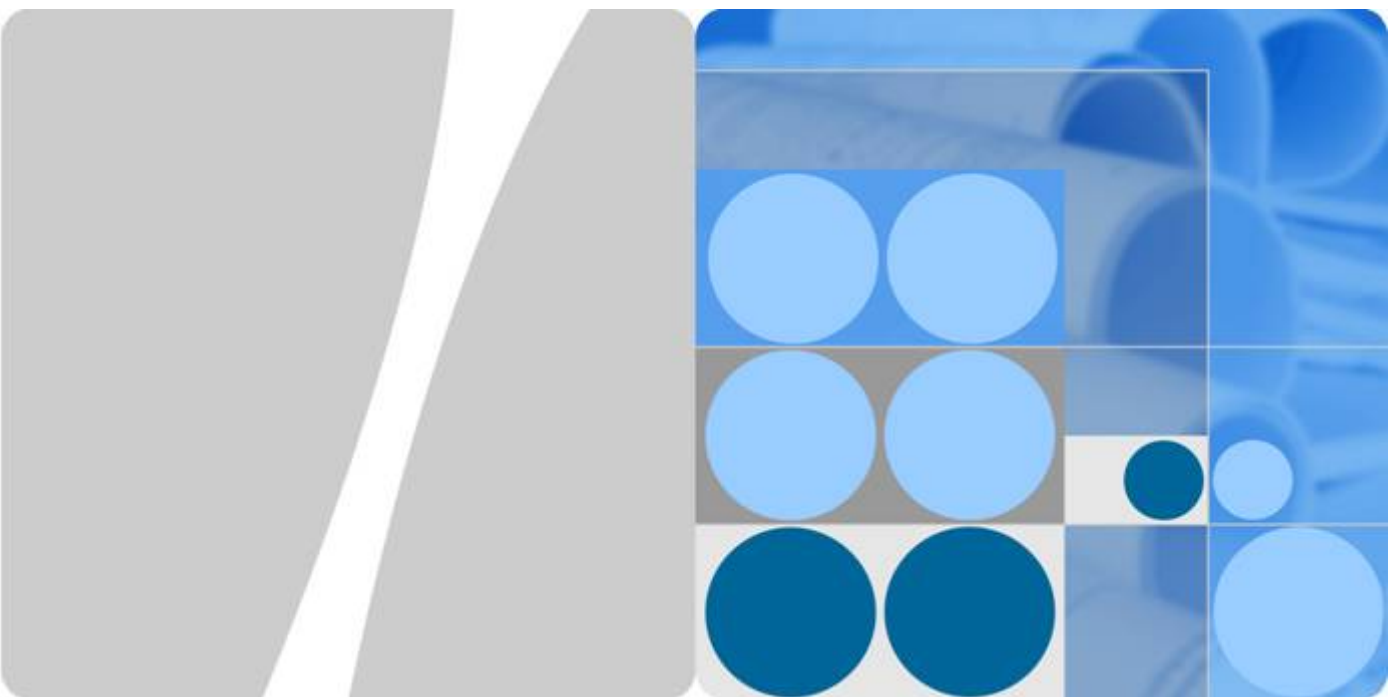




iClient S100 V2.1.0 User Guide

Date 2022-09-27

Contents

1 User Notice.....	1
1.1 Conventions.....	1
1.2 Security Statement.....	3
1.3 Version Mapping.....	4
1.4 Change History.....	5
1.5 Feedback and Technical Support.....	17
2 Product Overview.....	18
2.1 Product Positioning and Highlights.....	18
2.2 Typical Network.....	19
2.3 Cable Connections for Access Control Devices.....	21
3 Installation and Login.....	25
3.1 Operating Environmental Requirements.....	25
3.2 Installing the iClient S100.....	27
3.3 Logging In to the iClient S100.....	30
3.4 Home Page Layout.....	33
4 Video Service Management (for NVR800).....	37
4.1 Device Access.....	37
4.1.1 Application Scenario.....	37
4.1.2 Device Connection.....	39
4.1.2.1 Adding NVR800s.....	40
4.1.2.2 Adding Cameras on the NVR800.....	44
4.1.2.2.1 Automatically Adding Cameras in Batches (Recommended).....	44
4.1.2.2.2 Manually Adding Devices in Batches.....	46
4.1.2.2.3 Manually Adding a Device.....	49
4.1.2.3 Connecting Cameras to the NVR800.....	51
4.1.2.3.1 Configuring Connection Through ONVIF in the Camera Web System.....	51
4.1.3 Verification.....	55
4.2 Video Viewing.....	56
4.2.1 Live Video Viewing.....	56
4.2.2 Camera Cycling.....	58
4.2.3 View Management.....	61
4.2.4 PTZ Controls.....	62

4.2.5 Snapshot Taking.....	68
4.2.6 OSD Settings.....	69
4.3 Recording.....	70
4.3.1 Application Scenario.....	70
4.3.2 Recording Configuration.....	71
4.3.2.1 Setting Recording Parameters.....	71
4.3.2.2 Configuring Scheduled Recording.....	71
4.3.3 Configuring Manual Local Recording.....	72
4.3.4 Recording Playback.....	73
4.3.5 Recording Download.....	75
4.3.5.1 Setting Recording Download Parameters.....	75
4.3.5.2 Configuring Recording Download.....	77
4.4 Video Wall.....	79
4.4.1 Configuring a Video Wall.....	79
4.4.1.1 Application Scenario.....	79
4.4.1.2 Configuring a Decoder for Video Display on a Video Wall.....	80
4.4.1.3 Verification.....	88
4.4.2 Live Video Viewing on a Video Wall.....	88
4.4.3 Cycling on the Video Wall.....	90
4.4.4 Video Wall View Management.....	92
4.4.5 Video Wall Window splicing.....	95
4.4.6 Video Wall Floating window.....	96
4.4.7 Alarm linkage Video Wall.....	97
4.5 Common Intelligence.....	100
4.5.1 Motion Detection.....	100
4.5.2 Lens Blocking Detection.....	103
4.5.3 Audio Diagnosis.....	105
4.5.4 Privacy Mask.....	108
4.6 Behavior Analysis.....	109
4.6.1 Function Description.....	109
4.6.2 Configuration Process.....	110
4.6.3 Global Configuration.....	111
4.6.4 Tripwire Crossing Detection.....	113
4.6.5 Intrusion Detection.....	119
4.6.6 Abandoned Object Detection.....	124
4.6.7 Removed Object Detection.....	129
4.6.8 Loitering Detection.....	134
4.6.9 Area Entry Detection.....	139
4.6.10 Area Exit Detection.....	144
4.6.11 Fast Movement Detection.....	149
4.6.12 Electric Bike Detection.....	154
4.7 Intelligent target Analysis.....	159

4.7.1 Global Configuration.....	159
4.7.2 Computing Power Sharing.....	166
4.7.3 1 + N.....	172
4.7.4 Target List Management.....	173
4.7.5 Target Search.....	176
4.7.6 Person Frequency Search.....	181
4.7.7 Appearance Frequency.....	185
4.7.8 List-based Target Alert.....	188
4.7.9 Target Recognition Attendance.....	189
4.7.10 VIP Recognition.....	189
4.7.11 Mask Detection.....	190
4.7.12 Customer Flow Analysis.....	191
4.7.13 Customer Flow Statistics.....	192
4.8 Person Intelligence.....	193
4.8.1 Person Search.....	193
4.9 Situation Analysis.....	195
4.9.1 Head Counting.....	195
4.9.2 Queue Length Detection.....	201
4.9.3 Crowd Density Detection.....	207
4.9.4 Heat Map.....	212
4.9.5 Off-Duty Detection.....	214
4.10 Vehicle Intelligence.....	220
4.10.1 Global Configuration.....	220
4.10.2 Vehicle Search.....	222
4.10.3 Object Classification Statistics.....	225
4.10.4 Parking Violation Detection.....	226
4.11 Third-Party Algorithms.....	230
4.12 Alarm Management.....	233
4.12.1 Video Alarm.....	233
4.12.1.1 Latest Alarms.....	235
4.12.1.2 Historical Alarms.....	237
4.12.2 Alarm Linkage.....	240
4.12.2.1 Application Scenario.....	240
4.12.2.2 Configuring an Alarm Linkage Policy.....	240
4.12.2.3 Verification.....	244
4.12.3 Alarm Parameter Settings.....	247
5 Video Service Management (for IVS1800).....	250
5.1 Device Access.....	250
5.1.1 Application Scenario.....	250
5.1.2 Device Connection.....	252
5.1.2.1 Adding IVS1800s.....	252
5.1.2.2 Adding Cameras on the IVS1800.....	256

5.1.2.2.1 Automatically Adding Cameras in Batches (Recommended).....	256
5.1.2.2.2 Manually Adding Devices in Batches.....	259
5.1.2.2.3 Manually Adding a Device.....	262
5.1.2.3 Connecting Cameras to the IVS1800.....	265
5.1.2.3.1 Configuring Connection Through GB/T 28181 in the Camera Web System.....	265
5.1.2.3.2 Configuring Connection Through ONVIF in the Camera Web System.....	268
5.1.3 Verification.....	272
5.2 Video Viewing.....	273
5.2.1 Live Video Viewing.....	274
5.2.2 Camera Cycling.....	276
5.2.3 View Management.....	278
5.2.4 PTZ Controls.....	280
5.2.5 Snapshot Taking.....	286
5.2.6 OSD Settings.....	286
5.3 Recording.....	288
5.3.1 Application Scenario.....	288
5.3.2 Overall Process.....	288
5.3.3 Recording Configuration.....	289
5.3.3.1 Setting Recording Parameters.....	289
5.3.3.1.1 Configuring a Recording Storage Policy.....	290
5.3.3.1.2 (Optional) Configuring Video Buffering.....	293
5.3.3.2 Configuring Scheduled Recording.....	295
5.3.3.2.1 Configuring Scheduled Server Recording.....	295
5.3.4 Configuring Manual Local Recording.....	296
5.3.5 Recording Playback.....	297
5.3.6 Recording Download.....	300
5.3.6.1 Setting Recording Download Parameters.....	300
5.3.6.2 Configuring Recording Download.....	301
5.4 Video Wall.....	304
5.4.1 Configuring a Video Wall.....	304
5.4.1.1 Application Scenario.....	304
5.4.1.2 Configuring a Decoder for Video Display on a Video Wall.....	304
5.4.1.3 Verification.....	312
5.4.2 Live Video Viewing on Video Walls.....	312
5.4.3 Cycling on Video Walls.....	314
5.4.4 Video Wall View Management.....	316
5.4.5 Recording Playback on the Video Wall.....	319
5.4.6 Video Wall Window splicing.....	322
5.4.7 Video Wall Floating window.....	323
5.4.8 Alarm linkage Video Wall.....	324
5.5 Common Intelligence.....	326
5.5.1 Motion Detection.....	327

5.5.2 Lens Blocking Detection.....	330
5.5.3 Privacy Mask.....	332
5.6 Behavior Analysis.....	334
5.6.1 Frontend Behavior Analysis.....	334
5.6.1.1 Function Description.....	334
5.6.1.2 Configuration Process.....	335
5.6.1.3 Global Configuration.....	336
5.6.1.4 Tripwire Crossing Detection.....	338
5.6.1.5 Intrusion Detection.....	344
5.6.1.6 Abandoned Object Detection.....	349
5.6.1.7 Removed Object Detection.....	354
5.6.1.8 Loitering Detection.....	359
5.6.1.9 Area Entry Detection.....	364
5.6.1.10 Area Exit Detection.....	369
5.6.1.11 Fast Movement Detection.....	374
5.6.1.12 Electric Bike Detection.....	379
5.6.2 Backend Behavior Analysis	384
5.6.2.1 Function Description.....	384
5.6.2.2 (Optional) Common Configuration.....	384
5.6.2.3 Intrusion Detection.....	386
5.6.2.4 Tripwire Crossing Detection.....	390
5.6.2.5 Area Entry Detection.....	393
5.6.2.6 Area Exit Detection.....	397
5.6.2.7 Fast Movement Detection.....	400
5.6.2.8 Loitering Detection.....	404
5.7 Target Intelligence.....	407
5.7.1 Target Intelligence (Based on Cameras).....	407
5.7.1.1 Global Configuration.....	407
5.7.1.2 Mask Detection.....	414
5.7.2 Target Intelligence (Based on IVS1800).....	415
5.7.2.1 Target List Management.....	415
5.7.2.2 Target Search.....	418
5.7.2.3 1:1 Target Match.....	425
5.7.2.4 List-based Target Alert.....	427
5.7.2.4.1 Application Scenario.....	427
5.7.2.4.2 Prerequisites.....	427
5.7.2.4.3 Procedure.....	427
5.7.2.4.4 Verification.....	432
5.7.2.5 Target Recognition Attendance.....	433
5.7.2.6 VIP Recognition.....	433
5.7.3 Customer Flow Analysis.....	434
5.7.4 Customer Flow Statistics.....	435

5.8 Person Intelligence.....	436
5.8.1 Person Search.....	436
5.8.1.1 Application Scenario.....	436
5.8.1.2 Prerequisites.....	436
5.8.1.3 (Optional) Configuring a Person Recognition Task.....	437
5.8.1.4 Verification.....	438
5.9 Situation Analysis.....	439
5.9.1 Head Counting.....	439
5.9.2 Queue Length Detection.....	445
5.9.3 Crowd Density Detection.....	451
5.9.4 Heat Map.....	456
5.9.5 Off-Duty Detection.....	458
5.10 Intelligent Vehicle Analysis.....	464
5.10.1 Vehicle Intelligence (Based on Cameras).....	464
5.10.1.1 Global Configuration.....	464
5.10.1.2 Parking Violation Detection.....	466
5.10.2 Vehicle Intelligence (Based on IVS1800).....	470
5.10.2.1 Vehicle Library.....	470
5.10.2.1.1 Application Scenario.....	470
5.10.2.1.2 Adding a Vehicle List.....	470
5.10.2.1.3 Adding Vehicle Records to a Vehicle List.....	471
5.10.2.2 Vehicle Search.....	474
5.10.2.2.1 Application Scenario.....	474
5.10.2.2.2 Prerequisites.....	475
5.10.2.2.3 (Optional) Creating a Video Structuring Task.....	475
5.10.2.2.4 Verification.....	477
5.10.2.3 Vehicle Alert.....	479
5.10.2.3.1 Application Scenario.....	479
5.10.2.3.2 Prerequisites.....	479
5.10.2.3.3 Creating a Vehicle Alert Task.....	480
5.10.2.3.4 Viewing Vehicle Alert Results.....	481
5.10.3 Object Classification Statistics.....	481
5.11 Third-Party Algorithms.....	482
5.11.1 Context.....	482
5.11.2 Third-Party Algorithm Installation.....	483
5.11.2.1 Offline Installation.....	483
5.11.3 Third-Party Algorithm Configuration.....	484
5.12 Alarm Management.....	492
5.12.1 Video Alarm.....	492
5.12.1.1 Latest Alarms.....	494
5.12.1.2 Historical Alarms.....	496
5.12.2 Alarm Linkage.....	499

5.12.2.1 Application Scenario.....	499
5.12.2.2 Configuration Process.....	500
5.12.2.3 Prerequisites.....	500
5.12.2.4 Configuring an Alarm Linkage Policy.....	501
5.12.2.5 Verification.....	504
5.12.3 Alarm Management Configuration.....	507
5.12.3.1 Alarm Parameter Settings.....	507
5.12.3.2 Alarm Severity.....	509
5.13 Media Transmission.....	511
5.13.1 Feature Description.....	511
5.13.2 Setting Bandwidth Adaptation Parameters.....	513
6 Comprehensive Services.....	515
6.1 Personnel Management.....	515
6.1.1 Configuration Process.....	515
6.1.2 Adding Departments.....	516
6.1.2.1 Importing Departments in Batches.....	517
6.1.2.2 Adding Departments One by One.....	518
6.1.3 Position Configuration.....	519
6.1.3.1 Adding Positions One by One.....	519
6.1.4 Adding Persons.....	520
6.1.4.1 Importing Persons in Batches on the iClient S100.....	521
6.1.4.1.1 Importing Person Information.....	521
6.1.4.1.2 (Optional) Importing Biometric Recognition Data.....	523
6.1.4.1.3 (Optional) Importing Person Photos.....	523
6.1.4.2 Manually Adding Persons One by One on the iClient S100.....	526
6.1.4.2.1 Adding Person Information.....	526
6.1.4.2.2 Importing Biometric Recognition Data.....	529
6.1.4.3 Adding Persons Through Devices.....	530
6.2 Access Control Management.....	532
6.2.1 Application Scenario.....	532
6.2.2 Configuration Process.....	532
6.2.3 Adding Devices.....	533
6.2.3.1 Prerequisites.....	533
6.2.3.2 Adding Access Control Devices.....	534
6.2.4 Configuring Access Control Rules.....	536
6.2.4.1 Setting Door Parameters.....	536
6.2.4.2 Binding Reader/Auxiliary Input Devices to Cameras.....	539
6.2.4.3 Setting Valid Time Periods.....	540
6.2.4.4 Setting Holidays.....	541
6.2.4.5 Configuring Linkage Policies.....	543
6.2.4.5.1 Application Scenario.....	543
6.2.4.5.2 Prerequisites.....	543

6.2.4.5.3 Adding Linkage Policies.....	544
6.2.5 Setting Access Levels.....	547
6.2.5.1 Creating Access Levels.....	547
6.2.5.2 Adding Doors to Access Levels.....	548
6.2.6 Assigning Access Permissions.....	549
6.2.6.1 Assigning Access Permissions by Access Level.....	549
6.2.6.2 Assigning Access Permissions by Person.....	550
6.2.7 Verification.....	551
6.3 Configuring Electronic Maps.....	554
6.3.1 Adding Maps.....	554
6.3.2 Adding Devices.....	556
6.3.3 Verification.....	557
6.4 Attendance Management Service Configuration.....	560
6.4.1 Application Scenario.....	560
6.4.2 Configuration Process.....	560
6.4.3 Adding Personnel to an Attendance Area.....	561
6.4.4 Adding Devices.....	562
6.4.4.1 Attendance Device Description.....	562
6.4.4.2 Using an Attendance Device as the Attendance Data Source.....	563
6.4.4.2.1 Prerequisites.....	563
6.4.4.2.2 Automatically Adding an Attendance Device.....	563
6.4.4.2.3 Adding an Attendance Device by Authorization.....	564
6.4.4.3 Using a Camera as the Attendance Data Source.....	565
6.4.4.4 Using an Access Control Device as the Attendance Data Source.....	567
6.4.5 Attendance Setting.....	569
6.4.5.1 Setting the Attendance Rules.....	569
6.4.5.2 Adding a Holiday.....	571
6.4.5.3 Adding a Leave Type.....	572
6.4.6 Regular Shift Setting.....	573
6.4.6.1 Add a Normal Time Slot.....	573
6.4.6.2 Adding a Regular Shift.....	575
6.4.7 Schedule Setting.....	577
6.4.7.1 Personnel Schedule.....	577
6.4.7.2 Group Schedule.....	578
6.4.8 Verification.....	580
6.5 Configuring Epidemic Prevention Management.....	582
6.5.1 Application Scenario.....	582
6.5.2 Prerequisites.....	583
6.5.3 Setting Epidemic Prevention Parameters.....	583
6.5.4 Verification.....	583
6.6 Configuring User Permission Management.....	584
6.6.1 Application Scenario.....	584

6.6.2 Adding a Role.....	584
6.6.3 Adding a User.....	585
6.6.4 Verification.....	587
7 Local/Personal Configuration.....	589
7.1 Local Settings.....	589
7.2 Personal Settings.....	590
8 FAQs.....	597
8.1 Video Service.....	597
8.1.1 Viewing Live Video.....	597
8.1.1.1 How Do I Define the Layout for Live Video Viewing or Recording Playback?.....	597
8.1.1.2 How Do I Add Cameras to a Favorites Folder?.....	598
8.1.1.3 How Do I Use Voice Intercom?.....	600
8.1.1.4 How Do I Use Voice Broadcast?.....	601
8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?.....	603
8.1.1.6 How Do I Adjusting the Video Grouping Sequence.....	606
8.1.2 Client.....	607
8.1.2.1 How Do I Use the Multiple Windows Function?.....	607
8.1.2.2 What Is the Default Password for Logging in to the Client?.....	607
8.1.2.3 How Do I Set the System Time and Time Zone?.....	607
8.1.2.4 How Do I Set the Server IP Address When the Computer Running the iClient S100 Server Has Two Network Adapters?.....	607
8.1.3 User Management.....	608
8.1.3.1 Configuring a User Role.....	608
8.1.4 Camera.....	614
8.1.4.1 How Do I Set Alarm Input and Output Parameters for a Camera?.....	614
8.1.5 Others.....	616
8.1.5.1 How Do I Check the Target Image Resolution?.....	616
8.2 Comprehensive Services.....	618
8.2.1 Basic Management.....	618
8.2.1.1 How Can I View Logs Recording My Operations on the iClient S100?.....	618
8.2.1.2 How Can I Back Up a Database?.....	620
8.2.1.3 How Can I Restore a Database?.....	620
8.2.1.4 How Can I Set Up an Area?.....	622
8.2.1.5 How Can I Configure Support for Sending Emails?.....	623
8.2.2 Communication Management.....	624
8.2.2.1 How Can I View Records of Commands Issued by the Server?.....	625
8.2.2.2 How Can I Check Communication Status of Devices Added to the iClient S100?.....	626
8.2.2.3 How Can I Check Communication Status of the Server?.....	626
8.2.3 Device Addition.....	627
8.2.3.1 How Can I Set or Change the IP Address of an Access Control Device Using a Tool?.....	627
8.2.4 Tablet Source Management.....	629
8.2.4.1 How Can I Customize the Image Display of Specific Pages on a Tablet Device?.....	629

8.2.4.1.1 Resource Addition.....	629
8.2.4.1.2 Resource Allocation.....	630
8.2.4.2 How Can I Set a Customized Message Prompting an Event to Occur on a Tablet Device?.....	632
8.2.4.2.1 Resource Addition.....	632
8.2.4.2.2 Resource Allocation.....	633
8.2.5 Person Addition.....	634
8.2.5.1 How Can I Add Person Information on a Device?.....	635
9 Troubleshooting.....	636
9.1 Client.....	636
9.1.1 Login Fails After the iClient S100 Is Installed.....	636
9.1.2 An Error Message Is Displayed During Login to the iClient S100.....	638
9.1.3 File Loss Error Displayed When Running the iClient S100 Client.....	639
9.1.4 iClient S100 Server Fails to Be Started.....	639
9.1.5 Login to the iClient S100 Server Fails Occasionally After the Computer Where the iClient S100 Server Is Located Restarts Unexpectedly.....	639
9.1.6 The iClient S100 Suddenly Shuts Down During Service Running and Fails to Be Re-logged in.....	640
9.1.7 A Specific Recording Can Be Played Back on a Client But Cannot Be Played on the Other Client....	641
9.1.8 The iClient S100 Fails to Receive Messages (Such as Alarms) from the IVS1800 Due to the Change of the IP Address of the Computer Where the iClient S100 Server Is Located.....	641
9.2 Video Devices.....	642
9.2.1 No Refresh and Add Buttons in the Device List.....	642
9.2.2 Failure to Connect an IVS1800/NVR800 to the iClient S100.....	643
9.2.3 After You Connect Cameras to a Registered IVS1800 on the iClient S100, None of the Cameras Is Displayed; When You Connect Them Again, a Message Is Displayed Indicating Connection Failure Due to Duplicate IP Addresses.....	644
9.2.4 When You Attempt to Connect or Log In to an NVR800 on the iClient S100, a Message Is Displayed Indicating that the Account Has Logged In Elsewhere.....	646
9.2.5 After an IVS1800 Is Upgraded Through Reinstallation, Some of Its Functions Are Unavailable on the iClient S100.....	646
9.3 Basic Operations.....	647
9.3.1 Video from an IVS1800/NVR800 Pushed to the Video Wall Through the iClient S100 Is Abnormal	647
9.3.2 The Intelligent Overlay Function on the Live Video Viewing Page and Regular Customer Detection Are Unavailable After an NVR800 Is Connected to the iClient S100.....	648
9.3.3 Video Streams Are Interrupted and Then Being Reconnected When You Attempt to View Live Video from Cameras Connected to an NVR800 or IVS1800 on Multiple Clients.....	648
9.4 Intelligent Applications.....	649
9.4.1 No Snapshot Alarm Is Displayed on the Target Recognition or Object Classification Page of the iClient S100.....	649
9.4.2 Failure to Import Dynamic Lists to the NVR800.....	649
9.4.3 Target Snapshot Alarms Cannot Be Displayed on the Intelligent Recognition Page of the iClient S100, But Can Be Displayed on the NVR800 LDU.....	650
9.5 Comprehensive Services.....	650
9.5.1 Personnel Management.....	650
9.5.2 Access Control.....	651

9.5.3 Attendance..... 651

10 Reference..... 652

10.1 Password Maintenance Suggestions..... 652

10.2 Communication Matrix..... 653

1 User Notice

- [1.1 Conventions](#)
- [1.2 Security Statement](#)
- [1.3 Version Mapping](#)
- [1.4 Change History](#)
- [1.5 Feedback and Technical Support](#)

1.1 Conventions

This section provides the general conventions, command conventions, GUI conventions, keyboard operations, and mouse operations that may be found in the document.

Symbol Conventions

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

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk which, if not avoided, could result in death or serious injury.
 WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
 CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
 NOTICE	Indicates a potentially hazardous situation which if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

Symbol	Description
 NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

GUI Conventions

Format	Description
""	Buttons, menus, parameters, tabs, window, and dialog titles are in boldtarget. For example, click OK .
>	Multi-level menus are in boldtarget and separated by right angle brackets (>). For example, choose File > Create > Folder .

Keyboard Operation Conventions

Format	Description
Boldtarget	Key names are in boldtarget. For example, press Enter , Tab , Backspace , and a .
Key 1+Key 2	Keys are pressed concurrently. For example, pressing Ctrl+Alt+A means that the three keys should be pressed concurrently.
Key 1, Key 2	Press the keys in turn. For example, pressing Alt, F means the two keys should be pressed in turn.

Mouse Operation Conventions

Format	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

1.2 Security Statement

This section presents the security statement of the document.

Content Conventions

The purchased products, services, and features are stipulated by the contract made between the vendor and the customer. All or part of the products, services, and features described in this document may not be within the purchase scope or usage scope. Contents in this document do not constitute a warranty of any kind, express or implied, unless a contract stipulates otherwise.

Notices About Security Operations

Before performing maintenance operations, engineers must comply with the following specifications:

- Perform maintenance only after being authorized by the customer.
- Obtain the customer's authorization before taking troubleshooting data out of the customer's network. Personal information in such data must be rendered anonymous to ensure that the device provider cannot restore personal information in any ways.

Notices About Personal Data

The product, service, or feature you purchased may obtain or use some personal data during service operation or fault locating, so you must observe the local laws to protect users' private information.

You are advised to use a professional video or image editing tool to shield irrelevant persons in downloaded or exported video or images and meet the HD requirements of the data subject. The recommended procedure is as follows:

1. Download the required video to the local computer and decompress it to common video or export image data to the local computer.
2. Use a video or an image editing tool to anonymize irrelevant targets and only retain the HD part of the data subject.
3. Export the anonymized video or images to meet the data transfer requirements of the data subject.
4. To ensure personal information security, delete the downloaded or exported images and recordings in a timely manner.

Notices About Feature Usage

** WARNING**

Target recognition and person recognition are sensitive features. To use these features, users must sign agreements for using sensitive features as permitted by related laws and install the sensitive feature software packages.

- In response to explicit customer requests, the company has worked hard to provide the target recognition and person recognition features (these features for short). These features are used to recognize targets or persons that pass through a specified detection area and generate alarms when particular targets are detected. The system can search for targets based on images that have been uploaded. The company is unable to enable or use these features, or acquire any information about customer usage or maintenance of the features without customer authorization. The customer and its authorized parties shall, as required by the relevant laws and regulations, provide users, governmental bodies, and any other third parties, with the necessary information, and obtain and reserve all necessary consents, licenses, and authorizations when using and maintaining these features. Applicable laws and regulations, user agreements, terms of use, privacy statement, any other lawful agreements, or public or targeted statements shall not be violated. The company provides the features for the customer and the customer has a commitment to the company that the customer will only use and maintain these features as permitted by applicable laws and regulations, agreements and statements. The company will not bear any legal obligations or liabilities, including but not limited to, claims, liabilities, obligations, costs, expenses, penalties, injunctions, and judgments that are not caused by the misconduct of the company when the customer or its authorized parties are using and maintaining the feature.

In the event that any governmental body adopts laws and regulations, or a customer signs agreements with third parties or makes statements, which materially affects the legitimacy or provisioning of these features, wholly or partially, the company reserves the right, at their sole discretion, to terminate the provisioning of these features without any liability to the extent permitted by law.

- Strictly follow your local laws and regulations when using video-related services, for example, recording video, recording voice, and taking snapshots. Do not use them for illegitimate purposes, for example, snooping on people's privacy or illegally installing such devices in offices to observe employee behavior.
- The HTTP protocol is used for upgrading clients, uploading snapshots, and downloading logs, which may bring some security risks. You need to export the logs on a trusted network.

Notices About Passwords

- When you use a default password at the first login, change it in time.
- For device security purposes, enable the password complexity check function and select **Verify the old password when changing a new password**. Change the password periodically.
- For security purposes, the new password must meet complexity requirements. A strong password is highly recommended.

1.3 Version Mapping

The following table describes the version mapping between the iClient S100 and video service devices.

iClient S100 Version	NVR800	IVS1800	
V1.0.0	8.1.RC1	8.1.RC2	
V1.1.0	8.1.0	8.1.0	
V1.2.0	8.1.0	8.1.0/8.1.1	
V1.3.0	9.0.RC1	9.0.RC2	NOTE - The client of V1.3.0 and later versions must be used with the IVS1800 9.0.0 and later versions, - and SDCs connected to the IVS1800 should be 9.0.0 and later versions. Otherwise, some functions may be unavailable.
V1.4.0 & V1.5.0	9.0.0	9.0.0/9.0.0.SP C1	
V1.6.0	9.0.0.SPC3	9.1.RC1	
V1.7.0	9.0.0.SPC3	9.1.0	
V1.8.0	9.0.0.SPC3	9.1.0	
V1.9.0	9.0.0.SPC6	10.0.0.RC1	
V2.0.0	9.0.0.SPC7	10.0.0.RC2	
V2.1.0	9.0.0.SPC8	10.0.0.RC2	

1.4 Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

NOTICE

The user manual must match the software version. For details, see the user manual that matches the software version. For the user manual of an earlier version, you can view the online help delivered with the software of the earlier version.

If the configuration in the user manual is inconsistent with the actual software intertarget, the actual software intertarget is used.

Issue V2.1.0 (2022-09-30)

Compared with V2.0.0, this issue has the following updates.

Section	Path	Update
Video Service Management (for 1800)	User Guide > Video Service Management (for IVS1800)>Behavior Analysis	Added the function of "Parking detection".

Issue V2.0.0 (2022-07-30)

Compared with V1.9.0, this issue has the following updates.

Section	Path	Update
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800)	Added the function of "Receive operation and maintenance alarm".

Issue V1.9.0 (2022-04-20)

Compared with V1.8.0, this issue has the following updates.

Section	Path	Update
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Devices Access > Device Connection > Adding IVS1800	Added the function of "batch access to IVS1800 device".
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Target Intelligence > Target Intelligence > Target Recognition	Added the function of "target recognition and mask alarm audio configuration functions".
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Target Intelligence > Target Intelligence > Global Configuration	Added "target intelligent switch configuration" function.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Target Intelligence > Target Intelligence > Global Configuration	Added "target intelligent switch configuration" function.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Target Intelligence > Target Intelligence > Mask Detection	Added the function of "mask alarm audio configuration functions".
iClient S100 Installation and Login	User Guide > Installation and Login > Forgot password	Added the function of "password retrieval using custom question method".

Issue V1.8.0 (2022-01-30)

Compared with V1.7.0, this issue has the following updates.

Section	Path	Update
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Video Wall > Configuring a Video Wall > Configuring a Decoder for Video Display on a Video Wall	Added the function of multi screen splicing and floating window of Video Wall
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Video Wall > Configuring a Video Wall > Configuring a Decoder for Video Display on a Video Wall	Added the function of alarm linkage on Video Wall
iClient S100 Installation and Login	User Guide > Installation and Login > Logging In to the iClient S100	Can manage cloud services and offline devices separately in login page

Issue V1.7.0 (2021-11-30)

Compared with V1.6.0, this issue has the following updates.

Section	Path	Update
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Recording > Recording Configuration	Added the NVR800 recording configuration function
FAQ	User Guide > FAQs > Video Service > Viewing Live Video > How Do I Adjusting the Video Grouping Sequence?	Added the adjusting the Video Grouping Sequence function
iClient S100 Installation and Login	User Guide > Installation and Login > Logging In to the iClient S100	Initialize the account upon the first login.

Issue V1.6.0 (2021-09-30)

Compared with V1.5.0, this issue has the following updates.

Section	Path	Update
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Device Access > Device Connection > Adding NVR800s	Added the function of automatically searching for NVR800 devices in the same VLAN and adding them to the client in batches.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Video Wall > Configuring a Video Wall > Configuring a Decoder for Video Display on a Video Wall	Added the Jovision DEC6109 decoder on the client.
Video Service Management (for NVR800)	- User Guide > Video Service Management (for NVR800) > Target Intelligence > Target Search - User Guide > Video Service Management (for NVR800) > Person Intelligence > Person Search - User Guide > Video Service Management (for NVR800) > Vehicle Intelligence > Vehicle Search	Added the function of searching for images from cameras connected to various main devices at the same time.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Person Intelligence > Person Search	Added the function of configuring person search for the NVR800 on the client.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Alarm Management > Video Alarm > Historical Alarms	Added the function of searching for historical alarms from cameras connected to multiple NVR800 devices.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Device Access > Device Connection	Added the function of switching to the IVS1800 OMU portal on the client.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Video Wall > Configuring a Video Wall > Configuring a Decoder for Video Display on a Video Wall	Added the Jovision DEC6109 decoder on the client.

Section	Path	Update
Video Service Management (for IVS1800)	- User Guide > Video Service Management (for IVS1800) > Target Intelligence > Target Intelligence (Based on IVS1800) > Target Search - User Guide > Video Service Management (for IVS1800) > Person Intelligence > Person Search - User Guide > Video Service Management (for IVS1800) > Vehicle Intelligence > Vehicle Intelligence (Based on IVS1800) > Vehicle Search	Added the function of searching for images from cameras connected to various main devices.
Video Service Management (for IVS1800)	- User Guide > Video Service Management (for IVS1800) > Target Intelligence > Target Intelligence (Based on IVS1800) > Target Search - User Guide > Video Service Management (for IVS1800) > Target Intelligence > Target Intelligence (Based on IVS1800) > List-based Target Alert - User Guide > Video Service Management (for IVS1800) > Person Intelligence > Person Search - User Guide > Video Service Management (for IVS1800) > Vehicle Intelligence > Vehicle Intelligence (Based on IVS1800) > Vehicle Search - User Guide > Video Service Management (for IVS1800) > Vehicle Intelligence > Vehicle Intelligence (Based on IVS1800) > Vehicle Alert	Added the function of configuring a time plan for backend intelligent analysis tasks on the client.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Vehicle Intelligence > Object Classification Statistics	Added the function of configuring object classification statistics for the IVS1800 on the client.

Section	Path	Update
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Third-Party Algorithms	- Added the Algorithm Management page on the client for users to install and manage third-party algorithms for the IVS1800 and check the computing power usage. - Added the function of creating intelligent analysis tasks based on third-party algorithms of the IVS1800 on the client.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Alarm Management > Video Alarm > Historical Alarms	Added the function of searching for historical alarms from cameras connected to multiple IVS1800 devices.

Issue V1.5.0 (2021-06-30)

Compared with V1.4.0, this issue optimizes the home page layout and has the updates listed in the following table.

Section	Path	Update
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Intelligent Target Analysis > 1 + N	Added the 1 + N function.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Vehicle Intelligence > Global Configuration	Added the section about object classification verification.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Intelligent Target Analysis > Global Configuration	- Added the section about target recognition verification. - Added description about advanced parameters in section "Setting Target Parameters."
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Intelligent Vehicle Analysis > Vehicle Intelligence (Based on Cameras) > Global Configuration	Added the section about object classification verification.

Section	Path	Update
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Target Intelligence > Target Intelligence (Based on Cameras) > Global Configuration	- Added the section about target recognition verification. - Added description about advanced parameters in section "Setting Target Parameters."

Issue V1.4.0 (2021-05-30)

Compared with V1.3.0, this issue has the updates listed in the following table.

Section	Path	Update
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Third-Party Algorithms	Added the functions of viewing and configuring third-party algorithms that have been installed on the IVS1800 on the client.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Alarm Management > Video Alarm	Added the functions of adding targets to target lists, searching targets by image, and viewing trajectories on the target recognition alarm details page of the client.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Situation Analysis > Off-Duty Detection	Added the function of configuring off-duty detection on the client.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Alarm Management > Alarm Linkage	Added the function of configuring an alarm linkage action for multiple NVR800s at a time on the client.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Alarm Management > Video Alarm	Added the functions of receiving and querying appearance frequency alarms and off-duty detection alarms from the NVR800 on the client.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Alarm Management > Video Alarm	Added the functions of adding targets to target lists, searching targets by image, and viewing trajectories on the target recognition alarm details page of the client.

Section	Path	Update
Comprehensive Services	User Guide > Comprehensive Services > Configuring Electronic Maps > Verification	Added the multi-layer hotspot function to the client.
Comprehensive Services	User Guide > Configuring User Permission Management > Adding a User	Added the function of configuring whether a user is allowed to log in to the client on multiple computers at the same time.
FAQs	User Guide > FAQs > Video Service > Viewing Live Video > How Do I Superimpose a Behavior Analysis Task on Live Video?	Added the intelligent analysis types supported by intelligent overlay.

Issue V1.3.0 (2021-04-15)

Compared with V1.2.0, the name, style, and some configuration paths of GUI icons are adjusted. The following table lists the main changes in the current issue.

Section	Path	Change Description
Video Service Management (for IVS1800)	- User Guide > Video Service Management (for IVS1800) > Behavior Analysis > Backend Behavior Analysis - User Guide > Video Service Management (for IVS1800) > Target Intelligence/Person Intelligence/Vehicle Intelligence	Added the function of connecting the IVS1800 storage model (IVS1800-B08 and IVS1800-B16) to the client without supporting backend intelligent analysis.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Device Access	Added the function of connecting cameras to the IVS1800 through GB/T 28181 on the client.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Behavior Analysis > Frontend Behavior Analysis	Added the function of configuring area entry detection, area exit detection, fast movement detection, electric bike detection, and audible and visual alarming for the IVS1800 on the client.

Section	Path	Change Description
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Vehicle Intelligence > Vehicle Intelligence (Based on Cameras)	Added the function of configuring intelligent vehicle analysis functions based on cameras for the IVS1800 on the client, including object classification, object classification statistics, and parking violation alarm.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Target Intelligence > Target Intelligence (Based on Cameras)	Added the function of configuring intelligent target analysis functions based on cameras for the IVS1800 on the client, including target recognition and mask recognition.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Situation Analysis	Added the function of configuring intelligent situation analysis functions based on cameras for the IVS1800 on the client, including head counting, queue length detection, crowd flow analysis, and heat map.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Alarm Management > Video Alarm	Classified alarms reported by various devices into six categories on the client, and modified the GUI for displaying latest and historical alarms on the video alarm page.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Alarm Management > Alarm Linkage	Added the function of configuring alarm email linkage for the IVS1800 on the client.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Live Video Viewing > PTZ Controls	Added the function of configuring tours and customizing preset position names for the NVR800 on the client.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Behavior Analysis	Added the function of configuring abandoned object detection, removed object detection, electric bike detection, and audible and visual alarming for the NVR800 on the client.

Section	Path	Change Description
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Device Access	Added the function of automatically adding cameras to the NVR800 in batches on the client.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Vehicle Intelligence	Added the function of configuring intelligent vehicle analysis functions for the NVR800 on the client, including object classification, object classification statistics, vehicle search, and parking violation alarming.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Target Intelligence > Personal Frequency Analysis	Added the function of filtering out alarms triggered by minors for personal frequency analysis.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Alarm Management > Video Alarm	Classified alarms reported by various devices into six categories on the client, and modified the GUI for displaying latest and historical alarms on the video alarm page. Added the function of querying historical alarms of NVR800 on the client.
Comprehensive Services	User Guide > Comprehensive Services > Personnel Management > Adding Persons > Import Persons in Batches on the iClient S100 > (Optional) Importing Biometric Recognition Data	Added the function of importing palm veins on the client.
Comprehensive Services	User Guide > Comprehensive Services > Configuring Electronic Maps > Verification	Added the function of personnel trajectory search on the client.
Comprehensive Services	User Guide > Comprehensive Services > Attendance Management Service Configuration > Attendance Setting > Setting the Attendance Rules	Added the function of setting the frequency of obtaining attendance records from the attendance device on the iClient.

Section	Path	Change Description
Comprehensive Services	User Guide > Comprehensive Services > Attendance Management Service Configuration > Regular Shift Setting > Adding a Regular Shift	Modified the method of adding a time slot on the client.
FAQs	User Guide > FAQs > Video Service > Live Video Viewing	Added the voice intercom and voice broadcast functions on the client.
Troubleshooting	User Guide > Troubleshooting	Added troubleshooting cases related to video devices, video display on the video wall, and intelligent applications.

Issue V1.2.0 (2021-01-10)

Compared with V1.1.1, this issue has the updates listed in the following table.

Section	Path	Change Description
Installation and Login	User Guide > Installation and Login > Logging In to the iClient S100	The client supports the function of remembering the login password.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Device Access > Device Connection > Adding NVR800s	Added the configuration for changing the initial password of an NVR800.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Device Access > Device Connection > Adding Cameras on the NVR800 > Manually Adding a Device	Added the function for users to set areas when adding cameras.
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Target Intelligence	Added section "Computing Power Sharing."
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Target Intelligence > Regular Customer Search	Added the function of searching for regular customers by list, and importing the search results to lists.

Section	Path	Change Description
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Target Intelligence > Regular Customer Detection (on Entry and Exit Frequency)	Added section "Regular Customer Detection (on Entry and Exit Frequency)."
Video Service Management (for NVR800)	User Guide > Video Service Management (for NVR800) > Target Intelligence > Target Search	The image search supports list as the search criteria.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Device Access > Device Connection > Adding Cameras on the IVS1800 > Manually Adding a Device	Added the function for users to set areas when adding cameras.
Video Service Management (for IVS1800)	User Guide > Video Service Management (for IVS1800) > Target Intelligence > Target Search	- Added the function of image search by list. - Added the function of displaying body temperature in the result of search using a Dahua thermal camera.
FAQs	User Guide > FAQs > Video Service > Live Video Viewing	Added section "How Do I Superimpose a Behavior Analysis Task on Live Video?"
Troubleshooting	User Guide > Troubleshooting > Client	Added section "Login Fails After iClient S100 Installation."

