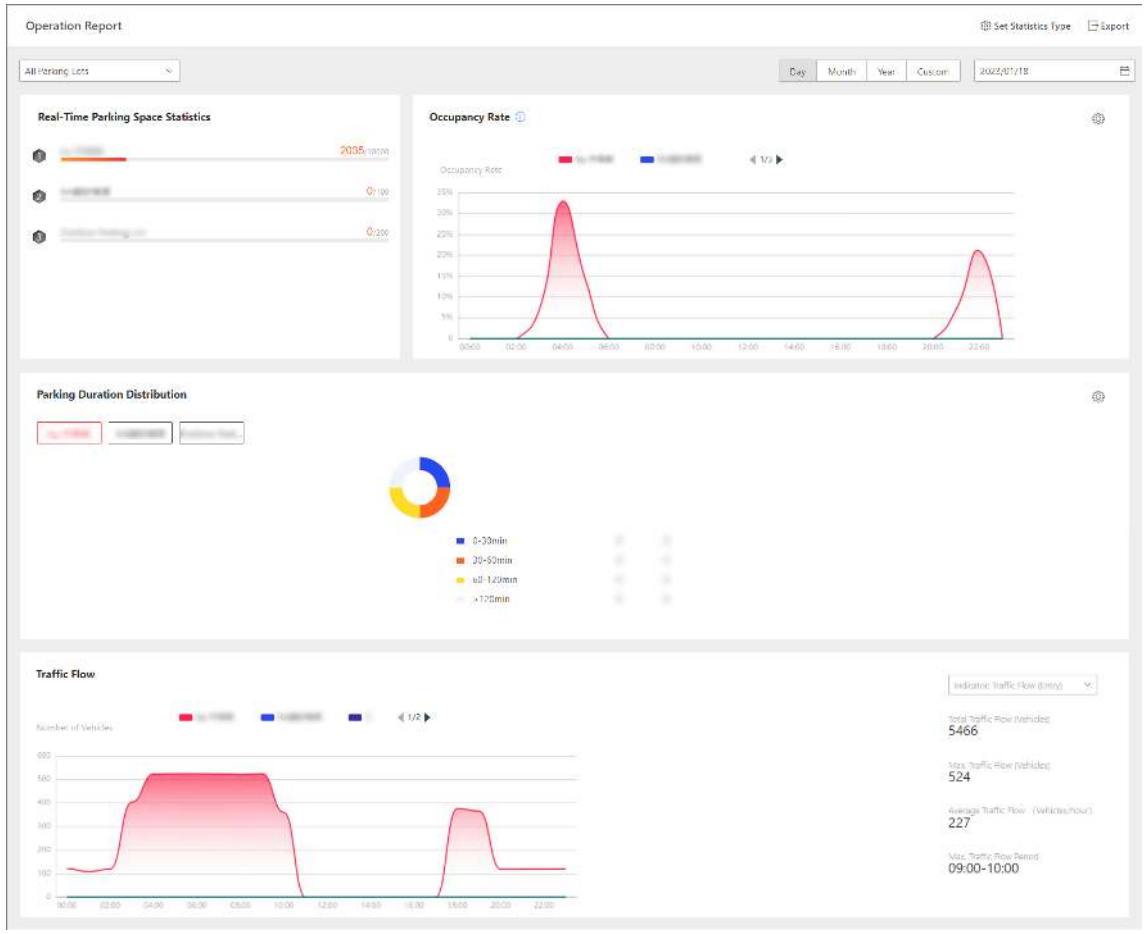


Figure 25-50 Operation Report of All Parking Lots

Table 25-1 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. The distribution of the selected parking duration(s) will be displayed. Click tabs above the pie chart to switch among 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) The total number of vehicles entered all parking lots. **Traffic Flow (Exit)** The total number of vehicles exited all parking lots. **Note** If the user only has permissions related to parking guidance, there will be no drop-down list in this area used for selecting indicators.

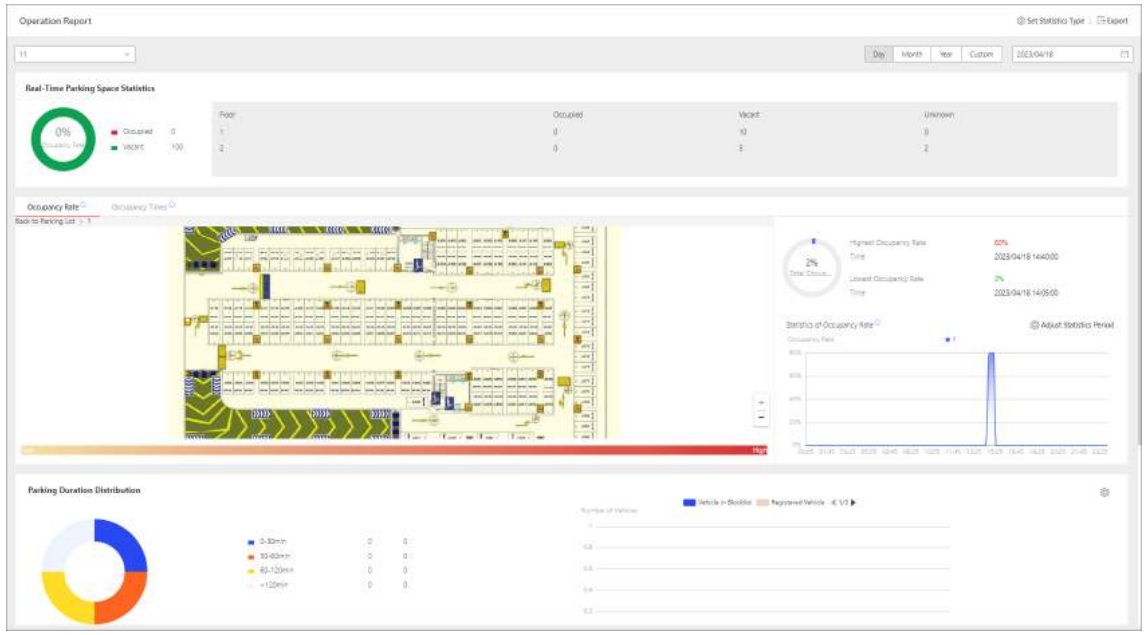


Figure 25-51 Operation Report of a Parking Lot

Table 25-2 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. 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

Statistics Type	Description
	indicate different occupancy rates. The deeper the color, the higher the occupancy rate of the parking space during the selected time. 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.
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. Click **Adjust Time Period** at the right to set a time period. 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. 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. The distribution of the selected parking duration(s) will be displayed in a pie chart. The number(s) of vehicles with the selected parking duration(s) will be displayed by vehicle lists.
Traffic Flow	In the top right corner of the area, select one or multiple indicators from the drop-down list. **Traffic Flow (Entry)** The number of vehicles that entered the parking lots. **Traffic Flow (Exit)** The number of vehicles that exited the parking lots. **By: Entrance and Exit** If only one indicator is selected, you can select the entrance(s) and exits(s) for displaying the traffic flow by entrance and exit.

Statistics Type	Description
	By: Vehicle List If only one indicator is selected, you can select the vehicle list(s) for displaying the traffic flow by vehicle list. **Note** 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.

25.5.2 Export Transaction Reports of Parking Lots

You can view the statistics related to the revenue and expenditure of parking lots, such as the trend and type of revenue and expenditure, the revenue and expenditure generated in a specific period. The statistics can give you a general picture of the transactions done in the parking lots.

Steps

1. On the top navigation bar, select → **Passing Management** → **Parking Lot** → **Statistics and Reports** .

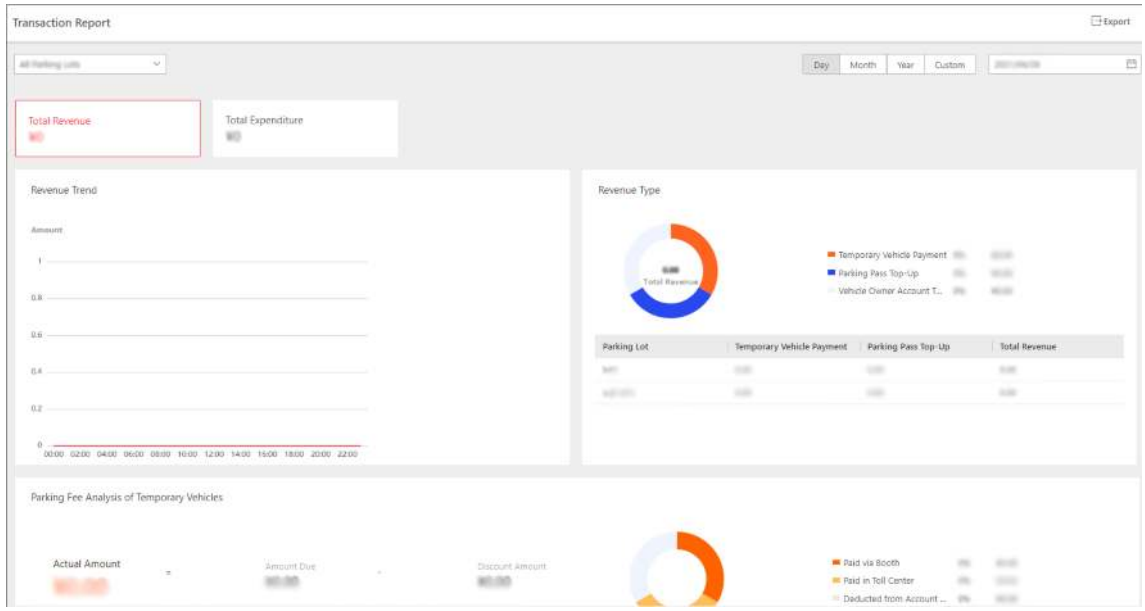


Figure 25-52 Transaction Report Page

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 in 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:** In the upper-right corner, click **Export** to save the analysis report to your PC.

25.5.3 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. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set email settings such as the sender's email address, name, and SMTP server address and port No. For details, refer to ***Configure Email Account*** .
- Make sure you have added the parking lot(s). For details, refer to ***Add Parking Lot*** .

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** → **Parking Lot** → **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.

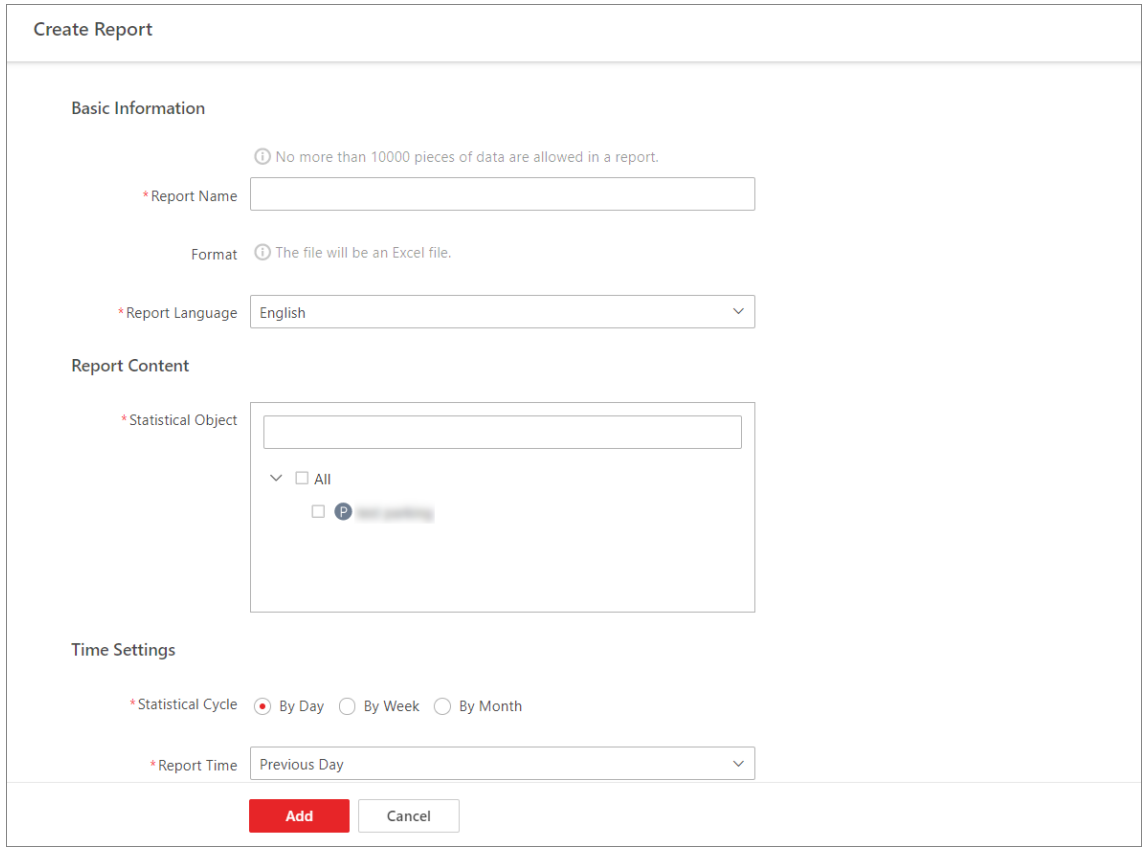


Figure 25-53 Configure Scheduled Report

3. Create a name for the report and select a report language from the drop-down list.

   Note

   By default, the language matches with the one you selected when logging in to the Web Client.
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.

Send On / Send At

- When the statistical cycle is set to **By Day**, the Send On 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 On field, and set the Send At 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 Send At 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 Send At 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. For details about adding email templates, refer to ***Add Email Template for Sending Report Regularly*** .

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.

25.6 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 top navigation bar, select → **Passing Management** → **Parking Lot** → **Basic Configuration** → **Basic Parameter** .

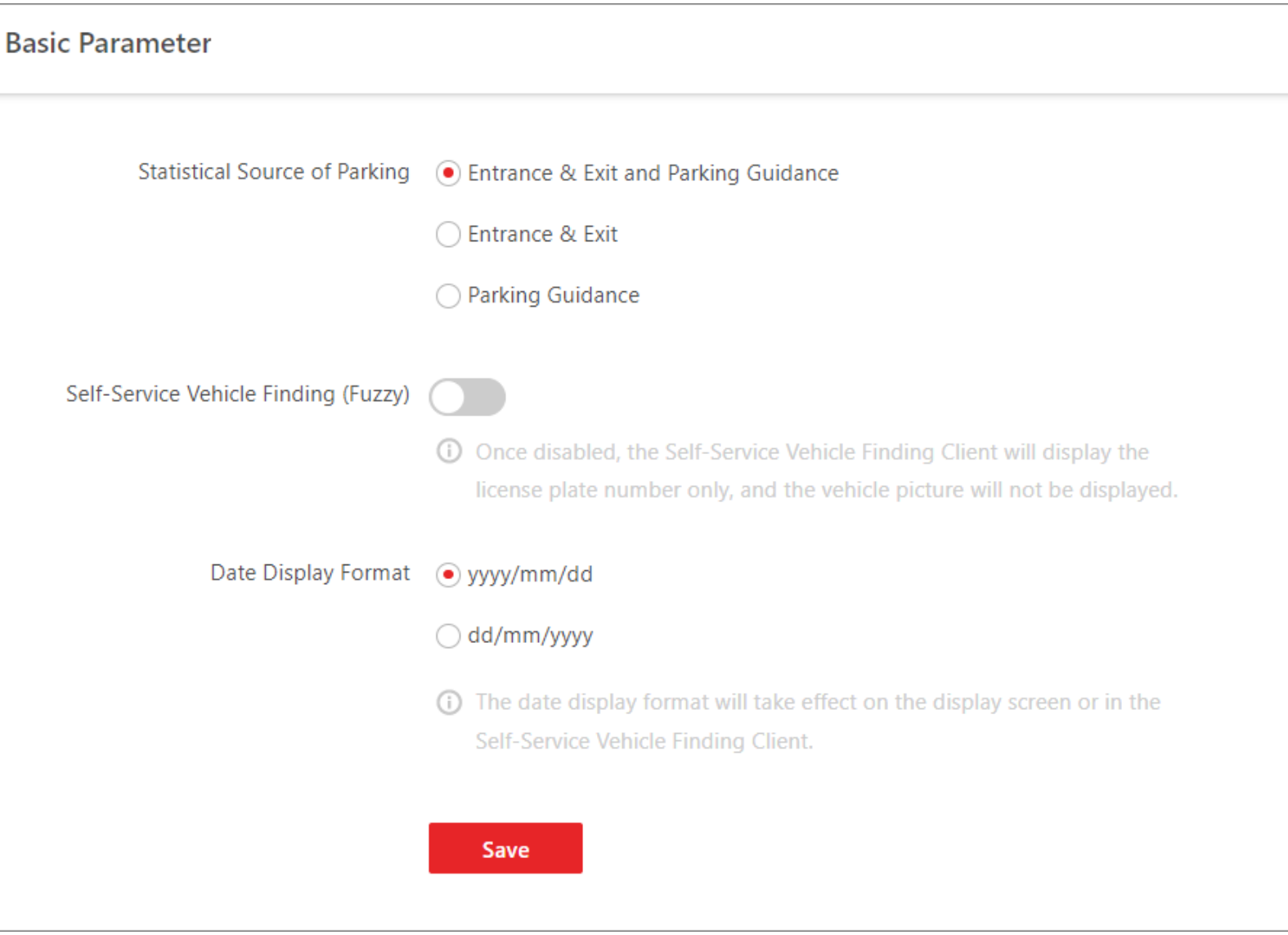


Figure 25-54 Set Basic Parameters

Statistical Source of Parking

Select a source for parking statistics. The following table shows the relations between statistics types and sources.

Table 25-3 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
	(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
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
Parking Guidance Mode	(Web Client) Real-Time Parking Space Statistics in Operation Report	Parking Guidance

Mode	Statistics Type	Source
	(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.
	(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

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.

25.7 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.

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*** .

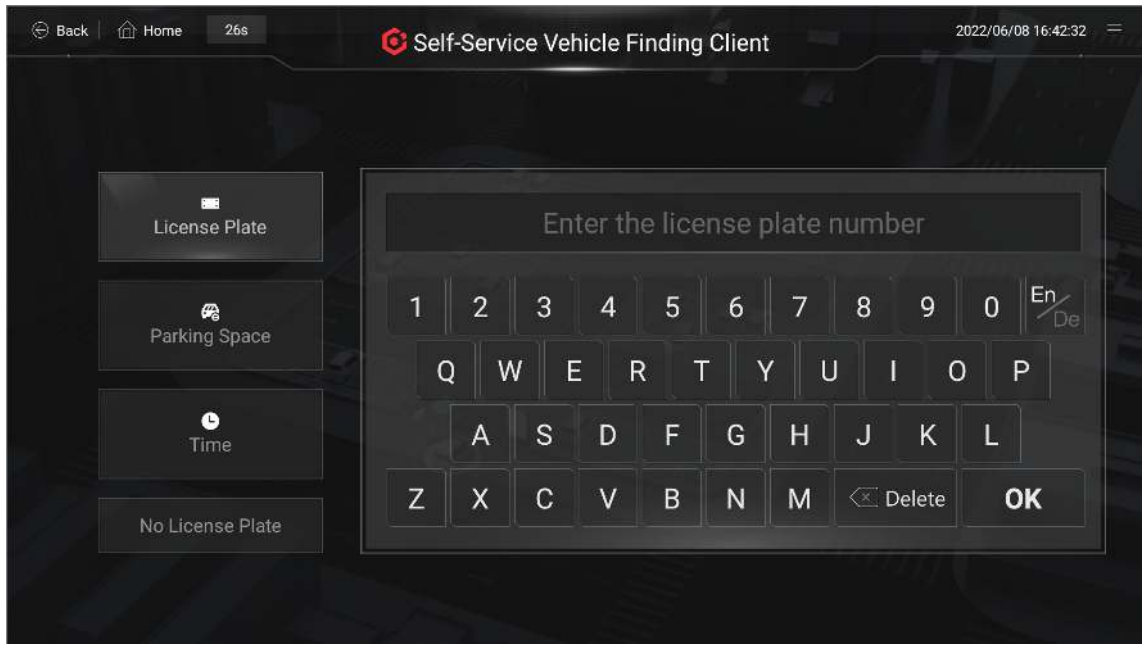


Figure 25-55 Self-Service Vehicle Finding Client

Chapter 26 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.

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.

26.1 Access Control Overview

On the Access Control Overview page, you can view the system data, health status, person credential status, etc.

In the upper-left corner of the Home page, select → **Passing Management** → **Access Control** .

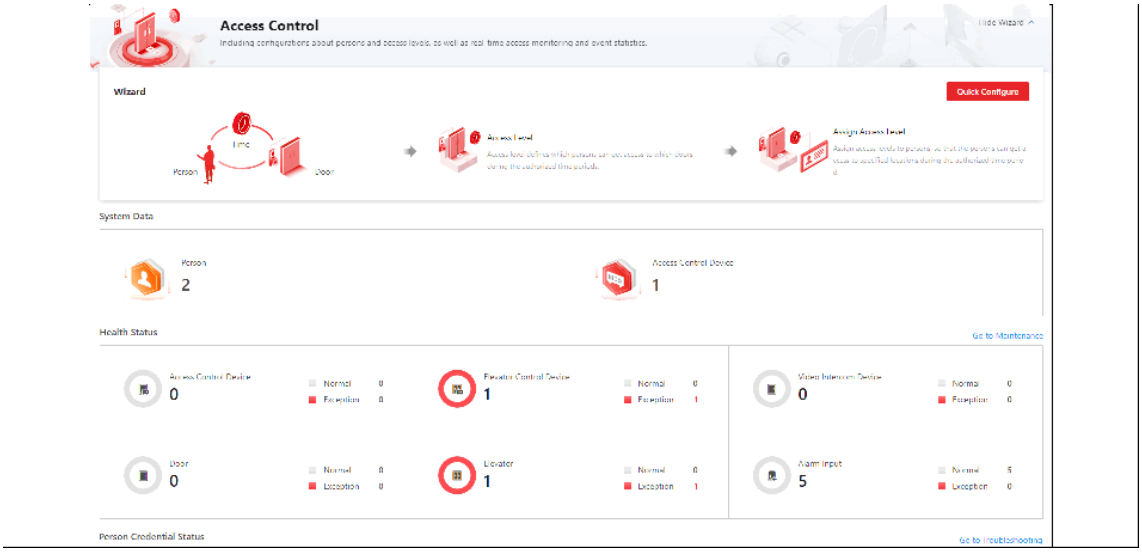


Figure 26-1 Access Control Overview

Perform the following operations as needed.

Operation	Description
Guide	You can view the brief introduction of the Access Control function and the major steps of configuration, including adding door,

Operation	Description
	adding person, setting time period for entry and exit, managing access level, and assigning access level. You can hover the mouse cursor over each step and click ↗ to go to the corresponding page; you can also click **Quick Configure** to complete the configuration process step by step in the Access Control Wizard.
View System Data	In System Data, click the number under person or device to go to the Person Management page or Device page.
View Resource Status	In Health Status, click the number under the resource type or the number besides **Abnormal** to go to the Maintenance page to view details of resources status or alarm input.
Go to Maintenance	In the upper-right corner, click **Go to Maintenance** to enter the Maintenance module. For more about the Maintenance module, refer to ***Maintenance*** .
View Person Credential Status	Click the number of credential not configured to go to the person management page. You can also view the number of each applied credential, and the application status of access levels.
Filter Access Event Statistics	Click ⌄ and select a period to view the statistics of this period.
Export Access Event Statistics	Hover over ⊡ , select a file format, and click **Export** to export the data generated in the selected period.

26.2 Manage Access Level

In access control, access level is a group of access points. Assigning access level to persons, departments, or access groups can define the access permission that which persons can get access to which access points during the authorized time period.

26.2.1 Add Access Level

To define access permission, you need to add an access level to group the access points.

Steps

1. Select **Access Level → Manage Access Level** on the left.
2. In the top left corner of Home page, select ⊞ → **Passing Management → Access Control → Access Level** .
3. Click **Manage Access Level** on the left.
4. Click **Add** to enter the Add Access Level page.
5. Create a name for the access level.

6. **Optional:** Edit the description for the access level.
7. Select the access point type.
8. Select the access point(s) to add to the access level.
   1) In the **Available** list, select the access point(s) you want to add to the system and click > . You can view your selection in the **Selected** list.
   2) **Optional:** In the **Selected** list, select the access point(s) that you no longer want to add to the system, and click < to undo selection.

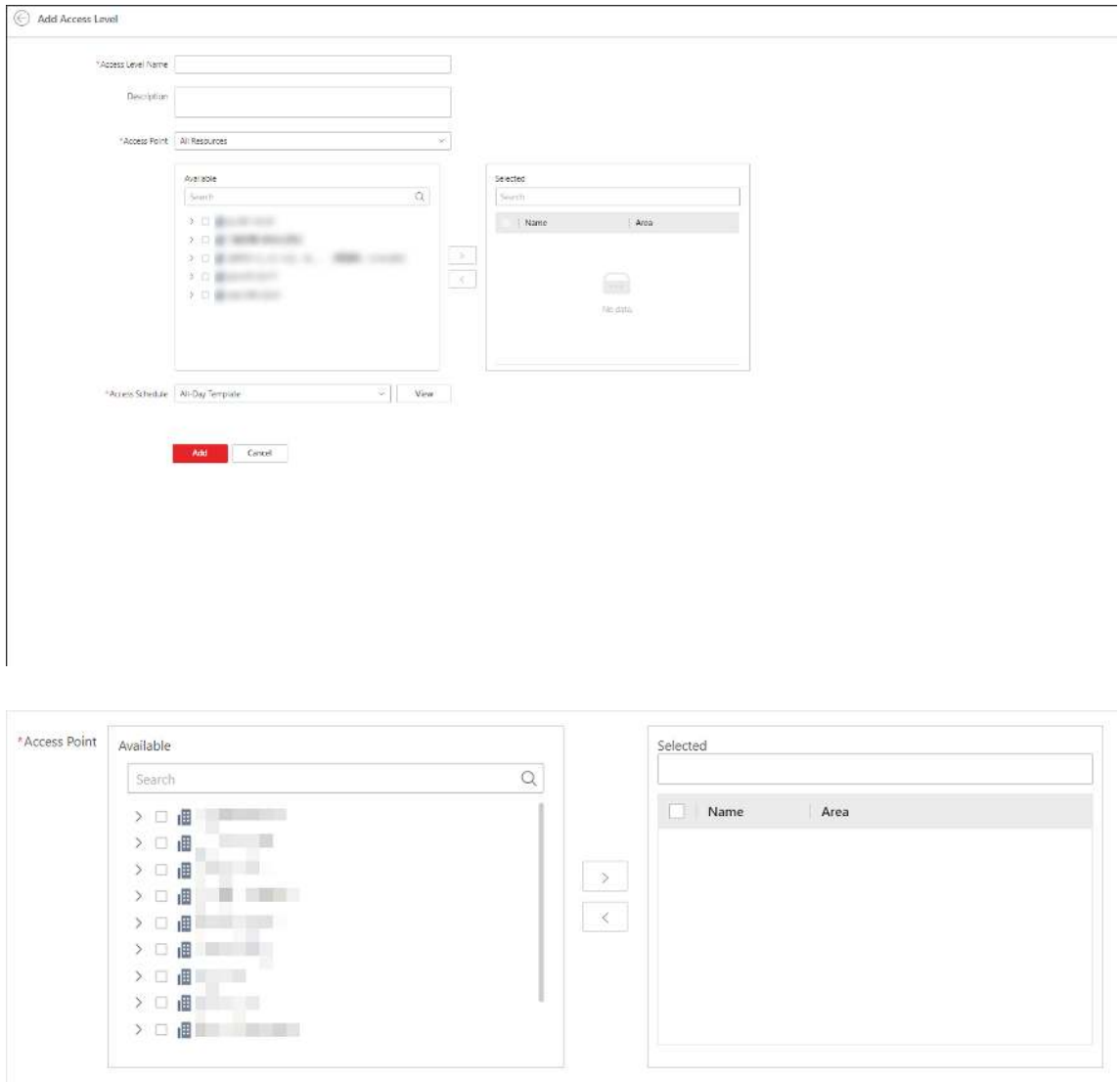


Figure 26-2 Select Access Points

9. 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*** .

10. Click **Add** to add the access level and return to the access level management page.
11. **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.
Delete All Access Levels	Click → **Delete All** to delete all access levels.

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 ***Assign Access Level*** .

26.2.2 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.

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 **Access Level → Assign by Access Level** on the left.
2. In the top left corner of Home page, select → **Passing Management → Access Control → Access Level** .
3. Click **Assign by Access Level** on the left.
4. Click on the access level that you want to assign to persons.

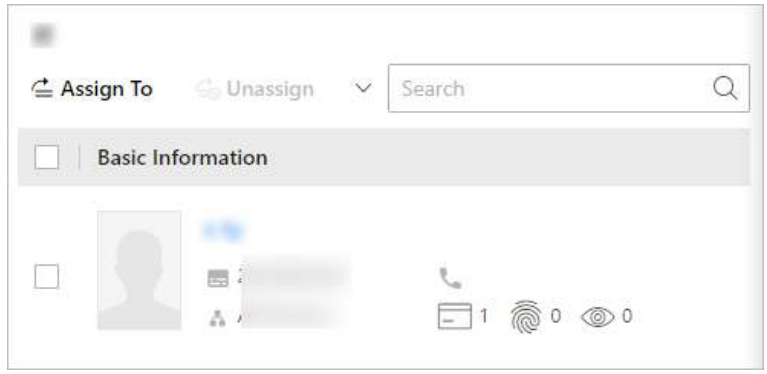


Figure 26-3 Assignee Panel

5. On the assignee panel, click **Assign To** to show person list.
6. Select the persons whom you want to assign the access level to and click **Add**.

Note

If you check **Select All Persons**, all persons who matched the search conditions you set will be selected.

The access level settings will be applied to devices automatically.

7. **Optional:** You can also apply access level settings to devices manually or regularly.

Note

For details, refer to ***Manually Apply Access Level Settings to Device*** and ***Regularly Apply Access Level Settings to Devices*** .

8. **Optional:** To unassign a person from the access level, select the person and click **Unassign**. To unassign all, click → **Unassign All** .

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 **Access Level** → **Assign by Person** on the left.

2. In the top left corner of Home page, select → **Passing Management** → **Access Control** → **Access Level** .
3. Click **Assign by Person** on the left.
4. In the department list, select a department.
5. In the person information panel on the right, select the persons to whom you want to assign access levels.

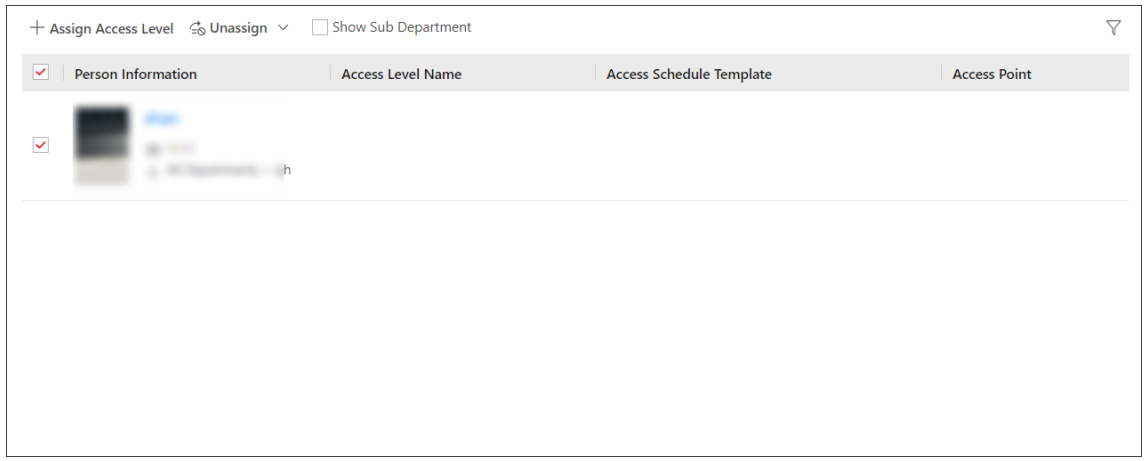


Figure 26-4 Person Information Panel

Note

You can click on person's name to view the details about the person.

6. Click **Assign Access Level**.
7. In the Assign Access Level panel, select the access levels that you want to assign to the selected persons.
8. Click **Assign**.

   The access level settings will be applied to devices automatically.
9. **Optional:** You can also apply access level settings to devices manually or regularly.

Note

For details, refer to ***Manually Apply Access Level Settings to Device*** and ***Regularly Apply Access Level Settings to Devices*** .

10. **Optional:** To unassign a person's access levels, select the person and choose **Unassign All Access levels** or **Unassign Specified Access Levels**.

Note

For details, refer to ***Clear Persons' Access Levels*** .

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 **Access Level → Assign by Person** on the left.
2. In the top left corner of Home page, select → **Passing Management → Access Control → Access Level** .
3. Click **Assign by department** on the left.
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 on a department.
     b. In the assigned access level panel on the right, click **Assign Access Level**.
     c. In the Assign Access Level panel, 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**.
     b. In the department list, select the departments where you want to assign access levels.

     Note

     Sub-groups are excluded from selection by default. To include all sub-groups of each department, check **Select Sub-Groups**.

     c. In access level list, select the access levels you want to assign to the departments.
     d. Click **Save**.

Note

After assigning access levels to a department, you can still modify the access levels for each person in the group, and it will not affect the settings for the department. For details, refer to ***Assign by Person*** .

The access level settings will be applied to devices automatically.

5. **Optional:** You can also apply access level settings to devices manually or regularly.

Note

For details, refer to ***Manually Apply Access Level Settings to Device*** and ***Regularly Apply Access Level Settings to Devices*** .

6. **Optional:** To unassign an access level from the department, select the access level and click **Unassign**. To unassign all access levels, click → **Unassign All** .

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 permission (In the 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. One or multiple access levels can be assigned 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 **Access Level → Assign by Access Group** on the left.
2. In the upper-left corner of the Home page, select → **Passing Management → Access Control → Access Level** .
3. Click **Assign by Access Group** on the left.
4. Perform one of the following operations to enter the Add Access Group page.
   - Click at the top of the access group list to enter the Manage Access Group page, and then click **Add** to enter the Add Access Group page.
   - 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.
5. In the **Group Name** field, enter the name of the access group.
6. In the **Group Member** area, click **Add** to open the person list, select the person(s) to be added to the access group.
7. Click **Add** to add the selected person(s) to the access group.
8. After configuration, click **Add** at the bottom.
9. Select an access group to assign access levels to.
10. Click **Assign Access Level** on the right.
11. In the Assign Access Level page, select the access level(s) to be assigned to.
12. Click **Assign**.

    The access level settings will be applied to devices automatically.
13. **Optional:** You can also apply access level settings to devices manually or regularly.

Note

For details, refer to ***Manually Apply Access Level Settings to Device*** and ***Regularly Apply Access Level Settings to Devices*** .

14. **Optional:** Unassign access level(s) from the access group.
    - In the assigned access level list, select the access level(s) and click **Dissociate** to unassign the access level(s) from the access group.
    - In the assigned access level list, click → **Unassign All** to unassign all access levels from the access group.

What to do next

Test your access control configurations and devices before putting them into use. For details, refer to ***Access Control Test*** .

26.2.3 Apply Persons' Access Levels to Device

After setting or modifying the linkage between persons and access levels, you need to apply the access level settings to the access control devices or elevator control devices to take effect. After that, the persons can access these access points during the authorized time period defined by the related access level.

Manually Apply Access Level Settings to Device

After setting access levels and assigning access levels to persons, departments, or access groups, you need to apply the relations between persons and access points to the devices.

Before You Start

Make sure you have assigned access levels to persons in the system. For details, refer to ***Assign Access Level*** .

Steps

1. In the top left corner of Home page, select → **Access Control** → **Access Level** .
2. Click **Assign by Access Level**, **Assign by Person**, **Assign by department**, or **Assign by Access Group** on the left.
3. Click **Apply Access Level Settings**.
4. On the Apply Access Level Settings panel, select the persons to apply the access level settings.
    - To apply the access level settings of all persons, select **All Persons**.
    - To apply the access level settings of specific persons, select **Specified Persons**, click , select the persons, and click **Add**.
5. Select the access points to apply the persons' access level settings.
    - To apply the access level settings of all access points, switch off **Specified Access Point**.
    - To apply the access level settings of specific access points, switch on **Specified Access Point** and select the access points.
6. Apply access level settings to devices.

- To clear all persons' access level configurations on the devices first and then apply the configurations in the platform to the devices, check **Apply (Initial)** and click **Apply**.

  Note

  - Only available when you select **All Persons** previously.
  - During the initialization process, the devices will be offline, and persons cannot access these access points.

- To apply changed (newly added, edited, deleted) access level settings to the devices, uncheck **Apply (Initial)** and click **Apply**.

7. **Optional:** If persons' access level settings (such as linked access levels, person credentials, etc.) are changed or the applying process failed, will appear next to , indicating some access level settings are pending to be applied to the devices. You can hover the cursor over to view the details.

   Note

   For troubleshooting the applying process, refer to ***Access Control Test*** .

Regularly Apply Access Level Settings to Devices

You can set a schedule to apply the access level settings in the system to devices automatically.

Before You Start

Make sure you have assigned access levels to persons in the system. For details, refer to ***Assign Access Level*** .

Steps

1. In the top left corner of Home page, click → **Access Control** → **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**.

26.2.4 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.

In the top left corner of Home page, click → **Passing Management → Access Control → Access Level → Assign by Person** .

Select a department to show all persons in the group. You can filter the target persons by setting search conditions.

Select the target person and click **Unassign** to choose **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.
After clearing, the previous access level settings of the persons cannot be restored. You need to re-assign access levels for them again when needed.

After clearing the access level settings of the selected persons, these persons will be removed from the related access groups. You need to apply the access level settings of these persons to the devices to take effect. For details, refer to ***Manually Apply Access Level Settings to Device*** for details. You can also set a schedule to apply automatically. For details, refer to ***Regularly Apply Access Level Settings to Devices*** .

After applying to the devices, the access level settings of the persons will be deleted from the devices.

26.2.5 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, Weekday Template, and Weekend Template. You can also add customized templates according to your needs.

Steps

1. In the top left corner of Home page, click → **Passing Management → Access Control → Basic Configuration** .
2. Click **Access Schedule Template** on the left.
3. Click + to create a blank template.
4. Configure the template in the template information panel on the right.

   Name

   Create a name for the template.

   Copy from

   Optionally, you can select to copy the settings from existing templates.
5. In the **Weekly Schedule Template** box, set a schedule pattern for each day.

1) Click **Authorize** and 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.
2) **Optional:** Click **Erase** and select or draw on the authorized time periods to clear the selection.

Note

You can set up to 8 separate time periods for each day.

6. **Optional:** Set a holiday schedule if you want different schedules for specific days.

Note

Holiday schedule has a higher priority than weekly schedule.

1) Click **Add Holiday**.
2) Select existing holiday templates, or click **Add New** to create a new holiday template (see ***Set Holiday*** for details).
3) Click **Add**.
4) Set a schedule pattern for holidays.

7. Click **Add** to save the template.
8. **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.

What to do next

Set access schedule for access level to define in which time period persons are authorized to access the access points in the access level. For details, refer to ***Add Access Level*** .

26.2.6 Enable Authentication via Password

Authentication via password allows you to authenticate only via your password. After this function is enabled, all the passwords in the platform should be different from each other. You can update the password manually or automatically.

Steps

1. Click → **Passing Management → Access Control → Basic Configuration** .
2. Click **General** on the left to enter the General page.
3. Switch on **Authenticate via PIN Code**.
4. Select **Manual** or **Auto** as the PIN code update mode.

Manual Mode

You need to export users whose passwords are duplicated or not configured from the Person module, and then notify these users to update the passwords by themselves. A password should consist of 4 to 8 characters.

Auto Mode

The platform will change the duplicate password to a unique one or customize a unique password for each user whose password is not configured, and then notify these users.

5. Click **Save**.

26.2.7 Advanced Functions

Configure Free Access and Access Forbidden Rules

You may need to set access points accessible or inaccessible during certain periods. To perform this function, you need to configure free access and access forbidden rule for certain access points.

Steps

Note

This function should be supported by the device.

1. In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Access Control Application** → **Free Access & Access Forbidden** .
2. Click **Add** to enter the Add Free Access and Access Forbidden Rule page.
3. Enter the rule name.
4. Select an access point from the following area list.
5. Select free access schedule or access forbidden schedule.

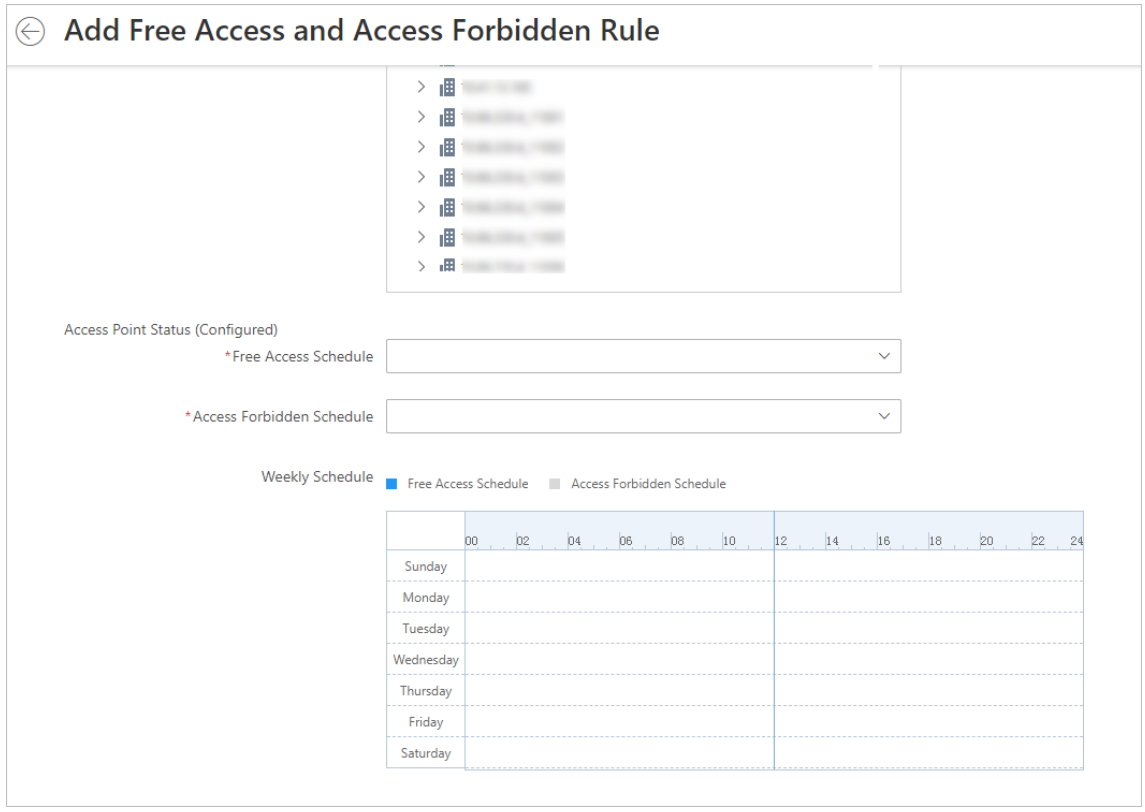


Figure 26-5 Add Free Access and Access Forbidden Rule Page

Free Access Schedule

During free access period, all persons can access the selected access points without credentials required.

Access Forbidden Schedule

During access forbidden period, no persons can access the selected access points even if he/she has the authorized credentials, except the super users.

Note

- You can click **Add** to add a custom access schedule or holiday schedule. See ***Set Access Schedule Template*** for details.

6. Click **Add**.

The system will automatically apply the schedule(s) to devices.

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

View Schedule Details	Click to show the schedule details.
Copy Schedule to Other Access Point	Click a rule name to enter the rule page. Click **Copy To** on the top right to copy the schedule to other access points.

Configure First Person In Rule

First Person In refers to a rule that only after the first person is authorized to enter with his or her card, fingerprint, or face, can other people's permission be activated. There are two modes for First Person In, the Remaining Open after First Person and the Authorization by First Person.

Steps

Note

This function should be supported by the device.

1. In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Access Control Application** → **First Person In** .
2. Click **Add** to enter the Add First Person In Rules page.
3. Enter the rule name.
4. Select a door from the area list.
5. Set **Rule of Opening Door**.

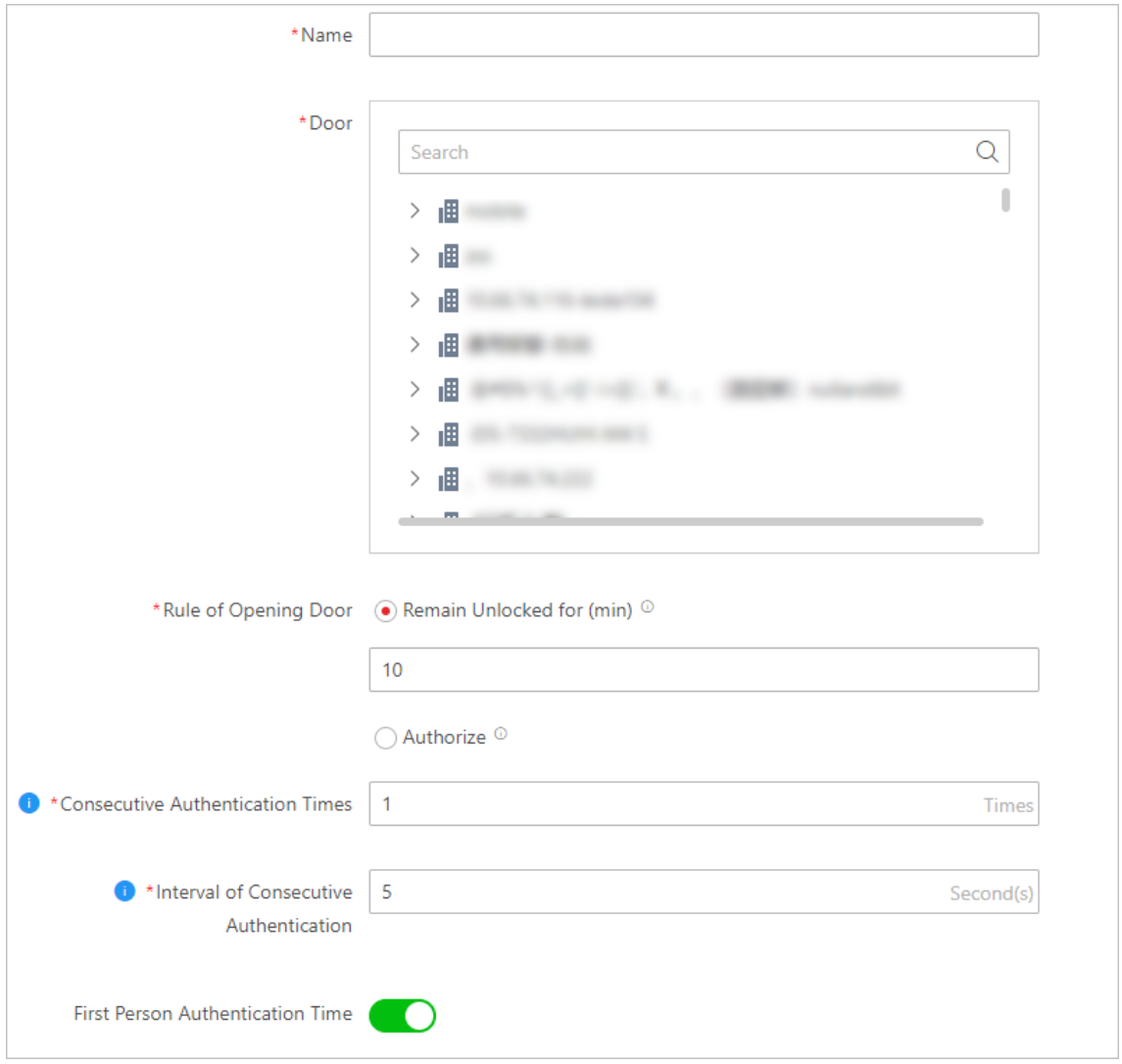


Figure 26-6 Add First Person In Rule Page

Remain Unlocked for (min)

When the door is locked, if the first person swipes card, the door will remain unlocked during the configured period.

Authorized

The door is locked and access is denied with any credentials (except during the free access schedule) until you swipe the first card. After the first person swipes card, the door is authorized and the persons with corresponding access level are granted to access. The authorization will be invalid at 00:00 a.m. every day.

6. Click **Add** to select first person(s).
7. Click **Add** to add the rule.

Add Emergency Operation Group

An emergency operation group is a group for access points which need to be operated (remaining locked/unlocked) in a batch. This function is mainly applicable for emergent situation.

Before You Start

Add the access points into different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. In the top left corner of Home page, select → **Passing Management** → **Access Control** → **Access Control Application** → **Emergency Operation Group** .
2. Click **Add**.

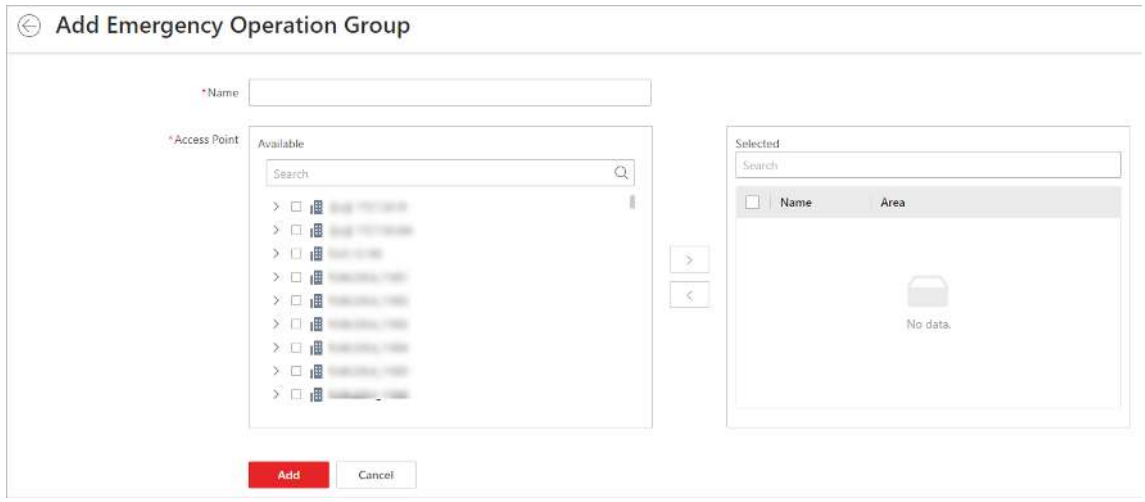


Figure 26-7 Add Emergency Operation Group Page

3. Create a name for the group.
4. Select the access points and click to add them to the group.

Note

You can add doors of access control devices, doors of video intercom devices, and floors of elevator control devices to the emergency operation group.

5. Click **Save**.

   The emergency operation group is added in the table and you can view the access points in the group.

Configure Anti-Passback Rules

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 swiping the card. You can configure area anti-passback rules or route anti-

passback rules for different scenarios. This function is mainly used to enhance the access security of some important or specific places (e.g., laboratories, offices).

Configure Area Anti-Passback Rules

The area anti-passback function establishes a specific door group for an area. When a person accesses the area by swiping card, he/she should exit the area via the door in the anti-passback group if he/she enters the area via the door in the group, and he/she cannot enter the area via the door in the anti-passback group if he/she exited the area not by swiping card at the door in the group before.

Before You Start

Add the access points to different areas first. For details, refer to ***Add Element to Area*** .

Steps

1. In the upper-left corner of the Home page, click → **Passing Management** → **Access Control** → **Access Control Application** → **Anti-Passback** → **Area Anti-Passback** .
2. Click **Add**.
3. Create a name for the door group.
4. Select doors in the Available list and click › to add them to the Selected list.
5. **Optional:** Switch on **Forgive Anti-Passback** and set a fixed time so that the platform can forgive the anti-passback violations occurred in this group automatically everyday.

   Anti-Passback Violation

   When a person attempts to use a card without following the rule, the access will be denied. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven.
6. Click **Add**.
7. **Optional:** Perform the following operations after adding the anti-passback group to the area.

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	When a person attempts to use a card without following the rule, the access will be denied. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no access is allowed unless the anti-passback violation event is forgiven. 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).

Delete Anti-Passback Group	Select the group(s) and click **Delete** to delete the anti-passback group(s).

Configure Route Anti-Passback Rules

The route anti-passback depends on the card swiping route. This function establishes a specific card reader sequence in which cards must be used in order to grant access. You should set the first card reader and the subsequent ones. It will authenticate the anti-passback according to the entrance and exit information stored in the card reader.

Steps

1. In the upper-left corner of the Home page, click → **Passing Management** → **Access Control** → **Access Control Applications** → **Anti-Passback** → **Route Anti-Passback** .
2. Click **Add** to enter the Add Route Anti-Passback page.
3. Create a name for the route anti-passback rule in the **Name** field.
4. Set the card reader order in the Card Reader Order area.
   1) Click **Add**, select a card reader in the list, and click **Add** to add a card reader.
   2) Hover the cursor on the added card reader and click ⊕ to add another card reader.

   Note

   You can repeat this step to add card readers according to a specific sequence as needed.
   3) **Optional:** Click the card reader and click **Change Card Reader** to select another card reader to replace it.
   4) **Optional:** Click the card reader and click **Delete** to delete the card reader and its subsequent card reader(s).
5. **Optional:** Switch on **First Card Reader** and select a card reader from the drop-down list to set it as the first card reader.

   Note

   If you violate the route anti-passback rule, you should swipe the card again from the first card reader.
6. **Optional:** Switch on **Forgive Anti-Passback** to set a fixed time so that the platform can forgive the anti-passback violations automatically everyday.

   Anti-Passback Violation

   When a person attempts to use a card out of the route anti-passback rule's sequence, the access will be denied. This is called "Anti-Passback Violation". When an anti-passback violation occurs, no entry is allowed unless the anti-passback violation event is forgiven.
7. Click **Add**.
8. **Optional:** Perform the following operations after adding the route anti-passback rule.

View Card Reader Order	Click 👁 in the Operation column to view the card reader order of the rule.

Edit Anti-Passback Rule	Click the rule name to edit the anti-passback rule settings. You can edit the name of the rule, add, change, or delete card readers in the order, change the first card reader, or change the settings of forgiving anti-passback violation regularly.
Set/Cancel Forgiving Anti-Passback Regularly	When a person attempts to use a card out of the route anti-passback rule's sequence, the access will be denied. This is called "Anti-Passback Violation". When anti-passback violation occurs, no entry is allowed unless the anti-passback violation event is forgiven. Select the rule(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 rule(s) at that time everyday. You can also select the rule(s) and click **Cancel Forgiving Anti-Passback Regularly** to cancel the settings of the selected rule(s).
Delete Anti-Passback Rule	Select the rule(s) and click **Delete** to delete the route anti-passback rule(s).

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. In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Access Control Application** → **Multi-Door Interlocking** .
2. Click **Add**.
3. Create a name for the group.
4. Select doors and click .
5. Click **Add**.

Manage Multi-Factor Authentication

Multi-Factor Authentication is an access authentication scheme which requires all the predefined persons to be present and get authentication. Multi-Factor Authentication is generally used in places such as bank vault to ensure the security of important assets and data. To perform this function, you need to configure multi-factor authentication rule and add multi-factor authentication group first. Besides, you can add persons to receive remote door open request.

Configure Multi-Factor Authentication Rule

In access control, multi-factor authentication is an authentication method in which the door will unlock only after multiple persons present authenticating multiple credentials in turn. This method is mainly used for locations with high security requirements, such as bank vault. With the mutual supervision of the persons, multi-factor authentication provides higher security for the assets in these locations.

Steps

Note

This function should be supported by the device.

1. In the top left corner of the Home page, select → **Passing Management → Access Control → Access Control Application → Multi-Factor Authentication** .
2. Click **Add**.
3. Enter the rule name.
4. Select a door from the following area list.
5. Set the access mode of the door.

   Unlock After Access Granted

   The door will be unlocked automatically after the persons swiping 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 swiping their cards (or other type of credentials) on the card readers of the door and the access is granted, a window will pop up. The operator should confirm to unlock the door remotely and then the door will be unlocked successfully.

   Enter Super Password After Granted

   After the persons swiping 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.
6. Set the access schedule to define in which time period, the persons are authorized to access the door.

   Note

   The default and customized access schedules are displayed in the drop-down list. You can click **Add** to customize a new schedule. For details, refer to ***Set Access Schedule Template*** .

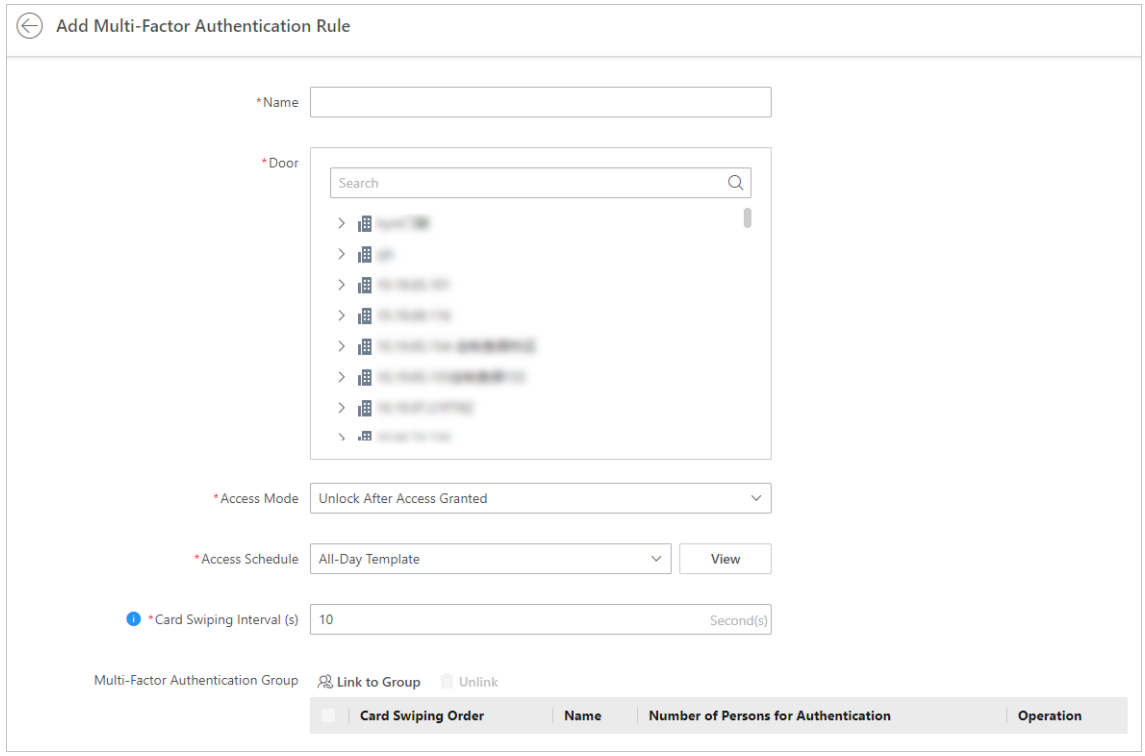


Figure 26-8 Add Multi-Factor Authentication Rule

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 **Link to Group** to set the access group(s) to define who have the permission to access the door.

Note

When adding groups, if you check **Select All Persons**, all persons who matched the search conditions you set will be selected.

Card Swiping Order

Click ↑ or ↓ in the **Operation** column to set the authentication order of different access groups.

Number of Persons for Authentications

Define how many persons should authenticate on the card reader.

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.

Note

This value should be no larger than the number of persons in the access group.

9. Click **Add**.

Add Multi-Factor Authentication Group

To perform the multi-factor authentication function, you need to create a multi-factor authentication group and appoint persons as the member of the group first. Persons in the group have the permission for multi-factor authentication of specific doors.

Steps

1. In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Access Control Application** .
2. Click **Multi-Factor Authentication** on the left.
3. Click **Multi-Factor Authentication Group Management** on the top.
4. Click **Add** to open the Add Multi-Factor Authentication Group panel.
5. Enter the multi-factor authentication group name.
6. Click **Add** to select group members from the person list.

Note

When adding groups, if you check **Select All Persons**, all persons who matched the search conditions you set will be selected.

7. Click **Add**.

Add User to Receive Remote Door Open Request

To handle remote door open requests on the Control Client, you need to appoint persons to receive these requests beforehand.

Steps

1. In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Access Control Application** → **Multi-Factor Authentication** .
2. Click **User to Receive Remote Door Open Request** on the top.
3. Click **Add** to open the User to Receive Remote Door Open Request pane.
4. Select users from the list.

Note

If you check **All**, all persons will be selected.

5. Click **Add**.

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. In the upper-left corner of the Home page, select → **Passing Management** → **Access Control** → **Access Control Application** → **Authentication Mode** .
2. Select the **Card Reader Authentication Mode** tab.
3. Select an area from the area list.
4. Click a door name on the right.
5. 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.
6. 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.

7. **Optional:** Click **Copy To** in the upper-right corner to apply the settings to other doors.
8. Click **Save**.

Set Person Private Authentication Mode

In some situations, different persons need to use different authentication modes for accessing the same access point, and a person may need to use different authentication modes for accessing different access points. Setting the private authentication modes for different persons can provide an easy way for them to authenticate by less credentials or enhance the security of some important places by forcing them to use more credentials.

Steps

Note

The person's private authentication mode has higher priority than the existing authentication mode of the device.

1. In the upper-left corner of the Home page, select → **Passing Management → Access Control → Access Control Application → Authentication Mode** .
2. Select the **Private Authentication Mode** tab.
3. Select a department from the left list.

   All persons in the department will be listed on the right panel.
4. Click in the Operation column to open the Authentication Device pane.
5. Click **Add**, check the device(s) from the list, and select the authentication mode from the drop-down list for the selected device(s).
6. Click **OK** to add the device(s) for authentication for the person.
7. **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.
8. **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.

Add Entry and Exit Counting Group

The entry and exit counting group is used to group the access points in a certain region. You can set certain access points as the region border. Only the persons accessing these access points are counted, and other access points inside the region are ignored. 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

Note

After setting entry & exit counting group, you can perform entry & exit counting in **Access Control Retrieval → Entry & Exit Counting** on the Control Client to count the number of people who are still in the region and view who enters/exits this region.

1. In the top left corner of the Home page, select → **Passing Management → Access Control → Access Control Application → Entry and Exit Counting Group** .
2. Click **Add**.
3. Create a name for the group.
4. Click **Add** and select doors from the area list.
5. Set the entering or exiting direction of the card readers of the selected access points.

   The access records on the entering card reader will be counted as a person enters this region while the access records on the exiting one will be counted as a person exits this region.
6. Click **Save**.

   The entry & exit counting group is added to the table and you can view the access points in the group.

Add Audio Broadcast

You can add daily audio broadcasts for daily use and add particular broadcasts for holidays or specific days. After adding broadcasts, you can apply them to devices.

Steps

1. In the top left corner of Home page, select → **Passing Management → Access Control → Access Control Application → Audio Broadcast** .
2. Click **Add Audio Broadcast**.
3. Select the broadcast device(s).
4. Enable the daily broadcast.

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.

5. In the Particular Broadcast area, click **Add** to add particular broadcasts.

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

- On the days without particular broadcasts, daily broadcasts will be played. 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**.

6. Click **Add**.

   The settings will be applied to the selected device(s).

7. **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**. • 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.

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. In the upper-left corner of the Home page, select → **Passing Management → Access Control → Access Control Application → 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 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.

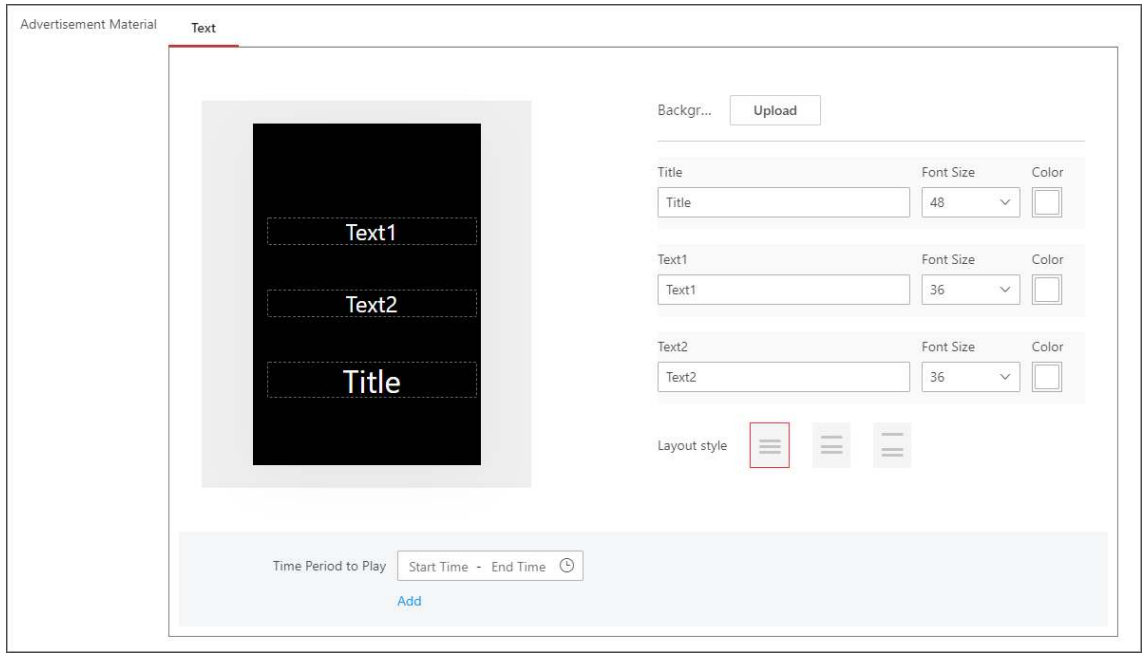


Figure 26-9 Add Text in Advertisement

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).
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.

26.2.8 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.

In the top left corner of the Home page, click → **Passing Management** → **Access Control** → **Troubleshooting** .

Check Credential Status

Select the **Credential Status** tab to view the status of the added credentials.

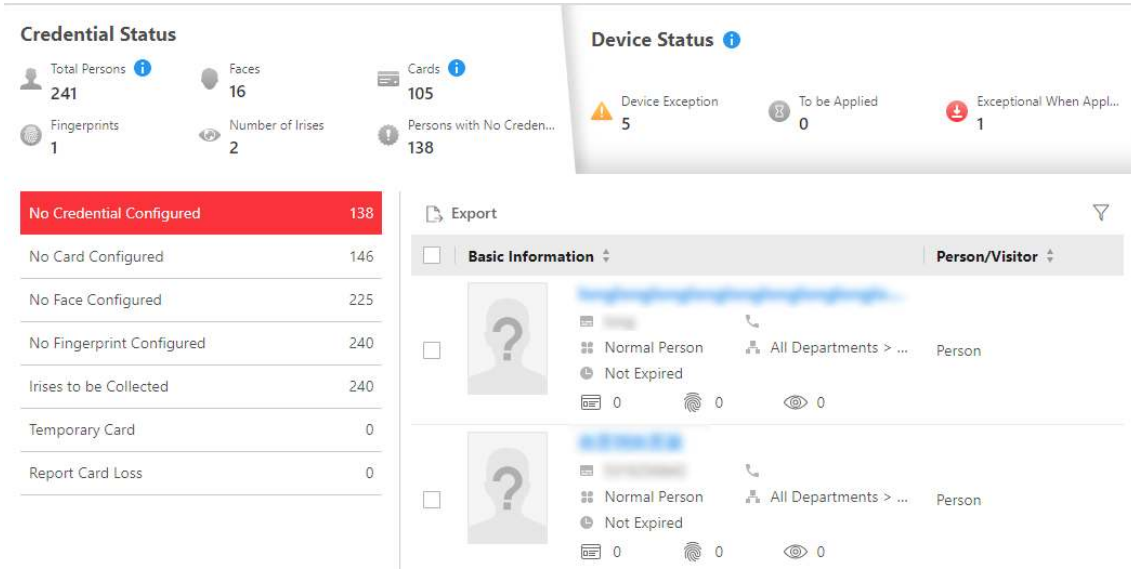


Figure 26-10 Credential Status

There are 6 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 Status** 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.

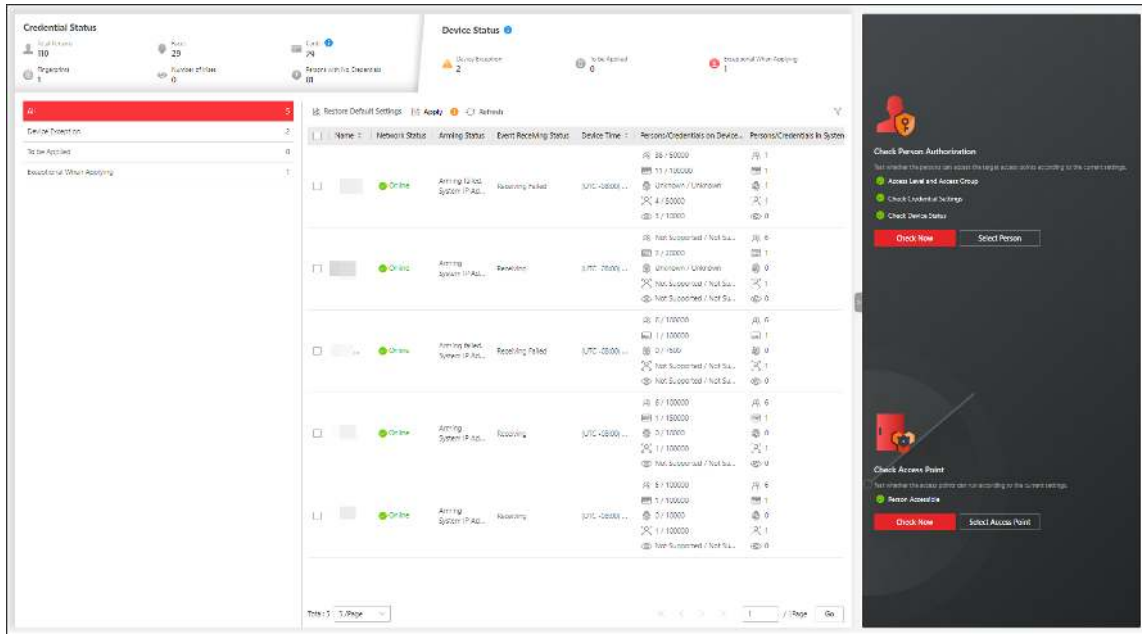


Figure 26-11 Device Status

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.