Issue V1.1.1 (2020-11-15)

Compared with V1.1.0, this issue has the updates listed in the following table.

Section	Path	Change Description
Installation and Login	User Guide > Installation and Login > Installing the iClient S100	Added the description of installing the client by overwriting the previous version.
FAQs	User Guide > FAQ > Integrated Service Management FAQ > Basic Management	Added section "How to Restore a Database."

Issue V1.1.0 (2020-10-30)

This issue is the first official release.

1.5 Feedback and Technical Support

- You can provide feedback and seek technical support based on the contact provided by the channel partners.

2 Product Overview

[2.1 Product Positioning and Highlights](#)

[2.2 Typical Network](#)

[2.3 Cable Connections for Access Control Devices](#)

2.1 Product Positioning and Highlights

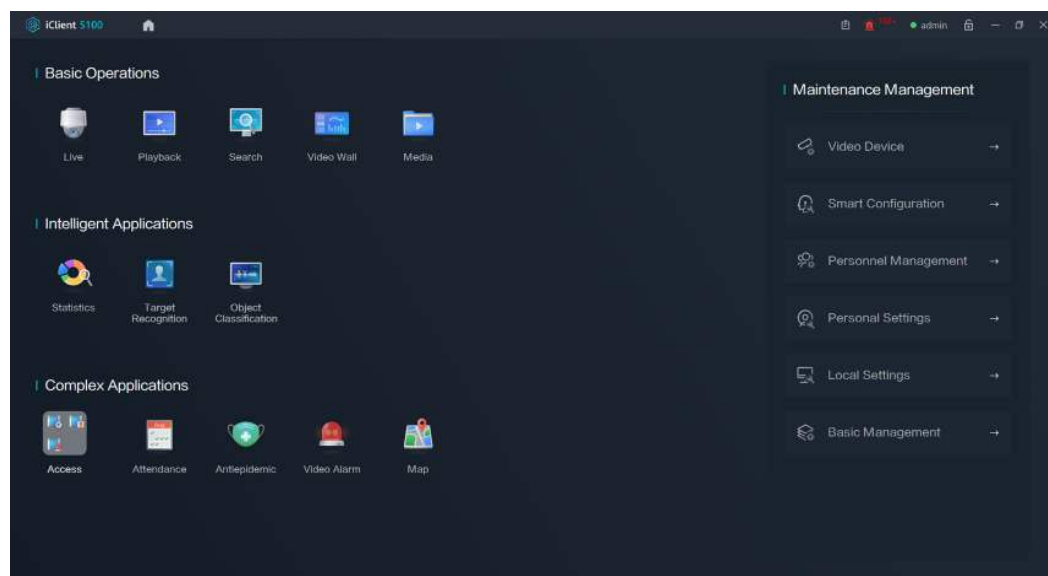
The iClient S100 is a management system that integrates basic and intelligent video-related applications, as well as access control, attendance, and epidemic prevention applications. It is designed for edge application scenarios such as small- and medium-sized enterprise campuses and small-sized branches.

On the iClient S100, you can manage cameras mounted to local IVS1800s and NVR800s, and perform video-related operations. In addition, the iClient S100 provides you with multiple subsystems to implement management of personnel, access control, attendance, and epidemic prevention.

Figure 2-1 shows the iClient S100 client home page.

NOTE

The client layout shown in the following figure is for reference only.

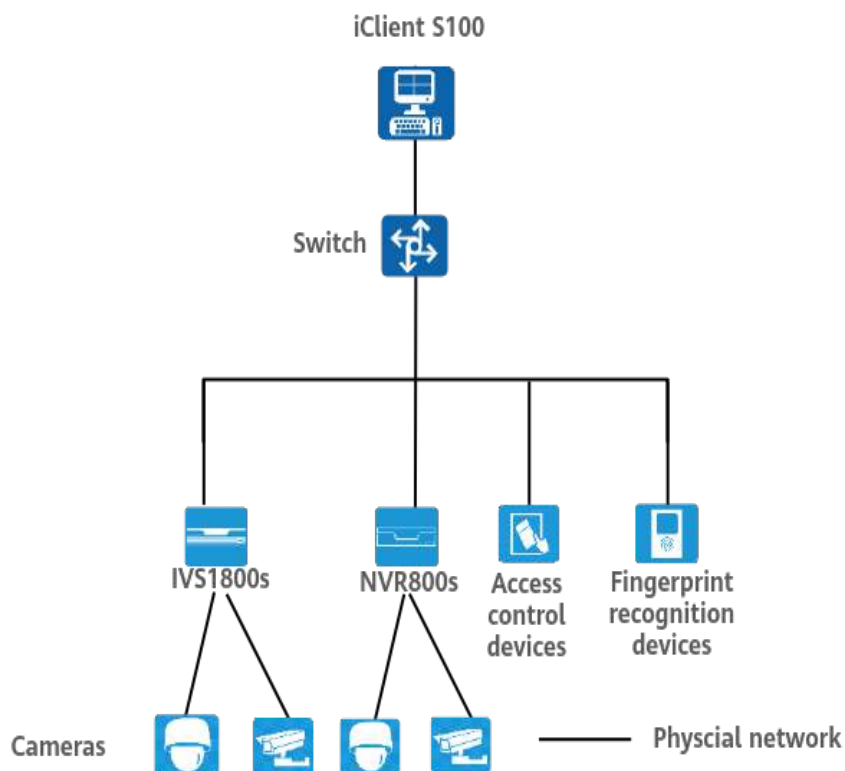
Figure 2-1 Home page of the iClient S100 client

Product Highlights

- Capability building
 - Supports concurrent access of multiple main devices (IVS1800s and NVR800s).
 - Supports connection to a maximum of 16 IVS1800s or 64 NVR800s and 1024 cameras in local mode. If both IVS1800s and NVR800s are connected, one IVS1800 is considered as two NVR800s.
 - Manages peripheral devices, such as alarming and access control devices.
 - Supports video decoding and viewing on the video wall, and centrally manages messages and alarms.
 - Supports personnel, access control, and attendance management.
 - Supports the alarm center.
- Closed-loop intelligence
 - Supports analysis over eight types of perimeter behavior.
 - Supports target- and vehicle-related intelligent applications.
 - Supports crowd flow analysis.
 - Supports common intelligence for video diagnosis.
 - Supports audio diagnosis.

2.2 Typical Network

Figure 2-2 shows the typical network of the iClient S100.

Figure 2-2 Typical network of the iClient S100

- An iClient S100 system consists of one server and multiple clients. You can install the iClient S100 in **Server+Client** or **Client** mode. [Table 2-1](#) describes the installation modes.
- You can directly add the IVS1800s and NVR800s to the local system, configure video services, and perform video-related operations on the devices connected to the iClient S100.

NOTE

If both the NVR800 and IVS1800 are connected to the iClient S100 through local network:

- You are advised to connect the NVR800 and IVS1800 directly to the iClient S100, instead of connecting the NVR800-connected IVS1800 to the iClient S100.
- You cannot directly connect an NVR800 to an IVS1800 on the iClient S100. Configure the upper-lower level cascading of an NVR800 and IVS1800 in the web system of the NVR800.

Table 2-1 Installation modes

Installation Mode	Scenario and Restrictions
Server+Client	• One iClient S100 server must be installed in an iClient S100 system. • When only one client is required for service configuration and operations, you only need to complete the installation in this mode. • In this mode, you can enter the local IP address 127.0.0.1 to log in to the local iClient S100 server, or enter the IP address of another iClient S100 server to log in to that server.
Client	• To configure and operate multiple clients, you need to install the iClient S100 in Server+Client mode on the local computer and install it in Client mode on other computers. • Currently, an iClient S100 server can connect to a maximum of 16 clients (including the clients installed on the computer in Server+Client mode). • To log in this mode, enter the IP address of the computer where the server is located.

2.3 Cable Connections for Access Control Devices

NOTE

Only some devices have the cable ports shown in the following figures. The cable ports vary depending on devices. The ones shown in the following figure are for reference only.

Figure 2-3 Tablet

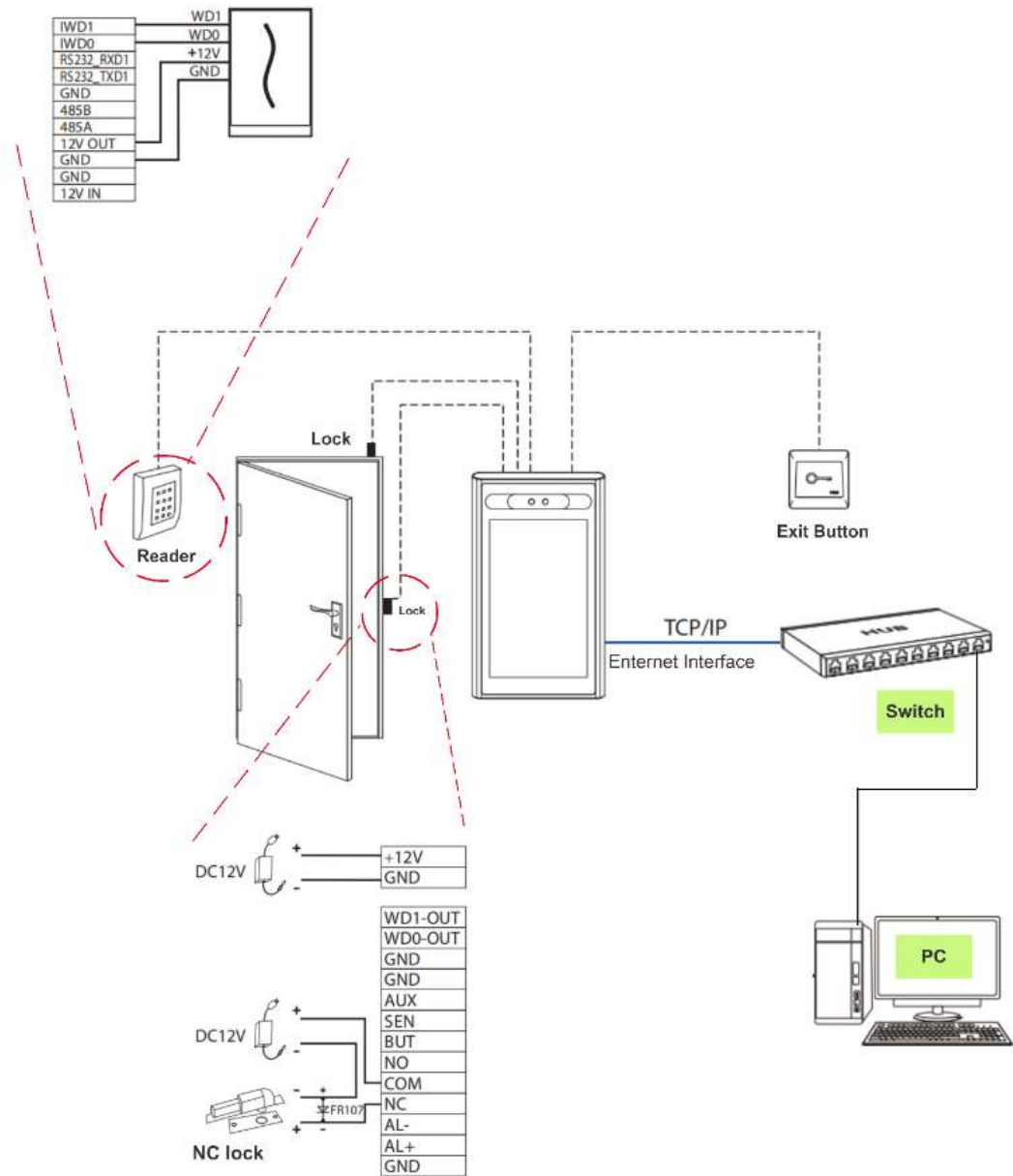


Figure 2-4 Access controller

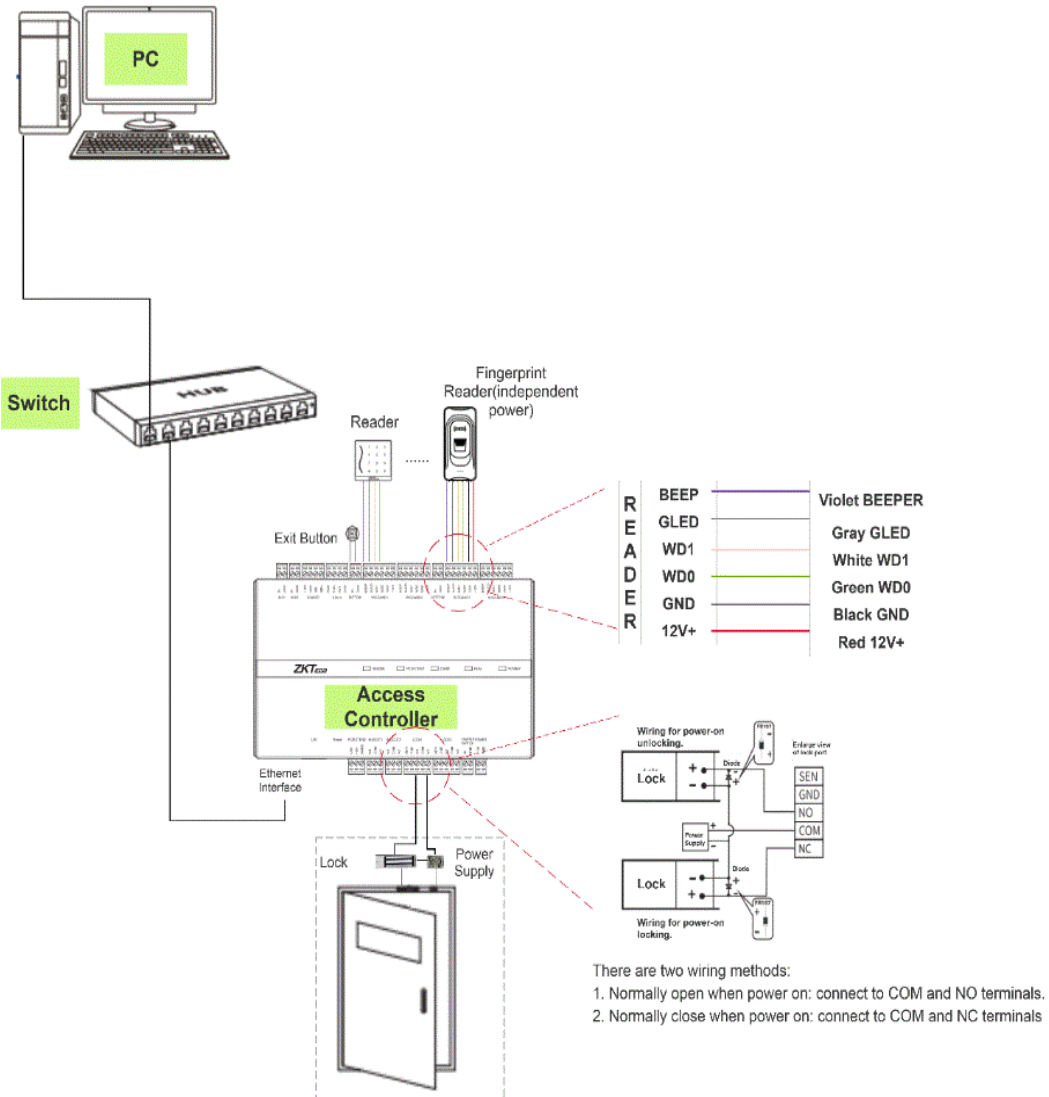
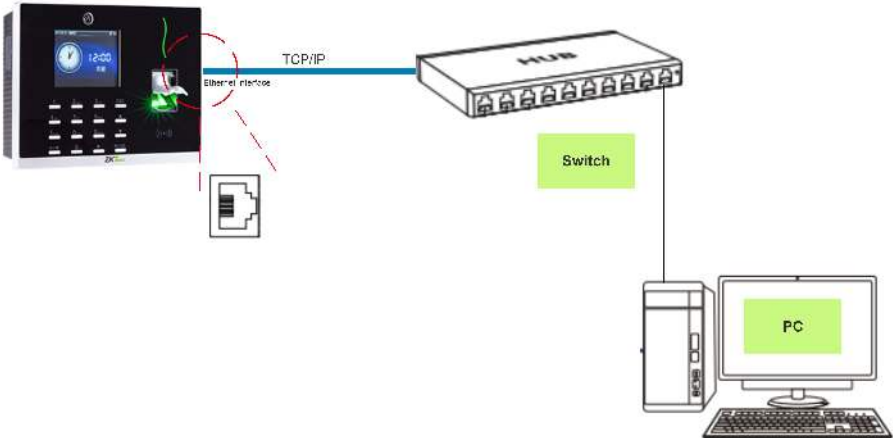


Figure 2-5 Attendance device



3 Installation and Login

[3.1 Operating Environmental Requirements](#)

[3.2 Installing the iClient S100](#)

[3.3 Logging In to the iClient S100](#)

[3.4 Home Page Layout](#)

3.1 Operating Environmental Requirements

Table 3-1 Configuration requirements

Type	Minimum Configuration	Recommended Configuration
CPU	Intel i5-6600	Intel Core i7-8700 or later
Available memory	8 GB	At least 16 GB (DDR4 1600 MHz or higher)
Hard disk	500 GB (adjusted based on the size of the local recording and snapshot storage space) and 15 GB available system disk space	At least 500 GB (adjusted based on the size of the local recording and snapshot storage space) and at least 15 GB available system disk space
Operating system	64-bit Windows 7 Professional and 64-bit Windows 10	64-bit Windows 10
Graphics card	Intel integrated graphics card with a video RAM of 2.0 GB (Intel® HD Graphics 530 or higher is recommended.)	Intel integrated graphics card with a video RAM of more than 2.0 GB (Intel® HD Graphics 620 or higher is recommended.)
Network adapter	One 1000 Mbit/s network adapter	At least one 1000 Mbit/s network adapter

Type	Minimum Configuration	Recommended Configuration
Monitor	To ensure the display effect, you are advised to use a monitor of at least 22 inches, and set the resolution to 1920 x 1080 pixels and aspect ratio to 100%.	To ensure the display effect, you are advised to use a monitor of at least 22 inches, and set the resolution to 1920 x 1080 pixels and aspect ratio to 100%.
System time and time zone	The system time and time zone of the computer running the server and clients must be the same as those of the main device (NVR800/IVS1800). You can set the system time and time zone on the computer under Start > Control Panel > Clock, Language, and Region .	

NOTE

- The system cannot run in the following environments (not supported if any of the following conditions is met):
 - Operating systems running as VMs
 - Operating systems except Windows 7 and Windows 10
 - Computer memory being less than 8 GB
 - System disks whose available space is less than 2 GB
 - Operating systems except Microsoft official ones
- The system cannot be installed in the following environments (not supported if any of the following conditions is met):
 - Operating systems whose users are not administrators
 - 32-bit operating system
- All export and import functions can be used only when the Office Excel has been installed with a license activated and runs properly.

Table 3-2 describes the number of live video channels supported under different configurations.

- Configuration A: i5-6600 CPU @3.10 GHz; memory: 8 GB; 64-bit Windows 7 Professional; integrated graphics card: Intel® HD Graphics 530.
- Configuration B: i7-6700 CPU @3.2 GHz; memory: 16 GB; 64-bit Windows 10 Professional (subversion: 17763); integrated graphics card: Intel® HD Graphics 530.
- Configuration C: i7-8700 CPU @3.2 GHz; memory: 16 GB; 64-bit Windows 10 Professional (subversion: 17763); integrated graphics card: Intel® UHD Graphics 630.

Table 3-2 Number of live video channels supported by the client

Resolution	Configurati on A (H. 264)	Configurati on A (H. 265)	Configurati on B (H. 264)	Configurati on B (H. 265)	Configurati on C (H. 264)	Configurati on C (H. 265)
CIF (512 Kbit/s)	38	38	60	42	64	60

Resolution	Configurati on A (H. 264)	Configurati on A (H. 265)	Configurati on B (H. 264)	Configurati on B (H. 265)	Configurati on C (H. 264)	Configurati on C (H. 265)
4CIF/D1 (1 Mbit/s)	22	22	45	36	50	45
720p (2 Mbit/s at 25 fps)	10	10	16	14	34	30
1080p (4 Mbit/s at 25 fps)	6	6	14	10	20	14
3840 x 2160 (12 Mbit/s at 25 fps)	1	1	3	1	4	4

3.2 Installing the iClient S100

NOTICE

To ensure that new functions can be properly used on each client in the iClient S100 system, you need to upgrade the software versions of the server and all clients in the system at the same time.

For the iClient S100 of V1.3.0 and later versions, the client version must be the same as the server version. Otherwise, the client cannot access the server.

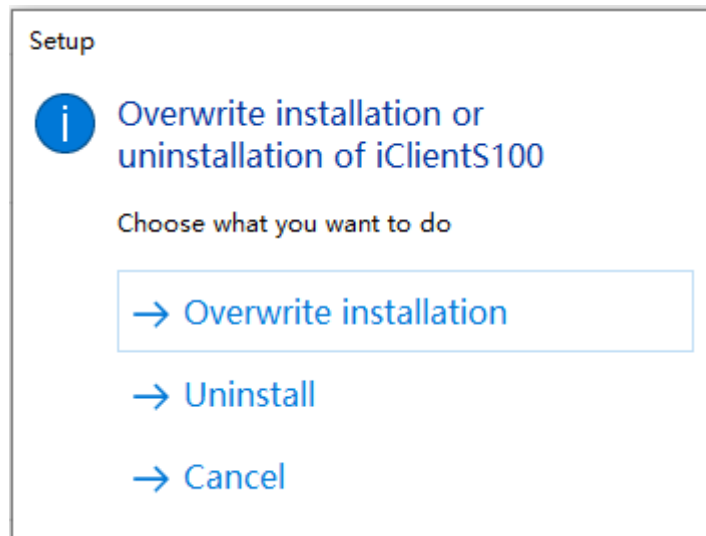
Step 1 You can download the iClient S100 installation package to the local computer.

NOTE

- You are advised to disable the installed or Windows OS-provided antivirus software on the computer before installation, to prevent environment check failures. You can ignore any antivirus software exceptions detected during the environment check.
- The check takes several seconds after you run an application.

Step 2 Right-click the client installation program and choose **Run as administrator** from the shortcut menu. Select a language and click **OK**.

Step 3 (Optional) Click **Overwrite installation** or **Uninstall** when the system detects that the iClient S100 client has been installed on the computer, as shown in [Figure 3-1](#). (This step is not required for first installation.)

Figure 3-1 Overwrite installation or uninstallation of iClient S100

1. Click **Overwrite installation**. Then, go to the next step. For details, see [Step 5](#).
2. Click **Uninstall** and uninstall the original iClient S100 as prompted. After the uninstallation, the environment check automatically starts. Then, go to the next step. For details, see [Step 4](#).

NOTE

You are advised to choose **Overwrite installation**, in which case devices (including their configurations) added and basic configurations set on the previous iClient S100 will be retained.

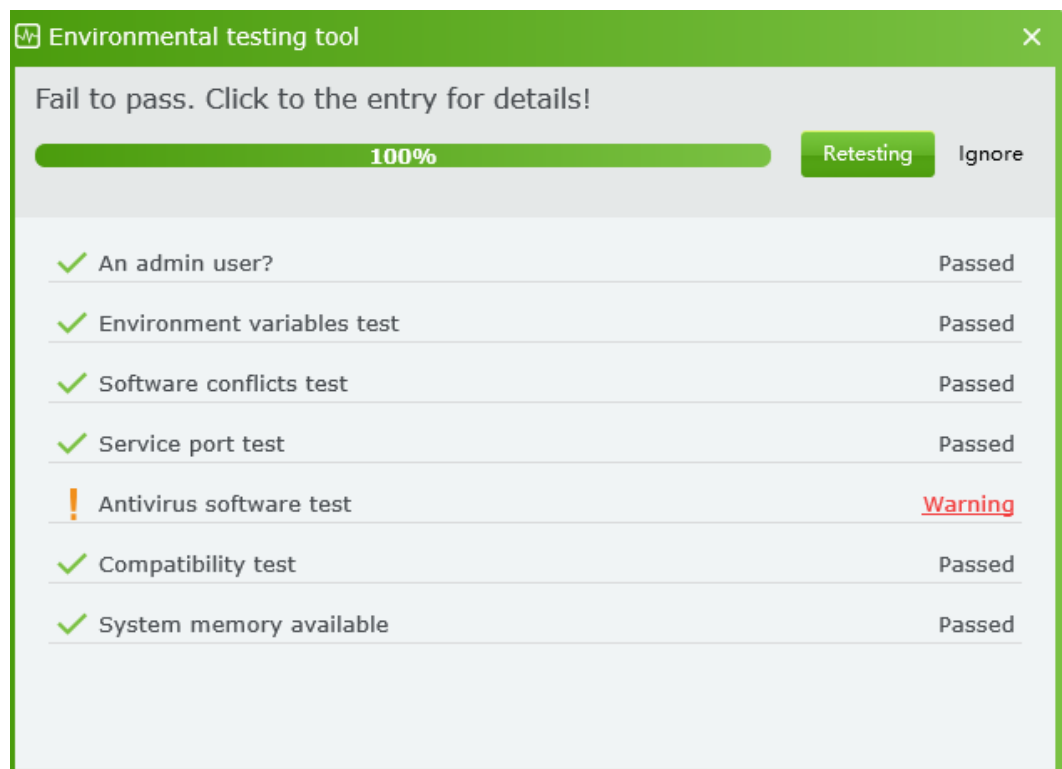
Step 4 Check whether any exception is detected during the environment check.

The check takes several seconds after you run an application (here specified by **Environmental testing tool**).

- If no exception is detected, click **Continue**.
- If any exception is detected, the message "Fail to pass. Click to the entry for details!" is displayed, as shown in [Figure 3-2](#). You can rectify the exception as prompted. After the rectification, perform the environment check again. When all check items are passed, go to the next step.

NOTE

Messages displayed in [Figure 3-2](#) indicate that antivirus software is detected on the local computer, which may cause an installation failure. You are advised to disable the antivirus software before installation, or click **Ignore** to finish the installation progress.

Figure 3-2 Environmental testing tool

Step 5 Select an installation mode (for example, click **Server+Client**), and click **Next**.

Installation modes include the **Server+Client** mode and the **Client** mode. You can select a mode based on the site requirements. For details, see [Table 2-1](#).

Step 6 Select **I accept this agreement (A)** and click **Next**.

After you click **Next** during overwrite installation, the port number and installation path of the server remain unchanged and you will be redirect to [Step 9](#).

Step 7 Set related parameters, for example, the server port, and click **Next**.

NOTE

- By default, the value of **Web Port** and **Adms Port** is **8098** and **8088**, respectively.
If the port is occupied, manually change the port number. Use a port number that is not in use and that is not the database port number **5442** or Redis port number **6390**, **21**, or **80**.
- Select **Add firewall exceptions for this port** to prevent the Windows firewall from blocking the program.

Step 8 Configure the installation directory and click **Next**.

NOTE

The default installation path is **C:\Program Files\iClient S100**. You can also click **Browse** to specify an installation path. Ensure that the selected installation path has sufficient disk space as prompted.

Step 9 Configure the path for saving the backup file and click **Next**.

 NOTE

By default, the system scans all disks, locates the disk with the largest available space, and creates the **SecurityDBBack** directory. You can also click **Browse** to specify a path for storing backup files.

Step 10 Select the components to be installed and used and click **Next**.

 NOTE

Video and personnel components are installed by default, and other components are installed according to the use requirements.

Step 11 Click **Install** to install the software.

Step 12 A message is displayed at the end of installation, asking whether to restart the computer immediately (the default option is **Yes**). If **Yes** is selected, click **Finish** and restart the computer to complete the installation.

 NOTE

- After the software is installed, you need to wait for about 2 minutes until all services start.
- If the computer running the server has two network adapters, you need to set the service IP address on the server based to the site requirements. For details, see [8.1.2.4 How Do I Set the Server IP Address When the Computer Running the iClient S100 Server Has Two Network Adapters?](#).

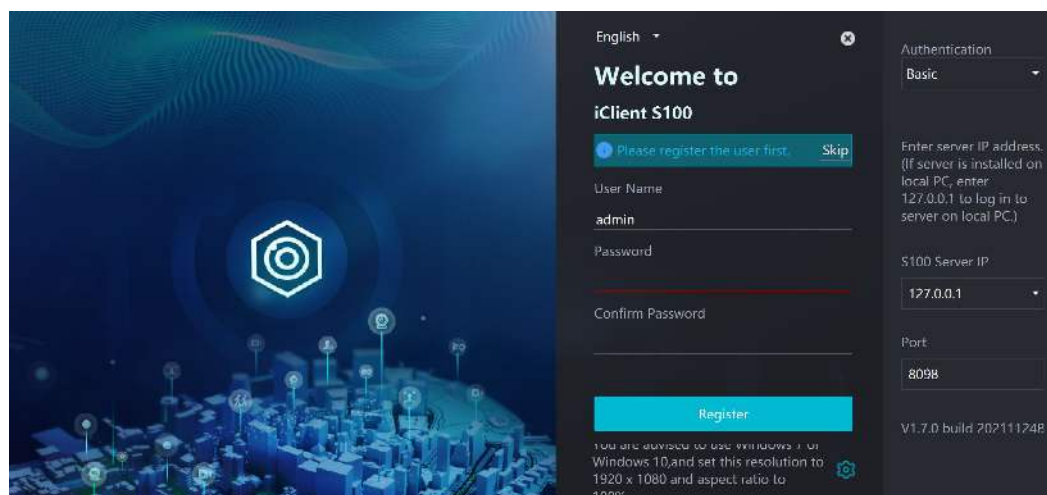
----End

3.3 Logging In to the iClient S100

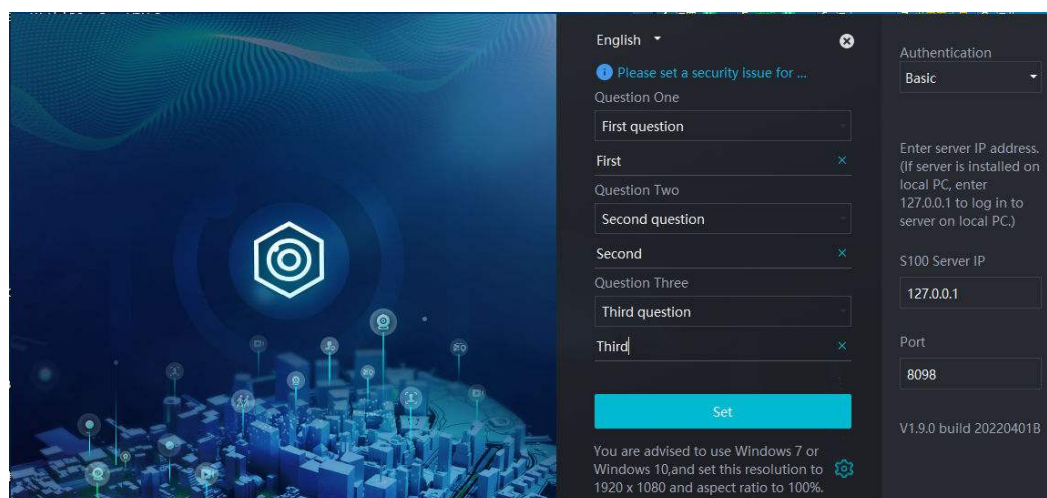
Step 1 Start the iClient S100.

- On Windows 7, double-click the client icon. The client login page is displayed.
- On Windows 10, right-click the client icon, choose **Properties** from the shortcut menu, click the **Compatibility** tab, select **Run this program as an administrator**, and click **OK**. Then double-click the client icon on the desktop. The client login page is displayed.

Step 2 The password of the admin account must be set upon the first login, as shown in [Figure 3-3](#).

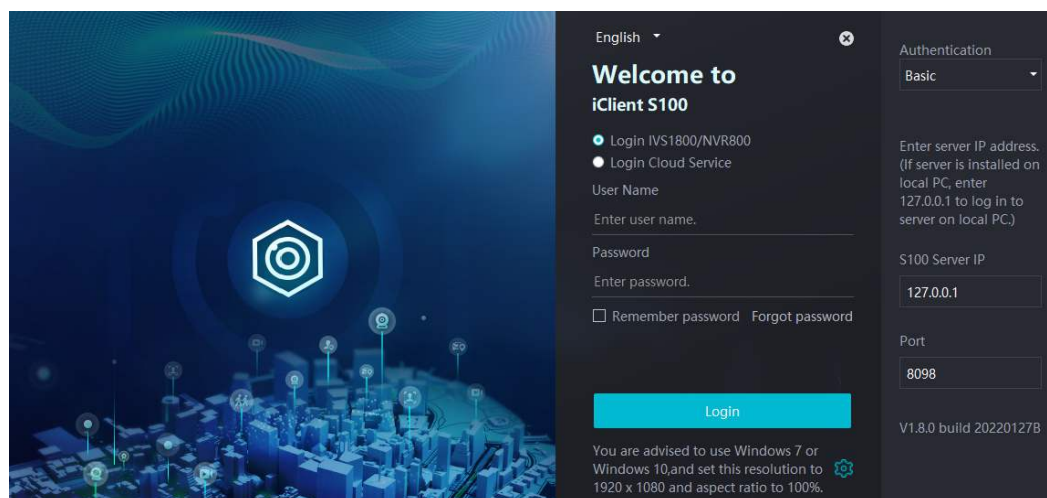
Figure 3-3 register user account

iClient S100 retrieves the password by setting the security problem. After the initialization of admin account, enter the password retrieval parameter setting window, as shown in the figure. After entering the security question and answer, click the "setting" button to complete the setting.

Figure 3-4 Setting Password Retrieval Parameters

After the admin account is initialized, the system automatically logs in to the system as the admin account.

Step 3 Scenarios that are not the first login, On the login page shown in [Figure 3-5](#), set login parameters by referring to [Table 3-3](#) and click **Login**.

Figure 3-5 iClient S100 login page**Table 3-3** Parameter/Button description

Parameter/ Button	Description
Chinese/ English	Language to be displayed on the iClient S100.
User Name/ Password	User name and password of the administrator (admin and Changeme_123 respectively by default) or new users (customized name and password, or customized name and Changeme_123 by default, respectively) for logging in to the iClient S100. For details about how to add a user, see Comprehensive Services > Authority Management > Adding a User. NOTE - The system prompts you to change the password at the first login. - You can click  to clear the password. You can also hold the mouse button down on  to display the current password.
Remember password	Indicates whether to save the password corresponding to the user name (automatically saved by default) you used to log in to the iClient S100 last time.
Forgot password	Button for password retrieval. If you have bound your account to an email address, you can retrieve your password using the email address. For details about how to bind an email address, see Comprehensive Services > Authority Management > Adding a User. For details about how to set email parameters, see FAQ > Comprehensive Services > Basic Operations > How to Configure Support for Sending Emails?.

Parameter/ Button	Description
Authentication	Basic: Use the default user admin or a new user to log in. This is the most common login method.
Login IVS1800 / NVR800	After logging in, you can manage ivs1800 and nvr800 devices in offline LAN.
Login Cloud services	After logging in, you can manage the devices on Haowang cloud.
Port	Port number set in Step 7 when the server is installed. The default value is 8098 . If NAT has been configured, the port number is a post-NAT port number.
S100 Server IP	• If the Server+Client mode is enabled during the installation: – Enter the local IP address 127.0.0.1 to use the local server. – Enter the IP address of the computer where other servers are located to log in to the servers. • If the Client mode is enabled during the installation: Enter the IP address of the computer where the server to be connected is located. CAUTION Ensure that the computer where the iClient S100 server is installed is powered on and the network is normal. Otherwise, the client will fail to log in to the server.

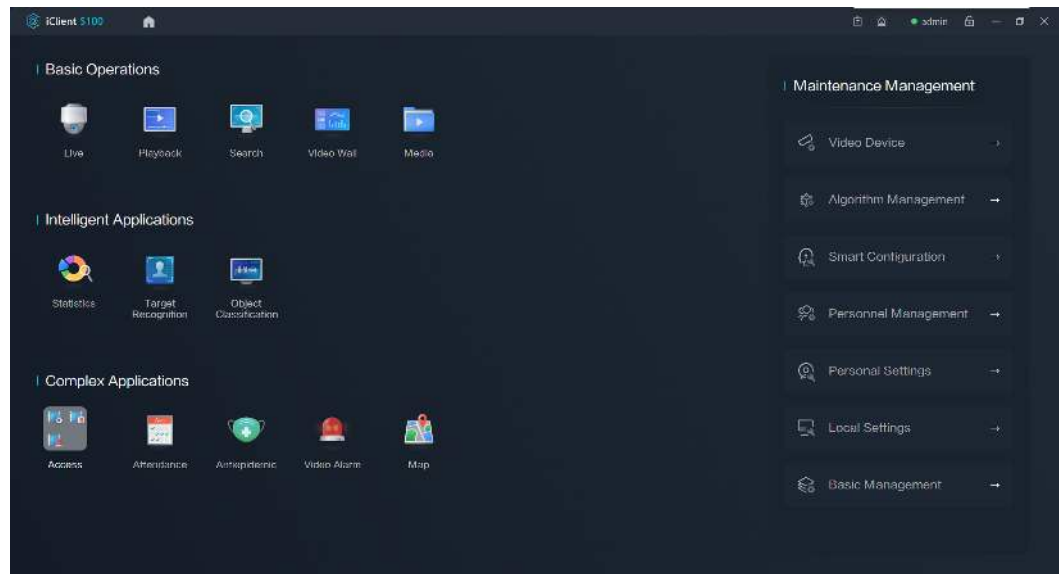
----End

3.4 Home Page Layout

Figure 3-6 shows the home page of the iClient S100 client. **Table 3-4** describes the icons on the home page. The function tabs on the home page are subject to the actual login environment.

NOTE

The client layout shown in the following figure is for reference only.

Figure 3-6 Home page of the iClient S100 client for local mode**Table 3-4** Icon description

Icon	Description
	Views the weak prompts of various operations. For example, if a message is displayed when an operation fails, the system places the message in the toast message area. You can view the historical message.
	Views various alarms generated by the system.

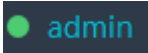
Icon	Description
	• Status indicator of the iClient S100 client. The status indicator can be steady green, steady yellow, or steady red. – Steady green: When the iClient S100 client is running properly, the status indicator is steady green. – Steady yellow: When the CPU or memory usage of the iClient S100 client reaches 70%, the status indicator is steady yellow. – Steady red: When the iClient S100 client CPU usage reaches 85% or the memory usage reaches 80%, or when the CPU or memory usage of the iClient S100 client exceeds the threshold, the status indicator is steady red. • When only I-frames are decoded (the video image is not smooth), the status indicator is steady red. • You can click this icon to log out of the current user, change the current user's password, view client version information, or open the <i>Help Document</i>. NOTE You can also open the help document under the iClient S100 installation path, for example, C:\Program Files\iClient S100\iClientS100\Help.
	You can lock the screen in either of the following ways: • Click this icon to lock the screen immediately. • Choose Maintenance Management > Local Settings and set Auto-Lock Time (min). If no operation is performed within the configured interval, the screen is automatically locked. NOTE • If you enter incorrect passwords for five consecutive times, the account will be locked for 5 minutes. After 5 minutes, you can enter the password to log in again. • If you forget the password for unlocking the screen or attempt to switch to the other mode, you can click Re-log In to go to the login page and log in again. • The screen locking password is the same as the login password.

Table 3-5 describes the shortcut keys on the iClient S100 client home page.

Table 3-5 Shortcut keys

Shortcut Key	Operation
Alt+1	Opens or switches to the Live tab page.

Shortcut Key	Operation
Alt+2	Opens or switches to the Playback tab page.
Ctrl+W	Closes the current tab page.

4 Video Service Management (for NVR800)

- 4.1 Device Access
- 4.2 Video Viewing
- 4.3 Recording
- 4.4 Video Wall
- 4.5 Common Intelligence
- 4.6 Behavior Analysis
- 4.7 Intelligent target Analysis
- 4.8 Person Intelligence
- 4.9 Situation Analysis
- 4.10 Vehicle Intelligence
- 4.11 Third-Party Algorithms
- 4.12 Alarm Management

4.1 Device Access

4.1.1 Application Scenario

This section describes how to connect and manage NVR800s and cameras connected to the NVR800s on the iClient S100 client. You can centrally manage the connected devices on the iClient S100 client, for example, viewing live video and recordings from the cameras. **Figure 4-1** shows the specific scenario.

- A maximum of 64 NVR800s can be added to an iClient S100 client.
- Cameras can be added to an NVR800 connected to the iClient S100 client. **Table 4-1** lists the supported connection modes and protocols.

- iClient S100 clients can be connected to the upper-level platform, for example, IVS3800 or IVS1800, through the NVR800 web page on the iClient S100 client.

 NOTE

- You can configure the connection between the NVR800 and an upper-level platform on the LDU or NVR800 web page. For details about how to configure the connection, see the *NVR800 User Guide*.
- To switch to the NVR800 web page on the iClient S100, perform the following operations:

Choose **Maintenance Management > Video Device > Device List > Main Devices**, right-click an NVR800, and choose **Maintenance**.

Figure 4-1 Device connection scenario

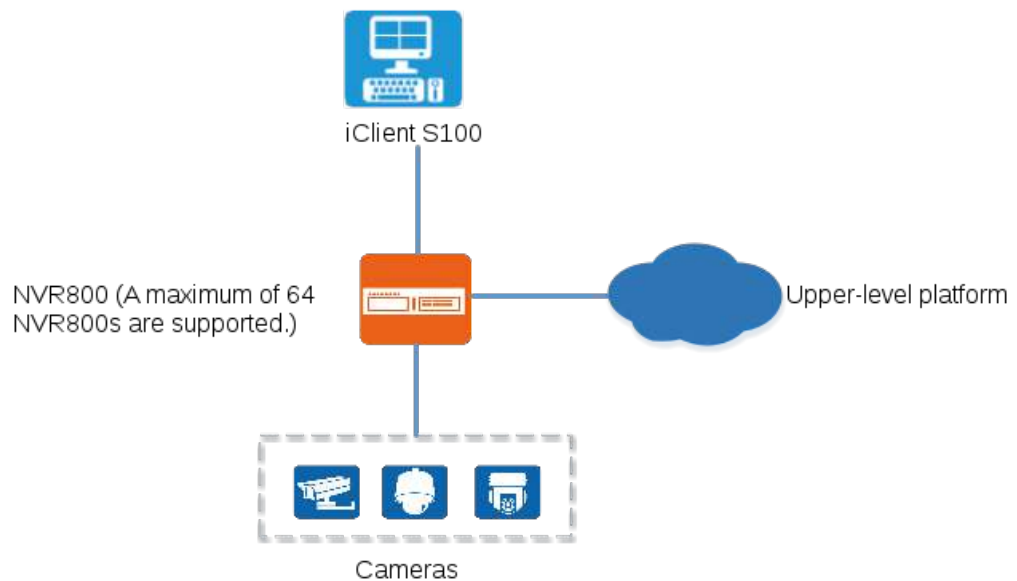


Table 4-1 Camera connection modes

Connection Mode	Application Scenario	Supported Protocol
Automatically adding cameras in batches (recommended)	If a large number of online cameras that support HWS SDK or ONVIF need to connect to the NVR800, you can configure the mode for automatically adding cameras in batches. In this mode, only online cameras can be automatically added in batches, and the camera IP addresses do not need to be specified. This method applies to scenarios where a large number of cameras need to be added. Compared with the method of manually adding cameras in batches, this method enables quicker camera access. However, this method cannot be used to add offline cameras.	HWS SDK and ONVIF NOTE - A camera can be connected to an NVR800 on the iClient S100 client only through HWS SDK in passive registration. That is, the NVR800 proactively initiates a connection request to the camera. After receiving the request, the camera connects to the NVR800. - You are advised to connect cameras to an NVR800 through HWS SDK for the configuration and operation of intelligent services. ONVIF allows only configuration and operation of non-intelligent services such as live video viewing and recording playback.
Manually adding cameras in batches	If IP addresses have been planned for a large number of cameras and the cameras need to be connected to the NVR800, you can manually add the cameras in batches.	
Manually adding cameras one by one	If only a few cameras need to be connected to the NVR800, you can add the cameras one by one.	

4.1.2 Device Connection

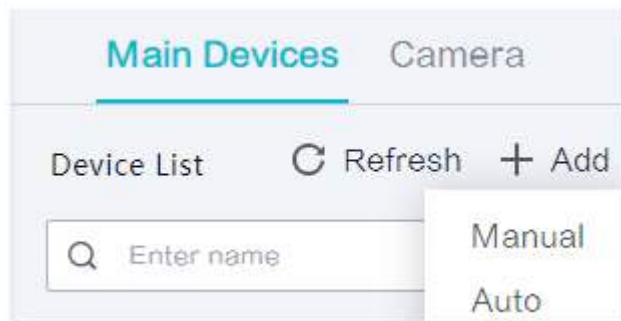
4.1.2.1 Adding NVR800s

You can add a maximum of 64 NVR800s and connect a maximum of 1024 video channels (including the video channels connected to the NVR800s) to an iClient S100 server. This section describes the procedure for adding NVR800s to an iClient S100 server.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Click **Add** in the upper left corner and select **Manual** or **Auto** as required, as shown in [4.1.2.1 Adding NVR800s](#).

Figure 4-2 Adding a main device



- [Figure 4-3](#) shows the page for adding a main device manually. [Table 4-2](#) describes the parameters. Set the parameters as prompted and click **OK**.

Figure 4-3 Manually adding an NVR800

New Device [X]

Device Type
NVR800

Name
NVR800-1

Address
192.168.0.10

Port
443

User Name
apiadmin

Password
[Masked Password]

OK Cancel

Table 4-2 Parameters for adding an NVR800

Parameter	Description
Device Type	A drop-down list for adding a new device. Select the desired type of a device (here specified by NVR800) to be added.
Device Name	User-defined device name.
Address	IP address of the NVR800 to be added. The address is in xxx.xxx.xxx.xxx format, for example, 192.168.10.1 .

Parameter	Description
Port	Port number of the NVR800 to be added. The default port number is 443 .
User Name	- User name and password of the NVR800. You are advised to use the apiadmin user on the NVR800 for interconnection only. If another user is used, personnel information will fail to be delivered to the device due to insufficient permissions. - After an NVR800 is connected to the iClient S100, if its password is changed on the NVR800, it goes offline on the iClient S100. In this case, you can update the password of the NVR800 on the iClient S100 and it will go online again. NOTE To connect the same NVR800 to different iClient S100 servers, you need to create multiple users on the NVR800. - Configuration path on the NVR800 LDU: Settings > System > Multi-user Management - Configuration path in the NVR800 web system: Remote Settings > System > Multi-user Management
Password	

- After you click **Auto**, the system searches for NVR800s in the same subnet as the iClient S100 server. Then, enter the user name and password to verify and connect to the devices. If the user names and passwords of multiple devices are the same, you can verify them in batches. **Figure 4-4** shows the page for automatically connecting to an NVR800.

Figure 4-4 Automatically connecting to an NVR800

Automatically Found Device(s)

Tip: the iClient S100 server must be in the same subnet as the searched device, and ensure that ports 9333 and 32902 of the iClient S100 server is not blocked by the firewall. It's recommended to close the firewall. To activate the device in batches, the default user name is admin, no need to configure the user name, just enter the password to activate.

User Name: Password:

Current progress 100% Search Again

☒ Filter out added devices

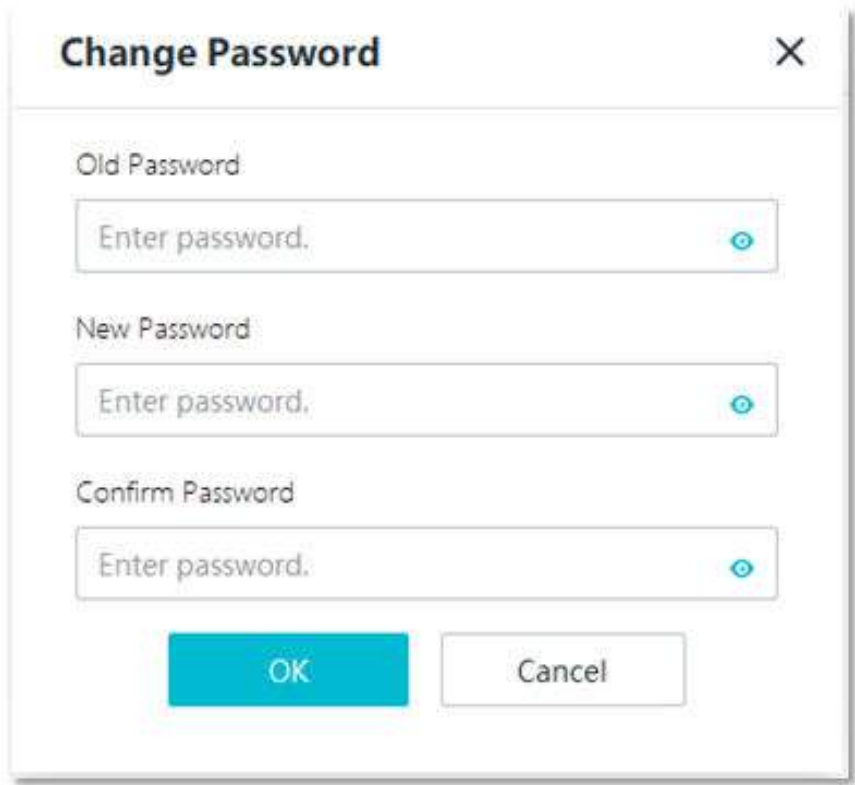
No.	IP Address	MAC	Version	Device Name	Port	User Name	Password	Status
48	192.168.3.111	843E92F366A2	IVS-B	192.168.3.111	10531	admin		Access
49	90.85.60.41	843E92F366AD	IVS-B	90.85.60.41	10531	admin		Access
50	90.85.58.111	843E92F36688	IVS-B	90.85.58.111	10531	admin		Access
51	90.85.59.89	50464A8C2C92	IVS-B	90.85.59.89	10531	admin		Access
52	90.85.60.112	1C3D2FAD2C03	IVS-B	90.85.60.112	10531	admin		Access
53	90.85.51.102	843E92F366C8	IVS-B	90.85.51.102	10531	admin		Access
54	90.85.58.90	843E9210C1A6	IVS-B	90.85.58.90	10531	admin		Access

Batch Access Batch Activate Cancel

- Step 3 Optional:** When verifying devices, if a user account is used for logging in to an NVR800 for the first time, a dialog box is displayed prompting you to change the original password, as shown in **Figure 4-5**.

Enter and confirm passwords as prompted, and click **OK**. The NVR800 is displayed in the **Device List**, indicating successful access. If you click **Cancel**, the NVR800 fails to be added. In this case, you need to perform the preceding steps again to add an NVR800.

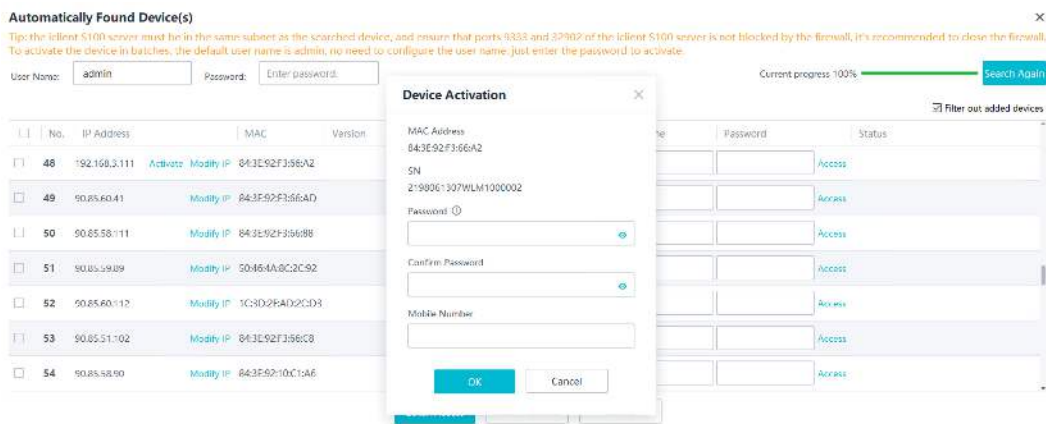
Figure 4-5 Change Password



The 'Change Password' dialog box contains three password input fields labeled 'Old Password', 'New Password', and 'Confirm Password'. Each field has a placeholder text 'Enter password.' and a toggle icon on the right. At the bottom, there are 'OK' and 'Cancel' buttons.

Step 4 If the nvr800 is a new and inactive device, click the activate button on the searched device list to activate the device.

Figure 4-6



The 'Device Activation' dialog box is shown over a background of a device list. The dialog box contains the following fields: 'MAC Address' (843E92F356A2), 'SN' (2199061307WLM1000002), 'Password' (with a toggle icon), 'Confirm Password' (with a toggle icon), and 'Mobile Number'. At the bottom are 'OK' and 'Cancel' buttons. The background shows a table of devices with columns for No., IP Address, MAC, and Version, and buttons for 'Activate' and 'Modify IP'.

Step 5 If you need to modify the IP of NVR equipment, you can click the modify IP button to modify the IP.

Figure 4-7

Modify IP-related Parameters ✕

Tip: After modifying the IP successfully, it will take effect in about 2 minutes.

Destination MAC Address
84:3E:92:F3:66:A2

SN
2198061307WLM1000002

Destination IP Address

Subnet Mask

Gateway Address

DNS 1

DNS 2

----End

4.1.2.2 Adding Cameras on the NVR800

4.1.2.2.1 Automatically Adding Cameras in Batches (Recommended)

This section describes the procedure for automatically adding cameras in batches on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Select a desired NVR800 to which the cameras to be added are mounted and click **Add** in the upper right corner of the page. Alternatively, right-click the NVR800

and choose **Camera Access** from the shortcut menu. The **Device Access** tab page is displayed.

Step 3 Select **Auto Batch Access (Recommended)** and click **Start**.

Step 4 Search for cameras by IP address.

1. Select the driver supported by the device, that is, the protocol for connecting cameras (HWSDK or ONVIF, with HWSDK recommended).
2. Click **Add Network Segment** and enter the start and end IP addresses of cameras.

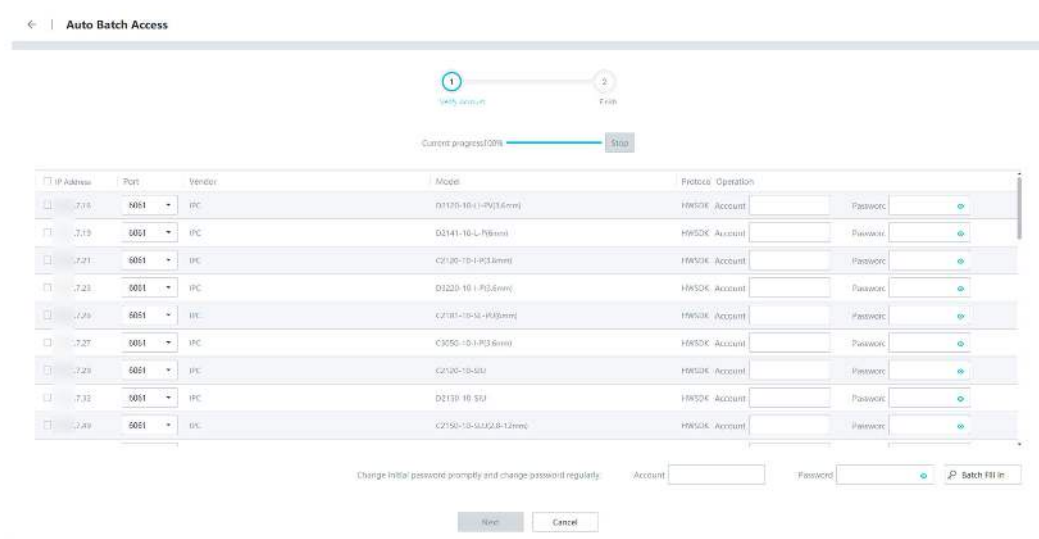
NOTE

- It is recommended that you specify a proper network segment to shorten the search time.
 - If a network segment is set, the system searches this network segment for cameras in unicast mode. You can set multiple network segments so that you can search multiple VLANs for cameras.
 - If you do not set a network segment, the system searches for cameras in broadcast mode. In this case, the system can only search for cameras located on the same network segment as the IP address of the local server. You are advised to search for cameras by network segment or add cameras in batches.
3. Click **Next** to search for cameras.
 4. (Optional) Click **Stop** to stop the search.

Step 5 Select the cameras to be added and enter the user names and passwords of the cameras. (The user name and password of a camera are the registration user name and password of the camera.)

- If the user names and passwords of the cameras are different, enter the user name and password of each camera line by line.
- If the user names and passwords of the cameras are the same, you are advised to enter the user names and passwords in batches. (Enter the user names and passwords in the lower right corner and click **Batch Fill in**, as shown in [Figure 4-8](#).)

Figure 4-8 Verifying accounts



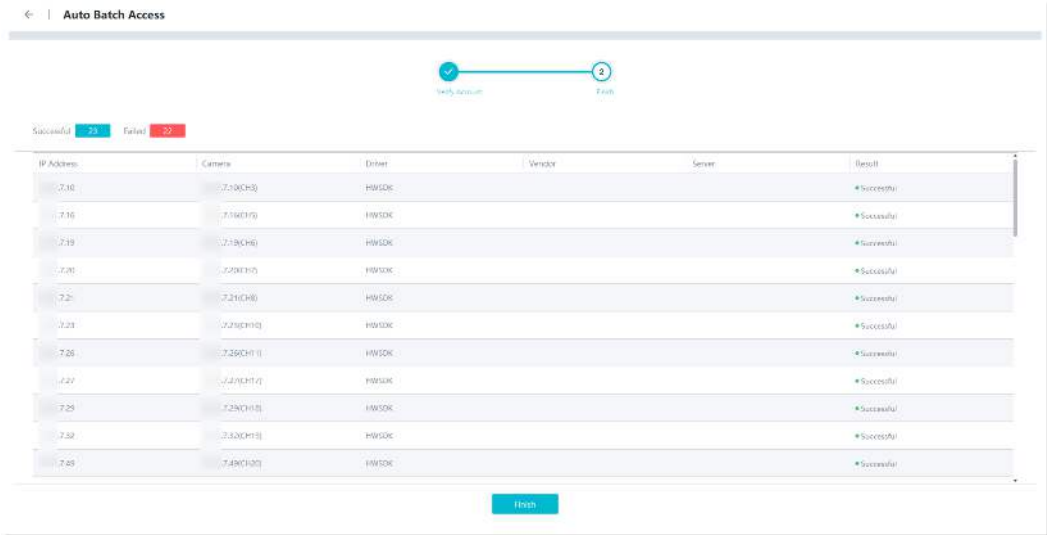
The screenshot shows the 'Auto Batch Access' window. At the top, there is a progress bar labeled 'Current progress: 20%' with a 'Stop' button. Below the progress bar is a table with the following columns: IP Address, Port, Vendor, Model, Protocol, Operation, Account, and Password. The table contains 8 rows of camera data. At the bottom of the window, there are input fields for 'Account' and 'Password', a 'Batch Fill in' button, and a 'Cancel' button.

IP Address	Port	Vendor	Model	Protocol	Operation	Account	Password
1.1.1.1	8081	IPC	D1119-16 (1-P)16mm	HWSDK	Account		Password
1.1.1.2	8081	IPC	D3141-16 L-P16mm	HWSDK	Account		Password
1.1.1.3	8081	IPC	C2120-16 (1-P)16mm	HWSDK	Account		Password
1.1.1.4	8081	IPC	D1220-16 (1-P)16mm	HWSDK	Account		Password
1.1.1.5	8081	IPC	C2181-16 (1-P)16mm	HWSDK	Account		Password
1.1.1.6	8081	IPC	C3050-16 (1-P)16mm	HWSDK	Account		Password
1.1.1.7	8081	IPC	C2120-16 (1-P)16mm	HWSDK	Account		Password
1.1.1.8	8081	IPC	D2119-16 (1-P)16mm	HWSDK	Account		Password

Change initial password promptly and change password regularly: Account Password

Step 6 Click **Next**. The system starts to add cameras. The result is displayed, as shown in [Figure 4-9](#).

Figure 4-9 Camera adding result



Step 7 Click **Finish**.

Step 8 For details about follow-up configurations, see [Table 4-3](#).

Table 4-3 Follow-up configurations

Scenario	Where to Configure	Configuration
Adding cameras through ONVIF	Camera web system	Set parameters for camera access. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0283977334.xml.
Adding cameras to a group	Maintenance Management > Video Device > Group Device	Add cameras to a group to facilitate camera management.
Adjust Area	Maintenance Management > Video Device > Device List	Select one or multiple cameras and click  Adjust Area to adjust the area to which the cameras belong on the Main Device or Camera tab page.

-----End

4.1.2.2.2 Manually Adding Devices in Batches

This section describes the procedure for manually adding cameras in batches on the iClient S100.

Procedure

Before adding cameras in batches, you need to complete a system-provided template based on actual requirements. After importing the completed template, you can add cameras in batches on the device management page.

NOTE

The number of cameras to be added in batches using a template cannot exceed the maximum number of cameras supported by an NVR800. Otherwise, the excess cameras will fail to be added.

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Select a desired NVR800 to which the cameras to be added are mounted and click **Add** in the upper right corner of the page. Alternatively, right-click the NVR800 and choose **Camera Access** from the shortcut menu. The **Device Access** tab page is displayed.
- Step 3** Select **Manual Batch Access** and click **Start**.
- Step 4** Click **Download Template** to download the **Device Batch Import.xlsx** file to the local computer.
- Step 5** Open the **Device Batch Import.xlsx** file and fill in required sheets in the file by referring to [Table 4-4](#) and [Table 4-5](#).

NOTE

In [Table 4-4](#), **M** indicates mandatory, **O** indicates optional, and - indicates not required or involved.

Table 4-4 Parameters in the batch import template

Parameter	HWSDK (Recommended)	ONVIF
Camera Name	M	M
Vendor	M	O
Device Form Type	M	M
Device Model	O	O
Main Device Code	M	M
IP Address	M	M
Port	M	M
User Name	M	M
Password	M	M

Table 4-5 Parameters in the template for manually adding cameras in batches

Parameter	Description
Camera Name	Camera name to be displayed on the iClient S100. You are advised to enter the camera installation location or observation area.
Vendor	Camera vendor.
Device Form Type	Type of the main camera. Set this parameter to IPC .
Device Model	Actual camera model.
Main Device Code	Obtain the main device code of the current domain from the first sheet in the template.
IP Address	IP address of a camera.
Port	Number of the port for camera access, whose value must be the same as that set on the camera side. You are advised to use the default port number. If the port number is changed on the camera side, set this parameter based on the actual requirements. NOTICE • If the HWSKD protocol is used for registration, set the port number to 6061. Messages are encrypted after the camera is added, improving transmission security. • If you change the port number after a camera is connected, the camera will be disconnected and reconnected within 1–5s. The reconnection duration depends on the network conditions.
User Name/ Password	Registration user name and password used to connect the camera to the NVR800. For cameras, the navigation path of the registration password on the camera web page varies depending on the protocol. • HWSKD: Choose Settings > Network > Platform Connection > Password Management. On the SDK Password tab page, the value of Current password is the registration password. • ONVIF: Choose Settings > Network > Platform Connection > Password Management. On the ONVIF Password tab page, the value of Current password is the registration password.

Step 6 Import the completed template file to the iClient S100. You can click **Browse** and select the file, or drag the file from the local path to the **Drag file here.** area on the **Manual Batch Access** page.

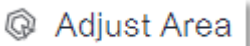
Cameras to be added are displayed on different tab pages based on their protocols.

Step 7 Click **Next**. The camera adding result is displayed.

Step 8 Click **Finish**.

Step 9 For details about follow-up configurations, see [Table 4-6](#).

Table 4-6 Follow-up configurations

Scenario	Where to Configure	Configuration
Adding cameras through ONVIF	Camera web system	Set parameters for camera access. For details, see 4.1.2.3.1 Configuring Connection Through ONVIF in the Camera Web System .
Adding cameras to a group	Maintenance Management > Video Device > Group Device	Add cameras to a group to facilitate camera management.
Adjust Area	Maintenance Management > Video Device > Device List	Select one or multiple cameras and click  Adjust Area to adjust the area to which the cameras belong on the Main Device or Camera tab page.

----End

4.1.2.2.3 Manually Adding a Device

This section describes the procedure for manually adding a camera on the iClient S100.

Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Select a desired NVR800 to which the cameras to be added are mounted and click **Add** in the upper right corner of the page. Alternatively, right-click the NVR800 and choose **Camera Access** from the shortcut menu. The **Device Access** tab page is displayed.

Step 3 Select **Manual Single Access** and click **Start**.

Step 4 Set the parameters for adding a camera. [Table 4-7](#) describes the parameters.

Table 4-7 Parameters for manually adding a camera

Parameter	Description
Device Name	Camera name to be displayed on the iClient S100. You are advised to enter the camera installation location or observation area.
Driver	Protocol through which the camera is connected. NOTE You are advised to connect cameras to an NVR800 through HWSDK for the configuration and operation of intelligent services. ONVIF allows only configuration and operation of non-intelligent services such as live video viewing and recording playback.
Area	Area to which the camera belongs. If no area is specified, the camera belongs to the default area. The value of Area has been configured under Basic Management > Basic Management > Area Settings on the iClient S100. (You can configure an area by referring to "How to Set Up an Area" under FAQs > Comprehensive Services > Basic Operations.) Only users granted permissions of an area can perform operations on devices in the current area.
User Name/ Password	Registration user name and password used to connect the camera to the NVR800. For cameras, the navigation path of the registration password on the camera web page varies depending on the protocol. • HWSDK: Choose Settings > Network > Platform Connection > Password Management. On the SDK Password tab page, the value of Current password is the registration password. • ONVIF: Choose Settings > Network > Platform Connection > Password Management. On the ONVIF Password tab page, the value of Current password is the registration password.
IP Address	IP address of a camera.
Device Login Port	Number of the port for camera access, whose value must be the same as that set on the camera side. You are advised to use the default port number. If the port number is changed on the camera side, set this parameter based on the actual requirements. NOTICE • If the HWSDK protocol is used for registration, set the port number to 6061. Messages are encrypted after the camera is added, improving transmission security. • If you change the port number after a camera is connected, the camera will be disconnected and reconnected within 1–5s. The reconnection duration depends on the network conditions.
Transmission Protocol	When the ONVIF protocol is used to connect cameras, you can set the transmission protocol to HTTP (default), HTTPS, or HTTP/HTTPS.

Step 5 Click **Finish**.

Step 6 For details about follow-up configurations, see [Table 4-8](#).

Table 4-8 Follow-up configurations

Scenario	Where to Configure	Configuration
Adding cameras through ONVIF	Camera web system	Set parameters for camera access. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0283977334.xml.
Adding cameras to a group	Maintenance Management > Video Device > Group Device	Add cameras to a group to facilitate camera management.
Adjust Area	Maintenance Management > Video Device > Device List	Select one or multiple cameras and click  Adjust Area to adjust the area to which the cameras belong on the Main Device or Camera tab page.

----End

4.1.2.3 Connecting Cameras to the NVR800

4.1.2.3.1 Configuring Connection Through ONVIF in the Camera Web System

When the ONVIF protocol is used to connect a camera to the IVS1800/NVR800, you need to set the connection parameters in the camera web system.

Prerequisites

- The ONVIF protocol is used on a trusted network. Otherwise, security risks may exist. The protocol uses MD5 digest authentication. The MD5 algorithm is a weak algorithm, and media streams are not encrypted, which may result in security risks.
- The ONVIF protocol and the IVS1800/NVR800 support the H.265 encoding protocol if the ONVIF protocol needs to use the H.265 encoding protocol. cameras must be of V200R003C10 or later versions. As for the IVS1800/NVR800, contact the vendor to obtain the protocol support information. If the camera or IVS1800/NVR800 does not support H.265, set the encoding protocol (for the primary streams and secondary streams) to H.264 and then set parameters on devices. The detailed procedure is as follows: log in to the camera web system, choose **Settings > Video/Audio/Image > Video**, and set **Encoding protocol** to **H.264**.
- By default, the ONVIF protocol uses the HTTP/HTTPS transmission protocol.
- The ONVIF protocol supports only the G711U audio encoding format.

- The default port number is 80.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Settings > Network > Platform Connection**.

The **Platform Connection** page is displayed.

Step 3 Choose **Second Protocol Parameters > ONVIF** to access the page for setting ONVIF parameters.

Step 4 Set ONVIF parameters, as shown in [Figure 4-10](#). [Table 4-9](#) describes the ONVIF parameters.

Figure 4-10 Setting ONVIF parameters

Second Protocol Parameters

☒ Enable media stream keep-alive (Note: After the function is enabled, if the SDC does not periodically receive keep-alive messages from the video surveillance platform, the SDC stops sending media streams. Set this parameter based on platform requirements.)

Keep-alive duration: 60 Save

ONVIF T28181 T28181-2 GA/T 1400 GA/T 1400-2 REST DB3311

(Note: When the video encoding format is H.265, the ONVIF protocol is not compatible with the old device on the live network. You need to change the video encoding format to H.264.)

☒ Enable ONVIF

☒ Validity period (Note: After the function is enabled, if the current SDC time is beyond the validity period specified on the platform, ONVIF messages become invalid. This parameter is valid only when the platform supports the ONVIF validity period function.)

☒ Onvif metadata flow switch (Note: Please select whether to turn on the metadata stream switch according to the requirements of the decoding platform, so as not to be unable to decode)

Stream type: Elementary stream (Note: Select a stream transmission type based on the requirements of the decoding device to prevent decoding failure.)

Authentication mode: Digest_MD5(priority)/WSSE (Note: Enabling WSSE brings security risks. Exercise caution when performing this operation.)

Version: ONVIF 16.12

ONVIF Trans Protocol Type: HTTP/HTTPS (Note: HTTP is an insecure protocol and has security risks. Exercise caution when using this protocol.)

Table 4-9 Parameter description

Parameter	Description
Enable media stream keep-alive	Indicates whether to enable the keep-alive function for media streams. To enable the function, select Enable media stream keep-alive . If the keep-alive function is enabled for media streams and a camera does not receive keep-alive packets sent by the IVS1800/NVR800 within a specified period, the camera stops sending media streams. If the platform supports the keep-alive function, you are advised to select Enable media stream keep-alive .
Keep-alive duration	Duration that the camera and IVS1800/NVR800 keep alive connections for media streams. The value is an integer ranging from 10 to 120. For example, if this parameter is set to 60s, the camera does not stop sending media streams even if it does not receive media keep-alive packets within 60s and stops sending media streams if it does not receive media keep-alive packets for more than 60s.

Parameter	Description
Enable ONVIF	To enable the ONVIF protocol, select Enable ONVIF .
Validity period	To enable the ONVIF message validity period function, select Validity period. After this function is enabled, an ONVIF message will become invalid when the specified validity period elapses. NOTE The ONVIF message validity period function is valid only when supported by the IVS1800/NVR800. If the platform does not support this function but this parameter is selected in the camera web system, the camera will fail to connect to the IVS1800/NVR800. You are advised to enable this function only when security risks exist. The ONVIF message validity period function is disabled by default.
ONVIF metadata flow switch	If this parameter is selected, the camera's metadata can be obtained. Otherwise, only video and audio streams can be obtained. This function is enabled by default.
Stream type	Select a media transmission type from the Stream type drop-down list box. The options are as follows: • Elementary stream: uses the ES compression mode. • Program stream: uses the PS compression mode. NOTE • Select the stream type based on the requirements of the decoder to prevent decoding failure. • The ONVIF media stream can be configured only when the camera is connected to the platform through the ONVIF protocol.

Parameter	Description
Authentication mode	Select a desired authentication mode from the Authentication mode drop-down list box. The options are as follows: • Digest_MD5: Digest authentication with MD5 encryption. • Digest_SHA256: Digest authentication with SHA256 encryption. • Digest_MD5/Digest_SHA256: Both Digest_MD5 and Digest_SHA256 authentication modes are supported. • Digest_MD5(priority)/WSSE: Both Digest_MD5 and WSSE authentication modes are supported, but Digest_MD5 authentication is preferred. • WSSE: indicates the Web Service Security (WSSE) authentication mode. • None: indicates that authentication is not performed. NOTE • The ONVIF WSSE authentication mode has security risks. – When some platforms to which the cameras connect support ONVIF WSSE authentication only, you are advised to enable the Digest_MD5(priority)/WSSE authentication mode. – When all platforms to which the cameras connect support ONVIF WSSE authentication only, you are advised to enable the WSSE authentication mode. – You are advised to enable the WSSE authentication mode when some platforms cannot correctly process Digest messages. • Security risks may exist when you select None. It is recommended that this authentication mode be enabled only when the platform does not support authentication. If None is selected, the system does not perform authentication if you request live video through the RTSP or ONVIF protocol.
Version	Ensure that the ONVIF version supported by the camera is consistent with that supported by the platform.
ONVIF Trans Protocol Type	ONVIF transmission protocol. The options are as follows: • HTTP/HTTPS: Data is transmitted through HTTP or HTTPS. • HTTP: Data is transmitted through HTTP. • HTTPS: Data is transmitted through HTTPS. NOTE HTTP is an insecure protocol and has security risks. Therefore, exercise caution when using this protocol.

Parameter	Description
Password Management	Method 1: 1. In the Password Management area, click ONVIF Password. 2. On the ONVIF Password tab page, set Current password, New password, and Confirm password. 3. Click Save. Method 2: 1. Choose Settings > System > Password Management. 2. Click Protocol Password. 3. On the ONVIF Password tab page, set Current password, New password, and Confirm password. 4. Click Save. NOTE • Change the ONVIF password for data security purposes. When the camera uses the ONVIF protocol to connect to the IVS1800/NVR800, you must enter this password. Otherwise, the connection cannot be set up. If platform authentication fails for 20 consecutive times, the camera is locked for 5 minutes. After the password is changed, record and keep the new password secure. • The default user name is admin. The value of Current password must be the same as the password of the admin user who logs in to the camera web system. For security purposes, the password must consist of 8 to 20 characters and contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters. For system security purposes, the following weak passwords are not recommended: 1qaz!QAZ, admin123, admin123!, Admin123!, Administrator, datacache1, datacache2, datacache3, "datacache4", datacache5, dlsDb001, dlsDls01, guest123, HWbss123, LcaP2010, lcap_oracle, lcap_uoa, password1, Password, password123, PortalONE, prmt_iddeploy, Promotion, SDP Report, u+versioncode, and Change_Me.

----End

4.1.3 Verification

If a camera is added successfully, the status of the camera is **Online** and you can view live video from this camera.

Procedure

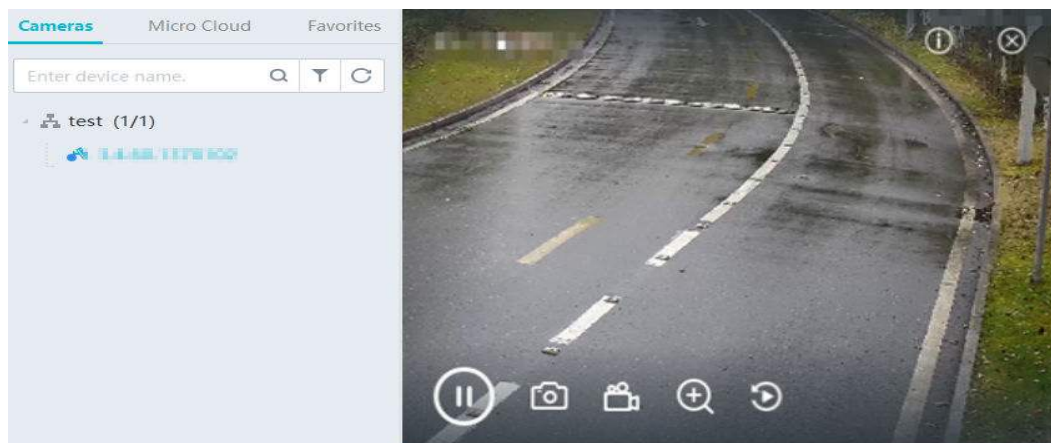
Step 1 Check the device status.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Check whether the NVR800s in the device list in the middle of the page are online, and check whether the camera status is **Online** in the **Device Status** column on the right.

Step 2 View live video from the camera.

1. On the iClient S100 home page, choose **Basic Operations > Live**.
2. Drag the added camera to the live video pane. If the live video can be properly played, the access is successful, as shown in [Figure 4-11](#).

Figure 4-11 Viewing live video from the camera



NOTE

- If the added camera is not displayed on the camera list, click  to refresh the camera list.
- You can also drag the entire camera group to the live video layout to view the live video from all the cameras in the group. You can create camera groups as required. To create a customized camera group, choose **Live > Groups**.
 - **Groups**: displays all camera groups and cameras in the groups. You can view live video from a camera or a group of cameras.
 - **Micro Cloud**: displays all NVR800s and allows users to view live video from cameras connected to each NVR800.
 - **Favorites**: displays favorited cameras and views. You can view live video from a favorited camera and invoke a favorited view.

----End

4.2 Video Viewing

4.2.1 Live Video Viewing

NOTE

You need to strictly comply with your local laws and regulations when using video-related services, for example, recording video, recording voice, and taking snapshots. Do not use them for illegitimate purposes such as infringing on personal privacy or observing employee behaviors.

Viewing Live Video from a Single Camera

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.

----End

NOTE

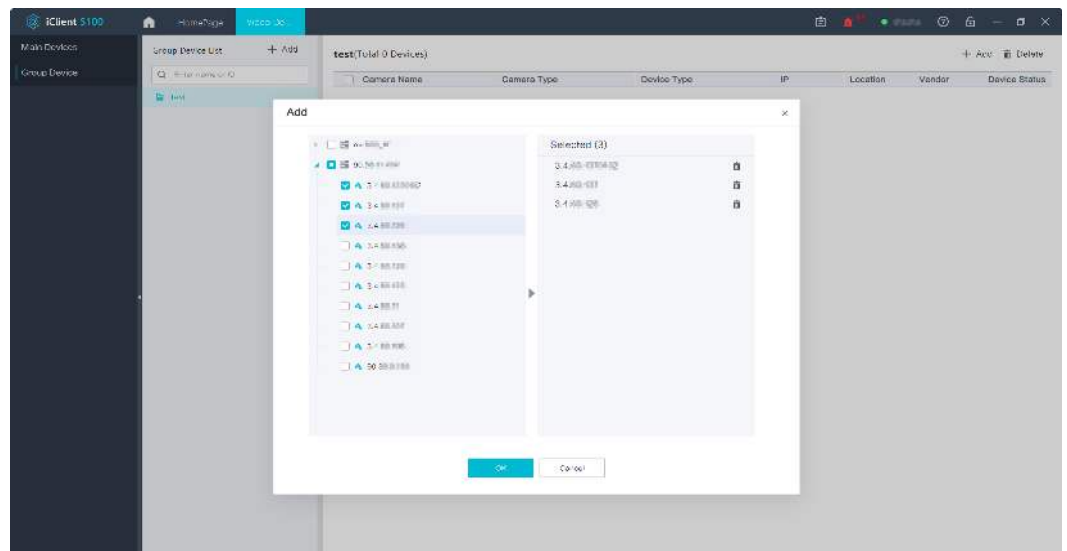
- During live video viewing, do not overlap the video pane that is playing live video with the window or dialog box of another program. The overlap may cause artifacts or even frozen images.
- If the live network is unstable, frame freezing or artifacts may occur on the live video. In this case, you are advised to enable the bandwidth adaptation function in the camera web system. After bandwidth adaptation is enabled, the camera can reduce or increase the bit rate based on the network condition to ensure smooth live video playing.

Viewing Live Video from Grouped Cameras

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Group Device** and group cameras.

1. Click **Add** on the right of the **Group Device List**, enter the group name, and click .
2. Click the newly added camera group and click **Add** in the upper right corner. On the page that is displayed, select cameras and click **OK**, as shown in [Figure 4-12](#).

Figure 4-12 Grouping cameras



Step 2 Choose **Basic Operations > Live** on the iClient S100 home page to view live video from cameras in a group (containing more than one camera and excluding cameras in subgroups).

In the device list (for device groups or all devices):

- Hold down **Ctrl** or **Shift**, select multiple cameras from the device tree, and drag the cameras to live video panes.
- Drag a group or main device to live video panes.

- Click  next to a group or main device.

Select **Tile** or **Cycling** to start viewing live video from cameras in the group or under the main device.

- In tile mode:
 - Video from selected cameras is displayed in the camera selection sequence.
 - If the number of idle live video panes is less than the number of online cameras in the group, video from some cameras will not be played. You need to manually adjust the video pane layout and view live video.
 - Live video can be played in sequence only in the selected video pane. For example, if you drag four cameras to the fourth video pane in the layout of four video panes, live video from the cameras is played in the fourth video pane in sequence, and the first three video panes do not play live video even if they are idle.
- In cycling mode:
 - a. Click **Advanced** and set parameters. [Table 4-10](#) lists the key parameters.

Table 4-10 Key parameters

Parameter	Description
Panes	Number of cycling panes, which must be less than the number of cameras to cycle.
Arrangement	▪ Tile ▪ Custom: In the Customize Panes window that is displayed, select panes and click Start.
Interval	Dwell time for selected cameras to play live video, in seconds.
Stream Type	The default value is Primary .

- b. Click **OK** to start cycling.

----End

4.2.2 Camera Cycling

Application Scenario

You can configure a cycling policy to view live video from multiple cameras at a certain interval. For example, multiple cameras are deployed on the Tianmushan Road. However, live video panes are insufficient for playing live video from all cameras at the same time. You can configure a cycling policy to view live video from the cameras at an interval of 30 seconds.

Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Click  in the lower right corner of the **Live** page. To add a cycle group for the first time, click **+**. Otherwise, click **New Group**.

Step 3 In the **New Cycle** window, configure cycle group information, as shown in [Figure 4-13](#). [Table 4-11](#) describes the key parameters.

Figure 4-13 New Cycle window

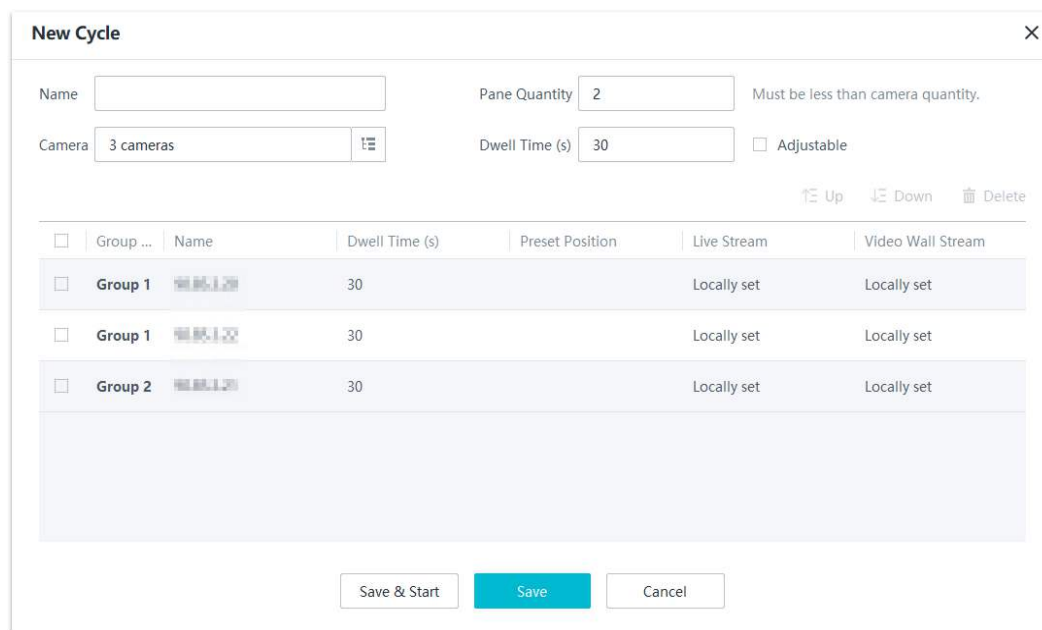


Table 4-11 Key parameters and icons for adding a cycle group

Parameter	Description
Pane Quantity	Number of cycling panes, which must be less than the number of cameras to cycle.
Dwell Time (s)	Dwell time at the selected cameras. The dwell time can be configured for cameras in batches or one by one. In this example, the dwell time is configured for a single group as an example.

Parameter	Description
Live Stream	• Locally set: The settings are the same as those in the Personal Settings area. • Automatic: No stream is specified. After this option is selected, the stream that the camera has transmitted to the platform is preferentially used. If the camera has not transmitted any streams to the platform, the primary stream of the camera is used by default. • Primary: The primary stream of the camera is used. The primary stream features a high bit rate, definition, and bandwidth usage. • Secondary 1: Secondary stream 1 of the camera is used. The secondary stream features low definition and bandwidth usage. • Secondary 2: Secondary stream 2 of the camera is used. The secondary stream features low definition and bandwidth usage. NOTE When bandwidth resources are limited, set this parameter to Secondary 1 or Secondary 2.
Video Wall Stream	• Locally set: The settings are the same as those in the Personal Settings area. • Primary: The primary stream of the camera is used. The primary stream features a high bit rate, definition, and bandwidth usage. • Secondary 1: Secondary stream 1 of the camera is used. The secondary stream features low definition and bandwidth usage. • Secondary 2: Secondary stream 2 of the camera is used. The secondary stream features low definition and bandwidth usage. NOTE When bandwidth resources are limited, set this parameter to Secondary 1 or Secondary 2.
Up/Down	Select a camera and click Up or Down to adjust the camera cycling sequence.

Step 4 Click  in the lower right corner of the **Live** page. The added cycle groups are displayed in the **Cycle Cameras** window. You can perform the following operations:

- Click . The selected pane is regarded as the first pane. The live video from corresponding cameras is played in sequence in cycling mode. For example, if pane 2 is selected, and the number of panes is three, live video is displayed in panes 2, 3, and 4 in cycling mode.

- Click  to customize panes for live video viewing in cycling mode.