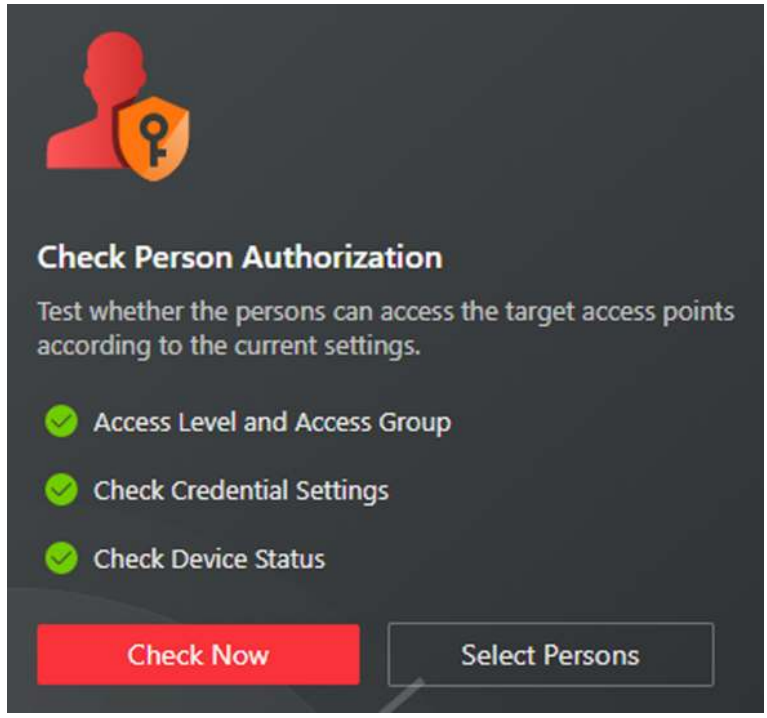


Figure 26-12 Check Authorization Settings

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.

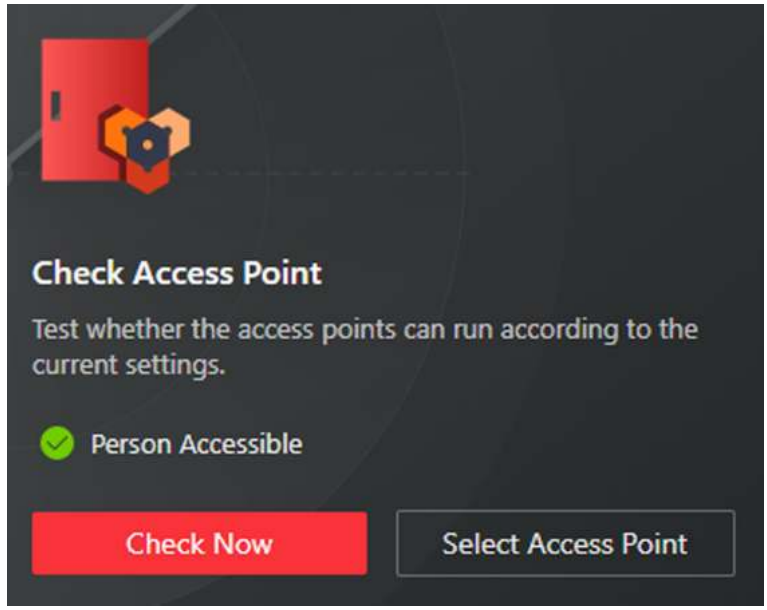


Figure 26-13 Check Access Point Settings

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.

26.3 Door and Elevator Control

With emergency operation group, you can control door and elevator status in a batch when an emergency happens. For example, after grouping the doors of a school's main entrances and exits into one emergency operation group, school's security personnel can lock down the doors 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.

Note

Only the users with Administrator or Operator role can control all doors/floors in a batch.

You can control all or part of the doors and floors in the selected site andarea according to your need. When the emergency is over, you can restore the status to Access with Credential.

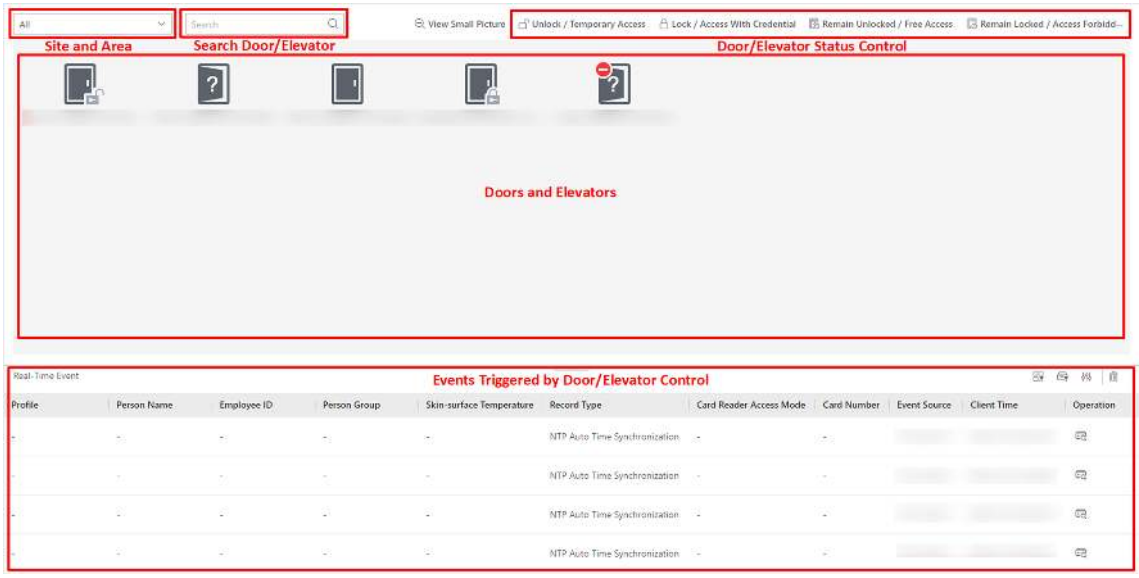


Figure 26-14 Access Control Real-time Monitoring

26.3.1 Start Live View of Access Control / Elevator 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.

Before You Start

Make sure you have added the devices to the platform.

Steps

1. In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Real-Time Monitoring** .
2. Click a device and select **Live View**.

   The live view window of the device will be displayed on the right.

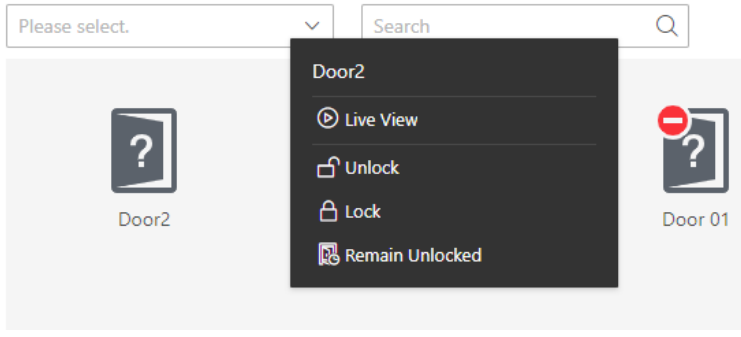


Figure 26-15 Start Live View

3. Hover the cursor on the live view window to show the tool bar at the bottom. You can click different buttons according to your need.

   Example

   You can click to start two-way audio with persons by the device.

26.3.2 View Real-Time Access Event

In the Access Control module, you can view events triggered by doors and elevators. You can also control door and elevator status according to the event details, search for more event information, and so on.

In the top left corner of the Home page, select → **Passing Management** → **Access Control** → **Real-Time Monitoring** .

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.

Search 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. **Note** To view the columns about electrostatic discharge testing, you can select **Resistance Value of Hand / Left Foot / Right Foot (KΩ)** and **Failed Part**.
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-switch to the Latest Record** to display the person/visitor information contained in the newest access record. If you uncheck the **Auto-switch to the Latest Record**, the platform will display the person/visitor information contained in the historical access records. The platform supports hiding the window.

26.3.3 Door Control

You can change the status of all doors in a site or doors in specific emergency operation groups to locked, unlocked, remaining locked, or remaining unlocked.

Note

Make sure you have grouped doors into an emergency operation group. See details in ***Add Emergency Operation Group*** .

In the top left corner of the Home page, select → **Passing Management → Access Control → Real-Time Monitoring** .

Control all or part of the doors in the current site.

Unlock

When a door is locked, if you unlock the door, it will be unlocked. When open duration is over, the door will be locked again automatically.

Click **Unlock / Temporary Access → All** to unlock all doors in the current site.

Click **Unlock / Temporary Access → Part** and select the emergency operation groups you want to unlock. Click **OK** to unlock the doors in the selected emergency operation groups.

Note

For details about setting the door's open duration, see ***Edit Door for Current Site*** .

Lock

When the door is unlocked, if you lock the door, it will be closed and locked. The person who has the access permission can access the door with credentials.

Click **Lock / Access with Credential → All** to lock all doors in the current site.

Click **Lock / Access with Credential → Part** and select the emergency operation groups that you want to lock. Click **OK** to lock the doors in the selected emergency operation groups.

Remain Unlocked

Doors will be unlocked. All persons can access the door with no credentials required (free access). 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.

Click **Remain Unlocked / Free Access → All** and all doors in the current site will remain unlocked.

Click **Remain Unlocked / Free Access → Part** and select the emergency operation groups. Click **OK** and the doors in the selected emergency operation groups will remain unlocked.

Remain Locked

Door will be closed and locked. No person, except for the super users, can access the door even with authorized credentials. This function is applicable for situations such as preventing a thief in the building from getting away.

Click **Remain Locked / Access Forbidden → All** to lock down all the doors in the site.

Click **Remain Locked / Access Forbidden → Part** and select the emergency operation groups. Click **OK** and the doors in the selected emergency operation groups will remain locked.

Note

For setting person's super user permission, refer to ***Role and User Management*** .

26.3.4 Elevator Control

You can change the status of all floors in a site or floors in specific emergency operation groups to temporary access, access with credential, free access, or access forbidden.

Note

Make sure you have grouped floors into an emergency operation group. See details in ***Add Emergency Operation Group*** .

In the top left corner of the Home page, select → **Passing Management → Access Control → Real-Time Monitoring** .

Control all or part of floors in the current site.

Temporary Access

During the temporary access time, the persons can access this floor with no credentials required. After the access time, the floor will recover to Access with Credential status.

Click **Unlock / Temporary Access → All** to set all the floors in the current site to Temporary Access.

Click **Unlock / Temporary Access → Part** and select one or more emergency operation groups to set all floors in the group(s) to Temporary Access.

For details about setting the temporary access duration, see ***Edit Elevator for Current Site*** .

Access with Credential

Person who has the access permission can access this floor with credentials.

Click **Lock / Access with Credential → All** to set all the floors in the current site to Access with Credential.

Click **Lock / Access with Credential → Part** and select one or more emergency operation groups to set all the floors in the group(s) to Access with Credential.

Free Access

All persons can access this floor with no credentials required.

Click **Remain Unlocked / Free Access → All** to set all floors in the current site to Free Access.

Click **Remain Unlocked / Free Access → Part** and select one or more emergency operation groups to set all floors in the group(s) to Free Access.

Access Forbidden

No person, except the super users, can access this floor even with authorized credentials. This function is applicable for situations such as preventing a thief in the building from getting away.

Click **Remain Locked / Access Forbidden → All** to set all floors in the current site to Access Forbidden.

Click **Remain Locked / Access Forbidden → Part** and select one or more emergency operation groups to set all floors in the group(s) to Access Forbidden.

Note

For setting person's super user privilege, refer to ***Role and User Management*** .

26.4 Subscribe to Device and Access Events

You can subscribe to device events and access events, so that when these events occur, you can see the real-time event records via the Web Client and Mobile Client.

Follow the steps to enable the subscription to device and access events.

Steps

1. In the top left corner of the Home page, select → **Passing Management → Access Control → Basic Configuration → Device Event Subscription** .
2. Select an event category from **Device Event**, **Normal Access Event**, and **Abnormal Access Event**.
3. Switch on the event types to subscribe to these events.
4. **Optional:** Switch off the event types whose real-time event records you do not want to receive.

   Note

   If you switch off an event type, the Web Client and Mobile Client will no longer receive real-time event records of the event. However, you can still search for the device/access records via the Web Client. For details, see ***Search Access Records*** and ***Search Data Recorded on Access Control Devices and Elevator Control Devices*** .
5. Click **Save** to save the settings.

What to do next

View the real-time event records of the device and access events that you subscribe to. For details, see ***View Real-Time Access Event*** .

26.5 Set User to Receive Access Control Calls

You can specify users to receive calls from the access control devices on the Control Client, and then the users can remotely perform the access control, such as remotely open door.

In the top left corner of the Home page, select → **Passing Management → Access Control → Basic Configuration → Call Recipient Settings** .

Click **Add** to select user(s) to receive access control calls on the Control Client.

26.6 Synchronize Access Records to System Regularly

Access records stored in devices can be synchronized to the system for central management. You can specify a fixed time in order to automatically synchronize access records from devices to the system at the specified time every day.

Click → **Passing Management** → **Access Control** → **Basic Configuration** → **General** .

In the Synchronize Records (Scheduled) area, switch on **Synchronize (Scheduled)**, set a fixed time, and click **Save** to synchronize access records from the devices to the system regularly.

26.7 Enable Open Door via Bluetooth

You can enable open door via bluetooth and select a door opening mode.

Note

You can enable persons to open door via bluetooth in **Person Management** → **Person** .

On the top, select **Access Control**. Then, select **Basic Configuration** → **General** on the left. On **Open Door via Bluetooth**, choose from **Auto Open Door** and **Open Door Manually**.

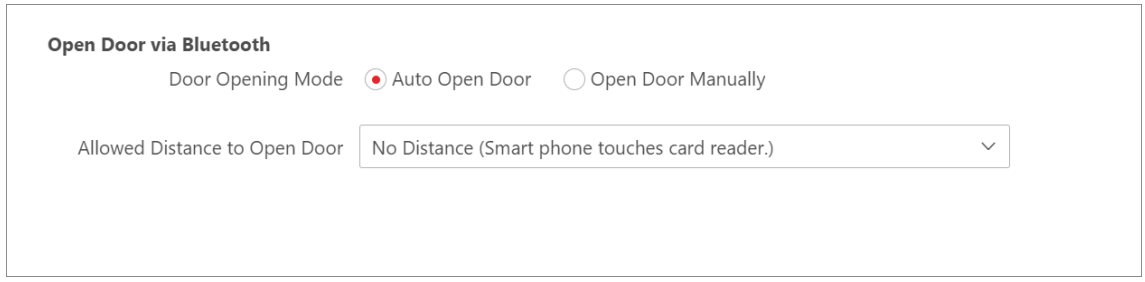


Figure 26-16 Open Door via Bluetooth

Auto Open Door

The door will open automatically when you get close to the door in a specific distance.

Allowed Distance to Open Door

You can select an allowed distance to open the door. You can choose from **Near (The distance between smart phone and card reader is about 20 cm)**, **Far (The distance between smart phone and card reader is about 300 cm)**, and **Customize (Enter a custom RSSI value)**.

Customize RSSI Value

You can set an RSSI value (a negative integer ranging from -1000 to -1). If the RSSI value of a nearby door is higher than or equal to the value you entered, the door will open automatically. It is recommended that you set this value according to the actual RSSI value displayed on the Mobile Client.

Open Door Manually

You can manually open a specific door on the Mobile Client.

26.8 Search Access Records

You can search for persons' access records triggered on specified access points (including doors and elevators) via the Client 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.

Before You Start

Make sure you have configured the access point event. For details, refer to ***Add Normal Event and Alarm*** .

Steps

1. In the upper-left corner of the Home page, select → **Passing Management → Access Control → Search → Identity Access Search** .
2. **Optional:** Import access records to the system.
   - Import access records from the device(s).
     a. Click **Import Event → Import from Device** to enter the Import from Device page.
     b. Select the device(s) from the device list.
     c. Optional: Switch on **Specified Time Range** and set the start time and end time to import access records generated in the specified time period.

     Note

     - If the device has uploaded access record(s) to the system before, switching on **Specified Time Range** is not required and access 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 access record to the system before, you must switch on **Specified Time Range** for importing access records from the selected device(s).

     d. Click **OK** to start importing.

     A window will pop up to display the importing progress and the failure details.
   - Import access records from the file which is exported from the device.
     a. Click **Import Event → Import from File** to enter the Import from File page.
     b. Click to select the file to be imported.

     Note

     Only the encrypted file can be imported.

     c. Enter the password in the **Password** field.
     d. Click **OK**.
3. In the **Time** drop-down list, select the time during which the access records are generated.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

4. **Optional:** In the **Access Point** area, click , select the area on the left list, and select door(s) and elevator(s) or select all on the right list.
5. **Optional:** In the **Event Type** area, click to select the event type(s).
6. In the **Authentication Result** drop-down list, select an access result type to quickly filter access granted records or access denied records.
7. Set the searching mode.
   - a. Select **Person/Visitor** as the searching mode.
   b. Select **Select Person** or **Fuzzy Matching** as the searching mode.

   Select Person

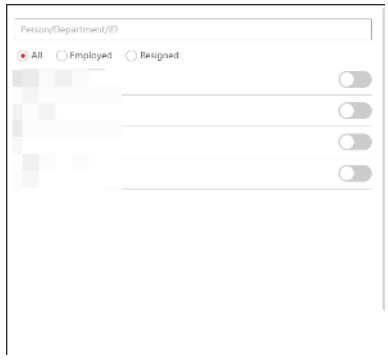
   Click to select the person(s)

   Note

   - You can click **More** to enable custom information items and enter the keyword in the text field to search for matched persons.

     Note

     Make sure you have customized additional information about persons. For details about customizing additional information, refer to ***Object Missing*** .
   - If you check **Select All Persons**, all persons who matched the search conditions you set will be selected.
   - You can check **Include Sub Department** to display the persons of sub-departments.
   - You can click **More** to select **Employed**/**Resigned** to select the employed/resigned person(s).

   Fuzzy Matching

   Enter a keyword to search for persons whose name contains the keyword.

   c. Click **Add** to select the person(s), or enter the keywords of the person's name for fuzzy matching.
   - a. Select **Card No.** as the search mode.
   b. Enter the card number.
8. **Optional:** Switch on **Temperature Status** and select **Normal** or **Abnormal**.

9. **Optional:** Switch on **Mask Wearing Status** and select **Wearing Mask** or **No Mask**.
10. Click **Search**.

    Matched access records are listed on the right.
11. **Optional:** Perform the following operations after searching for access records.

Custom Column Items	On the top right, click to select column items to be displayed. You can click **Reset** to select again.
View Record Details	Click the person name in the Full Name column to view the record details, such as person information, and access information.
Filter Search Results by Person Type	Click next to the column name **Person** and select persons to filter the search results.
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. 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 file on your PC, including the event details, the person information, person profile, recorded video file (if configured), etc.
Export All Searched Records	Click **Export** in the upper-right corner to save the searched access record details in your PC. You can select the file format as an Excel or a CSV file, and select items to export. If you select **Excel**, you can check **Profile Picture** to save the captured pictures and person profile photos. **Note** Up to 500 records can be exported each time.

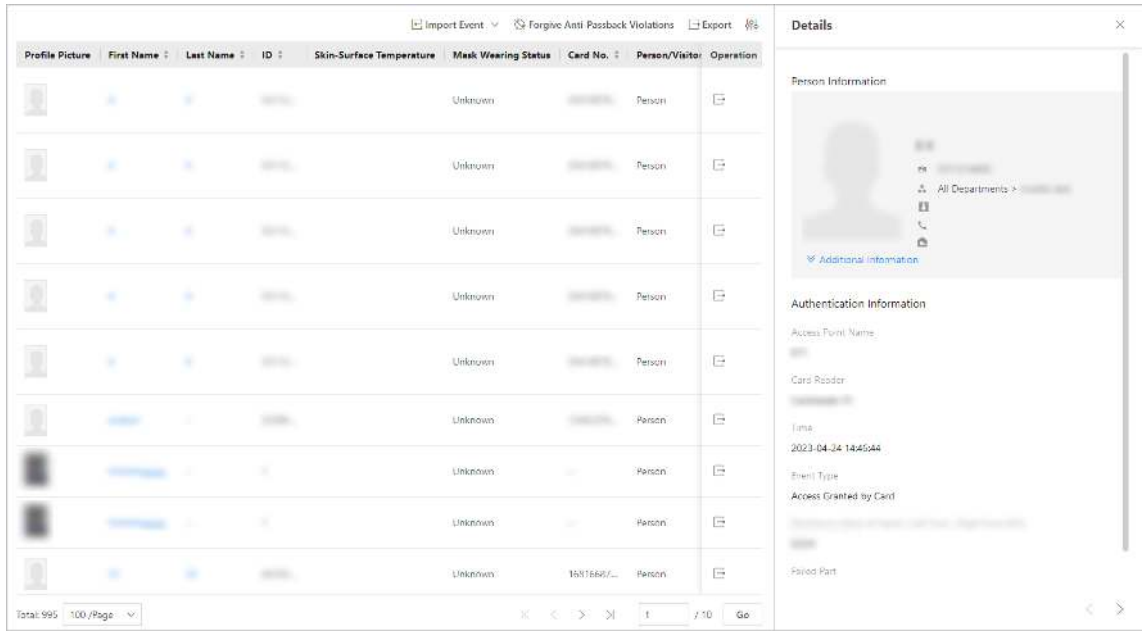


Figure 26-17 Real-Time Events

26.9 Search Data Recorded on Access Control Devices and Elevator Control Devices

The records can be events/alarms triggered by human behaviors detected by devices and those triggered by devices (such as device faults). You can search for the records in different dimensions according to your needs.

Steps

1. In the upper-left corner of the Home page, select → **Passing Management** → **Access Control** → **Search** → **Device Recorded Data Retrieval** .
2. In the drop-down list, select a time range for searching.

Note

You can select **Custom Time Interval** to set a precise start time and end time.

3. Switch on the resource types where you want to search for records.

Access Point(s)

Access points include doors of access control devices and video intercom devices, and floors of elevator control devices. The records 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 data recorded in these devices can cover all events triggered by devices (such as device faults).

Alarm Input

The alarm inputs included in devices. The records are arming status changes.

4. Select the event source(s) and event type(s) for each switched-on resource type.

Source

Select the sources for events. For access points and alarm inputs, select the area on the left list, and then select the resources or select all on the right list.

Event Type

Select the types of events for each resource type.

5. Click **Search**.

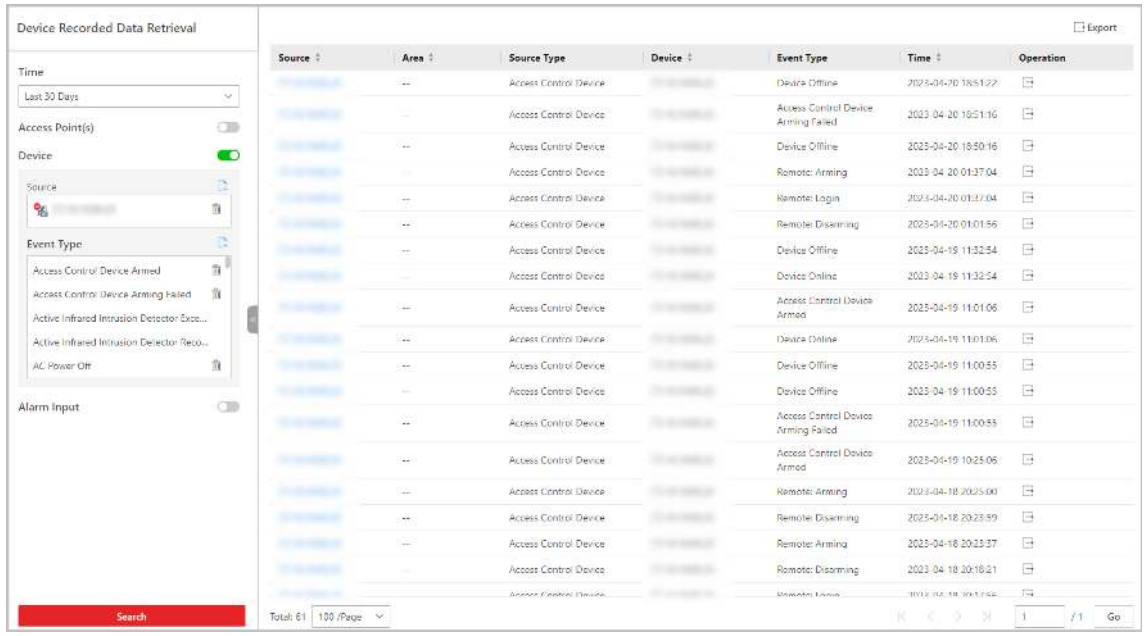


Figure 26-18 Device Recorded Data Retrieval

6. **Optional:** Perform further operations on the searched records.

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 or a CSV file.

26.10 Perform Entry & Exit Counting

By grouping the doors (adding entry & exit counting group), the system provides counting functions based on the entry and exit records on these doors. With this function, you can check who enters/exits this region and how many persons still stay in this region. The function is applicable for certain emergency scene. For example, during a fire escape, all people are required to exit the region.

Before You Start

Make sure you have added entry & exit counting groups to group the doors. See ***Add Entry and Exit Counting Group*** .

Steps

Note

Currently, the platform only supports searching persons with access records in the last 24 hours.

1. In the top left corner of Home page, select → **Passing Management → Access Control → Search → Entry & Exit Counting** .
2. In the **Source** list, select an entry & exit counting group.
3. In the **Entry & Exit Counting Type** drop-down list, select the type of persons you want to search.

   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.
4. Click **Search**.

   All matched access records will be listed, showing information such as person details, location of last access, etc.
5. **Optional:** Perform further operations after searching.

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.).

Note

Up to 100,000 records can be exported each time.

Chapter 27 Visitor Management

The system provides an entire process for visitor management from reservation to check-out. You can group visitors to different visitor groups for convenient management, determine the areas where the visitors can access, and assign visitors access credentials like visitor passes.

On the Web Client, 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.

The Visitor Information Overview page shows the wizard for visitor management and the chart of the visit trend today.

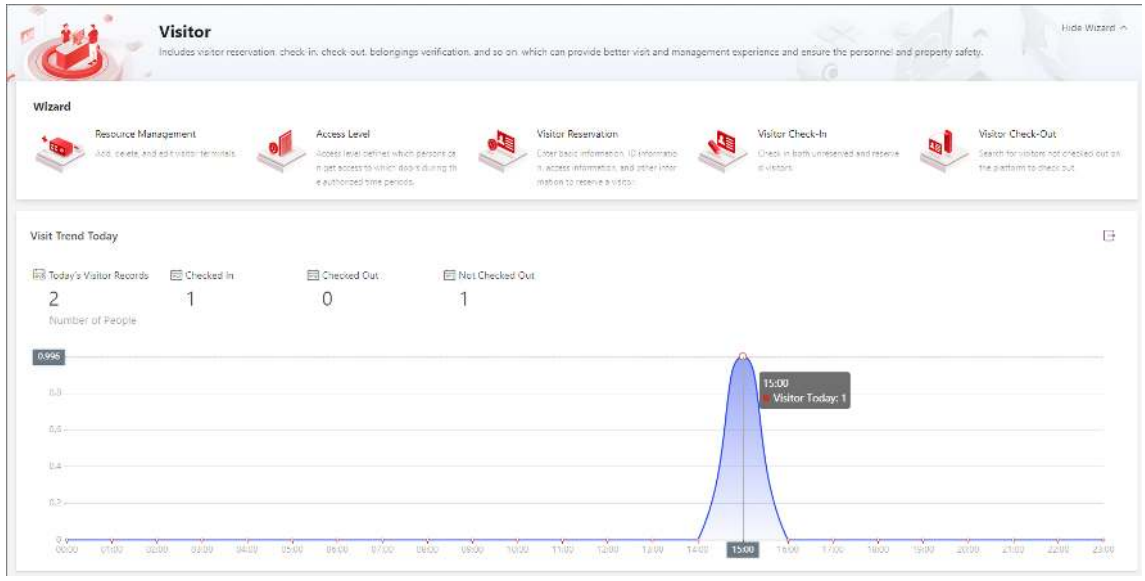


Figure 27-1 Visitor Information Overview

Wizard

The wizard shows you the entire process for visitor management, including the resource management, access level management, visitor reservation, visitor check-in, and visitor check-out. Move your cursor to each section and click to go to the corresponding page for configurations and operations. For example, you can move your cursor to the Resource Management section and click to go to the page for managing visitor terminals.

Visit Trend Today

You can view the variation trend of the number of visitors on the current day through a line chart. Also, you can view the numbers of today's visitor records, checked-in visitors, checked-out visitors, and not-checked-out visitors.

On the line chart, you can perform the following operations:

- Move the cursor to a specific point on the chart to view the number of visitors at the corresponding time.
- Click on the right side to export the chart to the local PC as a file in the format of PDF, PNG, or JPG.

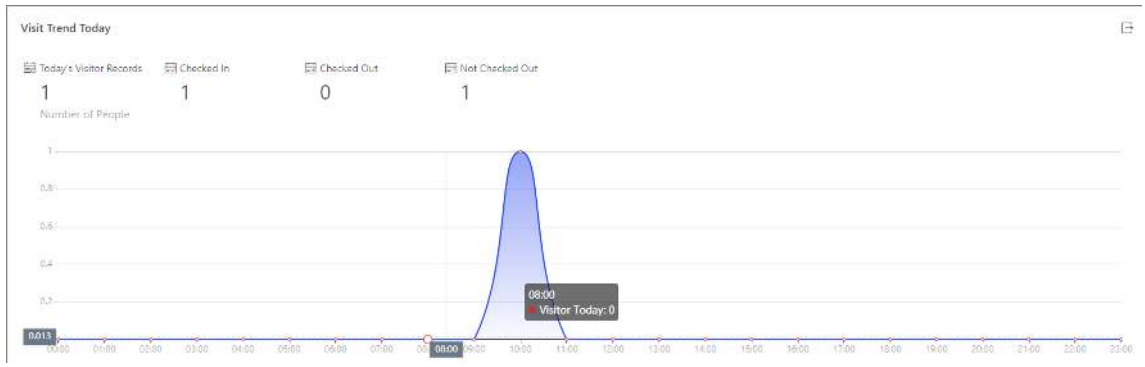


Figure 27-2 Visit Trend Today

27.1 Configurations 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.

27.1.1 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. For details about permission settings, see ***Add Role*** .

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.

27.1.2 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. See details in ***Add Access Level*** .

Steps

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**.

   The added access levels will be displayed in the access level list. You can view its accessible access points and time periods.
5. **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. See ***Set Access Schedule Template*** for details about setting the access schedule template.
View Access Point Details	Click in the Access Point column to view the name of related access points.
Set Default Access Level	Select an added access level and switch on the button in the Default Access Level column. 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 Self-Service Reservation Parameters***). 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 ***View Visitor Information***).
Delete Access Levels for Visitors	Select access levels and click **Delete** to delete the selected access level. 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.

27.1.3 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. See ***Add Access Level for Visitors*** for details.
- Make sure you have added the visitor terminal to the platform. See ***Manage Visitor Terminals*** for details.

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.

27.1.4 Set Self-Service Reservation Parameters

Self-service reservations refer to visit reservations made by visitors themselves. You can 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. For details about setting the default access level, see ***Add Access Level for Visitors*** .

To configure a different access level for a visitor, you need to make a reservation for them. For details, see ***Reserve a Visitor*** .

1. On the top left of the Web Client, select → **Passing Management → Visitor → Basic Configuration → Self-Service Reservation** .
2. 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 allow different users to manage their own visitors independently.
3. **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.

   Self-Service Reservation Approval

   If you enable this, after the visitor self-service reservation, you need to review the visitor information on the Visitor to Be Approved page. After review, the visitor will be added to the selected visitor group. See ***Review Visitor Reservations*** for details about how to review.

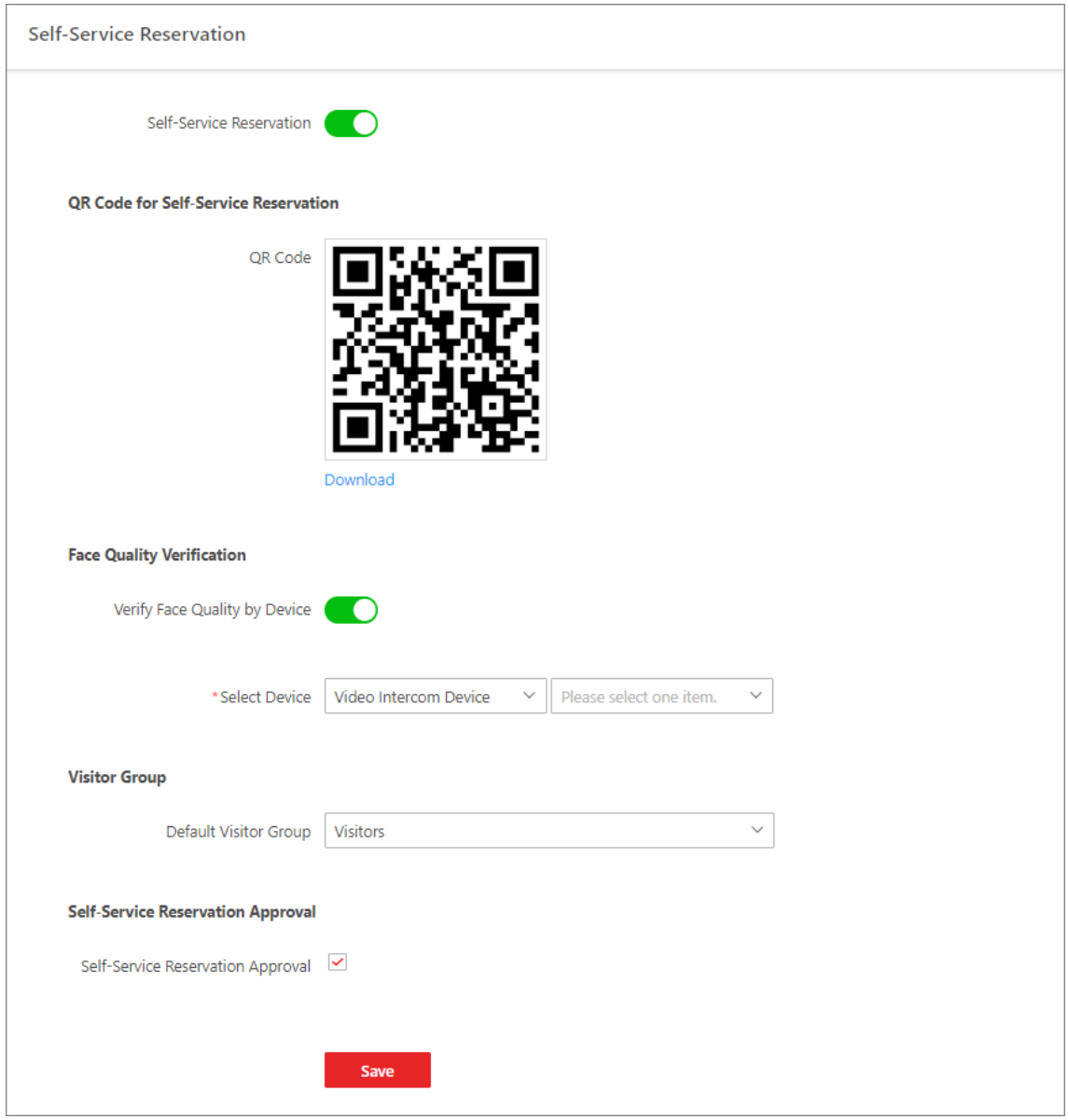


Figure 27-3 Self-Service Reservation

4. Click **Save**.

27.1.5 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 and click **Add**.

   Note

   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 27-4 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.

27.1.6 Add Visitor Email Template

You can set email templates (including specifying email type, email subject, and content) for sending emails automatically so that the platform can send emails to the specified recipient according to the predefined email template.

Before You Start

Before adding the email template, you should set the sender's email account first. See ***Configure Email Account*** for details.

Steps

1. In the top left corner of Home page, select → **All Modules** → **Visitor** → **Basic Settings** → **Email Template** .
2. Click **Add**.
3. Enter the required parameters.

   Email Type

   Define when the platform automatically sends an email containing the information you predefined to the specified recipient.

   Send Email When Reservation Approved

   The platform automatically sends an email to the specified recipient when a visit reservation is approved.

   Send Email When Checked-In

   The platform automatically sends an email to the specified recipient when a visitor checks in.

   Send Email When Reservation Rejected

   The platform automatically sends an email to the specified recipient when a visit reservation is rejected.

   Recipient

   Set the type of the email recipient (visitor or host).

   Assume that you have set **Email Type** to **Send Email when Reservation Approved** and **Recipient** to **Visitor**, a visitor will receive an email when their visit reservation is approved, as long as their email address is provided in the reservation.

   Name

   Create a name for the template.

   Subject

   Enter the email subject as desired. You can also click the button in the lower part of the window to add the related information to the subject.

   Email Content

   Define the report content to be sent. You can also click the buttons below the **Content** parameter 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.
4. Finish adding the email 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.

5. **Optional:** Perform the following operation(s) after adding the email template:

Edit Template	Click ✎ in the Operation column to edit template details.
Delete All Templates	Click **Delete All** to delete all the added templates.

Note

On the email template list page, there are two default templates. You can view or edit default templates but not delete them.

27.1.7 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.

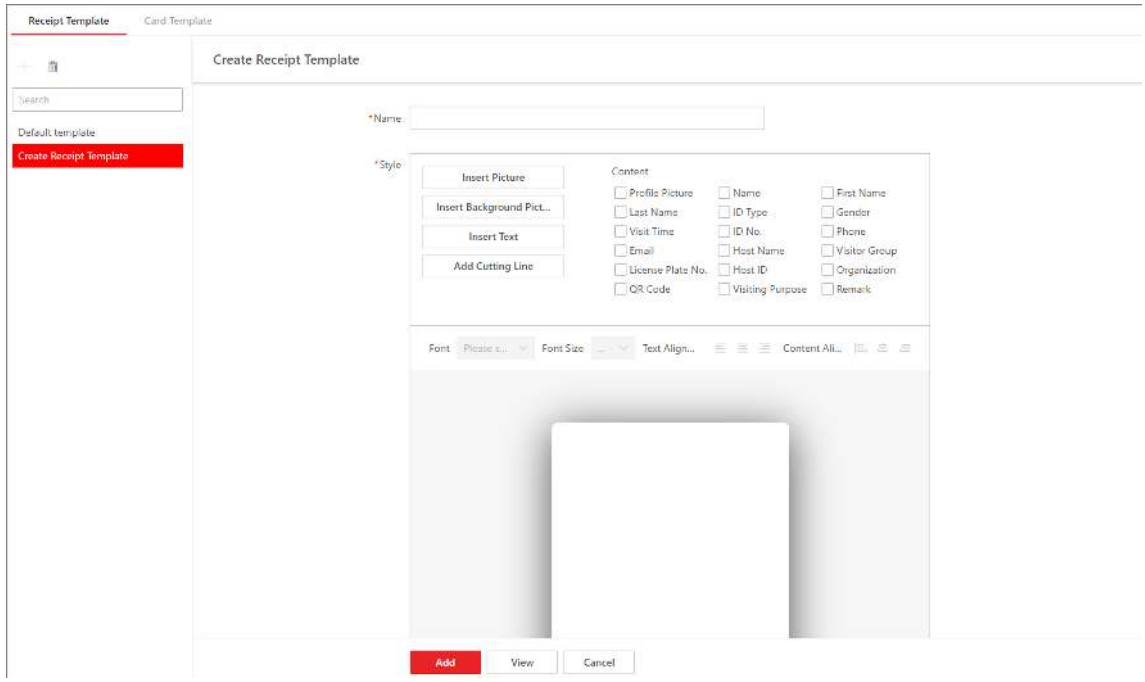


Figure 27-5 Create Receipt Template Page

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.

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.

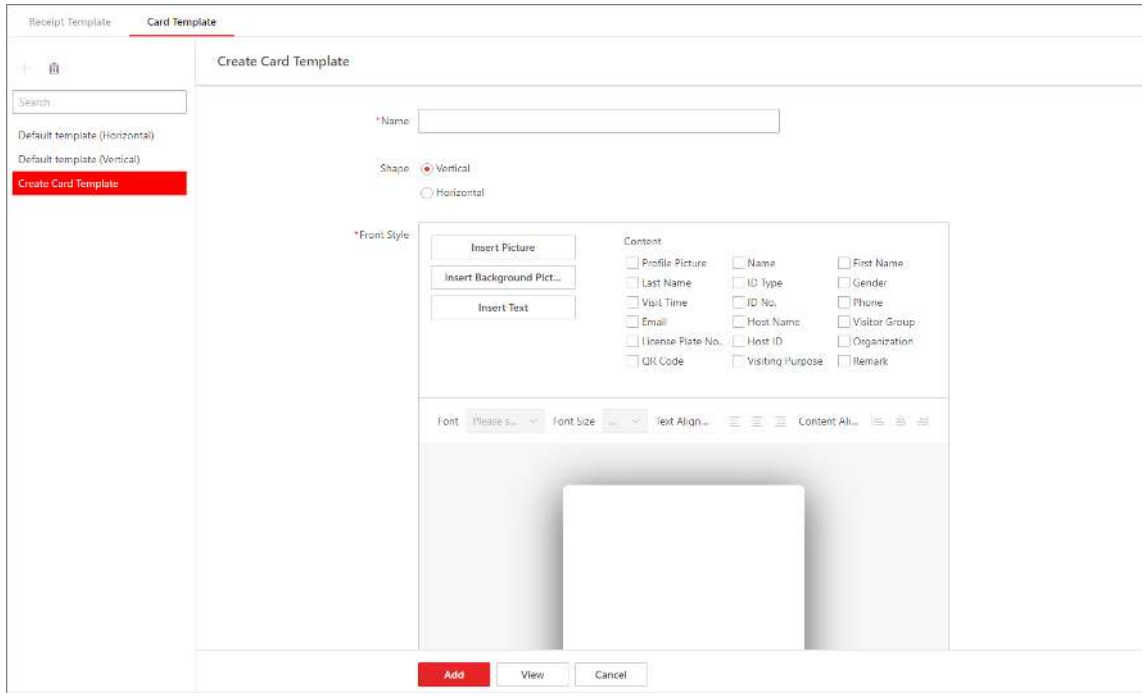


Figure 27-6 Create Card Template Page

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. You can set the font, font size, 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 .

27.1.8 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. See ***Reserve a Visitor*** or ***Check In a Visitor Without Reservation*** for details.

   Visiting 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.

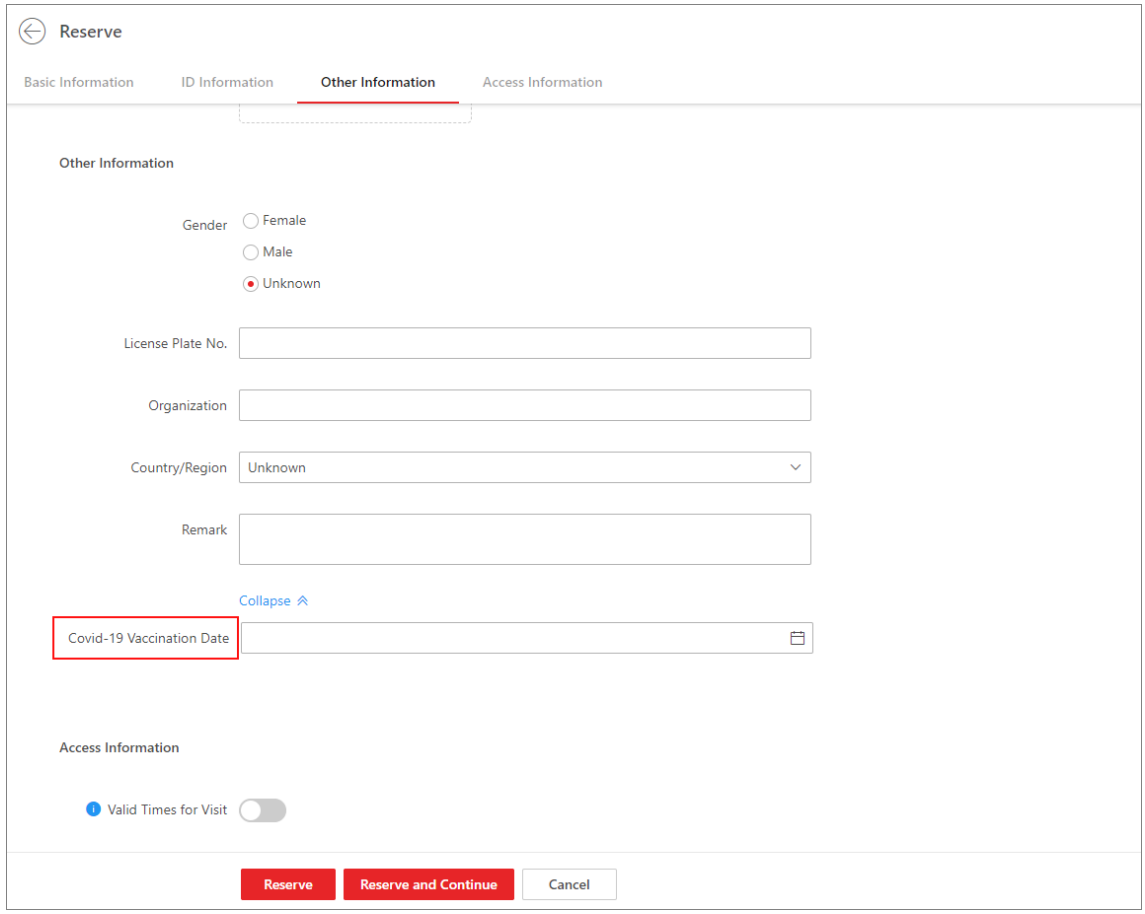


Figure 27-7 Example

Custom Field for Reservation & Check-In

Check fields to display on the visitor reservation page and the visitor check-in page.

Moreover, you can turn on the switches in the Set as Required column to set corresponding fields as required fields.

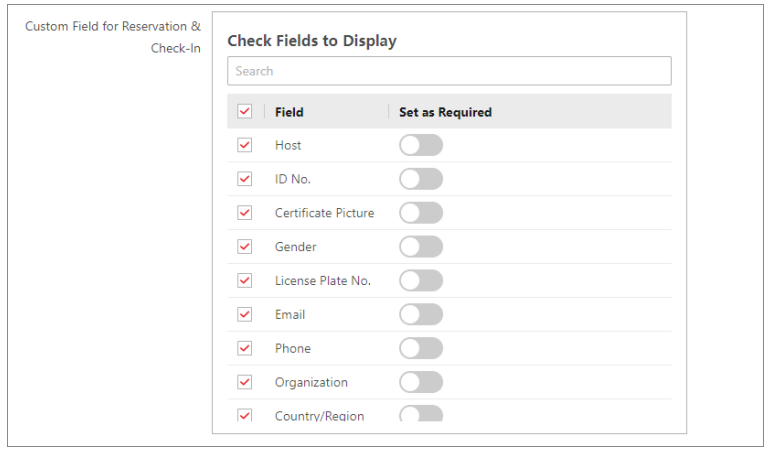


Figure 27-8 Check Fields to Display

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. See ***Manage Visitor Terminals*** for details.

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.

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*** .
  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 Email 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*** .
  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 Email 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.

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.

27.1.9 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

For details about editing the entry & exit rule, see ***Configure Entry & Exit Rules*** .

Note

This rule cannot be deleted.

27.2 Watch List Management

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.

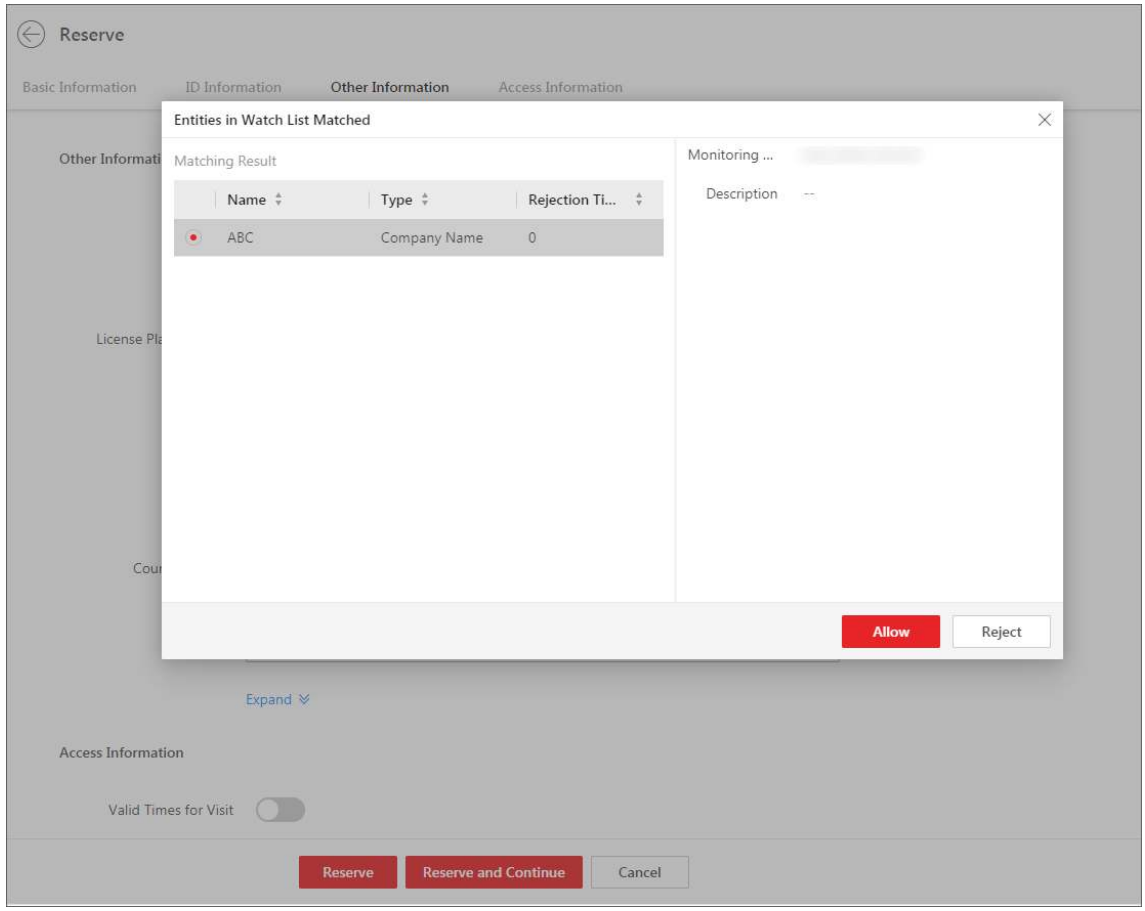


Figure 27-9 The Entities in Watch List Window

27.2.1 Add Entity Type

You can add and define the types of entities to be monitored.

Steps

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. **Optional:** Enter a remark for the type.
6. Click **Add** to finish adding the type.
7. **Optional:** 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.

27.2.2 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.

Steps

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**.

27.2.3 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.

Steps

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.
   - For **Person**, set other information including the first name, last name, category, effective period, ID type, ID number, and ID picture.
   - For **Company**, set other information including the company name, category, and effective period.
   - For **Country/Region**, set other information including the country/region, category, and effective period.

   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**. For details, see ***Add Entity Type*** .

   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. **Optional:** 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.
Delete Entities	Select entities and then click **Delete** to delete them. Or hover the cursor over and then click **Delete All** to delete all entities.

27.2.4 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.

Steps

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**.

   The selected visitors will be displayed on the pane.

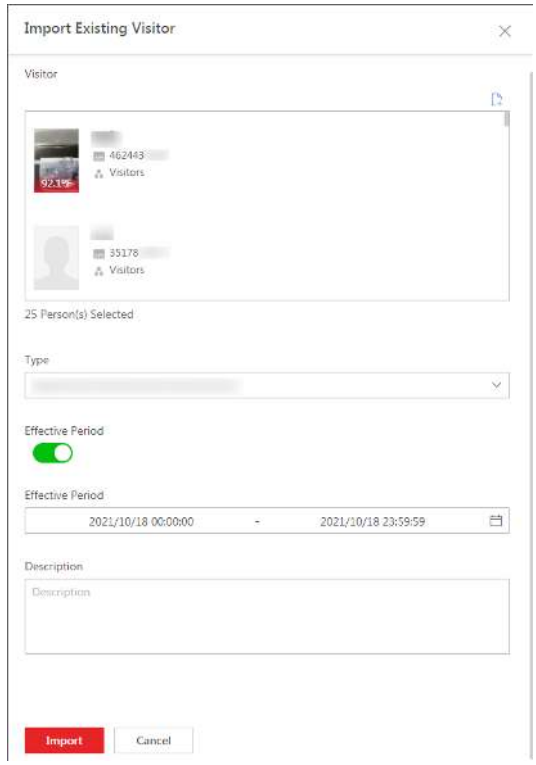


Figure 27-10 Import Existing Visitor

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**. For details, see ***Add Entity Type*** .

   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**.

   The visitors will be displayed in the watch list.

6. **Optional:** 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.
Delete Existing Visitors from Watch List	Select visitors and then click **Delete** to delete them.

Or hover the cursor over ⌄ and then click **Delete All** to delete all visitors.

27.3 Visitor Reservation

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.

27.3.1 Reserve a Visitor

You can make a reservation for one visitor by entering the visitor and host information on the platform.

Before You Start

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 ***Configurations Before Visitor Management*** for details.

Steps

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 basic information for the visitor, such as the name, host, visit purpose, estimated entry time, visitor group, email, and phone. 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 Take ID Photo as Visitor Profile Picture on the Basic Parameters page in order to read the ID photo and set it as the visitor profile picture. 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.

4. Set ID information for the visitor, including the ID type, ID No., and ID picture.
5. Set other information.
   1) Set the license plate number, organization, country/region, and remark.

Note

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.

2) **Optional:** Click **Expand** to show the additional information fields and then enter additional information of the visitor.

Note

Make sure you have set custom visitor attributes, otherwise the additional information fields will be unavailable. For details about how to set custom visitor attributes, see ***Set Basic Parameters*** .

6. Set the access information.

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.

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 for Visitors*** .

Electrostatic Discharge Testing Mode

If there is electrostatic discharge during the operations of electronic devices, it may cause damage to electronic devices. Therefore, some factories need to carry out electrostatic discharge testing when employees enter and exit the relevant workshops.

Select **Detect Hand**, **Detect Foot**, or **Detect Hand and Foot** for electrostatic discharge testing. If the testing is not required, select **Detection Not Required**.

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.

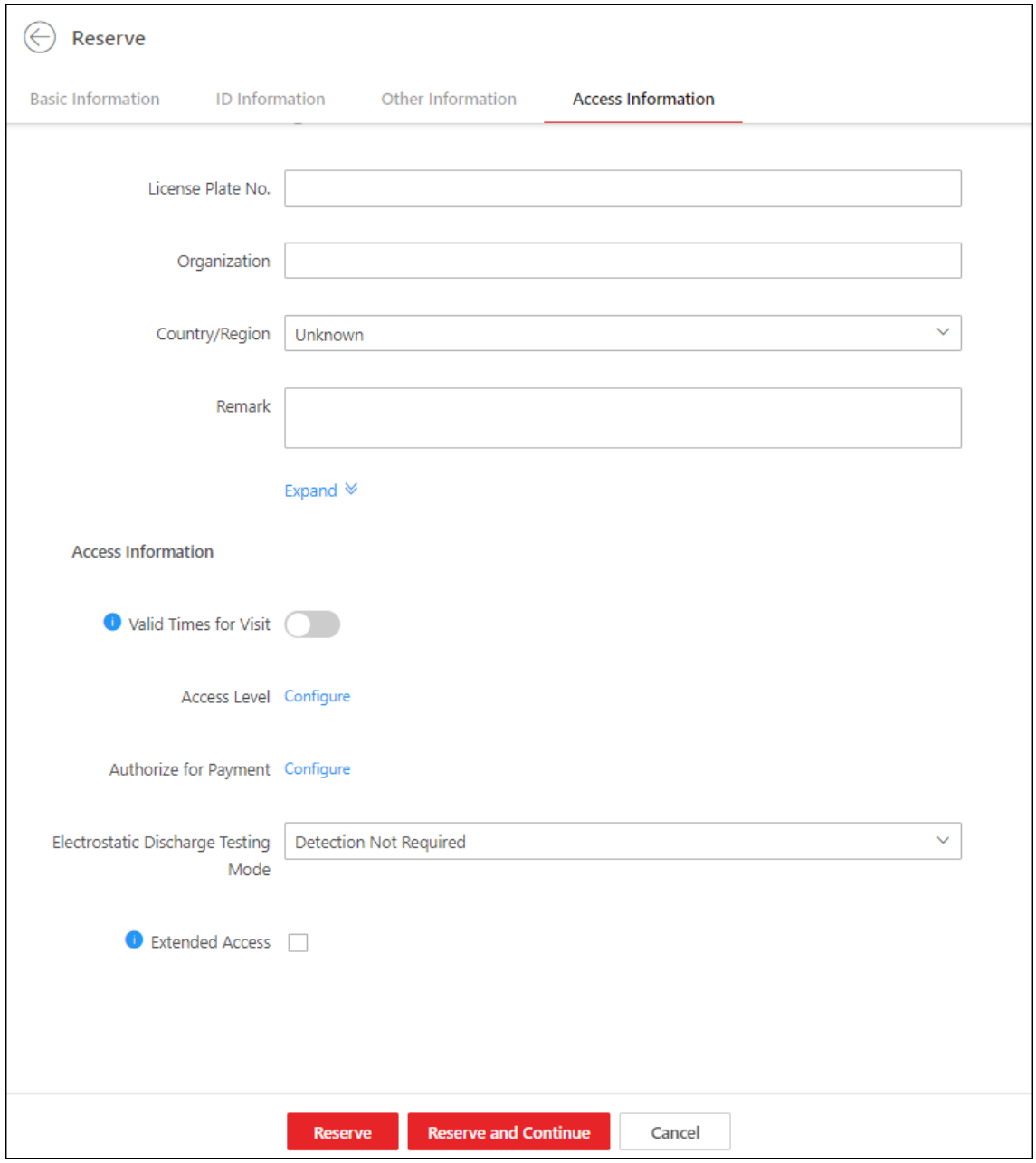


Figure 27-11 Set Access Information

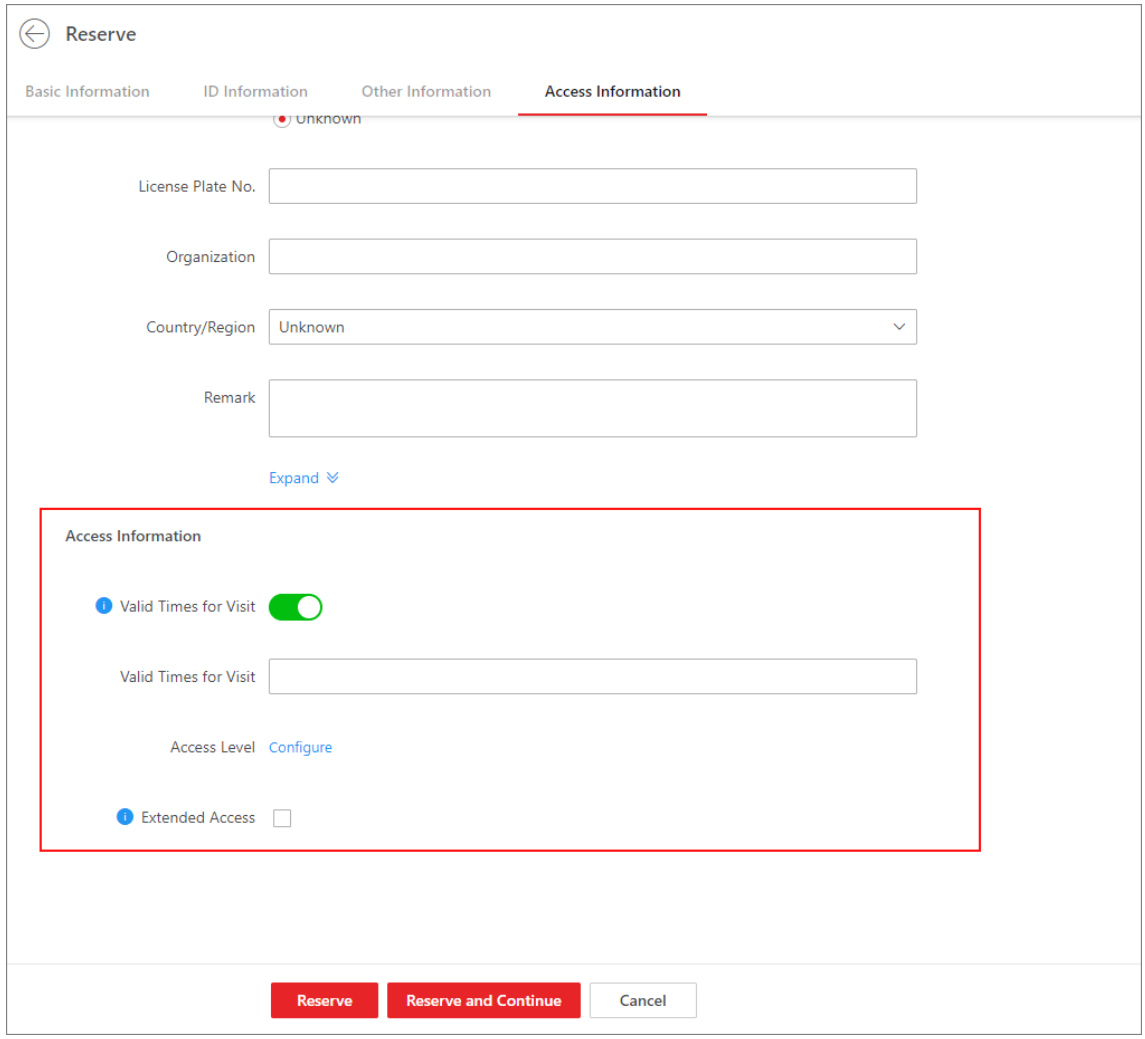


Figure 27-12 Set Access Information

7. 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).

8. **Optional:** Perform the following operations on the reservation list page if needed.

Delete Reservation(s)	Select one or more visitors and then click **Delete** to delete the reservations of the selected visitor(s).

	Or hover the cursor onto ∨ and then click **Delete All** to delete all reservations.
Edit a Reservation	Click the name of a visitor to edit the reservation for the visitor.
Filter Reservations	Set conditions, such as the phone and visit purpose, and then click **Filter** to filter reservations. For the **Status** condition, you can click ∨ to select one or more reservation status (reserved, expired, checked in, etc.) to filter reservations. You can also click **Select Additional Information** to filter reservations.

Note

If a reservation has not expired, the reservation will expire after it is deleted.

27.3.2 Batch Import the Visitor Reservation Information

You can add the information of multiple visitors to the platform by importing an excel file with visitor information. Also, by entering the names of visitor groups of multiple persons in the excel file, you can add them to different groups in a batch.

Before You Start

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 ***Configurations Before Visitor Management*** for details.

Steps

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. **Optional:** 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.

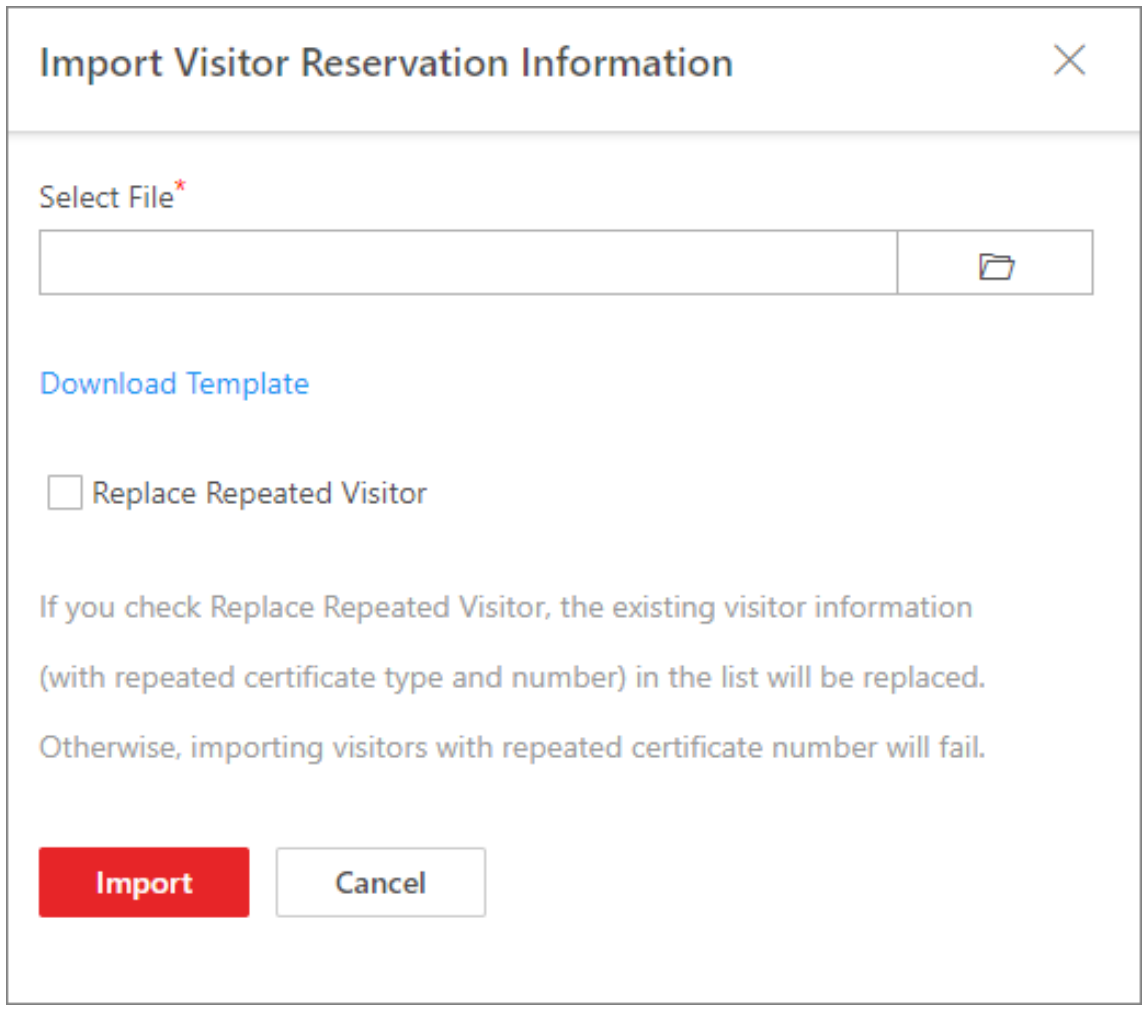


Figure 27-13 Import Visitor Reservation Information

7. Click **Import**.
8. **Optional:** Check one or more visitor(s) and click **Delete** to delete the reservations for the selected visitor(s); or click → **Delete All** to delete all the reservation information.

Note

If a reservation has not expired, the reservation will expire after you delete it.

27.3.3 Review Visitor 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.

Before You Start

Make sure you have enabled self-service reservation and configured related parameters. See ***Set Self-Service Reservation Parameters*** for details.

Steps

Note

You need to have the permission (**User Permission → Configuration Permission → Visitor → Reservation Approval**) shown in the picture below before you can review reservations.

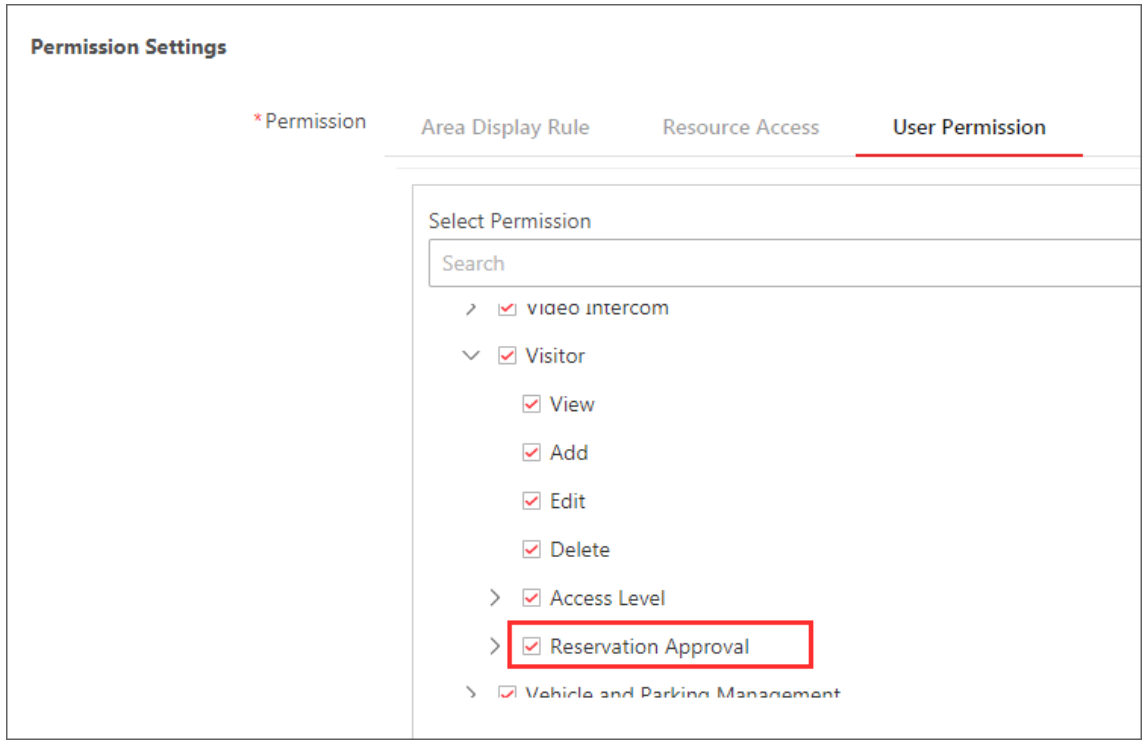


Figure 27-14 The Permission for Reviewing Reservations

1. On the top left of the Web Client, select → **Passing Management → Visitor → Visitor Reservation** .

Note

- If there are visitors to be approved, the number of the to-be-approved visitors will be displayed.

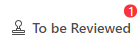


Figure 27-15 The Number of The To-Be-Approved Visitors

- You can only review the visitors reserved via the QR code you generated for self-service reservation, which allows different users to manage their own visitors independently. See ***Set Self-Service Reservation Parameters*** for details.

2. Click **To Be Reviewed** on the top to enter the following page.

   On the page, you can view the information of the to-be-approved visitors, such as their companies and whether their attributes match entities in the watch list.

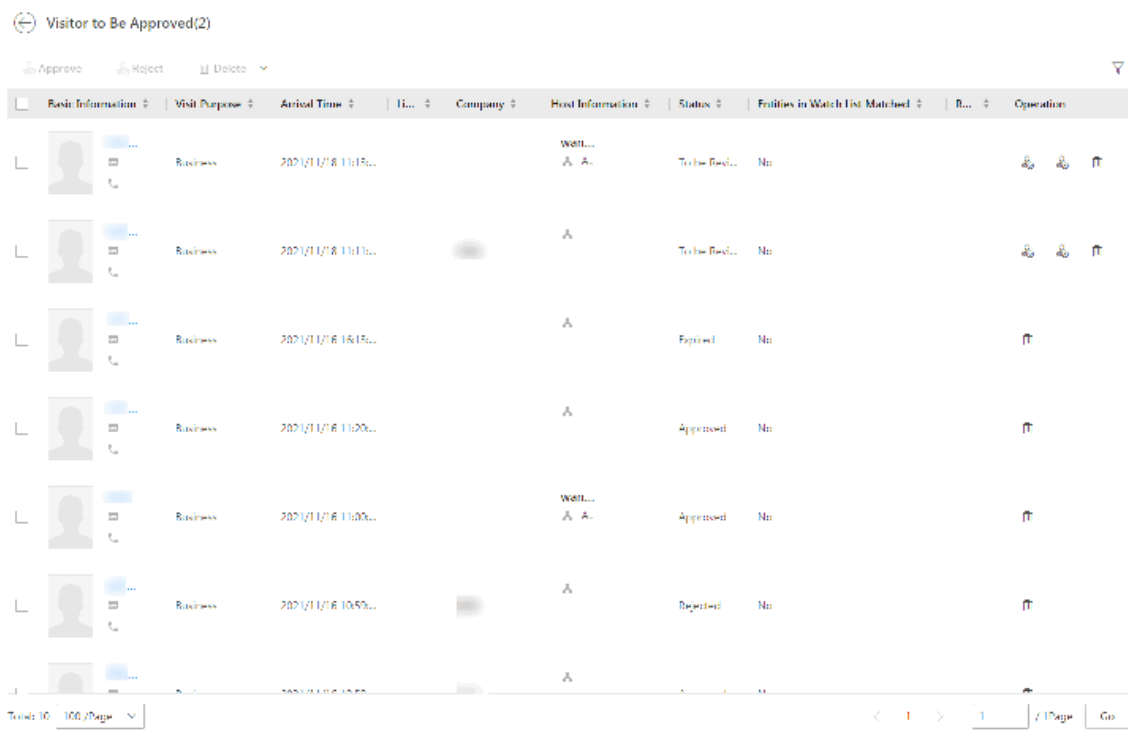


Figure 27-16 Visitor To Be Approved

3. **Optional:** Click ▽ to filter reserved visitors by name, ID, status, etc. to quickly find your wanted visitors.
4. Review the displayed visitor information and verify them.