----End

4.2.3 View Management

Application Scenario

Live video pane layout settings (including camera settings) and cycling settings can be stored as views to facilitate your later use.

- View favoriting: You are responsible for viewing live video from cameras on the Tianmushan Road (four-pane layout) and Xixi Road (nine-pane layout). You can favorite the views to quickly switch between them without repeatedly dragging cameras to live video panes.
- View schedule configuration: You have configured multiple views to store live video from multiple cameras on the Xixi Road. You can configure view schedules so that these views can be automatically played in the specified periods every week.

Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Select the required live video pane layout. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.

NOTE

You can store cycling views after starting viewing live video in cycling mode. For details about how to configure and start camera cycling, see [4.2.2 Camera Cycling](#). You can then configure a view schedule to perform periodic cycling as scheduled.

Step 3 Click  and set **Save as** to **New** or **Overwrite**.

- If you set **Save as** to **New**, set **View Name** and save the view.
- If you set **Save as** to **Overwrite**, the new view overwrites the existing one.

Step 4 Click **OK**.

Step 5 Repeat [Step 2](#) through [Step 4](#) to save more views.

Step 6 Click the **Favorites** tab and view the favorited views in the **Favorited Views** area.

Step 7 Click  next to **Favorited Views**. The **View Schedule** page is displayed.

Step 8 Click **New Schedule**. In the **New Schedule** window that is displayed, set view schedule parameters, as shown in [Figure 4-14](#). [Table 4-12](#) lists related parameters.

Figure 4-14 New Schedule

The screenshot shows the 'New Schedule' dialog box. It has a title bar with a close button. Inside, there's a 'Schedule Name' input field containing 'test'. To its right is a 'Cycle' section with two radio buttons: 'Weekly' (selected) and 'Daily'. Below this is a time grid. The grid has days of the week as rows and time slots from 00:00 to 24:00 as columns. A period is highlighted from 05:00 to 12:00 on Sunday and Monday. The Sunday segment is labeled '111' and the Monday segment is labeled '222'. At the bottom, there are three buttons: 'Save & Enable...', 'Save', and 'Cancel'.

Table 4-12 Parameter description

Parameter	Description
Cycle	Cycle for executing a view schedule.
Period	Time segment for playing a view. Drag the mouse to configure a specified time segment for view playing. Right-click the time segment and choose a view from the shortcut menu. Click the time segment and set specific time points.

-----End

4.2.4 PTZ Controls

Application Scenario

You can perform PTZ controls to control the camera direction and focal length and invoke preset positions. You can configure preset positions and follow-up tours to periodically view live video of specified sites.

For example, area A is a key area for video observation. To achieve better observation effect, you can use the PTZ controls function to adjust the camera direction and focal length. You can set the adjusted direction and focal length as a preset position. When you need to view live video from area A in the future, you can directly invoke the preset position to adjust the camera to the specified direction and focal length. If you have multiple key areas for video observation, you can set preset positions for each area and configure a tour to periodically view live video of these areas.

Prerequisites

The camera is a PTZ dome camera or a camera of another type providing PTZ functions.

NOTE

- This section uses a PTZ dome camera as an example to describe how to perform PTZ controls.
- By default, PTZ dome cameras and PTZ box cameras provide all PTZ functions, and bullet cameras and fixed dome cameras only provide some PTZ functions such as zoom in/out and focal length adjustment. The specific functions are subject to that displayed on the **PTZ Control** page of the iClient S100.
- PTZ controls results vary depending on the specific functions supported by PUs. For details, see the camera compatibility list.

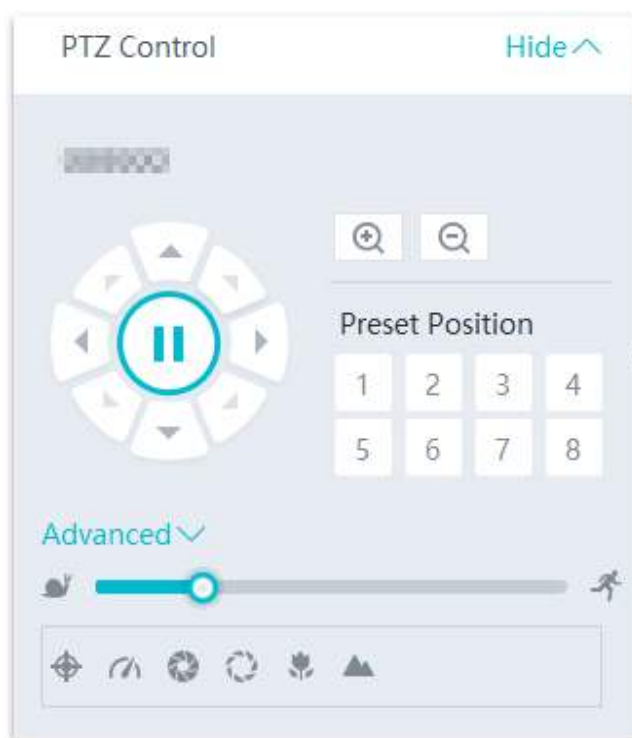
Basic Operations

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Drag an online PTZ camera in the **Devices** area to a live video pane.

Step 3 Click the expand icon next to **PTZ Control** in the lower left corner, as shown in [Figure 4-15](#).

Figure 4-15 PTZ Control panel



- Use the eight arrow buttons to rotate the PTZ device to adjust the camera shooting angle.

Click the expand icon next to **Advanced** and drag the slider on

   or click  or  to control the PTZ rotation speed.

- Drag the slider to the left or click  to slow down the PTZ rotation speed.

- Drag the slider to the right or click  to increase the PTZ rotation speed.
- Click  or  to zoom in or out on the live video image.

NOTE

If you zoom in on the video image for more than 30 times, the camera will enter the digital zoom mode. If you set the current position where the camera shoots as a preset position, the camera will not record the digital zoom ratio. When you invoke the preset position, the video image is zoomed in only for 30 times.

- Click a preset position ID in  to invoke the preset position.
You can set positions where the camera shoots objects as preset positions and quickly invoke a preset position to view the desired object. For details about how to set a preset position, see [Configuring Preset Positions and the Home Position](#).
- Click the expand icon next to **Advanced** and click buttons in



in the **Advanced** area to use other advanced functions of the PTZ device. [Table 4-13](#) describes the related buttons.

Table 4-13 Button description

Button	Description
3D Positioning	Automatically adjusts the PTZ camera shooting angle and focal length based on the ROI on the live video image. The procedure is as follows: – Click . Hold down the left mouse button and select an ROI on the live video image. The system automatically adjusts the shooting angle and focal length to the optimal using the ROI as the center. If you draw a frame from left to right, the video image within the frame is automatically zoomed in. If you draw a frame from right to left, the video image within the frame is automatically zoomed out. – Click  and click a position on the live video image. The system automatically rotates the PTZ camera to the position. NOTE If an ONVIF-compliant device needs to use the 3D zoom-in function, the device must implement the 3D zoom-in function in the same mode as the platform. For details about the mode used by the platform to implement the 3D zoom-in function, contact related engineers.
Horizontal Tour	Allows you to view live video from the camera that is performing a horizontal tour. The horizontal tour function allows unidirectional or back-and-forth scanning in either a clockwise or an anti-clockwise direction at a specified degree (including 360°).
Aperture-	Decreases the aperture.

Button	Description
Aperture+	Increases the aperture.
Focus+	Increases the focal length of the camera.
Focus-	Decreases the focal length of the camera.

Step 4 (Optional) Click  on the toolbar of the live video pane. Then, you can use the mouse to control the PTZ rotation direction.

The operation method is specified by **Move Controls** under **Maintenance Management > Personal Settings > PTZ Settings**.

----End

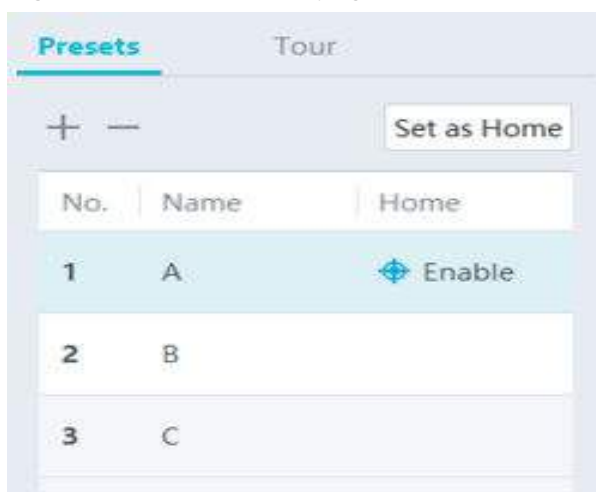
Configuring Preset Positions and the Home Position

NOTE

A home position is a special preset position to which a PTZ camera automatically rotates if users do not control the rotation direction of the camera within a specified period.

- Step 1** Click the live video pane of the selected PTZ dome camera, control the PTZ rotation direction and zoom ratio, and rotate the PTZ device to an observation site for which you want to add as a preset position.
- Step 2** Click the expand icon next to **Advanced** in the **PTZ Control** window and click the **Presets** tab. The **Presets** tab page is displayed, as shown in [Figure 4-16](#).

Figure 4-16 Presets tab page



- Step 3** Click . In the **Add Preset Position** window that is displayed, set **Preset Position Name**.

NOTE

Right-click a preset position and choose **Edit** from the shortcut menu to edit the preset position name.

Step 4 Click **OK**.

Step 5 Repeat [Step 1](#) through [Step 4](#) to add more preset positions.

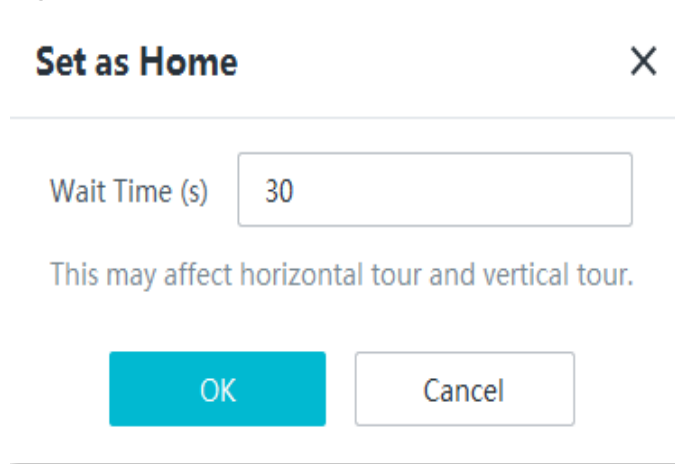
Step 6 Click a preset position and click **Set as Home**. In the **Set as Home** window that is displayed, set **Wait Time (s)** and click **OK**, as shown in [Figure 4-17](#).

If the current position of the PTZ camera is not the home position, the PTZ camera automatically rotates to the home position if no PTZ controls are performed before the configured waiting duration elapses.

 NOTE

Right-click a preset position and choose **Enable** or **Disable** from the shortcut menu to enable or disable the preset position.

Figure 4-17 Set as Home window



Step 7 You can invoke a preset position in either of the following ways:

1. Click the preset position button on the right of the PTZ steering wheel to quickly invoke the first eight preset positions.
2. Double-click a preset position in the preset position list.

----End

Tour

Step 1 Click the expand icon next to **Advanced** in the **PTZ Control** window and click the **Tour** tab, as shown in [Figure 4-18](#).

Figure 4-18 Tour

Presets		
Tour		
Set Tour		
Name	Time	Sp...
A	30	5
B	45	10
C	60	1

Step 2 Click **Set Tour** to add a tour, as shown in [Figure 4-19](#). [Table 4-14](#) describes the parameters and buttons.

Figure 4-19 Adding a tour

Set Tour

Up

Down

+

Add

✖

Delete

☐	Preset Position	Dwell Time (s)	Speed Level
☐	A	30	5
☐	B	45	10
☐	C	60	1

OK

Cancel

Table 4-14 Parameter/Button description

Parameter/ Button	Description
Up/Down	Select a preset position and click Up or Down to adjust the preset position sequence.
Add	Adds preset positions for the tour.
Delete	Deletes selected preset positions in batches.
Preset Position	Preset position. Each tour supports 1 to 20 preset positions.
Dwell Time (s)	Tour duration for each preset position. NOTE A short tour duration may shorten the service life of the camera motor and belt. If the preset positions do not need to be frequently switched onsite, you are advised to set the tour duration to be longer (for example, over 60 seconds).
Speed Level	Tour speed for each preset position.

Step 3 Click . The camera starts to play live video based on the tour.

----End

4.2.5 Snapshot Taking

Manual snapshots are local snapshots. [Table 4-15](#) describes the function of local snapshots.

Table 4-15 Manual snapshot types

Snapshot Type	Function
Local snapshot	Local snapshots taken during live video viewing are stored on the computer where the iClient S100 client is located. NOTE Do not perform local snapshot taking in an alarm pane, because the alarm pane will play the alarm-triggered live video when the corresponding alarm is generated and interrupt the local snapshot taking.

Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Double-click an online camera in the **Devices** area or drag the online camera to a live video pane. Then, you can view the live video.

Step 3 Capture a snapshot and save it on the local computer.



Click  on the toolbar of the live video pane, or right-click the live video pane and choose **Snapshot** from the shortcut menu to take a snapshot of the current video image.

In this example, use the default storage directory. After the snapshot is taken, the message "Snapshot successful" is displayed in the lower right corner of the client page. You can click **Click here to open folder** to go to the snapshot storage directory.

Step 4 View the snapshot.

View the snapshot stored on the local computer.

Choose **Maintenance Management > Local Settings** on the iClient S100 home page. You can view the snapshot in the local snapshot storage directory.

----End

4.2.6 OSD Settings

Application Scenario

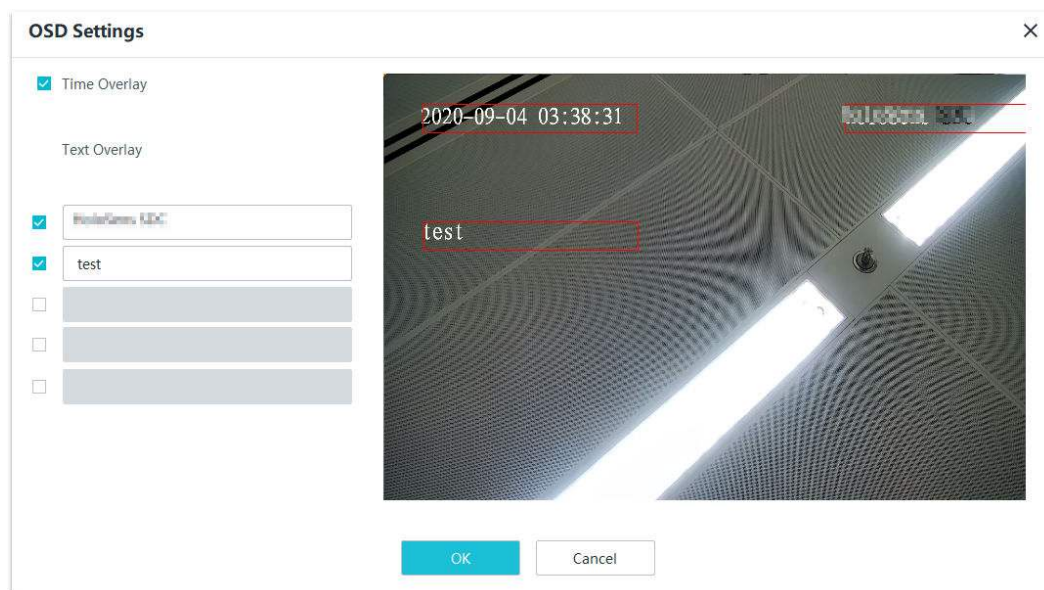
After setting On Screen Display (OSD) parameters, you can set whether to display the specified text and time, and whether to enable the text blinking function on the video.

Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Double-click an online camera in the **Devices** area or drag the online camera to a live video pane. Then, you can view the live video.

Step 3 Right-click a live video pane, choose **OSD Settings** from the shortcut menu, and set OSD parameters, as shown in [Figure 4-20](#). [Table 4-16](#) describes the parameters.

Figure 4-20 OSD Settings page**Table 4-16** OSD parameter description

Parameter	Description
Time Overlay	Indicates whether to display the current camera time on live video images.
Text Overlay	Indicates whether to display text on live video images. After this check box is selected, you can enter the text to be displayed in the text boxes. You are advised to set this parameter to the IP address or installation location of the camera. NOTE - To display multiple lines of texts on video images, select multiple check boxes under Text Overlay and enter the texts to display in the text boxes. - The maximum number of characters is determined by PU capabilities.
Red text box	Red-framed area. You can move it to adjust the display position.

----End

4.3 Recording

4.3.1 Application Scenario

This section describes how to record video after cameras are connected to the NVR800.

By default, the video from all cameras is recorded on the NVR800, and recordings are stored in the hard disk of the NVR800. Currently, you can only perform manual

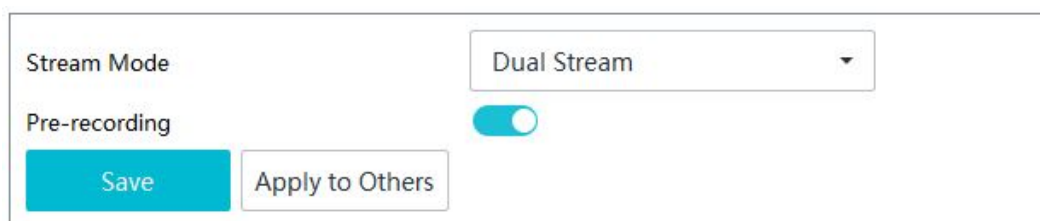
local recording for the NVR800 on the iClient S100. When emergencies occur in detection areas, you can manually record video and store it to the computer where the client is installed.

4.3.2 Recording Configuration

4.3.2.1 Setting Recording Parameters

- Step 1** Right-click a device in **Device List** and choose **Storage Management**.
- Step 2** Click the Storage Policy tab on the left of the page and select a desired camera in the camera list, The page for configuring a storage policy is displayed, as shown in [Figure 4-21](#).

Figure 4-21 Configuring a storage policy



- Step 3** Set storage policy parameters , and Click Save
- Step 4** (Optional) Click **Apply to Others**, select cameras to which the current camera's recording storage policy is to be copied, and click **OK** to complete the batch setting.

----End

4.3.2.2 Configuring Scheduled Recording

The system can record video in a user-defined time segment and store the recorded video to server disks.

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click a device and choose **Storage Management**.
- Step 3** Click the **Server Recording Plan** tab. The tab page for configuring a server recording plan is displayed.
- Step 4** Configure server recording plans.
1. In the **Cameras** area on the left, select a camera whose recording storage policy has been configured.
 2. In the **Server Recording Plan** area on the right, click  next to **Enable Recording**, as shown in [Figure 4-22](#).

Figure 4-22 Creating a recording plan

Enable Recording ☒

☒ All

	00:00	02:00	04:00	06:00	08:00	10:00	12:00	14:00	16:00	18:00	20:00	22:00	24:00		
Mon	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	Reset	Apply to All
Tue	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	Reset	Apply to All
Wed	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	Reset	Apply to All
Thu	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	Reset	Apply to All
Fri	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	Reset	Apply to All
Sat	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	Reset	Apply to All
Sun	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	Reset	Apply to All

3. Drag the slider on the timeline to select a time segment for executing the server recording plan.
If you click **Continuous**, you do not need to select a recording time segment.
4. Click **Save**

Step 5 (Optional) Click **Apply to Others**, select cameras to which the current camera's recording storage policy is to be copied, and click **OK** to complete the batch setting.

----End

4.3.3 Configuring Manual Local Recording

You can manually record video during live video viewing and store the recorded video to the computer where the iClient S100 client is installed.

Prerequisites

The recording storage path has been set. For details, see [7.1 Local Settings](#).

Procedure

- Step 1** On the iClient S100 home page, choose **Basic Operations > Live**.
- Step 2** Double-click an online camera in **Devices** or drag an online camera to a live video pane. The live video is played.

NOTICE

During live video viewing, ensure that no window or dialog box of another program overlaps the video pane that is playing live video. The overlap may cause artifacts or even frozen images.

Step 3 Right-click the live video pane and choose **Recording** from the shortcut menu, or

click  in the live video pane. The  icon turns blue, indicating that the iClient S100 starts recording video.

Right-click the live video pane and choose  from the shortcut menu, or click . Then, the  icon turns gray, indicating that the iClient S100 stops recording video.

----End

4.3.4 Recording Playback

You can play back recordings on the iClient S100. You can also perform related operations during recording playback.

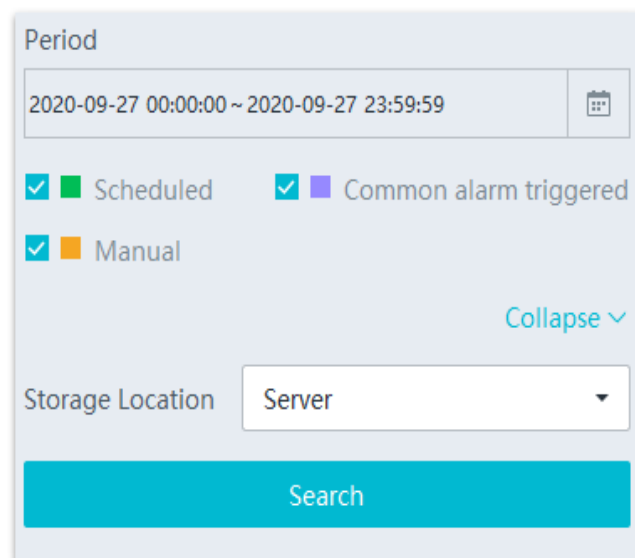
Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Playback**.

Step 2 Set recording playback parameters.

1. Select a camera whose recordings are to be played back in **Devices**.
Alternatively, click  to set search criteria, and obtain the camera whose recordings are to be played back.
2. In the recording search area, set search criteria, as shown in [Figure 4-23](#). [Table 4-17](#) describes the parameters.

Figure 4-23 Recording search

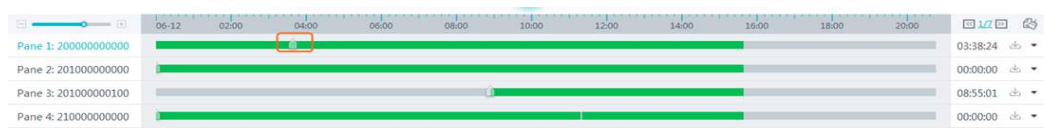


The image shows a 'Recording search' dialog box. It has a 'Period' section with a date range '2020-09-27 00:00:00 ~ 2020-09-27 23:59:59' and a calendar icon. Below this are three checked checkboxes: 'Scheduled' (green), 'Common alarm triggered' (purple), and 'Manual' (orange). A 'Collapse' button with a downward arrow is to the right. At the bottom, there is a 'Storage Location' dropdown menu set to 'Server' and a large blue 'Search' button.

Table 4-17 Recording search parameters

Parameter	Description
Period	Time segment for recording search. The default time segment is 00:00:00-23:59:59 of the current day. Recordings in any time segment within the latest 30 days can be searched.
Scheduled/Manual/Common alarm-triggered	Recording type. – Scheduled recording: Video recorded based on a recording plan is stored on the server disk. For details about how to configure a scheduled recording plan, see 5.3.3.2 Configuring Scheduled Recording. Currently, the iClient S100 supports only scheduled recording for the IVS1800. By default, global recording is enabled on the NVR800. You do not need to enable scheduled recording on the iClient S100. – Manual recording: You can click  on the video preview page to perform manual recording (manual recordings are stored on the computer where the iClient S100 is installed) or download recordings from the server and save them to the local host during recording playback. – Common alarm-triggered recording: When the alarm linkage action is set to recording for a device and alarms are triggered, the system performs alarm-triggered recording. By default, data is stored on the hard disk of the server.
Storage Location	Recording storage location. The options are as follows: – Server: Search for video files stored on hard disks of the IVS1800/NVR800. Video files can be stored on the server after scheduled recording is performed on the iClient S100 or stored on the local host after the server is connected to cameras. – Local: Search for recordings generated during manual recording triggered on the live video viewing page and stored on the local computer.

3. Click **Search**.
The recording search result is displayed in the timeline area under the recording playback window.
4. Drag the slider on a timeline to select the playback start time, as shown in [Figure 4-24](#).

Figure 4-24 Recording playback**NOTE**

- Each recording playback pane maps the timeline of a camera. If the number of cameras is greater than the number of recording playback panes, you can click the page-up or page-down button on the right of the timeline area to view the timelines of more cameras and play back their recordings.
- Play back recordings on a gigabit network. If the network bandwidth is lower than 1000 Gbit/s, artifacts or video stuttering may occur.
- If you want to change the layout of recording playback panes, select and load the video again.

5. (Optional) Cyclically play back recordings.

- a. In the timeline area of the search result, click  on the right and click **Loop**.
- b. On the timeline of the recording to be played cyclically, click the timeline and drag to select a time segment. Click . The selected recording is played cyclically in the playback window.

Click  on the right of the time line to cancel cyclic playback.

6. (Optional) Play back recordings by segment.

- a. Click  in the lower left corner of the live video pane.
- b. In the dialog box that is displayed, segment a recording into multiple video clips by time segment and play the video clips in multiple video panes simultaneously.

NOTE

Enabling segment-based playback will automatically stop all recordings that are being played.

----End

4.3.5 Recording Download

4.3.5.1 Setting Recording Download Parameters

Personal Settings

Step 1 On the iClient S100 home page, choose **Maintenance Management > Personal Settings**.

Step 2 Set recording download parameters. [Table 4-18](#) describes the parameters.

Table 4-18 Parameter description

Parameter	Description
Default Clip Length (5 min - 48 hours)	Default duration of a video clip that is manually recorded. This parameter applies to both manual local recording and manual server recording.
Split Files Every	Mode for splitting a single recording into several smaller data files. This parameter applies to manual local recording and recording download without encryption. The options are as follows: • Time (min): A single recording is split by time. • Capacity (MB): A single recording is split by storage space.
Reserved Space (MB)	Minimum disk space for storing recordings. To ensure that recordings can be stored correctly, the available disk space must be greater than the minimum disk space.
Space Limit Warning (MB)	Disk storage threshold for triggering an alarm. During video recording, when the available disk space is less than the value of this parameter, the system generates an alarm. In addition, the value of this parameter must be greater than that of Reserved Space .
Format	Video file storage format. The default format is MP4 .
Naming Format	Rule for naming a recording file. This parameter applies to manual local recording and recording download. The options are as follows: • Camera name_No._Time (YYYY-MM-DD-hh-mm-ss) • Camera name_Time (YYYY-MM-DD-hh-mm-ss)_No. • Time (YYYY-MM-DD-hh-mm-ss)_Camera name_No.
Download Threads	Maximum number of recordings that can be downloaded at the same time.
Download Speed (from Server)	Download speed. Server-based recordings can be downloaded at 1/4, 1/2, or 1x camera bit rate, or high speed (maximum speed that the server, client, and current network can bear). If the bit rate is 4 Mbit/s, 1/4 of it is 1 Mbit/s.
Skip Losses Under (s)	Maximum time interval for ignored interruption. During recording search, if the recording is interrupted for a specified period that is less than the value of this parameter, the recording is played as a complete recording without any interruption.

Step 3 Click **Save**.

----End

Local Settings

Step 1 On the iClient S100 home page, choose **Maintenance Management > Local Settings**.

Step 2 Set **Download Server-based Recordings to** under **Recording Directories**, and click **Save**.

----End

4.3.5.2 Configuring Recording Download

You can download recordings from the server and PUs to your local computer for later viewing. This function is sensitive. Therefore, you are advised to implement control on recording download, for example, control the content, quantity, size, and download time of recordings.

On the iClient S100, you can download recordings in either of the following ways:

- Search for recordings on the **Playback** page and download the recordings. For details, see [Downloading Recordings on Recording Playback Page](#).
- Choose **Basic Operations > Media > Recordings**, search for recordings by criteria, and download the recordings. For details, see [Downloading Recordings On the Networked Video Page](#).

NOTE

- All export and import functions can be used only in the following environments:
 - The WPS Office software is used by default.
 - The Microsoft Office software (later than Microsoft Office 2007) is installed properly. The legal license is activated and can run properly.
- You are advised to use professional video or image editing tools to shield irrelevant persons in downloaded or exported video or images and meet the HD requirements of the data subject. The recommended procedure is as follows:
 1. Download the required video to the local computer and decompress it to common video or export image data to the local computer.
 2. Use a video or an image editing tool to anonymize irrelevant targets and only retain the HD part of the data subject.
 3. Export the anonymized video or images to meet the data transfer requirements of the data subject.
 4. To ensure personal information security, delete the downloaded or exported images and recordings in a timely manner.

Downloading Recordings on Recording Playback Page

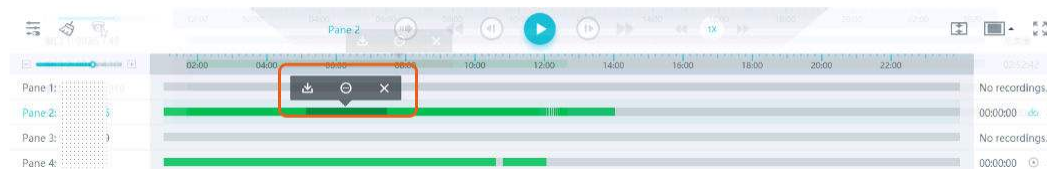
Step 1 On the iClient S100 home page, choose **Basic Operations > Playback**.

Step 2 Select a camera whose recordings are to be downloaded in **Devices**.

Step 3 In the recording search area, set search criteria and click **Search**.

- Step 4** In the search result, click  on the right of a timeline and click **Download** to switch to the recording download.
- Step 5** Drag the slider on the timeline to select time segments for recording download, as shown in [Figure 4-25](#).

Figure 4-25 Selecting time segments



- Step 6** Download the recordings to a local directory.
- Recording download
 - a. Click .
 - b. Set **Video** and Click **OK** to download the recording generated in the selected time segment to the specified local directory.
 - Batch download

Click  to download recordings of multiple time segments of the current camera to the specified local directory. You can also download encrypted recordings of multiple time segments of the current camera to the specified local directory.
- Step 7** On the iClient S100 client home page, choose **Basic Operations > Media > Downloads > All** and view the recording download progress.

After the download is complete, go to the local directory to view the downloaded recordings.

NOTE

- If the encoding format of the downloaded recording is H.265, it is recommended that the recording be played back by the VLC player.
- If the network condition is poor, the camera bit rate is high, and UDP is used for data transmission between the local domain and the external domain, packets may be lost when you download recordings from an external domain at a high speed.
- Recordings whose encoding format is MJPEG cannot be downloaded.

----End

Downloading Recordings On the Networked Video Page

- Step 1** On the iClient S100 home page, choose **Basic Operations > Media > Recordings**.
- Step 2** Set search criteria and click **Search**. [Table 4-19](#) describes the search parameters.

Table 4-19 Search parameters

Parameter	Description
Camera	Camera used for recording search. You can select cameras from the device list or on the map.
Period	Period used for recording search. In this case, the search result varies according to the recording type. • When Recording Type is set to Scheduled, Normal alarm triggered, or Manual, recordings whose time spans intersect with the value of Period are displayed in search results. • When Recording Type is set to Bookmarked, recording bookmarks attached during the specified recording time in Period are displayed in search results.
Recording Type	Recording type used for recording search.

Step 3 Download the recordings to a local directory.

1. On the timeline of the camera whose recordings need to be downloaded, select the recording segments to be downloaded and click .
2. Set **Video** and **Save Path**.
3. Click **OK** to download the recordings generated in the selected time segments to the specified local directory.
4. (Optional) Download recordings in batches. Select the cameras whose recordings need to be downloaded (multiple cameras can be selected), select the recording segments to be downloaded, and click  in the upper right corner to download recordings of multiple time segments to the local computer.

 NOTE

If you do not select recording segments, all recordings from the current camera are downloaded by default.

----End

4.4 Video Wall

4.4.1 Configuring a Video Wall

4.4.1.1 Application Scenario

You can use the iClient S100 to push live or recorded video to a video wall for viewing. To display video on the video wall, you need to set decoder parameters,

create a video wall layout on the iClient S100, add a decoder to the iClient S100, and bind decoder channels to panes on the video wall.

For example, if personnel in a security room need to view live video from multiple cameras in the building at the same time, they can configure a decoder and a video wall layout so that live video can be displayed on the video wall to facilitate management.

4.4.1.2 Configuring a Decoder for Video Display on a Video Wall

Prerequisites

- You have connected a decoder to the video wall.
- To ensure continuous streaming on the video wall, ensure that the network between the decoder and the IVS1800/NVR800 is normal.

NOTE

When the iClient S100 is connected to the NVR800, only the Pearmain PEMXP70 and Jovision DEC6109 decoders can be used.

When the iClient S100 is connected to the IVS1800, supported decoders vary depending on the iClient S100 version. The details are as follows:

- When the **iClient S100 of V1.3.0 or a later version** is connected to the IVS1800, only the Pearmain PEMXP70 and Jovision DEC6109 decoders can be used.
- When the **iClient S100 of a version earlier than V1.3.0** is connected to the IVS1800, the DEC6108, Pearmain PEMXP70, and Jovision DEC6109 decoders can be used.
- If the iClient S100 is upgraded from an earlier version to V1.3.0 and the DEC6108 decoder is required, you are advised to download and use the [iClient software](#) to configure and operate the decoder. For details about the configuration and operation methods, see the iClient product documentation.

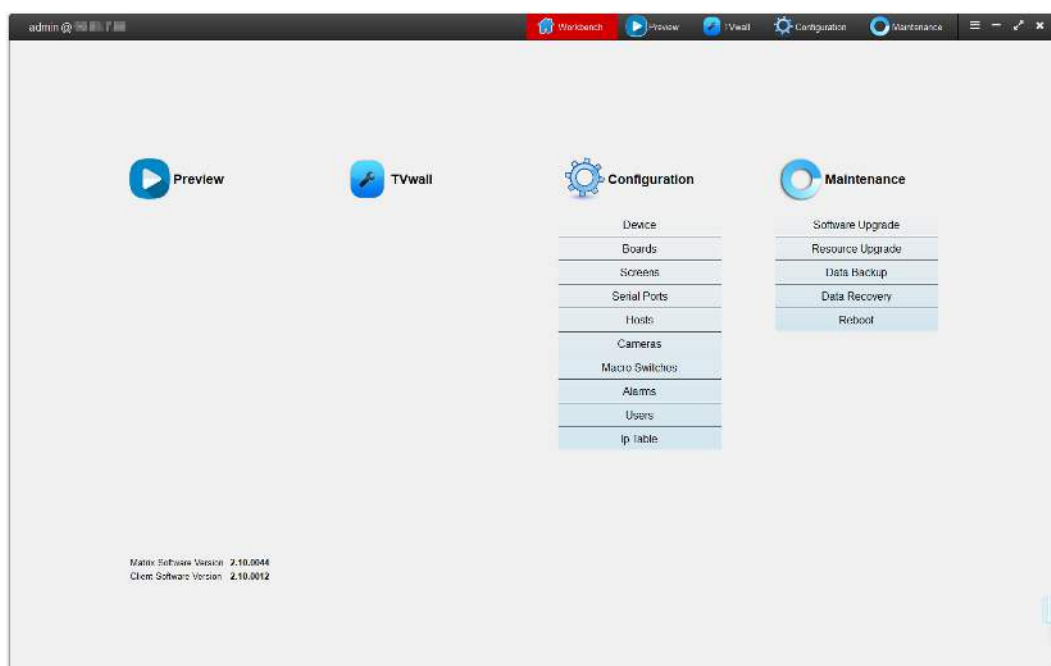
Setting the Service Parameters of a PEMXP70 Decoder

- Step 1** Start the IP MATRIX CLIENT, and enter the IP address (**192.168.0.70** by default), user name (**admin** by default), and password (**12345** by default), as shown in [Figure 4-26](#).

Figure 4-26 Login page

The login page for the IP Matrix Client features a blue gradient background. At the top right, there is a language dropdown menu set to 'English'. The title 'IP MATRIX CLIENT' is centered in large, bold, black letters. Below the title, there are three input fields: 'Ip Address' with a home icon and the value '192.168.0.70', 'User Name' with a person icon and the value 'admin', and 'Password' with a lock icon and masked characters. At the bottom, there are three buttons: 'IP Search' with a magnifying glass icon, 'LOGIN', and 'CANCEL'. The version number '2.10.0012' is displayed in the bottom right corner.

Step 2 Click **LOGIN**. The home page of the client is displayed, as shown in [Figure 4-27](#).

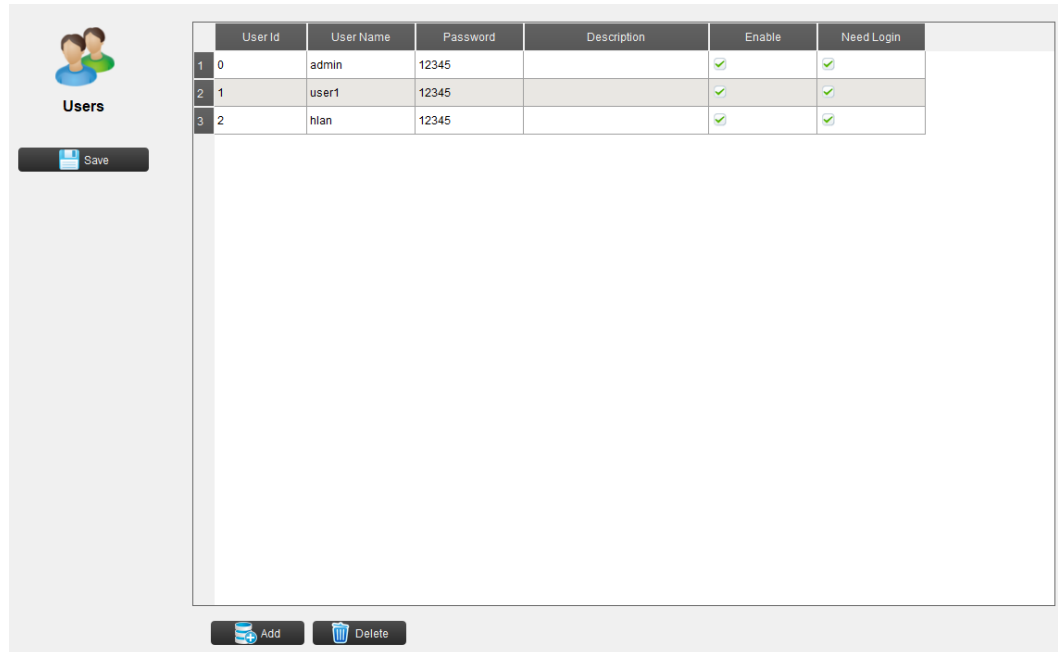
Figure 4-27 Home page of the client

Step 3 Choose **Workbench > Configuration > Users**. The user configuration page is displayed, as shown in [Figure 4-28](#).

On this page, you can add and delete users, and change user names and passwords.

 NOTE

- By default, the user ID of the administrator is **0**, the user name is **admin**, and the password is **12345**. The user ID and user name cannot be changed.
- For system security purposes, change the password regularly. Remember the new password after the change.

Figure 4-28 User configuration page

The screenshot shows the 'Users' configuration page. On the left, there is a sidebar with a 'Users' icon and a 'Save' button. The main area contains a table with the following data:

	User Id	User Name	Password	Description	Enable	Need Login
1	0	admin	12345		✓	✓
2	1	user1	12345		✓	✓
3	2	hlan	12345		✓	✓

At the bottom of the page, there are 'Add' and 'Delete' buttons.

Step 4 Choose **Workbench > Configuration > Ip Table**. The IP table configuration page is displayed, as shown in [Figure 4-29](#). On this page, you can set the external IP address, subnet mask, and gateway for each board in the matrix.

 NOTE

The IP addresses of all boards in the matrix must be in the same network segment. The IP address must be set for a board to connect to the network cable. Otherwise, the device will not run properly.

Figure 4-29 IP table configuration page

 Ip Table ✕

Board Id	Ip Address
1	192.168.0.70
2	
3	
4	
5	
6	
7	
8	

Mask

255.255.255.0

Gateway

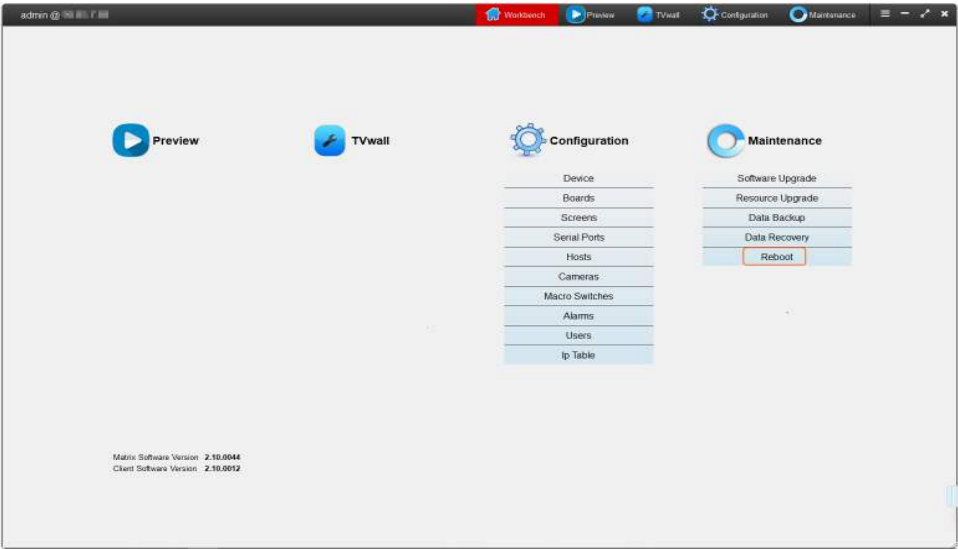
192.168.0.1

OK

Cancel

Step 5 Restart the IP MATRIX CLIENT, as shown in [Figure 4-30](#).

Figure 4-30 Restarting the client



----End

Creating a Video Wall

Step 1 Choose **Basic Operations > Video Wall** on the iClient S100 home page.

 NOTE

If decoders are stored locally, enter the passwords of all decoders.

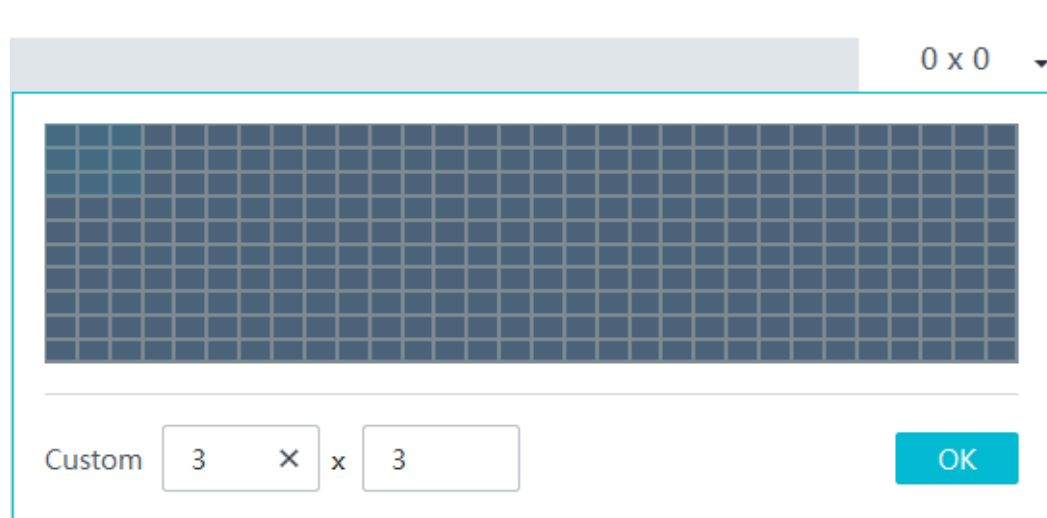
Step 2 On the page that is displayed, click **New Video Wall** or **+**. The **New Video Wall** page is displayed.

Step 3 Set **Wall Name** as required.

Step 4 Click **0 x 0** on the right of the video wall layout page. [Figure 4-31](#) shows the page that is displayed. Drag the mouse and select a layout. When you release the mouse, the layout is created.

Alternatively, you can set **Custom** to the number of columns and number of rows and click **OK** to create a layout.

Figure 4-31 Creating a video wall layout



Step 5 (Optional) If you want to customize the video wall layout on the iClient S100 to be the same as the actual one, merge panes.

To merge selected panes, drag the mouse, select several panes, and click **Merge**. To split the merged pane, select the pane and click **Split**.

Step 6 Click **Next**.

Step 7 Add decoders.

Click  next to **Decoder**. The **Add Decoders** window is displayed.

- You can add decoders one by one, as shown in [Figure 4-32](#). [Table 4-20](#) describes key parameters and buttons.

Figure 4-32 Adding decoders one by one

The 'Add Decoders' dialog box is shown. It features a table with the following data:

Decoder Name	IP Address	Port	Type	Verify	Status
Device 1	192.168.1.10	10200	PEMXP70	admin	Not ver

At the bottom of the dialog, there are input fields for 'User Name' and 'Password', a 'Batch Verify' button, and an 'Add' button. An information message states: 'Info: Remember to change the initial password and update it regularly.'

Table 4-20 Parameters and buttons for adding decoders one by one

Parameter/ Button	Description
IP Address	IP address of the decoder.
Port	Port number of the decoder. Set this parameter to 10200 (for the PEMXP70 decoder) or 28000 (for the DEC6109 decoder).
Type	Decoder model. The options are PEMXP70 (Pearmain) and DEC6109 (Jovision).
User Name	- If each decoder uses a unique service user name and password for registration, enter the service user name and password in each decoder record separately and click Verify. - If different decoders use the same service user name and password for registration, enter the service user name and password at the bottom of the window and click Batch Verify.
Password	
Verify/Batch Verify	
Add	If Verification succeeded is displayed, decoder registration is successful. Button for adding decoders. New decoders are displayed in the Decoder pane.

- You can add decoders in batches, as shown in [Figure 4-33](#). [Table 4-21](#) describes key parameters and buttons.

Figure 4-33 Adding decoders in batches

Add Decoders

Decoder Name	IP Address	Port	Type	Verify	Status
device1	192.168.1.10	10200	PEMXP70	User Name: Password: Verify	Not ver
device2	192.168.1.11	10200	PEMXP	User Name: Password: Verify	Not ver
device3	192.168.1.12	10200	PEMXP	User Name: Password: Verify	Not ver

User Name: Password:

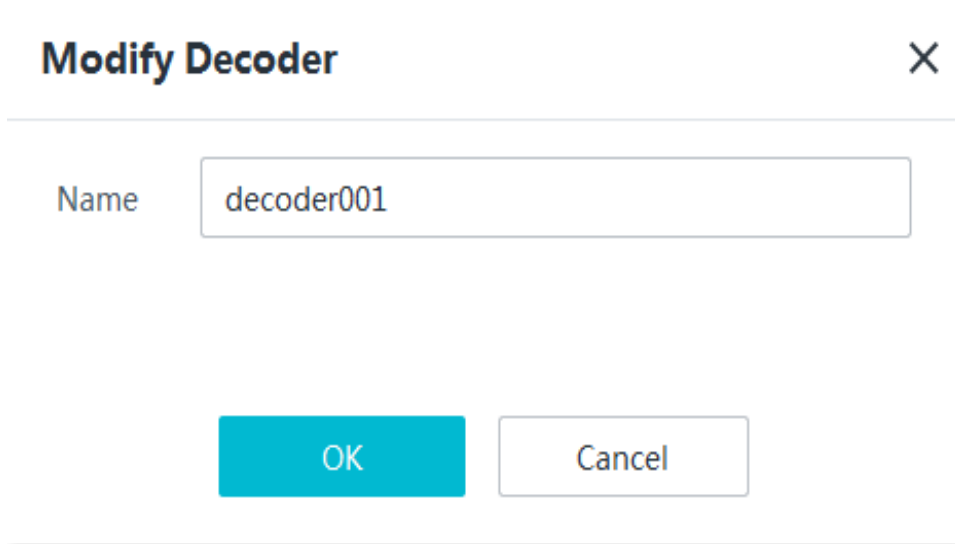
Info: Remember to change the initial password and update it regularly.

Table 4-21 Parameters and buttons for adding decoders in batches

Parameter/ Button	Description
Export	Used to export the .csv file to the local computer. You can open the .csv file, enter decoder information, and save the file.
Import	Used to import the .csv file containing decoder information to the iClient S100.
Port	Port number of the decoder. Set this parameter to 10200 (for the PEMXP70 decoder) or 28000 (for the DEC6109 decoder).
Type	Decoder model. The options are PEMXP70 (Pearmain) and DEC6109 (Jovision).
User Name	- If each decoder uses a unique service user name and password for registration, enter the service user name and password in each decoder record separately and click Verify. - If different decoders use the same service user name and password for registration, enter the service user name and password at the bottom of the window and click Batch Verify. If Verification succeeded is displayed, decoder registration is successful.
Password	
Verify/Batch Verify	
Add	Button for adding decoders. New decoders are displayed in the Decoder pane.

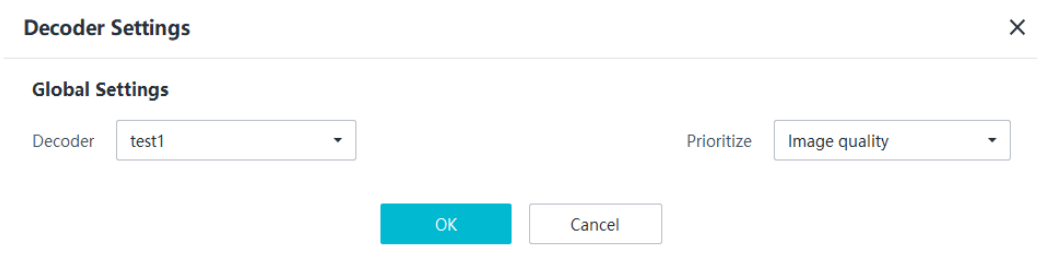
Step 8 (Optional) Change a decoder name.

1. In the **Decoder** pane, select a decoder whose name is to be changed and click . The window shown in [Figure 4-34](#) is displayed.

Figure 4-34 Modify DecoderA dialog box titled "Modify Decoder" with a close button (X) in the top right corner. It contains a text input field labeled "Name" with the value "decoder001". At the bottom, there are two buttons: "OK" (blue) and "Cancel" (white with blue border).

2. Set **Name** and click **OK**.

Step 9 Select a decoder, click  on the right of **Decoder** to configure the decoder playing mode, as shown in [Figure 4-35](#). [Table 4-22](#) describes the key parameters.

Figure 4-35 Decoder SettingsA dialog box titled "Decoder Settings" with a close button (X) in the top right corner. It has a section "Global Settings" containing two dropdown menus: "Decoder" (set to "test1") and "Prioritize" (set to "Image quality"). At the bottom, there are two buttons: "OK" (blue) and "Cancel" (white with blue border).**Table 4-22** Decoder parameters

Parameter	Description
Prioritize	• Image quality: video with more caching and a longer delay. • Smoothness: video with less caching and a shorter delay.

- Step 10** Drag decoder channels to idle video panes. To unbind channels from video panes, click **Unbind Selected** or **Unbind All** in the upper right corner.
- Step 11** (Optional) If the customized video wall layout is different from the actual physical video wall layout, you can merge or split the video wall panes to adjust their sizes.
- **Merge**: Drag the mouse to select the panes to be merged and click **Merge**.

- **Split:** Click the video pane to be split and click **Split**.

Step 12 Click **Save**.

----End

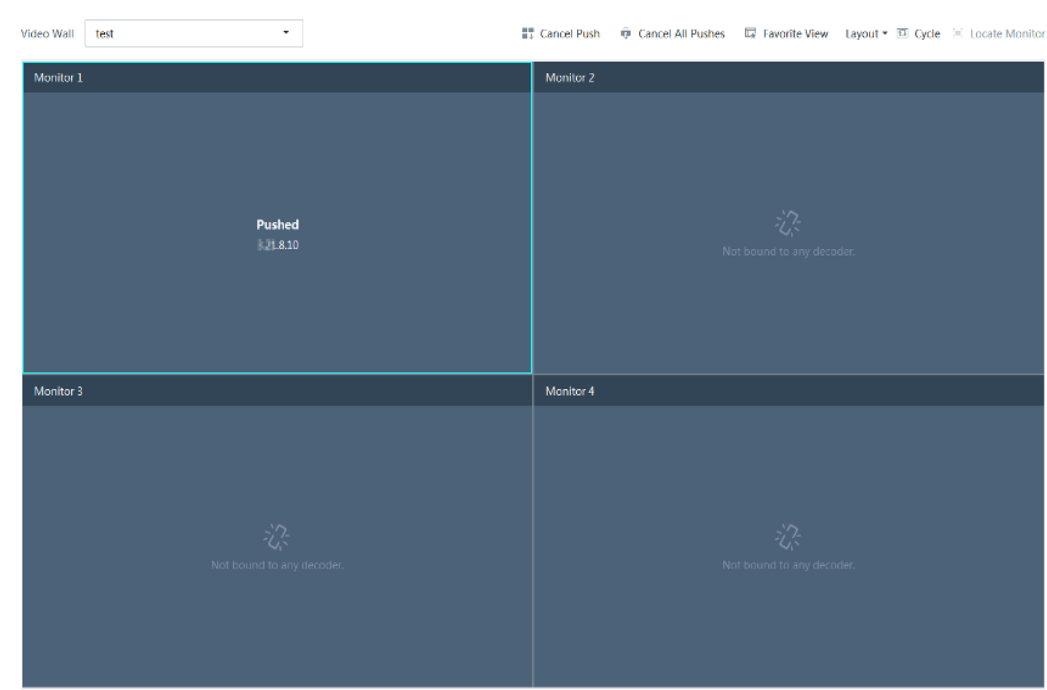
4.4.1.3 Verification

Step 1 Choose **Basic Operations > Video Wall** on the iClient S100 home page.

Step 2 On the **Set Decoder Password** page that is displayed, enter the passwords of all decoders and click **OK**.

Step 3 On the video wall page that is displayed, drag a camera whose video is to be displayed to a video pane, as shown in [Figure 4-36](#).

Figure 4-36 Video wall page



Step 4 View live video on the video wall.

----End

4.4.2 Live Video Viewing on a Video Wall

Prerequisites

You have created a video wall layout and connected a video wall to a decoder as an administrator. For details, see [4.4.1 Configuring a Video Wall](#).

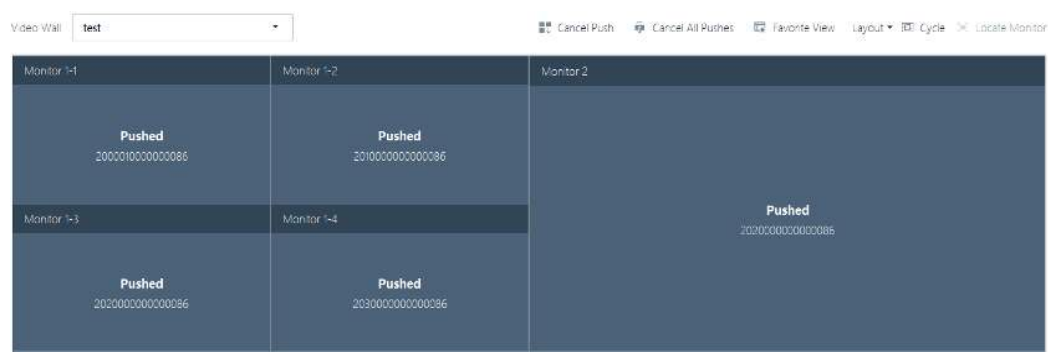
Live Video Display on the Video Wall

Step 1 On the iClient S100 home page, choose **Basic Operations > Video Wall**.

- Step 2** Double-click the created video wall to go to the **VideoWall** page.
- Step 3** Select the created video pane layout of the video wall from the **Video Wall** drop-down list box.
- Step 4** Select a video pane that is bound to a decoder channel and click **Layout**. You can select **1, 4, 8, 9, 16, 25, or 36** from the drop-down list box.

You can set **Layout** to specify the number of sub panes in a single video pane. Each sub pane can play the live video from a camera. [Figure 4-37](#) shows a 4-pane window as an example.

Figure 4-37 Layout



- Step 5** (Optional) Preview the video image of a camera if you need to know the video shot by the camera.

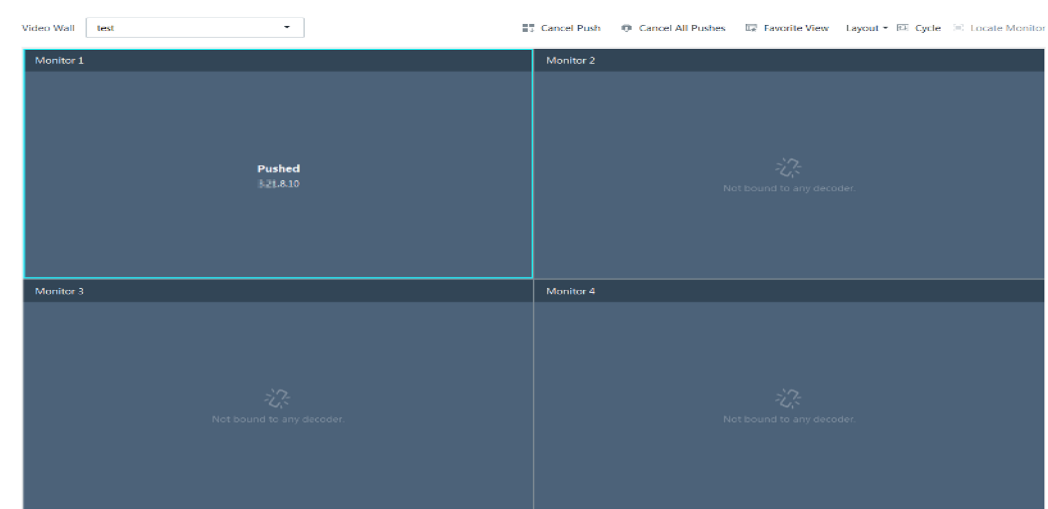
Drag the camera to **Preview Video** to view the live video shot by the camera.

Then select a video pane and click  to push the live video to the video wall.

- Step 6** Drag the camera to the video pane that has been bound to a decoder channel. [Figure 4-38](#) shows the video wall page.

You can view the live video on the video wall.

Figure 4-38 Video wall page



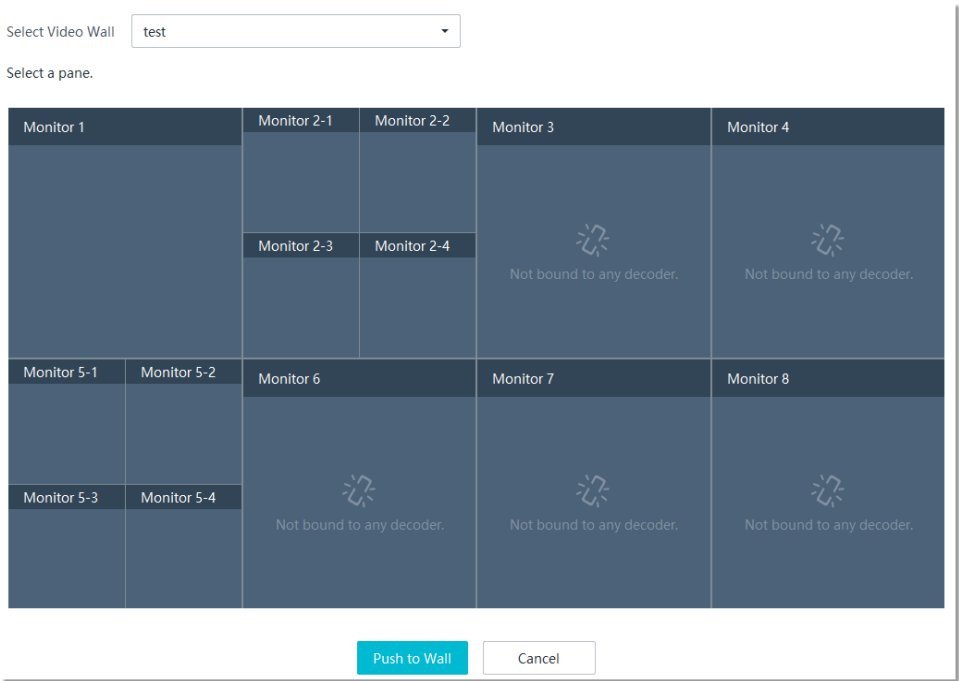
----End

Video Push to the Video Wall by One Click

- Step 1
- On the iClient S100 home page, choose **Basic Operations > Live**.
- Step 2
- Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
- Step 3
- Right-click the live video pane and choose **Push to Video Wall** from the shortcut menu.
- Step 4
- Select the created video pane layout of the video wall from the **Select Video Wall** drop-down list box.
- Step 5
- Drag the camera to the video pane that has been bound to a decoder channel.
[Figure 4-39](#) shows the video wall page.

You can view live video from cameras on the physical video wall.

Figure 4-39 Live video display on the video wall



----End

4.4.3 Cycling on the Video Wall

Prerequisites

You have created a video wall layout and connected a video wall to a decoder as an administrator. For details, see [4.4.1 Configuring a Video Wall](#).

Procedure

- Step 1
- On the iClient S100 home page, choose **Basic Operations > Video Wall**.
- Step 2
- On the **Set Decoder Password** page that is displayed, enter the passwords of all decoders and click **OK**.

- Step 3** Click  in the upper right corner of the page. To add a cycle group for the first time, click +. Otherwise, click **New Group**.
- Step 4** In the **Edit Cycle** window that is displayed, configure cycle group information, as shown in [Figure 4-40](#). [Table 4-23](#) describes the key parameters.

Figure 4-40 Edit Cycle window

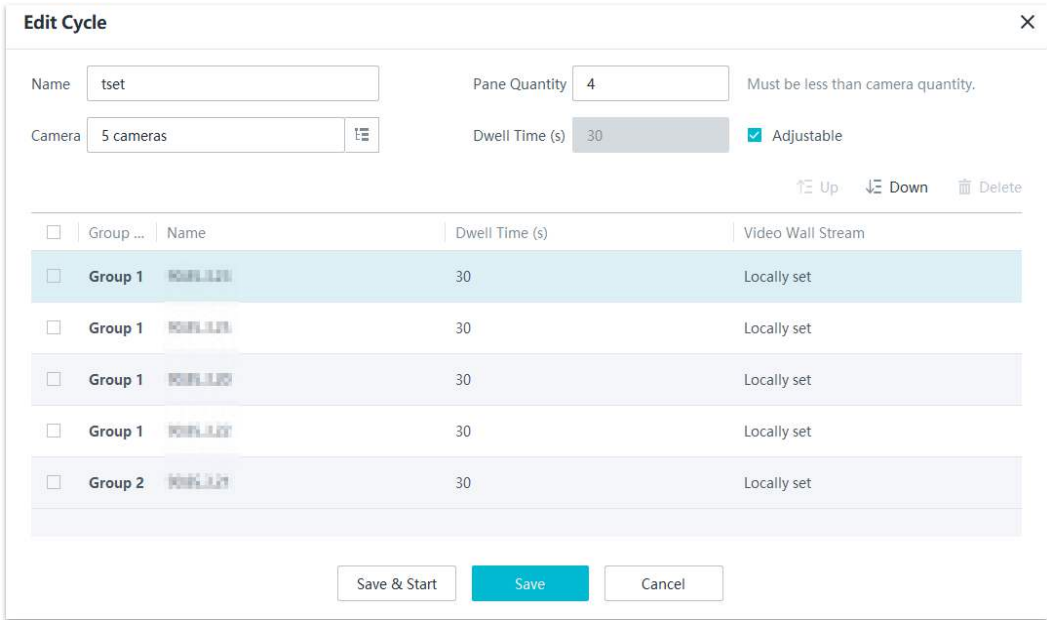
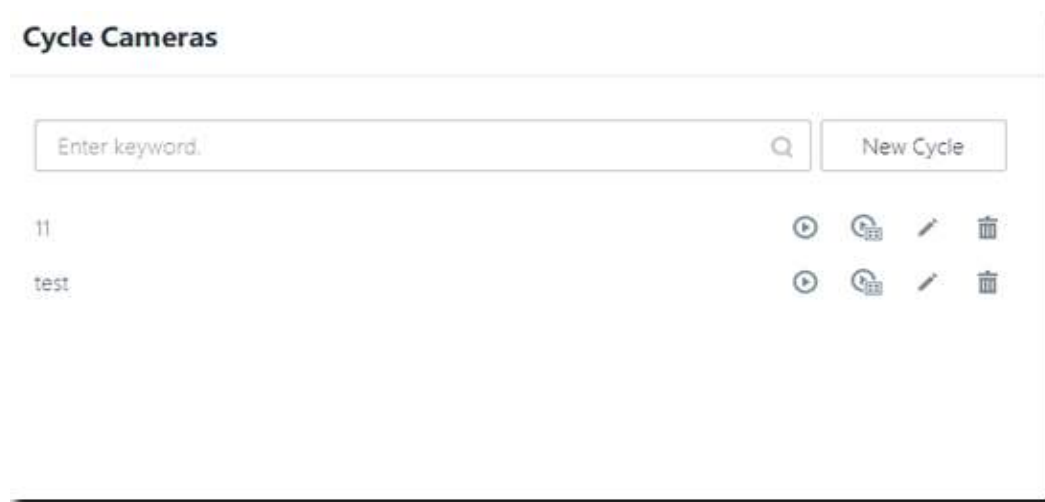


Table 4-23 Key parameters for adding a cycle group

Parameter	Description
Name	Cycle name.
Pane Quantity	Number of cycling panes, which must be less than the number of cameras to cycle.
Camera	Cameras in the cycle.
Dwell Time (s)	Dwell time at selected cameras, which can be manually adjusted. The dwell time can be configured for multiple groups in batches or for a single group. In this example, the dwell time is configured for a single group.

- Step 5** Click  in the upper right corner of the **Video Wall** tab page. The added cycle groups are displayed in the **Cycle Cameras** window, as shown in [Figure 4-41](#).

Figure 4-41 Cycle Cameras

- Click . The selected pane is regarded as the first pane. The live video from corresponding cameras is played in sequence in cycling mode. For example, if pane 2 is selected, and the number of panes is three, live video is displayed in panes 2, 3, and 4 in cycling mode.
- Click  to customize panes for live video viewing in cycling mode.

----End

4.4.4 Video Wall View Management

Application Scenario

This section describes how to configure and manage video wall views. You can add different views and view schedules and configure view cycling as planned to meet specified purposes, improving work efficiency.

Procedure

- Step 1** Choose **Basic Operations > Video Wall** on the iClient S100 home page and double-click the created video wall. The **VideoWall** tab page is displayed.

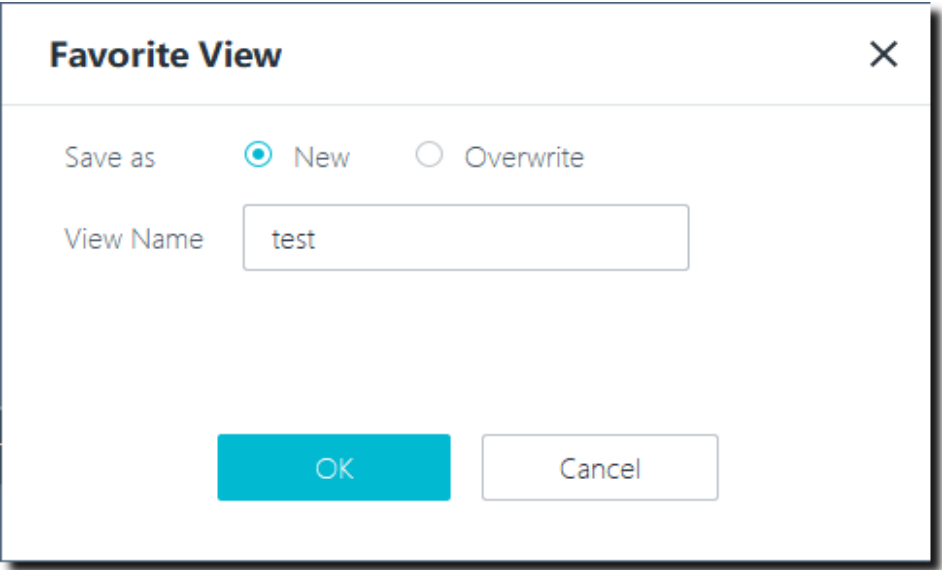
NOTE

If multiple decoders are stored locally, enter the passwords of all the decoders.

- Step 2** Add a view.

1. Choose **Favorites > Favorited Views**, click , and set **Save as** to **New** or **Overwrite**.
 - If you set **Save as** to **New**, set **View Name** and save the view.
 - If you set **Save as** to **Overwrite**, the existing view is overwritten, and the new view is saved.
2. Set **View Name** and click **OK**. The **Favorite View** window is displayed, as shown in [Figure 4-42](#).

Figure 4-42 Favorite View



- 3. Repeat [Step 2.1](#) and [Step 2.2](#) to save more views.

 NOTE

You can also click  Favorite View in the **Pane List** window to add a view.

Step 3 Add a view schedule.

- 1. Click the **Favorites** tab and view the favorited views in the **Favorited Views** panel.
- 2. Click  next to **Favorited Views**. The **View Schedule** page is displayed.
- 3. Click **New Schedule**. In the **New Schedule** window that is displayed, set view schedule parameters, as shown in [Figure 4-43](#). [Table 4-24](#) describes related parameters.

Figure 4-43 New Schedule window

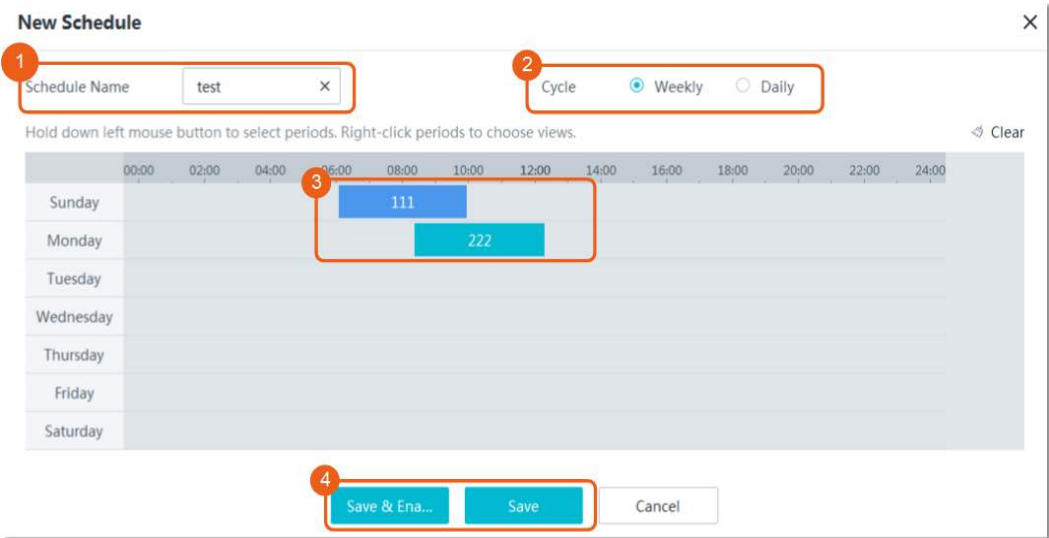
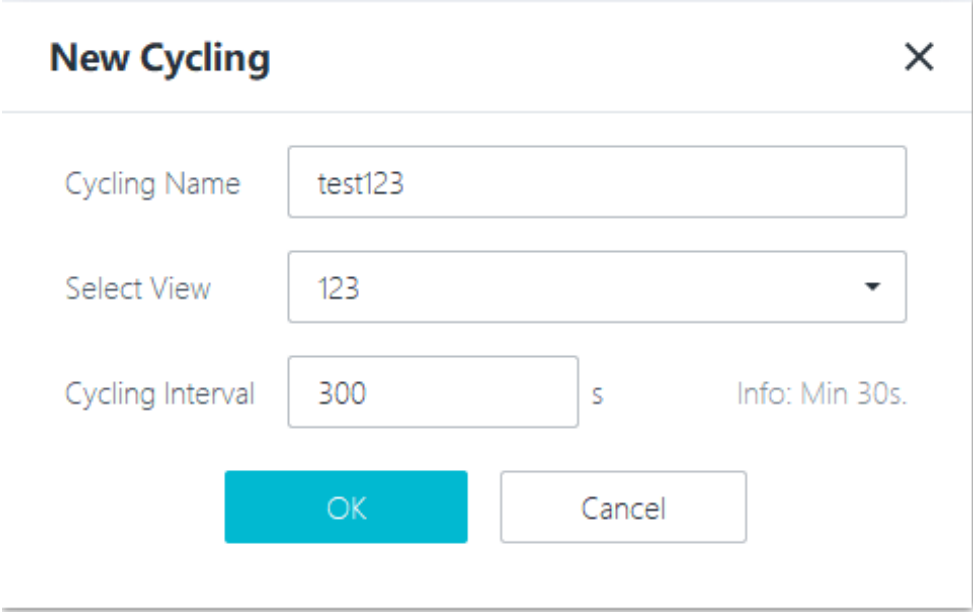


Table 4-24 Parameter description

Parameter	Description
Cycle	Cycle for executing a view schedule. In the preceding figure, this parameter is set to Weekly .
Period	Time range for playing a view. Drag the mouse to configure a specified time segment for view playing. Right-click the time segment and choose a view from the shortcut menu. Double-click the time segment and set specific time points.

Step 4 Add view cycling.

1. Click  next to **Favorited Views**. The **View Cycling** page is displayed.
2. Click **New**. In the **New Cycling** window that is displayed, set cycling parameters, as shown in [Figure 4-44](#). [Table 4-24](#) describes key parameters.

Figure 4-44 New Cycling

The **New Cycling** dialog box is shown with a close button (X) in the top right corner. It contains three input fields: **Cycling Name** with the value "test123", **Select View** with a dropdown menu showing "123", and **Cycling Interval** with a value of "300" and a unit "s". To the right of the interval field is the text "Info: Min 30s.". At the bottom are two buttons: **OK** (in a blue box) and **Cancel** (in a white box with a grey border).

Table 4-25 Key parameter description

Parameter	Description
Select View	Cycling view. Select an existing view from the drop-down list box.
Cycling Interval	Video wall cycling interval.

3. Click **OK**.

----End

4.4.5 Video Wall Window splicing

Application Scenario

Through the splicing of Video Wall windows, multiple small windows of the TV wall physical screen are combined into one large window, so as to highlight the key video pictures on the Video Wall

Prerequisites

You have created a video wall layout and connected a video wall to a decoder as an administrator. For details, see [4.4.1 Configuring a Video Wall](#).

Procedure

Step 1 Choose **Basic Operations > Video Wall** on the iClient S100 home page and double-click the created video wall. The **VideoWall** tab page is displayed.

NOTE

If multiple decoders are stored locally, enter the passwords of all the decoders.

Step 2 Window splicing.

1. Create a video wall, add and bind a decoder.
2. Click **Video Wall** to enter the large screen control and select adjacent screens for splicing. Only rectangular adjacent screens can be spliced. After splicing once, it cannot be spliced again.

Figure 4-45 Before splicing window

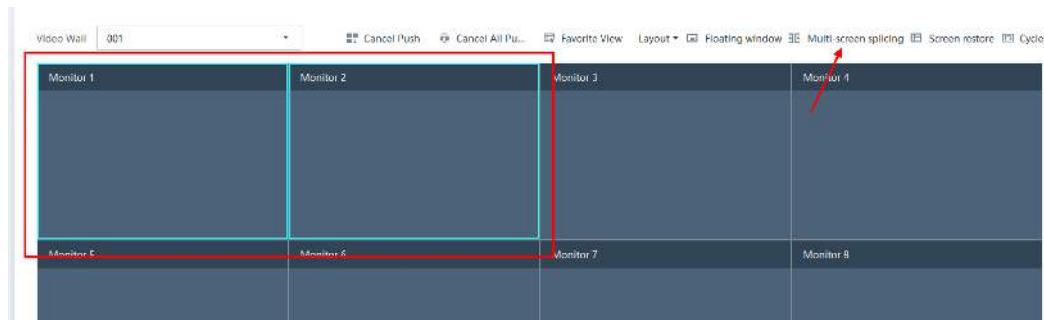
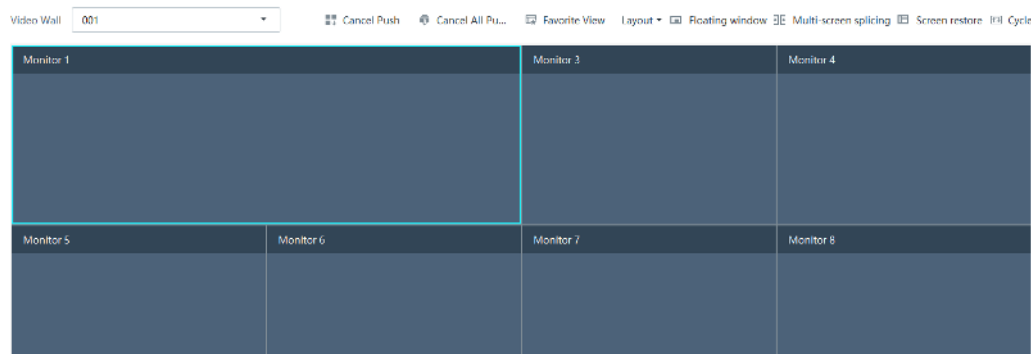


Figure 4-46 After splicing window

----End

4.4.6 Video Wall Floating window

Application Scenario

Open the floating window on the video wall window, and the video picture can be played on the physical screen.

Prerequisites

You have created a video wall layout and connected a video wall to a decoder as an administrator. For details, see [4.4.1 Configuring a Video Wall](#).

Procedure

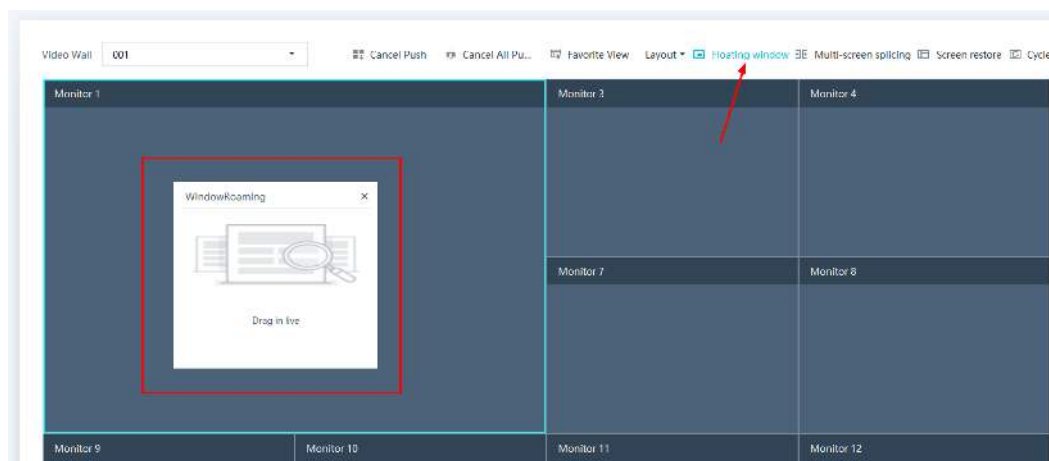
Step 1 Choose **Basic Operations > Video Wall** on the iClient S100 home page and double-click the created video wall. The **VideoWall** tab page is displayed.

NOTE

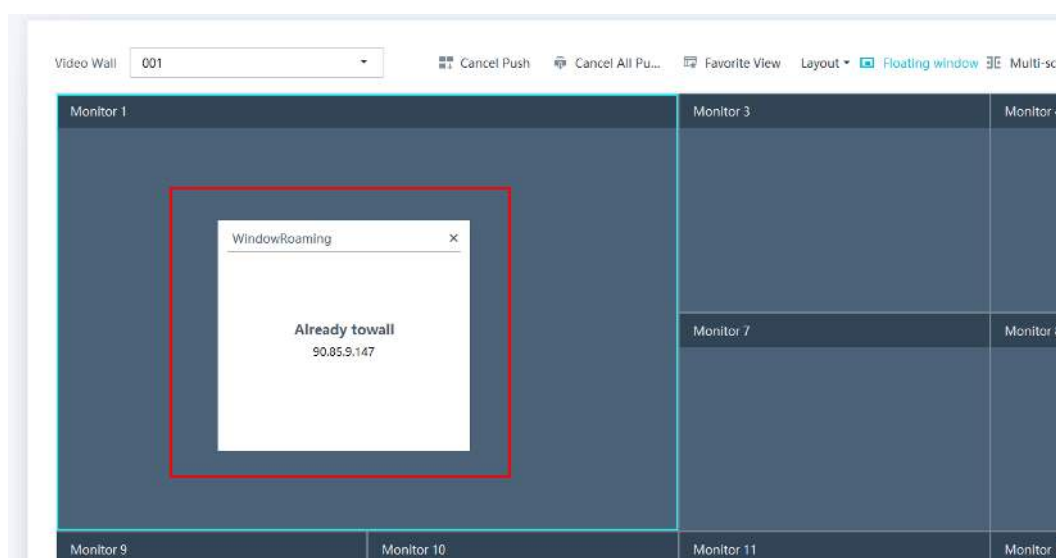
If multiple decoders are stored locally, enter the passwords of all the decoders.

Step 2 Add a floating window.

1. Create a video wall, add and bind a decoder.
2. Click the **Floating window** to draw the floating window on the screen. When you finish drawing the floating window, you need to click **Floating window** again to restore the color of the floating window to the default color.

Figure 4-47 Draw floating window

3. After drawing the floating window, drag the left video channel to the floating window for video playback.

Figure 4-48 Play video

----End

4.4.7 Alarm linkage Video Wall

Application Scenario

For the alarm information received by the iClient S100 client, the user configures the alarm linkage on the wall according to the demand, and pops up the video channel source configured by the user on the TV wall.

Prerequisites

You have created a video wall layout and connected a video wall to a decoder as an administrator. For details, see [4.4.1 Configuring a Video Wall](#).

Procedure

Step 1 Choose **Basic Operations > Video Wall** on the iClient S100 home page and double-click the created video wall. The **VideoWall** tab page is displayed.

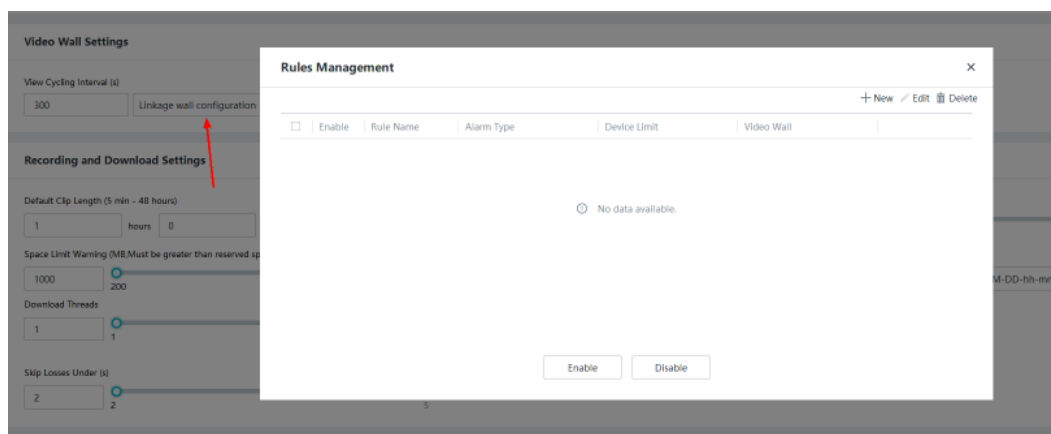
NOTE

If multiple decoders are stored locally, enter the passwords of all the decoders.

Step 2 Add one alarm linkage Video Wall rule.

1. Create a video wall, add and bind a decoder.
2. In the homepage of iclient S100, choose **Personal Configuration > Linkage wall configuration**.