Approve Self-Service Reserved Visitor Information	If the self-service reserved visitor information conforms to the rules and regulations of your company or organization, approve the information to add the visitors into the platform. Select one or more reserved visitors, and click **Approve** to approve the visitor(s).
Reject Self-Service Reserved Visitor Information	If the self-service reserved visitor information does not conform to the rules and regulations of your company or organization, reject the visitor and tell the visitor to reserve again with right information.

	Select one or more reserved visitors, and click **Reject** to reject the visitor(s).
Delete Self-Service Reserved Visitor Information	Select one or more reserved visitors, and click **Delete** to delete the visitor(s) from the list. You can also hover the cursor on **Delete** and click **Delete All** to delete all visitors from the list.

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.

27.4 Visitor Check-In

The platform supports checking in visitors both with or without a reservation.

See ***Check In a Visitor Without Reservation*** for details about checking in visitors without a reservation.

See ***Check In a Reserved Visitor*** for details about checking in visitors with a reservation.

27.4.1 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.

Steps

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. **Optional:** Set other basic information, including the profile picture, host, visiting purpose, exit time, visitor group, email, and phone.

Note

- For visitors who have visited before, you can click **Select** next to **First Name** to reuse the information.
- You can click **Select** next to **host** to select an existing person as the host.
- 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 Take ID Photo as Visitor Profile Picture on the Basic Parameters page in order to read the ID photo and set it as the visitor profile picture. 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).
- Hover the cursor on the uploaded profile picture and click × to delete it.
- Enter the email address for the visitor to receive an email containing the QR code or notification that the visitor has checked in.

5. **Optional:** Click **Credential Management** to set the credentials for the visitor, including the card and fingerprint.

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 27-17 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.

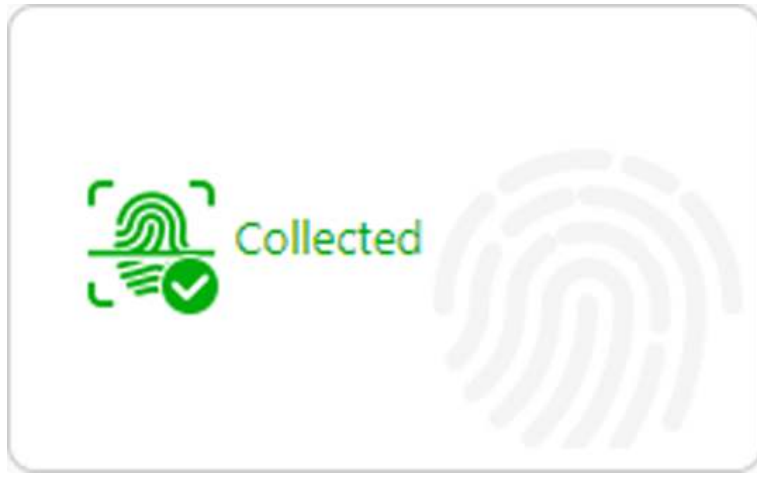


Figure 27-18 Fingerprint Recorded

Note

- No more than one fingerprint can be collected for 1 visitor.
- You can configure either cards or fingerprints.

6. **Optional:** Edit the ID information, including the ID type, ID No., and ID picture.
7. **Optional:** Take a phone of the visitor's belongings.

Note

Make sure you have enabled this function. See ***Set Basic Parameters*** for details.

8. Set other information.

1) Set other information, such as the license plate number, and skin-surface temperature.

Note

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.

2) Click **Expand** to show the additional information fields and then enter additional information about the visitor.

Note

Make sure you have set custom visitor attributes; otherwise, the additional information fields will be unavailable. For details about how to set custom visitor attributes, see ***Set Basic Parameters*** .

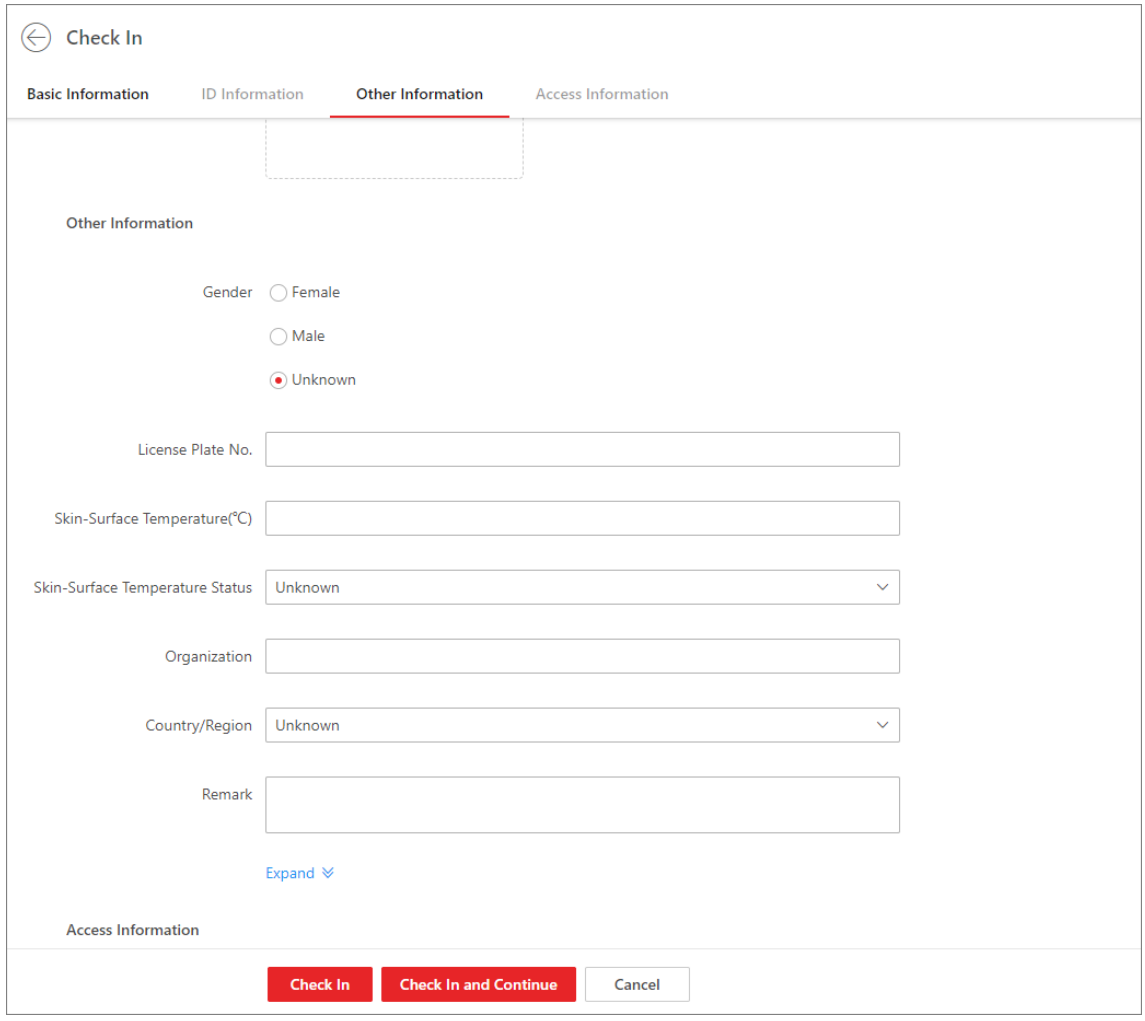


Figure 27-19 Set Other Information

9. Set the access information.

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.

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 for Visitors*** .

Electrostatic Discharge Testing Mode

If there is electrostatic discharge during the operations of electronic devices, it may cause damage to electronic devices. Therefore, some factories need to carry out electrostatic discharge testing when employees enter and exit the relevant workshops.

Select **Detect Hand**, **Detect Foot**, or **Detect Hand and Foot** for electrostatic discharge testing. If the testing is not required, select **Detection Not Required**.

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.

10. Complete checking in the visitor.
- Click **Check In**.
- Click **Check In and Continue** to check in the visitor and continue to check in another.

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.

11. 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.

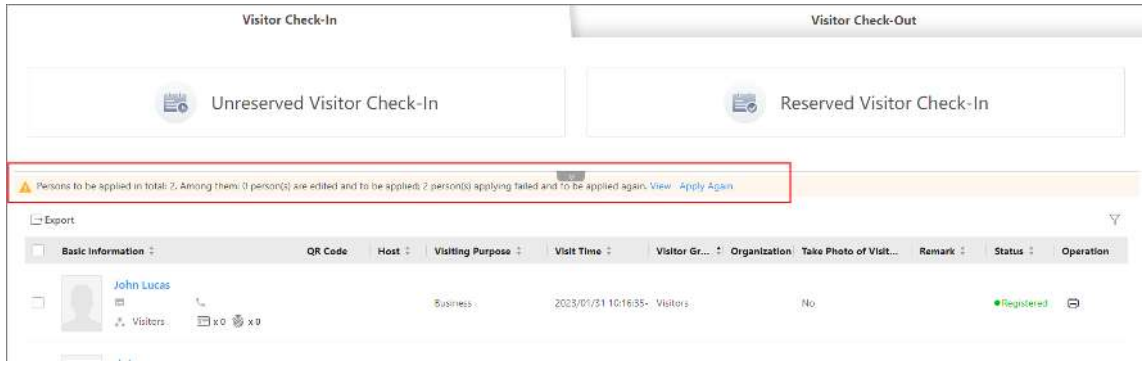


Figure 27-20 Notification of Applying Failures



Figure 27-21 Failure Details

12. **Optional:** Perform the following operations on the Visitor Check-In page if needed.

Filter Visitors

Click to filter visitors by conditions such as the ID No., name, phone, and organization.

For the **Status** condition, you can click to select one or more reservation status (reserved, expired, checked in, etc.) to filter visitors.

You can also click **Select Additional Information** to filter visitors.

Export Visitors

Select visitors and click **Export** to export checked-in visitors to the local PC as a file.

Note

You will be required to set a password for the exported file for security. 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.

Edit Visitor Information

Click on a visitor's name to edit the information.

Note

If the visitor is checked out, you cannot 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.

What to do next

You can view the added visitors in the Visitor List. For details, see ***View Visitor Information*** .

27.4.2 Check In a Reserved Visitor

If a visitor has a reservation, you can check in the visitor by entering reservation information and visitor information.

Steps

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.

   The Reservation Information window will show.
5. **Optional:** Click **Edit Visitor Information** to edit the visitor information. See ***Check In a Visitor Without Reservation*** for details.
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.

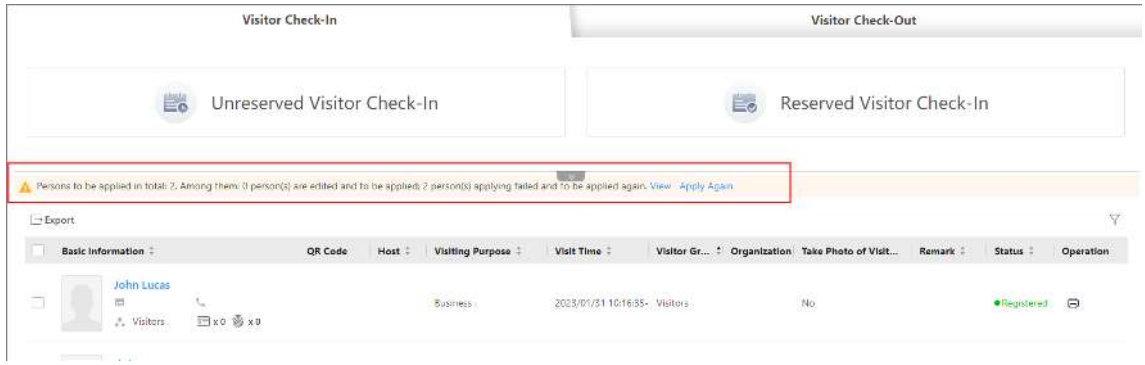


Figure 27-22 Notification of Applying Failures



Figure 27-23 Failure Details

8. **Optional:** Perform the following operations on the Visitor Check-In page if needed.

Filter Visitors

Click to filter visitors by conditions such as the ID No., name, phone, and organization.

For the **Status** condition, you can click to select one or more reservation status (reserved, expired, checked in, etc.) to filter visitors.

You can also click **Select Additional Information** to filter visitors.

Export Visitors

Select visitors and click **Export** to export checked-in visitors to the local PC as a file.

Note

You will be required to set a password for the exported file for security. 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.

Edit Visitor Information

Click on a visitor's name to edit the information.

Note

If the visitor is checked out, you cannot 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.

27.5 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.

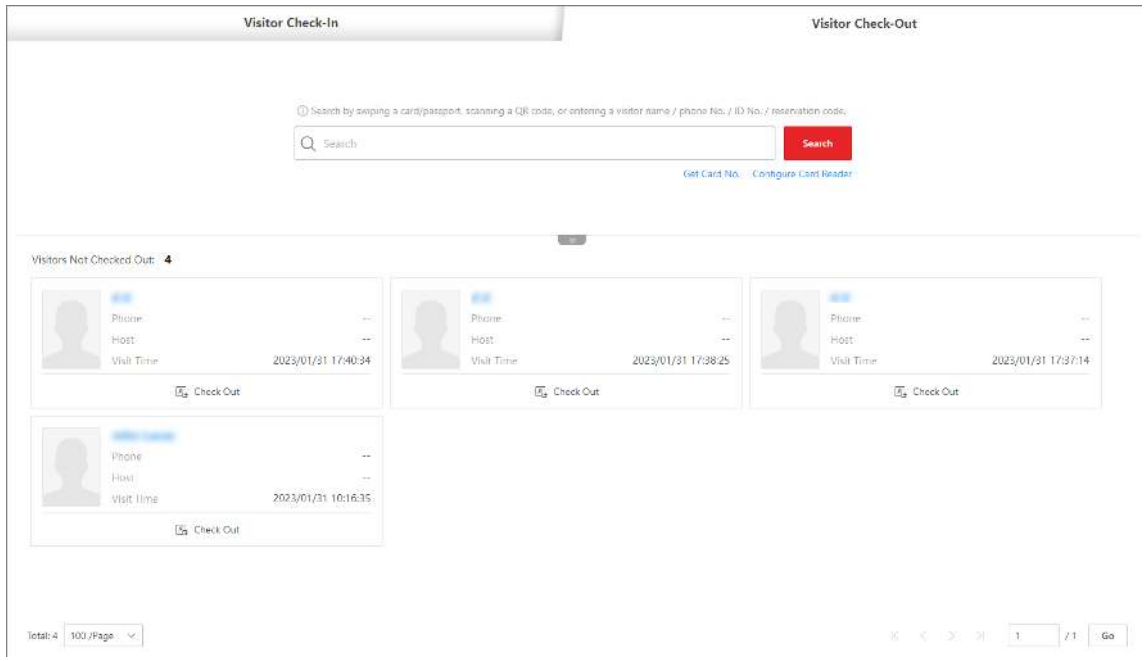


Figure 27-24 Visitor Check-Out Page

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.
For details about how to configure the card reader, see ***Set Card Issuing Parameters*** .

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, you can 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 is plugged into the PC where the platform runs, you can use the KR420 passport reader to swipe the card/passport 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*** .

27.6 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.

- Click on the top right to filter visitors by ID No., name, phone, company, skin-surface temperature, reservation/check-in time, and whether the visitor is in the blocklist.
  If you have set custom visitor attributes, you can click **Select Additional Information** to select additional information for the filtering. See ***Set Basic Parameters*** for details about how to set custom visitor attributes.
- **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.

27.7 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 (see ***Filter Visitors***).

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 28 Time & Attendance

In the Attendance module, you can easily manage the time & attendance system of your department and check your employees' attendance.

On the Home page, you can view the attendance report, attendance status statistics, and overall work hours / overtime.

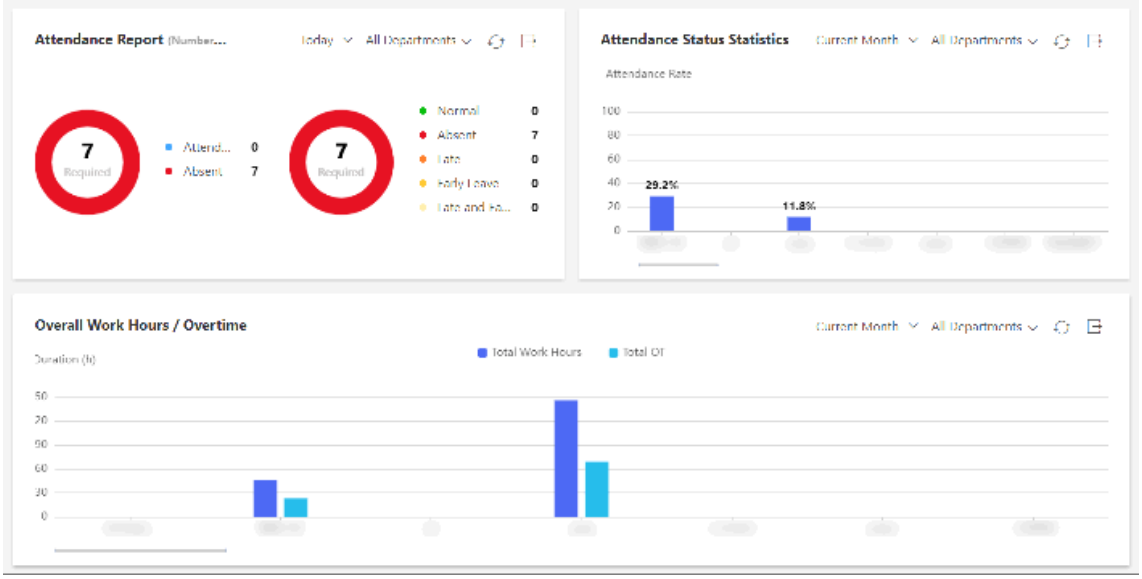


Figure 28-1 Attendance Charts

28.1 Time and Attendance Overview

The Attendance module provides time and attendance overview, including the attendance report, attendance status statistics, overall work hours / overtime, and personal credential status. In Time & Attendance Overview page, you can also set up a time & attendance system from the start.

On the top left, select → **Integrated Service** → **Attendance** . Select **Time & Attendance Overview** on the left.

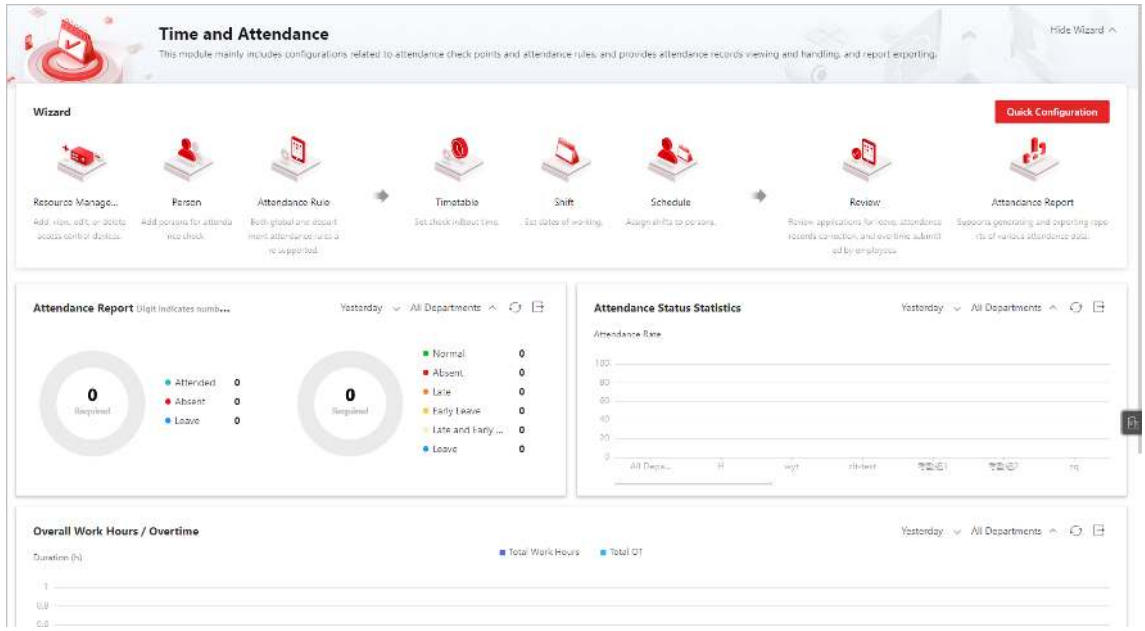


Figure 28-2 Attendance Overview

In the upper-right corner, click **Display Wizard** to view the flow chart of time and attendance configuration. To get detailed instructions on each step, refer to ***Flow Chart of Time and Attendance*** .

To set up a time & attendance system from the start, click **Quick Configuration** and follow the instructions on screen.

1. **Person**: Add persons for attendance. For more details, refer to ***Add Departments*** and ***Add Person*** .
2. **Timetable Configuration**: Set a working time period. For more details, refer to ***Add Timetable*** .
3. **Shift**: Set the working time of a day and set the repeat schedule by day, week, or month. For more details, refer to ***Add Shift*** .
4. **Schedule**: Assign a shift to persons and set schedules. For more details, refer to ***Manage Schedule*** .

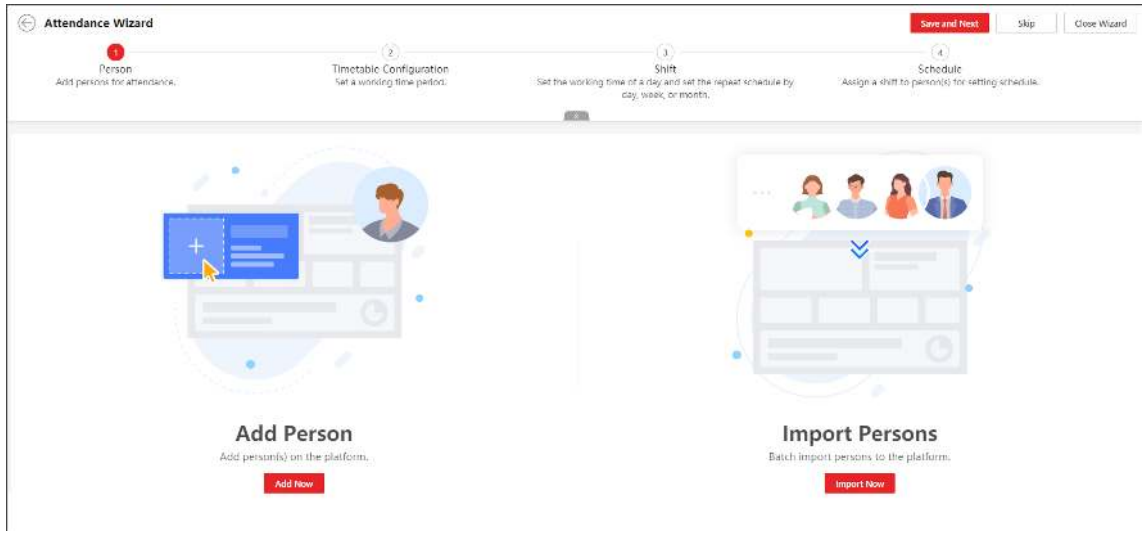


Figure 28-3 Attendance Wizard

You can view the attendance report, attendance status statistics, overall work hours / overtime, and personal credential status.

Note

- You can select the departments to view the attendance statistics. Also, you can select the time range from Today, Yesterday, Current Week, Last Week, Current Month, Last Month, Last 4 Months, Last 6 Months.
- You can click to export the current chart to local PC in the file format of PDF, PNG, or JPG.
- You can click to refresh the statistics data.

28.2 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. On the top left, select → **Integrated Service** → **Attendance** → **Attendance Group** .
2. Click **Add**.
3. On the Add Attendance Group pane, enter a name of the group.

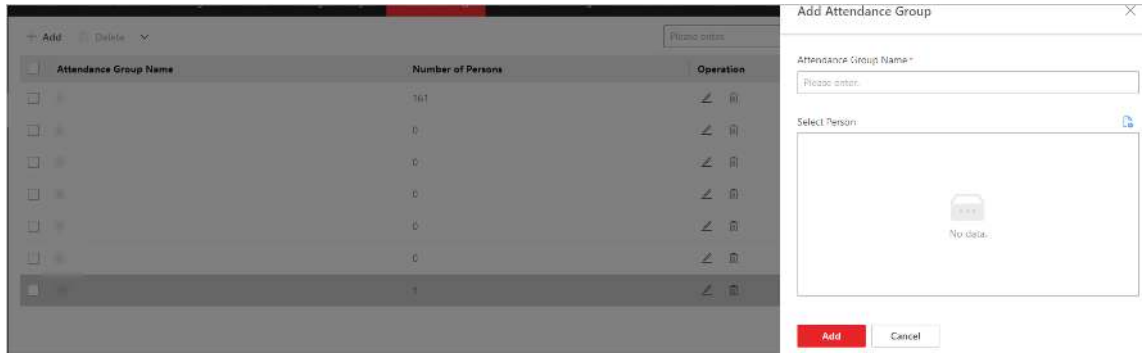


Figure 28-4 Add Attendance Group

4. Click and check persons in different departments, and click **Add** to save the selections.

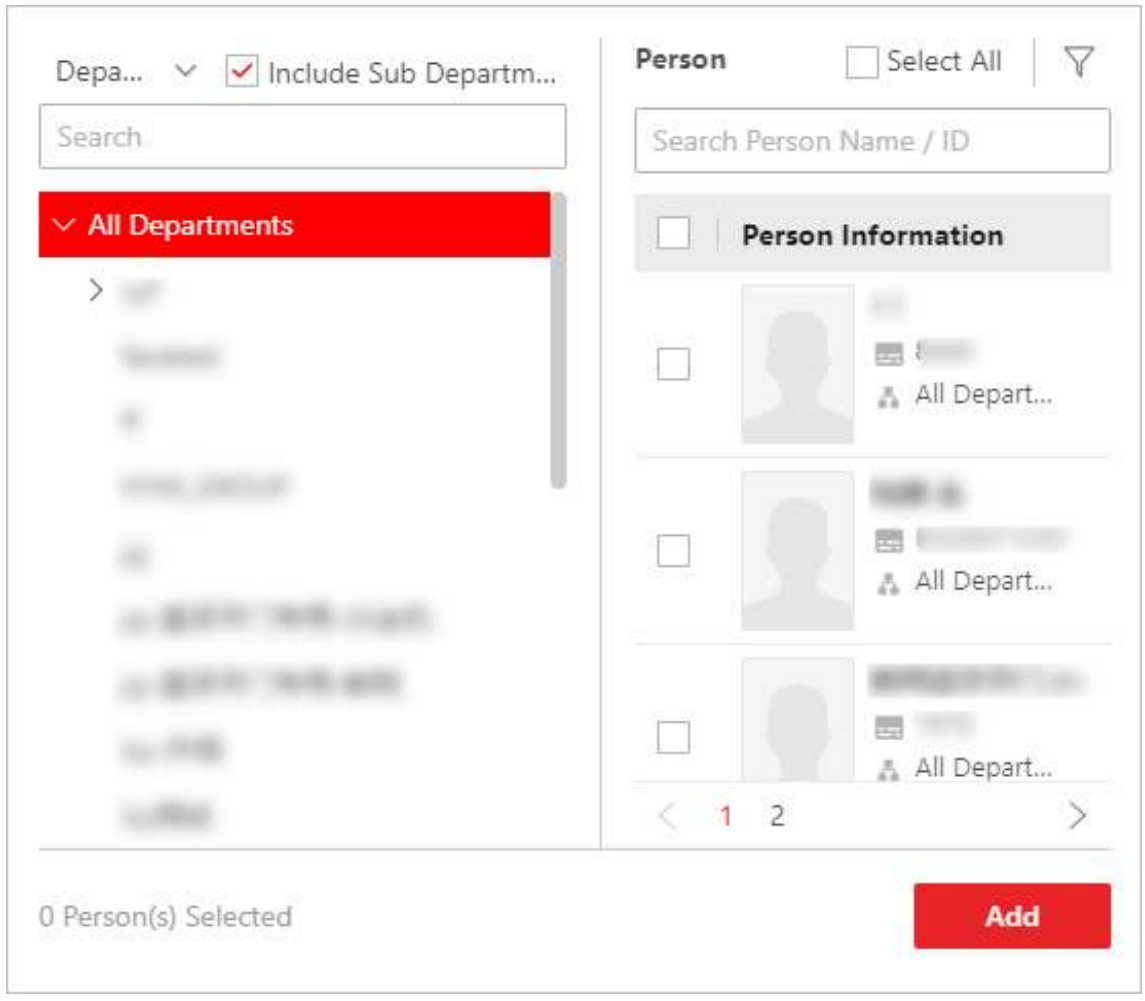


Figure 28-5 Add Persons to Attendance Group

Note

You can click on the top left to filter persons by additional information.

5. 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*** .

28.3 Basic Configuration

You can set basic parameters for the attendance module, such as adding pay codes, editing the fixed codes, setting the storage location, and customizing attendance status.

28.3.1 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. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Basic Configuration** → **Attendance Check Point** on the left.
3. **Optional:** Click **Customize Attendance Status** to select attendance mode and custom attendance parameters. For details, see ***Customize Attendance Status on Device*** .
4. **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.
5. Click **Specify** to start customizing attendance check points.
6. Click **Add**.
7. 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.

8. Select the resource type (e.g., door) from the drop-down list.

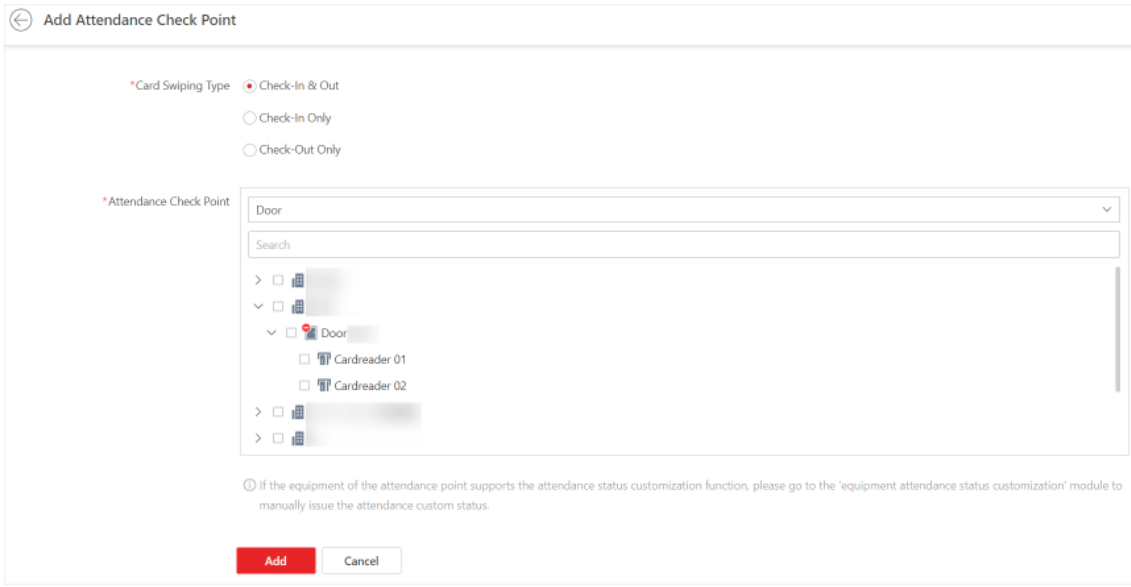


Figure 28-7 Add Attendance Check Point

All the resources which have not been set as attendance check point will be displayed.

9. 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.

10. Click **Add**.

The selected resources will be displayed in the attendance check point list.

11. **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.

Before You Start

Make sure the devices support this feature.

Steps

1. In the upper-left corner of Home page, select  → **Attendance** → **Basic Configuration** .
2. Select **Custom Attendance Status on Device** on the left.
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.

Schedule Template

Select a status and drag on the template to define the attendance status of a period of time.

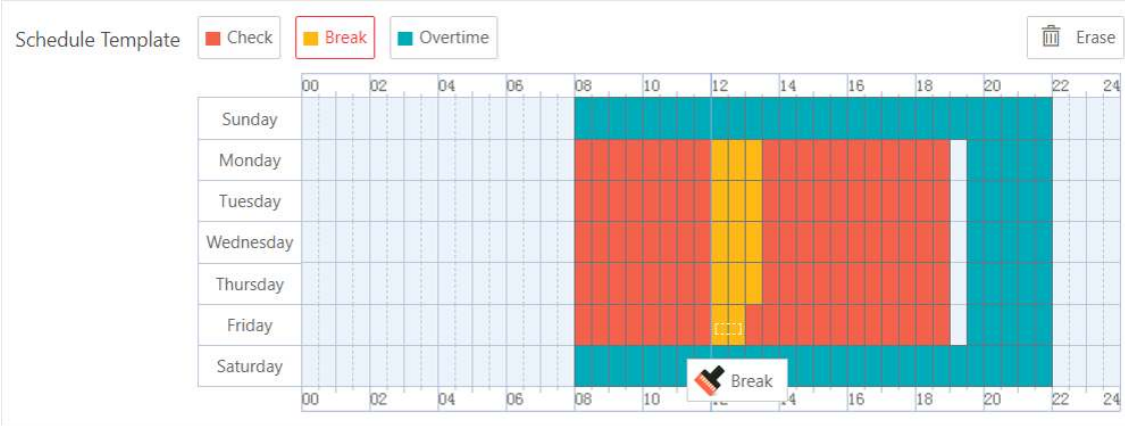


Figure 28-8 Schedule Template

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.

28.3.2 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. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Basic Configuration** → **Pay Code** on the left.
3. Click **Add** to open the Add Pay Code pane.
4. Create the pay code name.
5. 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.
6. 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.

7. Set the Min. Value for the rounding rule.
8. Set whether to display the pay code in report.
9. Click **Add**.
10. **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.

28.3.3 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.

On the top left, select → **Integrated Service** → **Attendance** .

Select **Basic Configuration** → **Fixed Code** on the left.

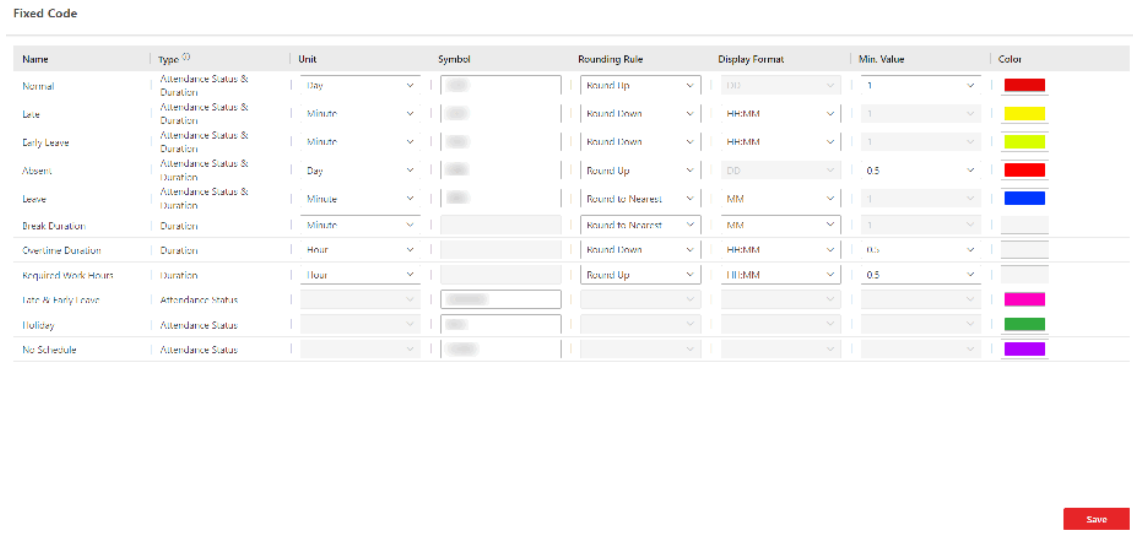


Figure 28-9 Edit Fixed Code

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.

Color

Used for making differences among fixed codes.

28.3.4 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. On the top left, select → **Integrated Service** → **Attendance** → **Basic Configuration** → **Leave Rule** .
2. Click **Add Leave Rule**.

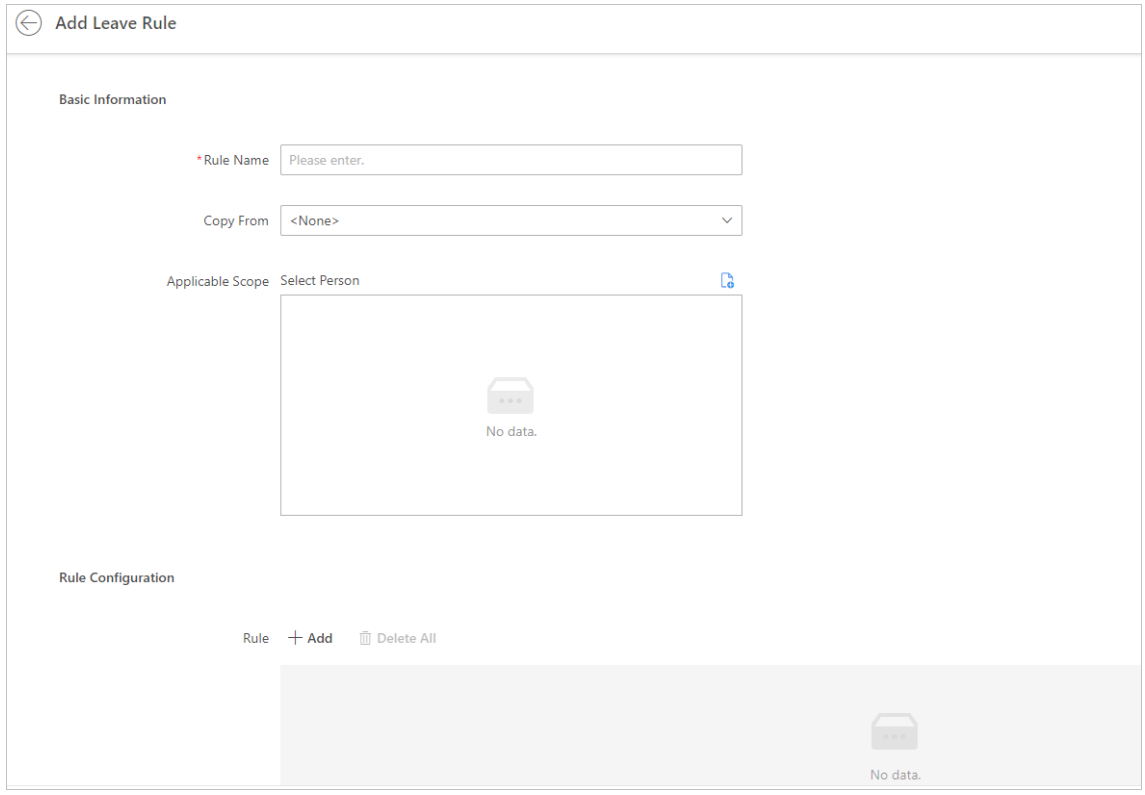


Figure 28-10 Add Leave Rule

3. Enter a rule name.
4. **Optional:** Select an existing leave rule from the drop-down list of **Copy From** to copy the persons using the selected leave rule here.
5. Click to select persons who are going to use the leave rule.
6. 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.

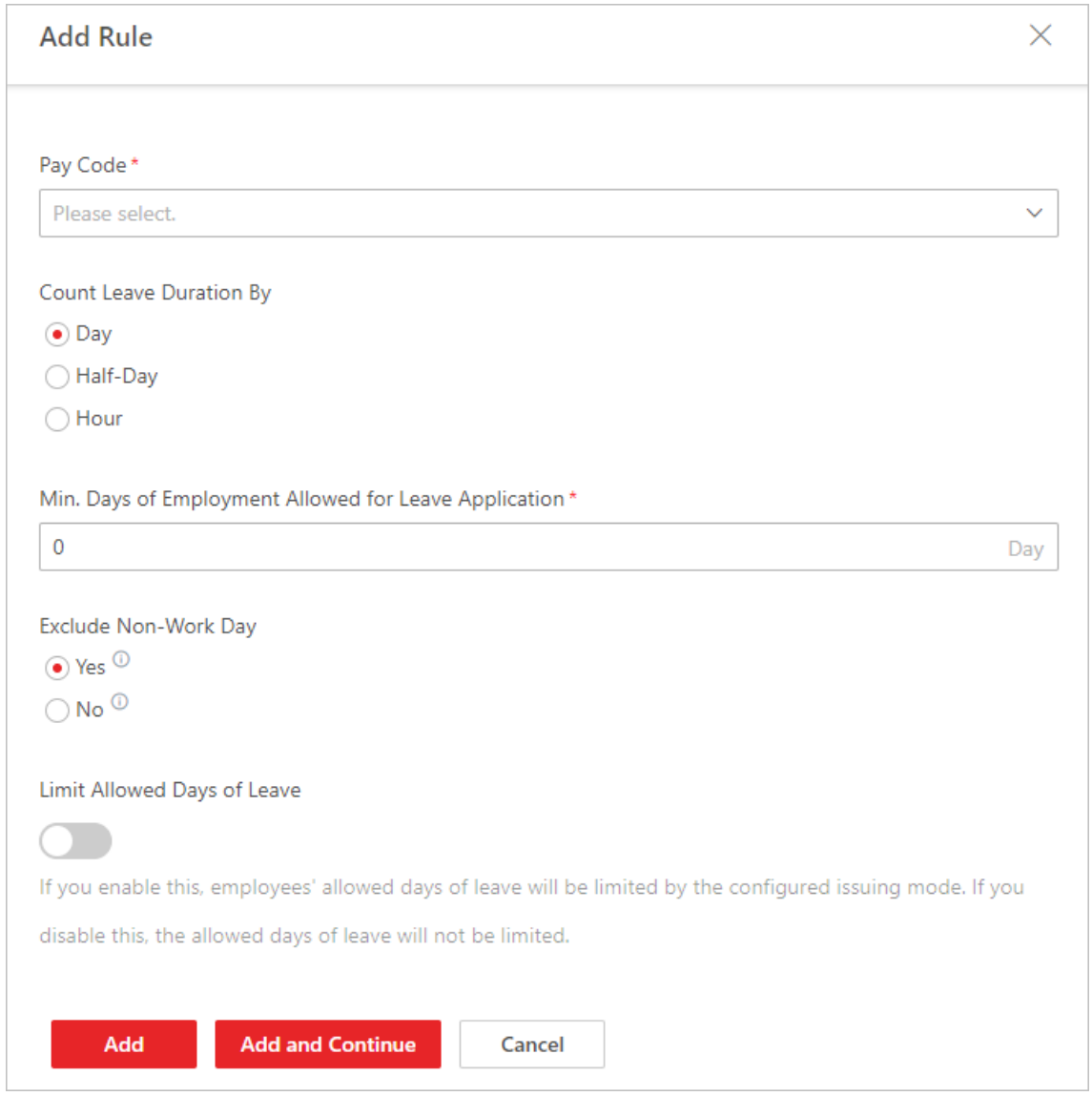


Figure 28-11 Add Rule

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.

7. Save the settings.

28.3.5 Configure Check-In/Check-Out via Mobile Client

After configuring the function of check-in/check-out via mobile client, employees in the platform will be able to check in/out inside the valid geographic scope via the Mobile Client. And the platform will perform attendance calculation of check-in records collected by the Mobile Client.

Steps

1. On the top left, select → **Integrated Service → Attendance → Basic Configuration → Check-In/Check-Out via Mobile Client** .
2. **Optional:** If there is no GIS map configured, click **Configure GIS Map**, then enable **GIS Map** and enter the GIS map API URL, and then save the settings.

Note

If there is already a GIS map configured and you want to change the map, click **GIS Map Settings** and repeat this step to change the map.

3. Draw the valid check-in/out scope on the map.
   1) Select a location on the map as the center of the valid check-in/out scope and click **OK** to start drawing the valid check-in/out scope according to the following to methods.
      - In the text box above the map, enter a location to search for it, select the location in the drop-down list, and click **OK**.
      - Click a location on the map and click **OK**.
   2) **Optional:** Click **Switch to Polygon** or **Switch to Circle** to change the shape of the scope.
   3) Enter the Max. radius or drag the mouse to draw a circle or a polygon.
   4) **Optional:** Drag the edge to change the shape.
   5) Save the scope.
4. Configure the advanced settings if needed, including **Taking Photo Required** and **Auto Approve Check-In/Out via Mobile Client**, and then save the settings.

Note

Make sure you have enabled the Allow Check-In/Out via Mobile Client function for the persons. See ***Add a Single Person*** .

28.3.6 Configure Storage Settings

You can set the storage location of the attachment in exception application.

1. On the top left, select → **Integrated Service → Attendance** .
2. Select **Basic Configuration → Storage Settings** on the left.
3. Select a backup file to be restored.
4. Click **Save**.

28.4 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 rule, department rule, or 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.

28.4.1 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.

On the top left, select → **Integrated Service → Attendance → 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.

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.

28.4.2 Configure Attendance Calculation Mode

You can set the mode of attendance calculation.

Choose a calculation mode of work duration.

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.

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.

28.4.3 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.

On the top left, select → **Integrated Service** → **Attendance** . Select **Attendance Rule** → **Global Rule / Department Rule / Group Rule** on the left. 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. Click **Attendance Calculation** on the right.

In the Absence Settings area, you can define the absence rules.

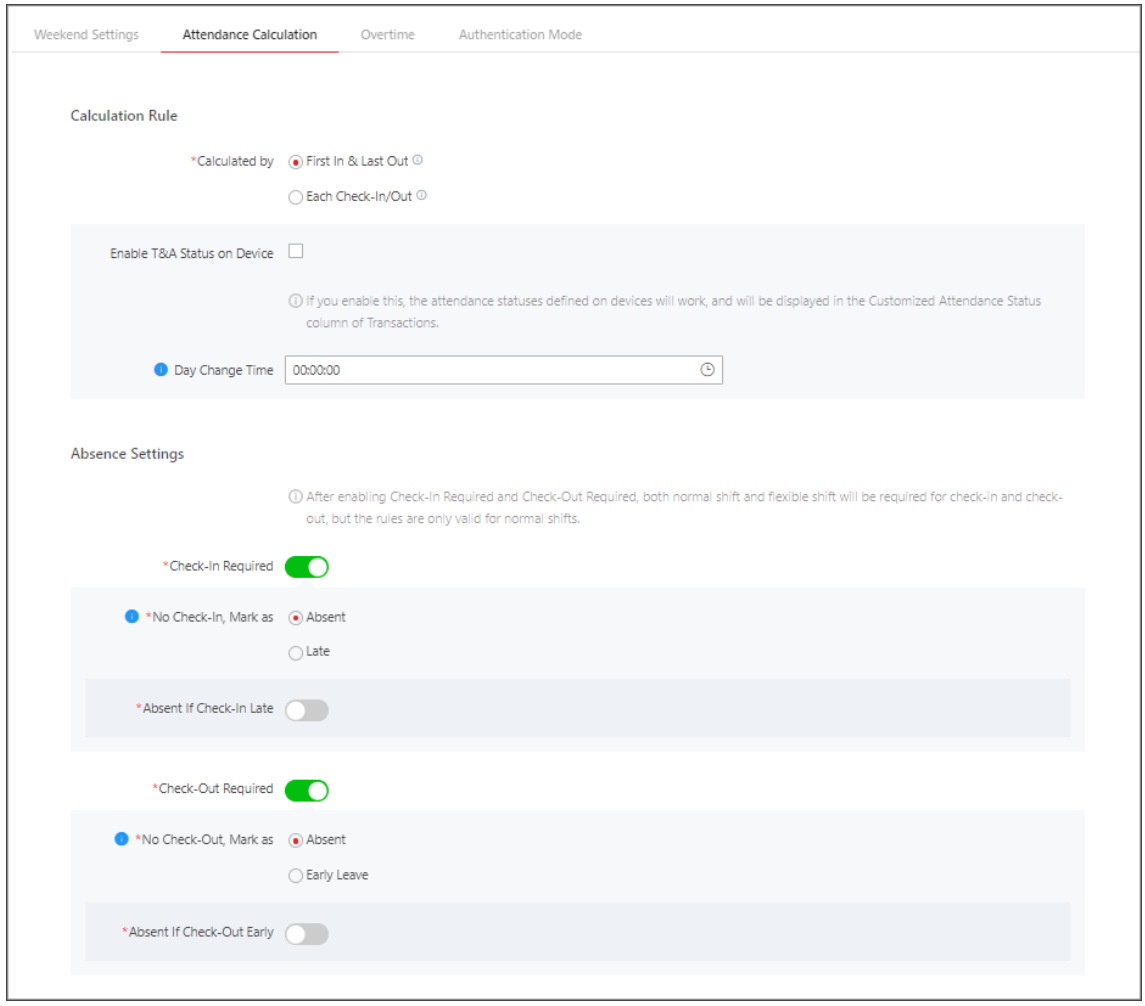


Figure 28-12 Absence Settings

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.

28.4.4 Add Holidays Requiring Attendance

You can set a holiday that requires normal attendance as in weekdays.

Steps

1. On the top left, select → **Integrated Service → Attendance** .
2. Select **Attendance Rule → Global Rule / Department Rule / Group Rule** on the left.
3. **Optional:** 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.
4. Select the **Attendance Calculation** tab.

Note

For details of adding a holiday, see ***Add a Holiday*** .

5. 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. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Basic Configuration** → **Holiday Settings** on the left. You can also access the Holiday Settings page in **System** on the top.
3. 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.

28.4.5 Calculation of Leaves

You can set the status of leaves as normal attendance, leave, or absent.

On the top left, select → **Attendance** . Select **Attendance Rule** → **Global Rule / Department Rule / Group Rule** on the left.

Note

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 the **Attendance Calculation** tab. In the **Leave Settings** area, you can choose to mark leave as **Normal**, **Leave**, or **Absent**. The leave status will be displayed in the attendance results.

28.4.6 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.

Steps

1. On the top left, select → **Integrated Service → Attendance** .
2. Select **Attendance Rule → Global Rule / Department Rule / Group Rule** on the left.
3. **Optional:** 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 on the left.
4. Select **Overtime** on the right to enter the overtime settings page.
5. In the Overtime on Workday/Weekend area, switch on **Calculate Overtime** to set the calculation mode of overtime duration on workdays and weekends.

   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.

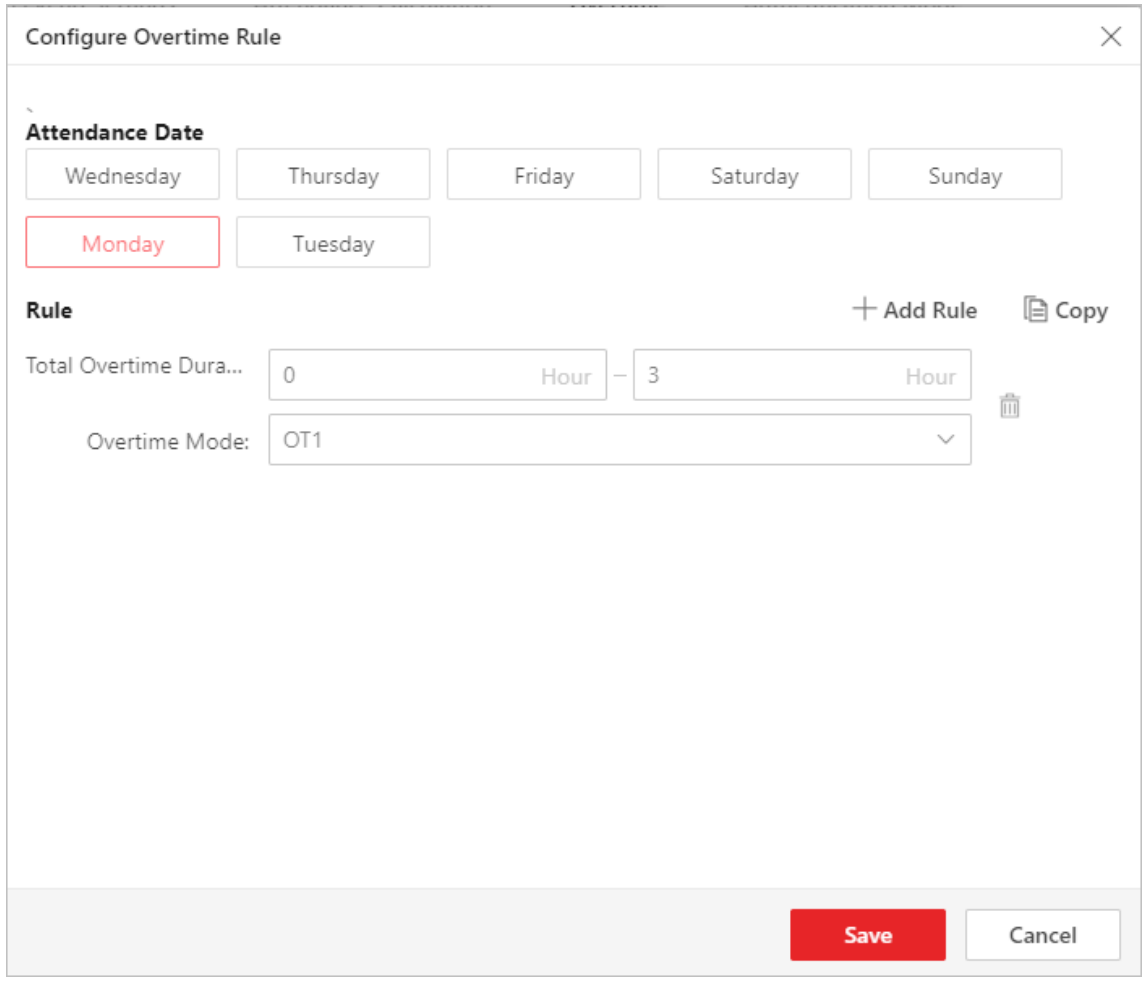


Figure 28-13 Configure Overtime Rule

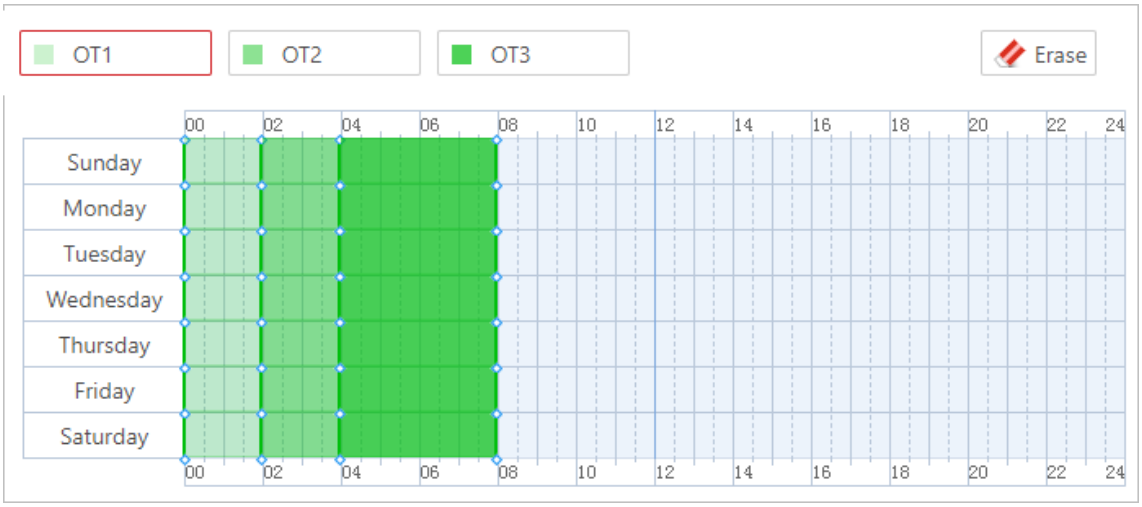


Figure 28-14 Overtime Level Settings

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.

6. In the Overtime on Holidays area, switch on **Calculate Overtime**, and then set the overtime rule for 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**.

7. **Optional:** Switch on **Calculate Overtime** in the Overtime Not in Valid Attendance Check Period area to count the extra work time outside the valid check-in/out period as valid overtime. And then select an overtime level from the drop-down list.
8. For global rules, click **Save**; for department rules, click **Add** on the top right.

28.4.7 Configure Authentication Mode

You can configure authentication modes, including card, fingerprint,, face, and iris. After setting authentication mode, you can get attendance records of the configured authentication mode and calculate attendance data of the configured authentication mode.

On the top left, select → **Attendance** . Select **Attendance Rule → Global Rule / Department Rule / Group Rule** on the left. Select **Authentication Mode** on the right.

Note

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.

Switch on **Customize Authentication Mode**, and select card, fingerprint, iris, or/and face as the authentication mode.

Note

This function requires device capability.

28.5 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.

28.5.1 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. On the top left, select → **Integrated Service → Attendance** .
2. Select **Shift → Break Timetable** on the left.
3. Click **Add**.
4. 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.

5. Click **Add** to finish adding the timetable, or click **Add and Continue** to finish adding the timetable and add a new break timetable.
6. **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*** .

28.5.2 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. On the top left, select → **Integrated Service** → **Attendance** . Select **Shift** → **Timetable** on the left.
2. Click **Add**.
3. On the top, create a timetable name.
4. 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.
5. In **Basic Settings**, 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**.

6. 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*** .

Count Break Time in Work Hours

Check the function to include the break time into work hours. It is checked by default.

7. In **Attendance Calculation**, switch on **Attendance Required During Time Period**, and set the following parameters.

Note

The attendance calculation rule has higher priority than the department and global rules.

Set Calculation Rule

Switch on to set the calculation method of work duration.

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.

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 Settings

Switch on to set the day change time.

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.

8. 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 an overtime timetable in ***Configure Overtime Parameters*** . You can also refer to this chapter for explanations of the parameters.

9. **Optional:** In **Timetable Overview**, view the timetable in a time line.



Figure 28-15 Timetable Overview

Note

You can drag the time line to the left or right.

10. 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*** .

28.5.3 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. On the top left, select → **Attendance** .
2. Select **Shift** → **Timetable** on the left.
3. Click **Add**.
4. On the top, create a timetable name.
5. 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.
6. In **Basic Settings**, 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.

7. 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*** .
- Check **Count Break Time in Work Hours** to include the break time into work hours.

8. 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

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.

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 Settings

Switch on to set the day change time.

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.

9. 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.

10. **Optional:** In **Timetable Overview**, view the timetable in a timeline.



Figure 28-16 Timetable Overview

Note

You can drag the timeline to the left or right.

11. 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*** .

28.6 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. On the top left, select → **Attendance** . Select **Shift** → **Shift** on the left.
2. Select **Shift** → **Shift** on the left.
3. Click **Add**.
4. Set the shift's basic information, including creating a descriptive name and editing its description.
5. **Optional:** Select another shift from the drop-down list of **Copy from** field to copy the shift information to the current shift.
6. 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.

7. Select **Normal Shift** or **Flexible Shift** as the shift type.

   The corresponding timetables of normal shift or flexible shift will be displayed.

8. Select a timetable and click on the table below to apply the timetable on each day.

Note

- For **Normal**, you can apply more than one timetable in one day which requires the employees to check in and check out according to each timetable. The start and end work time and the valid check-in and out time in different timetables can not be overlapped.
- You can use up to 8 different timetables in one shift.

9. 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*** .

10. 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*** .

28.7 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 department or persons, or add a temporary schedule, so that it will calculate the attendance records for persons according to this schedule.

28.7.1 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 top left, select → **Attendance** → **Schedule** → **Schedule Overview** .

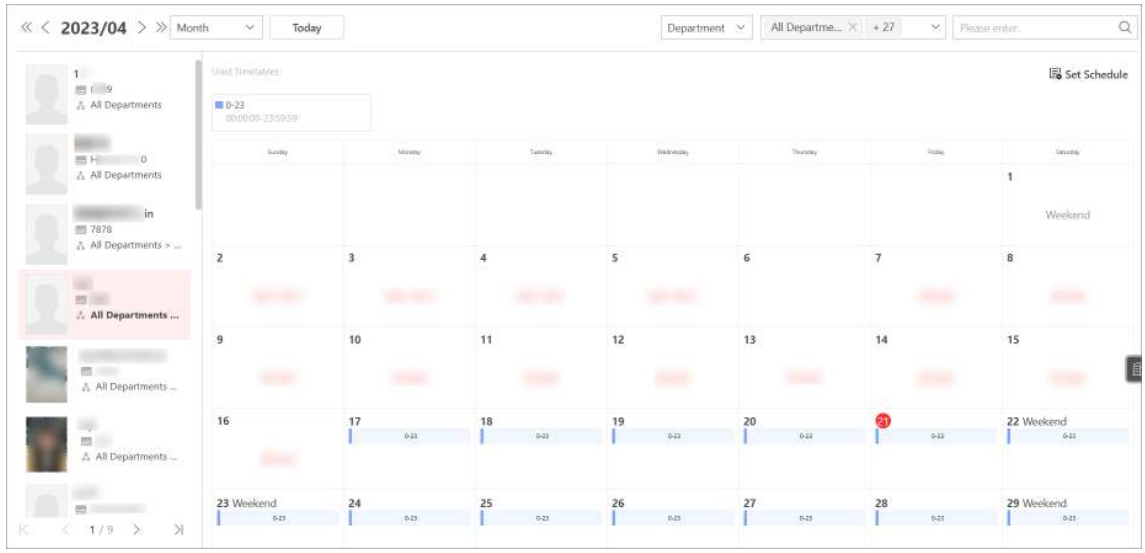


Figure 28-17 Schedule Overview

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 Department*** and ***Assign Schedule to Attendance Groups*** .
- On the upper-right corner, enter the keyword to search for specific persons to view schedules related to them.

28.7.2 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.

Before You Start

Make sure you have added departments and persons. For details, refer to ***Add Departments*** and ***Add Person*** .

Steps

1. On the top left, select → **Integrated Service** → **Attendance** . Select **Schedule** → **Department Schedule** on the left.
2. Perform one of the following to set the schedule.

Assign One by One	On the left, select a department you want to assign shift to, and click **Add Schedule**.
Batch Assign	Click **Batch Add Schedule** to open the panel. Select the departments.

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.

Note

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.

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.

6. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.
7. **Optional:** Perform the following operations.

Edit Schedule	Select a department in the list and click to edit the department's 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.

28.7.3 Assign Schedule to Attendance Groups

After setting the shift, you need to assign it to an attendance group so that it will calculate the attendance records for persons in the group according to this schedule.

Before You Start

Make sure you have added an attendance group and persons. For details, refer to ***Add an Attendance Group*** and ***Add Person*** .

Steps

1. On the top left, select → **Integrated Service → Attendance → Schedule → Attendance 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*** .

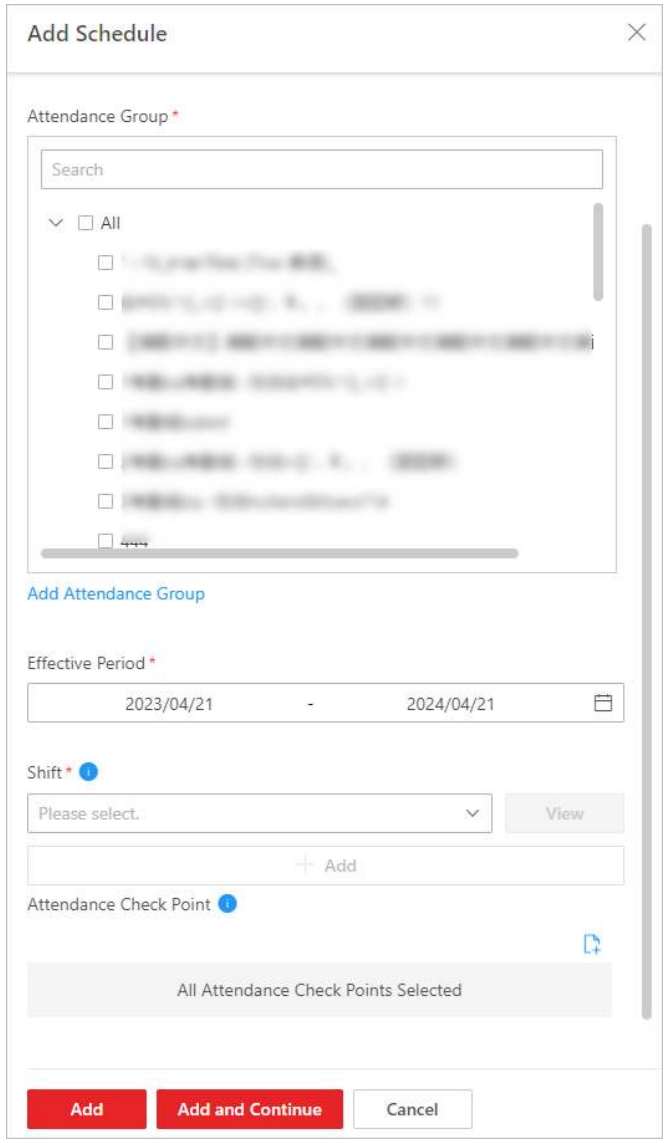


Figure 28-18 Add Schedule

5. **Optional:** Click to select attendance check point(s) linked with the schedule.

Note

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.

28.7.4 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.

Before You Start

Make sure you have added the person(s). For details, refer to ***Add Person*** .

Steps

Note

The person schedule has the higher priority than department schedule.

1. On the top left, select → **Integrated Service** → **Attendance** . Select **Schedule** → **Person Schedule** on the left.
2. **Optional:** Select a department on the left, enter keywords in text field, or check **Show Sub Department** to filter the persons.
3. Select the persons you want to assign the shift to.
4. Click **Add Schedule** to enter the Add Schedule page.
5. 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*** .
6. **Optional:** Click to select attendance check points linked with the schedule.

   Note

   Only authentications at the linked attendance check points will be counted.
7. **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.
8. Click **Add** to save the schedule, or click **Add and Continue** to continue adding another schedule.
9. **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.

28.7.5 Add Temporary Schedule

You can add a temporary schedule for the 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 → **Integrated Service** → **Attendance** . Select **Schedule** → **Temporary Schedule** on the left.
2. Click **Add** to enter Add Temporary Schedule page.
3. In **Select Person(s)** 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. In the top of the timetable, 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).

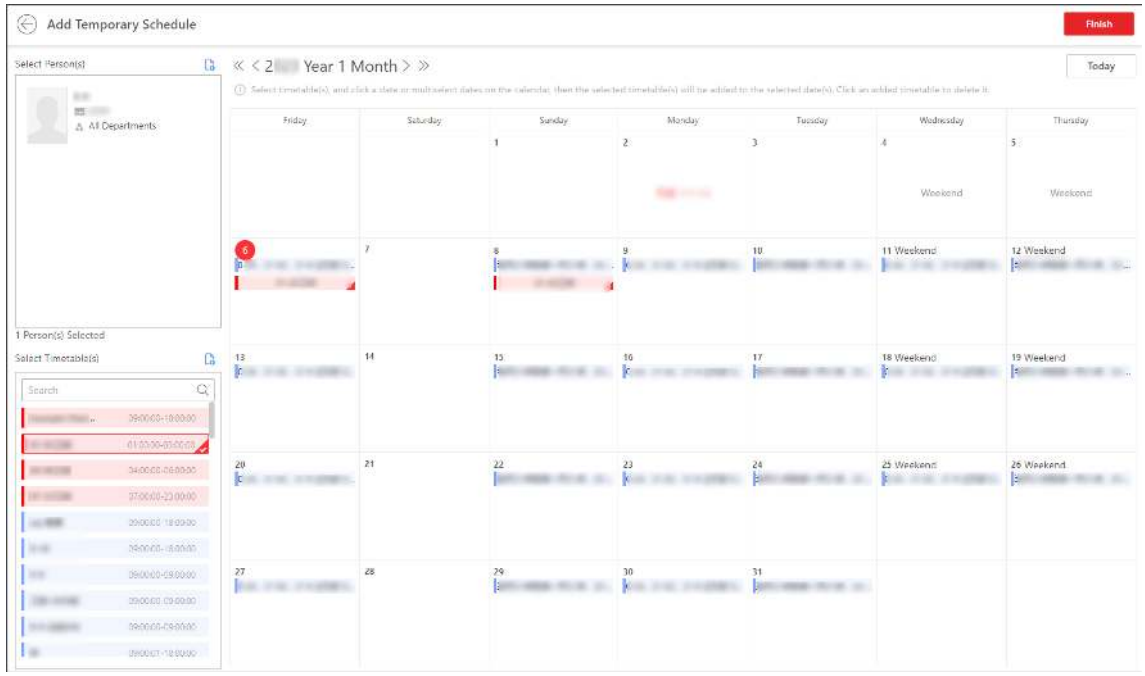


Figure 28-19 Add Temporary Schedule

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**.
9. After adding temporary schedules, you can perform the following operations.

Edit Temporary Schedule	Select a schedule in the list and click **Edit** to edit the schedule.
Delete Temporary Schedule	Select a schedule in the list and click **Delete Schedule** to delete the schedule. Also, you can click **Delete All** to delete all of the schedules.

28.8 Configure Calculation Mode of Attendance Results

You can set the attendance calculation mode as manual calculation or auto calculation.

28.8.1 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. On the top left, select → **Integrated Service → Attendance** .
2. Select **Attendance Calculation** on the left, and then select **Manual Calculation** on the right.
3. Set the start time and end time for attendance calculation.
4. 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.
5. Click **Calculate**.

Note

It can only calculate the attendance data recorded within three months.

28.8.2 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. On the top left, select → **Integrated Service → Attendance** .
2. Select **Attendance Calculation** on the left, and then select **Auto Calculation** on the right.
3. Select a time in **Calculate at**.
4. **Optional:** Enable **Recalculate Historical Data**.
5. Click **Save**.

28.9 Approval Management

The platform supports configuring approval flows for departments, attendance groups, and persons. The approval flow defines the approval process of department / attendance group /

personal applications. When configuring approval flows, you can specify application departments, applicants, reviewers, and persons to be notified of the review results via configuring approval roles. Applications from specified departments / attendance groups / persons need to be reviewed according to the configured approval flow.

28.9.1 Add an Approval Role

Approval roles are for specifying reviewers and persons to be notified of review results. You can add approval roles and assign them to persons. Persons assigned with the approval role that is defined as the reviewer have the permission to approve/reject applications of specified departments / attendance groups / persons, and persons assigned with the approval role that is defined to be notified have the permission to receive and view review results.