Figure 4-49 Open Linkage wall configuration



3. Click New and enter the information.

Figure 4-50 Add rule

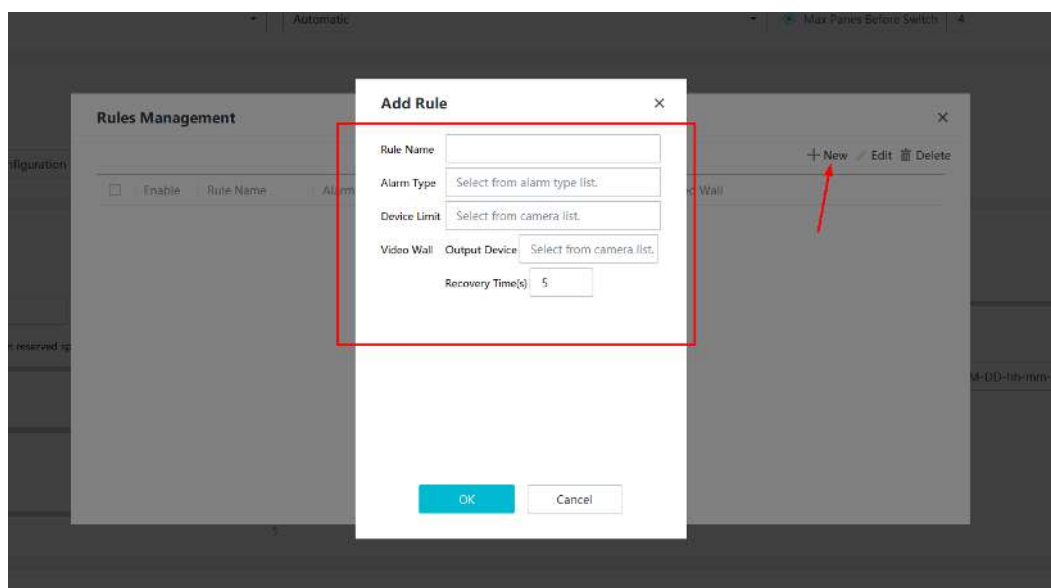
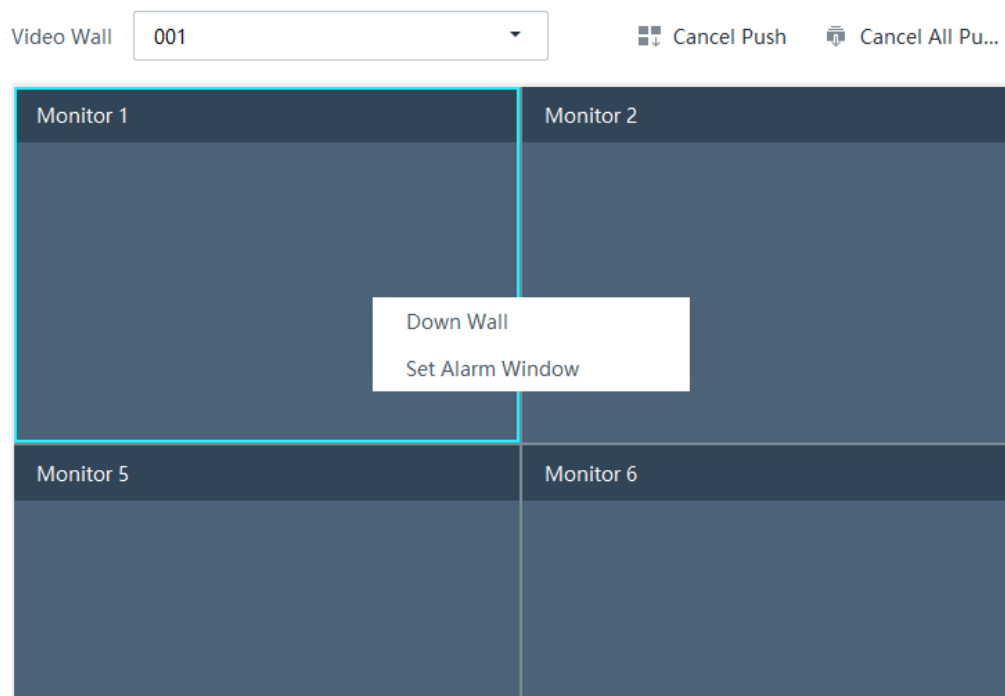


Table 4-26 Key parameter description

Parameter	Description
Rule name	User defined rule name.
Alarm Type	If the alarm type on the wall is selected, the preset alarm type on the wall will be triggered.
Device Limit	The camera managed by iClient S100 indicates that the selected camera will trigger alarm linkage to the wall.
Video Wall Output Device	The camera managed by iClient S100 indicates that after the alarm linkage is triggered, the selected output channel will be played in the TV wall alarm window in turn
Video Wall Recovery Time(s)	Indicates that after the alarm linkage video is played in the alarm window, after the recovery time, the video will automatically recover to the previously played video picture

Step 3 On the large screen control video wall page, select the video wall window and right-click to set the alarm window. After the setting is completed and the alarm linkage is triggered, the alarm output source video screen will pop up on the physical screen corresponding to the window

Figure 4-51 Set alarm window

----End

4.5 Common Intelligence

4.5.1 Motion Detection

The system automatically generates an alarm when a motion is detected in a specified area. Security personnel can view the video image to identify harmful objects and take necessary actions.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml.

NOTE

- Motion detection cannot be enabled for cameras connected to main devices through ONVIF. Therefore, it is recommended that cameras be connected to main devices through HWSDK.
- The following describes the configuration on the iClient S100. For details about the configuration in the camera web system, see the camera product documentation of the required series and version.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Ordinary Intelligence > MotionDetection**.
- Step 3** Toggle-on **Enable Motion Detection**, draw a detection area, and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 4-27](#) describes the parameters.

Table 4-27 Parameter description

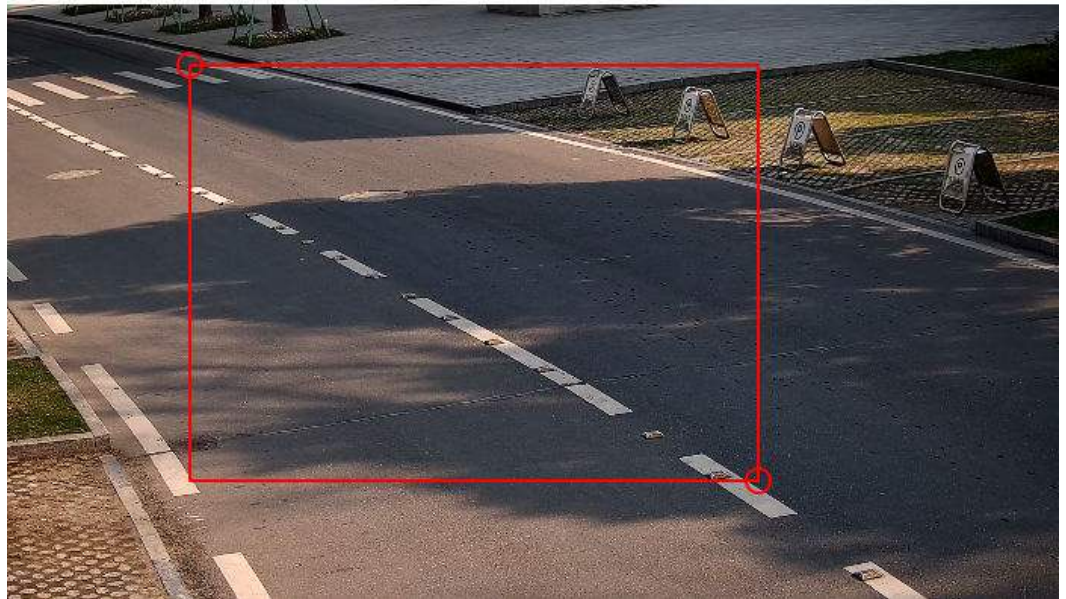
Parameter	Description
Alarm Detection Interval(s)	Interval at which the camera checks for object motion. If motion is detected, the camera reports an alarm. If an object keeps moving in the detection area, only one alarm is reported during each motion detection interval.
Sensitivity	Motion detection sensitivity. A larger value indicates a higher sensitivity. If a higher sensitivity level is used, more slight motions can be detected.

2. Set audible and visual alarm parameters. [Table 4-28](#) describes the parameters.

Table 4-28 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters, as shown in [Figure 4-52](#). [Table 4-29](#) describes the parameters.

Figure 4-52 Setting an area**▲ Area Settings**+ Area  Delete**Table 4-29** Area settings

Button	Description
+Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.

- Set plan parameters. [Table 4-30](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-30 Plan settings

Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.

Parameter/ Button	Description
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.5.2 Lens Blocking Detection

The system automatically generates an alarm when a camera lens is blocked by an object in a specified area. Security personnel can view the video image to check onsite situations and take necessary actions.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml.

NOTE

- Lens blocking detection cannot be enabled for cameras connected to main devices through ONVIF. Therefore, it is recommended that cameras be connected to main devices through HWSDK.
- The following describes the configuration on the iClient S100. For details about the configuration in the camera web system, see the camera product documentation of the required series and version.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Ordinary Intelligence > VideoOcclusion**.
- Step 3** Toggle-on **Enable Video Occlusion** and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 4-31](#) describes the parameters.

Table 4-31 Parameter description

Parameter	Description
Alarm Detection Interval(s)	Interval at which the camera checks for object motion. If motion is detected, the camera reports an alarm. If an object keeps moving in the detection area, only one alarm is reported during each motion detection interval.
Sensitivity	Motion detection sensitivity. A larger value indicates a higher sensitivity. If a higher sensitivity level is used, more slight motions can be detected.

2. Set audible and visual alarm parameters. [Table 4-32](#) describes the parameters.

Table 4-32 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	

Parameter	Description	Requirement on Cameras
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set plan parameters. [Table 4-33](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-33 Plan settings

Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.5.3 Audio Diagnosis

The system generates an alarm when abnormal sounds around a camera is detected. When abnormal sounds around the camera are detected, the NVR800 reports alarm information.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml.

NOTE

- Audio diagnosis cannot be enabled for cameras connected to main devices through ONVIF. Therefore, it is recommended that cameras be connected to main devices through HWSKD.
- Intelligent cameras with microphones are available.
- The following describes the configuration on the iClient S100. For details about the configuration in the camera web system, see the camera product documentation of the required series and version.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Ordinary Intelligent > SoundDiagnosis**.
- Step 3** Set parameters for audio diagnosis, as shown in [Figure 4-53](#). [Table 4-34](#) describes the parameters and button.

Figure 4-53 Setting parameters for audio diagnosis

Audio Abnormality
 Enable AudioAbnormality ☒
 Audio Abnormality Sensitivity
 Low

Audio Rise
 Enable Audio Rise ☒
 Audio Rise Sensitivity
 1 100 54

Audio Drop
 Enable Audio Drop ☒
 Audio Drop Sensitivity
 1 100 33

Plan
 Sound Diagnosis Type
 Audio Abnormality

+ Add - Delete All

No.	Execution Date	Start Time	End Time	Date	Mode	Operation
1	2021-03-24	00:00:00	23:59:59	Every Day	Weekly cycle	

Save Cancel

Table 4-34 Parameter/Button description

Parameter/Button		Description
Audio Abnormality	Enable AudioAbnormality	Indicates whether to enable audio abnormality detection. After this function is enabled, an alarm is generated if abnormal sound around a camera is detected.

Parameter/Button		Description
	Audio Abnormality Sensitivity	Audio abnormality detection sensitivity. • Low: corresponds to sound intensity 5. • Middle: corresponds to sound intensity 10. • High: corresponds to sound intensity 20.
Audio Rise	Enable Audio Rise	Indicates whether to enable sudden volume increase detection. After this function is enabled, an alarm is generated if the volume of ambient sound suddenly increases.
	Audio Rise Sensitivity	Sensitivity for sudden volume increase detection. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.
Audio Drop	Enable Audio Drop	Indicates whether to enable sudden volume decrease detection. After this function is enabled, an alarm is generated if the volume of ambient sound suddenly decreases.
	Audio Drop Sensitivity	Sensitivity for sudden volume decrease detection. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.
Plan	Sound Diagnosis Type	Select the audio diagnosis type for which you want to configure an alert plan. • Audio Abnormality • Audio Rise • Audio Drop
	Add	Adds an alert plan. A maximum of eight alert plans can be added.
	Execution Date	Start date when an audio diagnosis task is executed. The value is automatically generated based on the value of Date and cannot be changed. • If Date is set to Every Day, the value of this parameter is the current date. • If Date is set to Monday, the value of this parameter is the date of next Monday.
	Date	Date on which an alert plan is to be executed. • Every Day • Monday to Sunday
	Mode	Indicates whether to cyclically execute an alert plan. • Weekly cycle • Do not loop

Step 4 Click **Save**.

----End

Verification

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.5.4 Privacy Mask

In scenarios where the content in some areas (such as whiteboard information in an office) may involve business secrets and should not be viewed by others (including security personnel), the privacy mask function is required. You can configure the privacy mask function in the camera web system or on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Double-click a camera connected to a main device and choose **Video Channel > Privacy Mask**.
- Step 3** Set parameters for privacy mask, as shown in [Figure 4-54](#). [Table 4-35](#) describes the parameters.

Figure 4-54 Setting parameters for privacy mask

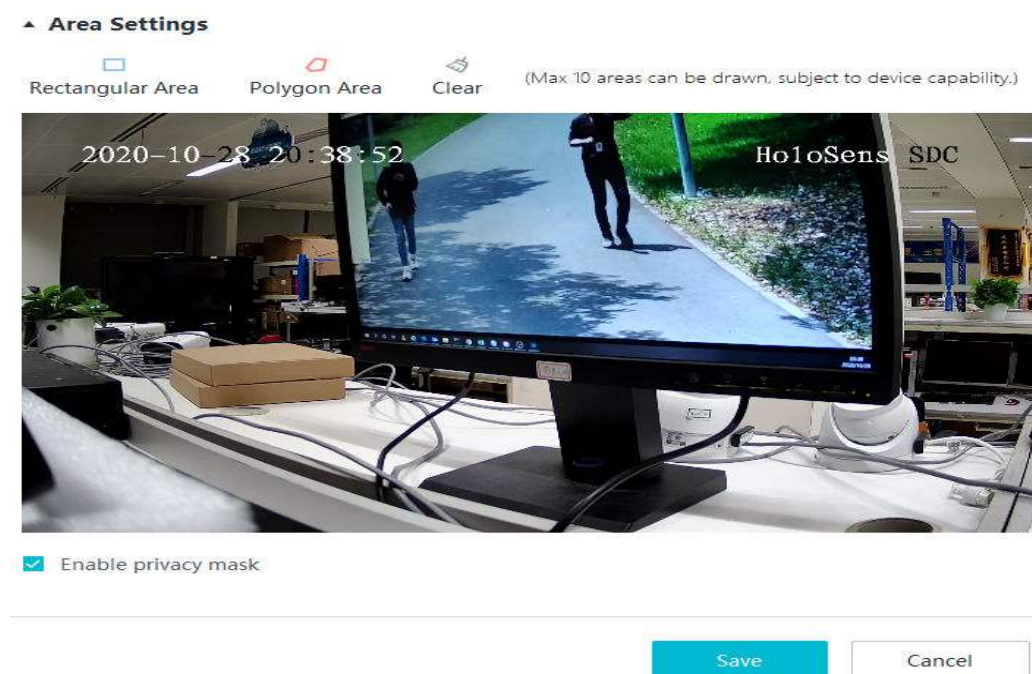


Table 4-35 Parameter description

Parameter	Description
Area Settings	You can box-select one or more rectangular areas on a video image for privacy mask. A maximum of 10 areas are allowed. NOTE You can select Polygon Area only for cameras connected through the HWSDK protocol.
Enable privacy mask	Indicates whether to enable privacy mask for the box-selected area.

Step 4 Click **Save**.

----End

Verification

After the privacy mask is configured, you can view the result on the **Live** and **Playback** page. The following takes the **Live** page as an example.

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 View the camera image. The image in the privacy mask area cannot be viewed during live video viewing or recording playback.

----End

4.6 Behavior Analysis

4.6.1 Function Description

The intelligent video analysis technology can be used to analyze and match the video signals captured by cameras based on preconfigured rules, decreasing the workload of observation personnel and reducing mistakes caused by negligence.

Based on the devices that execute intelligent analysis tasks, behavior analysis can be classified into frontend behavior analysis and backend behavior analysis. You can select frontend behavior analysis for a camera that supports behavior analysis and backend behavior analysis for one that does not.

- Frontend behavior analysis: Cameras themselves provide the behavior analysis function.. After you configure behavior analysis tasks on the client, the client delivers the tasks to cameras for execution.
- Backend behavior analysis: Required algorithm plug-ins should be installed on main devices to perform behavior analysis on video.

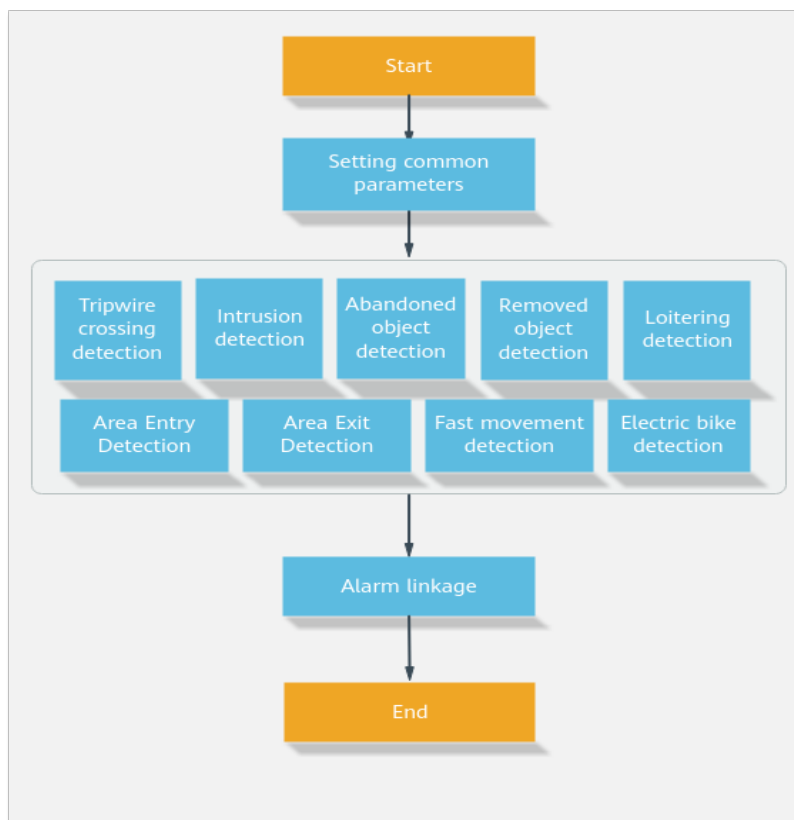
The main device NVR800 supports only frontend behavior analysis. That is, you can configure behavior analysis tasks only for cameras connected to the NVR800 on the iClient S100. [Table 4-36](#) lists the behavior analysis functions supported by the NVR800.

Table 4-36 Behavior analysis functions

Behavior Analysis	Description
Tripwire crossing detection	The system automatically generates an alarm when an object crosses a tripwire from the specified direction in a specified detection area.
Intrusion detection	The system automatically generates an alarm when an object enters a specified detection area.
Abandoned object detection	The system automatically generates an alarm when an object is abandoned in a specified detection area. The system allows you to specify the shape (rectangle or polygon) of a detection area.
Removed object detection	The system automatically generates an alarm when an object is removed from a specified detection area.
Loitering detection	The system automatically generates an alarm when a person is loitering in a specified detection area for a specified time.
Area entry detection	The system automatically generates an alarm when a person or an object enters an area that is not allowed to enter.
Area exit detection	The system automatically generates an alarm when a person or an object exits an area that is not allowed to exit.
Fast movement detection	The system automatically generates an alarm when an object moves fast to prevent security risks.
Electric bike detection	The system automatically generates an alarm when an electric bike enters a specified area.

4.6.2 Configuration Process

Before using frontend behavior analysis, you need to configure intelligent analysis tasks for cameras that support intelligent analysis. [Figure 4-55](#) shows the configuration process.

Figure 4-55 Process for configuring frontend behavior analysis tasks**NOTE**

- Currently, you can configure intelligent analysis tasks on the iClient S100 only for cameras that support intelligent analysis and are connected to main devices through HWSDK. In this way, alarms generated by these cameras can be reported to the iClient S100.
- This section describes the configuration on the iClient S100 as an example. For details about the configuration in the camera web system, see the camera product documentation of the corresponding series and version.

4.6.3 Global Configuration

Before configuring behavior analysis on the iClient S100, you need to complete the global configuration.

Prerequisites

You have connected cameras that support intelligent analysis to the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Global Configuration**. The tab page shown in [Figure 4-56](#) is displayed.

Figure 4-56 Global Configuration tab page

The screenshot shows the Global Configuration tab page with the following settings:

- Enable Behavior Analysis:** Toggle switch is turned on (blue).
- Send Metadata:** Toggle switch is turned on (blue).
- Perimeter enhancement:** Toggle switch is turned on (blue).
- Alarm suppression:** Toggle switch is turned on (blue).
- Information Superimposed on Alarm Images:** Toggle switch is turned on (blue).
- Shadow Mode:** Dropdown menu set to "Weak".
- Detection sensitivity:** Dropdown menu set to "Low".
- Background update rate:** Dropdown menu set to "Low".
- Min. object size:** Two input boxes with values "5" and "5", separated by an "X".
- Max. object size:** Two input boxes with values "100" and "200", separated by an "X".

1. Toggle-on **Enable Behavior Analysis** and set global parameters. [Table 4-37](#) describes the parameters.

Table 4-37 Parameter description

Parameter	Description
Send Metadata	Indicates whether to send metadata when the NVR800/IVS1800 is connected to the upper-level platform. If this function is enabled, cameras will send metadata such as snapshots and structured data to the upper-level platform. Then the upper-level platform can perform search by criteria based on the metadata sent by the main device.
Perimeter enhancement	Indicates whether to send a full image as TLV metadata.
Alarm suppression	Indicates whether to send only the alarm that is triggered for the first time.
Information Superimposed on Alarm Images	Indicates whether to superimpose the target frame and rule frame that trigger alarms on full images sent as metadata.

Parameter	Description
Shadow Mode	Shadow strength. The options are Weak , Common , and Strong .
Detection Sensitivity	Sensitivity for triggering alarms. The options are Low , Medium , and High . – A higher sensitivity indicates a higher possibility of triggering alarms, which may lead to false alarms. For example, after you set a high sensitivity for intrusion detection, a false alarm may be reported when an object passes by a sensitive area. – A lower sensitivity indicates a lower possibility of triggering alarms, which may lead to missing alarms. For example, after you set a low sensitivity for tripwire crossing detection, an alarm may not be reported when an object passes one end of a tripwire.
Background update rate	Speed of integrating an object with the background. A larger value indicates quicker object integration.
Min. object size	Minimum size of an object that can be detected on video images in the CIF (352 x 288) resolution. No alarm is generated when an object smaller than the minimum size violates the detection rules. NOTE The minimum object size supported by behavior analysis is 5 x 5 pixels (using 352 x 288 as the standard).
Max. object size	Maximum size of an object that can be detected on video images in the CIF (352 x 288) resolution. No alarm is generated when an object larger than the maximum size violates the detection rules. NOTE The maximum object size supported by behavior analysis is 200 x 200 (using 352 x 288 as the standard).

Step 4 Click **Save**.

----End

4.6.4 Tripwire Crossing Detection

Tripwire crossing detection is used to detect whether an object crosses the tripwire from the specified direction in a detection area. If so, an alarm is generated. Management personnel can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273283512.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Tripwire** and set related parameters.
1. Set parameters in the **Parameter Settings** area. [Table 4-38](#) describes the parameters.

Table 4-38 Parameter description

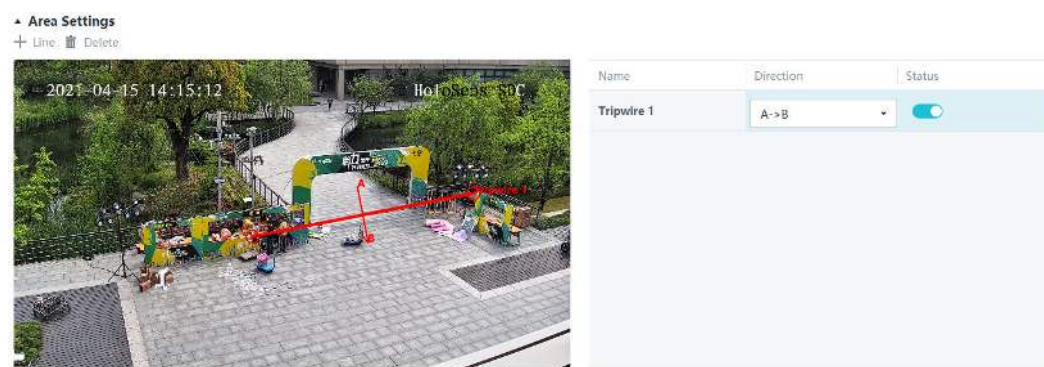
Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 4-39](#) describes the parameters.

Table 4-39 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters, as shown in [Figure 4-57](#). [Table 4-40](#) describes the parameters.

Figure 4-57 Configuring tripwire crossing detection**Table 4-40** Area settings

Parameter/ Button	Description
+ Line	Button for adding a detection line. A maximum of four detection lines are supported. You can select a detection line and drag it to change its location or change its length.
Delete	Button for deleting a selected detection area.
Direction	Specified direction in which a pedestrian crosses the detection line. The options are as follows: A<->B , A->B , and B->A
Status	- If the parameter is toggled-on, the detection line turns red and the detection takes effect. - If the parameter is toggled-off, the detection line turns white and the detection stops.

4. Set plan parameters. [Table 4-41](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-41 Plan settings

Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: - Every Day - Monday to Sunday

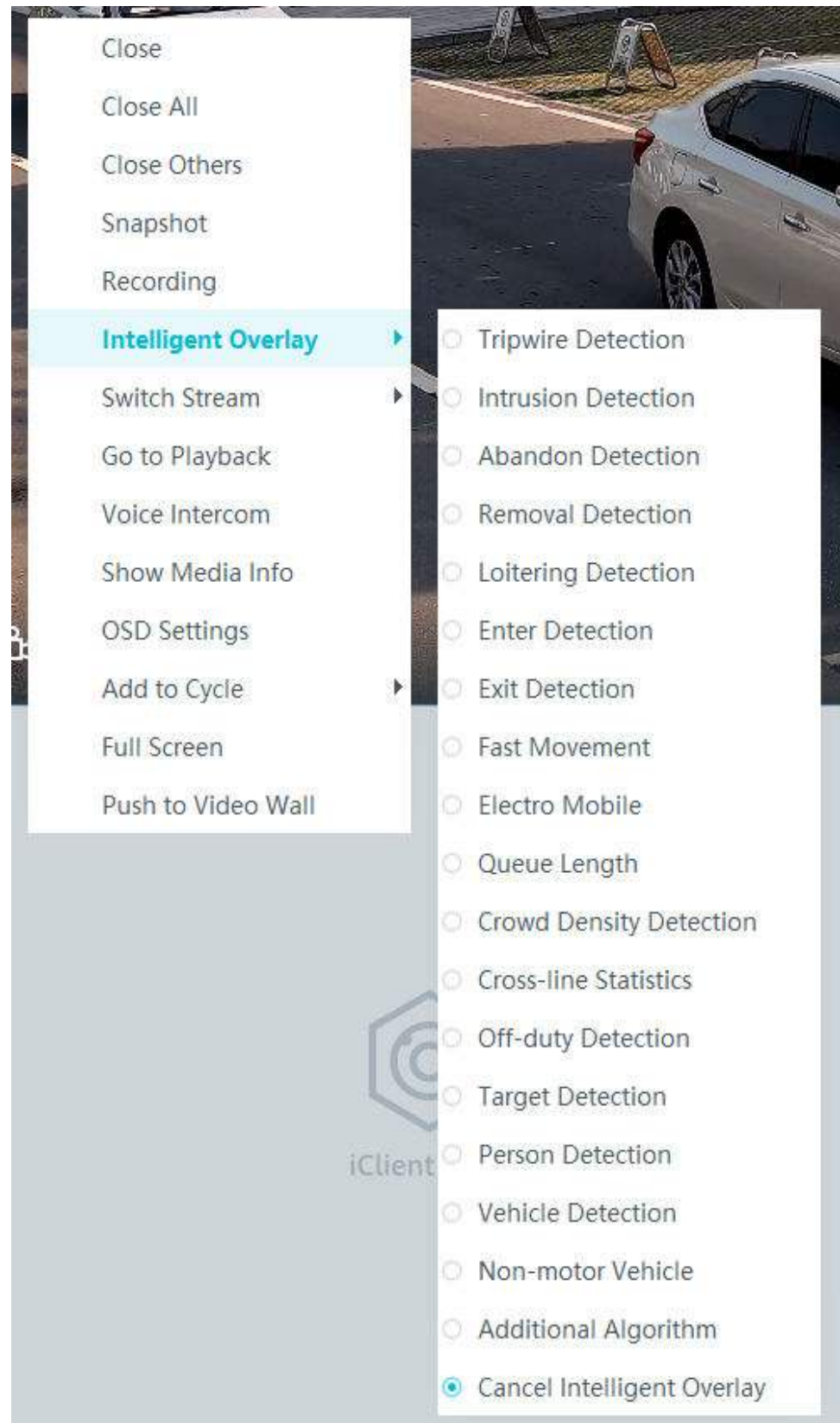
Parameter/ Button	Description
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-58](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-58 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.6.5 Intrusion Detection

Intrusion detection is used to detect whether an object enters an important detection area for which behavior analysis rules have been configured. If so, an alarm is generated. You can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273283512.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Intrusion** and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 4-42](#) describes the parameters.

Table 4-42 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 4-43](#) describes the parameters.

Table 4-43 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 4-59](#). [Table 4-44](#) describes the parameters.

Figure 4-59 Setting detection areas



Table 4-44 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 4-45](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-45 Plan settings

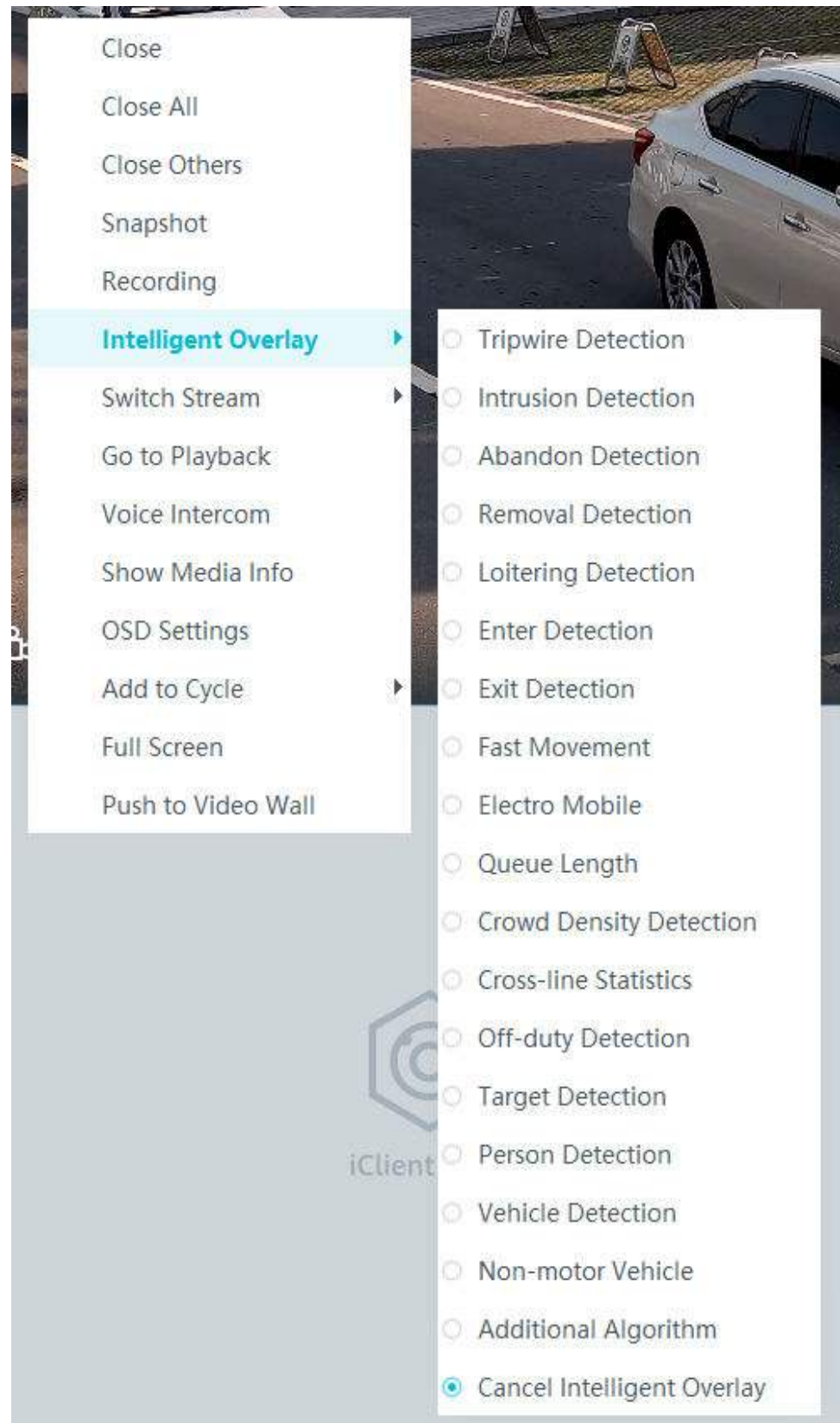
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-60](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-60 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

4.6.6 Abandoned Object Detection

Abandoned object detection is used to detect whether an object is abandoned in a detection area longer than the specified threshold (for example, 10 seconds). If so, an alarm is generated. Management personnel can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see [4.6.3 Global Configuration](#).

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Abandoned** and set related parameters.
1. Set parameters in the **Parameter Settings** area. [Table 4-46](#) describes the parameters.

Table 4-46 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 4-47](#) describes the parameters.

Table 4-47 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 4-61](#). [Table 4-48](#) describes the parameters.

Figure 4-61 Setting detection areas

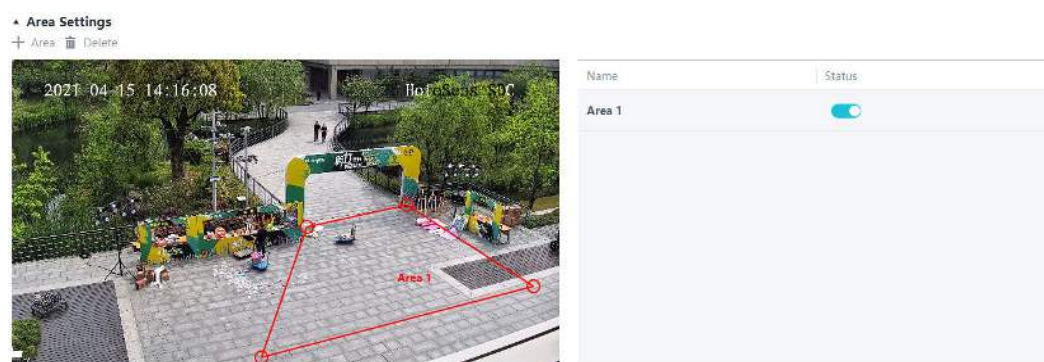


Table 4-48 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 4-49](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-49 Plan settings

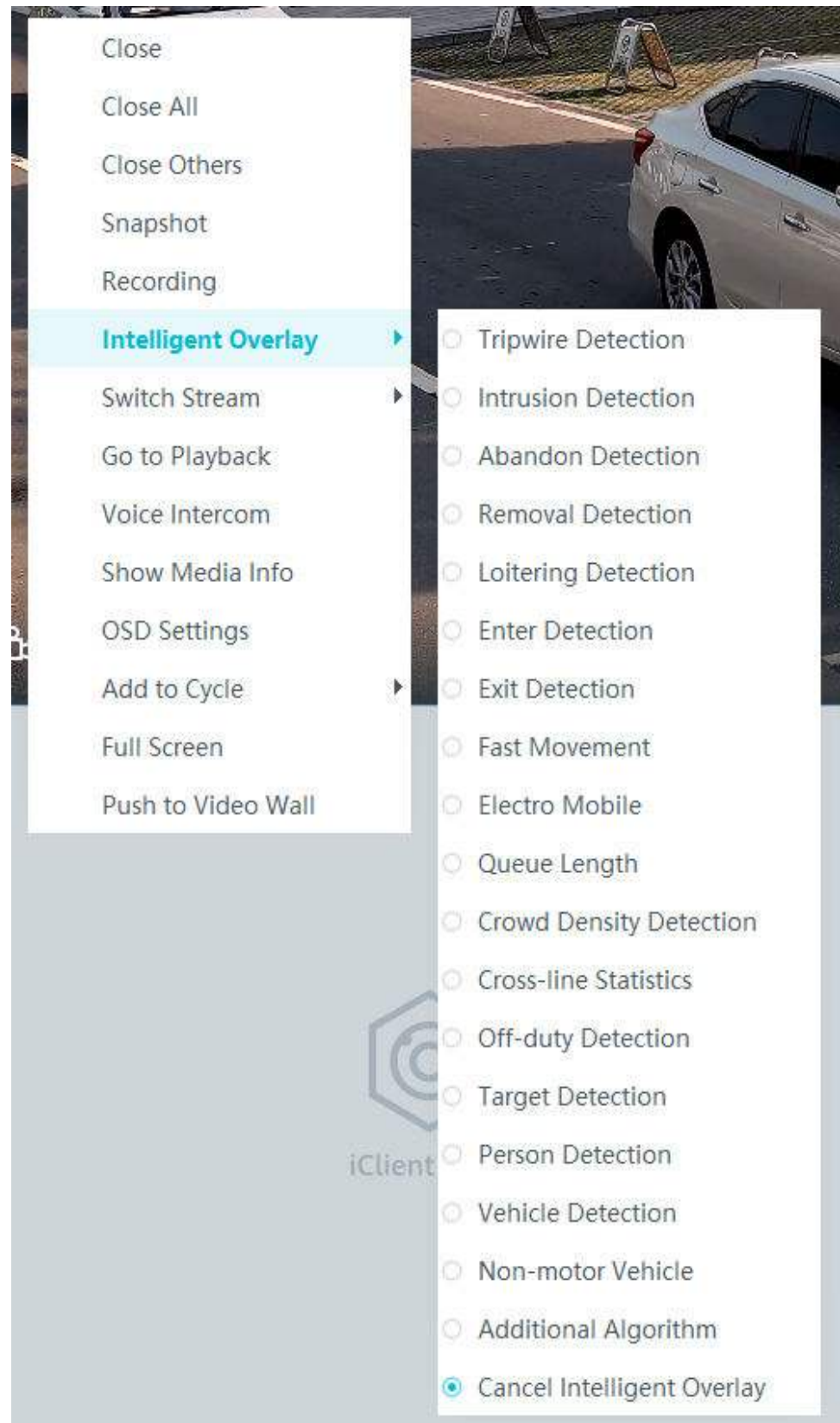
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-62](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-62 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

4.6.7 Removed Object Detection

Removed object detection is used to detect whether an object in a detection area is removed. If so, an alarm is generated. Management personnel can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see [4.6.3 Global Configuration](#).

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Removal** and set related parameters.
1. Set parameters in the **Parameter Settings** area. [Table 4-50](#) describes the parameters.

Table 4-50 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 4-51](#) describes the parameters.

Table 4-51 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 4-63](#). [Table 4-52](#) describes the parameters.

Figure 4-63 Setting detection areas

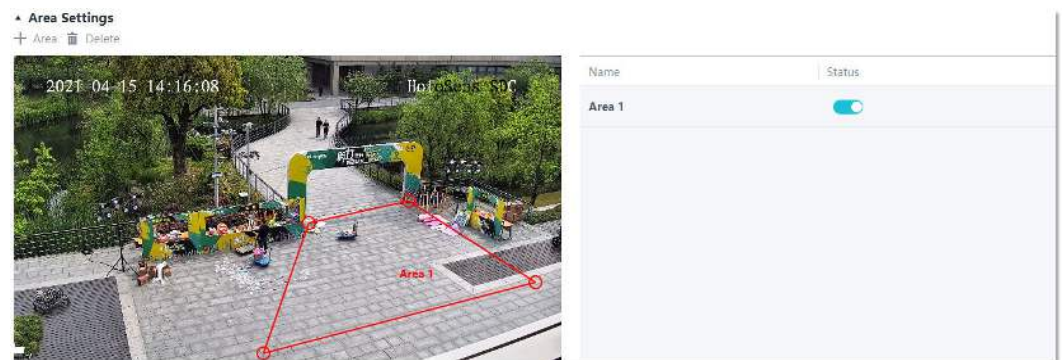


Table 4-52 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 4-53](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-53 Plan settings

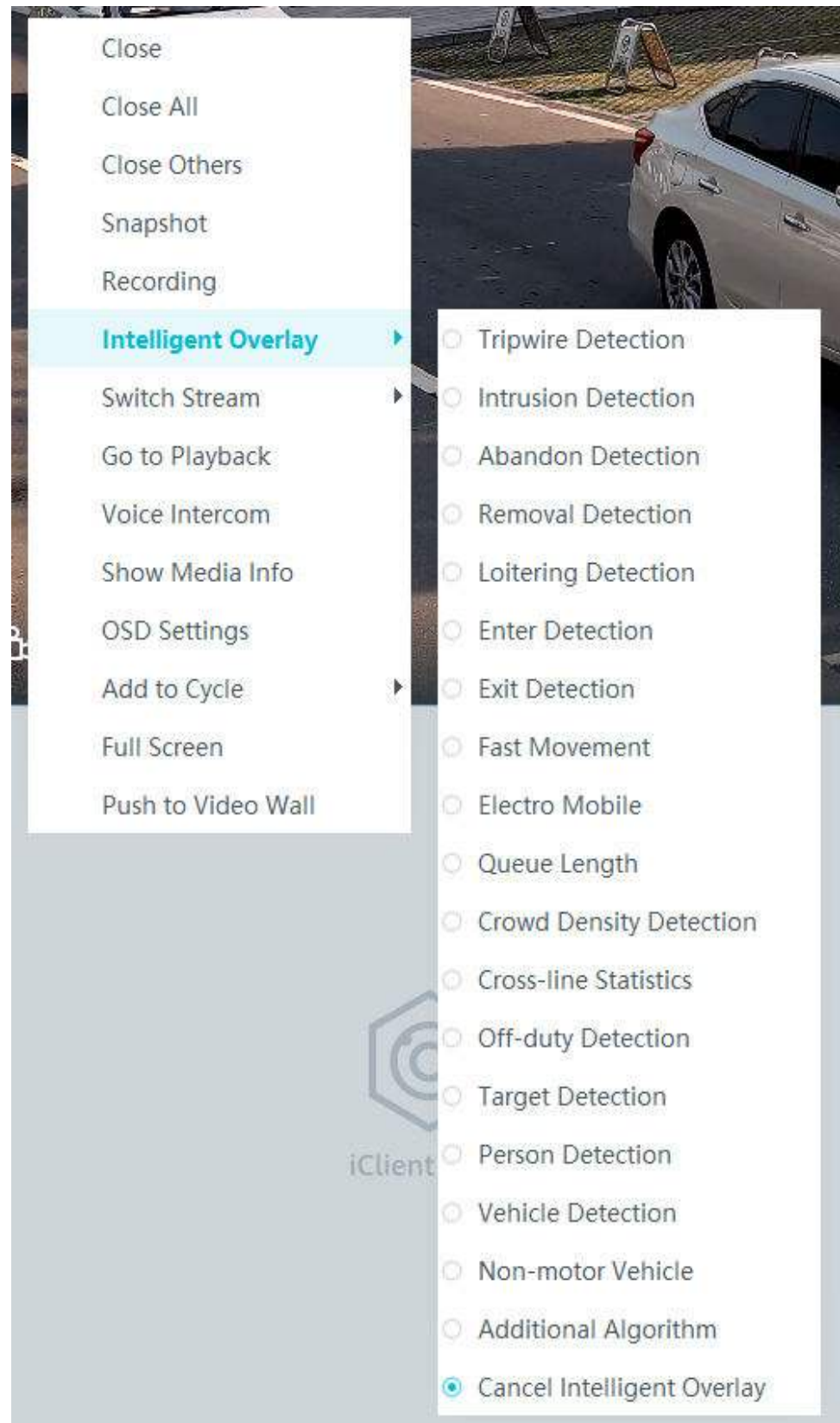
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-64](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-64 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

4.6.8 Loitering Detection

Loitering detection is used to detect whether an object loiters in a detection area for a duration longer than the specified threshold. If so, an alarm is generated. Management personnel can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273283512.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Loitering** and set parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 4-54](#) describes the parameters.

Table 4-54 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 4-55](#) describes the parameters.

Table 4-55 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 4-65](#). [Table 4-56](#) describes the parameters.