Before You Start

Make sure the current admin user has the permissions for configuring approval roles. For details about user permissions, refer to ***Role and User Management*** .

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Approval Management** → **Approval Role** on the left.
3. Click **Add** to add a new approval role.
4. Create a name for the approval role.
5. Click to open the person selection pane.

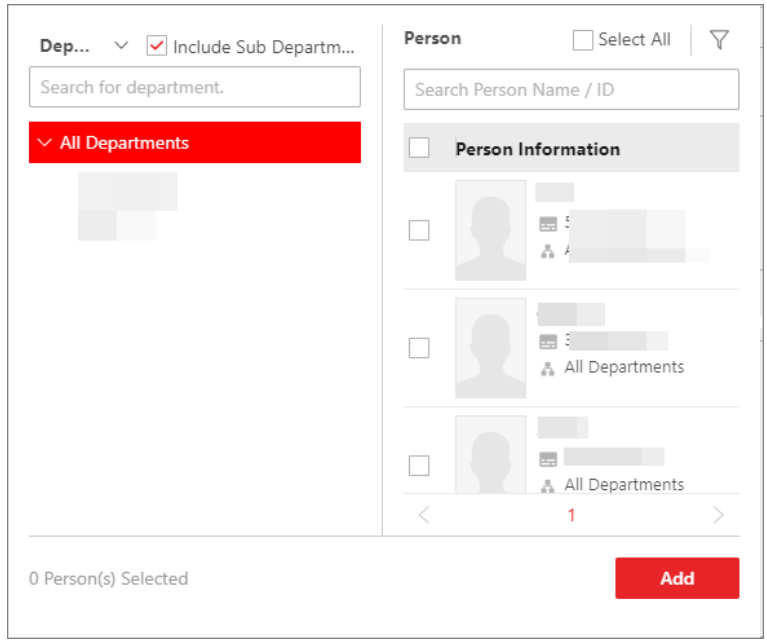


Figure 28-20 Select Person Pane

1) At the top of the left tree, click to select **Department** or **Attendance Group** to show all the selectable departments or attendance groups.

Note

If **Department** is selected, you can check **Include Sub Department** to display persons of sub-departments.

2) Select a department or an attendance group to display the linked person(s) on the right.
3) Check the person(s) select the person(s) to assign the approval role to.

Note

You can check **Select All** at the top of the right, or enter keywords to search for persons, or click to filter persons by the position or additional information. For details about customizing additional information items, refer to ***Object Missing*** .

6. Click **Add** to finish adding the approval role.
7. **Optional:** Perform the following operations as needed.

Edit Approval Role	Select an approval role in the list and click to edit it.
Delete Approval Role	• Select one or multiple approval roles in the list and click **Delete** to delete the approval roles. Also, you can click **Delete All** to delete all approval roles. • Select an approval role from the list, and click to delete it.
Assign Approval Role to More Persons	Select an approval role in the list, and click **Assign To** on the right pane to select persons to assign the approval role to.
Unassign Approval Role	Select an approval role in the list, and select the person(s) on the right pane, and click **Unassign** to unassign the approval role for the selected person(s). Also, you can click **Unassign All** to unassign the approval role for all persons.

28.9.2 Add a Department Approval Flow

Department approval flow defines the approval process of reviewing applications from a department. Applications of the persons in the specified application department should be reviewed according to the department approval flow.

Before You Start

- Make sure the current admin user has the permissions for configuring the approval flow. For details about user permissions, refer to ***Role and User Management*** .
- Make sure you have added roles of the approval flow. For details about adding roles, refer to ***Add an Approval Role*** .

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Approval** → **Approval Flow** on the left.

3. Move the cursor on **Add**, and click **Department Approval Flow**.
4. On the left, set the basic information of the approval flow.
   1) Enter the name of the approval flow.
   2) Set the start time and end time of the validity time period.
   3) Select the application type (leave, check in&out correction, overtime, and check in&out via Mobile Client).
   4) **Optional:** Switch off **Enable Approval Flow** to disable the approval flow.

Note

The approval flow is enabled by default.

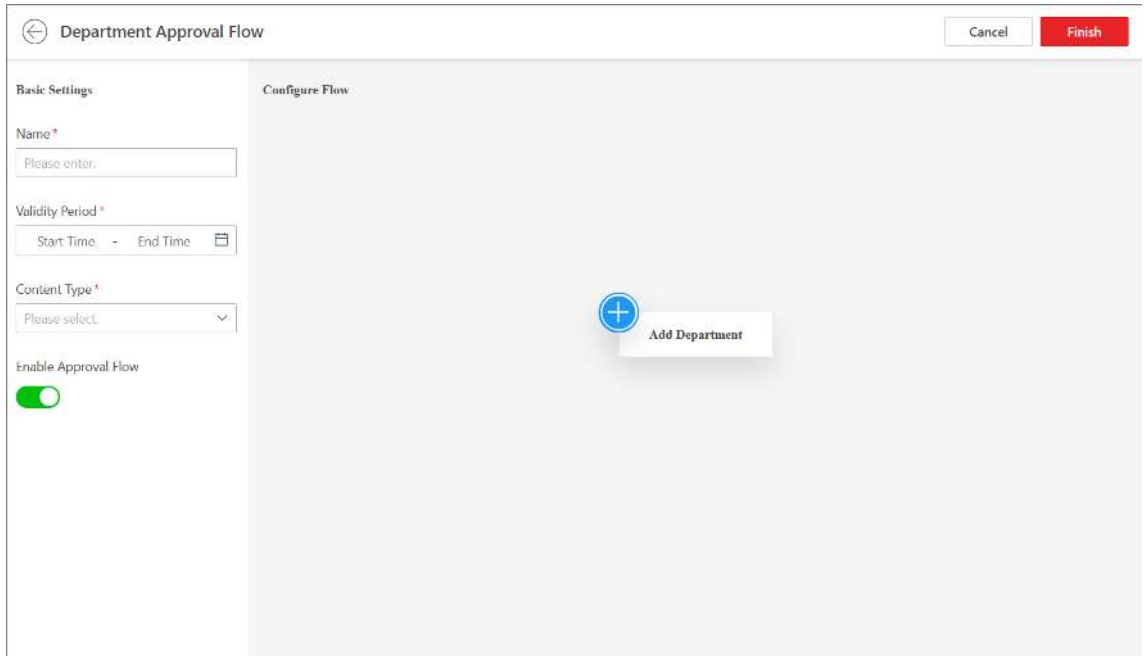


Figure 28-21 Add Department Approval Flow

5. Click **Add Department** to select the application department(s).
6. Click + to add the reviewer(s) for the approval flow.
   1) Select the approval role of the reviewer(s).
   2) Select the department(s) of the selected role(s) allowed to review applications.

   Note

   If the reviewers are from the different department, you need to select **All Departments**.
   3) **Optional:** Select the approval role(s) to be notified of the review results in the current node.
   4) **Optional:** Select the department(s) of the approval role(s) to be notified.

Note

If the person(s) to be notified are from the different department, you need to select **All Departments**.

5) Click **Add**.

Note

You can repeat this step to add more reviewers and persons to be notified for the approval flow.

7. Click **Finish**.

The approval flow will be added to the approval flow list.

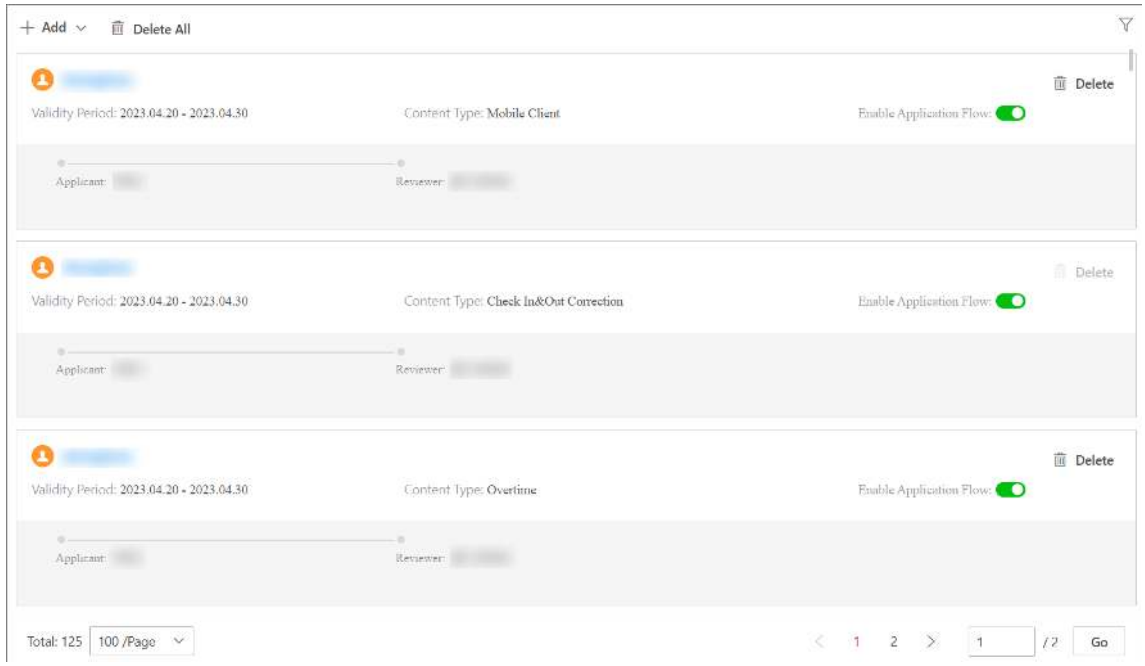


Figure 28-22 Approval Flow List

8. **Optional:** Perform the following operations as needed.

Edit Approval Flow	In the approval flow list, click the name of the approval flow to edit it. • Click **Reviewer** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete the node of the approval flow.
Disable Approval Flow	When adding an approval flow, it is enabled by default. You can disable it in the approval flow list.
Delete Approval Flow	In the approval flow list, you can click **Delete** to delete an approval flow, or click **Delete All** to delete all approval flows.

Filter Approval Flow	On the upper-right corner, click , specify conditions such as person name, approval flow type, or content type, and click **Filter** to filter the approval flows.

28.9.3 Add an Attendance Group Application Flow

Attendance group application flow defines the approval process of reviewing applications of an attendance group. Applications of the persons in the specified attendance group should be reviewed according to the group application flow.

Before You Start

- Make sure the current admin user has the permission for configuring the application flow. For details about user permissions, refer to ***Role and User Management*** .
- Make sure you have added roles of the application flow. See ***Add an Approval Role*** .

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Approval Management** → **Approval Flow** on the left.
3. Move the cursor on **Add**, and click **Attendance Group Approval Flow**.
4. On the left, set the basic information of the approval flow.

   Content Type

   Select what employees can apply for.

   Note

   The flow is enabled by default.
5. Click **Add Attendance Group** to select the attendance group(s).
6. Click to add the reviewer(s) for the application flow.
   1) Select the approval role of the reviewer(s).
   2) Select the department range from which the applications can be reviewed by the selected approval role(s).

      Note

      If the reviewers are from different departments, you need to select **All Departments**.

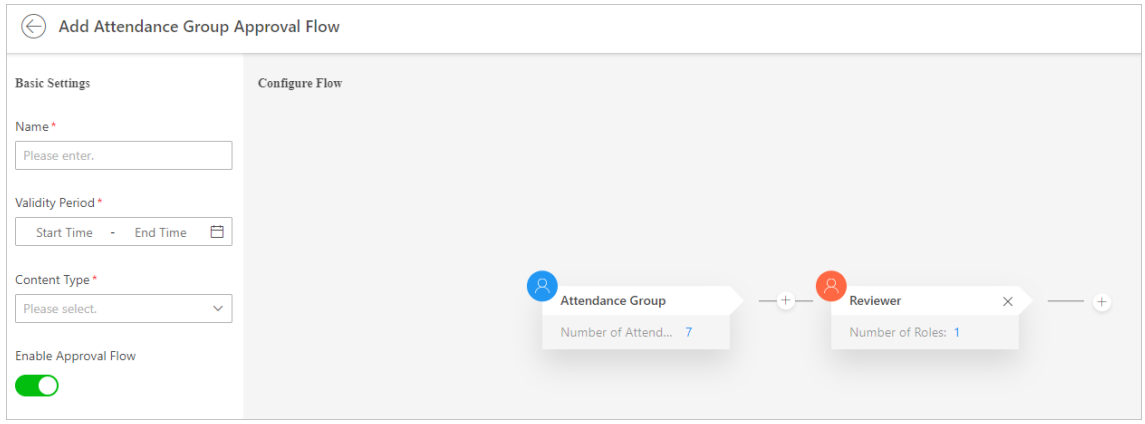


Figure 28-23 Add Attendance Group Application Flow

3) **Optional:** Select the approval role(s) to be notified of the review results.

4) **Optional:** Select the department range from which the approval role(s) will be notified.

Note

If the person(s) to be notified are from different departments, you need to select **All Departments**.

5) Click **Add**.

Note

You can repeat this step to add more reviewers and roles to be notified for the application flow.

7. Click **Finish** on the top right.
8. **Optional:** Perform the following operations as needed.

Edit Application Flow	In the application flow list, click the name of the application flow to edit it. • Click **Reviewer** or **Attendance Group** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete a node of the application flow.
Disable Application Flow	When adding an application flow, it is enabled by default. You can disable it in the application flow list.
Delete Application Flow	In the application flow list, you can click **Delete** to delete an application flow, or click **Delete All** to delete all application flows.

28.9.4 Add a Personal Approval Flow

Personal approval flow defines the approval process of reviewing applications of a person. Applications of the specified persons should be reviewed according to the personal approval flow.

Before You Start

- Make sure the current admin user has the permissions for configuring the approval flow. For details about user permissions, refer to ***Role and User Management*** .
- Make sure you have added roles of the approval flow. For details about adding roles, refer to ***Add an Approval Role*** .

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Approval** → **Approval Flow** on the left.
3. Move the cursor on **Add**, and click **Personal Approval Flow**.
4. On the left, set the basic information of the approval flow.
   1) Enter the name of the approval flow.
   2) Set the start time and end time of the validity time period.
   3) Select the application type (leave, check in&out correction, overtime, and check in&out via Mobile Client).
   4) **Optional:** Switch off **Enable Approval Flow** to disable the approval flow.

Note

The approval flow is enabled by default.

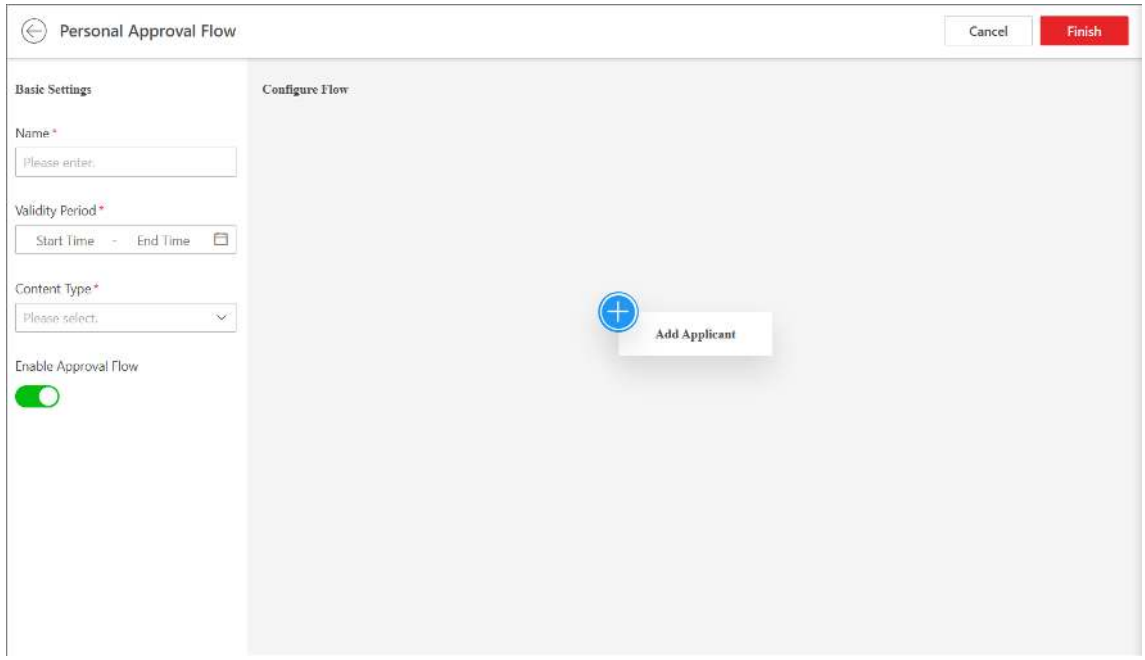


Figure 28-24 Add Personal Approval Flow

5. Click **Add Applicant** and to select the applicant(s).

Note

If you check **Select All Persons**, all persons who matched the search conditions you set will be selected.

6. Click + to add the reviewer(s) for the approval flow.
   1) Select the approval role of the reviewer(s).
   2) Select the department(s) of the selected role(s) allowed to review applications.

      Note

      If the reviewers are from the different department, you need to select **All Departments**.

   3) **Optional:** Select the approval role(s) to be notified of the review results in the current node.
   4) **Optional:** Select the department(s) of the approval role(s) to be notified.

      Note

      If the person(s) to be notified are from the different department, you need to select **All Departments**.

   5) Click **Add**.

Note

You can repeat this step to add more reviewers and persons to be notified for the approval flow.

7. Click **Finish**.

   The approval flow will be added to the approval flow list.

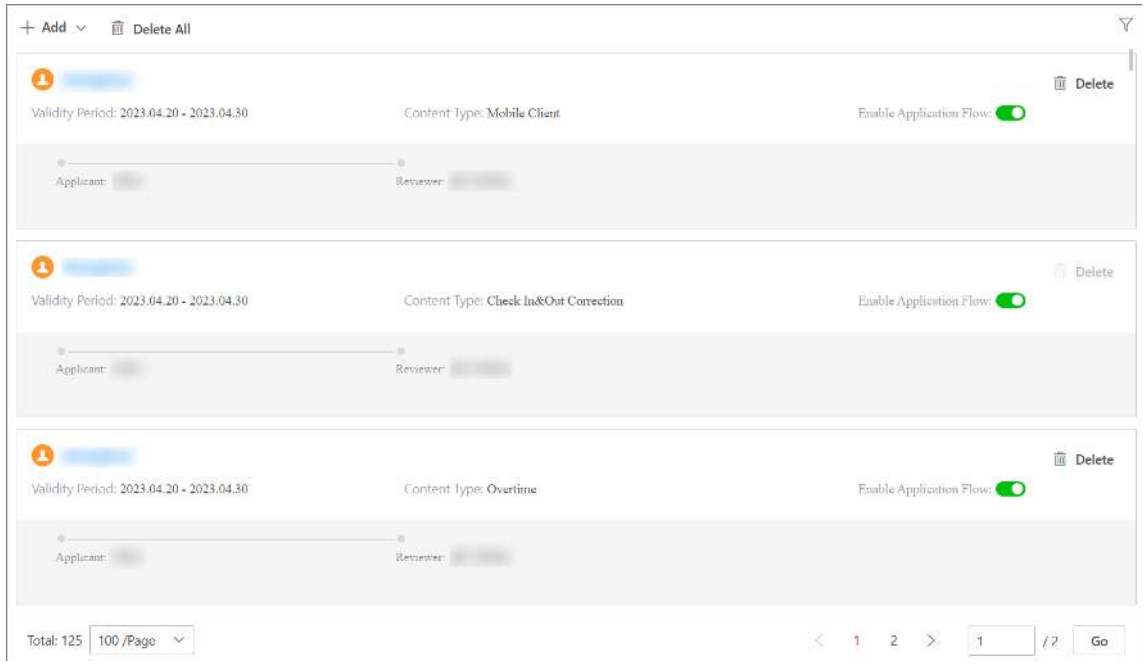


Figure 28-25 Approval Flow List

8. **Optional:** Perform the following operations as needed.

Edit Approval Flow	In the approval flow list, click the name of the approval flow to edit it. • Click **Reviewer** to edit the reviewer's approval role and the role to be notified (if any). • Click × to delete the node of the approval flow.
Disable Approval Flow	When adding an approval flow, it is enabled by default. You can disable the flow in the approval flow list.
Delete Approval Flow	In the approval flow list, you can click **Delete** to delete an approval flow, or click **Delete All** to delete all approval flows.
Filter Approval Flow	On the upper-right corner, click , specify conditions such as person name, approval flow type, or content type, and click **Filter** to filter the approval flows.

28.10 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.

28.10.1 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.

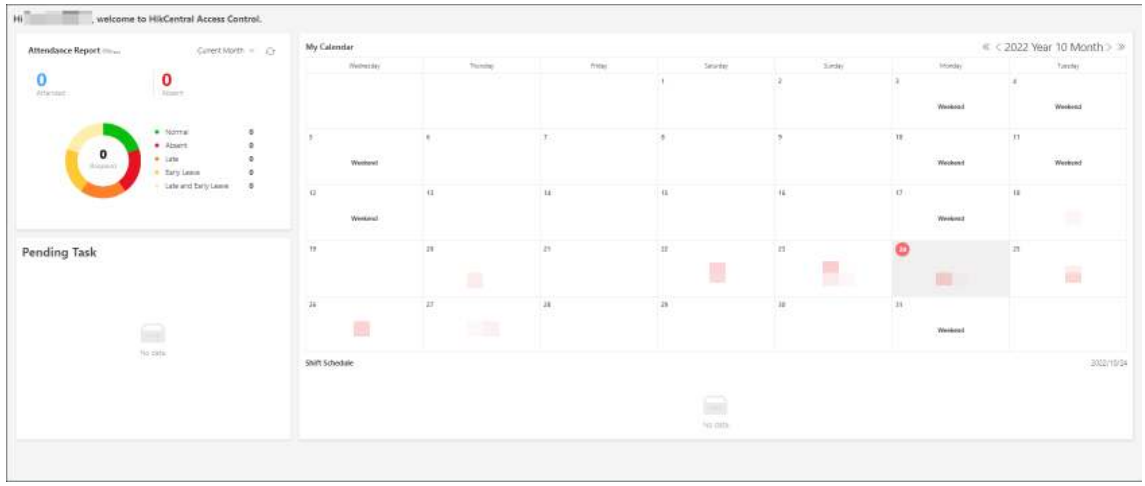


Figure 28-26 Overview of Personal Attendance Data

In **Attendance Report**, you can click ⌄ to select a time period to view the attendance records in the time period.

In **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*** .

In **Pending Task**, you can select an application and click **Handle** to handle the application.

28.10.2 Submit and View Applications

As an employee, you can submit attendance applications for leave, overtime, or attendance correction. Also, you can view the application details and the application flow to know the status of each handling.

Apply for a Leave

As an employee, you can apply for a leave by yourself. And the application will be reviewed by the administrator.

Before You Start

Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

Steps

1. Select **Apply → Leave** on the left.
2. Select the **Pending** tab.
3. Click **Add**.
4. In the pop-up window, set the following parameters as needed.

   Leave Type

The leave type such as sick leave, maternity leave, annual leave, etc.

Start Time

The start time of leave.

End Time

The end time of leave.

Application Reason (Optional)

The application reason for the leave.

Attachment (Optional)

The attachment for the leave application, such as the medical records for sick leave.

5. Click **Add**.

What to do next

View and export the submitted application. For details, refer to ***View and Export Attendance Records and Reports*** .

Apply for a Check-In/Out Correction

As an employee, you can apply for correcting the check-in or check-out records according to actual need (e.g., you forgot to check in or check out). And the application will be reviewed by the administrator.

Before You Start

Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

Steps

1. Select **Apply → Attendance Correction** on the left.
2. Select the **Pending** tab.
3. Click **Add**.
4. In the pop-up window, set the following parameters as needed.

Correction Item

The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.

Actual Time

The right time of the attendance item.

Application Reason (Optional)

The application reason for the correction.

Attachment (Optional)

The attachment for the correction application, such as the certificate of the right attendance time.

5. Click **Add**.

What to do next
View and export the submitted application. For details, refer to ***View and Export Attendance Records and Reports*** .

Apply for Overtime

As an employee, you can apply for working overtime. And the application will be reviewed by the administrator.

Before You Start
Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

Steps
1. Select **Apply → Overtime** on the left.
2. Select the **Pending** tab.
3. Click **Add**.
4. In the pop-up window, set the following parameters as needed.

   Overtime Type

   The type of working overtime.

   Start Time

   The start time of working overtime.

   End Time

   The end time of working overtime.

   Application Reason (Optional)

   The application reason for the leave.

   Attachment (Optional)

   The attachment for the overtime application.
5. Click **Add**.

What to do next
View and export the submitted application. For details, refer to ***View and Export Attendance Records and Reports*** .

View Submitted Applications

The employee can view the submitted application(s) for attendance.

Note
Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

1. Select **Apply → Leave/Overtime/Attendance Correction** on the left.
2. Select the **Pending** or **Closed** tab.

3. You can perform the following operations in the Operation column for application review.
   - Click to approve the employee's attendance application.
   - Click to reject the employee's attendance application.
   - Click to undo the employee's attendance application.
4. You can also select multiple employees to review or undo the employee's attendance applications.

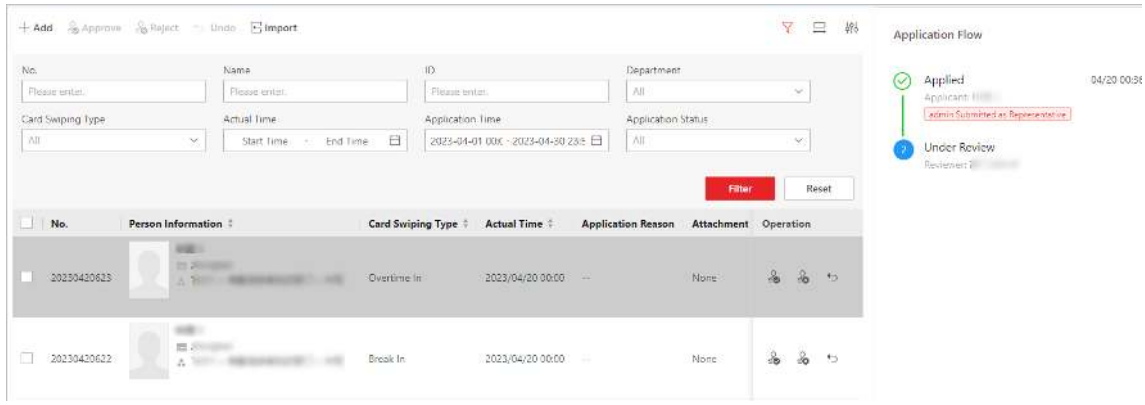


Figure 28-27 Review or Undo Employees' Applications

28.10.3 Review Employees' Applications

After employees submit the attendance applications for leave, overtime, attendance correction, and check-in/out via Mobile Client the administrator should review (including approving or rejecting) or undo the employee's applications.

On the top left, select → **Integrated Service → Attendance** . Select **Review → Leave / Check In&Out Correction / Overtime / Check-In/Out via Mobile Client** .

Click to filter target employees by setting conditions (such as name, ID, department). Select the target employee, the employee's application flow will be displayed on the right.

You can perform the following operations in the Operation column for application review.

- Click to approve the employee's attendance application.
- Click to reject the employee's attendance application.
- Click to undo the employee's attendance application.

You can also select multiple employees to review or undo the employee's attendance applications in a batch.

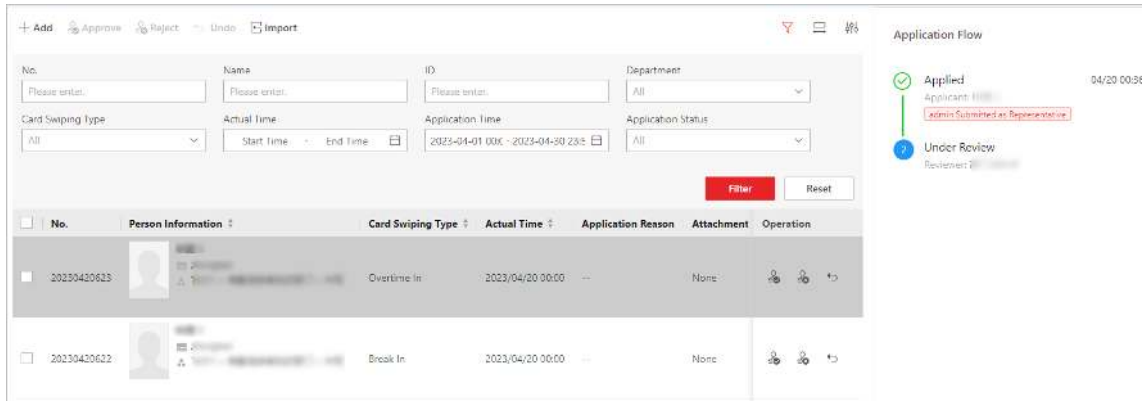


Figure 28-28 Review or Undo Employees' Applications

28.10.4 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.

Note

Log in to the platform via self-service. For details, refer to ***Login via Web Client (Employee)*** .

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.

28.11 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.

28.11.1 Apply for a Leave

As the administrator, you can perform leave application for the employee one by one.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Review** → **Leave** .
3. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
4. In the top left corner, click **Add**.
5. In the pop-up window, select the target person and then set the following parameters.

   Leave Type

   The leave type such as sick leave, maternity leave, annual leave, etc.

   Start Time

   The start time of leave.

   End Time

   The end time of leave.

   Application Reason (Optional)

   The application reason for the leave.

   Attachment (Optional)

   The attachment for the leave application, such as the medical records for sick leave.

   Auto Approve (Optional)

   If the box is checked, the added application for the person will be approved automatically.
6. Click **Add**.

What to do next

You can review or undo the application. For details, refer to ***Review or Undo Applications*** .

28.11.2 Apply for a Check-In/Out Correction

As the administrator, you can apply for correcting the check-in or check-out records for the employee one by one.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Review** → **Attendance Correction** .
3. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
4. In the top left corner, click **Add**.
5. In the pop-up window, select the target person and then set the following parameters.

   Correction Item

   The attendance item to be corrected, including check-in, check-out, break started, break ended, overtime-in, and overtime-out.

   Actual Time

The right time of the attendance item.

Application Reason (Optional)

The application reason for the correction.

Attachment (Optional)

The attachment for the correction application, such as the certificate of the right attendance time.

Auto Approve (Optional)

If the box is checked, the added application for the person will be approved automatically.

6. Click **Add**.

What to do next

You can review or undo the application. For details, refer to ***Review or Undo Applications*** .

28.11.3 Apply for Overtime

As the administrator, you can apply for working overtime for the employee one by one.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Review** → **Attendance Correction** .
3. **Optional:** Click , enter a person's full name, card No., ID, etc., and then click **Filter** to filter persons as required.
4. In the top left corner, click **Add**.
5. In the pop-up window, select the target person and then set the following parameters.

Overtime Type

The type of working overtime.

Start Time

The start time of working overtime.

End Time

The end time of working overtime.

Application Reason (Optional)

The application reason for the leave.

Attachment (Optional)

The attachment for the overtime application.

Auto Approve (Optional)

If the box is checked, the added application for the person will be approved automatically.

6. Click **Add**.

What to do next

You can review or undo the application. For details, refer to ***Review or Undo Applications*** .

28.11.4 Import Applications

As the administrator, you can batch apply for leave, overtime, or attendance correction for multiple employees.

Steps

1. On the top left, select → **Integrated Service → Attendance** .
2. Select **Review → Leave / Attendance Correction / Overtime** on the left.
3. **Optional:** Click , enter a person's full name, card No., ID etc., and then click **Filter** to filter persons as required.
4. Click **Import**.
5. In the pop-up window, click **Download Template** and edit the related information in the downloaded template.
6. Click and import the template with the corrected attendance records.
7. Click **Import**.

What to do next

You can review or undo the imported applications. For details, refer to ***Review or Undo Applications*** .

28.11.5 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 approve or reject) or undo the application.

1. On the top left, select → **Integrated Service → Attendance** .
2. Select **Review → Leave/Attendance Correction/Overtime/Mobile Client** .
3. (Optional) Click to filter the target employee by setting conditions (such as name, ID, department).
4. Select the target employee, the employee's application flow will be displayed on the right.
5. You can perform the following operations in the Operation column for application review.
   - Click to approve the employee's attendance application.
   - Click to reject the employee's attendance application.
   - Click to undo the employee's attendance application.
6. You can also select multiple employees to review or undo the employee's attendance applications.

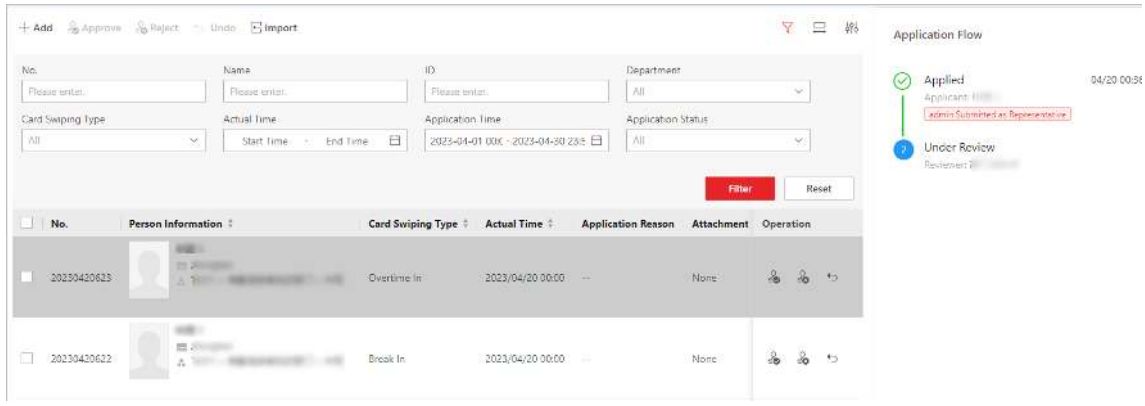


Figure 28-29 Review or Undo Employees' Applications

7. (Optional) On the upper-right corner, click to select the type of self-adaptive column width (complete or incomplete display of each column title).
8. (Optional) On the upper-right corner, click to select the items for custom display in the column.

28.12 View Attendance Records

Persons' attendance records will be recorded and stored in the system. You can view different types of attendance records.

On the top left, select → **Integrated Service** → **Attendance** . Then select **Attendance Record** on the left.

Click **Transaction**, **Time Card**, **Check In&Out Record**, **First & Last Access Report**, **Leave Record**, **Check In&Out Correction Record**, and **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.
- 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.

28.12.1 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.

On the top left, select → **Integrated Service** → **Attendance** . Then select **Attendance Record** → **Transaction** on the left.

Click **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.

28.13 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.

28.13.1 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 → **Integrated Service** → **Attendance** → **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.

28.13.2 View Daily/Weekly/Monthly/Summary Attendance Reports

You can view and export daily/weekly/monthly/summary attendance reports.

On the top left, select → **Integrated Service** → **Attendance** .

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.

Report Type	Description
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/ 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.
- 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.

28.13.3 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 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. For details, refer to ***Add Email Template for Sending Report Regularly*** .
- Set the email parameters such as sender address, SMTP server address and port, etc. For details, refer to ***Configure Email Account*** .

Steps

Note

The report is an Excel file.

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Basic Configuration** → **Report Settings** → **Scheduled Report** on the left.
3. Click **Add** (for first time) or click + .
4. Create a descriptive name for the report.
5. Select a type, format, and language for the scheduled report.

   Note

   You can select **TXT** as the format if the report type is **Time Card**.
6. In **Statistics Department**, check the department(s) / attendance group(s) of which the persons' attendance data will be delivered in this report.

   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).
7. **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.

   Note

   - You can check **Include Sub-Department** to display the persons of sub-departments.
   - You can click and select person status (all, employed, resigned), or enable **Additional Information** and enter the keyword in the text field to search for matched persons.
   - You can check **Select All** to select all persons.
8. Set the statistical cycle to **By Day**, **By Week**, or **By Month** and set the report time range and sending time.

   Daily Report

   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.

   Weekly/Monthly Report

The platform will send one report at the sending time every week or every month. The report contains the persons' attendance results of the recent one/two weeks or current/last month of the sending date.

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.

Note

- Daily or weekly report is not available when you set report type to monthly or weekly report.
- 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*** .

9. **Optional:** Click to set the effective period for the report.
10. **Optional:** Select and enable the way of sending the report from **Send Report via Email**, **Upload to SFTP**, and **Save to Local Storage**.

Note

To set up the SFTP or local storage, click > **SFTP Settings** or **Configure Local Storage**.

11. **Optional:** 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. For setting the email template, refer to ***Set Email Template*** .

12. Click **Add** to save the report schedule.

The report will be generated and sent to the recipient at the specified sending time.

28.13.4 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 → **Integrated Service** → **Attendance** .
2. Select **Custom Report** on the left.
3. Click + .
4. Create a descriptive name for the report in the **Report Name** field.
5. Choose whether to merge the data of the same person/department/date.
6. Select a sorting rule for records from the **Table Display Rule** drop-down list.
7. Select the data items you want to include in the report from **Optional Fields**.

Note

- Selected data items will show in **Selected Fields**.
- You can drag the items in **Selected Fields** to set the order of the items.

8. **Optional:** Click **Preview** to view the report to make sure the format and content are correct.
9. Click **Add** to save the custom report, or click **Add and Continue** to add another one.
10. **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.
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.

Steps

1. On the top left, select → **Integrated Service** → **Attendance** .
2. Select **Custom Report** on the left.
3. Select a custom report on the left pane, and click **Export** to open the Export Settings page.
4. On the Person Selection Method area, select **Department** / **Attendance Group**.
5. Check the desired departments / attendance groups.

Note

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).

6. **Optional:** Click **Select Extra Person**, and click to include individual persons whose attendance data will be delivered in this report.

Note

- 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.
- You can check **Select All** to select all persons.

7. Specify the time period by selecting the predefined time period, or clicking **Custom** to customize the start and end date..
8. Specify the report format.

9. Click **Export** to export the custom report to the local PC.

Chapter 29 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.

29.1 Video Intercom Overview

On the Video Intercom Overview page, you can view the resource health status and alarm input details including the statistics of calls and talks, and of notices in a specific period.

In the upper-left corner of the Home page, select → **Passing Management** → **Video Intercom** → **Overview** .

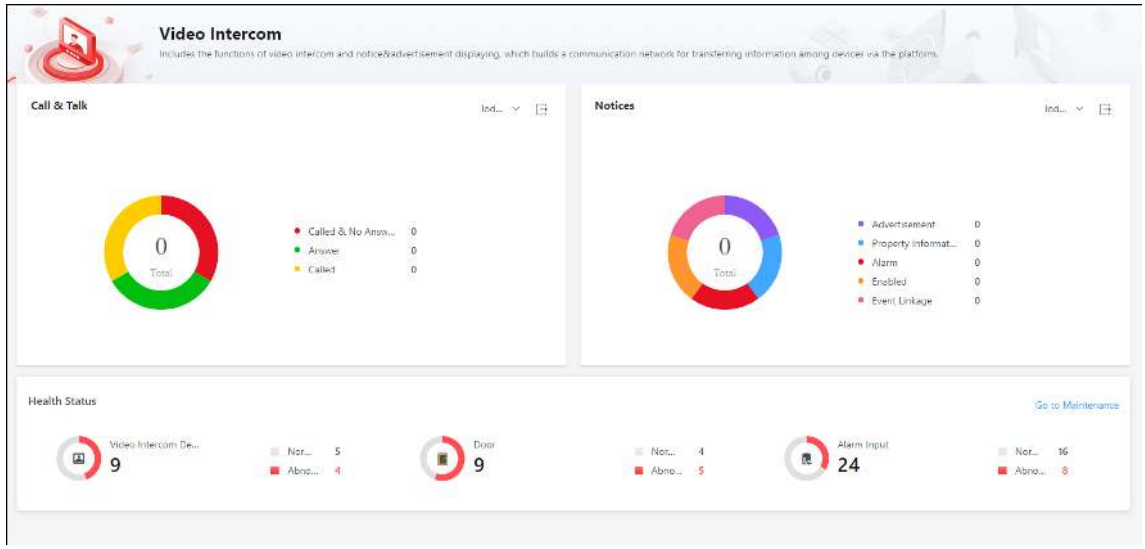


Figure 29-1 Video Intercom Overview

Perform the following operations as needed.

Operation	Description
View Resource Status	In Health Status, click the number under the resource type or the number besides **Abnormal** to go to the Maintenance page to view details of resources status or alarm input.
Go to Maintenance	In the upper-right corner of Health Status, click **Go to Maintenance** to enter the Maintenance module. For more about the Maintenance module, refer to ***Maintenance*** .
Filter Video Intercom Data	Click ⌄ and select a period to view the data of this period.
Export Video Intercom Data	Hover over ⊟ , select a file format, and click **Export** to export the data generated in the selected period.

29.2 Basic Settings of the Platform

You can add platform users as recipients of calls from devices and add receiving schedule templates. After adding recipients, when someone calls the platform, the recipient can receive the call according to the receiving schedule template. You can also add a call schedule template which defines when door stations can call indoor stations or call center. Besides, you can configure general parameters, including the storage location of configuration data and records, call parameters (such as the ring tone, auto hang up duration, and the maximum speaking duration with the device), and you can enable the function of receiving calls.

29.2.1 Add Call Recipients

After adding call recipients, when someone calls the system, the added recipient can receive and answer the call.

Note

Before recipients can receive calls form devices on the platform, you need to enable **Receive Calls** on the Call Parameter page. For details about enabling this function, refer to ***Configure General Parameters*** .

In the top left corner of Home page, select → **Passing Management → Video Intercom → Basic Configuration → Call Recipient** .

Click **Add** to enter the Add Call Recipient page.

Select users to receive calls, device(s) for receiving calls from, and receiving schedule template.

Note

Click **View** to view the schedule template details.

Click **Add**.

On the Call Recipients page, perform the following operations as needed.

- Check one or more call recipient and click **Delete** to delete the call recipient(s), or click → **Delete All** to delete all call recipients.
- In the upper-right corner, enter the keyword to search for specific users.
- Click to view the details of device(s) for receiving calls from or receiving schedule template.

29.2.2 Add Call Schedule Template

Call schedule template defines when door stations can call indoor stations or the call center. For example, if a resident is absent from home during workdays, while he/she is at home during weekends and holidays, the resident can customize a schedule template which calls the management center during workdays and calls the indoor station during weekends and holidays.

Steps

1. On the top navigation bar, select → **Passing Management** → **Video Intercom** → **Basic Configuration** → **Call Schedule Template** .
2. Click to add a schedule template.

   The two default templates, namely All-Day Call Schedule Template for Indoor Station and All-Day Call Schedule Template for Call Center, 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. Select **Indoor Station** or **Management Center**.

   Note

   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.
6. **Optional:** Edit weekly schedule.

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  .
Erase Task Time	Click **Erase**, and then click a grid or drag the cursor on the time line to erase the drawn time period.
7. **Optional:** Click **Add Holiday** to select an existing holiday template, or click **Add** to add a new template. For detailed information, see ***Set Holiday*** .
8. Click **Add** to save the template.
9. **Optional:** Select a template from the template list, and then click to delete it.

What to do next

Set call schedule for indoor stations and call center to define in which time period door stations can call indoor stations or call center. For details, refer to ***Add Call Schedule for Door Stations*** .

29.2.3 Configure General Parameters

You can configure general parameters, including the storage location of configuration data and records, and call parameters (such as the ring tone, auto hang up duration, and the maximum speaking duration with the device), and you can enable the function of receiving calls.

On the top navigation bar, select → **Passing Management** → **Video Intercom** → **Basic Configuration** → **General** .

Configure the following parameters as needed, then click **Save** to save settings.

Storage of Configuration Data

You can store the configuration data of video intercom.

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.

Storage of Records

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 ***Configure Storage for Imported Pictures and Files*** .
- For **pStor**, make sure you have added pStor as the recording server. For details, refer to ***Add pStor*** .

Call Parameter

Ringtone

Click ··· to select a ring tone and click **Play** to play the ring tone.

Auto Hang Up After

The call will be hung up automatically after the duration.

Max. Speaking Duration with Indoor Stations / Door Stations / Access Control Devices

Enter the maximum duration during which you can speak with the device.

Receive Calls

Switch on **Receive Calls** to receive the calling notification from the device to the platform.

29.2.4 Add or Configure 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. On the top navigation bar, select → **Passing Management → Video Intercom → Basic Configuration → 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.

29.3 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 Mifare encryption, you can enable **Mifare 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.

29.4 Manage Video Intercom Device

You can set location information for video intercom devices. After setting location information, you need to apply settings to all devices or the specified device(s).

29.4.1 Set Locations for Video Intercom Devices

You can add single device or batch add devices that have been added to the platform, and set location information for the added device(s).

Before You Start
Make sure you have added video intercom devices to the system.

Steps
1. On the top navigation bar, select → **Passing Management** → **Video Intercom** .
2. Select **Device Management** on the left.
3. Add the device(s).
   - Add single device.
     a. Click **Add** to add the device which has been added to the platform.
     b. Select a device type and a device.
     c. Set the location of the device, and click **Add**.
   - Add devices in a batch.
     a. Click → **Batch Add** to add devices which have been added to the platform.
     b. Select the device type.
     c. Select the adding mode to add device.

Manually Select	i. Select devices manually in the drop-down list. ii. Set required information. **Note** - If the community is divided into different sections, enter the corresponding number. If not,enter 1. - If the building is composed of only one unit, enter 1.
Batch Import	i. Click **Download Template** to download the template file to your PC. ii. Open the downloaded template file and enter the required information. iii. Click to select the file finished in the previous step.

     d. Click **Add**.
4. Click a device name.
5. In Location area, set parameters as needed.

Note

- If the community is divided into different sections, enter the corresponding number. If not,enter 1.
- If the building is composed of only one unit, enter 1.
- The parameters displayed vary with device types.

6. Set **Main and Sub Relation** to Main Module or Sub Module.

Note

This feature is only Available for door stations and indoor stations.

7. Click **Save** to save your edited information.

29.4.2 Apply Location to Video Intercom Devices

After setting location information for video intercom devices, you need to apply settings to devices.

On the top navigation bar, select → **Passing Management** → **Video Intercom** .

Select **Device Management** on the left.

Click **Apply Settings**.

Select the device(s) to apply.

All Devices

By default, the changed settings will be applied to all devices. If you check **Apply (Initial)**, first clear all former information applied to the devices, and then apply all settings configured on the platform this time to the devices.

Specified Device(s)

Click to select devices. The settings will be applied to the selected device(s).

Select an applying mode.

Apply Changes

Apply changes to the edited devices and devices linked to the edited devices.

Apply All

Apply all settings to the edited device and devices linked to the edited devices.

Apply (Initial)

First clear all former linkages applied to the devices, and then apply all linkages configured on the platform this time to the devices. This mode is mainly used for first-time deployment.

Click **Apply** to apply settings to the device(s).

The procedure of applying information will be displayed in the pop-up window, and the reasons for failures will be displayed in the Reason column. Move the cursor over , and click **Retry** to apply the settings to devices again. Also, move the cursor over , and click **View Details** to view the details. You can also click **Retry** to re-apply settings to devices.

29.5 Video Intercom Application

You can configure call schedule templates to define when indoor stations and call centers can receive the call from door stations. After you configure the templates, you can add the templates for door stations so that they will distribute calls to indoor stations or call centers as configured in the schedule template. Finally, you can apply call schedule to devices, so devices such as indoor/door stations and call centers can execute commands from the platform. Besides, after adding indoor station to the system, you can link camera with the added indoor station to view the video of the related camera(s) on the indoor station. You can also link single person to indoor stations for calling residents. In addition, you can 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.

29.5.1 Add Call Schedule for Door Stations

You can add call schedule for door stations to define when door stations can call indoor stations or call centers.

Before You Start

Make sure you have configured call schedule templates. For detailed information, see ***Add Call Schedule Template*** .

Steps

1. On the top navigation bar, select → **Passing Management** → **Video Intercom** → **Video Intercom Application** → **Door Station Call Schedule Settings** .
2. Click **Add** to add a door station call schedule.
3. Select a door station in the list.
4. Select a schedule template and room number for each button.

   Note

   As long as a template contains calling the call center, the Room cannot be selected. See ***Add Call Schedule Template*** for details about how to set a call schedule template.
5. **Optional:** Click to view the schedule details.
6. Click **Add** to save the schedule.

   The added schedule will be displayed in the list.
7. **Optional:** Perform the following operations.

Filter Door Stations	• Click on the top right to set conditions such as Door Station, Location Information, or Application Status to filter door stations. • Click **Reset** to reset search conditions.
Delete Door Stations	Select door stations and click **Delete** or click → **Delete All** to delete the door stations.

What to do next

You can apply call schedules to devices. For detailed information, see ***Apply Call Schedule to Door Stations*** .

29.5.2 Apply Call Schedule to Door Stations

You can apply call schedules to door stations so that the communication between devices and the platform will be supported.

Before You Start

Make sure that you have added call schedules for door stations. For detailed information, see ***Add Call Schedule for Door Stations*** .

Steps

1. On the top navigation bar, select → **Passing Management** → **Video Intercom** → **Video Intercom Application** → **Door Station Call Schedule Settings** .
2. Click **Apply Settings** on the top of the device list page.
3. Select **All Door Stations** or **Specified Door Station**.
4. **Optional:** If you choose **Specified Door Station**, select door station(s) or click to batch select the door station(s) that you want to apply the call schedule to and click **Add**.

   Note

   Only the door stations with added call schedules will be displayed.
5. **Optional:** Check **Apply (Initial)** to clear all former call schedules applied to the devices, and then apply all call schedules configured on the platform.
6. Click **Apply**.

   The procedure of applying information will be displayed in the pop-up window, and the reasons will be displayed in the Reason column. Move the cursor over , and click **Retry** to apply the schedules to devices again. Also, you can move the cursor over , and click **View Details** to view the details. You can also click **Retry** to re-apply the schedule to devices.

29.5.3 Link Resources with Indoor Stations

After adding an indoor station to the system, 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 single person with an indoor station or multiple persons with the indoor station(s) at a time, so that linked persons can calling residents. Besides, you can relate a doorbell with an indoor station.

Link Doorbell to an Indoor Station

You can link a doorbell with an indoor station. If the Call Management Center function of this doorbell is disabled, you can call the linked indoor station by the doorbell.

If you have added the doorbell to the system, you can link the doorbell with an indoor station as the following steps. If not, you can also link the doorbell with an indoor station when adding the doorbell (see ***Manage Video Intercom Device*** for more details).

Steps

1. On the top navigation bar, select → **Passing Management → Video Intercom → Video Intercom Application → Link Doorbell to Indoor Station** .
2. Click **Link** to enter the Link Doorbell with Indoor Station page.

   The added doorbells are displayed in the list.
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.
5. **Optional:** Check one or more doorbells and click **Unlink** to delete the doorbell(s).

Result

The doorbell will be linked to the selected indoor station(s).

Link Cameras to an Indoor Station

After adding indoor station to the system, you can link cameras to added indoor stations to view video of the linked camera(s) on the indoor station. Up to 16 cameras can be linked to one indoor station.

Before You Start

- Make sure you have added indoor station(s) to the system. For details, refer to ***Add a Video Intercom Device by IP Address*** .
- Make sure the camera(s) 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 Home page, select → **Passing Management → Video Intercom → Video Intercom Application → Link Camera to Indoor Station** .
2. Click **Link**.

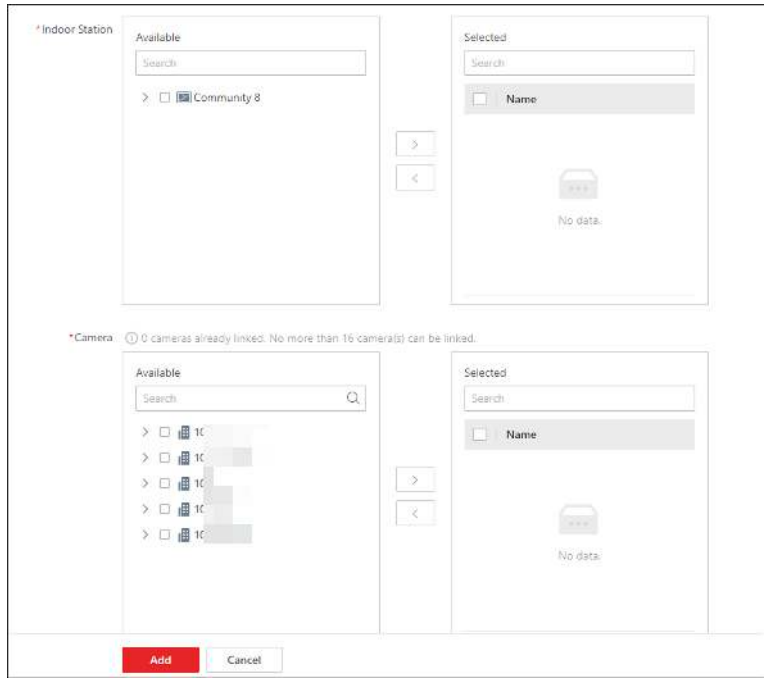


Figure 29-2 Add Linked Camera

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.

Note

You can enter a keyword to search for the target indoor station(s). And the keyword of corresponding device(s) will be displayed in red.

4. In the Camera list, check one or more cameras.

Note

No more than 16 cameras can be linked. You can enter a keyword to search for the target camera(s). And the keyword of corresponding camera(s) will be displayed in red.

5. Click **Add**.

Note

You can also delete the related camera(s) in the configuration page of the indoor station.

6. Click **Apply Settings** to apply the settings to devices.
7. **Optional:** Perform the following operations.

Filter Indoor Stations	• Click on the top right to set conditions such as Indoor Station, Location Information, or Application Status to filter door stations. • Click **Reset** to reset search conditions.
Unlink Doorbell from Indoor Stations	Select indoor stations and click **Unlink**.
View Linked Cameras	On the page of the added indoor station list, click › to view linked cameras.
Change Linked Cameras	On the page of the added indoor station list, click an indoor station name to change linked cameras.

Link Persons to an Indoor Station

The person needs to be linked to an indoor station, which is used for calling residents. You can link single person to an indoor station or multiple persons to indoor station(s) at a time. Here we introduce you how to batch link persons to indoor station(s).

Steps

Note

For details about linking single person to an indoor station, refer to ***Add a Single Person*** .

1. On the top navigation bar, select → **Passing Management** → **Video Intercom** .
2. Select **Video Intercom Application** → **Link Person to Indoor Station** on the left.
3. Click **Link**.

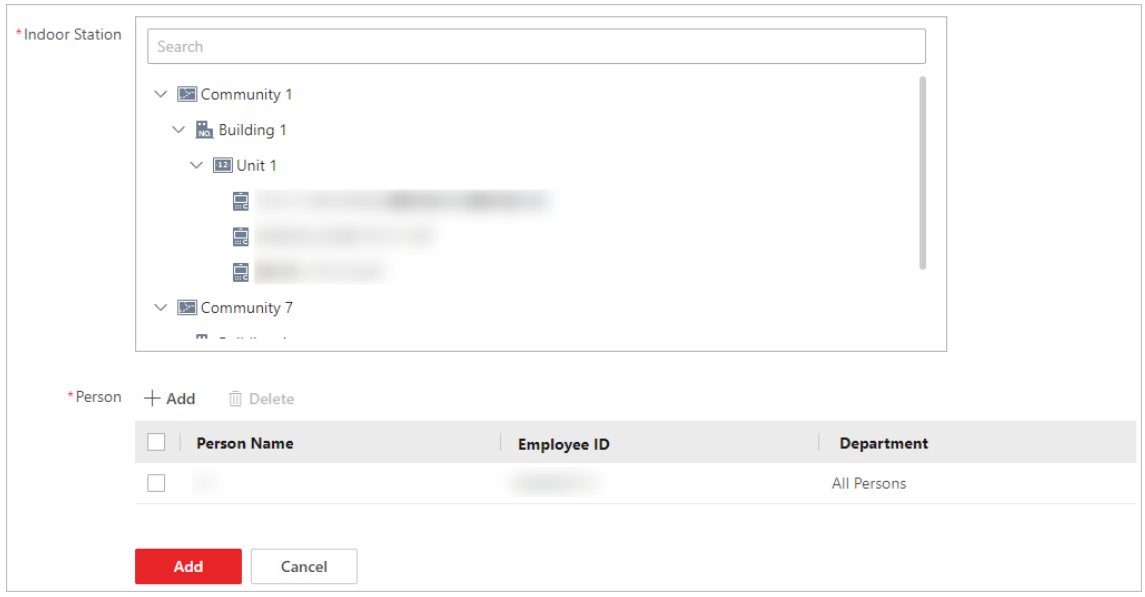


Figure 29-3 Add Linked Person

4. Select an indoor station.

Note

Up to 10 persons can be linked to one indoor station and the person cannot be linked to multiple indoor stations.

5. Click **Add** to select persons to be linked to the indoor station.
6. Click **Add**.

Note

A window will pop up for you to decide whether to overwrite the room No. linked to the person with one linked to the indoor station.

The linked person information will be applied to the indoor station(s).

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

Filter Indoor Stations	• Click on the top right to set conditions such as device name, location, person name, or employee ID to filter indoor stations. • Click **Reset** to reset search conditions.
Unlink Person from Indoor Stations	Select indoor stations and click **Unlink**.
View Linked Person	On the page of the added indoor station list, click › to view linked persons.
Change Linked Persons	On the page of the added indoor station list, click the name of the indoor station to change linked persons.

29.6 Apply Data to Indoor Station

The platform supports applying notices and software packages to indoor stations. This is used for scenes where you want to notify people an emergency in a batch, or install a software on indoor stations in a batch. After applying a software package to the indoor stations, the software will be installed automatically.

29.6.1 Manage Notices

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. Before applying the copied notice, you can also edit the notice.

Add and Apply a Notice

You add and apply notices to indoor stations. After adding and applying notices, you can delete, filter, and export them.

Steps

1. In the top left corner of the Home page, select → **Passing Management** → **Video Intercom** → **Apply Data to Indoor Station** → **Manage Notice** .
2. Select the **Apply Notice** tab, and click **Add** to add a notice.
3. Create a title of the notice.
4. Select a notice type.
5. **Optional:** Click + to add pictures.

   Note

   Up to 6 pictures can be added, and each picture should be no larger than 512 KB. The picture format should be JPG.
6. Enter the content of the notice.
7. Select indoor stations to receive the notice.
8. Click **Preview** to preview the notice.
9. Click **Apply** to apply the notice to indoor stations.
10. **Optional:** Perform the following operations.

Delete Notice	Check one or more notices and click **Delete**.
Export Notice	Check one or more notices and click **Export** to export notice information to the Excel/CVS file.

Filter Notices	In the upper-right corner, click to set filter conditions and click **Filter**.
View Notice Details	Click to view the basic information (title, notice type, etc.) and application status.

Note

On the Application Status page, you can also apply or search for notices.

Copy and Apply Notice to Indoor Stations

You can copy a notice and apply it to indoor stations conveniently. Before application, you can also edit the copied notice.

Note

Make sure you have added and applied a notice to indoor stations.

In the top left corner of the Home page, select → **Passing Management** → **Video Intercom** → **Apply Data to Indoor Station** → **Manage Notice** .

Select the **Apply Notice** tab.

The followings are two methods for copying and applying the notice(s).

1. If notice information needs no change, check one or more notices, and click **Copy and Apply**. The checked notice(s) will be copied and applied to indoor stations directly.
2. If notice information needs change, click to copy the current notice and edit the notice as needed. Click **Apply** to apply the notice to indoor stations.

29.6.2 Apply Software Package to Indoor Station

You can apply a software package to selected indoor stations and install the software automatically.

Before You Start

Make sure you have added indoor station(s) to the system. For details, refer to ***Add a Video Intercom Device by IP Address*** .

Steps

1. In the top left corner of the Home page, select → **Passing Management** → **Video Intercom** → **Apply Data to Indoor Station** → **Apply Software Package** .
2. Click **Apply Software Package** on the top.
3. Select **All Indoor Stations** or **Specified Indoor Station(s)**.

Note

If you select **Specified Indoor Station**, check indoor stations and click .

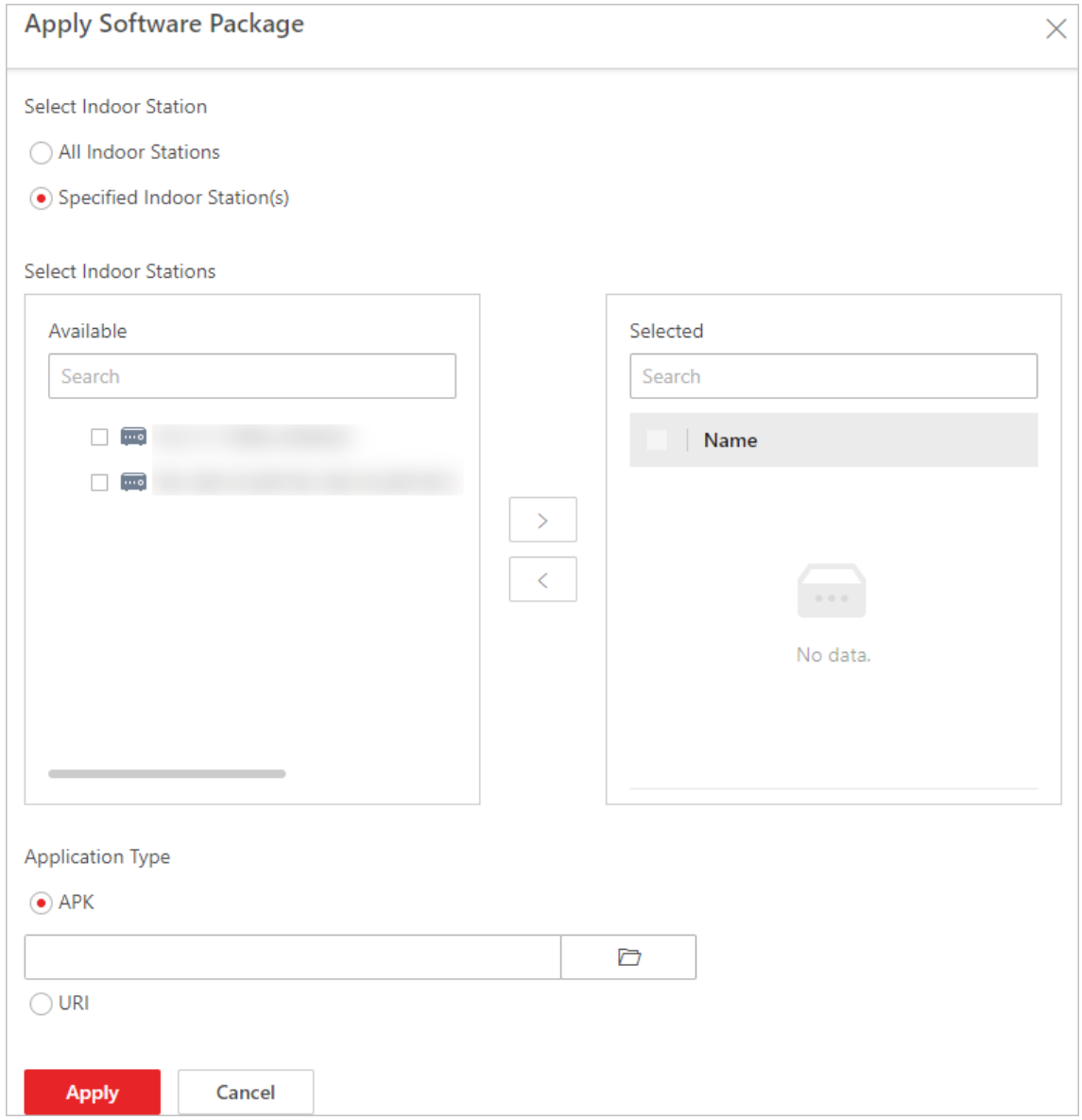


Figure 29-4 Apply Software Package

4. Select an application type.

   APK

   You need to upload an APK file so that the platform can send it to the device.

   URI

   Enter a URI so that the device will download the package via the URI and install it.

5. Click **Apply**.

   The device will install the software package automatically.

29.7 Apply Advertisements to Door Stations

You can add picture(s) or a video in the advertisements, then apply the advertisements to door stations. After applying advertisements, you can filter or delete them.

Steps

1. In the top left corner of the Home page, select → **Passing Management** → **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.

   Note

   You can click to remove it from the selected door station list on the left.
4. Add picture(s) or a video for an advertisement to be applied to door stations.

   Note

   For the picture advertisement, you can add more than one picture. For the video advertisement, you can add only one video.

   - 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**.
7. **Optional:** Perform the following operations.

Filter Advertisement	Click and set filter conditions such as device name, and then click **Filter**.
Delete Advertisement	Select one or multiple advertisements in the list and click **Delete** to delete the advertisements. Also, you can click **Delete All** to delete all of the advertisements.

29.8 View Event/Alarm Related Notices

You can filter and view event/alarm related notices by setting conditions. After filtering, you can export matched records, reapply failed notices, etc.

In the top left corner of the Home page, select → **Passing Management** → **Video Intercom** → **Manage Notice** .

Select the **Event/Alarm-Related Notice Applying Records** tab.

In the top right corner, click to set conditions to search for matched records. Click **Filter** and the matched records will be displayed.

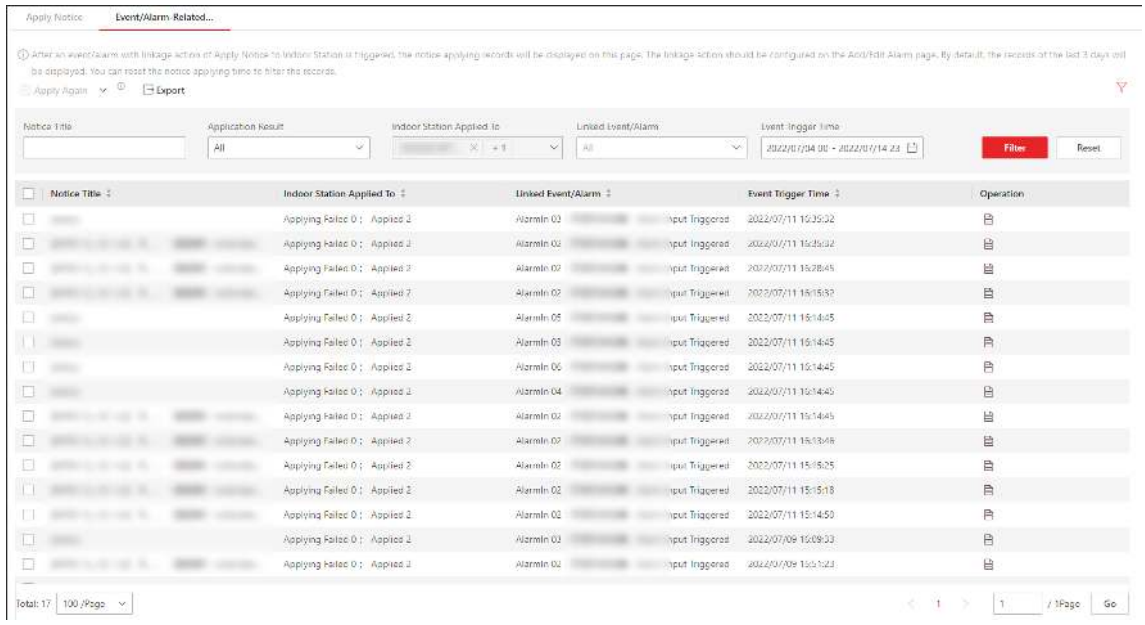


Figure 29-5 Filter Event/Alarm-Related Notice Applying Records

For the matched records, perform the following operations as needed.

Operation	Description
Reapply Failed Notice	• Check the failed notice(s) and click **Apply Again** in the top left corner to reapply the notice(s). • In the top left corner, click → **Reapply All** to reapply all failed notices.
Export Records	In the top left corner, click **Export** to export all matched records.
View Notice Details	In the Operation column, click to view the basic information and the application status of the notice.

Operation	Description
	Note If the notice fails to be applied, you can also click **Apply Again** to reapply it in the Details panel.

29.9 Call & Talk

In Call & Talk module, you can view contacts of indoor stations in a specific unit and call an indoor station conveniently. You can also view and export recents which include details such as the device name, call status, and device location. Besides, you can download recorded audios to the local PC.

29.9.1 Call an Indoor Stations

You can view names and locations of indoor stations, and person information. You can also call indoor stations directly on the platform in situations such as when the call the to the door station fails and when an emergency occurs.

In the top left corner of the Home page, select → **Passing Management → Video Intercom → Video Intercom → Contacts** .

On the left of the Contacts page, select an unit. The indoor stations in this unit will be listed on the right. In the upper-right corner, you can also set conditions and enter the keyword to search for indoor stations.

Click to call the indoor station.

29.9.2 View Recents

You can view and export call logs which include details such as the device name, call status, and device location. You can also download recorded audios to the local PC.

In the top left corner of the Home page, select → **Passing Management → Video Intercom → Video Intercom → Recents** .

Perform the following operations as needed.

Operation	Description
Export Logs	Check one or more devices and click **Export** to export call logs to Excel/CSV file format.
Filter Logs	Click to set conditions and click **Filter** to search for logs.
Download Recorded Audio	Click to download the recorded audio in MP4 format to the local PC.

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** .

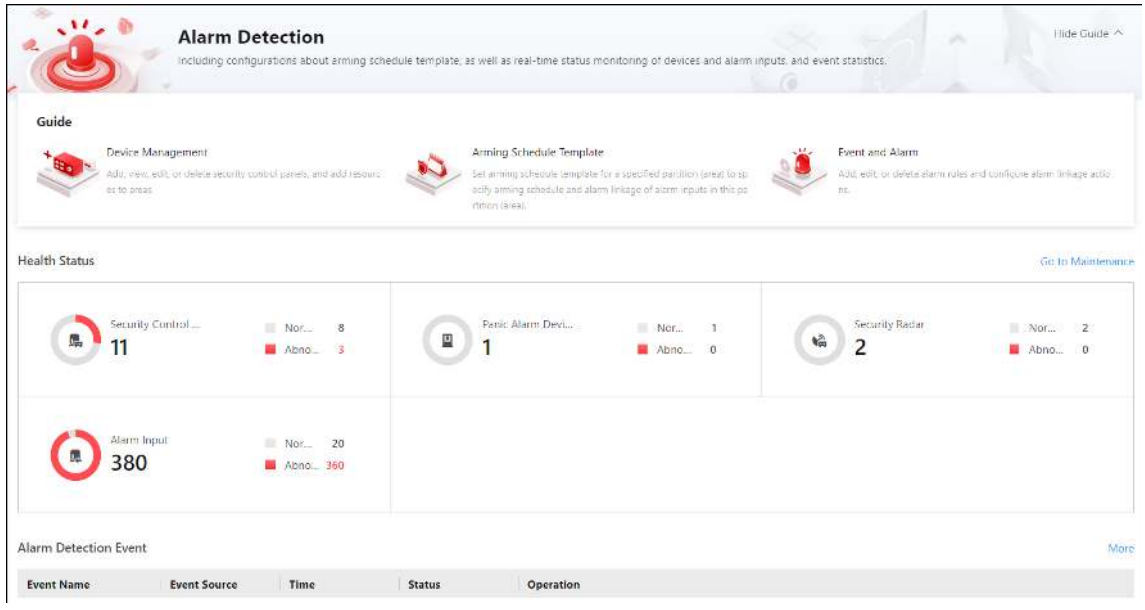


Figure 30-1 Alarm Detection Overview

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. Click **Go to Maintenance** to enter the Maintenance module. For more information, refer to ***Maintenance*** .
Alarm Detection Events	You can view the event details, including the event time, event source, time, status, and available operations.

30.2 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. See details in ***Manage Security Control Device*** .

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.

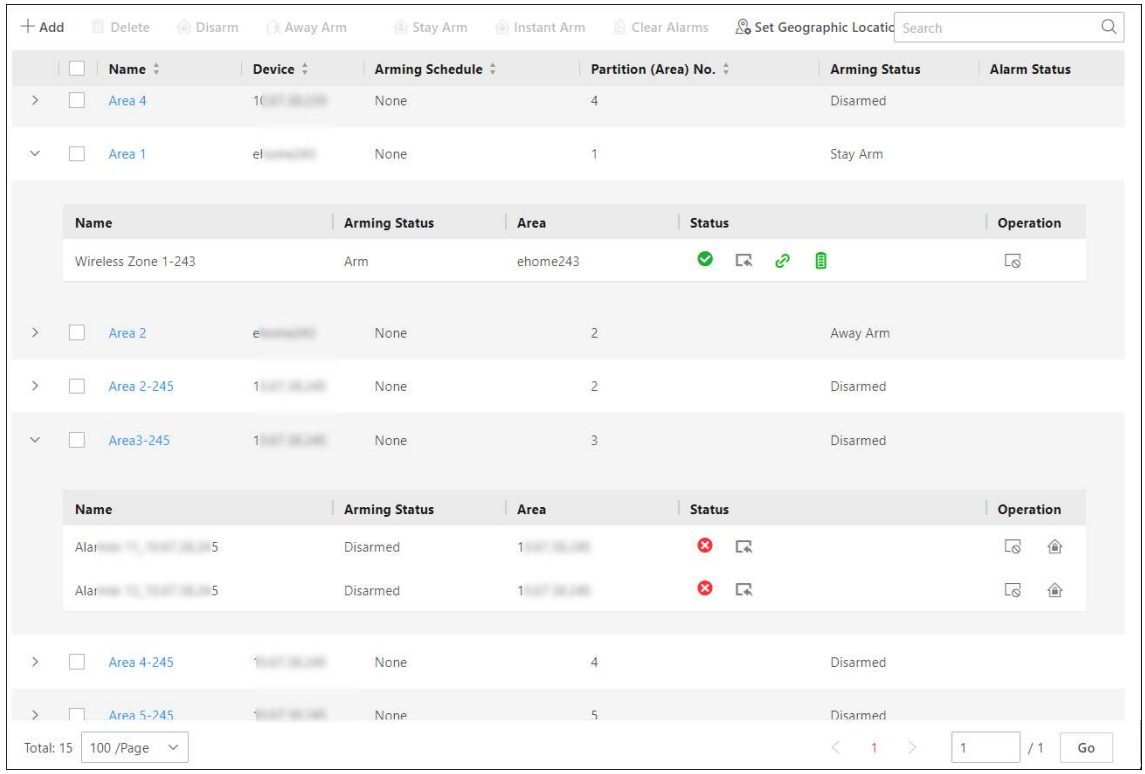


Figure 30-2 Partition (Area) List

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***). **Note** For the partition (area) of AX security control panel, you cannot edit the arming schedule via the platform. Only editing on the device is supported.
Delete Security Control Partition (Area)	Select one or multiple partitions (areas) and click **Delete**.
Arm/Disarm Security Control Partition (Area)	After arming the partitions (areas), the platform can receive the triggered alarms in the partitions (areas). 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.

Arm/Disarm Zone

Note

For partitions (areas) that are disarmed, you can arm only a part of their zones.

Click ⌄ to expand the partition (area) details and click / in the Operation column 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.

Click ⌄ to expand the partition (area) details and click / in the Operation column 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. See details in ***Add Hot Spot on Map*** .

30.3 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 Digital Signage Management

Digital signage management includes managing contents, schedules, release, materials, etc. It is widely applied to the industries of entertainment, finance, and traffic for information release. You can upload local and dynamic materials to the platform for creating contents. The contents should be reviewed before they are released and played on the terminals according to the configured schedule. Also, the platform supports more other functions such as cutting in programs.

Note

To perform operations in this module, make sure you are in the Digital Signage mode. See details in ***Switch Application Mode*** .

31.1 Digital Signage Overview

You can have an overview of the functions about digital signage and statistics for materials, programs, etc.

On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page, and then select **Digital Signage Overview** on the left navigation pane.

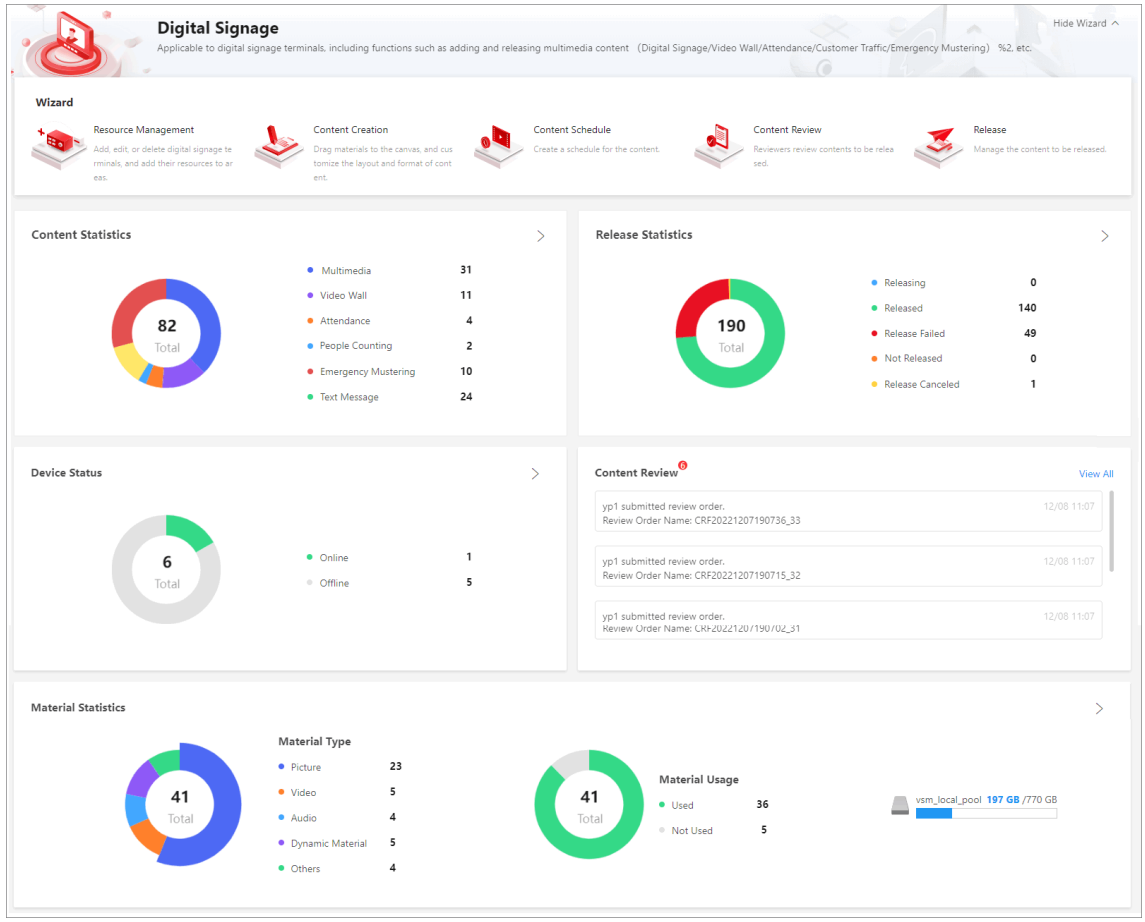


Figure 31-1 Digital Signage Overview

Table 31-1 Digital Signage Overview

Title	Description
Wizard	The wizard of the Digital Signage module, introducing the overall process.
Content Statistics	Displays the total number of contents and the number of contents in different types (i.e., Digital Signage, Video Wall, Attendance, People Counting, Emergency Mustering, and Text Message). You can click to enter the content creation page. For details about creating contents, refer to ***Content Creation*** .
Release Statistics	Displays different release status such as Releasing, Released, and Releasing Failed, as well as the number of each status. You can click to enter the Release page and view the release records. For details, refer to ***View Release Records*** .

Title	Description
Device Status	Displays total number of devices and status (Offline, Online), and the number of devices in each status. You can click to enter the Digital Signage Control page and do more operations. For details, refer to ***Control Digital Signage Terminal*** .
Content Review	Displays the details of content review, including the reviewer, submitted time, review order time, etc. You can click **View All** to enter the Content Review page and review content. For details, refer to ***Content Review*** .
Material Statistics	Displays the total number and the types (i.e., Picture, Video, Audio, Dynamic Material, and Others) of the added materials, the number of materials in each type, the number of used and unused materials, and the material usage. You can click to enter the material library page. For details about managing materials, refer to ***Material Library*** .

31.2 Content Creation

The platform supports creating contents and releasing them to the digital signage terminals. Then the contents can be played on the terminals to function as prompts, notices, etc. According to different application scenarios, you can create different contents, including multimedia program, video wall program, attendance program, people counting program, emergency mustering program, and text message. When creating programs, you can customize the layout of the program and add materials to the program as needed. When adding text messages, you can customize the font size, font color, etc., and preview the playing effects.

31.2.1 Create Multimedia Program

Multimedia program can be used in multiple application scenarios (e.g., playing a program related with commodity information at the entrance of a chain supermarket), helping to spread information in a convenient and efficient way.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Content Creation** → **Multimedia** .
3. Click **Add** or **Configure Now** (if you add the program for the first time).
4. In the pop-up window, configure program parameters.

   Name

   Define a program name that is easy to identify. You can enter up to 64 characters.

Screen Size

Select the screen size as Landscape Mode, Portrait Mode, or Custom.

Sharing Property

Public

All users in the current organization (i.e., the organization where the user who creates the program belongs to) and the higher-level organizations can see and use the program.

Private

All users in the current organization (i.e., the organization where the user who creates the program belongs to) can see and use the program.

Area

Set the area which the program belongs to.

Description

Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.

5. Click **Next**.
6. Select a template type and the corresponding template as needed.

Note

- You can click ☆ to add the template to My Favorites. Up to 1,000 templates can be added to My Favorites.
- You can click ☆ **My Favorites** in the lower-left corner to view and select the added template.

7. Click **OK** to enter the creating program page.

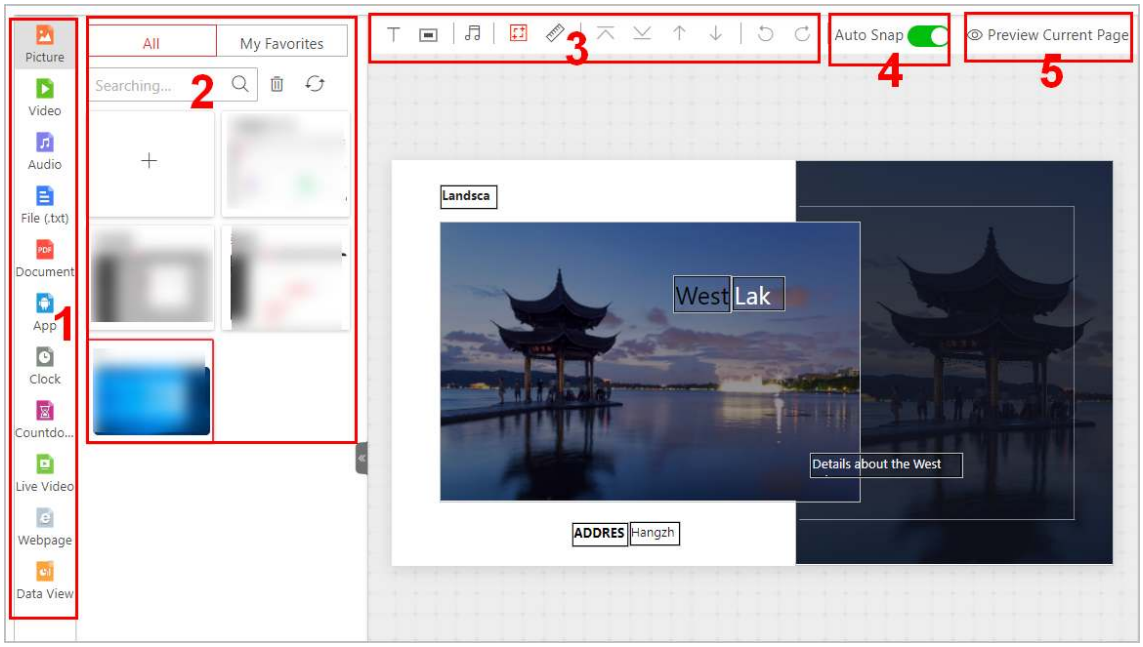


Figure 31-2 Create Program

Table 31-2 Page Description

Number	Description
1	There are multiple types of windows. An audio window cannot be added with a video window or live video window at the same time. Up to 16 windows can be added for one page.
2	You can select materials from **All** or **My Favorites** list. Click + to add other materials from local PC to the platform. Also, you can search materials, delete materials, and refresh material list. For the picture, video, and audio materials, you can move the mouse cursor to the upper-right corner of the material, and click to set its validity period. The material will be played within the validity period.
3	You can click to add a text window in the template; click to add a button window in the template (only available for touchscreen terminals); click / / / to make the window layer move up / move down / stick on top / stick at bottom. You can click to display the background panel, and drag an audio to the panel or to the current program page, then the selected audio will be added to the background music list. Click / to turn on or turn off the background music.

Number	Description
	You can click to align the material window with grid lines. You can click to display rulers in the right side and top side You can click / to undo or redo the operation.
4	You can enable **Auto Snap**, and the two windows will be connected when they are near enough.
5	• You can click **Preview Current Page** to preview the content of the current page. • During previewing, you can click or to pause or start playing. You can click or to adjust the playing speed as 1x, 2x, or 4x. Also, you can click to preview the current page in fullscreen.

8. Edit page properties, including page name, background, and play time type.

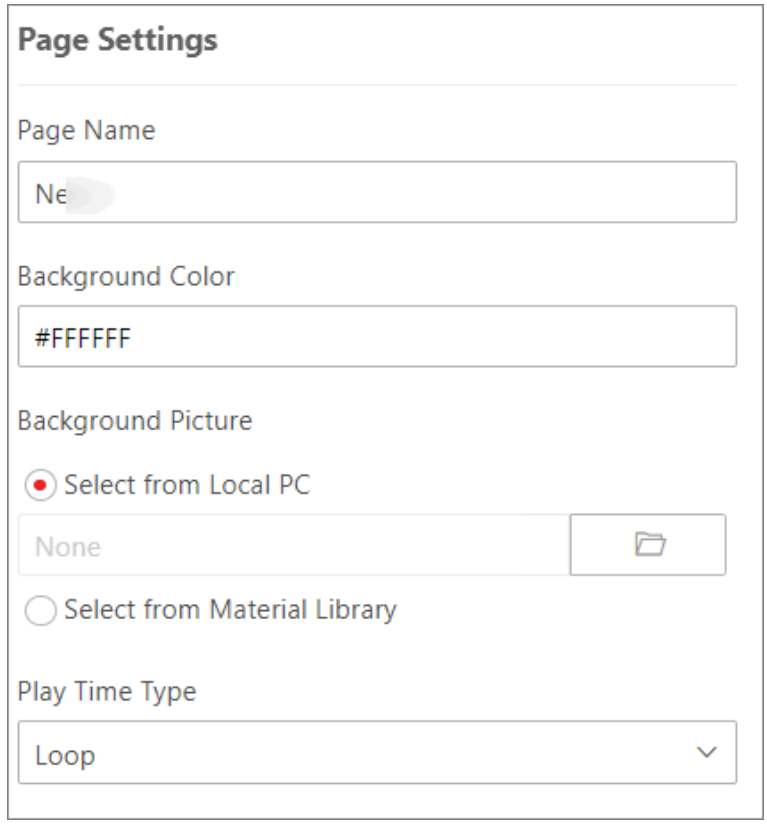


Figure 31-3 Page Settings

9. Optional: Add, delete, or adjust program pages at the bottom side.

Add Click / to add new page(s).

Delete Put the cursor on the page, and click on the upper right corner to delete the current page.

Adjust Sequence	Click a page and drag it to the desired location to adjust the sequence of program pages.

10. Select a material from the left list and drag it to the corresponding window in the template to add the selected material.

Note

- You can add the same or different types of materials to one window. When adding the same type of materials to one window, you can click **Create Window** to create a new window or click **Add More Material** to add more material to the current window.
- When adding pictures and videos, you can check **Actual Size** to display these materials in their original sizes.
- When adding texts, you can set the background color and transparency, as well as the scrolling direction and speed.
- When adding live videos, you can check **Close Audio**, then the program will be played without audio. Besides, only one Device Channel 1 can be added to one program page.
- When adding webpages, you can set the display format according to actual needs.
- When adding data view materials, you can select table, chart, dynamic picture, and dynamic text. For details about adding data view materials, refer to ***Create Dynamic Material*** .

11. Set window properties, including window position, window type, switching method, etc.

Note

You can set different parameters for different types of material windows.

Window Position

Set the window position by entering the width, height, and coordinate of the window.

Window Type

Normal

The normal window is displayed by default when the program is played. You can set a window jump link or page jump link for such a window.

Popup Window

The pop-up window is hidden by default. Only after setting a redirect link for a normal window and clicking the link, the hidden window will be popped up.

Switching Method

For Android touchscreen terminals, you can open the specified content by linking to a window or page.

No Skip

There is no linked window or page to the current window which is played on the terminal.

Jump to Next Window

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked window.

Jump to Next Page

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked page.

Move Window Layer

Click ↑ / ↓ / ⤒ / ⤓ to make the window layer move up / move down / stick on top / stick at bottom.

Switching Effect

Select the switching effect from the drop-down list for the current window. There are 11 types of switching effect.

Play Time (sec)

Set the playing duration for the current window.

Note

- The play time of a window can not exceed the playing time of a page, or the exceeding part of the program will not be played.
- For adding a webpage, you can set its play time as **Unlimited**.

12. Optional: On the current editing program page, perform the following operations.

Edit Program	Click ✎ to edit program parameters in the pop-up window. For details, refer to Step 3.
Preview Program	Click **Preview** to preview the program. During previewing, you can click ⏸ or ▶ to pause or start playing; click « or » to adjust the playing speed as 1x, 2x, or 4x; and click ⛶ to preview the program in fullscreen. For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click ‹ or › to preview the previous or the next page of the program.
Cut In Program	Click **Cut In** to cut in the current program. **Note** For details, refer to ***Cut in Program*** .
Create Schedule	Click **Next** to enter the managing schedules page and create a schedule for the program. **Note** For details, refer to ***Schedule Management*** .

13. Click **Save** to save the current program.
14. **Optional:** On the program list page, perform the following operations if needed.

View Program in List or Thumbnail Mode	Click / to view the added programs in the thumbnail mode or in the list mode.
Add Program to Favorites	Click ☆ to add the current program to Favorites.
Preview Program	Click to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in fullscreen. For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click or to preview the previous or the next page of the program.
Copy Program	Click to enter editing program page. Click **Save** on the upper right corner to copy the current program, and a new program with the same content is created. **Note** When copying a program (e.g., Program A) for the first time, the name of the new program (Program A_1) will be generated automatically. If you need to copy this program (Program A) for a second or more times, you should manually edit its name, or the program cannot be created successfully.
Cut In Program	Click to cut in the current program. For details, refer to ***Cut in Program*** .
Create Schedule	Click to enter the managing schedules page and create a schedule for the program. For details, refer to ***Schedule Management*** .
Enlarge Program Page	Click to enlarge the program page and view it.
Filter Program	Click , and filter programs by conditions such as name and sharing property.
Refresh Program List	Click **Refresh** to refresh the program list. The programs will be listed according to the time they are added.
Delete Program	Check one/more programs, or click **Select All** to select all programs, and click **Delete** to delete the selected programs.

Note

Programs that are releasing or cutting in cannot be deleted.

31.2.2 Create Video Wall Program

You can create video wall programs on the platform. The program can be used to display programs of multiple terminals joined in the video wall. The platform provides multiple layout choices for video wall programs. You can select a layout according to the actual scene and edit it as needed. After creating the program, you can preview the program, cut in program, etc.

Before You Start

You have configured video wall before applying the video wall programs. For details, refer to ***Configure Video Wall*** .

Steps

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Content Creation** → **Video Wall** .
3. Click **Add** or **Configure Now** (if you add the program for the first time).
4. In the pop-up window, configure program parameters.

Name

Define a program name that is easy to identify. You can enter up to 64 characters.

Video Wall Dimension

Set the video wall dimension.

Note

The maximum dimension is 1 × 10 or 10 × 1.

Digital Signage Screen Type

Select **Landscape Mode** or **Portrait Mode** as needed.

Sharing Property

Public

All users in the current organization (i.e., the organization where the user who creates the program belongs to) and the higher-level organizations can see and use the program.

Private

All users in the current organization (i.e., the organization where the user who creates the program belongs to) can see and use the program.

Area

Set the area which the program belongs to.

Description

Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.

5. Click **Next**.
6. **Optional:** Select video wall layout according to actual need.
   - When the dimension is no bigger than 1 × 5 or 5 × 1 (i.e., 1 × 2, 2 × 1, 1 × 3, 1 × 4, 1 × 5), select a predefined video wall layout from the list.
   - When the dimension is bigger than 1 × 5 or 5 × 1 (i.e., 1 × 6, 1 × 7, 1 × 8, 1 × 9, 1 × 10), select **No Layout** or **Custom Layout**.
7. Click **OK** to enter the creating program page.

Table 31-3 Page Description

Number	Description
1	There are 2 types of windows including Picture and Video.
2	You can select materials from **All** or **My Favorites** list. Click + to add other materials from local PC to the platform. Also, you can search materials, delete materials, and refresh material list.
3	You can click to display rulers in the right side and top side. You can click / / / to make the window layer move up / move down / stick on top / stick at bottom. You can click / to undo or redo the operation.
4	You can enable **Auto Snap**, and the two windows will be connected when they are near enough.
5	• You can click **Preview Current Page** to preview the content of the current page. • During previewing, you can click or to pause or start playing. You can click or to adjust the playing speed as 1x, 2x, or 4x. Also, you can click to preview the current page in fullscreen.

8. Edit page properties, including page name, background, and play time.

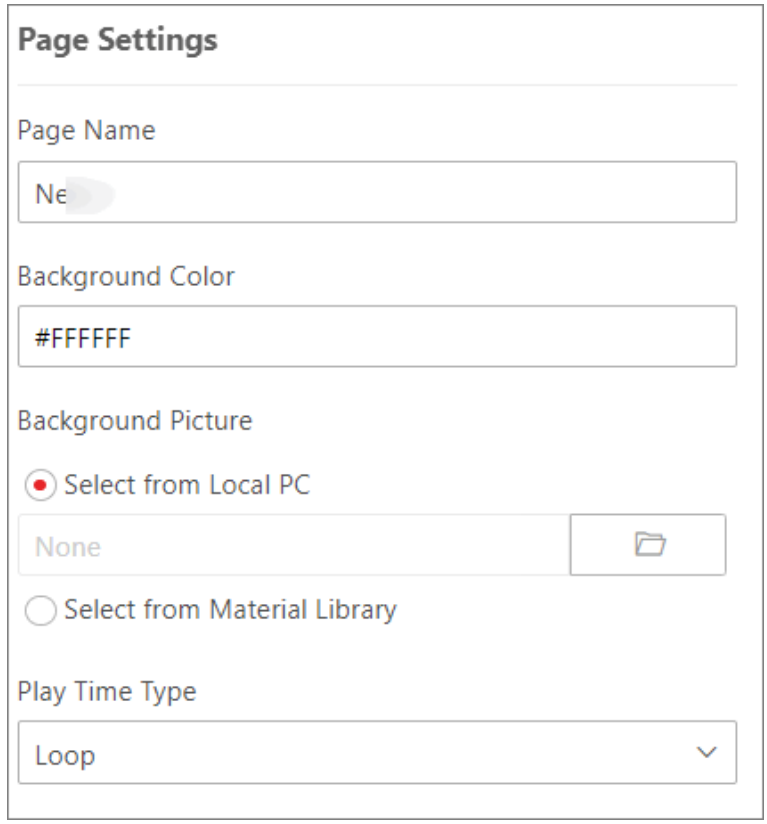


Figure 31-4 Page Settings

9. **Optional:** Add, adjust, or delete program page(s) at the bottom side.

Add	Click + / ⊕ to add new page(s).
Delete	Put the cursor on the page, and click ⊗ on the upper right corner to delete the current page.
Adjust Sequence	Click a page and drag it to the desired location to adjust the sequence of program pages.

10. Select a material from the left list and drag it to the corresponding section to add the selected material.

Note

- Only one material window is allowed in one section, and the size of window is the same as that of the section by default. When adding a new material to the section, the original material will be covered.
- You can select multiple materials simultaneously and add them to the same section.

11. Set window properties, including window position, window type, switching method, etc.

Current Window

Select the material added to the current window.

Window Position

Set the window position by entering the width, height, and coordinate of the window.

Window Type

Normal

The normal window is displayed by default when the program is played. You can set a window jump link or page jump link for such a window.

Popup Window

The pop-up window is hidden by default. Only after setting a redirect link for a normal window and clicking the link, the hidden window will be popped up.

Switching Method

For Android touchscreen terminals, you can open the specified content by linking to a window or page.

No Skip

When the Window A played on the terminal, there is no other pop-up window or page.

Jump to Next Window

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked window.

Jump to Next Page

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked page.

Move Window Layer

Click ↑ / ↓ / ⤒ / ⤓ to make the window layer move up / move down / stick on top / stick at bottom.

Switching Effect

Select the switching effect from the drop-down list for the current window. There are 11 types of switching effect.

Play Time (sec)

Set the playing duration for the current window.

Note

The play time of a window can not exceed the playing time of a page, or the exceeding part of the program will not be played.

12. Optional: On the current editing program page, perform the following operations if needed.

Edit Program	Click ✎ to edit program parameters in the pop-up window. For details, refer to Step 3.
Preview Program	Click **Preview** to preview the current program.

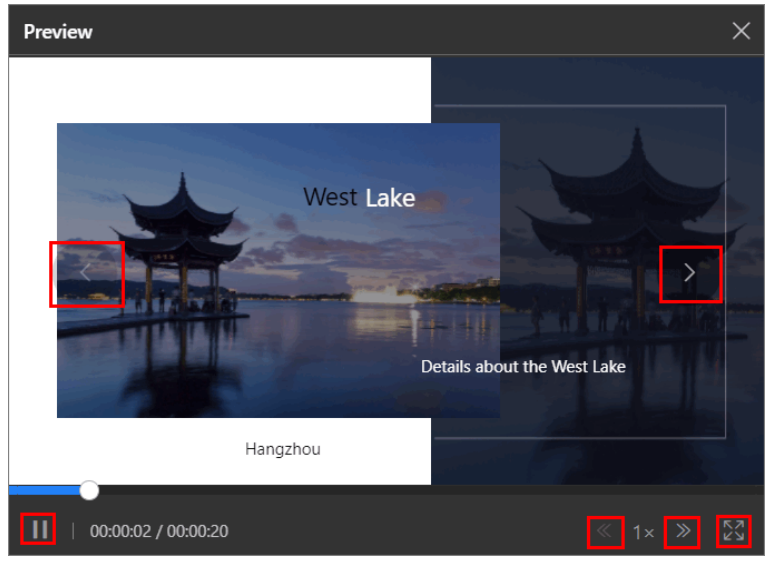


Figure 31-5 Preview Program

During previewing, you can click ⏸ or ▶ to pause or start playing; click « or » to adjust the playing speed as 1x, 2x, or 4x; and click ⛶ to preview the current page in fullscreen.

For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click ‹ or › to preview the previous or the next page of the program.

Cut In Program

Click **Cut In** to cut in the current program.

Note

For details, refer to ***Cut in Program*** .

Create Schedule

Click **Next** to enter the managing schedules page and create a schedule for the program.

Note

For details, refer to ***Schedule Management*** .

13. Click **Save** to save the current program.
14. **Optional:** On the program list page, perform the following operations if needed.

View Program in List or Thumbnail Mode

Click ⊞ / ☰ to view the added programs in the thumbnail mode or in the list mode.

Add Program to Favorites	Click ☆ to add the current program to Favorites.
Preview Program	Click to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in fullscreen. For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click or to preview the previous or the next page of the program.
Copy Program	Click to enter editing program page. Click **Save** on the upper right corner to copy the current program, and a new program with the same content is created. **Note** When copying a program (e.g., Program A) for the first time, the name of the new program (Program A_1) will be generated automatically. If you need to copy this program (Program A) for a second or more times, you should manually edit its name, or the program cannot be created successfully.
Cut In Program	Click to cut in the current program. For details, refer to ***Cut in Program*** .
Create Schedule	Click to enter the managing schedules page and create a schedule for the program. For details, refer to ***Schedule Management*** .
Enlarge Program Page	Click to enlarge the program page and view it.
Filter Program	Click , and filter programs by conditions such as name and sharing property.
Refresh Program List	Click **Refresh** to refresh the program list. The programs will be listed according to the time they are added.
Delete Program	Check one/more programs, or click **Select All** to select all programs, and click **Delete** to delete the selected programs. **Note** Programs that are releasing or cutting in cannot be deleted.

31.2.3 Create Attendance Program

You can create attendance programs on the platform. The program can be used to display the persons' basic information, check-in time and temperature information. You can also configure welcoming words for persons when they check in. The platform provides two types of program templates including Attendance and Temperature Screening Template and Attendance Template. You can select one template according to the actual scene and edit the predefined template as needed. After creating the program, you can preview the program, cut in program, etc.

Before You Start

You have added terminal(s) to the platform and have linked a device that supports face attendance with the terminal. For details, refer to ***Add Digital Signage Terminal*** and ***Link External Device to Terminal*** .

Steps

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Content Creation** → **Attendance** .
3. Click **Add** or **Configure Now** (if you add the program for the first time).
4. In the pop-up window, configure program parameters.

   Name

   Define a program name that is easy to identify. You can enter up to 64 characters.

   Screen Size

   Select the screen size as landscape mode or portrait mode.

   Sharing Property

   Public

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) and the higher-level organizations can see and use the program.

   Private

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) can see and use the program.

   Area

   Set the area which the program belongs to.

   Description

   Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.
5. Click **Next**.
6. Select a template type and the corresponding template as needed.

Note

- You can click ☆ to add the template to My Favorites. Up to 1,000 templates can be added to Favorites.
- You can click ☆ **My Favorites** in the lower-left corner to view and select the templates that have been added to Favorites.

7. Click **OK** to enter the creating program page.

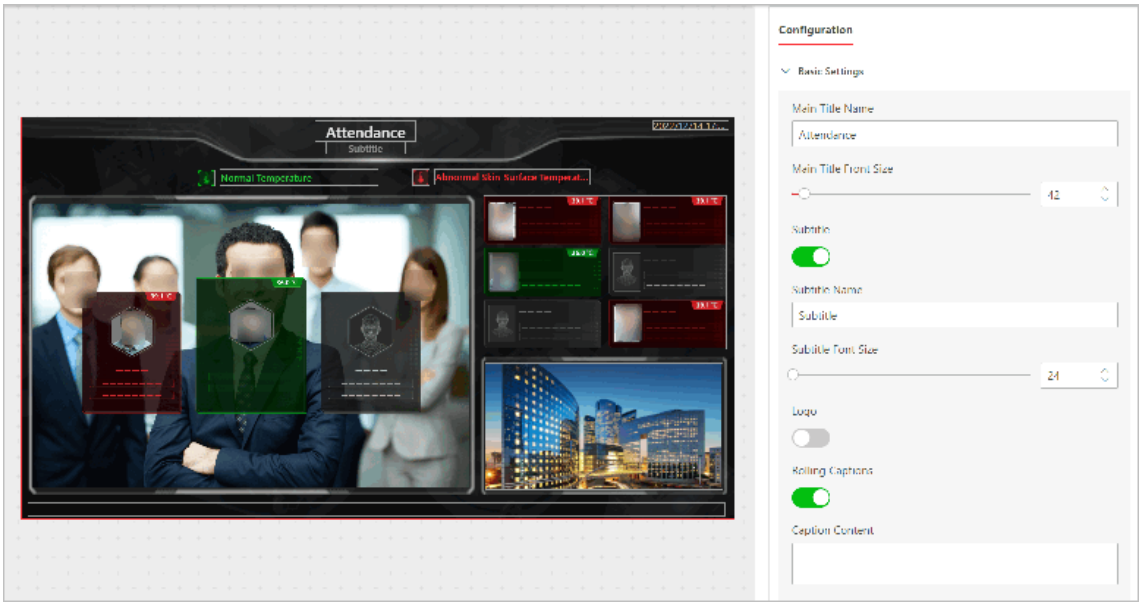


Figure 31-6 Create Program

Basic Settings

Configure the content and font size for main title and subtitle; enable **Logo** and select a logo from the local PC; enable **Rolling Captions** and configure the related content and scrolling direction; enable **Welcome Words** and configure the content of welcome words; enable **Audio Announcement** and configure the related settings such as announcement speed, the content of person's voice and voice prompt; and set the threshold of alarm temperature.

Check-in Information Display Settings

Select the time to show the check-in records or not to show records.

Note

There is some default information being displayed on the check-in records. If you need to display more check-in information, refer to ***Configure Device Privacy Settings*** .

More

Click 🗁 to set the background picture for the current program.

Note

Make sure you have added picture materials to the platform and the materials have been approved. For details, refer to ***Material Library*** and ***Content Review*** .

Advertisement Settings

You can add advertisements (pictures, videos, etc.) to the program, and configure switching effect and playing time for the advertisements.

Note

Only when selecting **Attendance Template**, you can configure advertisements.

8. **Optional:** On the current editing program page, perform the following operations if needed.

Edit Program	Click to edit program parameters in the pop-up window. For details, refer to Step 3.
Preview Program	Click **Preview** to preview the current program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in fullscreen.
Cut In Program	Click **Cut In** to cut in the current program. **Note** For details, refer to ***Cut in Program*** .
Create Schedule	Click **Next** to enter the managing schedules page and create a schedule for the program. **Note** For details, refer to ***Schedule Management*** .

9. Click **Save** to save the current program.
10. **Optional:** On the program list page, perform the following operations if needed.

View Program in List or Thumbnail Mode	Click / to view the added programs in the thumbnail mode or in the list mode.
Add Program to Favorites	Click to add the current program to Favorites.
Preview Program	Click to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the current page in fullscreen.

Copy Program	Click to enter editing program page. Click **Save** on the upper right corner to copy the current program, and a new program with the same content is created. **Note** When copying a program (e.g., Program A) for the first time, the name of the new program (Program A_1) will be generated automatically. If you need to copy this program (Program A) for a second or more times, you should manually edit its name, or the program cannot be created successfully.
Cut In Program	Click to cut in the current program. For details, refer to ***Cut in Program*** .
Create Schedule	Click to enter the managing schedules page and create a schedule for the program. For details, refer to ***Schedule Management*** .
Enlarge Program Page	Click to enlarge the program page and view it.
Filter Program	Click , and filter programs by conditions such as name and sharing property.
Refresh Program List	Click **Refresh** to refresh the program list. The programs will be listed according to the time they were added.
Delete Program	Check one/more programs, or click **Select All** to select all programs, and click **Delete** to delete the selected programs. **Note** Programs that are releasing or cutting in cannot be deleted.

31.2.4 Create People Counting Program

You can create people counting program on the platform. The program is used to display the people counting information (the remaining people and people stayed) in a certain location, mask information, and skin-surface temperature information. For people with no masks or whose temperature is abnormal, you can enable voice alarm for them. The platform provides two types of templates for different application scenarios: People Counting & Temperature Screening template, and Temperature Screening template. You can select a template according to the actual scene and edit the predefined template. After creating the program, you can preview the program, cut in program, etc.

Before You Start

You have added terminal(s) to the platform and have linked a device that supports people counting or temperature screening function with the terminal. For details, refer to ***Add Digital Signage Terminal*** and ***Link External Device to Terminal*** .

Steps

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Content Creation** → **People Counting** .
3. Click **Add** or **Configure Now** (if you add the program for the first time).
4. In the pop-up window, configure program parameters.

   Name

   Define a program name that is easy to identify. You can enter up to 64 characters.

   Screen Size

   Select the screen size as landscape mode or portrait mode.

   Sharing Property

   Public

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) and the higher-level organizations can see and use the program.

   Private

   All users in the current organization (i.e., the organization where the user who creates the program belongs to) can see and use the program.

   Area

   Set the area which the program belongs to.

   Description

   Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.
5. Click **Next**.
6. Select a template type and the corresponding template as needed.

   Note

   - You can click ☆ to add the template to My Favorites. Up to 1,000 templates can be added to Favorites.
   - You can click ☆ **My Favorites** in the lower-left corner to view and select the templates that have been added to Favorites.
7. Click **OK** to enter the creating program page.

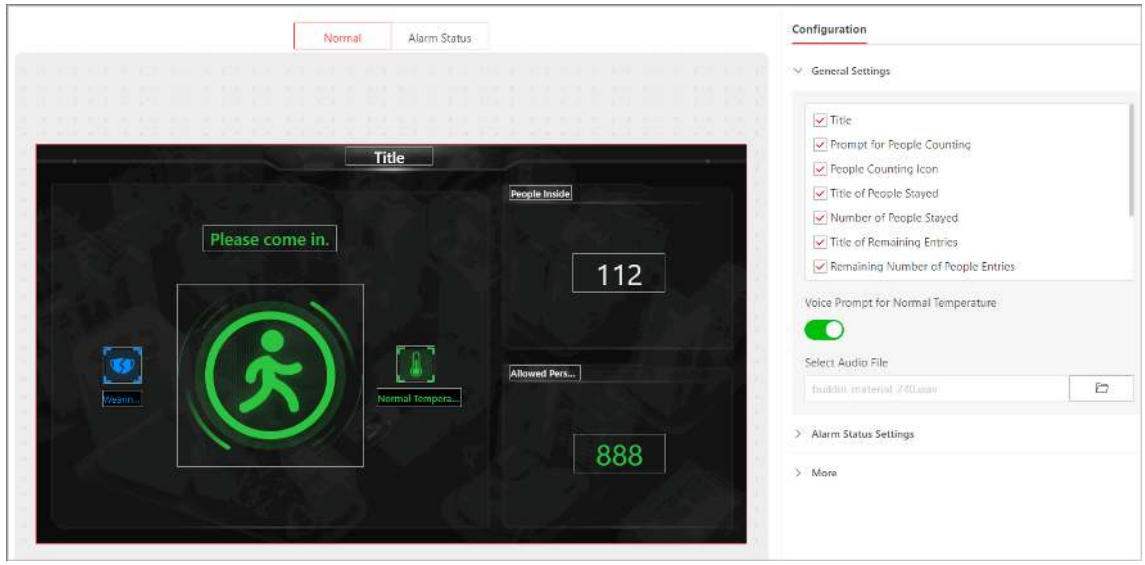


Figure 31-7 Create Program

Normal

The program only contains the people counting related information, such as remaining entry and people stayed.

Alarm Status

The program contains mask information, abnormal temperature information, and people counting related information.

General Settings

You can check whether to display title and people counting related information, such as prompt for people counting, people counting icon, and the number of people stayed. If you check **Title**, you can configure the font size and color for the title. You can enable audio prompt for normal temperature and select the corresponding audio file. The configurations in this area will be applied to **Normal** and **Alarm Status** simultaneously.

Alarm Status Settings

You can check whether to display alarm status related information, such as prompt for abnormal temperature; set maximum people stayed; enable voice alarm for no mask, abnormal temperature and people full, and configure the corresponding audio file for them.

Advertisement Settings

You can add advertisements (pictures, videos, etc.) to the program, and configure switching effect and playing time for the advertisements.

Note

Only when selecting **People Counting & Temperature Screening Template**, you can configure advertisements.

More

Click to set the background picture and the alarm picture for the current program.

8. **Optional:** On the current editing program page, perform the following operations if needed.

Edit Program	Click to edit program parameters in the pop-up window. For details, refer to Step 3.
Preview Program	Click **Preview** to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in fullscreen.
Cut In Program	Click **Cut In** to cut in the current program. **Note** For details, refer to ***Cut in Program*** .
Create Schedule	Click **Next** to enter the managing schedules page and create a schedule for the program. **Note** For details, refer to ***Schedule Management*** .

9. Click **Save** to save the current program.

10. **Optional:** On the program list page, perform the following operations if needed.

View Program in List or Thumbnail Mode	Click / to view the added programs in the thumbnail mode or in the list mode.
Add Program to Favorites	Click to add the current program to Favorites.
Preview Program	Click to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the current page in fullscreen.
Copy Program	Click to enter editing program page. Click **Save** on the upper right corner to copy the current program, and a new program with the same content is created. **Note** When copying a program (e.g., Program A) for the first time, the name of the new program (Program A_1) will be generated automatically. If you need to copy this program (Program A) for a second or more

times, you should manually edit its name, or the program cannot be created successfully.

Cut In Program	Click to cut in the current program. For details, refer to ***Cut in Program*** .
Create Schedule	Click to enter the managing schedules page and create a schedule for the program. For details, refer to ***Schedule Management*** .
Enlarge Program Page	Click to enlarge the program page and view it.
Filter Program	Click , and filter programs by conditions such as name and sharing property.
Refresh Program List	Click **Refresh** to refresh the program list. The programs will be listed according to the time they were added.
Delete Program	Check one or more programs, and click **Delete** to delete the selected programs.

Note

Programs that are releasing or cutting in cannot be deleted.

31.2.5 Create Emergency Mustering Program

Emergency mustering programs can be played when an emergency happens, helping people to receive timely emergency alerts and be out of danger as soon as possible.

Before You Start

You have added materials to the platform and the materials have been approved. For details, refer to ***Material Library*** and ***Content Review*** .

The created emergency mustering programs will be played on the device when the emergency is triggered.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Content Creation** → **Emergency Mustering** .
3. Click **Add** or **Configure Now** (if you add the program for the first time).
4. In the pop-up window, configure program parameters.

   Name

   Define a program name that is easy to identify. You can enter up to 64 characters.

   Screen Size

   Select the screen size as Landscape Mode, Portrait Mode, or Custom.

Sharing Property

Public

All users in the current organization (i.e., the organization where the user who creates the program belongs to) and the higher-level organizations can see and use the program.

Private

All users in the current organization (i.e., the organization where the user who creates the program belongs to) can see and use the program.

Area

Set the area which the program belongs to.

Description

Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.

5. Click **Next**.
6. Select a template.

Note

- You can click ☆ to add the template to My Favorites. Up to 1,000 templates can be added to My Favorites.
- You can click ☆ **My Favorites** in the lower-left corner to view and select the added template.

7. Click **OK** to enter the creating program page.

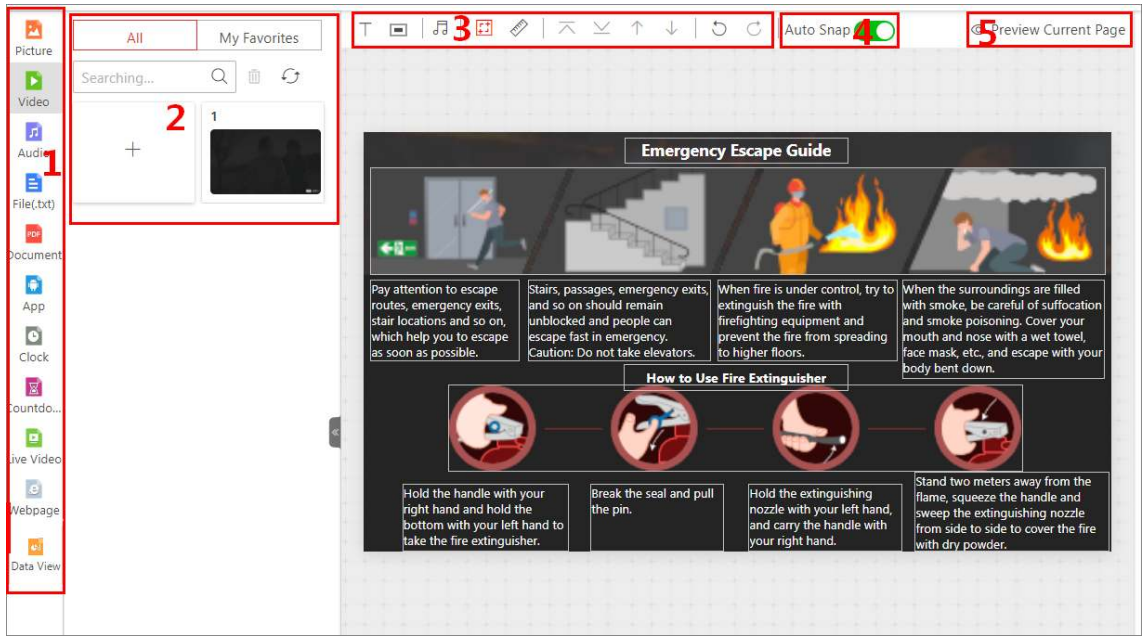


Figure 31-8 Create Program

Table 31-4 Page Description

Number	Description
1	There are multiple types of windows. An audio window cannot be added with a video window or live video window at the same time. Up to 16 windows can be added for one page.
2	You can select materials from **All** or **My Favorites** list. Click + to add other materials from local PC to the platform. Also, you can search materials, delete materials, and refresh material list. For the picture, video, and audio materials, you can move the mouse cursor to the upper-right corner of the material, and click to set its validity period. The material will be played within the validity period.
3	You can click to add a text window in the template; click to add a button window in the template (only available for touchscreen terminals); click / / / to make the window layer move up / move down / stick on top / stick at bottom. You can click  to display the background panel, and drag an audio to the panel or to the current program page, then the selected audio will be added to the background music list. Click / to turn on or turn off the background music. You can click to align the material window with grid lines. You can click to display rulers in the right side and top side You can click / to undo or redo the operation.
4	You can enable **Auto Snap**, and the two windows will be connected when they are near enough.
5	• You can click **Preview Current Page** to preview the content of the current page. • During previewing, you can click or to pause or start playing. You can click or to adjust the playing speed as 1x, 2x, or 4x. Also, you can click to preview the current page in fullscreen.

8. Edit page properties, including page name, background, and play time type.

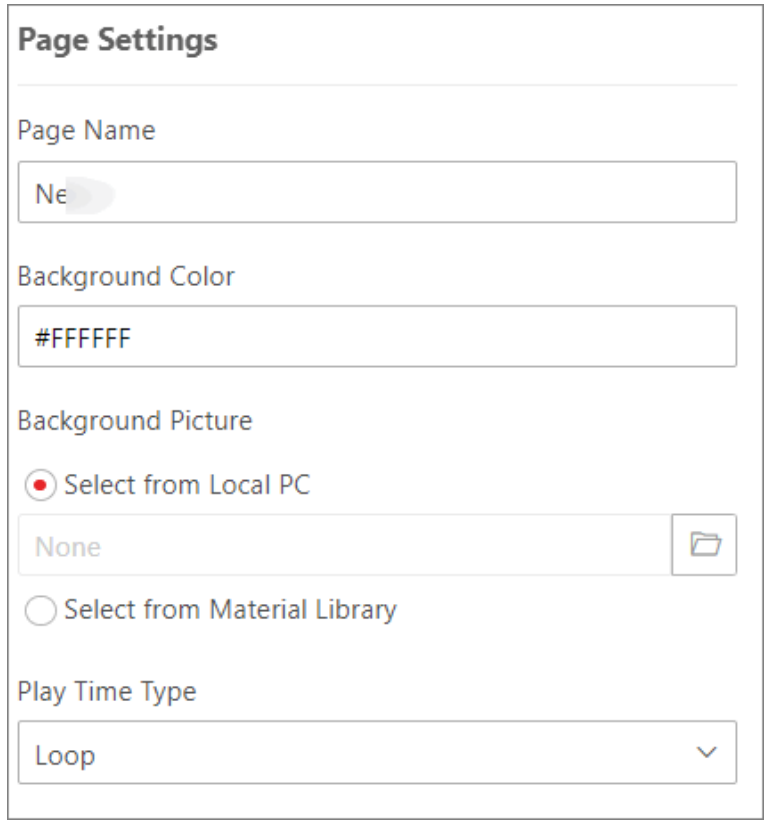


Figure 31-9 Page Settings

9. **Optional:** Add, delete, or adjust program pages at the bottom side.

Add	Click + / ⊕ to add new page(s).
Delete	Put the cursor on the page, and click ⊗ on the upper right corner to delete the current page.
Adjust Sequence	Click a page and drag it to the desired location to adjust the sequence of program pages.

10. Select a material from the left list and drag it to the corresponding window in the template to add the selected material.

Note

- You can add the same or different types of materials to one window. When adding the same type of materials to one window, you can click **Create Window** to create a new window or click **Add More Material** to add more material to the current window.
- When adding pictures and videos, you can check **Actual Size** to display these materials in their original sizes.
- When adding texts, you can set the background color and transparency, as well as the scrolling direction and speed.

- When adding live videos, you can check **Close Audio**, then the program will be played without audio. Besides, only one Device Channel 1 can be added to one program page.
- When adding webpages, you can set the display format according to actual needs.
- When adding data view materials, you can select table, chart, dynamic picture, and dynamic text. For details about adding data view materials, refer to ***Create Dynamic Material*** .

11. Set window properties, including window position, window type, switching method, etc.

Note

You can set different parameters for different types of material windows.

Window Position

Set the window position by entering the width, height, and coordinate of the window.

Window Type

Normal

The normal window is displayed by default when the program is played. You can set a window jump link or page jump link for such a window.

Popup Window

The pop-up window is hidden by default. Only after setting a redirect link for a normal window and clicking the link, the hidden window will be popped up.

Switching Method

For Android touchscreen terminals, you can open the specified content by linking to a window or page.

No Skip

There is no linked window or page to the current window which is played on the terminal.

Jump to Next Window

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked window.

Jump to Next Page

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked page.

Move Window Layer

Click ↑ / ↓ / ⤒ / ⤓ to make the window layer move up / move down / stick on top / stick at bottom.

Switching Effect

Select the switching effect from the drop-down list for the current window. There are 11 types of switching effect.

Play Time (sec)

Set the playing duration for the current window.

Note

- The play time of a window can not exceed the playing time of a page, or the exceeding part of the program will not be played.
- For adding a webpage, you can set its play time as **Unlimited**.

12. **Optional:** On the current editing program page, perform the following operations.

Edit Program	Click to edit program parameters in the pop-up window. For details, refer to Step 3.
Preview Program	Click **Preview** to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in fullscreen. For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click or to preview the previous or the next page of the program.
Release Program	Click **Release** to enter the Release page, select devices, and click **OK**. **Note** The program released will only be played when the emergency is triggered.

13. Click **Save** to save the current program.
14. **Optional:** On the program list page, perform the following operations if needed.

View Program in List or Thumbnail Mode	Click / to view the added programs in the thumbnail mode or in the list mode.
Add Program to Favorites	Click to add the current program to Favorites.
Preview Program	Click to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in fullscreen. For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click or to preview the previous or the next page of the program.

Copy Program	Click to enter editing program page. Click **Save** on the upper right corner to copy the current program, and a new program with the same content is created. **Note** When copying a program (e.g., Program A) for the first time, the name of the new program (Program A_1) will be generated automatically. If you need to copy this program (Program A) for a second or more times, you should manually edit its name, or the program cannot be created successfully.
Release Program	Click **Release** to enter the Release page, select devices, and click **OK**. **Note** The program released will only be played when the emergency is triggered.
Enlarge Program Page	Click to enlarge the program page and view it.
View Device Release Details	Click to view release details of the program on the device.
Filter Program	Click , and filter programs by conditions such as name and sharing property.
Refresh Program List	Click **Refresh** to refresh the program list. The programs will be listed according to the time they are added.
Delete Program	Check one or more programs, and click **Delete** to delete the selected programs. **Note** Programs that are releasing cannot be deleted.

31.2.6 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. For details, refer to ***Manage Digital Signage Terminals*** .

Steps

Note

For one device, only the latest added text notification can be displayed.

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Content Creation** → **Emergency Mustering** .
3. Click **Text Notification** → **Configure Now / Add** to enter Add Text Notification page.

   Note

   Click **Configure Now** if you have not added a text notification before.

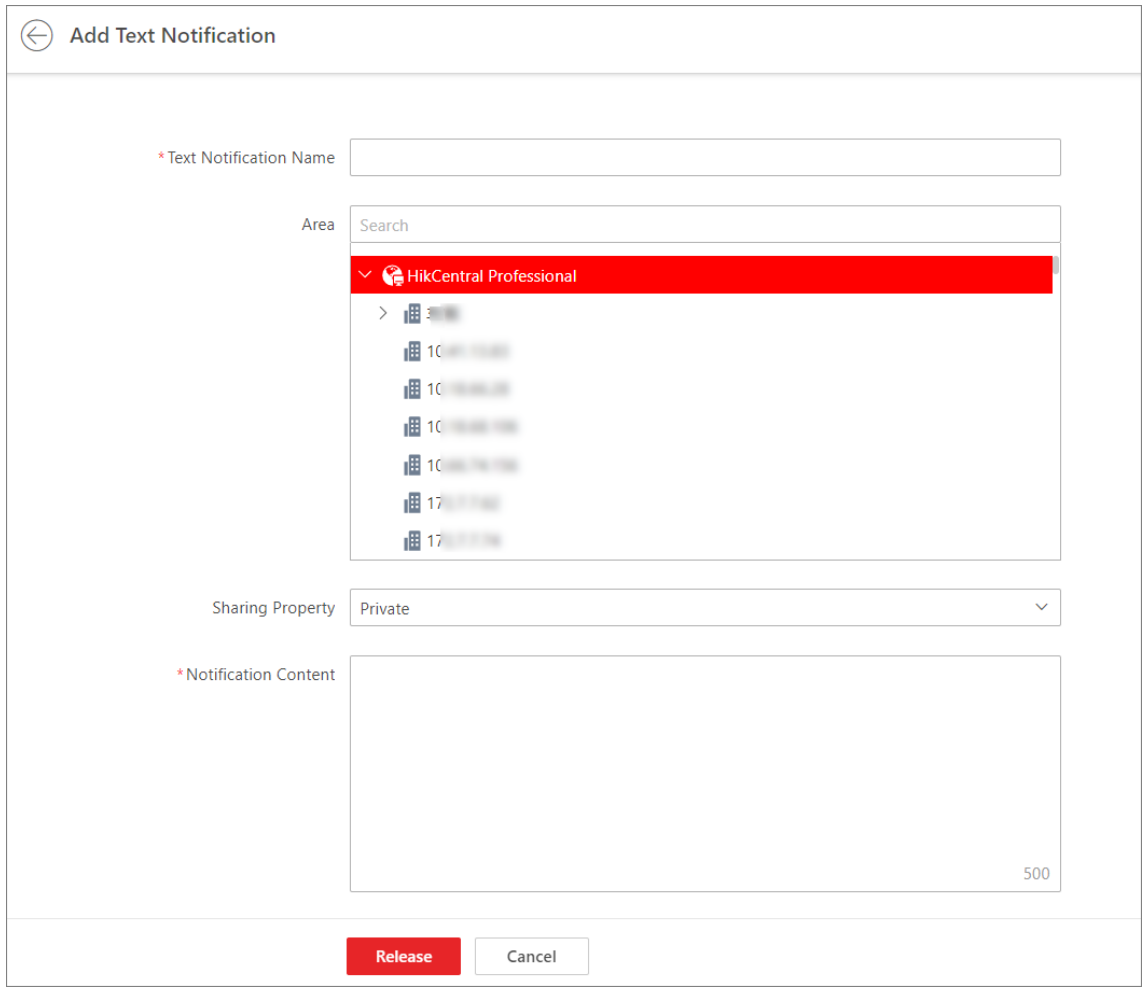


Figure 31-10 Add Text Notification

4. Set the needed parameters, such as text notification name and content.

   Text Notification Name

The name of the text notification.

Notification Content

The content of the text notification.

Select Device

Select device(s) in the left list and add them to the right list. The text notification will be displayed on the selected devices.

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.

5. Click **Release**.

Note

The text notification is released and will be displayed when the emergency is triggered.

6. **Optional:** Click **View Emergency Mustering Configuration** in the upper-right corner to enter Emergency Mustering module and view emergency mustering configurations.

Note

For details, refer to ***Emergency Solution Settings*** .

7. **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	Click 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. **Note** 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	Click to view release details of the text notification on the device.
Filter Text Notification	Click , and filter text notifications by conditions such as name and sharing property.
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.

31.2.7 Add Text Message

You can add text messages and apply them to terminals. When adding the text message, you can set the parameters and preview the displaying effect on the platform. After applying the text message to the terminal, the text message will be played according to the configured time and method.

Before You Start

Make sure you have added terminal(s) to the platform. For details, refer to ***Add Digital Signage Terminal*** .

Steps

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Content Creation** → **Text Message** .
3. Click **Add** or **Configure Now** (if you add the text message for the first time) to enter the Add Text Message page.
4. Enter the task name.
5. Select an area from the drop-down list.

   Note

   For details about how to add areas, refer to ***Add an Area for Current Site*** .
6. In the **Edit Text Message** area, set the text 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 right side of the page.
7. **Optional:** In the **Text Window Property** area, set parameters such as the configuration mode and font size for the text message.
8. Save or release the text message.
   - In the upper-right corner, click **Save** to save the above settings and release the text message later.
   - In the upper-right corner, click **Release** to enter Release Text Message page, select one or more devices in the list, and click **Release** to start releasing the text message to the selected devices.

     Note

     You can view the release progress and result on the right side of the page.
9. **Optional:** Perform the following operations in the text message list.

Refresh Text Message List	Click **Refresh** to refresh the list of text messages.
Edit Text Message	Click a name on the **Text Message Name** column to edit the text message, including its name, area, content, and text window property.
Release Text Message	Click a name on the **Text Message Name** column to enter the Edit Text Message page, and click **Release** in the upper-right corner to enter Release Text Message page. On the Release Text Message page, select one or more devices in the list, and click **Release** to start releasing the text message to the selected devices. **Note** You can view the release progress and result on the right side of the page.
Delete Text Message	Check one or more text messages, and click **Delete** to delete the selected text messages.

31.3 Schedule Management

You can create a schedule and define a playing schedule to play the added programs on the terminals according to the scheduled time or method. The platform supports default schedule, loop schedule, or you can customize your schedule including playing by date or by week. For the added schedules, you can perform more operations such as editing, releasing, searching, exporting, and adding to favorites.

31.3.1 Create a Schedule

You can create schedules for the added programs so that the programs will be played on the terminals according to the scheduled time or method. For the added schedules, you can perform more operations such as editing, exporting, and releasing the schedules.

Before You Start

Make sure you have created programs in the platform. For details, refer to ***Content Creation*** .

Steps

1. Enter the Create Schedules page.
   - After creating a program, click **Next**.
   - On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page, click **Content Schedule** on the left navigation pane, and then click **Add**.
2. In the pop-up Create Schedules window, set the related information, and click **OK**.

   Name

Define a schedule name that is easy to identify.

Program Type

Select **Other Program** or **Video Wall Program**.

Sharing Property

Public

All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) and the higher-level organizations can see and use the schedule.

Private

All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) can see and use the schedule.

Area

Set the area which the schedule belongs to.

Description

Enter the schedule description.

3. Select the play mode as **Play by Day**, **Play by Week** or **Custom**.

Play by Day/Week

Play the program according to a daily/weekly schedule.

Custom

Customize the schedule within up to 90 days.

4. Select program(s) from the program list and drag to the timeline on the right side.

Note

- You can click **All** or **My Favorites** to display all programs or programs that have been added to favorites.
- You can select **Landscape Mode**, **Portrait Mode**, or **Custom** from the drop-down list to filter programs.
- If you have selected the program type as video wall program in Step 2, you can filter programs by setting the video wall dimension.
- If you have selected the program type as other program in Step 2, you can select programs from the lists of multimedia programs, attendance programs, or people counting programs.
- You can enter keywords in the search box to filter programs.

5. Move the cursor to the timeline, and drag the cursor on the timeline to specify the playing time of the program.

Note

When hovering the cursor on the program's playing time, you can view the thumbnail of the program.

6. **Optional:** Adjust the program schedule.

- Move the cursor to the program bar on the timeline and drag the right and left edges to adjust the beginning time and end time of the program.
- Click the program bar on the timeline, and adjust the beginning time and end time of the program in the input box.
- Click to copy the program to other time periods.
- Click to delete the program in this time period.

7. Click **Save** to save the current schedule.
8. **Optional:** Click **Release** to enter the release page.

Note

For details, refer to ***Release a Program Schedule*** .

9. **Optional:** After creating schedules, perform the following operations as needed.

Edit Schedule	Click the name of the schedule and then click to enter Arrange Schedule page and you can edit the schedule information.
Delete Schedule	Select one or more schedules, click **Delete** to delete the selected schedules.
Release Schedule	Click to release the selected schedule. For details, refer to ***Release a Program Schedule*** .
Export Schedule	Click to export the schedule.
Add to / Cancel Favorites	Click or to add the schedule to favorites or move it from favorites. **Note** You can add up to 1,000 schedules to favorites.
Refresh Schedule	Click **Refresh** to refresh the schedule list.
Search Schedule	Click in the upper right corner of the page, and set the search conditions such as name and sharing property to quickly search for the target schedules.

31.3.2 Create a Loop Schedule

You can create a loop schedule for the added programs. With loop schedule configured, the added programs will be played repeatedly according to the play mode, including normal mode and period mode. You can add multiple playlists to meet different requirements.

Before You Start

Make sure you have created programs on the platform. For details, refer to ***Content Creation*** .

Steps

1. Enter the Create Schedules page.

- After creating a program, click **Next**.
- On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page, click **Content Schedule** on the left navigation pane, and then click **Add**.

2. In the pop-up Create Schedules window, set the related information, and click **OK**.

Name

Define a schedule name that is easy to identify.

Program Type

Select **Other Program** or **Video Wall Program**.

Sharing Property

Public

All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) and the higher-level organizations can see and use the schedule.

Private

All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) can see and use the schedule.

Area

Set the area which the schedule belongs to.

Description

Enter the schedule description.

3. Select the play mode as **Play In Loop**.
4. Select a program in the program list and drag the program to the playlist.

Note

- You can click **All** or **My Favorites** to display all programs or programs that have been added to favorites.
- You can select **Landscape Mode**, **Portrait Mode**, or **Custom** from the drop-down list to display corresponding programs.
- If you have selected the program type as video wall program in Step 2, you can filter programs by setting the video wall dimension.
- If you have selected the program type as other program in Step 2, you can select programs from the lists of multimedia programs, attendance programs, or people counting programs.
- You can enter keywords in the search box to filter programs.
- You can add up to 16 programs to a single playlist.

5. Set the play mode.

Normal Mode

Play the program orderly and repeatedly.

Period Mode

Play the programs orderly and repeatedly in specific time period. The time periods for different playlists cannot be overlapped.

Note

The priority of Period Mode is higher than that of Normal Mode. Only one playlist can be set to normal mode.

6. **Optional:** Click **Add Playlist** to add more playlists.

Note

You can add up to 8 playlists.

7. Click **Save** to save the current schedule.
8. **Optional:** Click **Release** to enter the release page.

Note

For details, refer to ***Release a Program Schedule*** .

9. **Optional:** After creating schedules, perform the following operations as needed.

Edit Schedule	Click the name of the schedule and then click to enter the Arrange Schedule page and you can edit the schedule information.
Delete Schedule	Select one or more schedules, click **Delete** to delete the selected schedules.
Release Schedule	Click to release the selected schedule. For details, refer to ***Release a Program Schedule*** .
Export Schedule	Click to export the schedule.
Add to / Cancel Favorites	Click or to add the schedule to favorites or move it from favorites. **Note** You can add up to 1,000 schedules to favorites.
Refresh Schedule	Click **Refresh** to refresh the schedule list.
Search Schedule	Click in the upper right corner of the page, and set the search conditions such as name and sharing property to quickly search for the target schedules.

31.3.3 Create a Default Schedule

With the default schedule enabled, the terminal will play the default video automatically if there is no program or cut-in. After creating a default schedule, you can perform more operations such as editing, exporting, and releasing the schedule.

Before You Start

Make sure you have created programs in the platform. For details, refer to ***Content Creation*** .

Steps

1. Enter the Create Schedules page.
   - After creating a program, click **Next**.
   - On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page, click **Content Schedule** on the left navigation pane, and then click **Add**.
2. In the pop-up Create Schedules window, set the related information, and click **OK**.

   Name

   Define a schedule name that is easy to identify.

   Program Type

   Select **Other Program** or **Video Wall Program**.

   Sharing Property

   Public

   All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) and the higher-level organizations can see and use the schedule.

   Private

   All users in the current organization (i.e., the organization where the user who creates the schedule belongs to) can see and use the schedule.

   Area

   Set the area which the schedule belongs to.

   Description

   Enter the schedule description.
3. Select the play mode as **Default Schedule**.
4. Select a program in the program list, and drag the program to the right.

   Note

   - You can click **All** or **My Favorites** to display all programs or programs that have been added to favorites.
   - You can select **Landscape Mode**, **Portrait Mode**, or **Custom** from the drop-down list.
   - If you have selected the program type as video wall program in Step 2, you can filter programs by setting the video wall dimension.
   - If you have selected the program type as other program in Step 2, you can select programs from the lists of multimedia programs, attendance programs, or people counting programs.
   - You can enter keywords in the search box to filter programs.
5. Click **Save** to save the current schedule.
6. **Optional:** Click **Release** to enter the release page.

Note

For details, refer to ***Release a Program Schedule*** .

7. **Optional:** After creating schedules, perform the following operations as needed.

Edit Schedule	Click the name of the schedule and then click to enter the Arrange Schedule page and you can edit the schedule information.
Delete Schedule	Select one or more schedules, click **Delete** to delete the selected schedules.
Release Schedule	Click to release the selected schedule. For details, refer to ***Release a Program Schedule*** .
Export Schedule	Click to export the schedule for offline view.
Add to / Cancel Favorites	Click or to add the schedule to favorites or move it from favorites. **Note** You can add up to 1,000 schedules to favorites.
Refresh Schedule	Click **Refresh** to refresh the schedule list.
Search Schedule	Click in the upper right corner of the page, and set the search conditions such as name and sharing property to quickly search for the target schedules.

31.4 Content Review

The added contents should be reviewed before they are used. After being reviewed, the contents can be released automatically.

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.

On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page, and then click **Content Review** on the left navigation pane.

Perform the following operations as needed.

Description	Operation
Review Content One by One	1. On the **All** and **To Be Reviewed** pages, click in the **Operation** column. 2. On the pop-up Content Review page, review the content.

Description	Operation
	3. Select the result as **Pass** or **Deny**. 4. Enter the comment. **Note** When the result is **Deny**, the comment is required. You can enter up to 128 characters. 5. Click **OK**.
Batch Review Contents	• On the **All** and **To Be Reviewed** pages, check multiple contents to be reviewed, click **Pass**, and enter the comment (optional) to batch pass the selected contents. • On the **All** and **To Be Reviewed** pages, check multiple contents to be reviewed, click **Deny**, and enter the comment (required) to batch deny the selected contents. **Note** When entering the comment, you can enter up to 128 characters.
Delete Content	On the **Denied** and **Passed** pages, check one or more contents, click **Delete** to delete them.
Refresh Content	On the **All**, **To Be Reviewed**, **Denied** and **Passed** pages, click **Refresh** to refresh the content list.
Search for Content	On the **All**, **To Be Reviewed**, **Denied** and **Passed** pages, enter keywords in the search box in the upper right corner to search for the target contents.

31.5 Content Release

You can view the release details and release progress of multiple tasks (such as schedule releasing and cutting in program). After being released, the above tasks can take effect on the terminals.

31.5.1 Release a Program Schedule

You should release the program schedule to the terminals. When releasing a schedule, you can set the release mode, effective mode, and the terminal(s). The program will then be played according to the configured method on the terminals.

Before You Start

Make sure you have added terminals to the platform. For details, please refer to ***Add Digital Signage Terminal*** .

Steps

Note

You cannot release a schedule for an emergency mustering program.

1. Enter the releasing schedule page.
   - After creating the programs, click **Next**. For details about creating programs, refer to ***Content Creation*** .
   - In the Digital Signage module, click **Content Creation** on the left navigation pane, select a program type, move the mouse cursor to a program, click to enter the adding schedules page, and click **Release** in the upper right corner.
   - In the Digital Signage module, click **Content Schedule** on the left navigation pane, and then click in the Operation column.
2. Enter the task name.
3. Select the release mode as **Release Later** or **Release Immediately**.

   Note

   When selecting **Release Later**, you should set the release time, and the program schedule will be released at the configured time period.
4. Select the effective mode as **Take Effect Immediately** or **Take Effect Later**.

   Note

   When selecting **Take Effect Later**, you should set the effective time. Only after the program takes effect, it can be played on the terminal.
5. Select an area, and check one or more devices in the selected area.

   Note

   You can enter a keyword in the search box to quickly search for the target areas or devices.
6. Click **OK** to start releasing the schedule.

   If you have the review permission, the contents can be released directly. If not, the contents will be reviewed by the user who has the review permission. For details about reviewing contents, refer to ***Content Review*** .

31.5.2 Cut in Program

You can cut in a program when creating or managing programs in the platform. The cut-in program will precede other programs and play on the terminal in the configured method.

Before You Start

Make sure you have added terminal(s) to the platform. For details, please refer to ***Add Digital Signage Terminal*** .

Steps

1. Enter Cut-in Program page.

- In the Digital Signage module, click **Content Creation** on the left navigation pane, select a program type, move the cursor to a program, and click .
- After creating a program, click **Cut In** in the upper right corner of the page.

2. Enter the task name.
3. Select the cut-in mode as **Play Duration (h/m/s)** or **End Time**.
4. Select one or more terminals for the cut-in programs.

Note

You can enter a keyword in the search box to quickly find the target device(s).

5. Click **OK**.

   If you have the review permission, the contents can be released directly. If not, the contents will be reviewed by the user who has the review permission. For details about reviewing contents, refer to ***Content Review*** .

31.5.3 View Release Records

You can view release records of all the tasks and the details of their release status.

On the top navigation bar, select → **Integrated Service** → **Digital Signage** , and then click **Release** on the left navigation pane. You can view release details of all the tasks on the platform, including task name and type, release time and status (Released or Failed), etc. Also, you can perform more of the following operations.

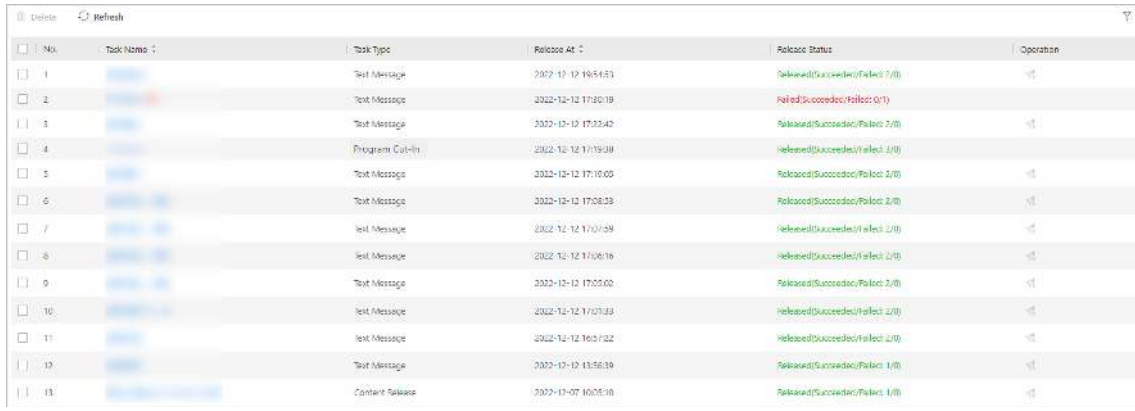


Figure 31-11 View Release Records

- **View Release Details**: Click the task name to view release details such as device name and release progress.