Figure 4-65 Setting detection areas

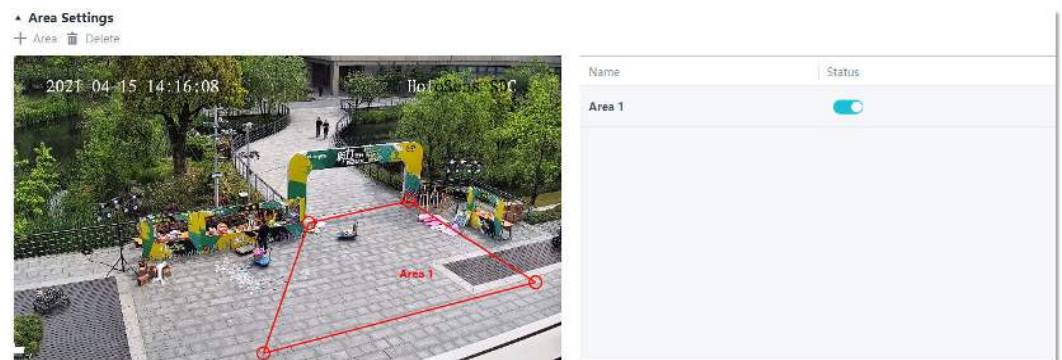


Table 4-56 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 4-57](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-57 Plan settings

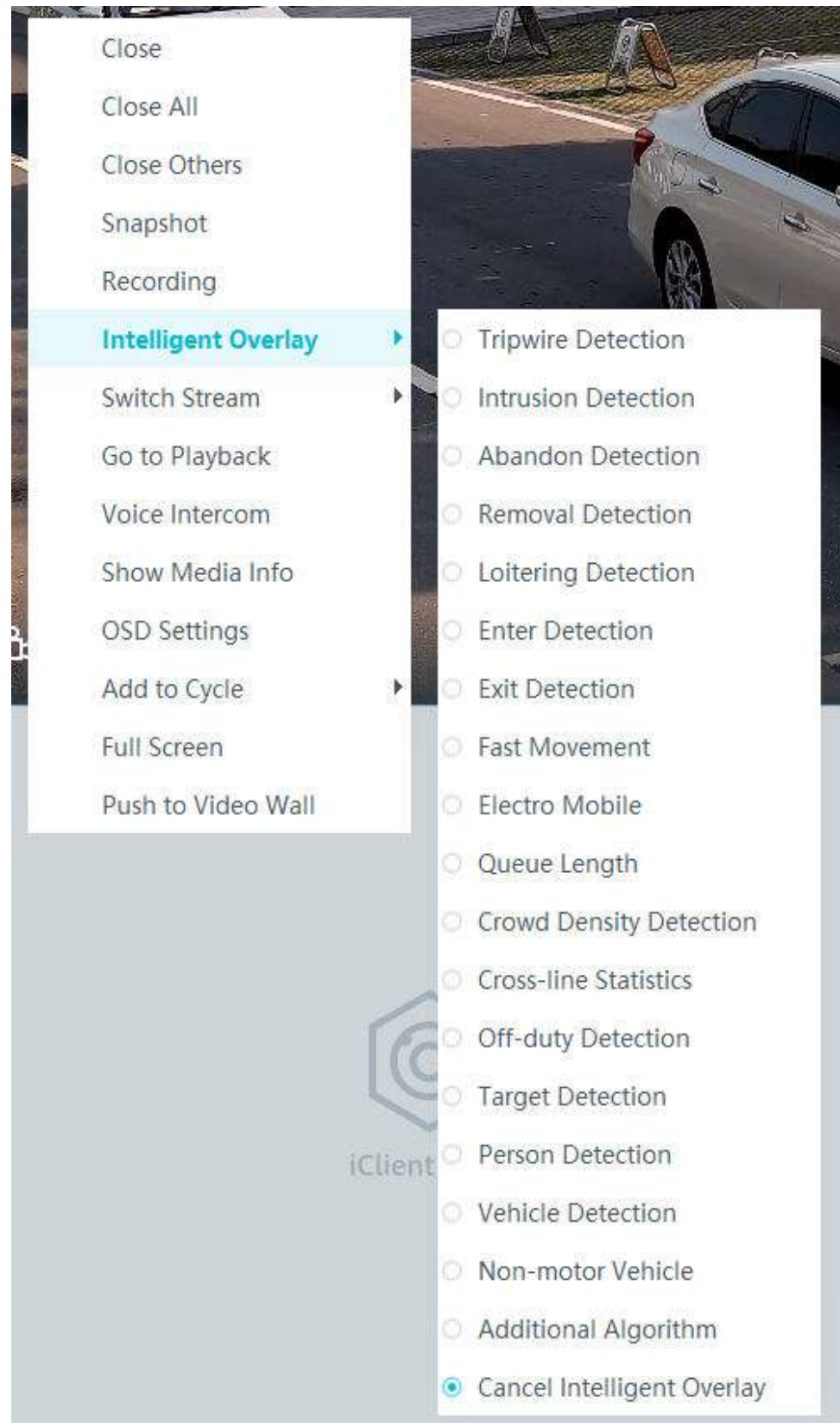
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-66](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-66 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

4.6.9 Area Entry Detection

Area entry detection is used to detect whether an object enters a detection area. If so, an alarm is generated. You can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Area Enter** and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 4-58](#) describes the parameters.

Table 4-58 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 4-59](#) describes the parameters.

Table 4-59 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 4-67](#). [Table 4-60](#) describes the parameters.

Figure 4-67 Setting detection areas



Table 4-60 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 4-61](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-61 Plan settings

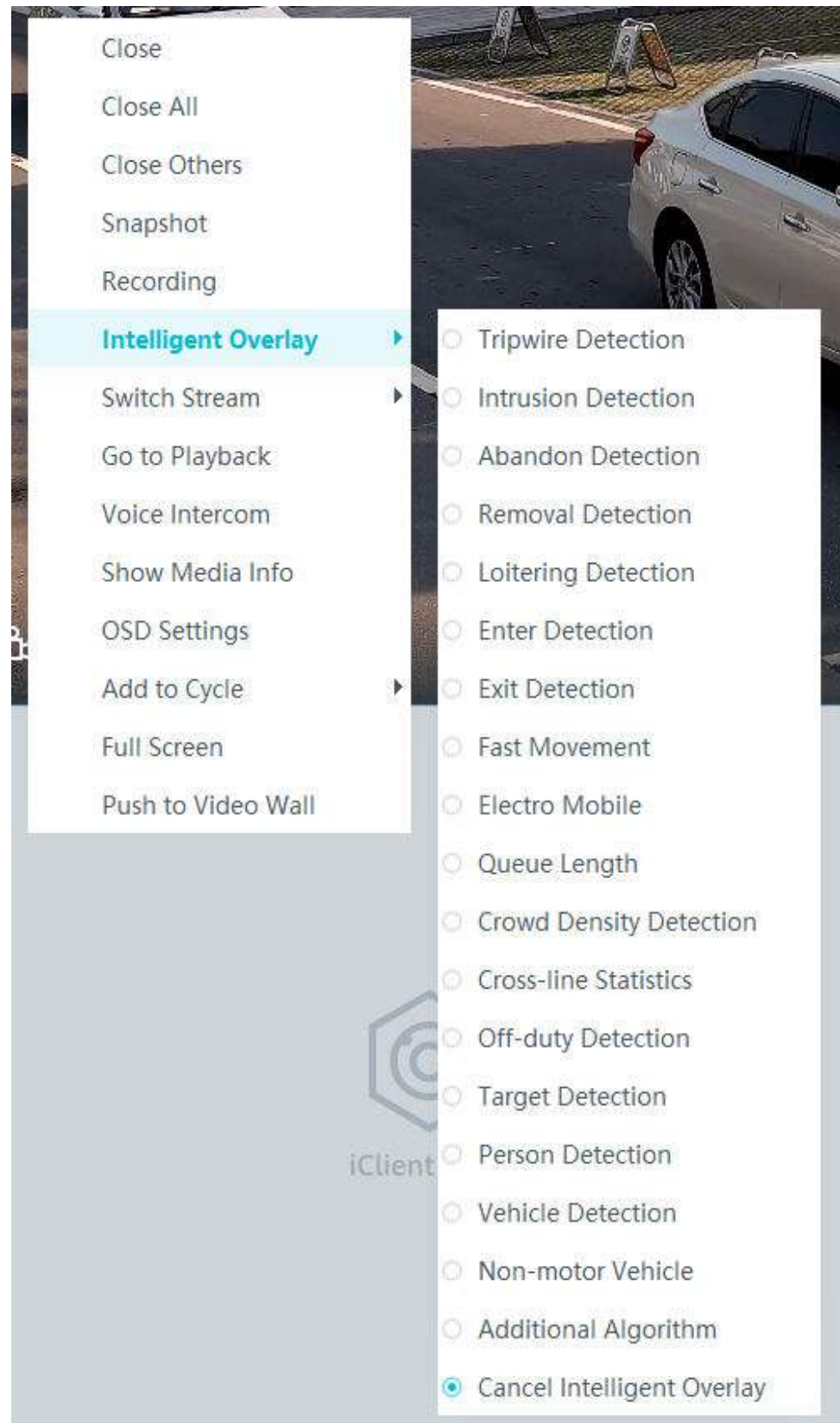
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-68](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-68 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

4.6.10 Area Exit Detection

Area exit detection is used to detect whether an object leaves a detection area. If so, an alarm is generated. You can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Click the **Behavior Analysis** tab and then the **Area Exit** tab, and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 4-62](#) describes the parameters.

Table 4-62 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 4-63](#) describes the parameters.

Table 4-63 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 4-69](#). [Table 4-64](#) describes the parameters.

Figure 4-69 Setting detection areas

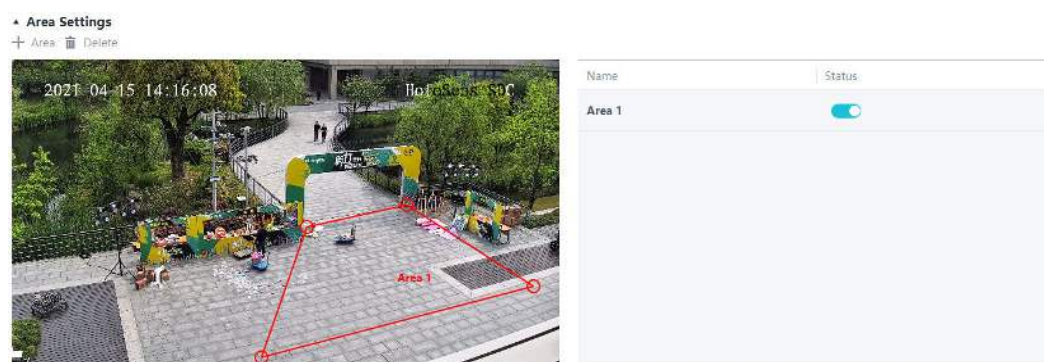


Table 4-64 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 4-65](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-65 Plan settings

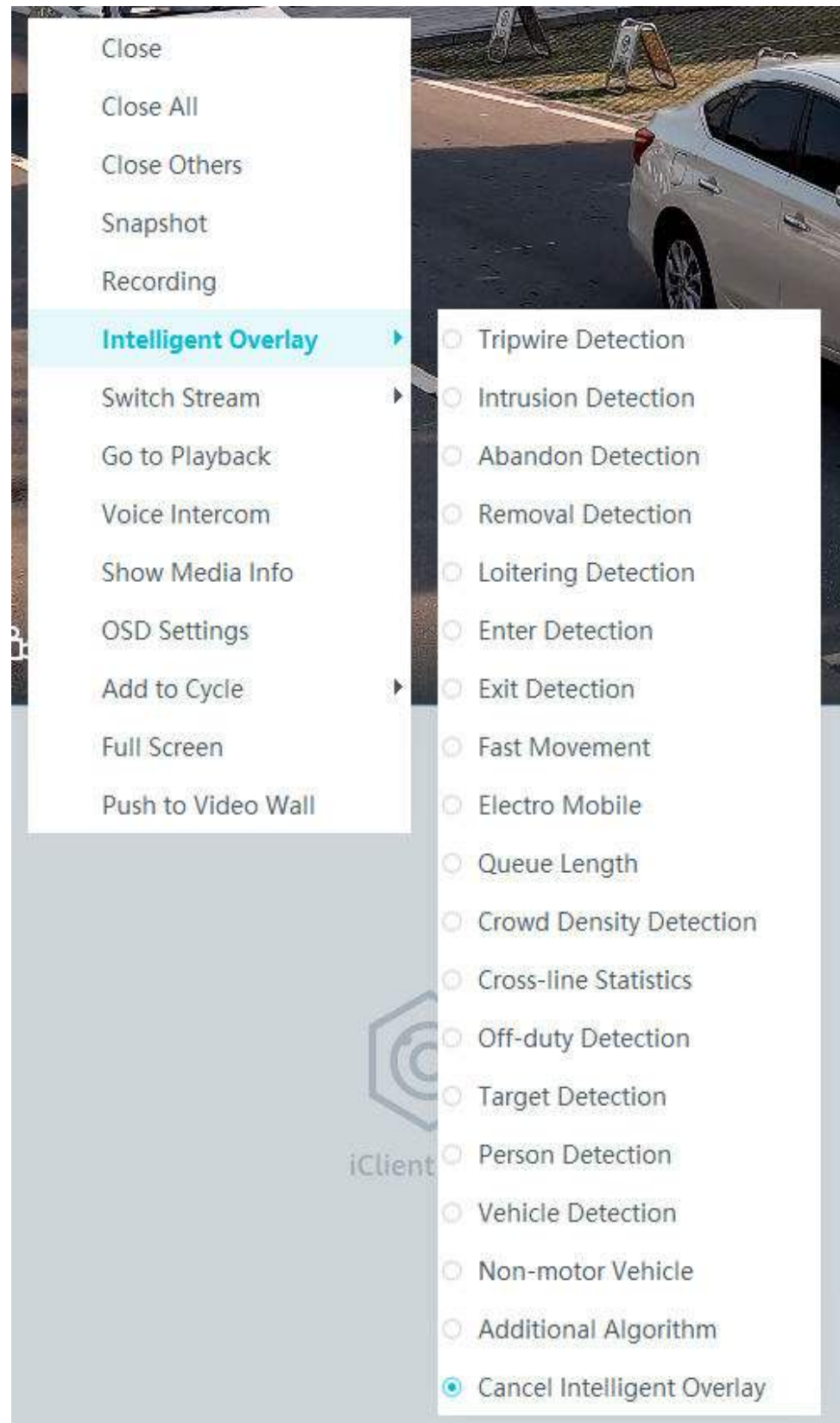
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-70](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-70 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

4.6.11 Fast Movement Detection

Fast movement detection is used to detect whether an object moves over in a detection area. If so, an alarm is generated. You can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Click the **Behavior Analysis** tab and then the **Fast Movement Detection** tab, and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 4-66](#) describes the parameters.

Table 4-66 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 4-67](#) describes the parameters.

Table 4-67 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 4-71](#). [Table 4-68](#) describes the parameters.

Figure 4-71 Setting detection areas

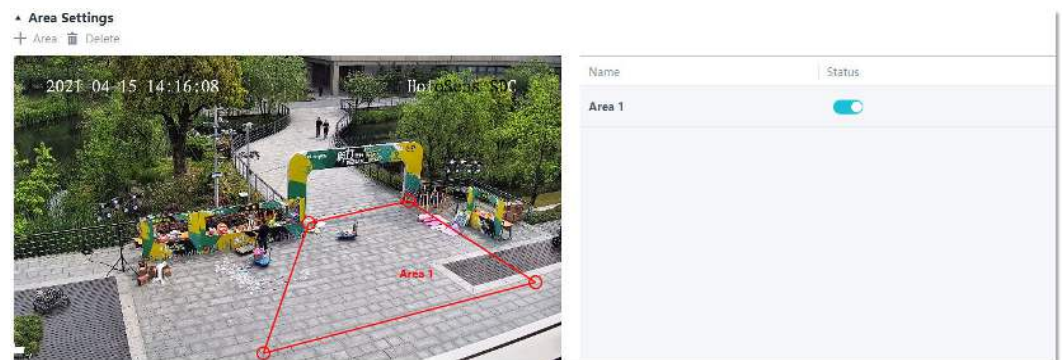


Table 4-68 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 4-69](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-69 Plan settings

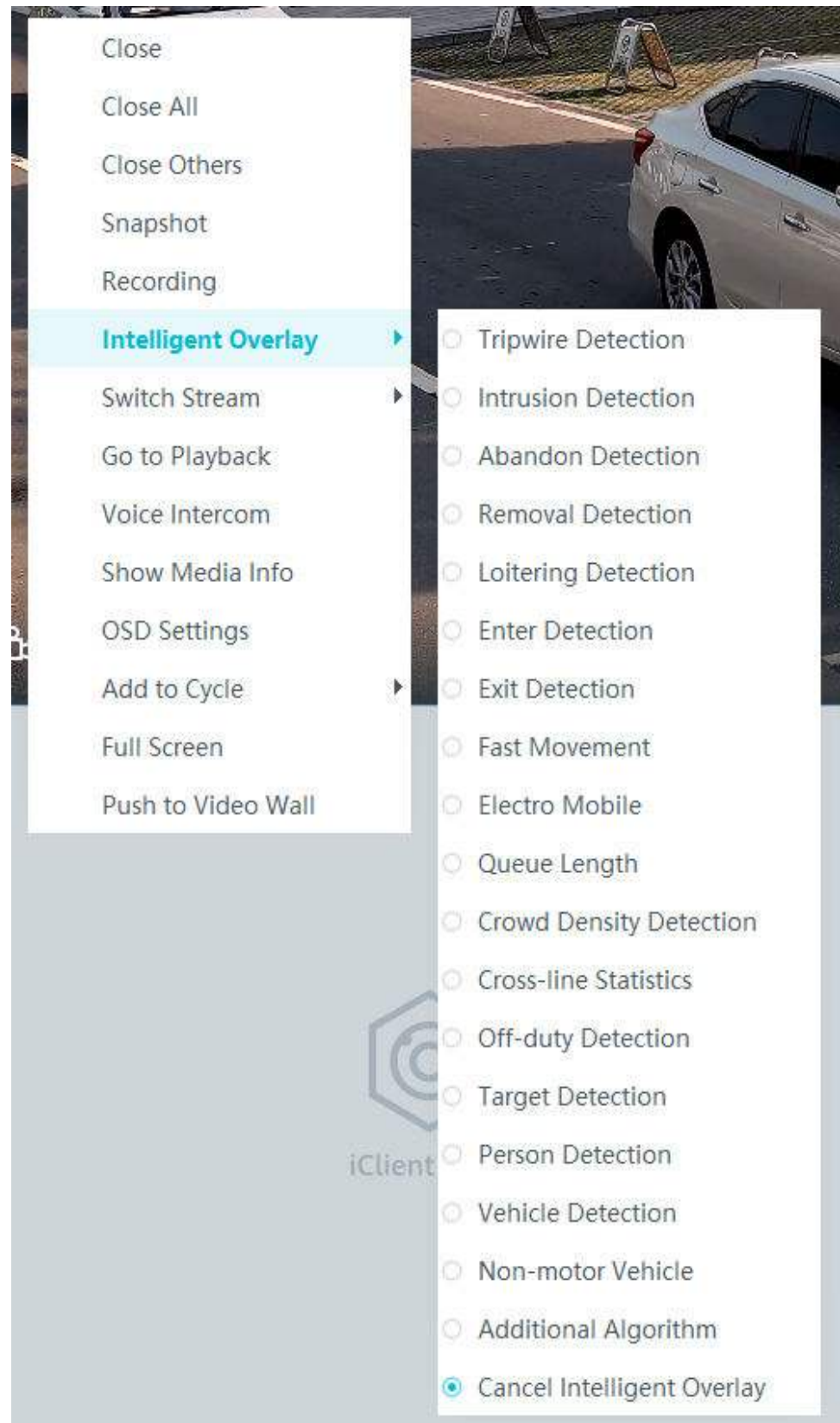
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-72](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-72 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

4.6.12 Electric Bike Detection

The system can generate an alarm when detecting an electric bike in areas such as elevators and corridors, where parking of electric bikes is not allowed.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Prerequisites

- You have connected cameras of the 9.0.0 version.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see [4.6.3 Global Configuration](#).

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Click the **Behavior Analysis** tab and then the **Electric Bike Detection** tab, and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 4-70](#) describes the parameters.

Table 4-70 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 4-71](#) describes the parameters.

Table 4-71 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set detection area parameters, as shown in [Figure 4-73](#). [Table 4-72](#) describes the parameters.

Figure 4-73 Setting detection areas

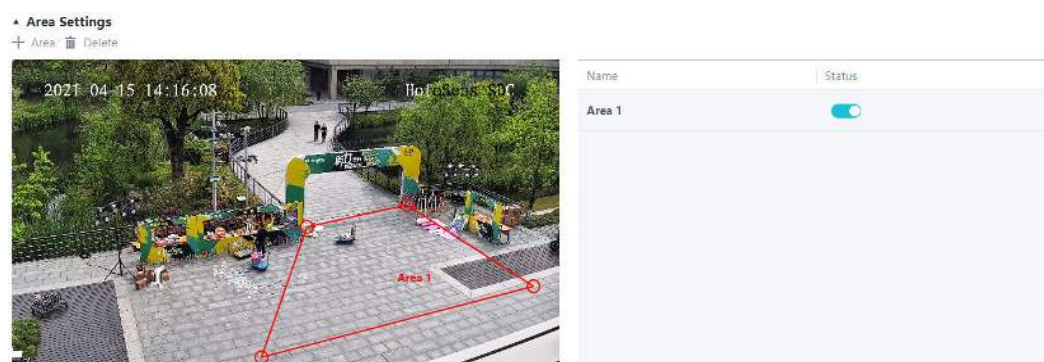


Table 4-72 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. Only one detection area can be configured for electric bike detection, and a maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 4-73](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-73 Plan settings

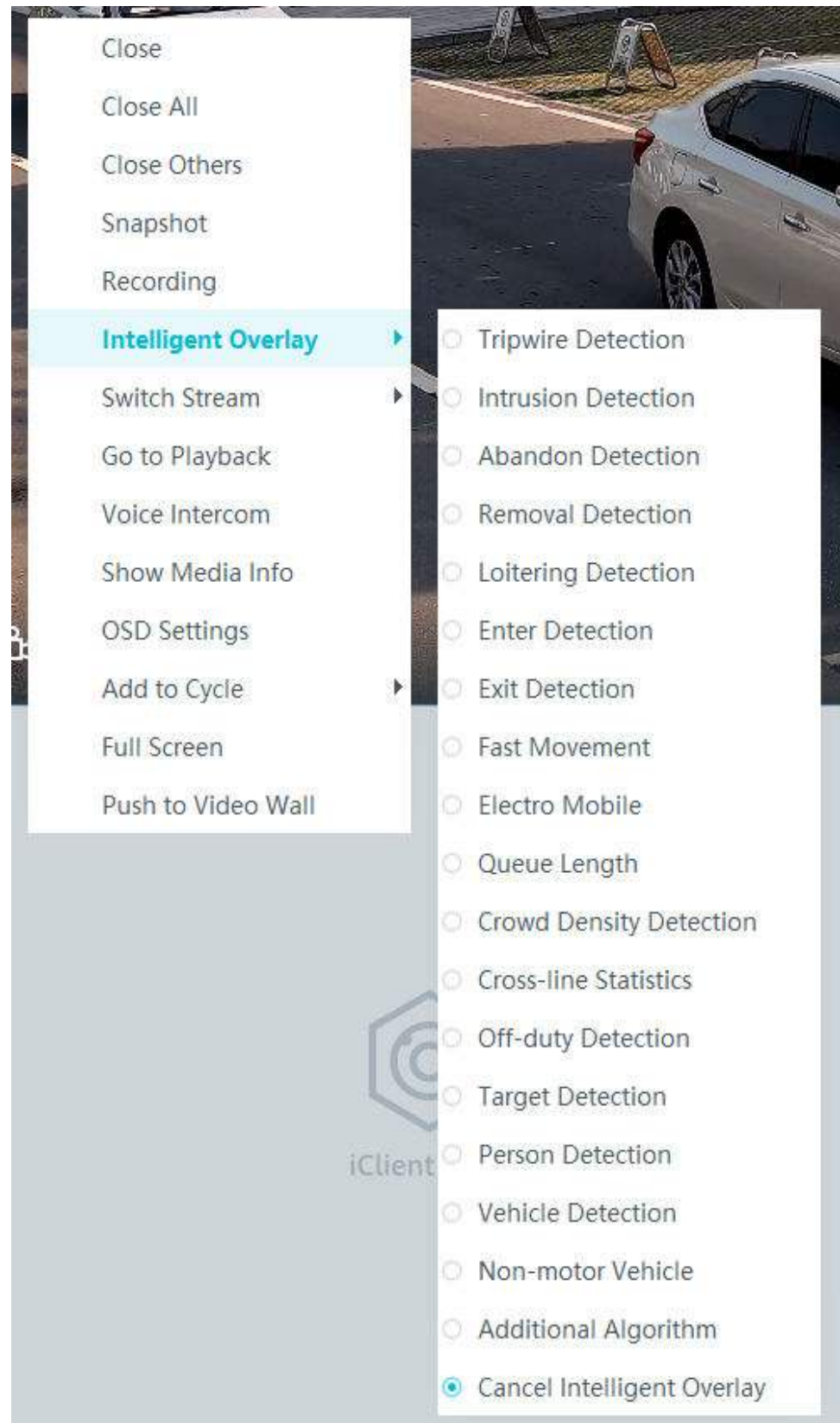
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-74](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-74 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

4.7 Intelligent target Analysis

4.7.1 Global Configuration

Application Scenario

Before configuring target intelligence on the iClient S100, you need to complete global configuration.

Table 4-74 Global configuration for target intelligence

Procedure	Application Scenario
Turn on the target intelligent switch	This step should be started in all scenes that need to use target recognition function.
Turn on the camera target intelligent switch	This step should be started in all scenes that need to use target recognition function.
Configuring the algorithm mode	Cameras that support target recognition, such as Dxxxx-10-SIU cameras
Configuring target recognition	
Setting target parameters	All Dxxxx-10 cameras

Turn on the target intelligent switch of the main device

This step should be started in all scenes where the target recognition function needs to be used.

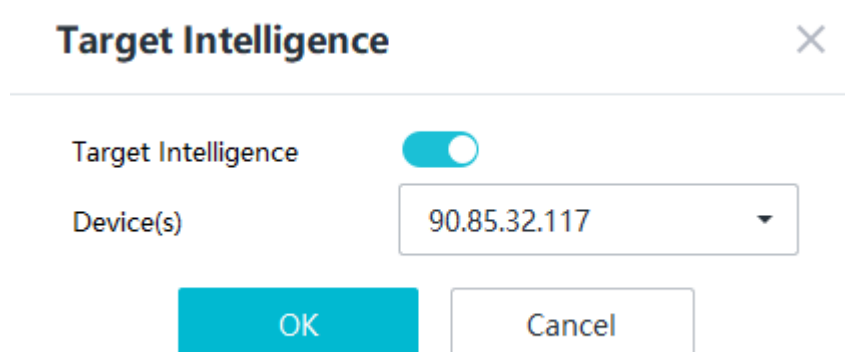
NOTE

- The use of target intelligence in business scenarios needs to be subject to legal constraints. Therefore, before starting the target intelligence function, you need to know the relevant laws and regulations, and then you can start the use of target recognition related functions with consent.

After target analysis is enabled, the NVR800 will restart for the setting to take effect.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right click a nvr800 device, select the target smart switch, and turn on the target smart switch

Figure 4-75 Target IntelligenceA dialog box titled "Target Intelligence" with a close button (X) in the top right corner. It contains a toggle switch for "Target Intelligence" which is turned on. Below it is a label "Device(s)" followed by a text box containing the IP address "90.85.32.117" and a dropdown arrow. At the bottom are two buttons: "OK" (blue) and "Cancel" (white with blue border).

Step 3 Click **OK**.

----End

Turn on the target intelligent switch of the main device

This step should be started in all scenes where the target recognition function needs to be used.

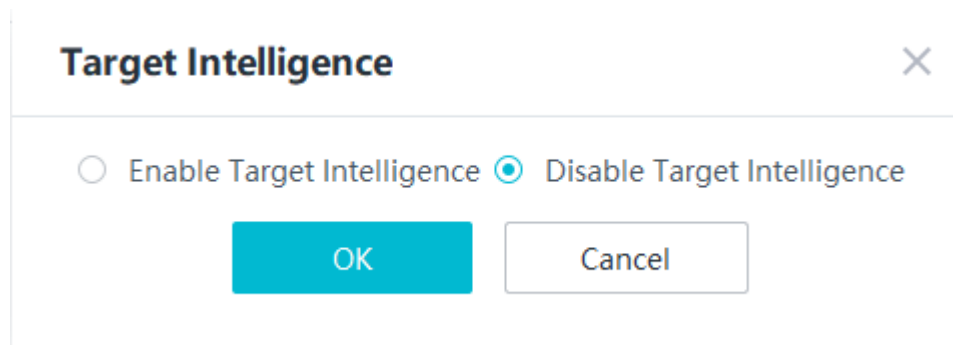
NOTE

- The use of target intelligence in business scenarios needs to be subject to legal constraints. Therefore, before starting the target intelligence function, you need to know the relevant laws and regulations, and then you can start the use of target recognition related functions with consent.

After target analysis is enabled, the NVR800 will restart for the setting to take effect.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right click a video camera, select the target smart switch, and turn on the target smart switch

Figure 4-76 Target IntelligenceA dialog box titled "Target Intelligence" with a close button (X) in the top right corner. It contains two radio buttons: "Enable Target Intelligence" (unselected) and "Disable Target Intelligence" (selected). At the bottom are two buttons: "OK" (blue) and "Cancel" (white with blue border).

Step 3 Click **OK**.

----End

Enabling Target Analysis

Perform the following steps only for the NVR800 with one or two disk trays.

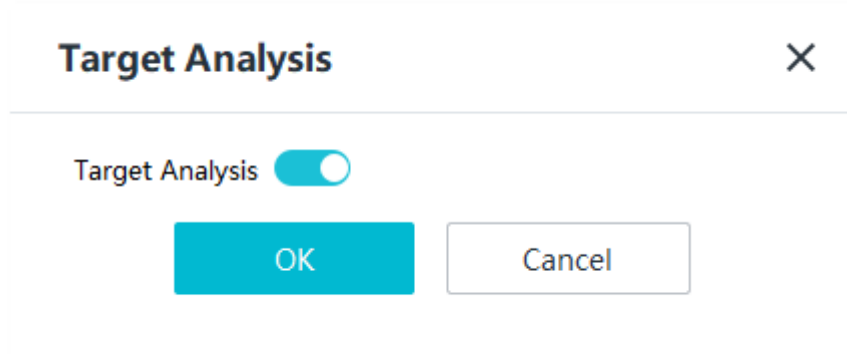
NOTE

- By default, target analysis is enabled for the NVR800 with one or two disk trays.
 - If target analysis is disabled, the NVR800 cannot use the intelligent target analysis function.
 - If target analysis is enabled, the video decoding specification of the NVR800 with one or two disk trays is halved on the LDU.
For example, the NVR800 with one disk tray supports 4-channel 1080p video decoding by default, and 2-channel 1080p video decoding when target analysis is enabled.
- Target analysis is always enabled for the NVR800 with four or eight disk trays, which will not affect the video decoding specification. Therefore, you do not need to manually configure the target analysis function for the NVR800 with four or eight disk trays.
- After target analysis is enabled, the NVR800 will restart for the setting to take effect.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an NVR800 and choose **Target analysis** from the shortcut menu. Then toggle-on **Target Analysis** on the page shown in [Figure 4-77](#).

Figure 4-77 Target Analysis



Step 3 Click **OK**.

----End

Configuring the Algorithm Mode

Perform the following steps only for Dxxxx-10-SIU cameras.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Smart Global Configuration > Algorithm Mode**.

Step 3 Set **Algorithm Mode** to **Target checkpoint**.

NOTE

After the algorithm mode is switched, the camera will restart for the setting to take effect. Wait for 3 minutes and then set intelligent services.

Step 4 Click **Save**.

----End

Setting Target Parameters

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Target Capture > Target Parameters**.

Step 3 Enable the target capture function and set parameters, as shown in [Figure 4-78](#). [Table 4-75](#) describes the parameters and buttons.

Figure 4-78 Setting target parameters

Table 4-75 Parameter/Button description

Parameter/Button		Description
Parameter Settings	Target Capture	Indicates whether to enable target capture. NOTE This function is mutually exclusive with behavior analysis and situation awareness. Before enabling this function, ensure that behavior analysis and situation awareness are disabled.
	Target Attributes	Indicates whether to enable target attribute recognition, which is supported by some camera models. After this function is enabled, you can view information such as the age and gender of the captured target on the target recognition page.

Parameter/Button		Description
	Detection Mode	Detection mode. • Target detection: detects only targets. • Person detection: detects only persons. • Both: detects both targets and persons.
	Capture Mode	Snapshot mode. • Optimal: When a target is in the view, the camera takes snapshots of the target and evaluates each snapshot. After the target leaves the view, the snapshot with the optimal quality is selected as the snapshot result. This mode applies to most target capture scenarios and ensures optimal quality of snapshots. • Fast: When a target enters the detection area, the camera takes snapshots of the target and evaluates each snapshot. The target snapshot that meets the requirement is used as the snapshot result. Then the camera still detects the target but does not take snapshots of the target. • Scheduled: When a target enters the detection area, the camera takes snapshots of the target and generates a snapshot with the optimal quality at a specified interval.
	Alarm Check Interval (s)	Interval at which alarms are checked.
	Target Detection Sensitivity	Target detection sensitivity. The value ranges from 1 to 5. A larger value indicates a higher sensitivity.
	Person Detection Sensitivity	Person detection sensitivity. The value ranges from 1 to 5. A larger value indicates a higher sensitivity.
	Min Target	Maximum and minimum size of targets that can be detected.
	Max Target	
Advanced Parameters	Send Target Images	Indicates whether to send target/person cutouts and full images.
	Send Person Images	
	Send Full Images	

Parameter/Button		Description
	Brightness Compensation	Indicates whether to enable brightness compensation. Open: Enables this function. After this function is enabled, the exposure is automatically decreased in highlight or increased in backlight to ensure ideal brightness in different environments. Close: Disables this function.
	Target Snapshot Quality	Image quality of target/person snapshots and full images. The value ranges from 1 to 5. A larger value indicates higher quality. Higher image quality consumes more storage space.
	Person Snapshot Quality	
	Full Image Quality	
	Compensation Coefficient	Maximum brightness compensation coefficient. The default value is 50 . The camera will automatically adjust the compensation level within the specified range based on the image brightness. The value of this parameter can be properly increased in frontlight or backlight conditions.
	Exposure Duration (min)	Duration of target exposure, in minutes. When a target is detected, target exposure is performed for a specified period of time. You are advised to set this parameter to 10 minutes in densely populated scenarios and 5 minutes in sparsely populated scenarios.
Area Settings	Area	Button for adding areas. You can click once to add the Direction Area and click twice to add the Non-detection Area .
	Delete	Button for deleting a selected detection area or non-detection area.

Step 4 Click **Save**.

----End

Configuring Target Recognition

Perform the following steps only for Dxxxx-10-SIU cameras.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Target Capture > Target Recognition**.

Step 3 Toggle-on **Enable target recognition**, as shown in [Figure 4-79](#).

Figure 4-79 Configuring target recognition

Enable target recognition ☒

Target recognition model SDC_FR V1.9.0b030s001

Target parameter model SDC TRAFFIC FACE V809

Feature Usage Mode Personal feature ▼

Personal feature

Access Control

Save Cancel

Step 4 Set **Feature Usage Mode** based on the site requirements. The following options are available:

- **Personal feature:** extracts features from an optimal target snapshot and reports the match result.

NOTE

When **Feature Usage Mode** is set to **Personal feature**, **Snapshot Mode** must be set to **Optimal**.

- **Access Control:** reports extracted features multiple times for target match, ensuring smooth access control.

NOTE

- The **Access Control** mode applies only to access control scenarios when up to four targets are queuing in the camera view.
- When **Snapshot Mode** is set to **Fast**, **Feature Usage Mode** must be set to **Access Control**.

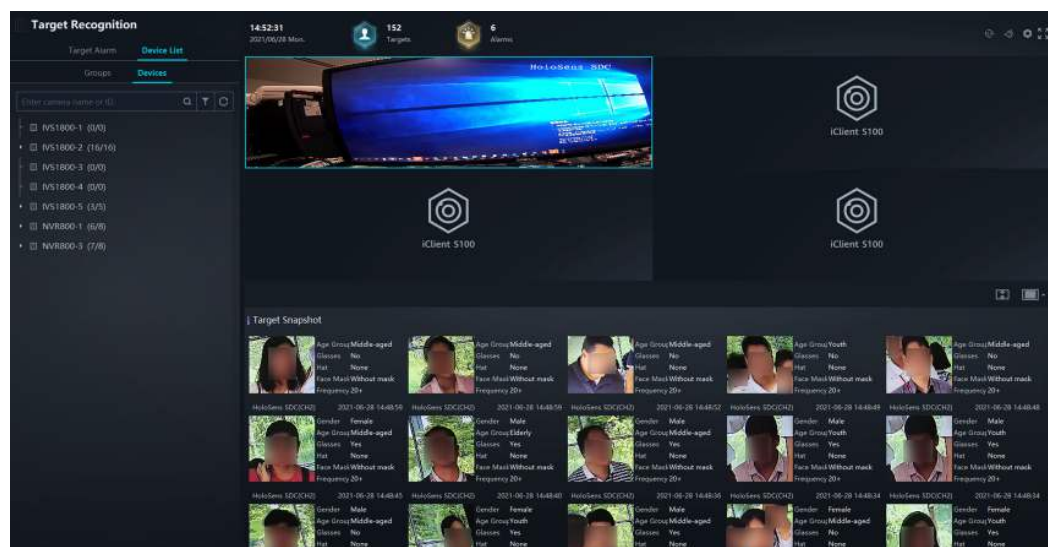
Step 5 Click **Save**.

----End

Verification

Step 1 On the iClient S100 home page, choose **Intelligent Applications > Target Recognition**.

Step 2 Drag the required camera to the video pane. Target recognition results and snapshots will be displayed under the video pane in real time, as shown in [Figure 4-80](#).

Figure 4-80 Target recognition results

----End

4.7.2 Computing Power Sharing

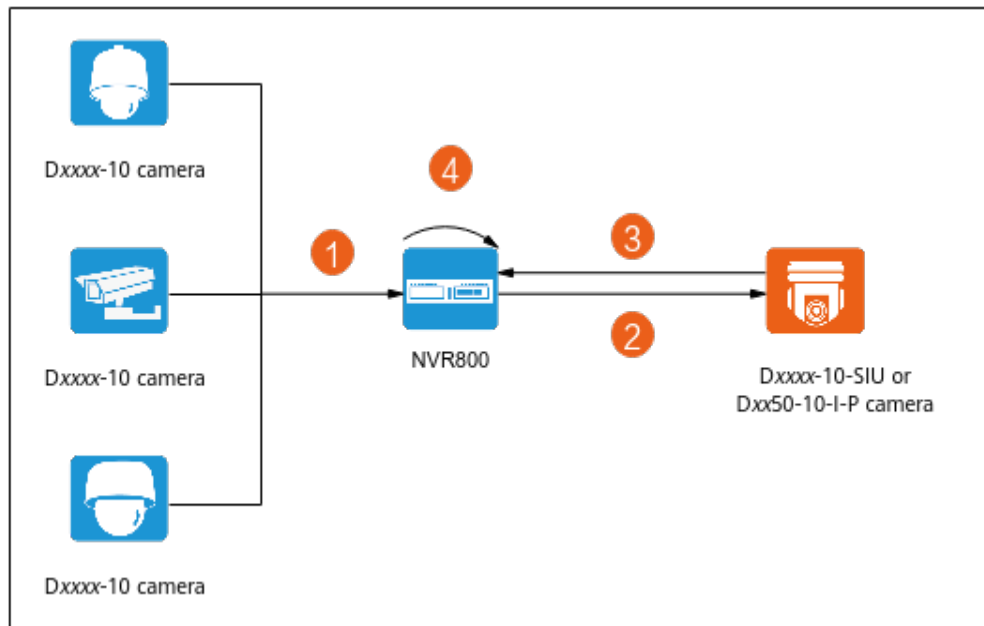
Restrictions

- One Dxxxx-10-SIU or Dxx50-10 camera can connect to a maximum of three Dxxxx-10 cameras.
- Only cameras connected through HWSKD can share computing power.
- If you connect multiple Dxxxx-10-SIU or Dxx50-10 cameras, use the same the target recognition algorithm for these cameras. This ensures the consistency of features extracted from the same target snapshot.

For details about how to check the target recognition algorithm, see [Configuring Target Recognition](#).

Networking

Figure 4-81 Networking



1. Target capture cameras upload snapshots to an NVR800 (without extracting features from the snapshots).
2. The NVR800 sends the snapshots to a Dxxxx-10-SIU or Dxx50-10 camera for analysis and feature extraction.
3. The Dxxxx-10-SIU or Dxx50-10 camera sends the extracted target features to the NVR800.
4. The NVR800 matches the received target features with those in the target list.

NOTE

- Before a Dxxxx-10-SIU or Dxx50-10 camera is connected, the Dxxxx-10 camera cannot extract target features and the detected target information cannot be used for target search.
- After a Dxxxx-10-SIU or Dxx50-10 camera is connected, the Dxxxx-10 camera can extract target features, but cannot re-extract target features from images collected earlier.

Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Connect a Dxxxx-10 camera to the NVR800 by referring to [4.1.2.2 Adding Cameras on the NVR800](#), as shown in [Figure 4-82](#).

Figure 4-82 Device connection

NVR800-6.230(Total 1 Devices)								+ Add Delete Restart Synchronize	
☐	Device Name	Channel No	Camera Type	Model	Driver	Vendor	IP Address	Device Status	
☐	HoloSens SDC	19	Bullet camera	D2120-10-I-P(6mm)	HWSDK	HUAWEI	.4.12	● Online	

- Step 3** Enable the target capture function for the Dxxxx-10 camera by referring to [Setting Target Parameters](#). In this case, the target snapshots taken by the Dxxxx-10 camera cannot be used for intelligent target analysis functions such as target search and alert. For details, see [Verification 1](#).
- Step 4** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 5** Connect a Dxxxx-10-SIU camera to the NVR800 by referring to [4.1.2.2 Adding Cameras on the NVR800](#), as shown in [Figure 4-83](#).