Note

For a task that is releasing, you can click **Cancel Release** to cancel releasing the task. For a task that failed to be released or was canceled releasing, you can click **Release again** to release the task again.

- **Delete Task**: Check one or multiple tasks, and click **Delete** to delete the selected tasks.
- **Release Again**: For a task that failed to be released, you can click to release the task again.
- 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.
- **Filter Tasks**: Click , and filter tasks by conditions such as task name and type.

31.6 Device Control

After adding devices to the platform, you can control them via the platform, such as remotely shutting down and rebooting. You can also control the video walls or manage applications on the platform according to the mode you have selected.

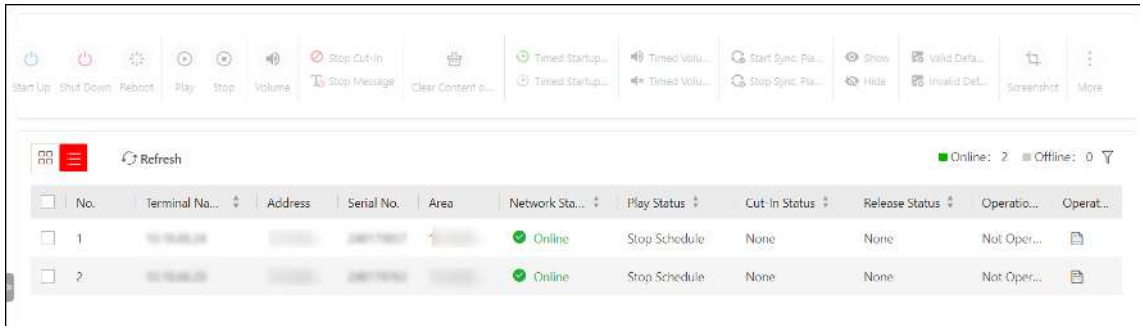
31.6.1 Control Digital Signage Terminal

After adding digital signage terminals to the platform, you can control the terminals on the platform, such as starting up, shutting down, playing programs, setting the volume, etc.

Note

- Make sure you have added digital signage terminals to the platform. See details in ***Add Digital Signage Terminal*** .

On the top navigation bar, select → **Integrated Service** → **Digital Signage** , and then click **Digital Signage Control** on the left navigation pane.



Operations When No Terminal Is Selected

Switch Display Mode

Click / to display the added terminals in thumbnail/list mode.

Refresh Terminal List

Click **Refresh** to refresh the terminal list.

View Terminal Details

Click in the Operation column to view the details of the terminal, such as software version, system version, IP address, MAC address, CPU usage, HDD usage, etc.

Search Terminals

Click , set the search conditions (such as network status, play status, cut-in status, and release status), and click **Search** to search for the target terminals.

Operations After Selecting Terminal(s)

Start Up / Shut Down / Reboot

Remotely start up / shut down / reboot the terminal(s).

Play/Stop

Play/stop the programs on the terminal(s).

Set Volume

Set the output volume of the terminal.

Stop Cut-In / Stop Message

Stop cutting in programs. / Stop cutting in messages.

Clear Content on Terminal

Clear all the contents to be played on the terminal(s), including programs, cut-in programs, etc.

Timed Startup/Shutdown Enabled/Disabled

The terminal(s) will start up / shut down according to the schedule.

The terminal(s) will not start up / shut down according to the schedule.

Note

For details about timed startup/shutdown, refer to ***Configure Device Display Settings*** .

Timed Volume On/Off

Turn on/off the volume of the terminal(s) based on the schedule you set.

Note

For details about timed volume on/off, refer to ***Configure Device Display Settings*** .

Start/Stop Sync. Playing on Terminal

Start or stop synchronous playing on terminals.

Show/Hide

Show or hide the release progress.

Valid/Invalid Default Schedule

If you create default video schedule for the terminal(s), you can manually control the schedule valid or invalid.

Note

For details about creating default video schedule, refer to ***Create a Default Schedule*** .

Screenshot

Take the screenshot(s) of the terminal(s), which is/are in JPG format.

More

NTP Time Sync

The time synchronization of NTP server should be enabled when starting synchronous playing on the terminals. See details in ***Set NTP*** .

Restore Default Settings

Restore the parameters of the terminal(s) to the default settings.

Display Offline Status

If it is enabled, the offline information will be displayed in the down right corner when the device is offline.

Remote Debugging

Enable the Android debug bridge for the terminal(s), and enter the debugging contents.

Log Export

Export the logs of the terminal(s) in ZIP format.

31.6.2 Control Video Wall

You can control the video walls after adding them to the platform.

Note

- Make sure you have added video walls. See details in ***Configure Video Wall*** .
- The multiple terminals that constitute the video wall should be controlled as a whole, or the playing status of different terminals will not be the same.

On the top navigation bar, select → **Integrated Service** → **Digital Signage** , and then click **Device Control** → **Video Wall Control** on the left navigation pane.

Operations When No Video Wall Is Selected

Switch Display Mode

Click / to display the added video walls in thumbnail/list mode.

Refresh Video Wall List

Click **Refresh** to refresh the video wall list.

Search Video Walls

Click , set the search conditions (dimension, screen type, network status, play status, cut-in status, etc.,), and click **Search** to search for the target video walls.

Operations After Selecting Video Wall(s)

Start Up / Shut Down / Reboot

Remotely start up, shut down, or reboot the video walls.

Play/Stop

Play or stop the programs on the video walls.

Volume

Set the volume of the video walls.

Stop Cut-In

Stop cutting in programs.

Clear Playing Content

Clear all contents to be played on the video walls.

Timed Startup/Shutdown Enabled/Disabled

Enable or disable startup/shutdown according to the schedule.

Note

For details about timed startup/shutdown, see details in ***Configure Device Display Settings*** .

Timed Volume On/Off

Turn on/off the volume of the video walls based on the configured schedule.

Note

For details about timed volume on/off, see details in ***Configure Device Display Settings*** .

NTP Time Sync.

The time synchronization of NTP server should be enabled when starting synchronous playing on the terminals. See details in ***Set NTP*** .

Restore Default

Restore the parameters of the terminals to the default settings.

31.7 Material Library

Material is used for creating programs. The platform supports various types of materials such as picture, video, and audio to meet with different program requirements. You can upload materials from local PC to the platform, and create dynamic materials on the platform. After uploading the

materials, you can view the number of all/used/unused materials and the storage of materials (local storage or pStor). Also, you can mange materials including editing, searching, replacing, etc.

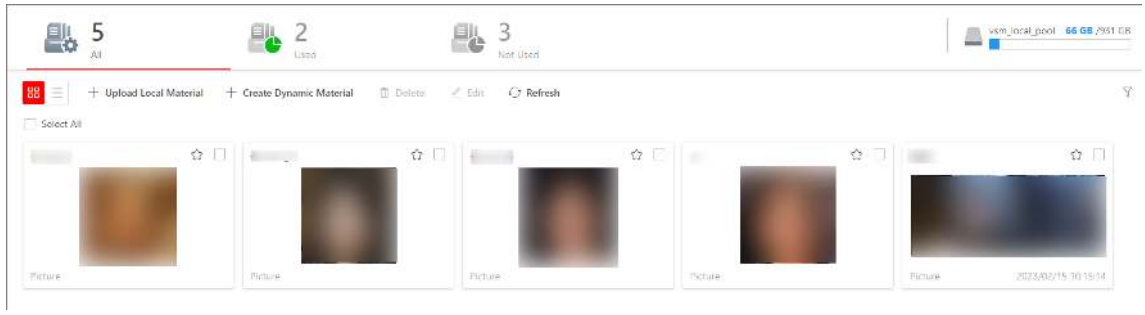


Figure 31-13 Material Library

31.7.1 Upload Local Material

You can upload local materials which can be used for creating programs. The materials supported to be uploaded include picture, video, audio, document, APP, etc. For the uploaded materials, you can perform more operations, including adding to favorites, editing, downloading, deleting, etc.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Material Library**.
3. On the **All** page, click **Upload Local Material** and select one or more materials to be uploaded from the local PC.

Table 31-5 Supported Material Types and Formats

Material Types	Formats
Picture	BMP, JPG, PNG, GIF, JPEG
Video	ASF, AVI, MPG, 3GP, MOV, MKV, WMV, FLV, MP4, RM, RMVB
Audio	MP3, WAV, WMA
Document	TXT、PDF、EXCEL、DOC、DOCX、PPT、PPTX
Webpage	HTML, HTM
APP	APK, ZIP

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.

4. Click **Open**.

   The selected local materials start to be uploaded. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails).

Note

- 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.

5. **Optional:** After uploading the materials, perform the following operations.

Add to Favorites or Not	Click ☆ to add the material to favorites. Click again to remove it from favorites.
Edit Material	Check one/more materials, or check **Select All** to select all materials, and click **Edit** to edit the selected materials, such as editing the name and the property.
Delete Material	Check one/more materials, or check **Select All** to select all materials, and click **Delete** to delete the selected materials. **Note** You cannot delete materials that have been added to a program or materials that are being released.
Download Material	Click to download single material to the local PC.
View Large Picture	Click to view large picture of the material.
Refresh Material	Click **Refresh** to refresh the material list.
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Search Material	Click in the upper right corner, and filter the added materials according to the name, uploaded time, sharing property, etc.

31.7.2 Create Dynamic Material

You can create and upload dynamic materials used for creating programs to the platform. The material types supported include webpage, network picture, stream media server, and network camera. For the uploaded materials, you can perform more operations, including adding to favorites, editing, downloading, deleting, etc.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Material Library**.
3. On the **All** page, click **Create Dynamic Material**.
4. Select the material type, and configure the related parameters.

Material Type

Webpage

When selecting this type, you should enter the URL address of the webpage.

URL Picture

When selecting this type, you should enter the URL address of the picture.

Third-Party Data Source

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.

Stream Media Server

Receive streams from the stream media server. You should enter the URL address of the stream media server.

Network Camera

Get video streams from network camera. You should enter the required information of network camera such as IP address, port No., and channel No.

Name

Define a material name that is easy to identify. Up to 64 characters can be entered.

Sharing Property

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.

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.

Description

Enter the detailed description of the material to be uploaded.

Area

Set the area which the material belongs to.

5. Finish uploading the material to the platform.
   - Click **Upload**.
   - Click **Upload and Continue** to upload the current material and continue to upload other materials.
6. **Optional:** Perform the following operations if needed.

Add to Favorites or Not	Click ☆ to add the material to favorites. Click again to remove it from favorites.
Edit Material	Check one/more materials, or click **Select All** to select all materials, and click **Edit** to edit the selected materials, such as editing the name and the property.
Delete Material	Check one/more materials, or click **Select All** to select all materials, and click **Delete** to delete the selected materials. **Note** You cannot delete materials that have been added to a program or materials that are releasing.
View Large Picture	Click to view large picture of the material.
Refresh Material	Click **Refresh** to refresh the material list.
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Search Material	Click in the upper right corner, and filter the added materials according to the name, uploaded time, sharing property, etc.

31.7.3 Mange Used or Unused Materials

You can manage used and unused materials, such as editing materials, filtering materials, and deleting materials.

On the top navigation bar, select → **Integrated Service** → **Digital Signage** , and then click **Material Library** on the left navigation pane.

Click **Used** or **Not Used** to enter the Used or Not Used page, and you can perform the following operations.

Table 31-6 Mange Materials

Description	Operation
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Add to Favorites or Not	Click or to add the material to Favorites or remove it from Favorites.
Edit Material	Select material(s) to be deleted, and click **Edit** to edit the selected materials, such as name and sharing property.
Refresh Material	Click **Refresh** to refresh the material list.
Download Material	Click to download the material to local PC. **Note** Dynamic materials cannot be downloaded.
View Large Picture	Click to view the large picture of the material.
Search Material	Click in the upper right corner, and search for the added materials according to the name, uploaded time, sharing property, etc.
Delete Material	Select material(s) to be deleted, and click **Delete** to delete the selected materials. **Note** You cannot delete materials that are added to a program or being released.
Clear Unused Materials	For materials that are not used, click **Quick Clear** to clear all materials in a batch.

31.8 Basic Settings

In Basic Settings module, you can set the application mode, configure material storage location, and configure video walls.

31.8.1 Switch Application Mode

You can switch between the Digital Signage mode and the Interactive Flat Panel mode. In the Digital Signage mode, you can create six types of contents, and release them to digital signage

terminals after reviewing contents and creating schedules for contents. In the Interactive Flat Panel mode, you can create two types of contents, and then release them to interactive flat panels. Also, you can add and manage applications in this mode.

On the top navigation bar, select → **Integrated Service → Digital Signage / Interactive Flat Panel** , and then click **Basic Configuration → Mode Switch** on the left navigation pane.

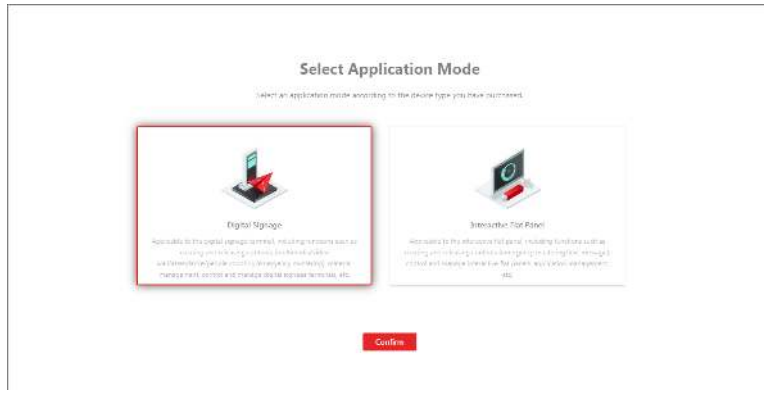


Figure 31-14 Select Application Mode

Select a mode according to the device type you have purchased, and click **Confirm** to go to the page of the selected mode.

Note

For using the platform for the first time, the default application mode is **Digital Signage**.

31.8.2 Set Material Storage Location

The materials uploaded can be saved to the local storage or pStor server.

Steps

1. On the top navigation bar, select → **Integrated Service → Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Basic Settings → Material Storage Location** .
3. Select a storage location from the drop-down list.

   Note

   To select **pStor** as the storage location, make sure you have added pStor servers to the platform. For details, refer to ***Add pStor*** .
4. Click **Save** to save the above settings.

31.8.3 Configure Video Wall

A video wall is made up of multiple terminals. After adding more than one terminals to the platform, you can configure video 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. See details in ***Add Digital Signage Terminal*** and ***Set NTP*** .

Steps

1. On the top navigation bar, select → **Integrated Service** → **Digital Signage** to enter the digital signage page.
2. On the left navigation pane, click **Basic Settings** → **Video Wall Configuration** .
3. Click **Add**.

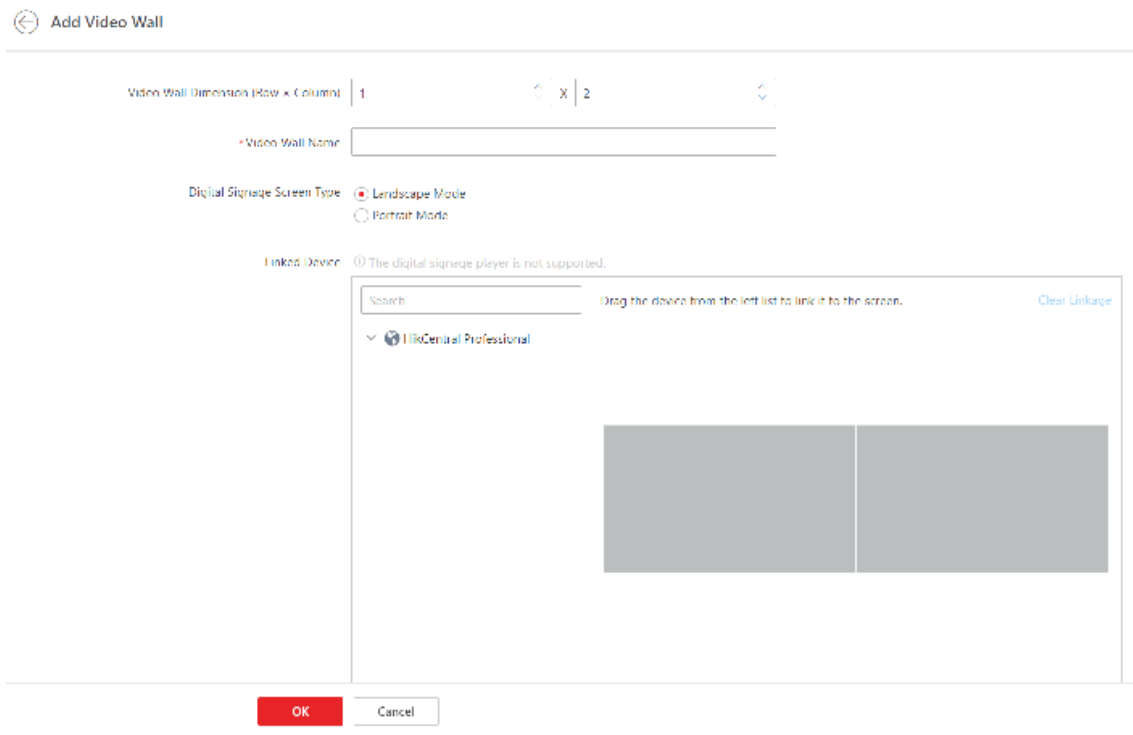


Figure 31-15 Add Video Wall

4. Specify the video wall dimension (row × column).
5. Enter the video wall name.
6. Select **Landscape Mode** or **Portrait Mode** as the screen type.
7. 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.

8. **Optional:** Click **Clear Linkage** to clear the linked devices from the screen.

9. **Optional:** Enter the description of the video wall.
10. Click **OK**.
11. **Optional:** After adding video walls, you can perform the following operations.

Switch Display Mode	Click / to display the added video walls in the thumbnail/list mode.
Edit Video Wall Information	• In thumbnail mode, click the video wall card to enter the video wall information page and edit the information. • In list mode, click the name of the video wall to enter the video wall information page and edit the information.
Delete Video Walls	Select one or multiple added video walls and click **Delete** to delete the selected video walls.
Set Video Wall Display Parameters	Select one or multiple added video walls, click **Video Wall Display Control** to set the display parameters.
Refresh Video Wall List	Click **Refresh** to refresh the video wall list.
Search Video Walls	Click , set the search conditions such as dimension and screen type, and click **Search** to search for the target video walls.

Chapter 32 Interactive Flat Panel Management

In the Interactive Flat Panel module, you can have an overview of the functions of interactive flat panel, create and release contents, view release records, manage applications, and control interactive flat panels.

Note

To perform operations in this module, make sure you are in the **Interactive Flat Panel** mode. See details in ***Switch Application Mode*** .

32.1 Interactive Flat Panel Overview

You can have an overview of the functions about interactive flat panel.

On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** , and then click **Interactive Flat Panel Overview** on the left navigation pane.

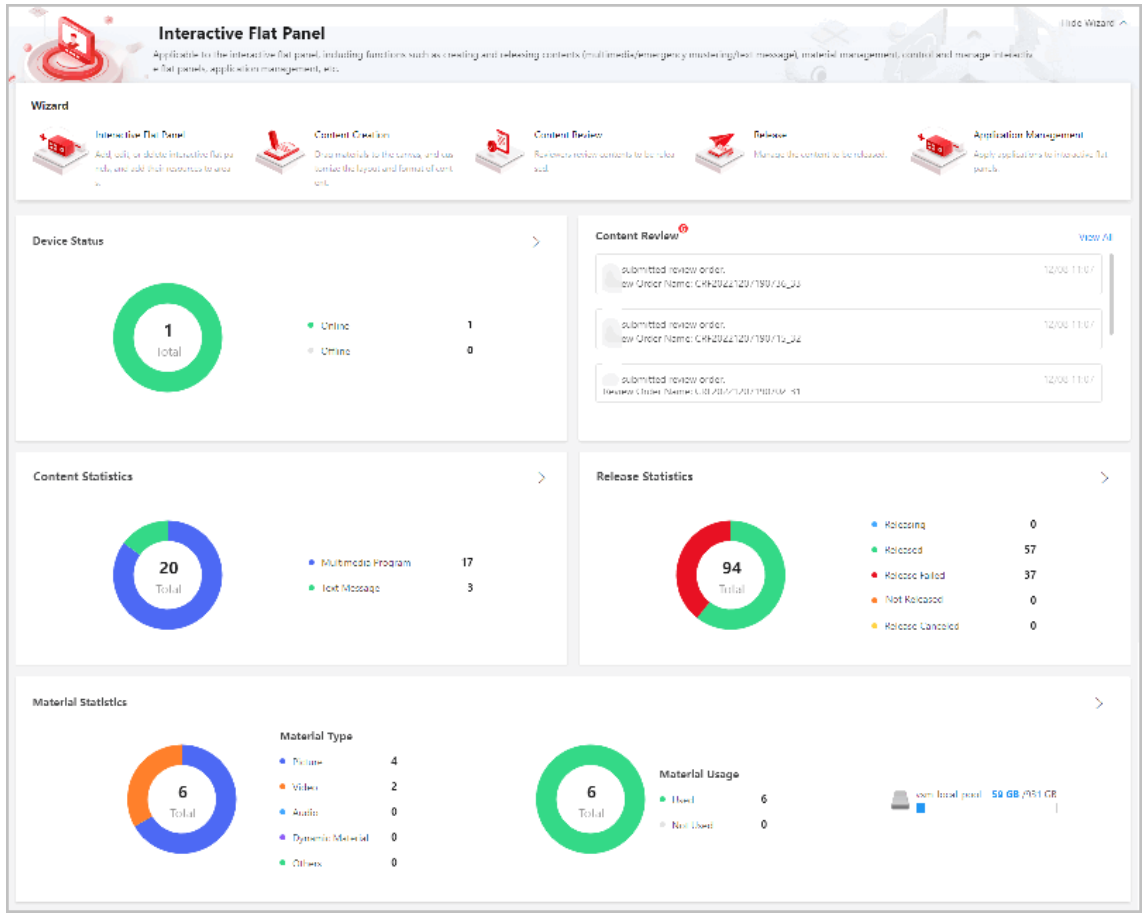


Figure 32-1 Interactive Flat Panel Overview

Table 32-1 Interactive Flat Panel Overview

Title	Description
Wizard	The wizard of the Interactive Flat Panel module, introducing the overall process.
Device Status	Displays total number of devices and status (Offline, Online), and the number of devices in each status. You can click to enter the Device Control page and do more operations. For details, refer to ***Control Interactive Flat Panel*** .
Content Review	Displays the details of content review, including the reviewer, submitted time, etc. You can click to enter the Content Review page and review contents. For details, refer to ***Content Review*** .

Title	Description
Content Statistics	Displays the total number of contents and the number of contents in different types. You can click to enter the content creation page. For details about creating contents, refer to ***Content Creation*** .
Release Statistics	Displays different release status such as Releasing, Released, and Releasing Failed, as well as the number of each status. You can click to enter Release page and view the release records. For details, refer to ***View Release Records*** .
Material Statistics	Displays the total number and the types (i.e., Picture, Video, Audio, Dynamic Material, and Others) of the added materials, the number of materials in each type, the number of used and unused materials, and the material usage. You can click to enter the material library page. For details about managing materials, refer to ***Material Library*** .

32.2 Content Creation

The platform supports creating contents and releasing them to the interactive flat panels. The released contents can be played on the panels to function as prompts, notices, etc. According to different application scenarios, you can create two types of contents, including text message and emergency mustering text notification.

32.2.1 Create Multimedia Program

Multimedia program can be used in multiple application scenarios (e.g., playing a program related with commodity information at the entrance of a chain supermarket), helping to spread information in a convenient and efficient way.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** to enter the interactive flat panel page.
2. On the left navigation pane, click **Content Creation** → **Multimedia** .
3. Click **Add** or **Configure Now** (if you add the program for the first time).
4. In the pop-up window, configure program parameters.

   Name

   Define a program name that is easy to identify. You can enter up to 64 characters.

   Screen Size

   Select the screen size as Landscape Mode, Portrait Mode, or Custom.

Sharing Property

Public

All users in the current organization (i.e., the organization which the user who creates the program belongs to) and the higher-level organizations can see and use the program.

Private

All users in the current organization (i.e., the organization which the user who creates the program belongs to) can see and use the program.

Area

Set the area which the program belongs to.

Description

Enter the program description, such as usage, applicable scenarios, and overview of program content. You can enter up to 64 characters.

5. Click **Next**.
6. Select a template type and the corresponding template as needed.

Note

- You can click ☆ to add the template to My Favorites. Up to 1,000 templates can be added to My Favorites.
- You can click ☆ **My Favorites** in the lower-left corner to view and select the added template.

7. Click **OK** to enter the creating program page.

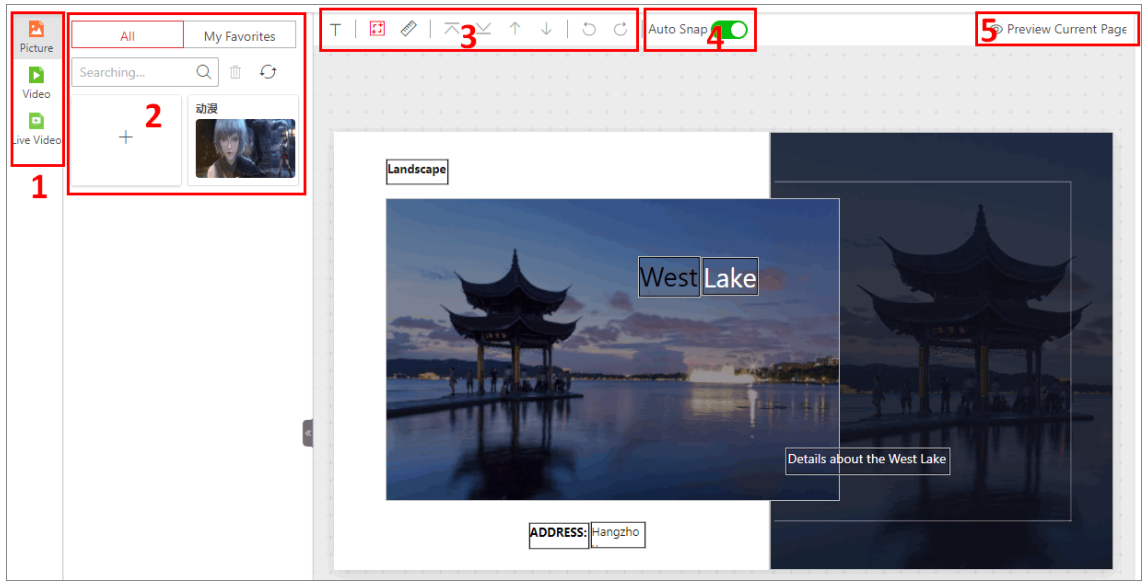


Figure 32-2 Create Program

Table 32-2 Page Description

Number	Description
1	There are multiple types of windows. Up to 16 windows can be added for one page.
2	You can select materials from **All** or **My Favorites** list. Click + to add other materials from local PC to the platform. Also, you can search for materials, delete materials, and refresh material list. For the picture and video materials, you can move the mouse cursor to the upper-right corner of the material, and click to set its validity period. The material will be played within the validity period.
3	You can click to add a text window in the template; click / / / / to make the window layer move up / move down / stick on top / stick at bottom. You can click to align the material window with grid lines. You can click to display rulers in the right side and top side. You can click / to undo or redo the operation.
4	You can enable **Auto Snap**, and the two windows will be connected when they are near enough.
5	• You can click **Preview Current Page** to preview the content of the current page. • During previewing, you can click or to pause or start playing. You can click or to adjust the playing speed as 1x, 2x, or 4x. Also, you can click to preview the current page in fullscreen.

8. Edit page properties, including page name, background, and play time type.

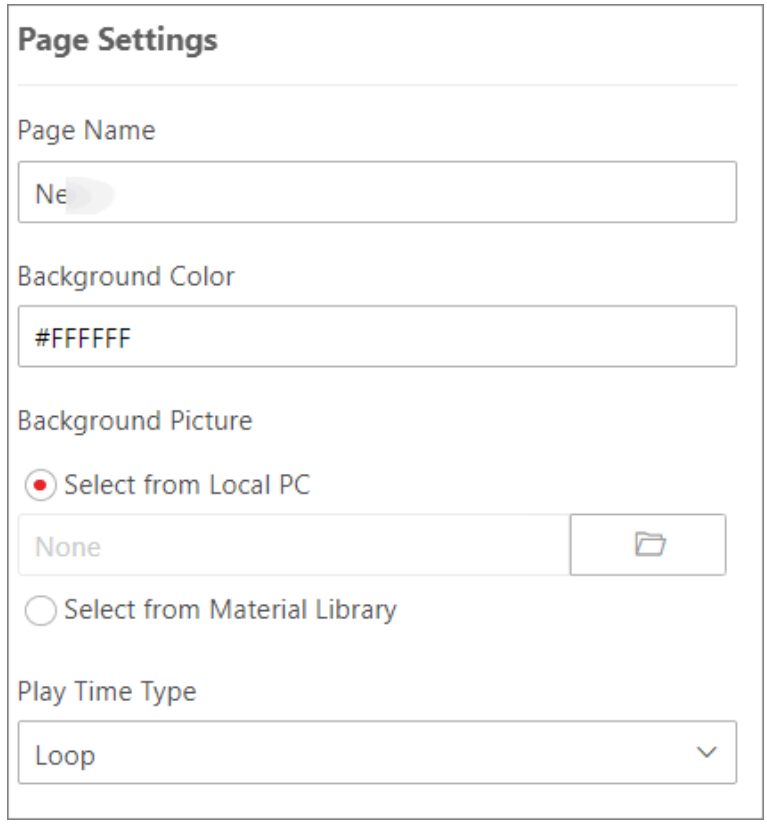


Figure 32-3 Page Settings

9. **Optional:** Add, delete, or adjust program pages at the bottom side.

Add	Click + / ⊕ to add new page(s).
Delete	Put the cursor on the page, and click ⊗ in the upper right corner to delete the current page.
Adjust Sequence	Click a page and drag it to the desired location to adjust the sequence of program pages.

10. Select a material from the left list and drag it to the corresponding window in the template to add the selected material.

Note

- You can add the same or different types of materials to one window. When adding the same type of materials to one window, you can click **Create Window** to create a new window or click **Add More Material** to add more material to the current window.
- When adding pictures and videos, you can check **Actual Size** to display these materials in their original sizes.

- When adding texts, you can set the background color and transparency, as well as the scrolling direction and speed.
- When adding live videos, you can check **Close Audio**, then the program will be played without audio. Besides, only one Device Channel 1 can be added to one program page.

11. Set window properties, including window position, window type, switching method, etc.

Note

You can set different parameters for different types of material windows.

Window Position

Set the window position by entering the width, height, and coordinate of the window.

Window Type

Normal

The normal window is displayed by default when the program is played. You can set a window jump link or page jump link for such a window.

Popup Window

The pop-up window is hidden by default. Only after setting a redirect link for a normal window and clicking the link, the hidden window will be popped up.

Switching Method

For Android touchscreen terminals, you can open the specified content by linking to a window or page.

No Skip

There is no linked window or page to the current window which is played on the terminal.

Jump to Next Window

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked window.

Jump to Next Page

You should set the jump link. When the Window A is played on the terminal, you can click the link to jump to its linked page.

Move Window Layer

Click ↑ / ↓ / ⤒ / ⤓ to make the window layer move up / move down / stick on top / stick at bottom.

Switching Effect

Select the switching effect from the drop-down list for the current window. There are 11 types of switching effect.

Play Time (sec)

Set the playing duration for the current window.

Note

The play time of a window can not exceed the playing time of a page, or the exceeding part of the program will not be played.

12. **Optional:** On the current editing program page, perform the following operations.

Edit Program	Click to edit program parameters in the pop-up window. For details, refer to the previous step.
Preview Program	Click **Preview** to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in fullscreen. For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click or to preview the previous or the next page of the program.
Create Schedule	Click **Release** to enter the release page and set the related parameters such as name and cut-in mode to release the program.

13. Click **Save** to save the current program.
14. **Optional:** On the program list page, perform the following operations.

View Program in List or Thumbnail Mode	Click / to view the added programs in the thumbnail mode or in the list mode.
Add Program to Favorites	Click to add the current program to Favorites.
Preview Program	Click to preview the program. During previewing, you can click or to pause or start playing; click or to adjust the playing speed as 1x, 2x, or 4x; and click to preview the program in fullscreen. For the program with multiple pages, it will be played automatically according to the page play time you have set. Also, you can manually click or to preview the previous or the next page of the program.
Copy Program	Click to enter editing program page. Click **Save** in the upper right corner to copy the current program, and a new program with the same content is created.

Note

When copying a program (e.g., Program A) for the first time, the name of the new program (Program A_1) will be generated automatically. If you need to copy this program (Program A) for a second or more times, you should manually edit its name, or the program cannot be created successfully.

Release Program	Click to enter the release page and set the related parameters such as name and cut-in mode to release the program.
Enlarge Program Page	Click to enlarge the program page and view it.
Filter Program	Click , and filter programs by conditions such as name and sharing property.
Refresh Program List	Click **Refresh** to refresh the program list. The programs will be listed according to the time they are added.
Delete Program	Check one/more programs, or check **Select All** to select all programs, and click **Delete** to delete the selected programs.

Note

Programs that are releasing or cutting in cannot be deleted.

32.2.2 Add Emergency Mustering Text Notification

You can add emergency mustering text notifications in the platform by configuring related parameters, and the added text notifications will be displayed on the interactive plat panels when the emergency is triggered.

Before You Start

- Make sure you have added devices to the platform. For details, refer to ***Manage Interactive Flat Panel*** .
- Make sure you have switched to the Interactive Flat Panel mode. See details in ***Switch Application Mode*** .

Steps

Note

For one device, only the latest added text notification can be displayed.

1. On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** to enter the interactive flat panel page.
2. On the left navigation pane, click **Content Creation** → **Emergency Mustering** .

3. Click **Add** or **Configure** (if you add the text notification for the first time) to enter the Add Text Notification page.

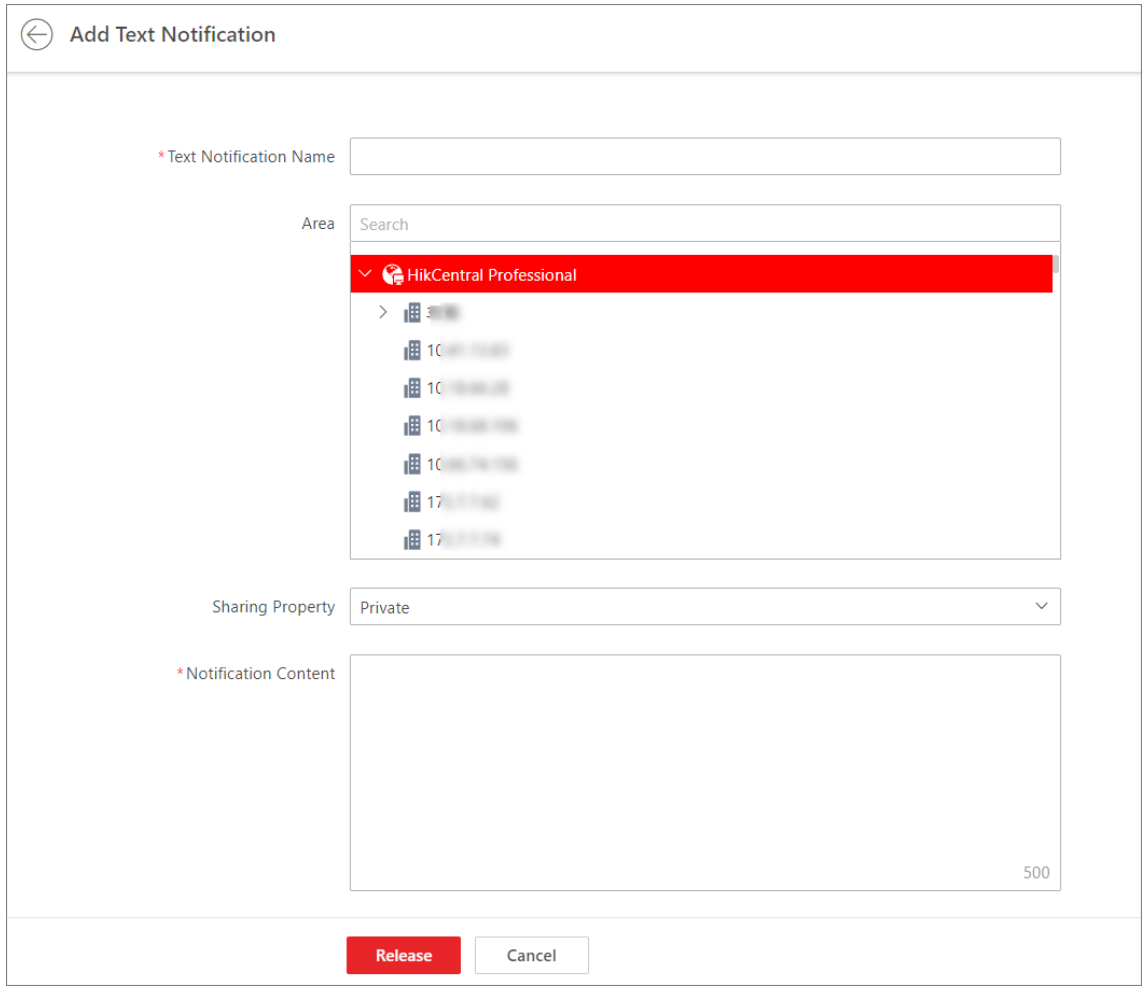


Figure 32-4 Add Text Notification

4. Set the required parameters.

Text Notification Name

The name of the text notification.

Notification Content

The content of the text notification.

Select Device

Select device(s) in the list on the left and add them to the list on the right. The text notification will be displayed on the selected devices.

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 not display any more.

5. Click **Release**.

Note

The text notifications is released and will be displayed when the emergency is triggered.

6. **Optional:** Click **View Emergency Mustering Configuration** in the upper right corner to enter the Emergency Mustering module and view emergency mustering configurations.

Note

For details, refer to ***Emergency Solution Settings*** .

7. **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	Click to enter the editing 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. **Note** 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 not display any more.
View Device Release Details	Click to view release details of the text notification on the device.
Filter Text Notification	Click , and filter text notifications by conditions such as name and sharing property.
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.

32.2.3 Add Text Message

You can add text messages and apply them to interactive flat panels. When adding the text message, you can set the parameters and preview the displaying effect on the platform. After applying the text message to the interactive flat panel, the text message will be played according to the configured time and method.

Before You Start

- Make sure you have added interactive flat panels to the platform. For details, refer to ***Manage Interactive Flat Panel*** .

Steps

1. On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** to enter the interactive flat panel page.
2. On the left navigation pane, click **Content Creation** → **Text Message** .
3. Click **Add** to enter the Add Text Message page.
4. Enter the name for the text message.
5. **Optional:** Select an area from the drop-down list.

   Note

   For details about how to add areas, refer to ***Add an Area for Current Site*** .
6. In the Edit Text Message area, enter the content of the text message.
7. Set playing parameters.

   Playing Method

   Display Scrolling Message

   The text message will scroll on the top of the interactive flat panel. Select this method when there is only a small amount of text.

   Display Pop-Up Message

   The text message will display in a pop-up window on the right side of the interactive flat panel. Select this method when there is a large amount of text.

   Take Effect on Schedule

   The text message will take effect according to the configured time schedule. You can select **Customize**, **Play by Day**, or **Play by Week**.
8. Save or release the text message.
   - In the upper-right corner, click **Save** to save the above settings and release the text message afterward.
   - In the upper-right corner, click **Release** to enter the Release Text Message page, select one or more devices in the list, and click **Release** to start releasing the text message to the selected devices.

Note

You can view the release progress and result on the right side of the page.

9. **Optional:** Perform the following operations in the text message list.

Refresh Text Message List	Click **Refresh** to refresh the list of text messages.
Edit Text Message	Click a name on the **Text Notification Name** column to edit the text notification, including its name, area, content, and playing parameters.
Release Text Message	Click a name on the **Text Notification Name** column to enter the Edit Text Message page, and click **Release** in the upper-right corner to enter the Release Text Message page. On the Release Text Message page, select one or more devices in the list, and click **Release** to start releasing the text message to the selected devices. **Note** You can view the release progress and result on the right side of the page.
Delete Text Message	Check one or more text messages, and click **Delete** to delete the selected text messages.

32.3 Content Review

The added contents should be reviewed before they are used. After being reviewed, they can be released to the interactive flat panels automatically.

Note

The user should have the permission to review contents.

On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** to enter the interactive flat panel page, and then click **Content Review** on the left navigation pane.

Perform the following operations.

Description	Operation
Review Content One by One	1. On the **All** and **To Be Reviewed** pages, click in the **Operation** column. 2. On the pop-up Content Review page, review the content. 3. Select the result as **Pass** or **Deny**. 4. Enter the comment.

Description	Operation
	Note When the result is **Deny**, the comment is required. You can enter up to 128 characters. 5. Click **OK**.
Batch Review Content	• On the **All** and **To Be Reviewed** pages, check multiple contents to be reviewed, click **Pass**, and enter the comment (optional) to pass the selected contents in a batch. • On the **All** and **To Be Reviewed** pages, check multiple contents to be reviewed, click **Deny**, and enter the comment (required) to deny the selected contents in a batch. **Note** When entering the comment, you can enter up to 128 characters.
Delete Content	On the **Denied** and **Passed** pages, check one or more contents, click **Delete** to delete them.
Refresh Content	On the **All**, **To Be Reviewed**, **Denied** and **Passed** pages, click **Refresh** to refresh the content list.
Search for Content	On the **All**, **To Be Reviewed**, **Denied** and **Passed** pages, enter keywords in the search box in the upper right corner to search for the target contents.

32.4 View Release Records

You can view release records of all the tasks and the details of their release status.

On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** to enter the interactive flat panel page, and then click **Release** on the left navigation pane. You can view release details of all the tasks on the platform, including task name and type, release time and status (Released or Failed), etc. Also, you can perform more of the following operations.

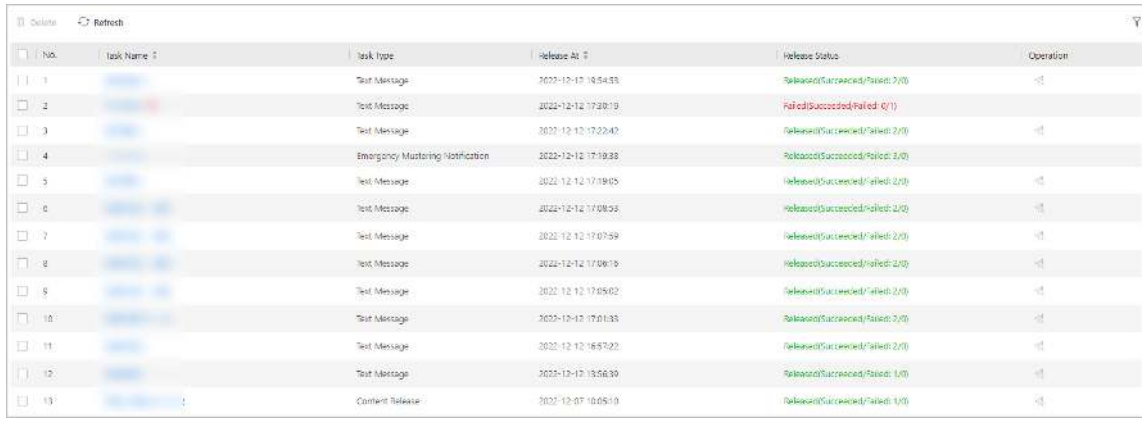


Figure 32-5 Release Records

- **View Release Details**: Click the task name to view release details such as device name and release progress.
- **Delete Task**: Check one or multiple tasks, and click **Delete** to delete the selected tasks.
- **Refresh Task List**: Click **Refresh** to refresh the task list.
- **Filter Tasks**: Click , and set conditions including release time, task type, and release status to filter tasks.

32.5 Manage Applications

You add and manage applications on the platform and apply them to the interactive flat panels.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** to enter the interactive flat panel page.
2. On the left navigation pane, click **Device Control**.
3. Click **Application Management** on the left.

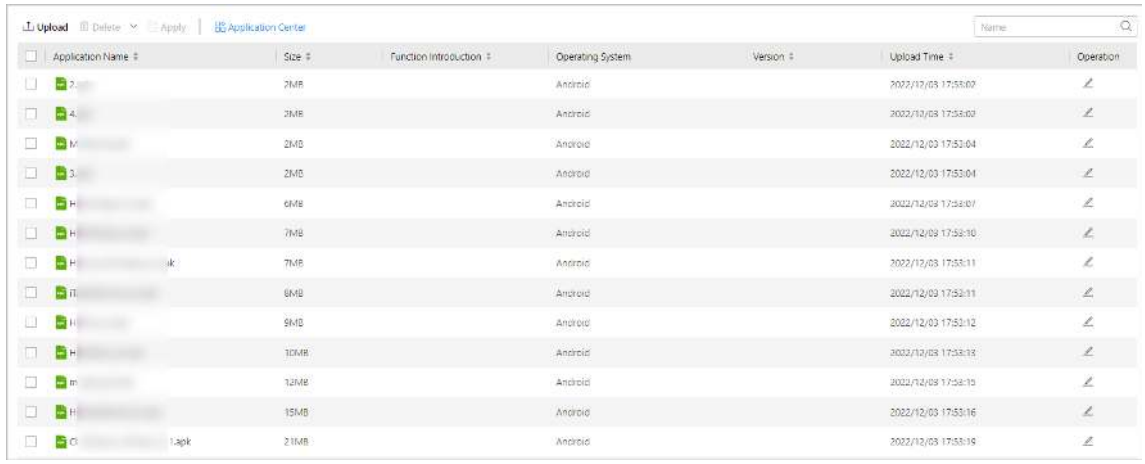


Figure 32-6 Applications List

4. **Optional:** Before adding applications, click **Application Center** to download applications from the Google application center and save them to local PC.
5. Add applications.

Note

Make sure you have downloaded applications to local PC.

1) Click **Upload**.
2) Select application(s) to be added from local PC.
3) Click **Open** to add the selected application(s) to the platform.

6. **Optional:** After adding applications, you can perform the following operations.

Edit Application	Click on the operation column to edit the function introduction of the application.
Apply to Device	Select one or more applications, click **Apply** to open the Apply panel. You can select all devices or some device(s) to apply the applications to.
Search Application	Enter keywords in the upper right corner to search for the target applications.
Sort Applications	Sort applications in the list according to the application name, size, and so on.
Delete Application	Select one or more applications, click **Delete** to delete the selected applications. Move the mouse cursor to beside **Delete**, and click **Delete All** to delete all the applications in the list.

32.6 Control Interactive Flat Panel

After adding interactive flat panels to the platform, you can control them on the platform, such as shutting down, rebooting, and setting the screen saver password.

Note

- Make sure you have added interactive flat panels to the platform. See details in ***Manage Interactive Flat Panel*** .

On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** to enter the interactive flat panel page, and then click **Device Control** on the left navigation pane.

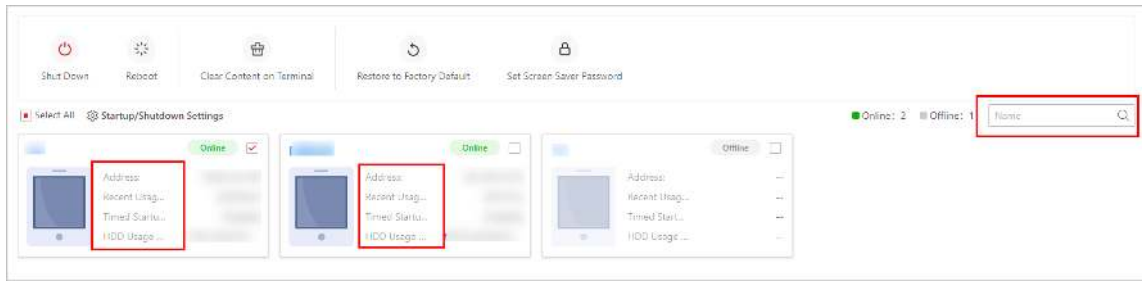


Figure 32-7 Control Interactive Flat Panel

You can search for the target interactive flat panels, and view the information about online interactive flat panels including IP address, recent usage time, timed startup/shutdown status, and HDD usage status.

Select one or multiple interactive flat panels and perform the following operations as needed.

Shut Down / Reboot

Remotely shut down or reboot interactive flat panels.

Clear Content on Terminal

Clear all the contents that have been released to the selected interactive flat panels.

Restore Default

Restore the parameters of interactive flat panels to the default settings.

Set Screen Saver Password

Set the screen saver password for interactive flat panels.

Startup/Shutdown Settings

Set the parameters related to startup or shutdown for interactive flat panels, such as standby strategy and wakeup strategy. If you enable **Timed Startup/Shutdown**, you should add startup/shutdown schedule by configuring startup and/or shutdown time, and the repetition mode.

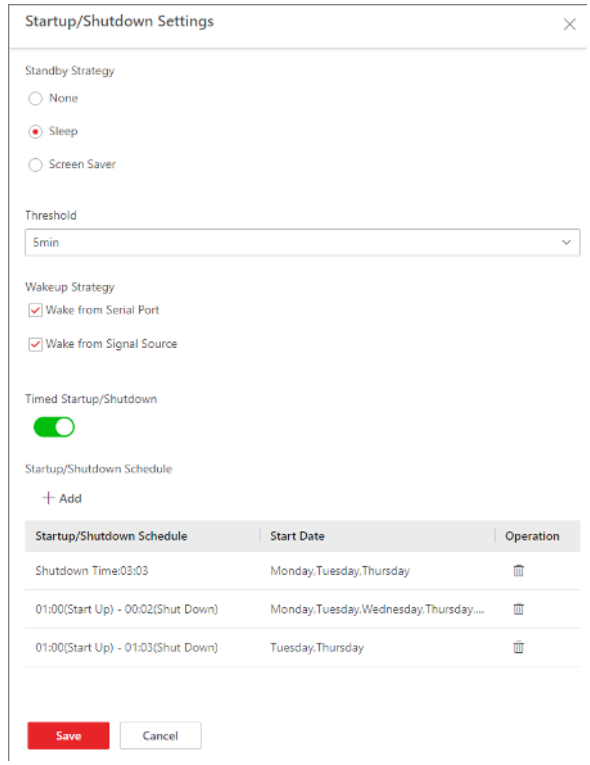


Figure 32-8 Startup/Shutdown Settings

32.7 Material Library

Material is used for creating multimedia programs. The platform supports various types of materials such as picture, video, and audio to meet with different program requirements. You can upload materials from local PC to the platform, and create dynamic materials on the platform. After uploading the materials, you can view the number of all/used/unused materials and the storage of materials (local storage or pStor). Also, you can mange materials including editing, searching, replacing, etc.

32.7.1 Upload Local Material

You can upload local materials which can be used for creating programs. The materials supported to be uploaded include picture, video, audio, document, APP, etc. For the uploaded materials, you can perform more operations, including adding to Favorites, editing, downloading, deleting, etc.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** .
2. On the left navigation pane, click **Material Library**.

3. On the **All** page, click **Upload Local Material** and select one or more materials to be uploaded from the local PC.

Table 32-3 Supported Material Types and Formats

Material Types	Formats
Picture	BMP, JPG, PNG, GIF, JPEG
Video	ASF, AVI, MPG, 3GP, MOV, MKV, WMV, FLV, MP4, RM, RMVB
Audio	MP3, WAV, WMA
Document	TXT, PDF, EXCEL, DOC, DOCX, PPT, PPTX
Webpage	HTML, HTM
APP	APK, ZIP

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.

4. Click **Open**.

The selected local materials start to be uploaded. Meanwhile, the uploading progress and the failure details will be displayed (when uploading fails).

Note

- 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.

5. **Optional:** After uploading the materials, perform the following operations.

Add to Favorites or Not	Click ☆ to add the material to Favorites. Click again to remove it from Favorites.
Edit Material	Check one/more materials, or check **Select All** to select all materials, and click **Edit** to edit the selected materials, such as editing the name and the property.
Delete Material	Check one/more materials, or check **Select All** to select all materials, and click **Delete** to delete the selected materials.

Note

You cannot delete materials that have been added to a program or materials that are being released.

Download Material	Click to download single material to the local PC.
View Large Picture	Click to view the large picture of the material.
Refresh Material	Click **Refresh** to refresh the material list.
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Search Material	Click in the upper right corner, and filter the added materials according to the name, uploaded time, sharing property, etc.

32.7.2 Create Dynamic Material

You can create and upload dynamic materials used for creating programs to the platform. The material types supported include network picture, stream media server, and network camera. For the uploaded materials, you can perform more operations, including adding to Favorites, editing, downloading, deleting, etc.

Steps

1. On the top navigation bar, go to → **Integrated Service** → **Interactive Flat Panel** .
2. On the left navigation pane, click **Material Library**.
3. On the **All** page, click **Create Dynamic Material**.
4. Select the material type, and configure the related parameters.

Material Type

URL Picture

When selecting this type, you should enter the URL address of the picture.

Stream Media Server

Receive streams from the stream media server. You should enter the URL address of the stream media server.

Network Camera

Get video streams from the network camera. You should enter the required information of network camera such as IP address, port No., and channel No.

Name

Define a material name that is easy to identify. Up to 64 characters are allowed.

Sharing Property

Public

All users in the current organization (i.e., the organization which the user who creates the material belongs to) and the higher-level organizations can see and use the material.

Private

All users in the current organization (i.e., the organization which the user who creates the material belongs to) can see and use the material.

Description

Enter the detailed description of the material to be uploaded.

Area

Set the area which the material belongs to.

5. Finish uploading the material to the platform.
   - Click **Upload**.
   - Click **Upload and Continue** to upload the current material and continue to upload other materials.
6. **Optional:** Perform the following operations.

Add to Favorites or Not	Click ☆ to add the material to Favorites. Click again to remove it from Favorites.
Edit Material	Check one/more materials, or check **Select All** to select all materials, and click **Edit** to edit the selected materials, such as editing the name and the property.
Delete Material	Check one/more materials, or check **Select All** to select all materials, and click **Delete** to delete the selected materials. **Note** You cannot delete materials that have been added to a program or materials that are being released.
View Large Picture	Click to view the large picture of the material.
Refresh Material	Click **Refresh** to refresh the material list.
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Search for Material	Click in the upper right corner, and filter the added materials according to the name, uploaded time, sharing property, etc.

32.7.3 Mange Used or Unused Materials

You can manage used and unused materials, such as editing materials, filtering materials, and deleting materials.

On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** , and then click **Material Library** on the left navigation pane.

Click **Used** or **Not Used** to enter the Used or Not Used page, and you can perform the following operations.

Table 32-4 Mange Materials

Description	Operation
Switch Display Mode of Materials	Click / to view the added materials in the thumbnail mode or in the list mode.
Add to Favorites or Not	Click or to add the material to Favorites or remove it from Favorites.
Edit Material	Check one/more materials, or check **Select All** to select all materials, and click **Edit** to edit the selected materials, such as name and sharing property.
Refresh Material	Click **Refresh** to refresh the material list.
Download Material	Click to download the material to local PC. **Note** Dynamic materials cannot be downloaded.
View Large Picture	Click to view the large picture of the material.
Search for Material	Click in the upper right corner, and search for the added materials according to the name, uploaded time, sharing property, etc.
Delete Material	Check one/more materials, or check **Select All** to select all materials, and click **Delete** to delete the selected materials. **Note** You cannot delete materials that have been added to a program or materials that are being released.
Clear Material	For materials that are not used, click **Quick Clear** to clear all materials in a batch.

32.8 Set Material Storage Location

The materials uploaded can be saved to the local storage or pStor server.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Interactive Flat Panel** .
2. Select **Basic Settings** → **Material Storage Location** on the left.
3. Select a storage location from the drop-down list.

   Note

   To select **pStor** as the storage location, make sure you have added pStor servers to the platform. For details, refer to ***Add pStor*** .
4. Click **Save** to save the above settings.

Chapter 33 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. For details, refer to ***Set User Preference*** .

33.1 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.

33.1.1 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 → 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. • 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** 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.

33.1.2 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. For details, refer to ***Configure Other Parameters*** .

33.2 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.

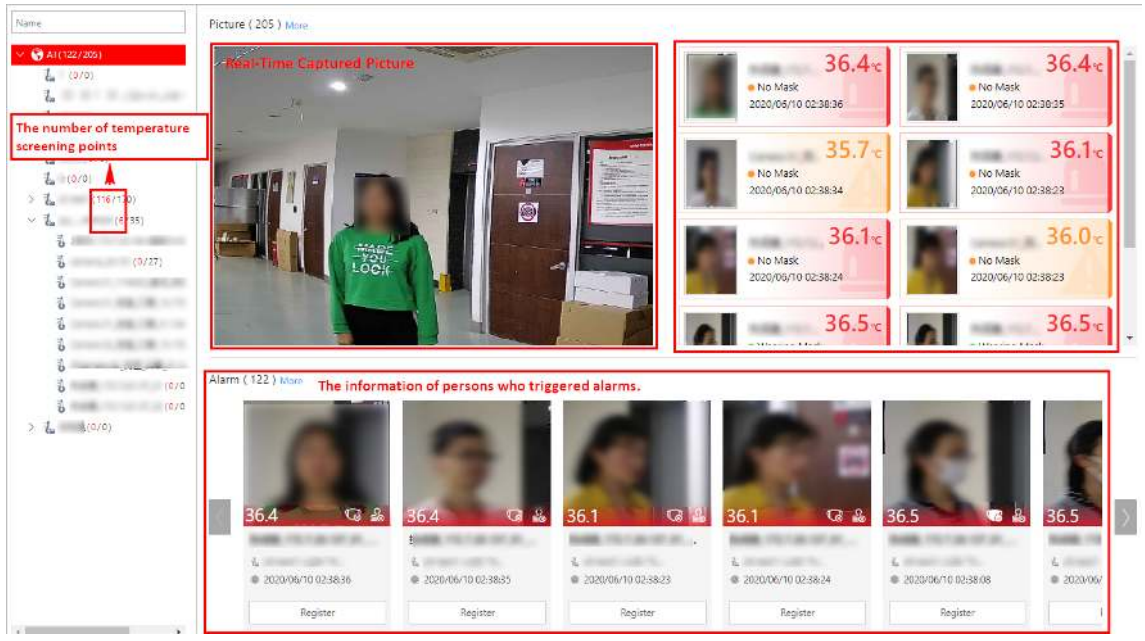


Figure 33-1 Real-Time Skin-Surface Temperature

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.

33.3 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. **Note** 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. • : The person is registered. For the registered person, click **Edit** to edit the person information. • : 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.

33.4 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.

33.4.1 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.

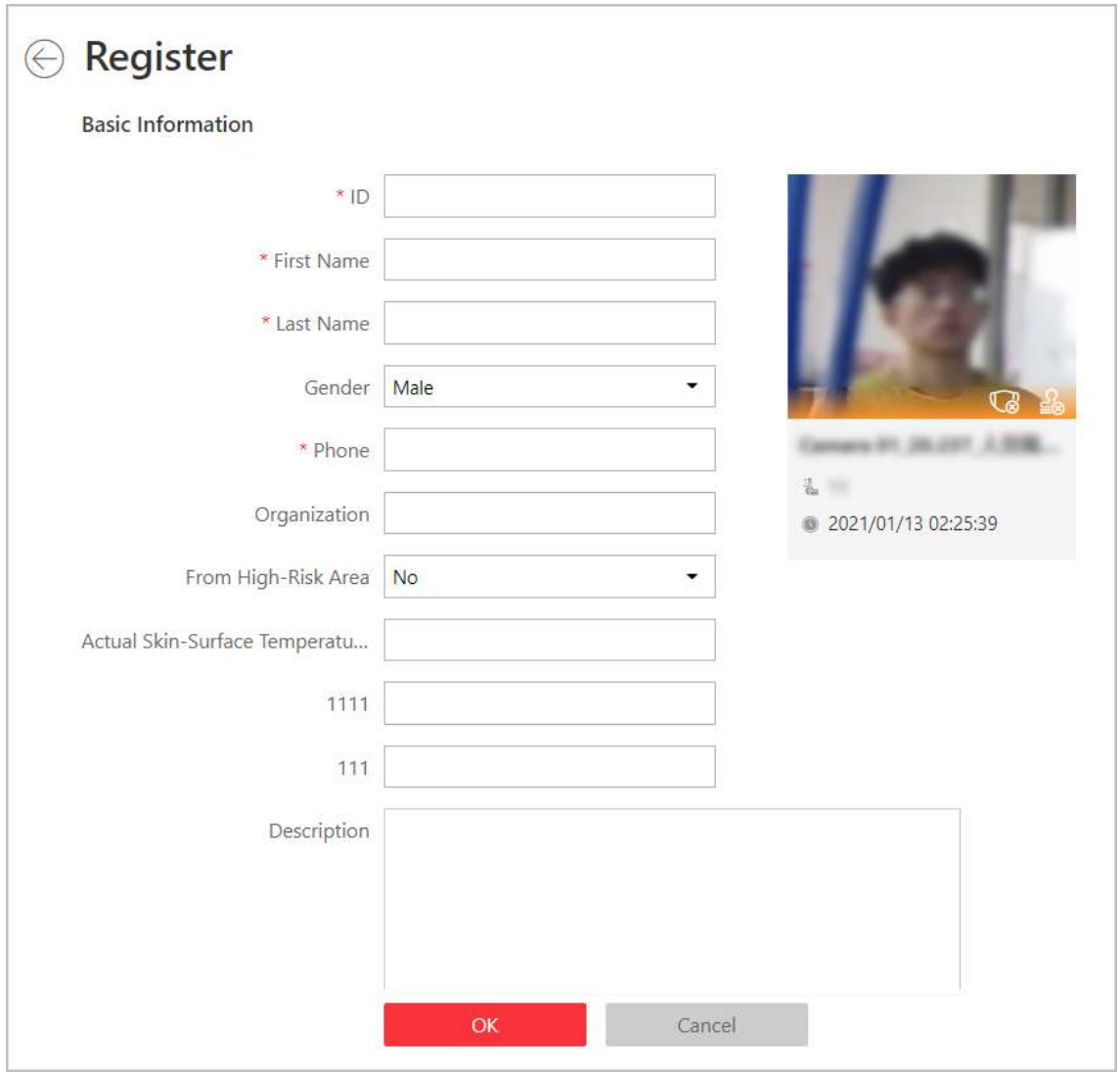


Figure 33-2 Register Page

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.

33.4.2 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.

33.4.3 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.

33.5 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**.

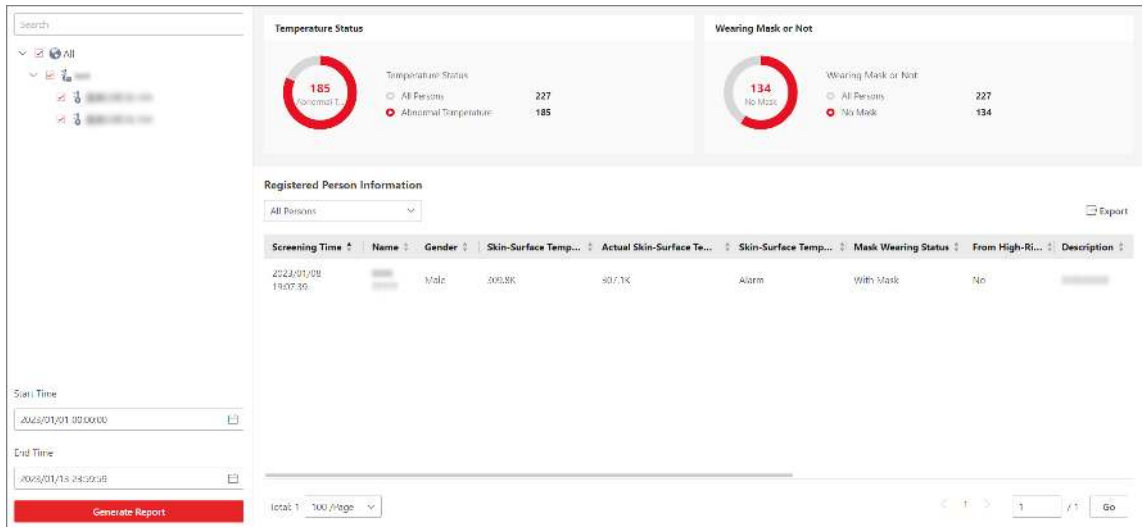


Figure 33-3 Skin-Surface Temperature Screening Records

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.

33.6 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 top navigation bar, select → **Passing Management** → **Temperature Screening** → **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 camera 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 33-4 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**.

33.7 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.

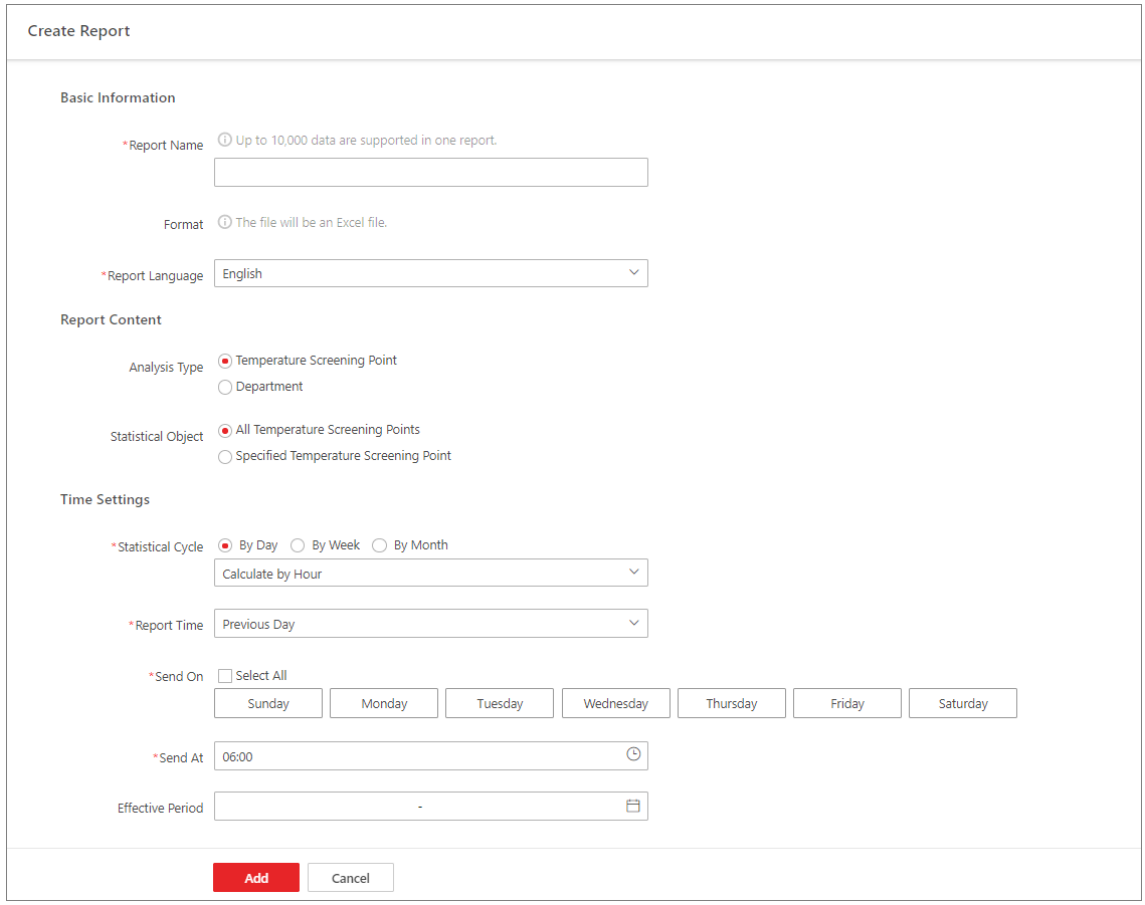


Figure 33-5 Configure Scheduled Report

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. For details about adding email templates, refer to ***Add Email Template for Sending Report Regularly*** .
- Refer to ***Configure Email Account*** for details about how to set email settings such as the sender's email address, name, and SMTP server address and port No.

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.

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.

34.1 Set Basic Settings for Broadcast

You can set locations to save the audio file and live broadcast recording file. Also, you can set parameters related with live broadcast, including broadcast mode and encoding format.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Basic Configuration**.
3. In Audio File area, select **Local Storage** or **pStor** as the location to save the audio file, and select the corresponding resource pool.

   Note

   When selecting pStor as the storage location, make sure you have added pStor to the platform. For details, refer to ***Add pStor*** .
4. In Live Broadcast Recording area, check **Live Broadcast Recording**.
5. Select **Local Storage** or **pStor** as the location to save the recording file, and select the corresponding resource pool.

   Note

   When selecting pStor as the storage location, make sure you have added pStor to the platform. For details, refer to ***Add pStor*** .
6. In Live Broadcast Parameters area, select the broadcast mode and the encoding format from the drop-down list.

   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.

7. Click **Save** to save the above settings.

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 top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Speaker Unit Group**.
3. Create a speaker unit group.
   1) Click .
   2) Enter the name for the group.
   3) Click **Add**.
4. 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**.
5. **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 **Volume** to adjust the volume of live broadcast or alarm-triggered broadcast for the selected devices. **Note** For Hikvision devices, you can only adjust the volume of live broadcast.

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 top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Media Library**.
3. 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.
4. Click **Add**.
5. Select one or more media files from local PC.

   Note

   The file should be in MP3 or WAV format, and no larger than 10 MB.
6. Click **Upload**.

   Note

   You can view the uploading progress and result(s).

   The uploaded media file(s) are displayed in the list.
7. **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 on the Operation column to download the media file to local PC.

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 speaker unit(s) to area(s). Refer to ***Add Speaker Unit to Area for Current Site*** 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 top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Live Broadcast and Recording** → **Live Broadcast** .
3. Select the online speaker unit(s) for live broadcast.
   - Select **Group**, and select one or more speaker units from speaker unit group(s).

Note

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.

4. Select the broadcast mode.
   - Check **Speak**.
   - Check **Audio File**, and select an audio file from the media library.

     Note

     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**, and enter the broadcast content as needed.
5. Select **Once** or **Specified Duration** as the play mode.
6. Click **Start**.

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 top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Live Broadcast and Recording** → **Live Broadcast Recording** .
3. Set the start time.
4. Set the end time.
5. Select a broadcaster from the drop-down list.
6. 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.
7. **Optional:** Perform the following operations.

Download	Click in the Operation column to download the broadcasted audio.

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.
- Make sure you have added speaker unit(s) to area(s). Refer to ***Add Speaker Unit to Area for Current Site*** for details.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Scheduled Broadcast**.
3. Click **Add** to enter Add Scheduled Broadcast page.
4. Enter the name for the scheduled broadcast task.
5. Select the speaker unit(s) to execute the task.
   - Check **Group**, and select one or more speaker units from speaker unit group(s).
   - Check **Area**, and select one or more speaker units from the area(s) where the speaker units are added.
6. Configure the period type.
   - When selecting **Every Day**, you should set the start date and end date.
   - When selecting **Every Week**, you should set the start date, end date, and the repetition day(s) of the week.
7. Configure the playing time.
   1) Click **Add**.
   2) Set the broadcast time as needed.
   3) Set **Once** or **Specified Duration** as the play mode.
   4) Click **Add** to finish adding.
8. Select the broadcast priority from the drop-down list.

   Note

   Broadcast priority ranges from 0 to 15. The larger the number, the higher the priority.
9. 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*** .

10. Click **Add** to save the above settings.

    A prompt of selecting the applying method pops up.
11. Apply the task.
    - Click **Apply Now** to apply the task immediately.
    - Click **Apply Later** to apply the task later.
12. **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. • Click **Stop** to stop playing the audio.
Apply	• Click **Apply All** to apply all the tasks to the speaker units. • 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.

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 platform. 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.
- Make sure you have added speaker unit(s) to area(s). Refer to ***Add Speaker Unit to Area for Current Site*** for details.

Steps

1. On the top navigation bar, select → **Integrated Service** → **Audio Broadcast** to enter the audio broadcast page.
2. On the left navigation pane, click **Linked Broadcast**.
3. Click **Add** to enter Add Broadcast Linkage page.
4. Enter the name for the linked broadcast task.
5. Select the speaker unit(s) to execute the task.
   - Check **Group**, and select one or more speaker units from speaker unit group(s).
   - Check **Area**, and select one or more speaker units from the area(s) where the speaker units are added.
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. 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.

   Broadcast Until Recovery

   The linked broadcast will be played continuously until the status of emergency is recovered.
8. Click **Add and Apply**.

   You can view the applying progress and the result.
9. **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. **Note** For details, refer to ***Emergency Solution Settings*** .

View Applying Failed Task(s)	indicates that the broadcast task(s) are failed to be applied. • Move the mouse cursor to beside the broadcast name, and click **View Details** to view the failure details of the current task. • 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. • Move the mouse cursor to beside the broadcast name, and click **Try Again** to apply the current task again. • 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.
Start/Stop Playing Broadcast Content	Click **Play/Stop** to start/stop playing the broadcast content of a task.
Search for Task(s)	Enter keywords in the search box in the upper-right corner, and click to search for the target task(s).
Delete a Task	Click **Delete** to delete a linked broadcast task.

Chapter 35 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.

35.1 Configure Security Inspection

You can configure the basic parameters for security inspection.

Steps

1. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Basic Settings** → **Parameter Configuration** .
2. Configure the following parameters and click **Save**.

   Match Detected Package with Face(s) Captured Within (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 behavior type(s) for behavior analysis, and the alarm type(s) for metal detection.

35.2 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. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Basic Settings** → **Security Inspection Channel Management** .
2. Select an area from the area list.
3. Click **Add** to enter the Add Security Inspection Channel page.
4. Enter the channel name and description.

5. **Optional:** In the Linkage 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. Click **Add**.

35.3 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*** .

In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Security Inspection Visualization** .

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.

Live View

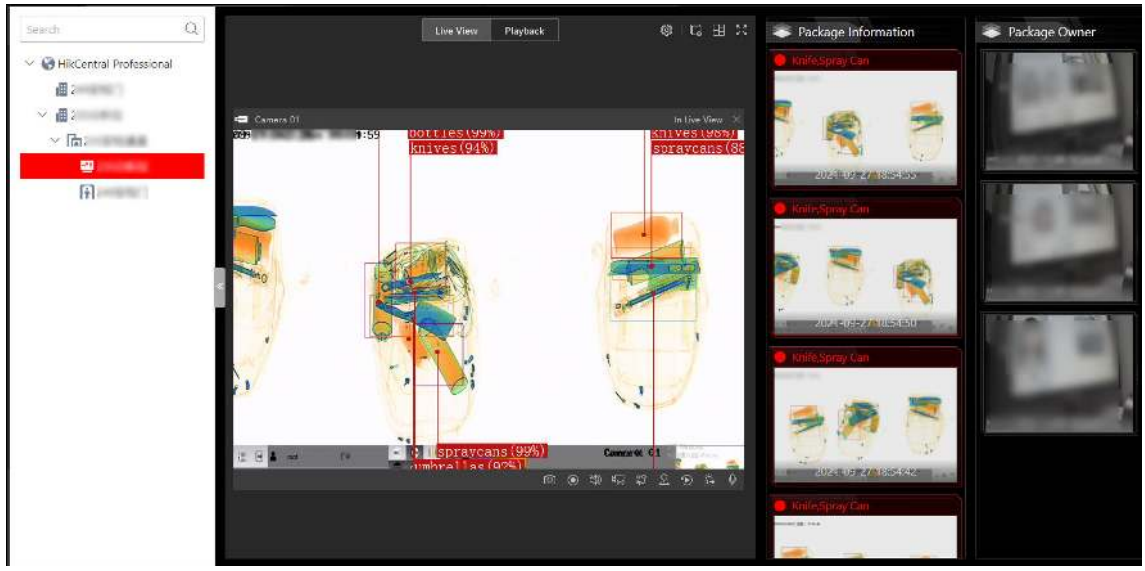


Figure 35-1 Live View

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.

Icon	Function	Description
	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

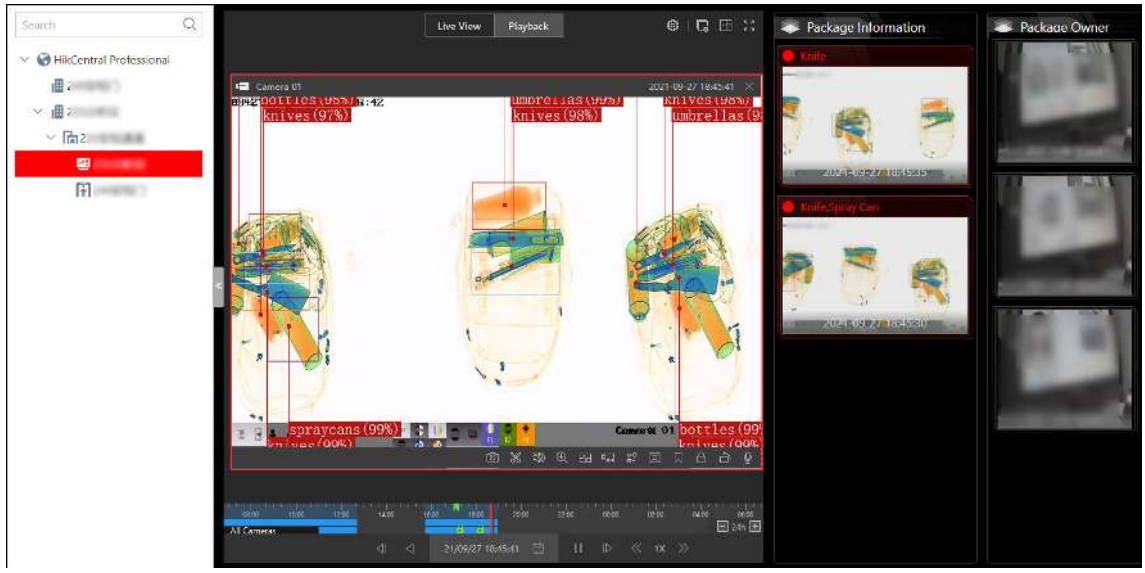


Figure 35-2 Playback

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.

Icon	Function	Description
	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. **Note** 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.

35.4 Historical Data Search

You can search for the historical data of security inspection, including package detection records, metal detection records, and inspector absence records.

35.4.1 Search for Package Detection Records

You can set search conditions, including time, article type, and location, to search for the package detection records.

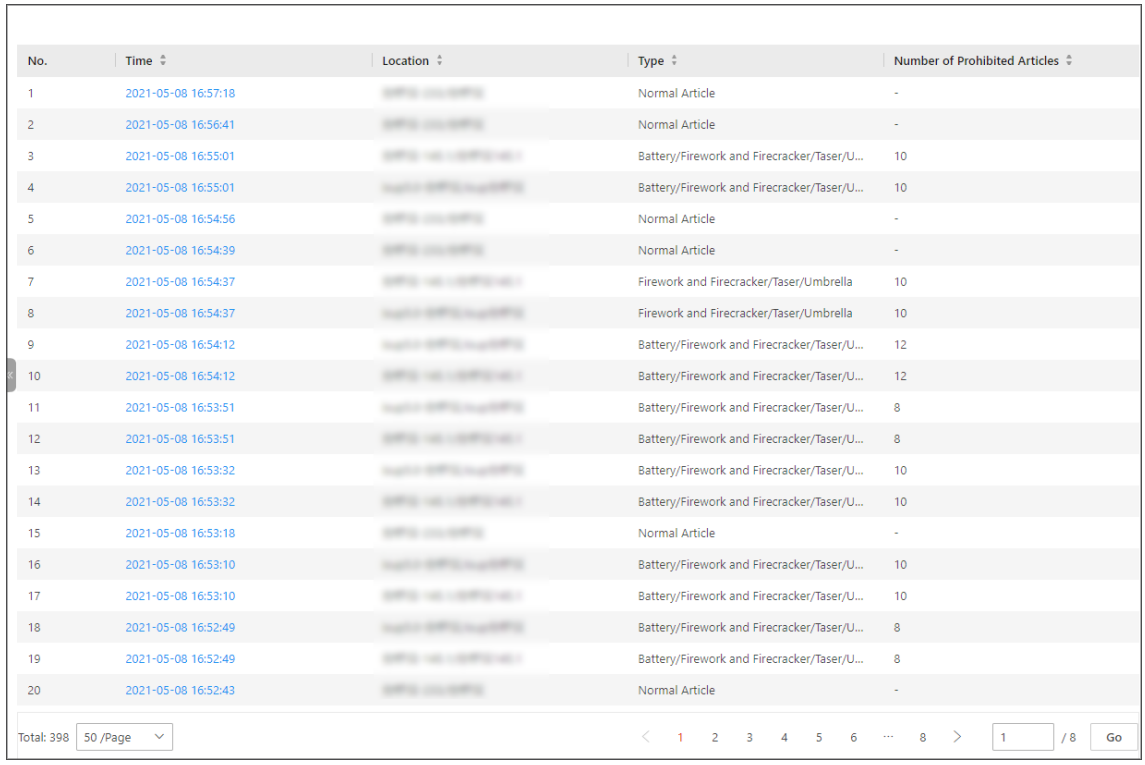
Steps

1. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Historical Data Search** → **Package Detection Record Search** .
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		Normal Article	-
2	2021-05-08 16:56:41		Normal Article	-
3	2021-05-08 16:55:01		Battery/Firework and Firecracker/Taser/U...	10
4	2021-05-08 16:55:01		Battery/Firework and Firecracker/Taser/U...	10
5	2021-05-08 16:54:56		Normal Article	-
6	2021-05-08 16:54:39		Normal Article	-
7	2021-05-08 16:54:37		Firework and Firecracker/Taser/Umbrella	10
8	2021-05-08 16:54:37		Firework and Firecracker/Taser/Umbrella	10
9	2021-05-08 16:54:12		Battery/Firework and Firecracker/Taser/U...	12
10	2021-05-08 16:54:12		Battery/Firework and Firecracker/Taser/U...	12
11	2021-05-08 16:53:51		Battery/Firework and Firecracker/Taser/U...	8
12	2021-05-08 16:53:51		Battery/Firework and Firecracker/Taser/U...	8
13	2021-05-08 16:53:32		Battery/Firework and Firecracker/Taser/U...	10
14	2021-05-08 16:53:32		Battery/Firework and Firecracker/Taser/U...	10
15	2021-05-08 16:53:18		Normal Article	-
16	2021-05-08 16:53:10		Battery/Firework and Firecracker/Taser/U...	10
17	2021-05-08 16:53:10		Battery/Firework and Firecracker/Taser/U...	10
18	2021-05-08 16:52:49		Battery/Firework and Firecracker/Taser/U...	8
19	2021-05-08 16:52:49		Battery/Firework and Firecracker/Taser/U...	8
20	2021-05-08 16:52:43		Normal Article	-

Total: 398 50 /Page 1 2 3 4 5 6 ··· 8 1 / 8 Go

Figure 35-3 Search for Package Detection Records

35.4.2 Search for Metal Detection Records

You can set the search conditions, including time and location, to search for the metal detection records.

Steps

1. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Historical Data Search** → **Metal Detection Record Search** .

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.

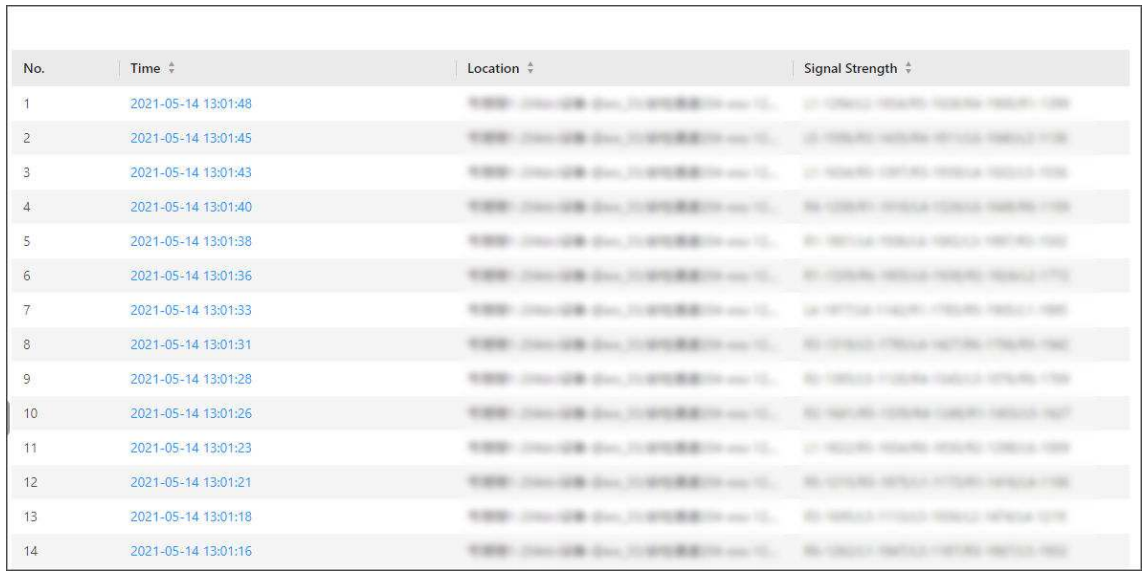


Figure 35-4 Search for Metal Detection Records

35.4.3 Search for Absence Records

You can set the search conditions, including time and location, to search for the absence records.

Steps

1. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Historical Data Search** → **Absence Record Search** .
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 35-5 Search for Absence Records

35.5 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. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Statistics and Reports** → **Package Detection Report** .
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.

35.6 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. In the top left corner of the Home page, select → **All Modules** → **Smart Security Inspection** → **Statistics and Reports** → **People Inspection Report** .
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 36 Emergency Mustering

The emergency mustering helps users get prepared to account for all staff in a quick and efficient manner in an emergency situation, such as a fire.

You can configure an emergency solution beforehand and start a roll call by one click. In an emergency, the users can:

- Conduct a roll call with real-time data.
- Get immediate access to personal contact information.
- Filter persons based on status (In, Out & Not Check In, Checked In, and Unknown)

Based on the information provided by the platform, users can rescue persons who are still in the place.

In the top left corner of Home page, select → **Integrated Service** → **Emergency Mustering** .

Select **Emergency Solution Settings** on the left.

Note

If you are configuring emergency solution for the first time, click **Configure**at the bottom of the page to enter the emergency solution configuration page.

Click **View Service Details** and configure the emergency solution following the guidance.

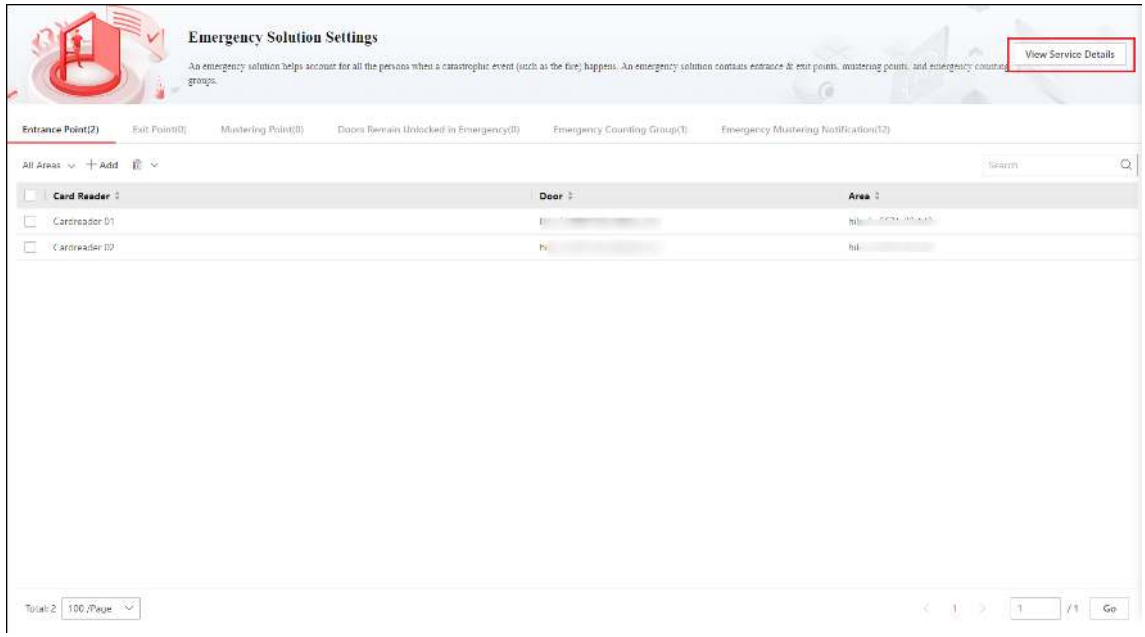


Figure 36-1 Entrance Point List

36.1 Emergency Solution Settings

An emergency solution refers to the preparation settings before a roll call. The emergency solution includes the settings of entrance points, exit points, mustering points, doors remaining unlocked in an emergency, emergency counting groups, and emergency mustering programs and text notifications. After setting the emergency solution, users can start a roll call by one click once an emergency happens.

In the top left corner of Home page, select → **Integrated Service** → **Emergency Mustering** .

Select **Emergency Solution Settings** on the left.

Note

If you are configuring emergency solution for the first time, click **Configure**at the bottom of the page to enter the emergency solution configuration page.

1. Add Entrance Points

An entrance point is the card reader by which persons authenticate to check in before entering a place. If a person authenticates by an entrance point, the person's status is In.

Click ⌄ besides **All Areas** and select an area. Click **Add** and select card readers to set them as entrance points of the area.

You can check card readers and click 🗑 to cancel setting them as entrance points, or click ⌄ → **Delete All** to cancel setting all card readers as entrance points. You can also enter a card reader name on the top right to search for it.

Note

- Make sure you have added the card reader to the platform before selecting the entrance points.
- To delete the entrance points, you should end the emergency first.

2. Add Exit Points

An exit point is the card reader by which persons authenticate for exiting from a place. If a person authenticates by an exit point, the person's status is Out.

Click ⌄ besides **All Areas** and select an area. Click **Add** and select card readers to set them as exit points in the area.

You can check card readers and click 🗑 to cancel setting them as exit points, or click ⌄ → **Delete All** to cancel setting all card readers as exit points. You can also enter a card reader name on the top right to search for it.

Note

- Make sure you have added the card reader to the platform before selecting the exit points.
- To delete the exit points, you should end the emergency first.

3. Add Mustering Points

A mustering point is the card reader located in a refuge. When an emergency happens, persons exit from the place where they are, go to the refuge, and check in by the mustering point. The status of persons who have checked in at the mustering point is Out & Checked In.
Click ⌄ besides **All Areas** and select an area. Click **Add** and select card readers to set them as mustering points in the area.
You can check card readers and click 🗑 to cancel setting them as mustering points, or click ⌄ → **Delete All** to cancel setting all card readers as mustering points. You can also enter a card reader name on the top right to search for it.

Note

- Make sure you have added the card reader to the platform before selecting the mustering points.
- To delete the mustering points, you should end the emergency first.

4. Add Doors Remaining Unlocked in Emergency

A door remaining unlocked in an emergency refers to the door that will be turned to the status of Remain Unlocked once an emergency happens. Thus the persons inside the place can exit from the place without authentication at the card reader.
Click ⌄ besides **All Areas** and select an area. Click **Add** and select doors to set them as doors remaining unlocked in an emergency in the area.
You can check doors and click 🗑 to delete them, or click ⌄ → **Delete All** to delete all doors. You can also enter a door name on the top right to search for it.

Note

- Make sure you have added the door to the platform before selecting the doors.
- To delete the doors, you should end the emergency first.

5. Add Emergency Counting Groups

An emergency counting group refers to a person group based on which you can know how many persons are in, out, or out & checked in when the platform is in an emergency.
Click + to open the Add Emergency Counting Group pane. Enter a name for the group and click 📄 to add persons to the group. Click **Add** under Person to add more persons to the group after adding the group.

Note

- Make sure you have added the persons to the platform beforehand.

You can perform the following operations.

- Hover over **1 Day(s) Before** and select the days before emergency is triggered to update the persons in the group.
- Hover over and select **Descending by Group Name** or **Ascending by Group Name** to sort the emergency counting groups.
- In the Person section, select **Descending by Person Name**/**Ascending by Person Name** to sort the persons.
- Click a person name to view person details.
- Select a group and click to delete it, or click → **Delete All** to all groups.
- Check persons and click **Delete** to remove the selected persons from the group, or click → **Delete All** to remove all the persons from the group.

6. Release Emergency Mustering Notification

You can configure emergency mustering programs and emergency text notifications for catastrophic event (e.g., fire and robbery). Emergency mustering programs or emergency mustering text notifications will be displayed on the digital signal terminals when an emergency is triggered, to help people receive timely emergency alerts and be out of danger as soon as possible when an emergency happens;

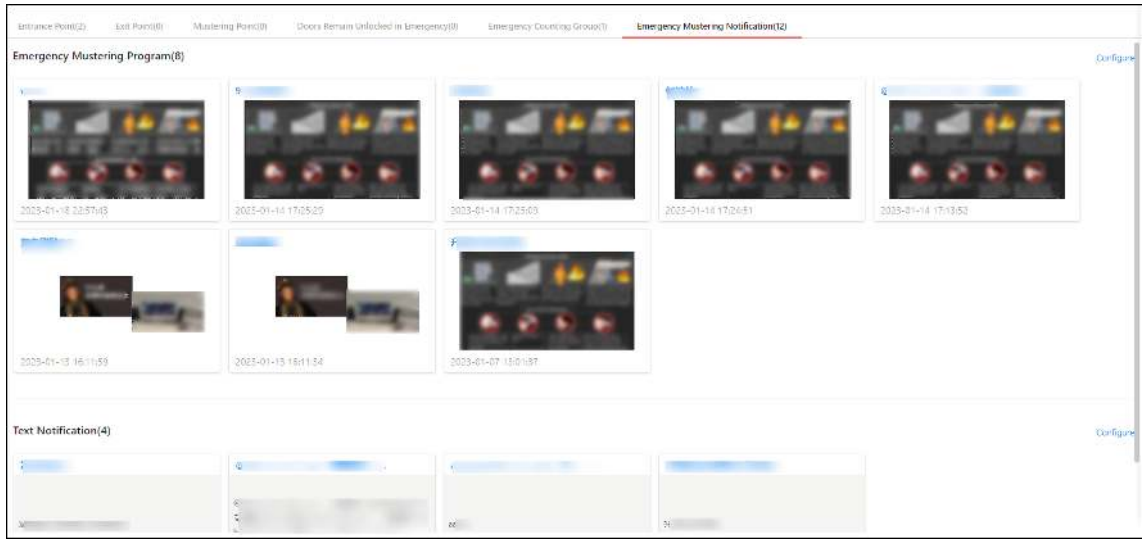


Figure 36-2 Emergency Mustering Notification

1. Click **Configure** on the right to configure emergency mustering programs or text notifications.

Note

You can switch application modes between **Digital Signage** and **Interactive Flat Panel**. See details in ***Switch Application Mode*** .

2. Emergency Mustering Program: Click + to enter the Create Programs page. Enter the program name, screen size and sharing property, and select an area as needed. Click **Next** to select a program template. Then you can configure more parameters of this program and click **Release** to release the program.

Emergency Text Notification: Click **Text Notification** → + to enter the Create Text Notification page. Enter the text notification name, sharing property, and notification content and select an area and devices as needed. Click **Release** to release the text notification.

3. When the emergency alarm is triggered, the normal transmissions will be interrupted and the screen will switch to the released emergency mustering programs or text notifications throughout the emergency; when it is no longer in emergency status, the normal transmission will be back.

Note

If you manually turn off emergency or delete the device from the platform, the emergency mustering programs or text notifications will not be played.

36.2 Start a Roll Call

After configuring the emergency solution, you can start a roll call by one click once an emergency happens.

In the top left corner of Home page, select → **Integrated Service** → **Emergency Mustering** → **Roll Call** .

Click **Trigger Emergency** to display the data of emergency counting groups.

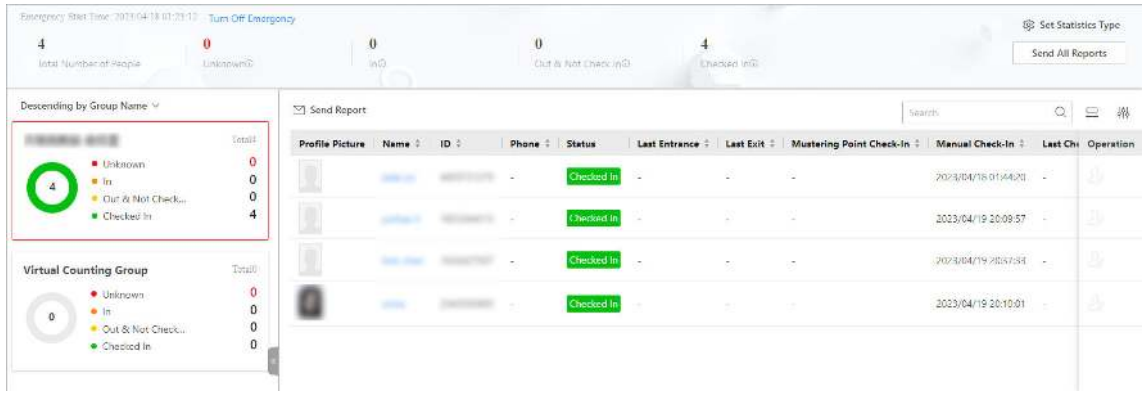


Figure 36-3 Data of Emergency Mustering

On the top left, the total number of persons in emergency counting groups is displayed. On the right of the total number of persons, the number of persons in danger and safe are both displayed. The persons in danger refer to persons who are still inside (checked in at the entrance point but did not check out at the exit point) the place where the emergency happens and the persons who did not check in at the entrance point. The persons who are safe refer to persons who have checked out at the exit point but not checked in at the mustering point and persons who have checked in at the mustering point.

You can click **Set Statistics Type** on the right and check person statuses that need to pay attention to, and the selected statuses will e displayed.

The data of each emergency counting group is also displayed. You can click a group name to enter the page of the group for details. Click to check in a person who shows at the mustering point but the person status is not Checked In.

The virtual counting group refers to a group consisting of persons who are not added to any emergency counting group.

Perform the following operations if you need.

- Click **Turn Off Emergency** to end the emergency status of the platform.
- Click **Send All Reports** and select an email template to send the data of all the emergency counting groups to the recipients.
- Click beside each column heading to sort the persons by name, ID, phone No., etc.
- Click and check the items to be displayed in the person list of the counting group.
- Click and select Complete Display of Each Column Title or Incomplete Display of Each Column Title. The column width will be self-adjusted according to the settings.

Note

- It is extremely important to remember that the data displayed and the reports contained in the email can only ever be accurate if all users follow the conventions of the system.
- During the emergency, editing the emergency solution is not allowed. You should end the emergency before editing it.

Chapter 37 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.

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).

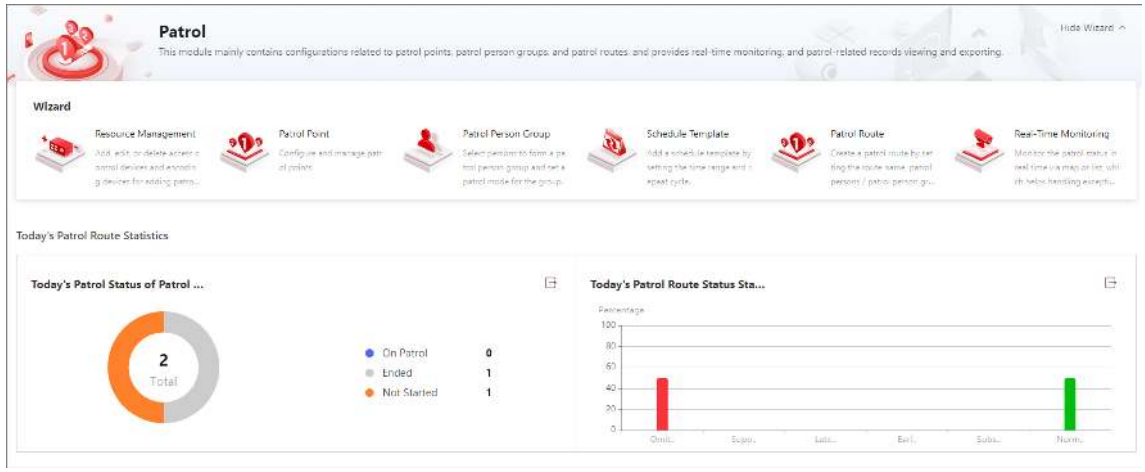


Figure 37-1 Patrol Overview

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.

37.1 Flow Chart of Patrol Management

The flow chart below shows the process of configuring and managing patrols.

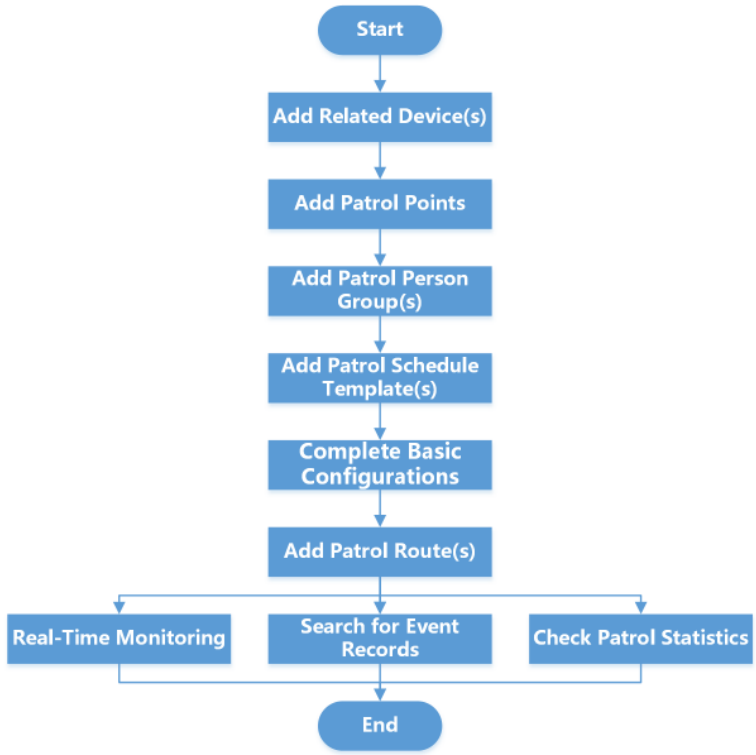


Figure 37-2 Flow Chart of Patrol Management

Table 37-1 Flow Chart Description

Step	Description
Add Related Device(s)	Add devices used for adding patrol points, real-time monitoring, etc. See ***Manage Access Control Device*** and ***Manage Encoding Device*** for details.
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.

37.2 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.

37.2.1 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**.

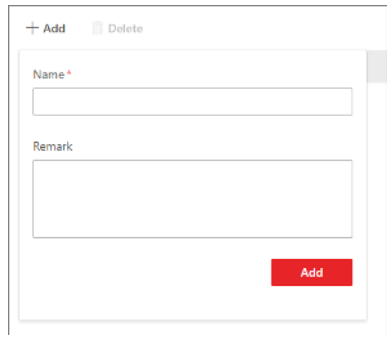


Figure 37-3 Add Exception Type

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.

37.2.2 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** .

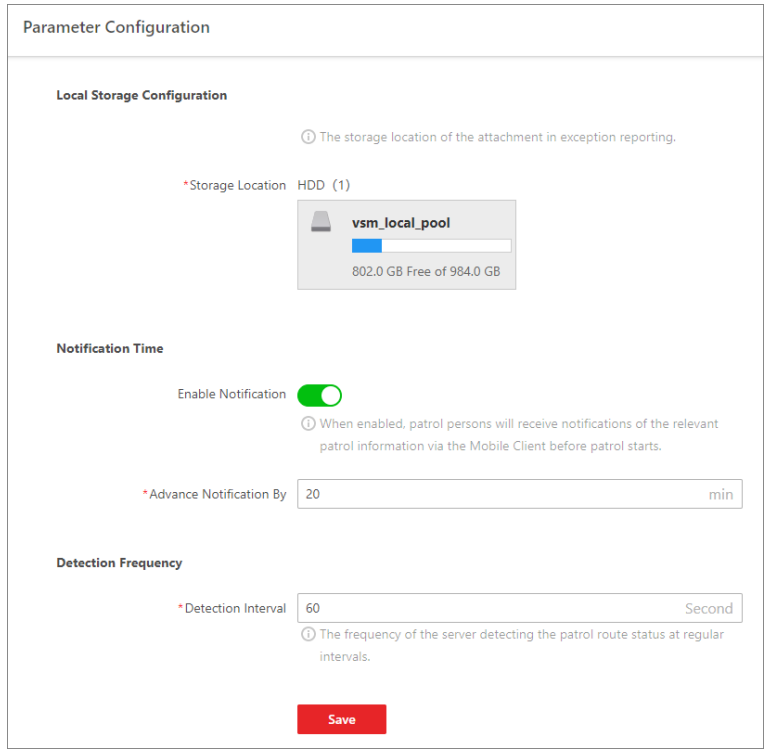


Figure 37-4 Parameter Configuration

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.

37.3 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**.

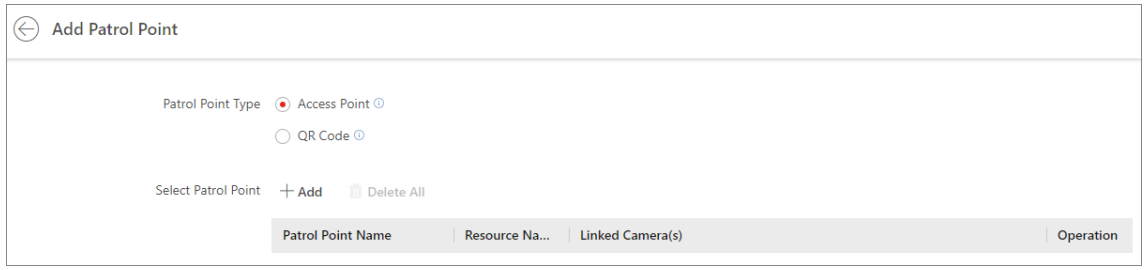


Figure 37-5 Add Patrol Point

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:** Click **Delete All** to delete all patrol points, or click to delete one patrol point.
6. Click **Save**.

   The added patrol points will be displayed on the patrol point list.
7. 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.

37.4 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.

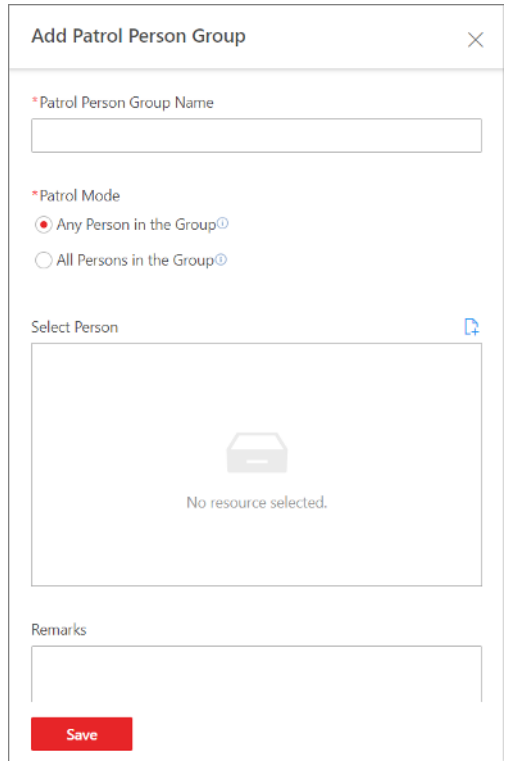


Figure 37-6 Add Patrol Person Group

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.

37.5 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.

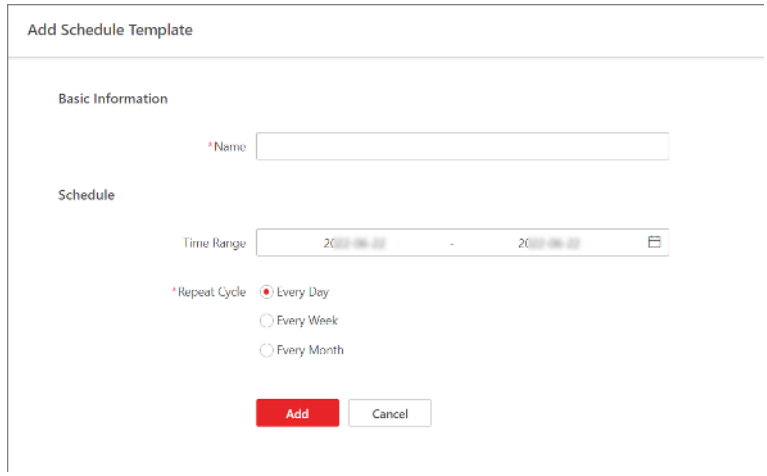


Figure 37-7 Add Schedule Template

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**. **Note** 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.

37.6 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 **Add** to open the patrol route configuration page.

Note

If you have already added a patrol route before, click **Save** to proceed.

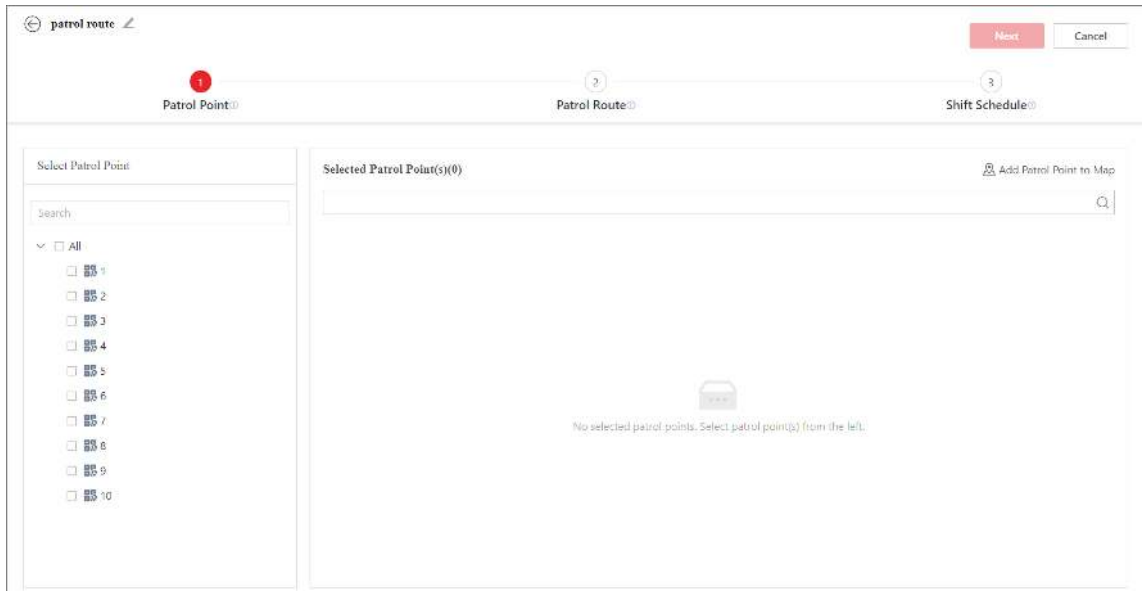


Figure 37-8 Patrol Route Configuration Page

6. Select the patrol point(s) that the patrol persons need to patrol on a route, and 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.
- You can click ↑ and ↓ to rearrange the patrol list order as needed.

7. Set the patrol pattern for the route.

Note

The patrol pattern is **In Order** by default. Click **Switch Patrol Pattern** to switch to another pattern from the list.

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. Set the total patrol duration (in minutes) for the patrol route.
9. 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.

10. Click **Add Shift Schedule**.

11. 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*** .

12. 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.

13. Click **Finish** to complete the patrol route configuration.

14. **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**.

37.7 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.

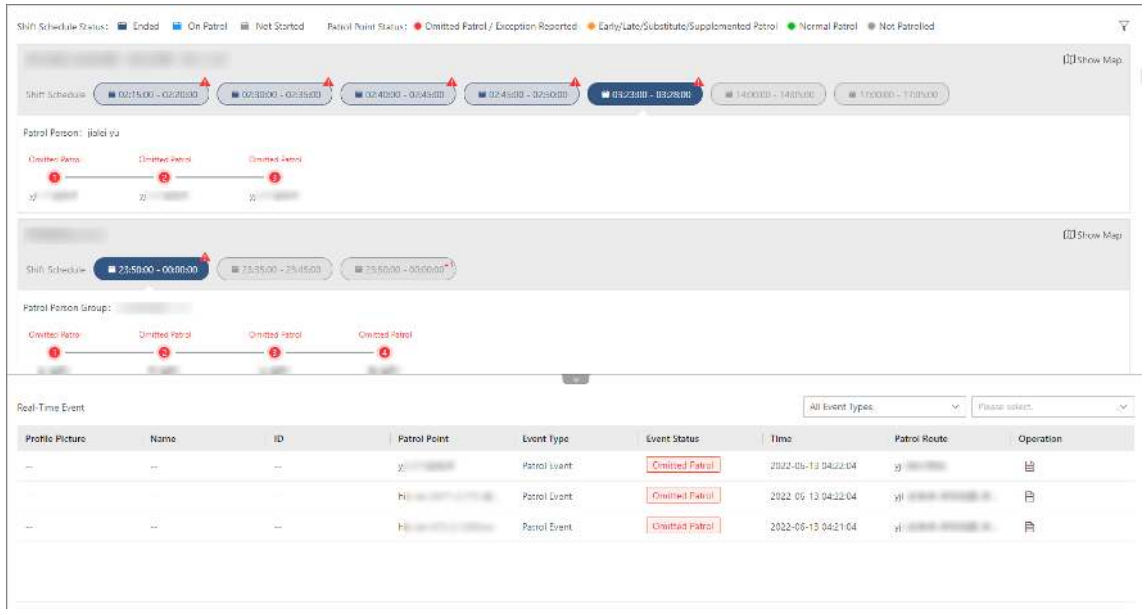


Figure 37-9 Real-Time Monitoring Page

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 reported, 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 and exception reporting), 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, 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.

37.8 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** .

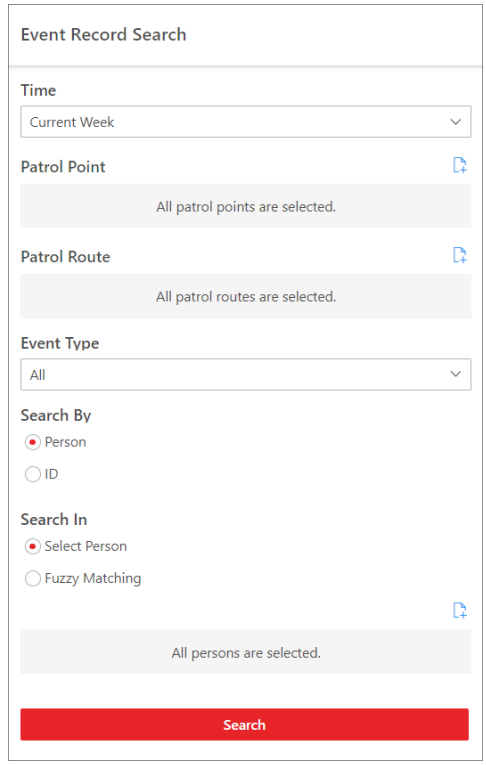


Figure 37-10 Event Record Search

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** or **Exception Reporting** from the drop-down list to search for the specified type of event records only.

Search By

Choose whether to search for the event records by **Person** or **ID**.

- Search by person: In the **Search In** field, choose whether to search by person selections or fuzzy matching of persons' names.
- Search by ID: 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. • For a patrol event, you can view the event information (e.g., patrol status), patrol information (e.g., patrol point, 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. • 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.

37.9 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.

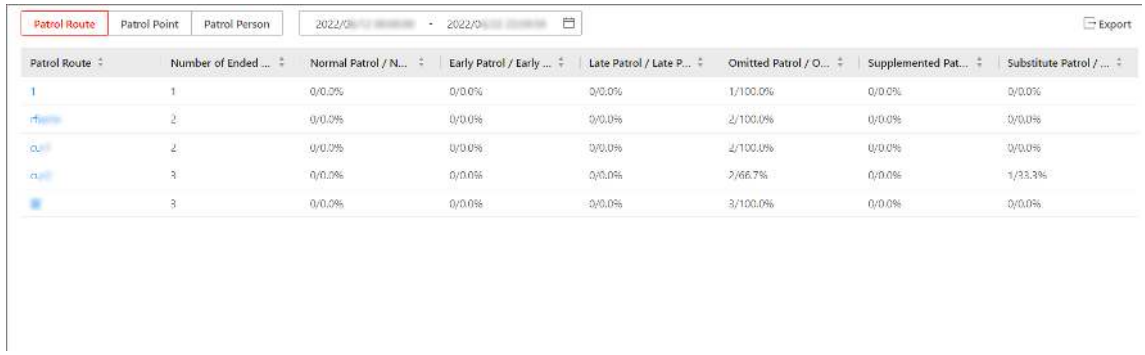


Figure 37-11 Patrol Statistics Page

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 38 Toll Verification

The platform allows you to search for the vehicle information and check it based on the captured pictures and recorded videos when a request is submitted for toll verification. You can also search for toll verification records by conditions and export the matched records to the local PC.

38.1 Basic Configuration

You can configure the basic parameters for the toll verification module, including the start and end time for playback.

On the top navigation bar, go to → **Toll Verification** → **Basic Configuration** , set the following parameter(s), and click **Save**.

Time Before/After Capture

Specify the start/end time for video playback.

38.2 Check Vehicle Information for Toll Verification

You can search for a pair of vehicle passing records (a vehicle's entering and leaving the highway) and check the vehicle information based on the captured pictures and recorded videos for toll verification.

Steps

1. On the top navigation bar, go to → **Toll Verification** .
2. Specify the time, camera(s), and license plate No. for record search.
3. Click **Search**.

   The matched records, including those of the vehicles' entering and leaving the highway, are displayed.
4. Select a pair of records (a vehicle's entering and leaving the highway) and click **Verification**.

   The Verification pane with vehicle information is displayed.

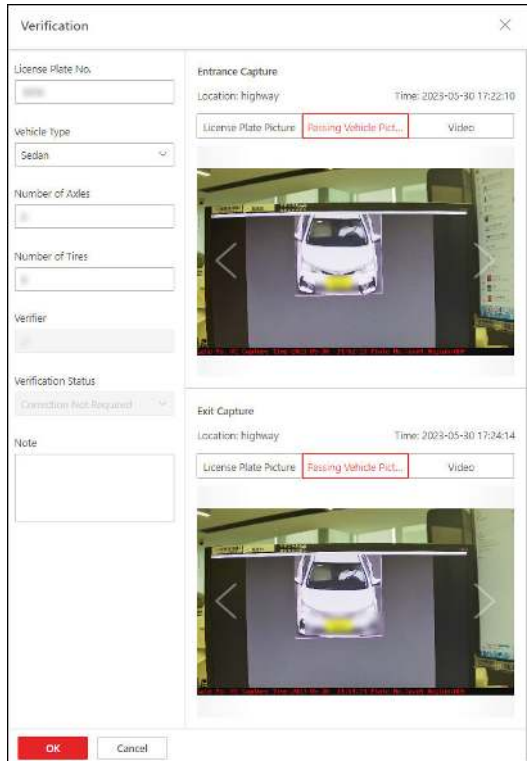


Figure 38-1 Verification Pane

5. Check and edit the license plate No., vehicle type, number of axles, and number of tires based on the captured pictures and recorded videos.

Note

If any vehicle information is changed, the verification status will be changed automatically from **Correction Not Required** to **Corrected**.

6. **Optional:** Enter notes in the box.
7. Click **OK**.

38.3 Search for Toll Verification Records

You can search for toll verification records to view their details and export them to your local PC.

Steps

1. On the top navigation bar, go to → **Toll Verification** → **Toll Verification Record** .
2. Specify a period for record search.
3. **Optional:** Switch on **License Plate No.** and enter a license plate No.
4. **Optional:** Switch on **Verification Result** and select **Corrected** or **Correction Not Required** from the drop-down list.
5. **Optional:** Switch on **Verifier** and enter a user name.

6. Click **Search**.

   The toll verification records are displayed.

7. **Optional:** Click **Export** and set the format to export the records to the local PC.

Chapter 39 Traffic Data Analysis

The Traffic Data Analysis module allows you to set the needed conditions such as the statistics type and the time to analyze the traffic data.

Note

To use this function, make sure you have added one or more events below "Traffic Event" as triggering events on the Add Event and Alarm page. For details, refer to ***Add Normal Event and Alarm*** .

On the top navigation bar, select → **Traffic Incident Detection** → **Traffic Data Analysis** to enter the Traffic Data Analysis page.

Set the conditions according to actual needs, and the corresponding analysis data will be displayed below. The conditions include the statistics type (By Traffic Incident Type, By Area, and By Time), device (up to 10 devices can be selected), and time (Day, Week, Month, Year, and Specific Time).

Note

The following figure is an analysis result for your reference.

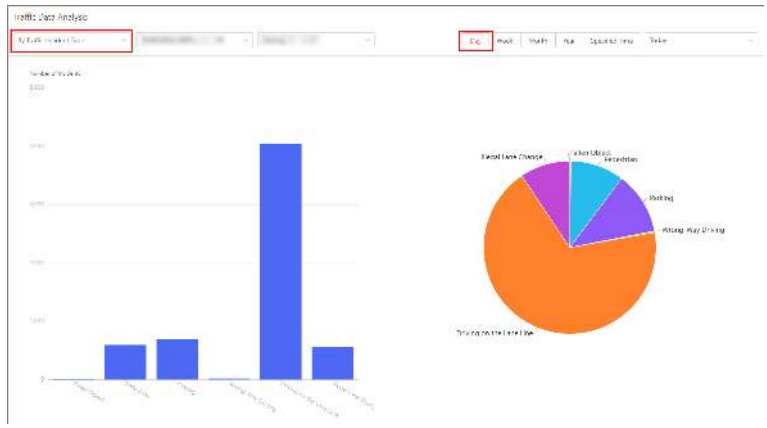


Figure 39-1 Traffic Data Analysis

Chapter 40 Street Data Analysis

The Street Data Analysis module allows you to set the needed conditions such as the statistics type and the incident type(s) to analyze the street data.

Note

To use this function, make sure you have added one or more events below "Intelligent Urban Management Analysis" as triggering events on the Add Event and Alarm page. For details, refer to ***Add Normal Event and Alarm*** .

On the top navigation bar, select → **Street Management** → **Street Data Analysis** to enter the Street Data Analysis page.

Set the conditions according to actual needs, and the corresponding analysis data will be displayed below. The conditions include the statistics type (By Time, By Area, By Urban Management Incident Type), device (up to 10 devices can be selected), incident type (Open-Air Vendor, Unregistered Street Vendor, Roadside Vender, and so on), and time (Day, Week, Month, Year, and Specific Time).

Note

The following figures are three analysis results for your reference.

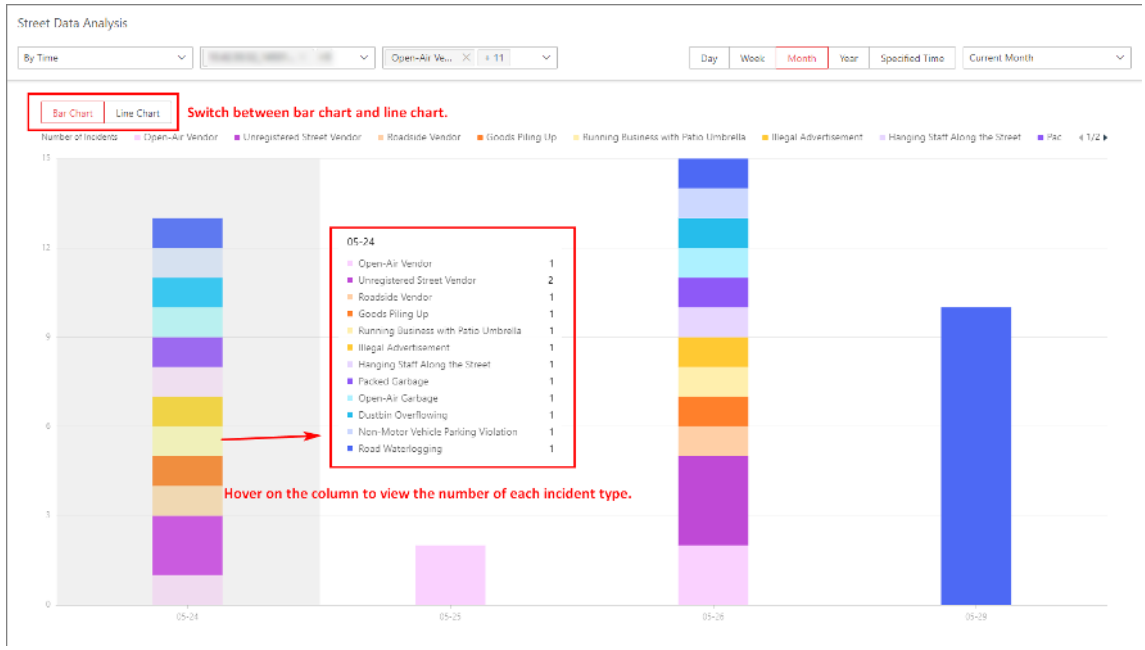


Figure 40-1 Street Data Analysis (By Time)

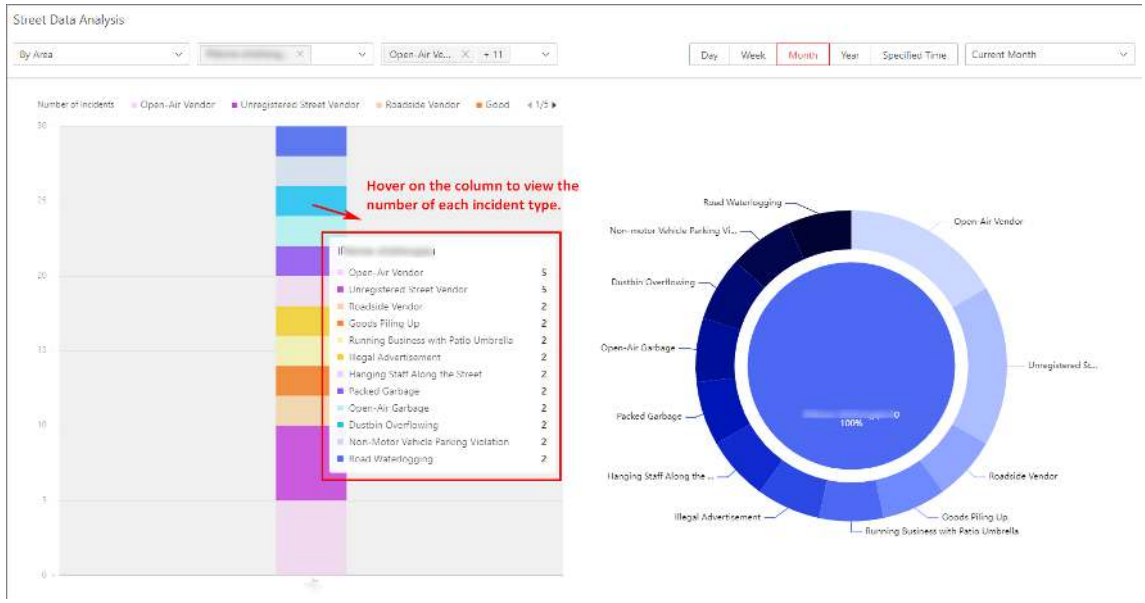


Figure 40-2 Street Data Analysis (By Area)

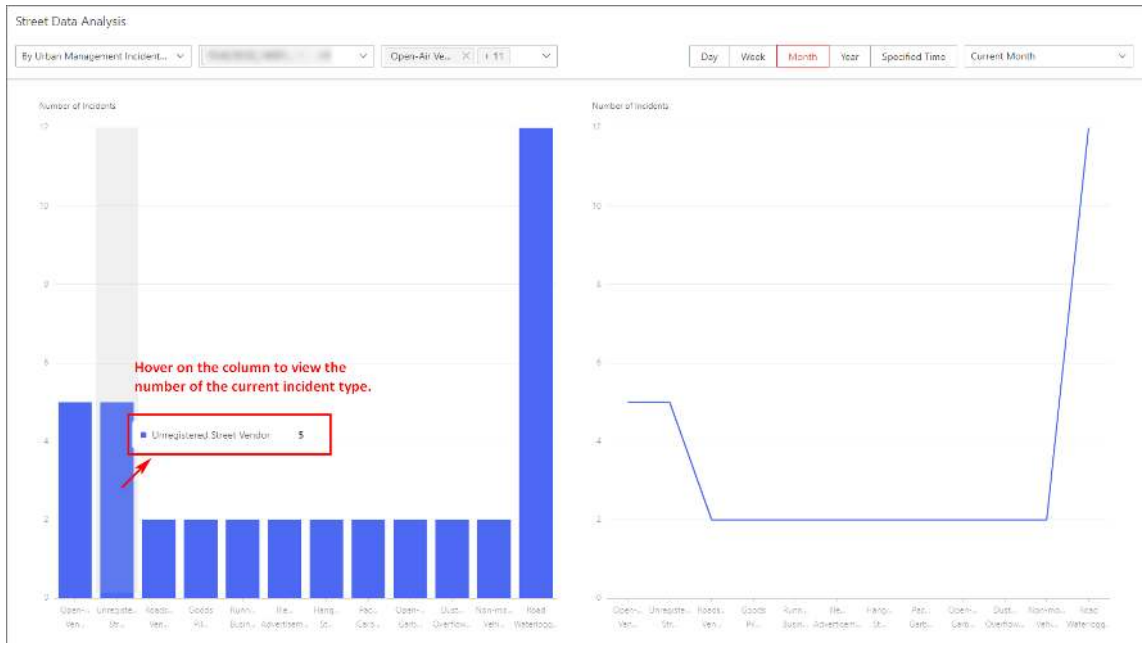


Figure 40-3 Street Data Analysis (By Urban Management Incident Type)

Chapter 41 Water Level Detection

The Water Level Detection Management module is for users to detect the water level according to actual needs and take the corresponding measures if the water level is not within the normal range. The functions supported in this module include searching for water level data according to time and detection station, and analyzing water level data in a certain detection station during the selected time.

Note

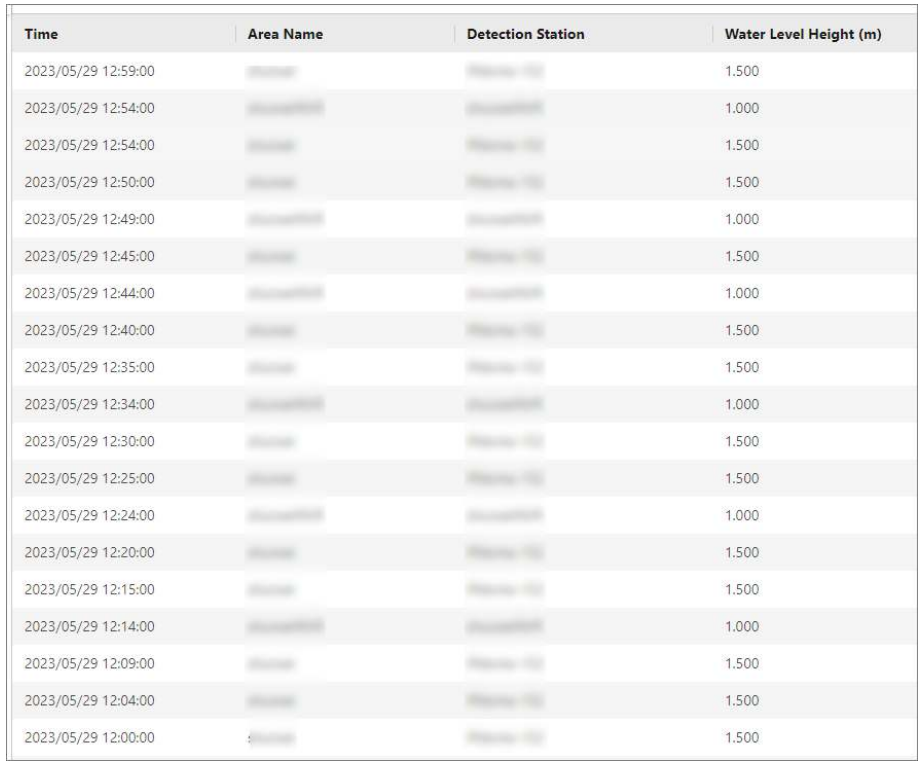
This function should be supported by the device. Make sure you have added water level detection PTZ cameras to the platform via Hikvision Private Protocol or Hikvision ISUP Protocol. For details, refer to the related contents in ***Manage Encoding Device*** .

41.1 Search for Water Level Data

You can set conditions such as time and detection station to search for the water level data. You can export the searched data to local PC if needed.

Steps

1. On the top navigation bar, select → **Water Level Management** → **Water Level Detection Management** .
2. Click **Search Water Level Data** on the left panel.
3. Set the search conditions including time and detection station.
4. **Optional:** Enable **Water Level Height**, and enter the height of water level.
5. Click **Search** to start searching.



Time	Area Name	Detection Station	Water Level Height (m)
2023/05/29 12:59:00	[redacted]	[redacted]	1.500
2023/05/29 12:54:00	[redacted]	[redacted]	1.000
2023/05/29 12:54:00	[redacted]	[redacted]	1.500
2023/05/29 12:50:00	[redacted]	[redacted]	1.500
2023/05/29 12:49:00	[redacted]	[redacted]	1.000
2023/05/29 12:45:00	[redacted]	[redacted]	1.500
2023/05/29 12:44:00	[redacted]	[redacted]	1.000
2023/05/29 12:40:00	[redacted]	[redacted]	1.500
2023/05/29 12:35:00	[redacted]	[redacted]	1.500
2023/05/29 12:34:00	[redacted]	[redacted]	1.000
2023/05/29 12:30:00	[redacted]	[redacted]	1.500
2023/05/29 12:25:00	[redacted]	[redacted]	1.500
2023/05/29 12:24:00	[redacted]	[redacted]	1.000
2023/05/29 12:20:00	[redacted]	[redacted]	1.500
2023/05/29 12:15:00	[redacted]	[redacted]	1.500
2023/05/29 12:14:00	[redacted]	[redacted]	1.000
2023/05/29 12:09:00	[redacted]	[redacted]	1.500
2023/05/29 12:04:00	[redacted]	[redacted]	1.500
2023/05/29 12:00:00	[redacted]	[redacted]	1.500

Figure 41-1 Search Results

6. **Optional:** Export the searched water level data.
   - Click **Export → Export to Excel** to export the searched data in an Excel file to local PC.
   - Click **Export → Export to CSV** to export the searched data in a CSV file to local PC.

41.2 Analyze Water Level Data

You can analyze the water level data of the water station by a line chart or bar chart. Also, you can define the time of analysis and export the analysis data to the local PC.

On the top navigation bar, select → **Water Level Management → Water Level Detection Management** , and click **Water Level Data Analysis** on the left panel.

In the upper left corner of the Water Level Data Analysis page, select a detection station from the drop-down list, and then define the time (Day or Month) of data analysis according to actual needs in the upper right corner.

Note

The following figures are two analysis results for your reference.

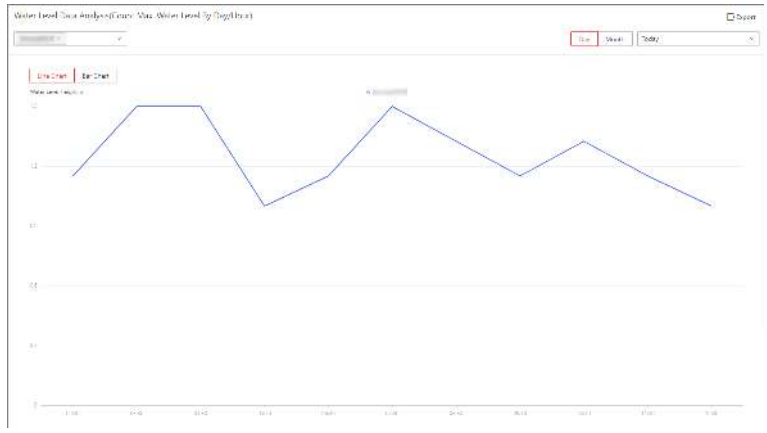


Figure 41-2 Water Level Data Analysis of Current Day (Line Chart)

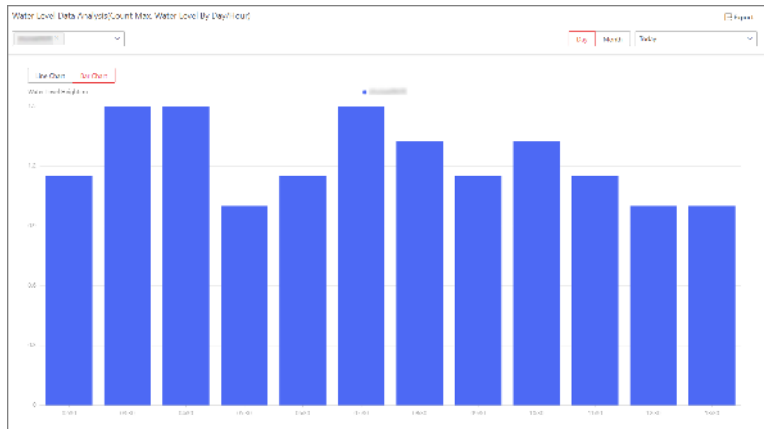


Figure 41-3 Water Level Data Analysis of Current Day (Bar Chart)

After analysis, you can click **Export** to export the analysis data in an Excel or CSV file to the local PC.

Chapter 42 Dock Management

The platform allows you to add dock areas and docks for convenient management. You can link cameras with docks for dock monitoring. Also, you can search for vehicle data and generate reports on dock usage, dock throughput, and dock using trend for business analysis and decision making.

42.1 Flow Chart of Dock Management

The flow chart below shows the process of dock management.

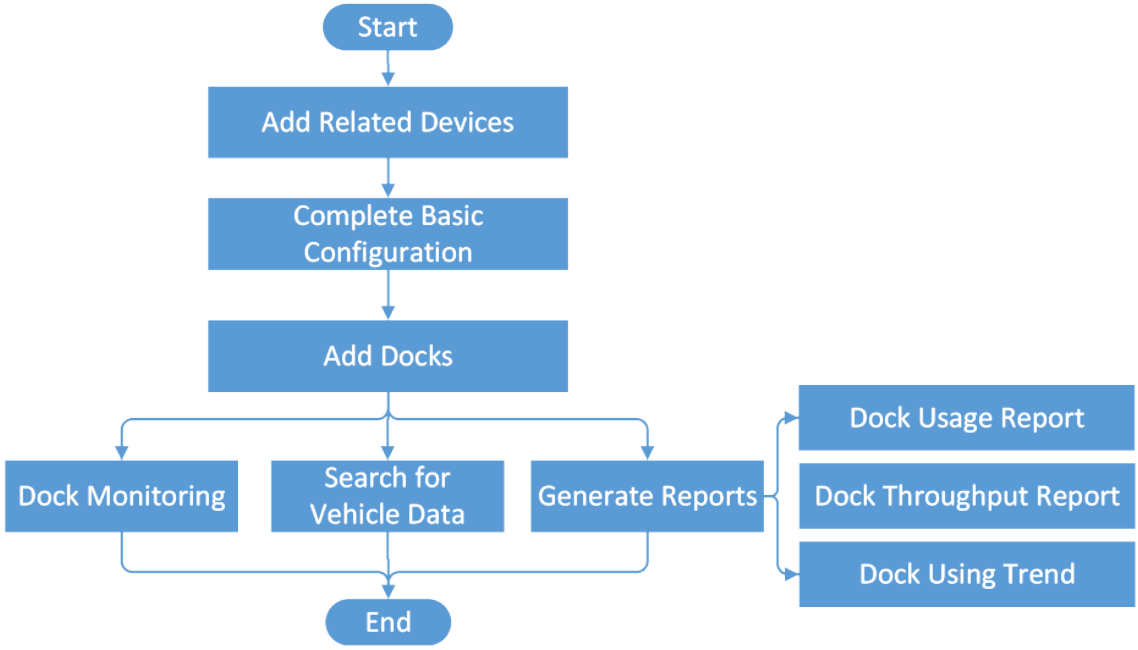


Figure 42-1 Flow Chart of Dock Management

Table 42-1 Flow Chart Description

Step	Description
Add Related Devices	Add devices used for dock monitoring. See ***Manage Encoding Device*** for details.
Complete Basic Configuration	You can configure the basic parameters for dock management. See ***Basic Configuration*** for details.
Add Docks	Add dock areas, add docks, and link docks with cameras. See ***Add Dock Area and Docks*** for details.

Step	Description
Dock Monitoring	You can view all the added dock areas and the details of each dock, and watch the live and recorded videos streamed from linked cameras. See ***Dock Monitoring*** for details.
Search for Vehicle Data	You can search for vehicle data and export the matched records to the local PC. See ***Search for Vehicle Data*** for details.
Generate Reports	You can view reports on dock usage, dock throughput, and dock using trend. See ***Generate Dock Usage Report*** , ***Generate Dock Throughput Report*** , and ***Generate Dock Using Trend Report*** for details.

42.2 Dashboard of Dock Management

The dashboard displays the total number of dock areas and the number of occupied/vacant docks. Also, it provides visualized dock operation statistics and charts on dock using trend, dock throughput, and dock usage.

On the top navigation bar, go to → **Industrial Application → Dock Management → Dashboard** and select an area from the drop-down list in the upper-right corner.

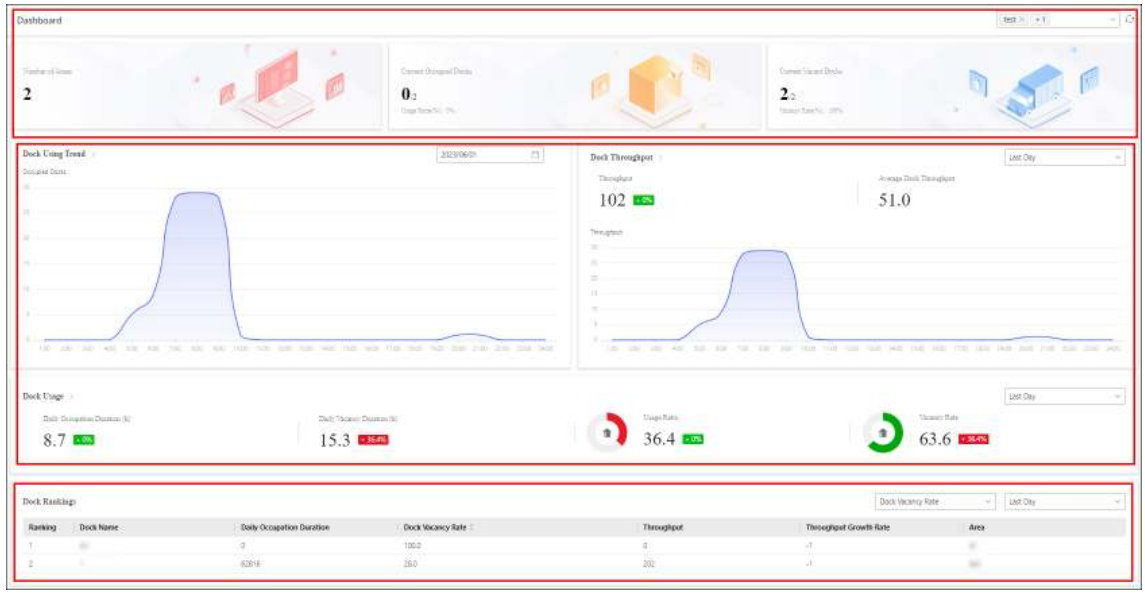


Figure 42-2 Dashboard of Dock Management

1	You can view the total number of dock areas, the number of occupied docks, and the number of vacant docks in the selected area.
2	You can view the charts on dock using trend, dock throughput, and dock usage in the selected area. You can select the time range in the upper-right corner of each chart. You can click **Dock Using Trend**, **Dock Throughput**, and **Dock Usage** to jump to the corresponding pages. See ***Generate Dock Using Trend Report*** , ***Generate Dock Throughput Report*** , and ***Generate Dock Usage Report*** for details. You can hover over the charts of dock using trend and dock throughput to view the detailed statistics of a specific time point.
3	You can select **Dock Vacancy Rate**, **Throughput**, or **Daily Occupation Duration** and a time period in the upper-right corner to view the dock ranking statistics.

42.3 Basic Configuration

You can configure the basic parameters for the dock management module, including the dock data retention time.

On the top navigation bar, go to → **Industrial Application** → **Dock Management** → **Basic Configuration** , set the following parameter(s), and click **Save**.

Dock Data

Specify the retention period of dock data.

42.4 Add Dock Area and Docks

As the Administrator, you can add dock areas and upload their maps to the platform, then add docks to the maps and link cameras with docks for dock monitoring. For non-administrator, you can view dock areas that you have permission to control and edit docks at the dock areas.

Steps

Note

For

1. On the top navigation bar, go to → **Industrial Application** → **Dock Management** → **Dock Management** .
2. Click **Add Area** in the upper-right corner.
3. Enter the dock area name and the total number of docks, and click **Add**.

4. Click **Add Map** and select a map from your local PC.
5. Add and edit docks on the map.

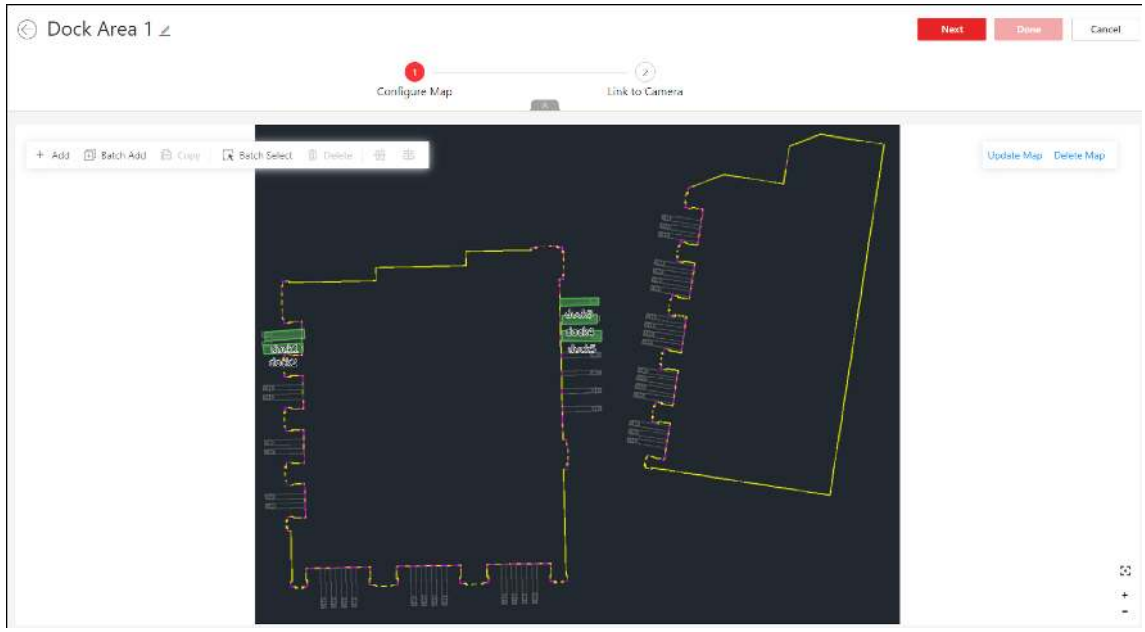


Figure 42-3 Add and Edit Docks on Map

Add Docks	Click **Add**, move your cursor to the map and click to enter the dock No., and click **Save**. Click **Batch Add**, move your cursor to the map and click twice to specify the start dock and end dock respectively, enter the number of docks and the start dock No., and click **Save**.
Copy Docks	Select an added dock on the map and click **Copy**, enter a dock No. for the new dock, and click **Save**.
Delete Docks	Click an added dock and click to delete it from the map. Click **Batch Select**, draw a rectangle on the map to select multiple docks, and click **Delete** to batch delete them.
Align Docks	Click **Batch Select**, draw a rectangle on the map to select multiple docks, and click / to align docks.

6. Click **Next** in the upper-right corner.
7. Link docks with cameras.
   1) Click an added dock on the map.
   2) Select camera(s) for the dock.

Note

- A dock specified camera can be used to both detect the status (vacant/occupied) of the dock and check the loading ratio of the vehicle if its installation location allows. If not, you can add another dock specified camera (indoor) to check the loading ratio.
- A dock specified camera can be linked with up to 2 docks. You need to switch the dock type for the camera on the remote configuration page of the device first. For details, refer to the user manual of the device.

8. Click **Done** in the upper-right corner.
9. **Optional:** Perform further operations.

Edit Dock Area Name and Number of Docks	Hover over an added dock area and click .
Delete Dock Area	Hover over an added dock area and click .
Edit Dock Area	Click the name of an added dock area to edit it.

42.5 Dock Monitoring

You can view all the added dock areas and corresponding docks in each area. The platform allows you to view the details of each dock and watch the live and recorded videos streamed from linked cameras.

Note

Make sure you have added dock areas and docks. See details in ***Add Dock Area and Docks*** .

On the top navigation bar, go to → **Industrial Application** → **Dock Management** → **Dock Monitoring** and select a dock area to view its details.

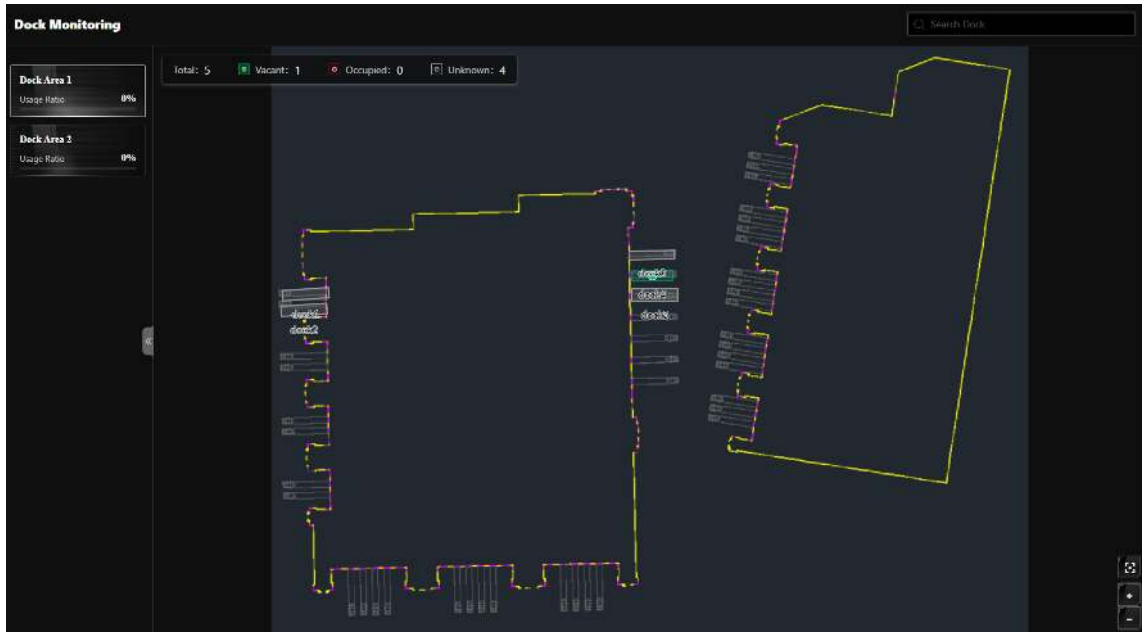


Figure 42-4 Dock Monitoring

At the top, you can view the total number of docks and the numbers of docks in different status (vacant, occupied, and unknown) in the selected dock area.

For each dock on the map, you can click its icon to view its details, including the dock No. and status. If the dock is linked with cameras, you can click → / to start live view or playback.

42.6 Search for Vehicle Data

You can set conditions to search for vehicle data and export the matched records to the local PC.

On the top navigation bar, go to → **Industrial Application** → **Dock Management** → **Search Vehicle Data** , set the search conditions, including the time, license plate No., and dock, and click **Search**.

You can perform further operations.

Table 42-2 Further Operations

Customize Columns to Be Displayed	Click in the upper-right corner to customize the columns to be displayed.
Export Records	Click **Export** in the upper-left corner to export the matched records to the local PC.

42.7 View Dock Statistics

The platform allows you to generate reports by specifying time range and conditions to check whether the business runs smoothly and effectively. You can view reports on dock usage, dock throughput, and dock using trend.

42.7.1 Generate Dock Usage Report

You can specify the dock area, report type, and time range to view the dock usage statistics in doughnut charts.

Steps

1. On the top navigation bar, go to → **Industrial Application → Dock Management → Statistics and Reports → Dock Usage** .
2. Specify the dock area, report type, and time.
3. Click **Generate Report**.
4. **Optional:** Perform further operations.

View Details	Hover over a ring to view the occupation/vacant duration of the dock.
Hide/Display Statistics	Click **Occupation Duration** / **Vacant Duration** to hide corresponding statistics and click again to display.
Export Report	Click **Export** in the upper-right corner, and set the report title and format to export it to the local PC.

42.7.2 Generate Dock Throughput Report

You can specify the dock area, report type, and time range to view the dock throughput statistics in bar charts.

Steps

1. On the top navigation bar, go to → **Industrial Application → Dock Management → Statistics and Reports → Dock Throughput** .
2. Specify the dock area, report type, and time.
3. Click **Generate Report**.
4. **Optional:** Perform further operations.

View Details	Hover over a column to view the number of vehicles in the dock.
Export Report	Click **Export** in the upper-right corner, and set the report title and format to export it to the local PC.

42.7.3 Generate Dock Using Trend Report

You can specify the dock area, report type, and time range to view the dock using trend in line charts.

Steps

1. On the top navigation bar, go to → **Industrial Application** → **Dock Management** → **Statistics and Reports** → **Dock Using Trend** .
2. Specify the dock area, report type, and time.
3. Click **Generate Report**.
4. **Optional:** Perform further operations.

View Details	Hover over the line to view the number of occupied docks at a specific time point.
Export Report	Click **Export** in the upper-right corner, and set the report title and format to export it to the local PC.

Chapter 43 Parcel Tracking

The platform allows you to add and manage check points for parcel tracking by specifying the data source at each check point and linking cameras to each check point. You can search for the barcode scanning records of each check point and view related pictures/videos to look for parcels.

43.1 Flow Chart

The flow chart below shows the overall process of parcel tracking.



Figure 43-1 Flow Chart of Parcel Tracking

Table 43-1 Flow Chart Description

Step	Description
Add Scanning Devices	Add devices for scanning barcodes on parcels. For details, see ***Manage Scanning Device*** .
Manage Scanning Resources	Add channels of scanning devices to the corresponding areas and configure the picture storage location for each scanning channel.

Step	Description
Complete Basic Configuration	Configure the basic parameters. For details, see ***Basic Configuration*** .
Manage Check Points	Add check points by specifying the data sources and linking cameras. For details, see ***Add a Check Point*** .
Search for Scanning Records	Search for parcel scanning records and download the records to the local PC. For details, see ***Search for Scanning Records*** .

43.2 Basic Configuration

You can configure the basic parameters for the parcel tracking module, such as the recording start/end time of each scan, the time threshold of exception, and the retention period of scanning records.

On the top navigation bar, select → **Industrial Application** → **Check Point Management** → **Basic Configuration** , set the following parameters, and click **Save**.

Recording Time Settings

Stop Code

Switch it on so that the related video of a scan will stop at the time when the barcode displayed on the page is scanned. The recording start time will be set to 10 seconds before the scan of the first parcel in a batch.

You can click **Download** to download the barcode to the local PC.

Start Time / End Time

Set the start time and end time respectively to specify the time range of the related video of each scan.

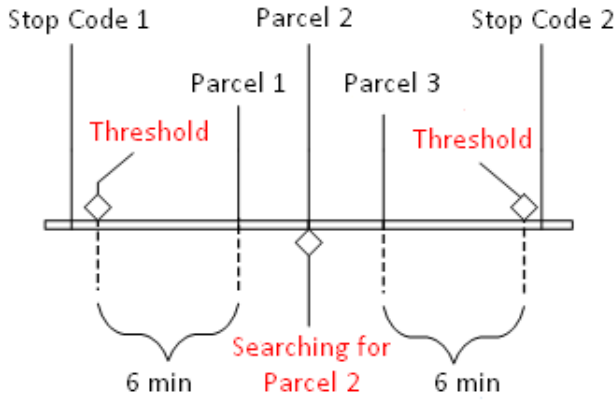
Note

- The parameters are displayed only when **Stop Code** is switched off.
- You can also configure these parameters for each individual check point. The individually configured rules have higher priority than the generic settings configured here. See ***Add a Check Point*** for details.

Exception Time

Time Threshold of Exception

Refer to the following diagrams for explanation about how the time range of the related video of each scan will be effected by the time threshold you configured here.

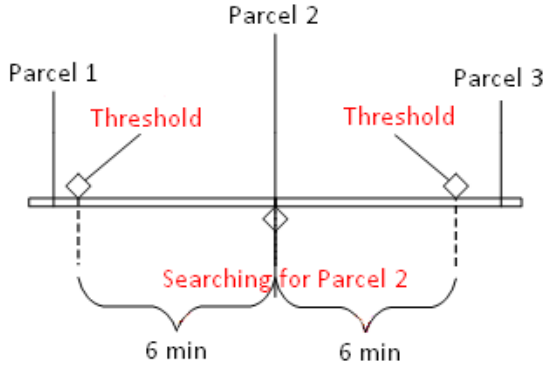


Condition:
1) Stop Code: Enabled
2) Time Threshold: 6 min

Outcome:
Recording Start Time: 6 min before the scan of parcel 1

Recording End Time: 6 min after the scan of parcel 3

Figure 43-2 Searching for Parcel 2 (Stop Code Enabled)



Condition:
1) Stop Code: Disabled
2) Start Time: Previous Scanning Time
3) End Time: Next Scanning Time
4) Time Threshold: 6 min

Outcome:
Recording Start Time: 6 min before the scan of parcel 2

Recording End Time: 6 min after the scan of parcel 2

Figure 43-3 Searching for Parcel 2 (Stop Code Disabled)

Data Retention Period

Scanning Record Data

Specify a retention period for the scanning records.

43.3 Add a Check Point

You can add a check point to the platform by specifying its data source and linking cameras to it.

Before You Start

Make sure you have added the related scanning devices to the platform. See ***Manage Scanning Device*** .

Steps

1. On the top navigation bar, select → **Industrial Application** → **Check Point Management** .
2. On the left navigation pane, select **Check Point Management**.

3. Select an area from the area list.
4. Click **Add** to enter the check point adding page.
5. Create a descriptive name for the check point.
6. **Optional:** Select a check point type from the drop-down list and enter any comments you have for the check point.
7. Select a channel of an added scanning device as the data source for this check point.
8. **Optional:** Switch **Recording Time Settings** to specify the time range of the related video of each scan by setting the recording start and end time respectively.

Note

The settings configured here have higher priority than the generic settings you have configured for all check points on the Basic Configuration page of the module.

9. Select available camera(s) to link to the check point for recording videos.
10. Click **Add** to finish adding the check point or click **Add and Continue** to add another check point.
11. **Optional:** Perform the following operations.

Edit Check Point	Click the name of a check point or in the Operation column of a check point to enter its details page and edit its information.
Delete Check Point(s)	• Click in the Operation column of a check point to delete it. • Select one or multiple check points and click **Delete** to delete the selected check point(s).
	Note The scanning records of a check point will be kept even after the check point is deleted.
Search for Check Points	Enter a keyword in the search box to search for matching check points by name. Supports fuzzy search.
Add to Favorites	• Click ☆ in the Operation column of a check point to add it to Favorites. • Select one or multiple check points and click **Add to Favorites** to add the selected check point(s) to Favorites.
	Note If being added to Favorites, the check points can be quickly filtered during scanning record search.
Remove from Favorites	• Click in the Operation column of a check point to remove it from Favorites. • Select one or multiple check points and click **Remove from Favorites** to remove the selected check point(s) from Favorites.

43.4 Search for Scanning Records

You can search for scanning records to view the scan details and download them to your local PC.

Steps

1. On the top navigation bar, select → **Industrial Application** → **Check Point Management** .
2. On the left navigation pane, select **Scanning Record**.
3. Specify the time period.
4. **Optional:** Enter a specific barcode and/or specify the check point(s) to be searched from.

   Note

   When selecting check points, if you have added check points to Favorites before, you can click to quickly select those check points in one click.
5. Click **Search**.

   The scanning records that match the search conditions will show in the list.
6. **Optional:** Click a barcode to view the scan details, such as the related picture/video.

   Note

   On the scan details pane, you can click **Search** next to the barcode to search for scanning records of this barcode specifically.
7. **Optional:** Select one or up to 20 results and click **Download** to download the selected scanning record(s) and/or the corresponding pictures/videos to the local PC in the format you select.

Chapter 44 Canteen Consumption

Designed for canteen payment, the module provides canteen management functions such as merchant management, payment rule configuration, permission configuration, and account management, and operation management functions such as account top-up, transaction search, and statistics and reports.

44.1 Flow Chart

The following flow chart shows the process of the configurations and operations of canteen consumption module.

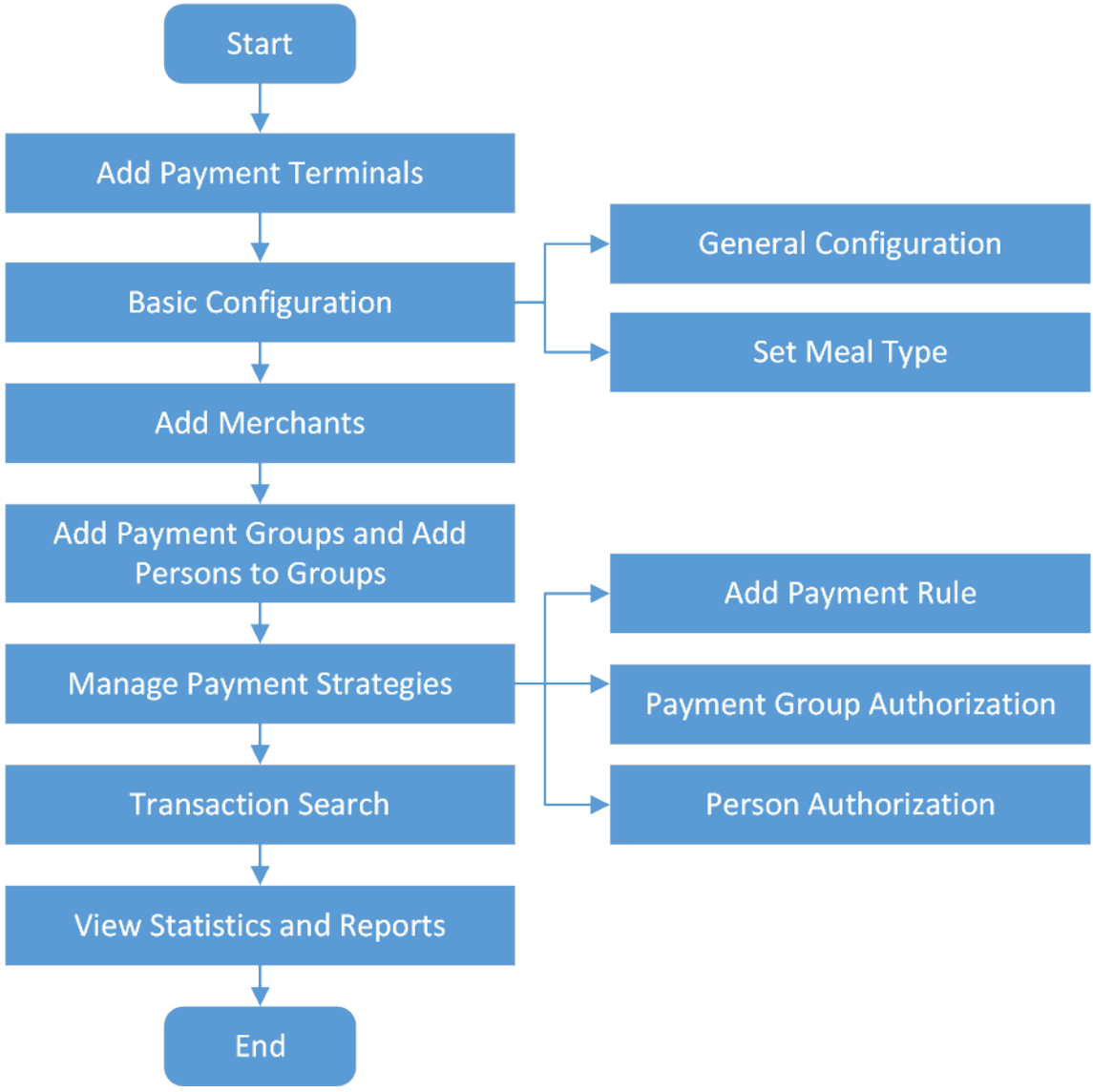


Figure 44-1 Flow Chart of Canteen Consumption

- Add Payment Terminals: at first, you should add payment terminals to the platform. See ***Manage Payment Terminal*** .
- Basic Configuration: you should configure basic parameters. See ***Basic Configuration*** .
- Manage Payment Groups: you should add payment groups and add persons to payment groups. See ***Add a Payment Group*** and ***Add Persons to Payment Group*** .
- Add Merchants: you should add merchants and link payment terminals to merchants. See ***Merchant Management*** .
- Manage Payment Strategies: you should add payment rules and authorize payment groups and/or persons. See ***Add Payment Rule*** , ***Payment Group Authorization*** , and ***Person Authorization*** .

- Transaction Search: you can search for transactions. See ***Transaction Search*** .
- View Statistics and Reports: you can view group payment statistics, person payment statistics, revenue report of merchants, and device payment statistics. See ***Statistics and Reports*** .

44.2 Payment Overview

On the Payment Overview page, you can go to different pages quickly and view payment statistics today.

In the top left corner of Home page, select → **Integrated Service** → **Canteen Consumption** → **Payment Overview** to enter the Payment Overview page.

You can perform the following operations.

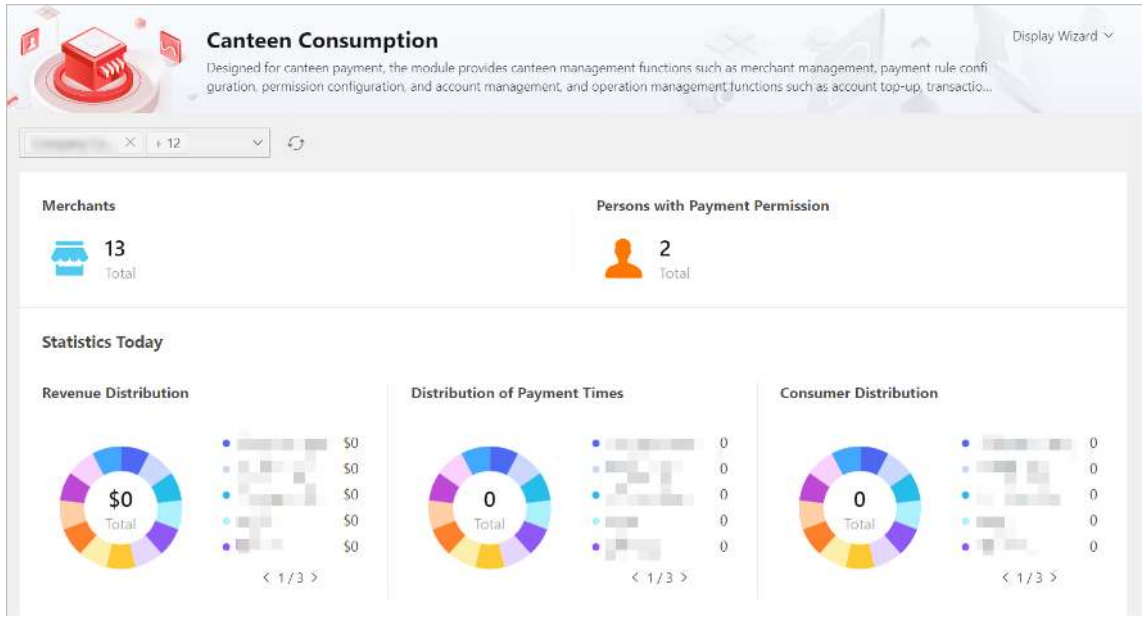


Figure 44-2 Payment Overview

Operation	Description
Display Wizard	Click **Display Wizard** / **Hide Wizard** to display or hide the wizard where you can redirect the page to another link.
Select Canteen	Click to select the canteen(s) whose information will be displayed on the page.
View Statistics	You can view the number of merchants and persons with the payment permission.

Operation	Description
	In the Statistics Today section, you can view statistics of selected canteens. You can click the colored dots near a pie chart, so the corresponding index will not be displayed in the pie chart. Click again to display it again.

44.3 Basic Configuration

In the Basic Configuration section, you can set general configurations (such as currency unit, auto apply, auto calculation) and meal settings (such as meal type).

44.3.1 General Configuration

You can set general configurations such as currency unit, whether to automatically apply payment permissions, whether to automatically calculate payment.

In the top left corner of Home page, select → **Integrated Service → Canteen Consumption → Basic Configuration → General Configuration** to enter the General Configuration page.

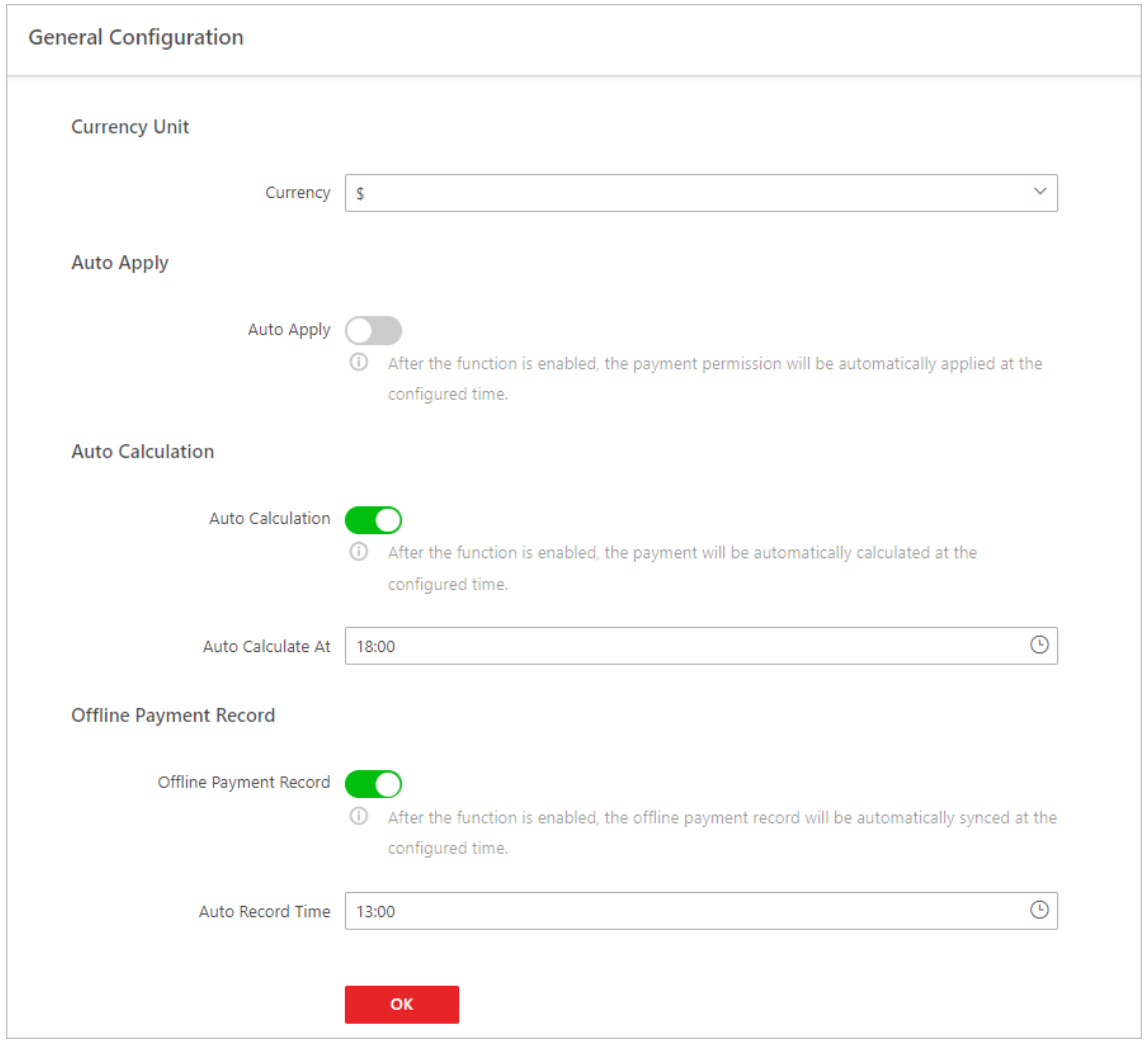


Figure 44-3 General Configuration

Currency Unit

Select a currency unit.

Auto Apply

After the function is enabled, the payment permission will be automatically applied at the configured time.

Auto Calculation

After the function is enabled, the payment will be automatically calculated at the configured time.

Offline Payment Record

After the function is enabled, the offline payment record will be automatically synced at the configured time.

44.3.2 Meal Settings

You can add and manage the meal types including adding meal types, editing meal type information, and deleting the added meal types.

Steps

1. In the top left corner of the client, select → **Integrated Service** → **Canteen Consumption** → **Basic Configuration** → **Meal Settings** .
2. Click **Add** to open the adding meal type pane.
3. Specify the meal type name and the time period, and enter the note if needed.

Note

The platform supports setting meal periods as cross-day periods which are within 24 hours.

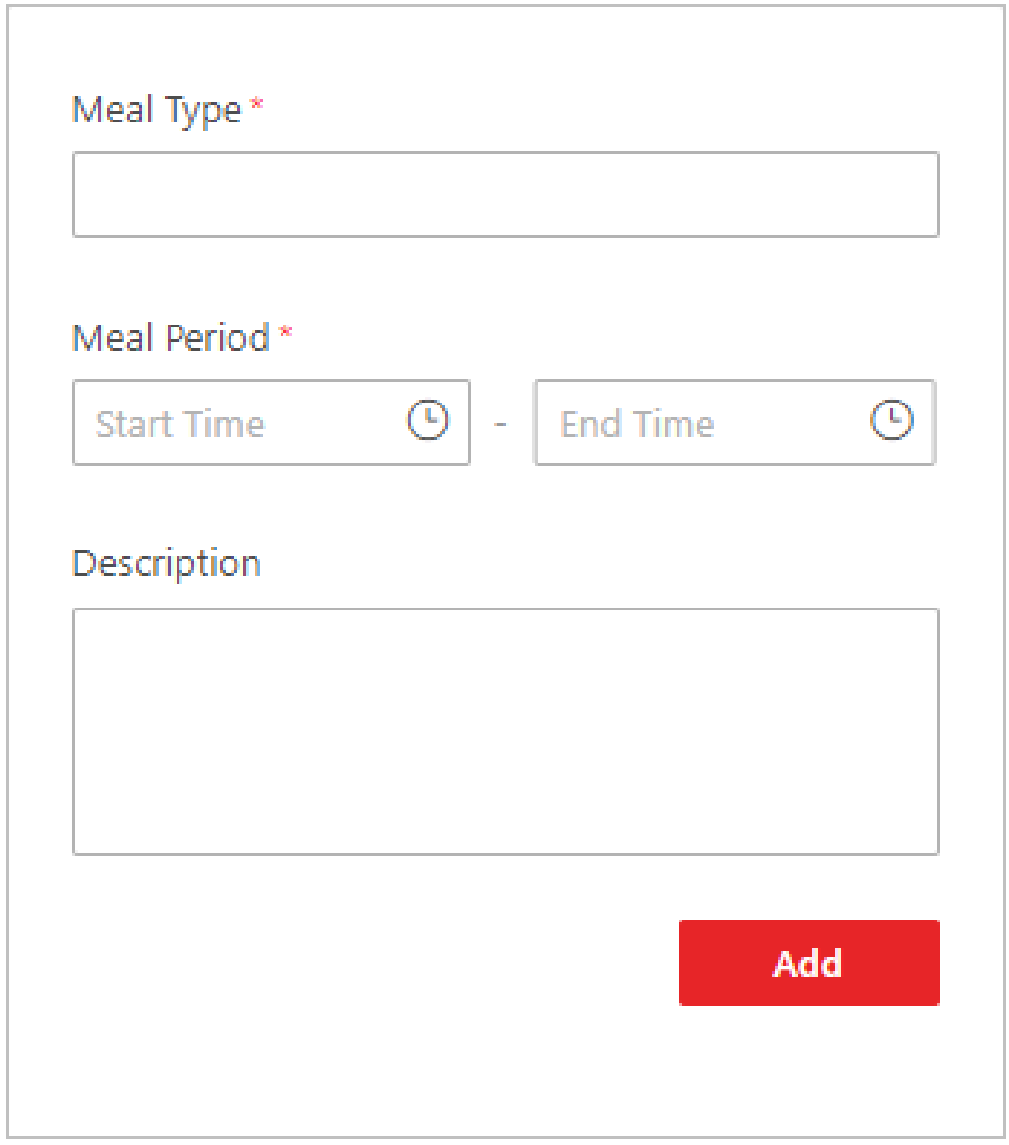


Figure 44-4 Set Meal Type

4. Click **Add** in the pane to add the new meal type to the list.

Note

No more than 8 meal types can be added and there should be no clash between slots.

5. You can perform the following operations.

Edit Meal Type	Click in the Operation column of a meal type to edit the information.
Delete Meal Type	Click in the Operation column to delete the meal type.

Note

The default meal types (Breakfast, Lunch, Dinner, and Late Snack) cannot be deleted.

44.4 Merchant Management

The platform supports managing merchants of different levels. You can add different merchants to the platform and link consumption devices to them.

Steps

1. In the top left corner of Home page, select → **Integrated Service** → **Canteen Consumption** → **Merchant Management** .
2. Click + on the top of the left pane, or select an existing merchant and then click + .
3. Enter the basic information about the merchant, including name, upper-level merchant, address, etc.
4. In the Payment Terminal area, check payment terminal(s) and click › .

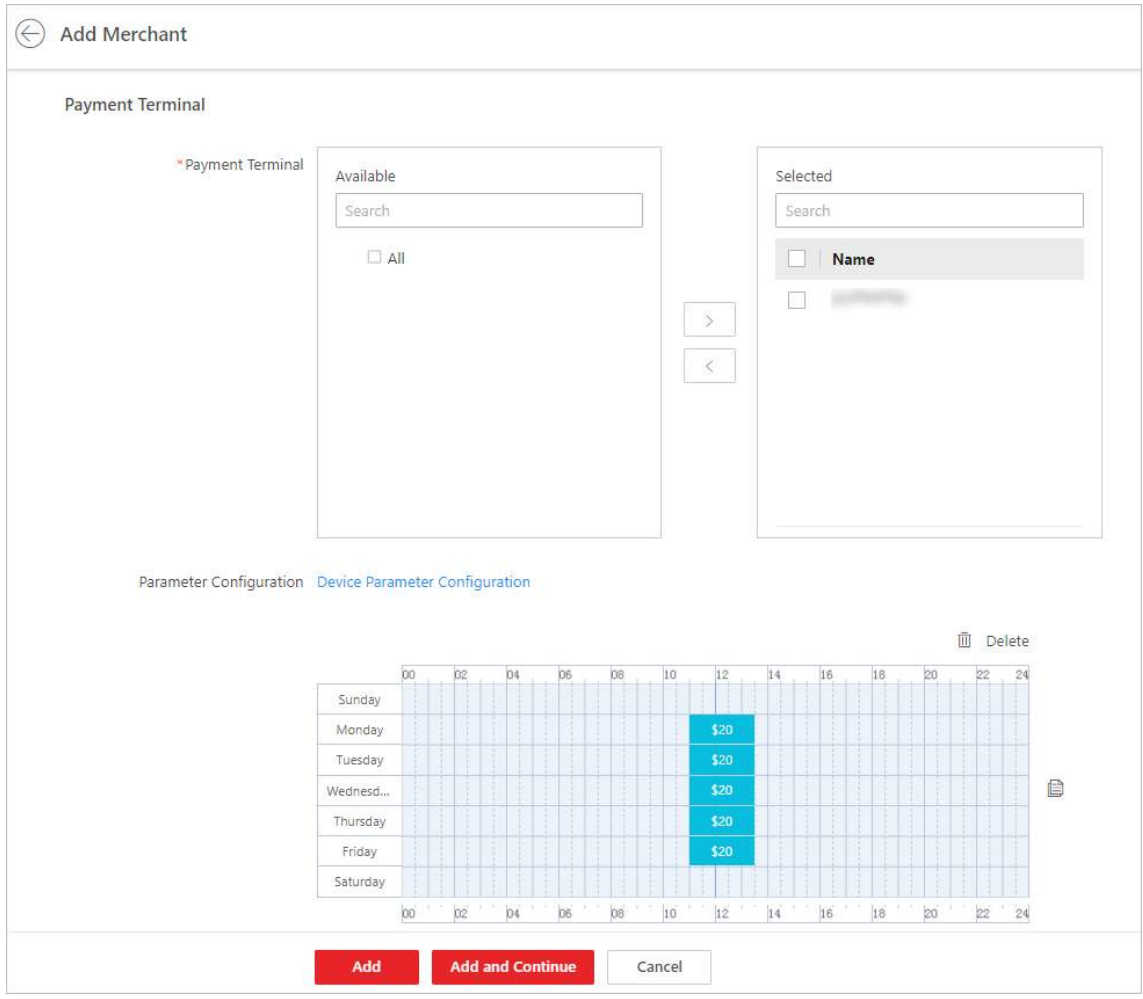


Figure 44-5 Link Terminal

5. **Optional:** Click **Device Parameter Configuration**.
   1) Select a payment day from the drop-down list.
   2) Select a meal type.
   3) Select a payment mode.

      Amount

      Set maximum single-payment amount to define the threshold of a single payment.

      Fixed Amount

      A fixed amount will be charged when a person pays.

      Payment Times

      The platform charges according to the payment times of a person. For example, you can set maximum payment times for different meal types of a factory. Workers at the factory can verify for a meal type no more than the threshold of payment times.
   4) Click **OK**.

The set parameters will be displayed on the graph.

6. **Optional:** Set the payment rule in non-meal period as **Amount**, **Fixed Amount**, or **Payment Times**.
7. Click **Add** to add the merchant and go back to the merchant list page; or click **Add and Continue** to add the current merchant and continue to add a new merchant.
8. **Optional:** Perform the following operations.

Edit a Merchant	Select a merchant on the left, and then click in the upper right corner to edit its information.
Clear Payment Terminals Linked to a Merchant	Select a merchant on the left, and then click **Clear** on the right to clear all consumption devices linked to the merchant.
Unlink a Consumption Device from a Merchant	Select a merchant on the left to show the linked consumption devices. Click to unlink the device from the merchant.

44.5 Payment Group Management

You can add, edit, and delete payment groups. After that, you can add persons to payment groups, so you can batch give allowances to persons in a payment group, top up money for them, etc.

44.5.1 Add a Payment Group

You can add, edit, and delete payment groups, and set scheduled allowance for a payment group.

Steps

1. In the top left corner of the client, select → **Integrated Service** → **Canteen Consumption** → **Payment Group Management** .
2. Click + on the top left pane.
3. Set the payment group name and click **Save**.
4. You can perform the following operations.

Edit Payment Group	Click a payment group, and click on the top of the left pane to edit the group name.
Delete Payment Group	Click a payment group, and click on the top of the left pane to delete the group name. Click → **Delete (All)** to delete all payment groups.
Set Scheduled Allowance for Payment Group	Check person(s), click on the top of the left pane. a. Select a payment group. b. Select allowance date. c. Set the allowance time. d. Set the allowance amount and/or the allowance times. e. Click **Save**.

Note

If you set scheduled allowances for a payment group, and also set allowances for persons from the group, only the later one will take effect.

What to do next

You can add persons to a person group. See ***Add Persons to Payment Group*** .

44.5.2 Add Persons to Payment Group

You can add persons to a payment group, so you can batch give allowance, give scheduled allowance, etc. to persons in the payment group.

Before You Start

Make sure you have added a payment group. For details, refer to ***Add a Payment Group*** .

Steps

1. In the top left corner of the client, select → **Integrated Service** → **Canteen Consumption** → **Payment Group Management** .
2. Click a payment group on the left pane.
3. On the top of the right pane, click **Add**, select a department, and check person(s) to add person(s) to the group.

   The person(s) will be displayed in the list.

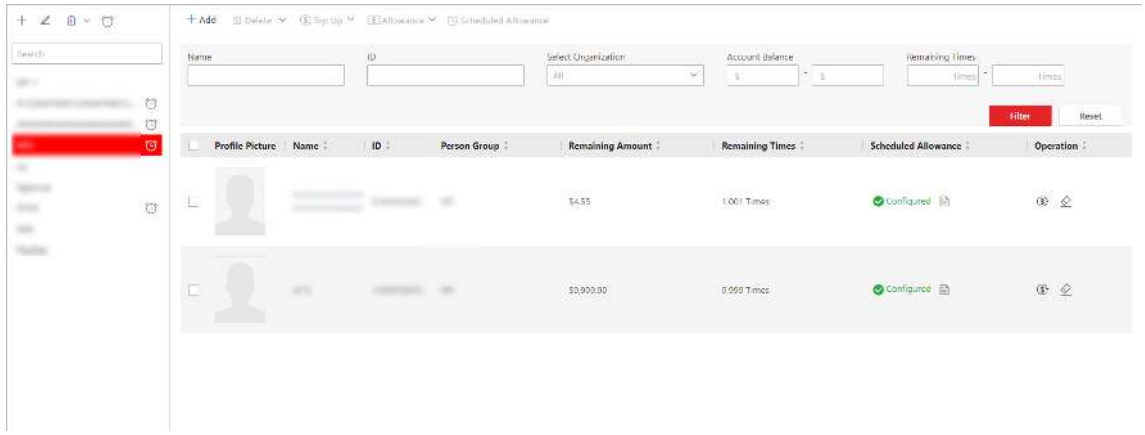


Figure 44-6 Add Persons to Payment Group

4. **Optional:** You can perform the following operations.

Top up for Person(s)	Check person(s), click **Top Up** on the top of the pane, and enter amount and/or times to top up money for the selected person(s). Click **Top Up** → **Top Up (All)** to top up money for all persons.

Give Allowance to Person(s) Immediately	Check person(s), click **Allowance** on the top of the pane, and enter amount and/or times to give allowance to the selected person(s) immediately. Click **Allowance** → **Allowance (All)** to give allowance to all persons. **Note** If you set scheduled allowances for a payment group, and also set allowances for persons from the group, only the later one will take effect.
Set Scheduled Allowance for Person(s)	Check person(s), click **Scheduled Allowance** on the top of the pane. a. Select allowance date. b. Set the allowance time. c. Set the allowance amount and/or the allowance times. d. Click **Save**. **Note** If you set scheduled allowances for a payment group, and also set allowances for persons from the group, only the later one will take effect.
Refund Money	Click in the Operation column of a person and specify the amount and/or times to refund money. You can click **Refund All** in the pop-up window to refund all money of the person.
Search Payment Records	Click in the Operation column of a person and specify the time range to search for a payment record.
Correct Payment Records	Click to go to the search records page, and click in the Operation column of a record to correct the record.
Filter Persons	Specify conditions such as name and ID, and click **Search** to filter persons.
Delete Person(s)	Check person(s), click **Delete** on the top of the pane to delete the selected person(s). Click **Delete** → **Delete All** to delete all persons.

44.6 Payment Strategy Management

You can add payment rules, authorize payment permissions to payment groups and persons, and apply permissions to payment terminals linked to related merchants.

44.6.1 Add Payment Rule

A payment rule defines the meal type, payment amount, and payment times the persons or payment groups can consume.

Steps

1. In the top left corner of Home page, select → **Integrated Service** → **Canteen Consumption** .
2. Select **Payment Strategy Management** → **Payment Rule** on the left.
3. Click **Add** to open the Add Payment Rule page.
4. Enter the rule name.
5. **Optional:** In the Copy From drop-down list, select a payment rule to copy.
6. **Optional:** Set the payment limit.

   Meal Type

   Meal types such as breakfast and lunch are listed by default according to Meal Settings. For details, see ***Meal Settings*** .

   Note

   A default payment rule named Unlimited Payment Rule is provided.

   Max. Total Payment Amount

   It indicates a threshold of payment amount for different meal types.

   Max. Payment Times per Person

   It indicates a threshold of payment times for different meal types.

   Note

   - You can click **Add** to add more payment limits.
   - You can click to delete the payment limit.
7. **Optional:** Switch on **Allow Payment in Non-Meal Period**, and set **Max. Total Payment Amount** and **Max. Payment Times per Person** accordingly.
8. Click **Add** to add the payment rule and go back to the payment rule list; or click **Add and Continue** to add the payment rule and continue to add a new one.
9. **Optional:** After adding the payment rule, perform the following operations.

Edit Payment Rule	Click in the Operation column to edit the payment rule.
Delete Payment Rule	Select one or multiple payment rules and click **Delete** to delete the selected payment rules. Or click → **Delete All** to delete all payment rules exclude the default payment rule.
Search for Payment Rule	Enter the rule name and click to search for payment rules.

44.6.2 Payment Group Authorization

You can assign payment groups the consumption permissions which specify during which time period(s) the payment group(s) can consume from which merchant(s).

Before You Start

Make sure you have added payment groups, merchants, and payment rules to the platform. For details, see ***Payment Group Management*** , ***Merchant Management*** , and ***Add Payment Rule*** .

Steps

1. In the top left corner of Home page, select → **Integrated Service → Canteen Consumption** .
2. Select **Payment Strategy Management → Payment Group Authorization** on the left.

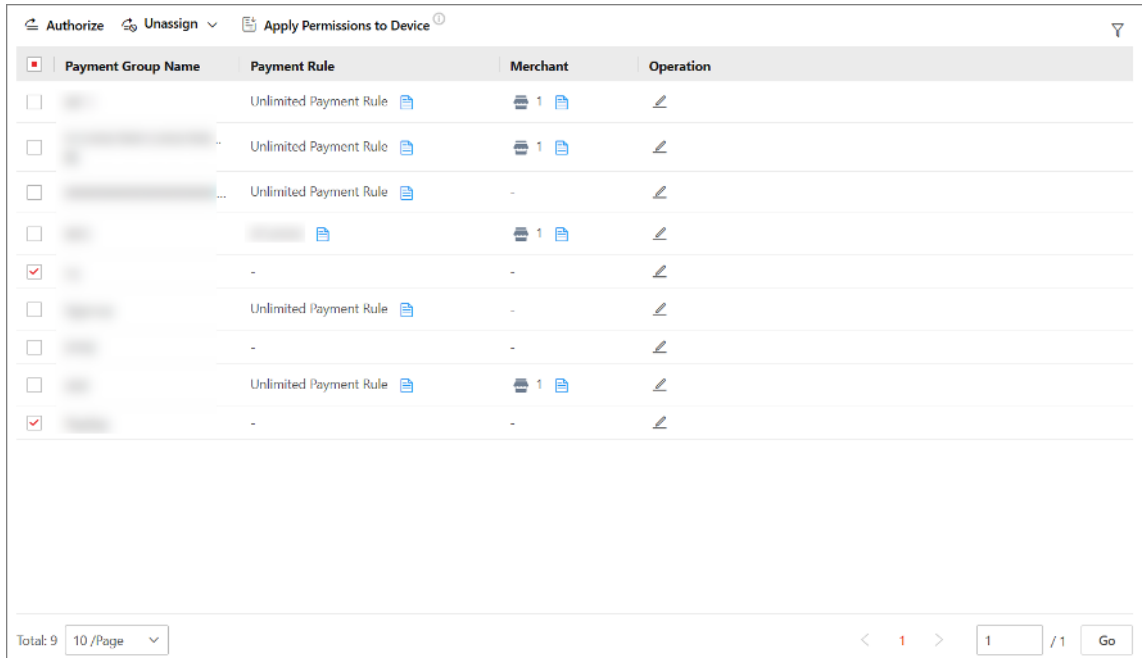


Figure 44-7 Payment Group Authorization

3. Select one or multiple payment groups and click **Authorize**.
4. Select the payment rule and merchant.

Note

- You can check **Include Sub-Merchants**, then the sub-merchants of the selected merchants will also be selected.
- You can also enter the keywords and click to search for merchants.

5. Click **OK**.

   The authorized payment permissions will be applied to devices linked to the selected merchants automatically.
6. **Optional:** If you need to apply permissions to devices manually, perform the following operations.

1) Click **Apply Permission to Device** to open the Apply Permissions to Device page.
2) Select person(s) to be applied.
3) **Optional:** Switch on **Specify Merchant** and select the merchant(s).
4) **Optional:** Check **Apply (Initial)** to apply permissions of all persons after clearing all previous payment permissions.
5) Click **OK**.

7. **Optional:** Perform more operations after assigning permissions.

Edit Permissions	Select a payment group, and click in the operation column to edit the consumption permissions.
Unassign Authorization	Select one or multiple payment groups, click **Unassign → Cancel Partial Authorization** , and select authorizations to be canceled. Select a payment group, and click **Unassign → Cancel All Authorizations** to clear all authorizations of the selected payment group(s).
Filter Authorizations	Click in the upper right corner, and set conditions to filter consumption authorizations.
View Details	Select a payment group, click to view the details of merchant(s) and the payment rule.

44.6.3 Person Authorization

You can assign specific persons the consumption permissions which specify during which time period(s) the person(s) can consume from which merchant(s).

Before You Start

Make sure you have added persons to payment groups, added merchants and link consumption devices, and payment rules to the platform. For details, see ***Add Persons to Payment Group*** .

Steps

1. In the top left corner of Home page, select → **Integrated Service → Canteen Consumption** .
2. Select **Payment Strategy Management → Person Authorization** on the left.

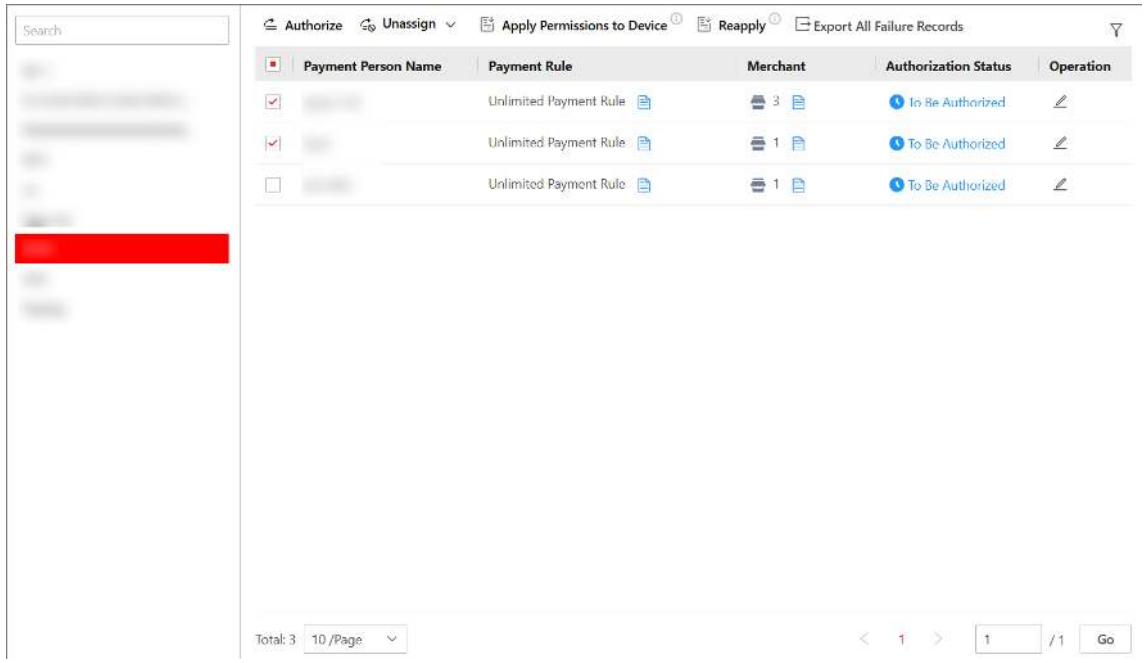


Figure 44-8 Person Authorization

3. Select an payment group on the left.
4. Select one or multiple persons and click **Authorize**.
5. Select the payment rule and merchant.

Note

- You can check **Include Sub-Merchants**, then the sub-merchants of the selected merchants will also be selected.
- You can enter the keywords and click to search for merchants.

6. Click **OK**.

   The authorized payment permissions will be applied to consumption devices linked to the selected merchants automatically.
7. **Optional:** If you need to apply permissions to devices manually, perform the following operations.
   1) Click **Apply Permission to Device** to open the Apply Permissions to Device page.
   2) Select person(s) to be applied.
   3) **Optional:** Switch on **Specify Merchant** and select the merchant(s).
   4) **Optional:** Check **Apply (Initial)** to apply permissions of all persons after clearing all previous payment permissions.
   5) Click **OK**.
8. **Optional:** Perform more operations after assigning permissions.

Edit Permissions	Select a person, and click in the operation column to edit the consumption permissions.

Unassign Permissions	Select one or multiple persons, click **Unassign → Cancel Partial Authorization** , and select authorizations to be canceled. Select one or multiple persons, and click **Unassign → Cancel All Authorizations** to clear all authorizations of the selected person(s).
Reapply Permissions	Click **Reapply** to reapply the permissions failed to be applied.
Export All Failure Records	Click **Export All Failure Records** to export all failure records to the local PC.
Filter Permissions	Click in the upper right corner, and set conditions to filter consumption permissions.
View Details	Select a person, click to view the details of merchant(s) and the payment rule. If the authorization status is "applying failed", you can click to view the details.

44.7 Transaction Search

You can search for transaction records such as top-up, allowance, correction, refund, and deduction, and search for payment records of specific persons by conditions such as merchant, payment terminal, and payment time.

44.7.1 Search for Transaction Record

You can search for transaction records by setting conditions and export the search results to the local PC.

Steps

1. In the top left corner of Home page, select → **Integrated Service → Canteen Consumption** .
2. Select **Transaction Search → Transaction Record** on the left.
3. Set the needed conditions, including transaction type, operation time, person, and person group.
4. Click **Search**.

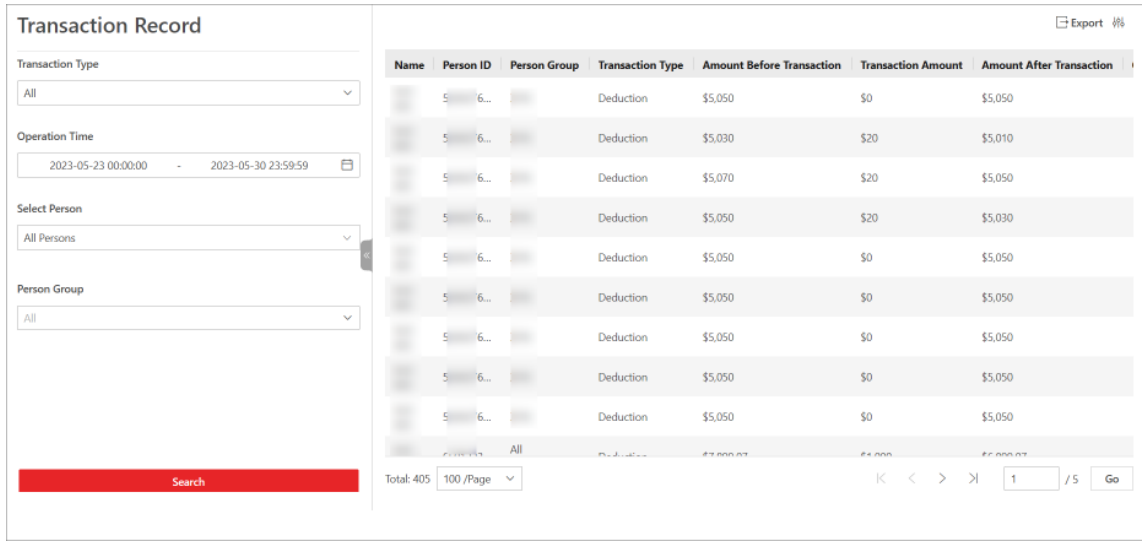


Figure 44-9 Search for Transaction Record

The transaction records that meet the conditions will be displayed on the right side.

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

Export Transaction Records	Click **Export** to export the transaction records.
Custom List Items	Click and select the items to be displayed in the list.

44.7.2 Search for Payment Record

You can set conditions to search for normal and abnormal payment records. Payment records without person information (person name, ID, and person group) are abnormal payment records. Also, abnormal payment records will be generated when a person's payment times for a certain type of meal exceed the configured value, or the payment permission of a person does not match with that configured on the platform.

Steps

1. In the top left corner of Home page, select → **Integrated Service** → **Canteen Consumption** .
2. Select **Transaction Search** → **Payment Record** on the left.
3. Click **Normal Payment Record** or **Abnormal Payment Record** on the top.

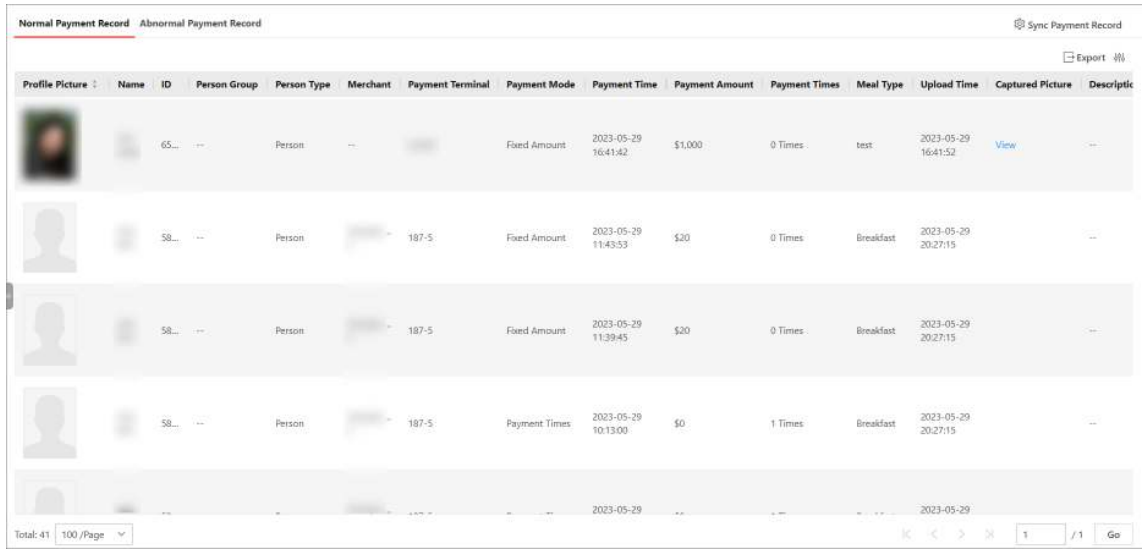


Figure 44-10 Normal Payment Records

4. Set the needed conditions, including merchant, person type, person, payment terminal, etc.
5. Click **Search**.

   The payment records that meet the conditions will be displayed on the right side.
6. **Optional:** Perform the following operations.

View Captured Picture	Click **View** in the Operation column to view the captured picture.
Export Payment Records	Click **Export** to export the payment records.
Custom List Items	Click and select the items to be displayed in the list.
Sync Payment Record	In the Normal Payment Record page, click **Sync Payment Record**, select the payment time and merchant(s), and click **Save** to synchronize payment records from the devices to the platform.

44.8 Statistics and Reports

There are four types of statistics including person payment statistics, group payment statistics, revenue reports of merchant, and device payment statistics. You can customize reports by setting conditions such as report target, meal type, and time. You can also export reports in Excel and PDF format.

44.8.1 Group Payment Statistics

You cam view payment statistics of a specified payment group or specified payment groups.

In the top left corner of Home page, select → **Integrated Service** → **Canteen Consumption** .

Select **Statistics and Reports** → **Payment Group Payment Statistics** on the left.

- Select target payment group(s), meal type, and time to generate statistics.
- Click **Calculate Again** in the upper-right corner, select target payment group(s) and time, and click **OK** to generate statistics.

In group payment statistics, you can view total payment amount, total payment times, total number of consumers in pie charts, and view the table of payment details of the specified payment group(s).

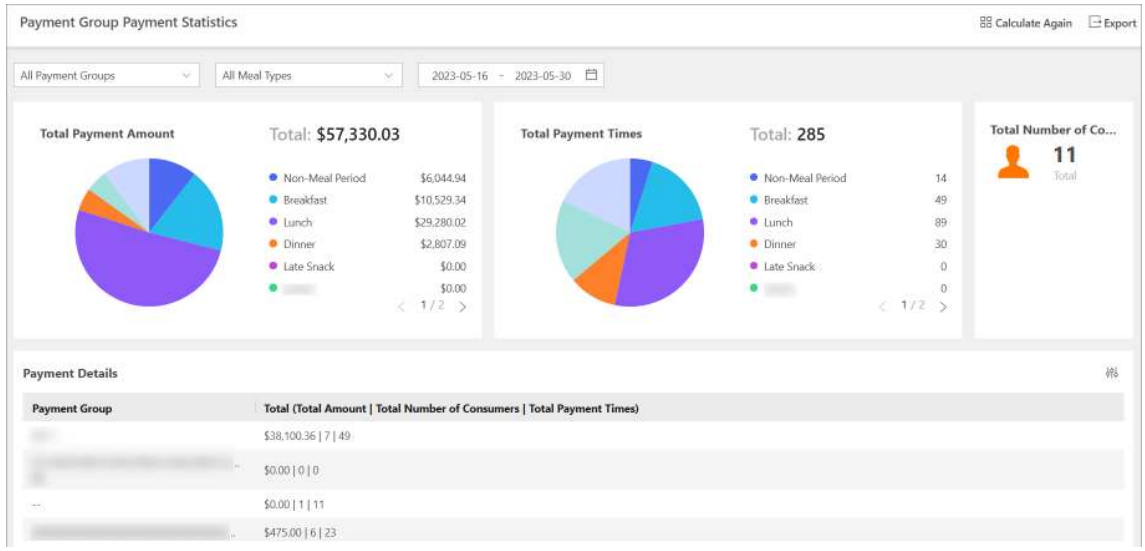


Figure 44-11 Group Payment Statistics

You can move the cursor on a part of the pie chart to view the corresponding meal type and payment amount. You can also click a meal type to cancel displaying it in the pie chart.

You can click to custom the list items to be displayed in the **Payment Details** table.

You can click **Export** to export the statistics in Excel or PDF format.

44.8.2 Person Payment Statistics

You cam view payment statistics of a specified person or specified persons.

In the top left corner of Home page, select → **Integrated Service** → **Canteen Consumption** .

Select **Statistics and Reports** → **Person Payment Statistics** on the left.

- Select target person(s), meal type, and time to generate statistics.
- Click **Calculate Again** in the upper-right corner, select the time period and target person(s), and click **OK** to generate statistics.

In person payment statistics, you can view total payment amount, and total payment times in pie charts, and view the table of payment details of the specified person(s).

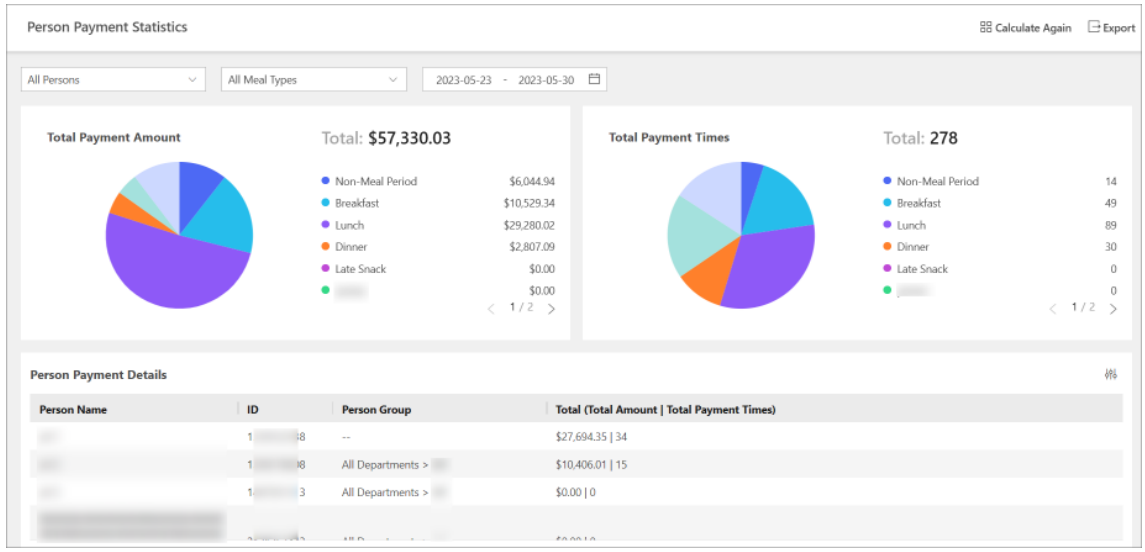


Figure 44-12 Person Payment Statistics

You can move the cursor on a part of the pie chart to view the corresponding meal type and payment amount. You can also click a meal type to cancel displaying it in the pie charts.

You can click to custom the list items to be displayed in the **Payment Details** table.

You can click **Export** to export the statistics in Excel or PDF format.

44.8.3 Revenue Report of Merchant

You cam view daily and monthly revenue reports of a specified merchant or specified merchants.

In the top left corner of Home page, select → **Integrated Service** → **Canteen Consumption** .

Select **Statistics and Reports** → **Revenue Report of Merchant** on the left.

- Select target merchant(s), meal type, and time to generate a report.
- Click **Calculate Again** in the upper-right corner, select the time period and target merchant(s), and click **OK** to generate a report.

In a revenue report of merchant(s), you can view revenue, payment times, number of consumers, and records of payment charged by times in pie charts and trend charts, and view the table daily revenue details of merchants.



Figure 44-13 Daily Revenue Report of Merchant

In a pie chart, you can move the cursor on a part to view the corresponding merchant and revenue, and click a merchant to cancel displaying it.

In a trend chart, you can adjust the time line of the chart to view corresponding trend in the set time period.

You can click to custom the list items to be displayed in the **Daily Revenue Details of Merchants** / **Monthly Revenue Details of Merchants** table.

You can click **Export** to export the report in Excel or PDF format.

44.8.4 Device Payment Statistics

You cam view daily and monthly revenue statistics of a specified device or specified devices.

In the top left corner of Home page, select → **Integrated Service** → **Canteen Consumption** .

Select **Statistics and Reports** → **Device Payment Statistics** on the left.

- Select target device(s), meal type, and time to generate statistics.
- Click **Calculate Again** in the upper-right corner, select the time period and target device(s), and click **OK** to generate statistics.

In device payment statistics, you can view total revenue, total payment times, and total number of consumers in pie charts, and view the table of revenue details of specific devices.

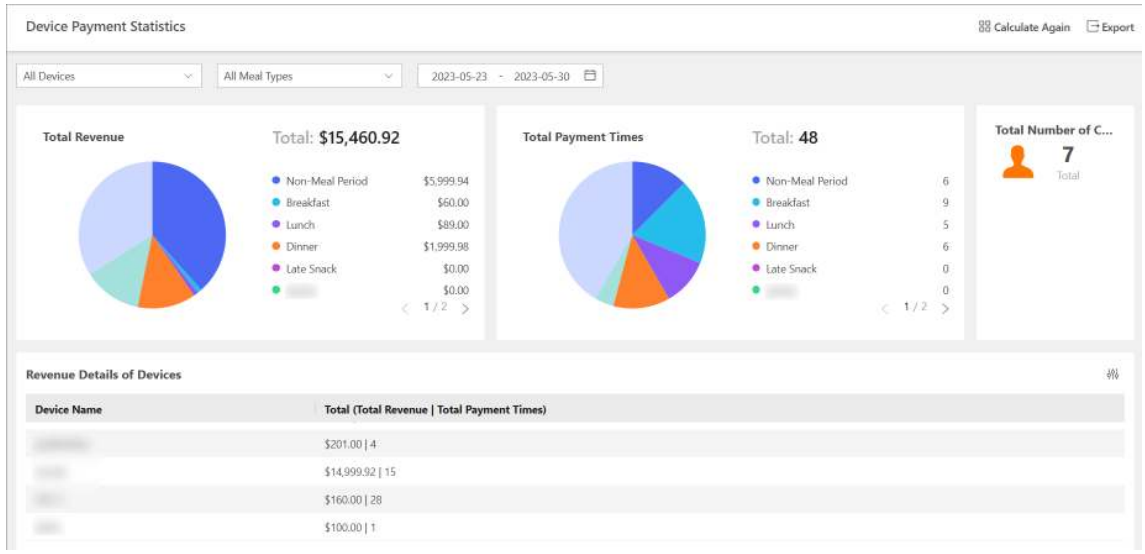


Figure 44-14 Device Payment Statistics

You can move the cursor on a part of the pie chart to view the corresponding meal type and revenue. You can also click a meal type to cancel displaying it in the pie charts.

You can click to custom the list items to be displayed in the **Payment Details** table.

You can click **Export** to export the statistics in Excel or PDF format.


See Far, Go Further