Figure 4-83 Device connection

NVR800-6.230(Total 2 Devices)								+ Add Delete Restart Synchronize	
☐	Device Name	Channel No	Camera Type	Model	Driver	Vendor	IP Address	Device Status	
☐	SDC	18	Bullet camera	D2120-10-SIU	HWSDK	HUAWEI	.4.107	● Online	
☐	HoloSens SDC	19	Bullet camera	D2120-10-I-P(6mm)	HWSDK	HUAWEI	.4.12	● Online	

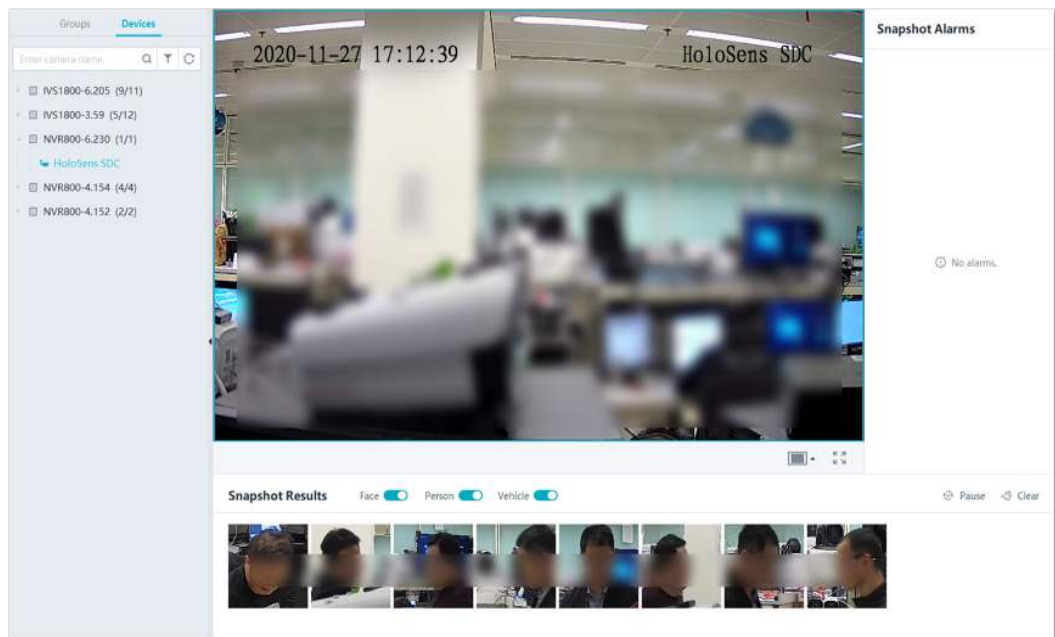
- Step 6** Enable the target recognition function for the Dxxxx-10-SIU camera by referring to [Configuring Target Recognition](#). In this case, the target snapshots taken by the Dxxxx-10 camera can be used for intelligent target analysis functions such as target search and alert. For details, see [Verification 2](#).

----End

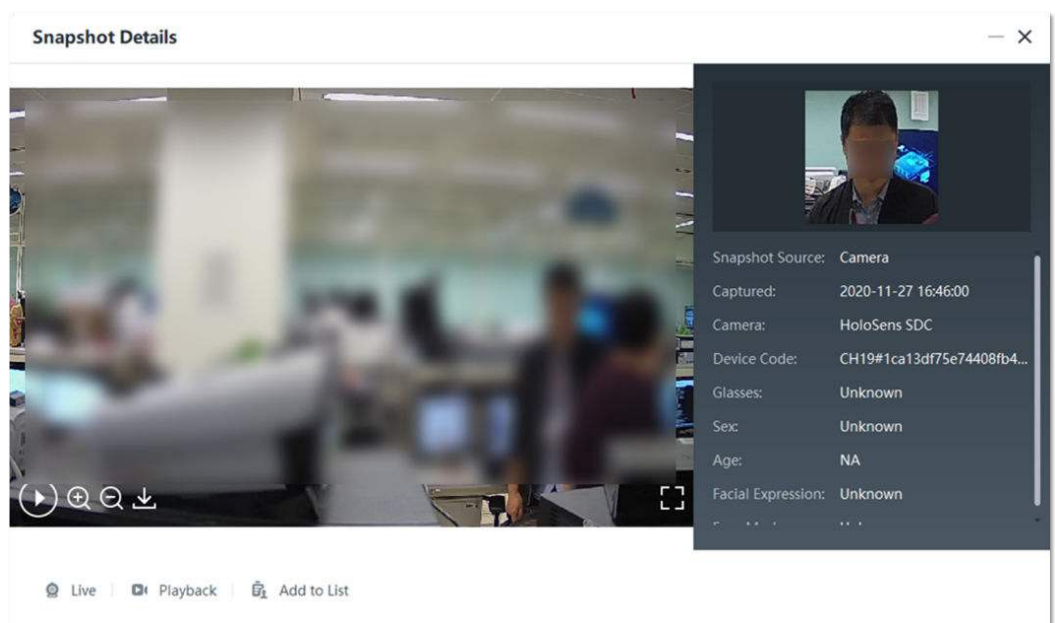
Verification

Verification 1: If only Dxxxx-10 cameras are connected to the NVR800, the target snapshots cannot be used for intelligent target analysis functions such as target search and alert.

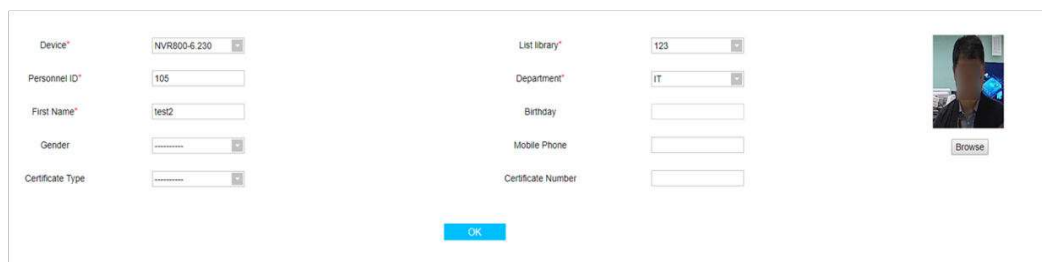
- Step 1** On the iClient S100 home page, choose **Intelligent Applications > Target Recognition**.
- Step 2** Double-click a Dxxxx-10 camera. You can view the real-time target snapshot results in the **Snapshot Results** area, as shown in [Figure 4-84](#).

Figure 4-84 Snapshot Results

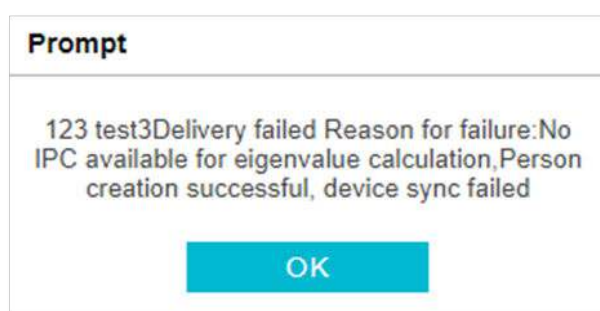
Step 3 Click a snapshot. The **Snapshot Details** window is displayed, as shown in [Figure 4-85](#).

Figure 4-85 Snapshot Details

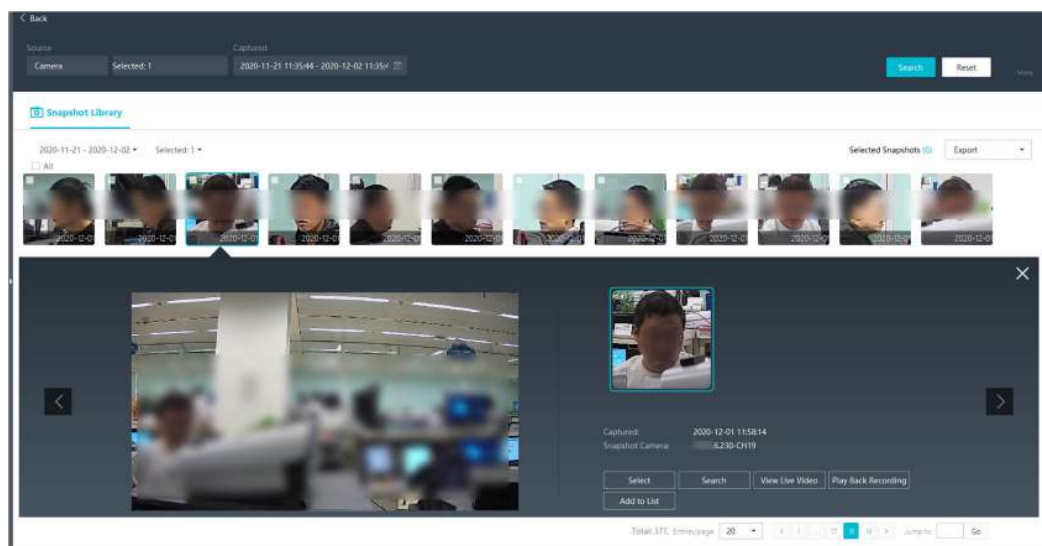
Step 4 Click **Add to List**. The **Target Library** tab page is displayed, as shown in [Figure 4-86](#).

Figure 4-86 List library

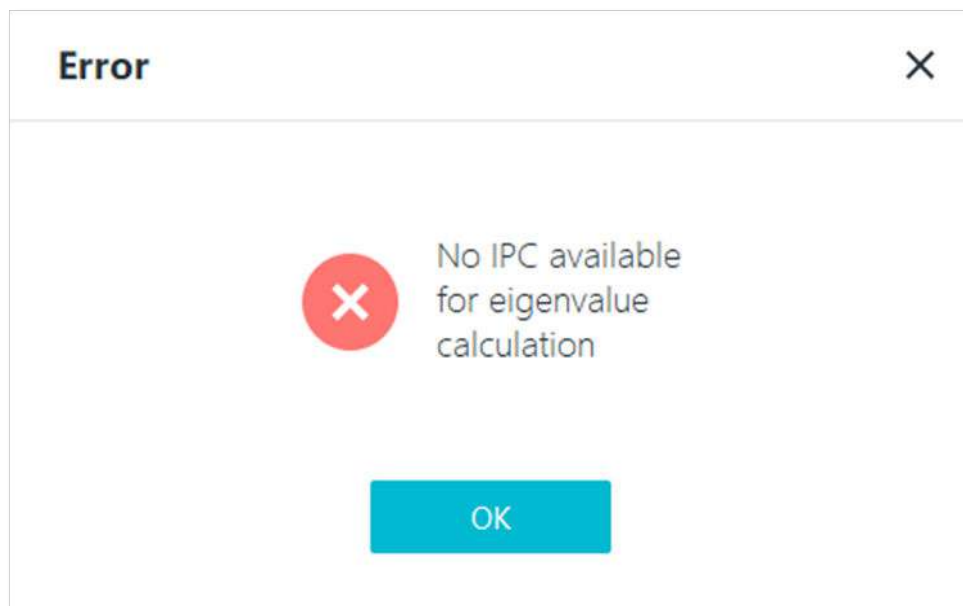
Step 5 Enter list information and click **OK**. The system displays a message indicating that the snapshot fails to be added to the list, as shown in [Figure 4-87](#).

Figure 4-87 Failure to add the snapshot

Step 6 Search for the target snapshots taken by the Dxxxx-10 camera in **Snapshot Library** by referring to [4.7.5 Target Search](#), as shown in [Figure 4-88](#).

Figure 4-88 Target search

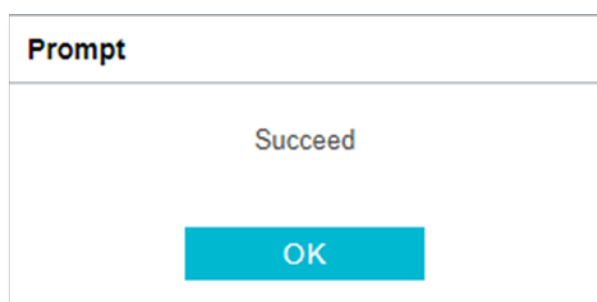
Step 7 Click a snapshot, click **Search**, frame the required target part, and click **OK**. The system displays a message indicating that target search fails, as shown in [Figure 4-89](#).

Figure 4-89 Target search failure

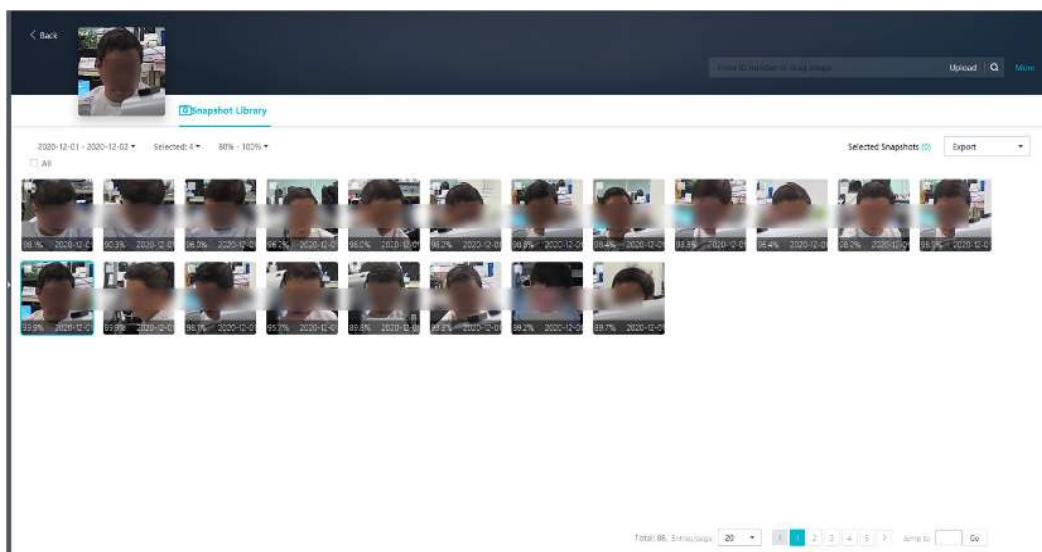
----End

Verification 2: After a Dxxxx-10-SIU camera is connected to the NVR800, the target snapshots taken by the Dxxxx-10 camera can be used for intelligent target analysis functions such as target search and alert.

- Step 1** On the iClient S100 home page, choose **Intelligent Applications > Target Recognition**.
- Step 2** Select a target snapshot taken by the Dxxxx-10 camera and add it to the list again. The system displays a message indicating that the snapshot is successfully added to the list, as shown in [Figure 4-90](#). You can create a target alert task for the list by referring to [4.7.8 List-based Target Alert](#).

Figure 4-90 Added successfully

- Step 3** Select a target snapshot taken by the Dxxxx-10 camera and initiate a target search again by referring to [4.7.5 Target Search](#). The page shown in [Figure 4-91](#) is displayed, indicating that the search is successful.

Figure 4-91 Search success

----End

4.7.3 1 + N

Description

Through the 1 + N function, the primary camera (SIU models) enables secondary cameras (D00 models) to provide target detection and capture, target recognition, and mask detection services, without affecting behavior analysis of the secondary cameras. You can configure the services based on the site requirements.

Prerequisites

- Camera requirements:
 - Primary camera: SIU model (for example, D3250-10-SIU) of 9.0.0 and later versions
 - Secondary camera: D00 model (for example, D3020-00-I) of 8.1.1 and later versions
- Before using the 1 + N function, log in to the web system of the secondary camera, choose **Settings > Network > Platform Connection > Second Protocol Parameters**, and select **Enable ONVIF**.
- Currently, a primary camera can be bound to only one secondary camera.
- The NVR800 must be 9.0.0 or a later version.

Procedure

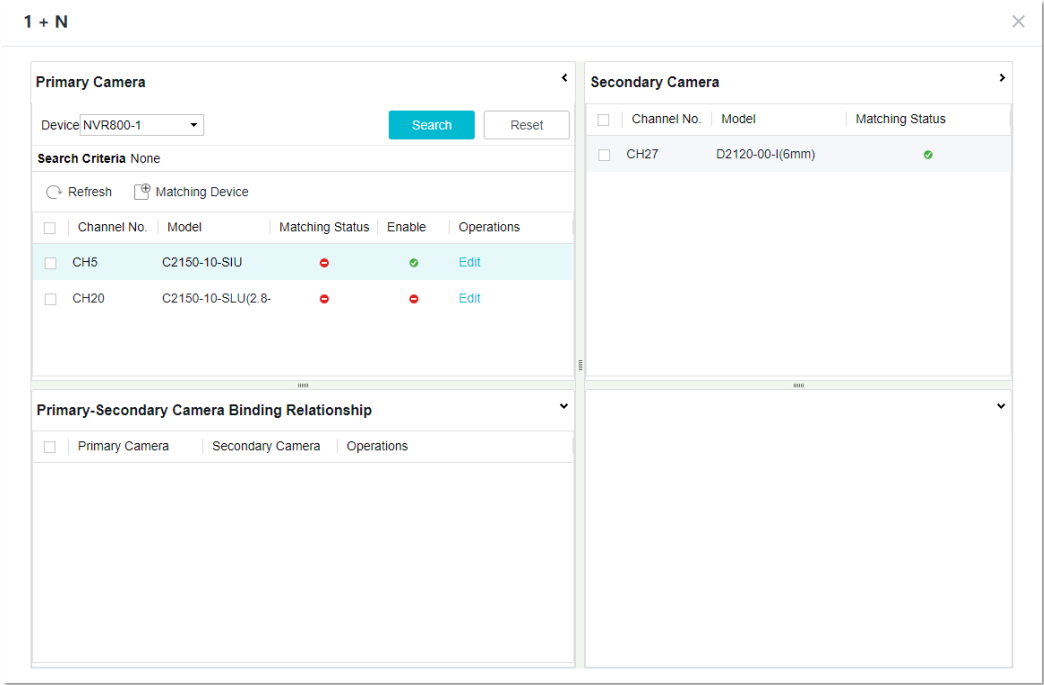
For details about the configuration and verification of the 1 + N function, see **Configuration Guide > Target-related Intelligence > 1+N** in the NVR800 product documentation.

The key steps for configuring 1 + N on the iClient S100 are as follows:

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click the NVR800 to be configured and choose **1 + N** from the shortcut menu. The **1 + N** dialog box is displayed, as shown in [Figure 4-92](#).

Figure 4-92 1 + N dialog box



- Step 3** Click **Edit** in the **Operations** column of the primary camera. In the **Edit** dialog box that is displayed, set **Enable** to **Open** and click **OK**. After the 1 + N function is enabled, the primary camera will restart, which takes 2 to 3 minutes.
- Step 4** Select the primary and secondary cameras to be bound and click **Matching Device**.
- Step 5** In the **Paired Device** dialog box, enter the ONVIF user name and password of the secondary camera.
- Step 6** Then the binding relationship will be displayed in the **Primary-Secondary Camera Binding Relationship** area.

----End

4.7.4 Target List Management

Application Scenario

List libraries are classified into two types: **Deny List** and **Allow List**. [Table 4-76](#) describes the application scenarios and functions of these types of list libraries.

Table 4-76 List library types

List Library Type	Application Scenario
Deny list	Used in scenarios such as swing gates, security gates, and straight-through pedestrian walkways. The system generates an alarm once a blocklisted target is detected.
Allow list	Used in scenarios such as swing gates and security gates. The system generates an alarm once an allowlisted target is detected.

Prerequisites

You have added target images for persons in a target alert task on the **Personal** page. For details, see [6.1.4 Adding Persons](#).

Creating a List Library

Step 1 Create a list library.

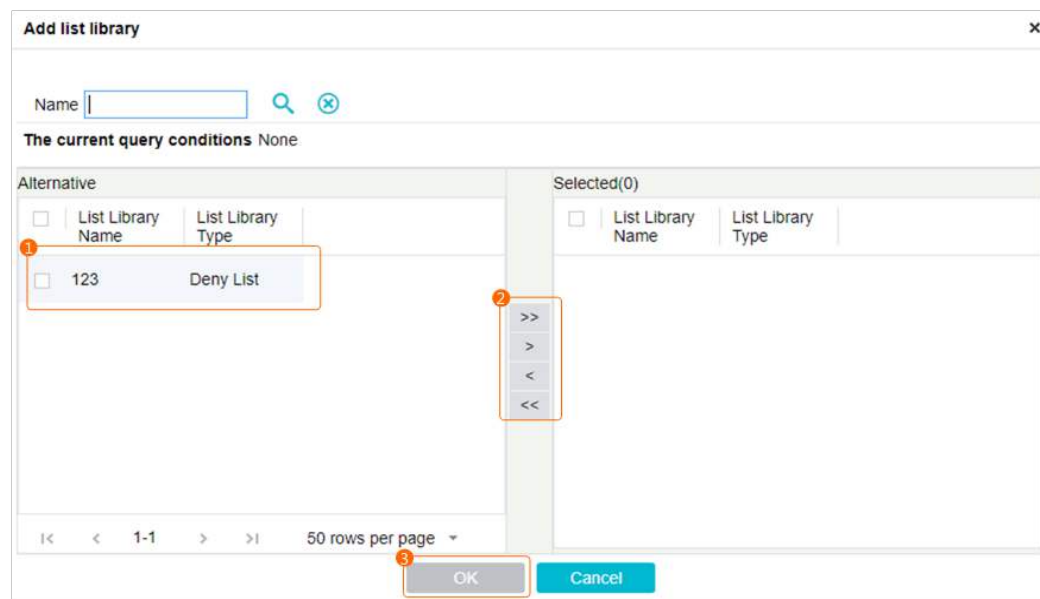
1. Choose **Maintenance Management > Personnel Management** on the iClient S100 home page.
2. Click the **List Library** tab.
3. On the list library page, click **New** and create a list library, as shown in [Figure 4-93](#). Click **OK**.

Figure 4-93 Adding a list library

4. Click **Add People** to add the person created on the **Personal** page to the current list library.

Step 2 Synchronize the list library.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Right-click a device and choose **Target Library**.
3. Click **Select Personnel List** and move the list library (under **Alternative**) created on the **Personal** page to the list library (under **Selected**) on the right, as shown in [Figure 4-94](#).

Figure 4-94 Synchronizing the list library

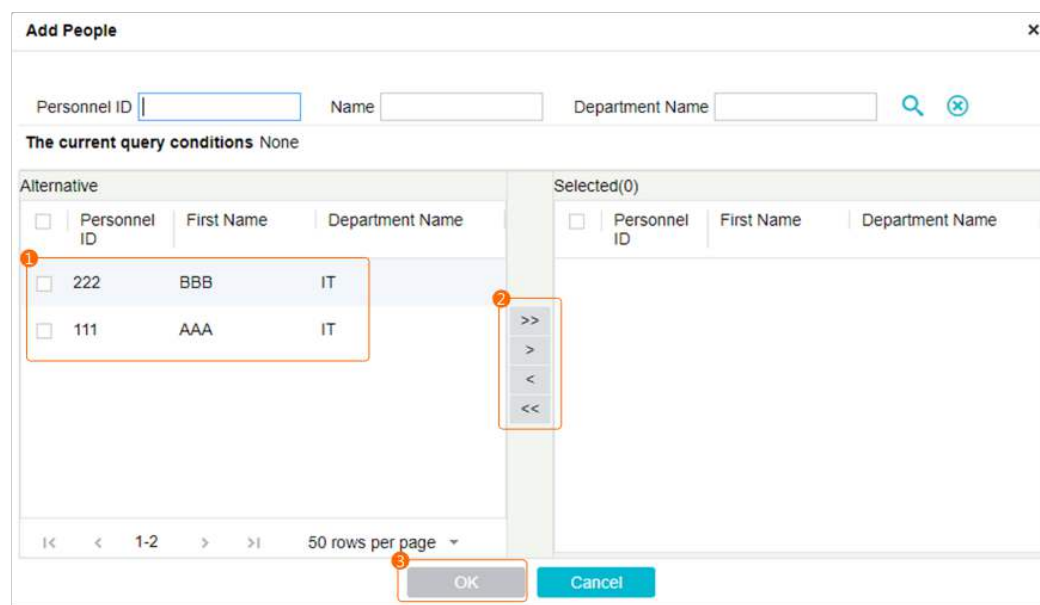
4. Click **OK**.

Step 3 Synchronize person information.

1. In the list library list, select the list library to which you want to add person information and click **Sync People**.
2. Move the persons (under **Alternative**) created on the **Personal** page to the list library (under **Selected**) on the right, as shown in [Figure 4-95](#).

NOTE

The synchronized person information will be used for target alert. target images of such persons must be uploaded on the **Personal** page. Otherwise, the person information will fail to be synchronized.

Figure 4-95 Synchronizing person information

3. Click **OK**.

----End

4.7.5 Target Search

Application Scenario

You can perform target search in either of the ways listed in the following table.

Table 4-77 Target search modes

Search Mode	Description
Search by image	After a target image is imported to the iClient S100, the system automatically extracts target features from the image and searches for targets based on the features.
Search by criterion	After target search criteria are entered, the system searches for matched target images based on the search criteria.

Search by Image

- Step 1** On the iClient S100 home page, choose **Basic Operations > Search > Search By Image**.
- Step 2** (Optional) Click **More** and set search criteria based on the site requirements. [Table 4-78](#) describes the parameters.

Table 4-78 Parameters for target search by image

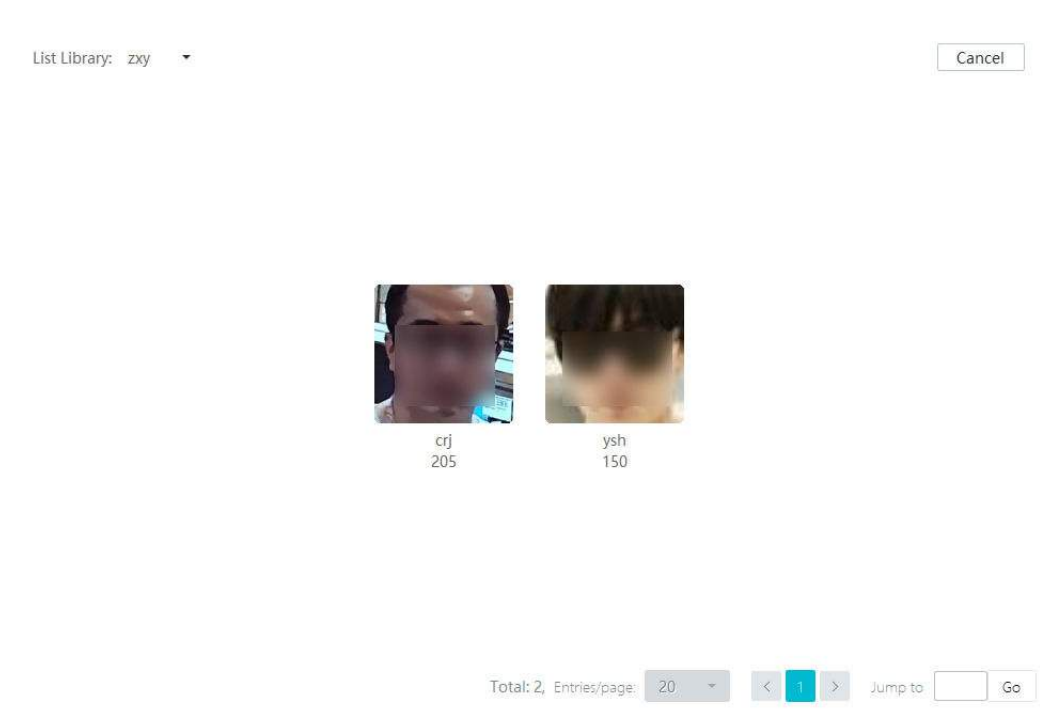
Parameter	Description
Period	Period during which the target images are captured. • Select Past 3 Days, Past Week, or Past Month. • Alternatively, specify a period in the calendar.
Match	Threshold of similarity to the target for search.
Source	Cameras from which target images are searched for. You can select multiple cameras from various main devices.

Step 3 Upload a target image for target search.

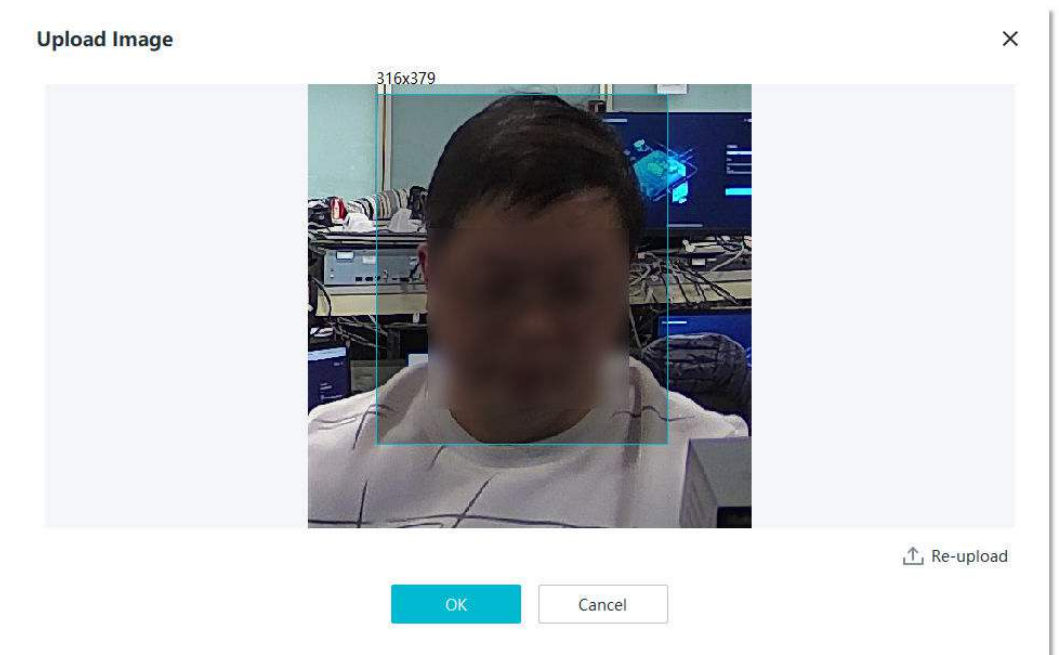
The options are as follows:

- Enter the full ID number or name in the search box and select the target image for target search from the drop-down list box.

- Click  next to the search box, and click  in the drop-down list box that is displayed. The page shown in [Figure 4-96](#) is displayed. Select a list library in the upper left corner and click a target image in the list library to start target search by image.

Figure 4-96 Search by list library

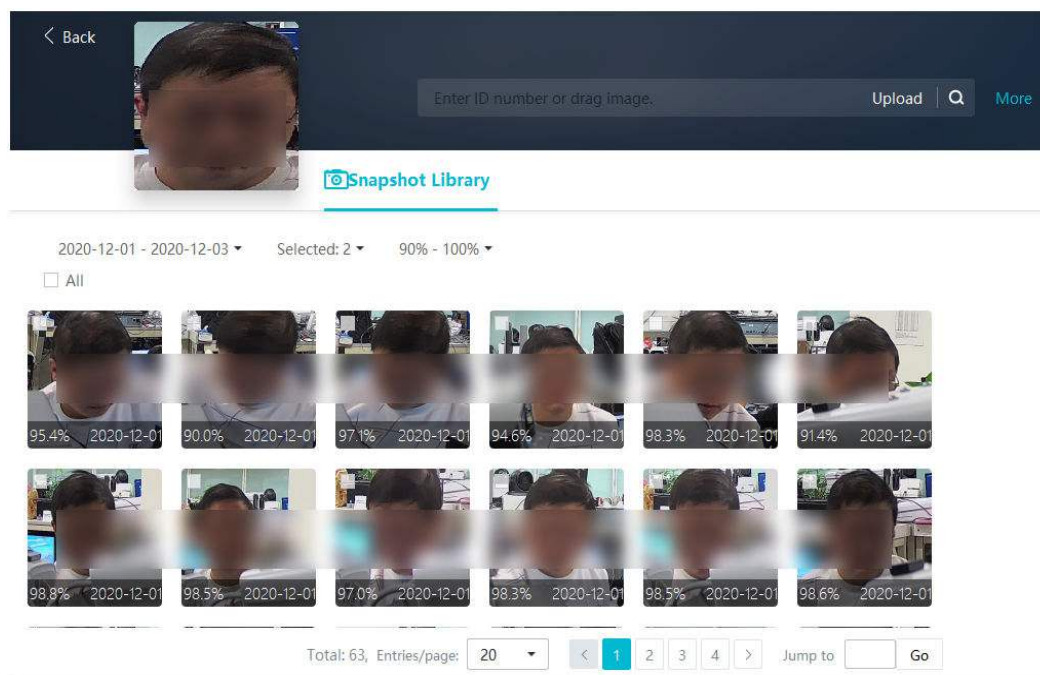
- Drag a target image to the search box. On the **Upload Image** page that is displayed, box-select the required target part and click **OK**, as shown in [Figure 4-97](#).

Figure 4-97 Box-selecting the required target part**NOTE**

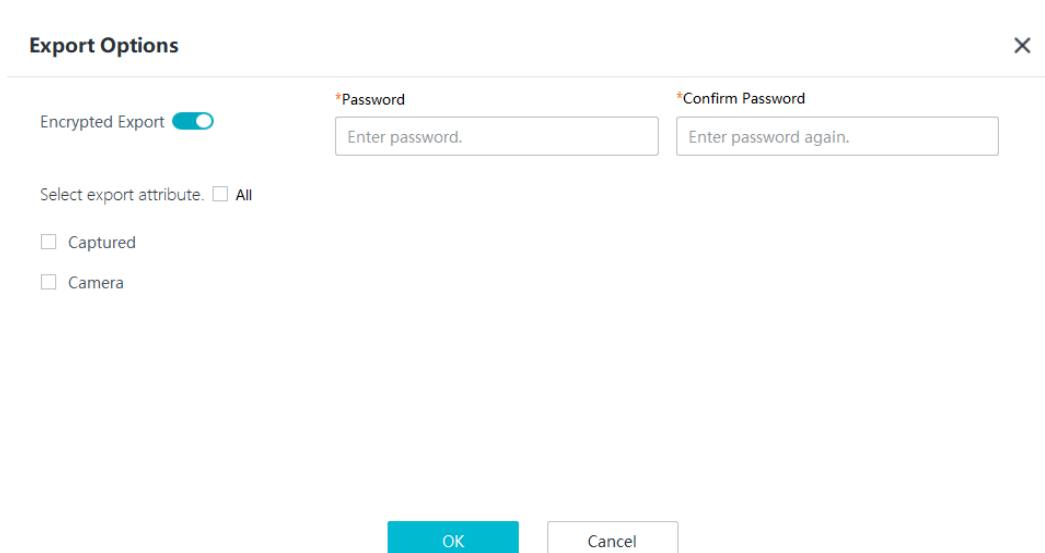
The target image to be uploaded must meet the following requirements:

- The image file format must be .jpg, .jpeg, .jpe, .dib, .bmp, or .png.
- The image size cannot exceed 5 MB, and the image resolution cannot exceed 4096 x 3000 pixels.
- The resolution of the selected target area ranges from 60 x 60 pixels to 800 x 1200 pixels.

Step 4 Wait until the search result is displayed, as shown in [Figure 4-98](#).

Figure 4-98 Result of target search by image

Step 5 (Optional) Select **Export Selected**, **Export This Page**, or **Export All** from the **Export** drop-down list as required. [Figure 4-99](#) shows the file export dialog box.

Figure 4-99 Export Options

NOTE

You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files.

----End

Search by Criteria

Step 1 On the iClient S100 home page, choose **Basic Operations > Search > Target Search**.

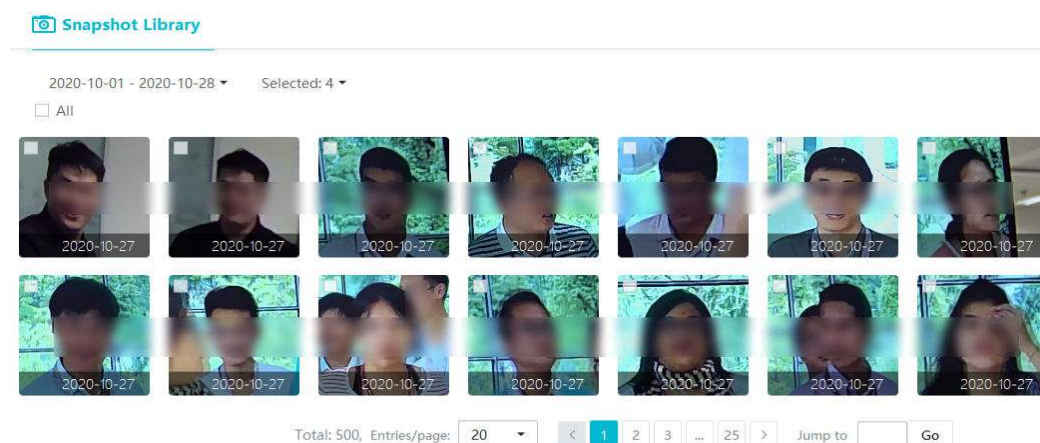
Step 2 Set search criteria. [Table 4-79](#) describes the parameters.

Table 4-79 Parameters for target search by criterion

Parameter	Description
Source	Cameras from which target images are searched for. You can select multiple cameras from various main devices.
Captured	Period during which the target images are captured.

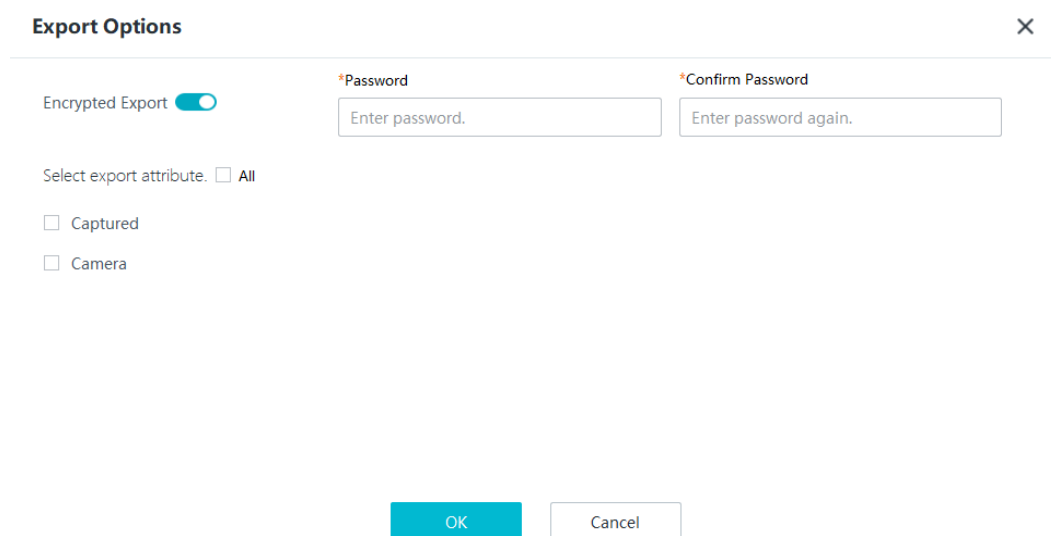
Step 3 Click **Search**. The **Snapshot Library** tab page is displayed with the search result, as shown in [Figure 4-100](#).

Figure 4-100 Result of target search by criterion



Step 4 (Optional) Use a clear target image for secondary search to obtain more target images. Click a target image in the search result. On the details page that is displayed, click **Search**.

Step 5 (Optional) Select **Export Selected**, **Export This Page**, or **Export All** from the **Export** drop-down list as required. [Figure 4-101](#) shows the file export dialog box.

Figure 4-101 Export OptionsThe image shows a dialog box titled "Export Options" with a close button (X) in the top right corner. Inside the dialog, there is a section for "Encrypted Export" with a toggle switch that is currently turned on. Below this, there is a label "Select export attribute." followed by a checkbox labeled "All". Underneath, there are two more checkboxes: "Captured" and "Camera". To the right of the "Encrypted Export" section, there are two input fields. The first is labeled "*Password" and contains the text "Enter password.". The second is labeled "*Confirm Password" and contains the text "Enter password again.". At the bottom of the dialog, there are two buttons: "OK" (highlighted in blue) and "Cancel".**NOTE**

You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files.

----End

4.7.6 Person Frequency Search

Application Scenario

The iClient S100 can quickly collect statistics on the customer entry and exit frequency, helping merchants identify regular customers.

Procedure

- Step 1** Choose **Basic Operations > Search > Person Frequency Search** on the iClient S100 home page.
- Step 2** Set search criteria and click **Search**. Items marked with a red asterisk are mandatory. The search result is displayed, as shown in [Figure 4-102](#). For the description of the key parameters, see [Table 4-80](#).

Figure 4-102 Person frequency search

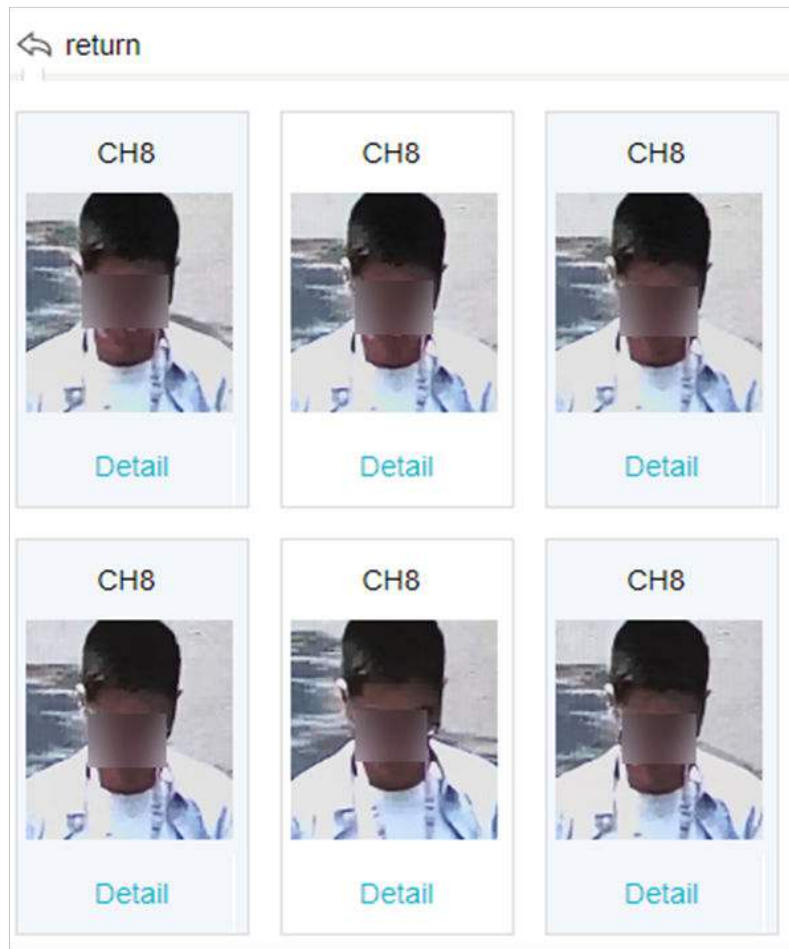
The interface is divided into two main sections. The left section, titled 'Personnel frequency search', contains various search criteria: NVR800 (NVR800-4.154), Channel (HoloSens SDC,Hua), List library, Starting Time (2021-03-23 00:00:00), End Time (2021-03-23 23:59:59), Min Interval(s) (0), Similarity (85), Gender, Age, Mouth Mask, Hair Style, Glasses, Hat, Maximum Display Quantity (10), and a Search button. The right section displays search results for four channels (CH3, CH4, CH3, CH4), each showing a person's face and a 'Frequency:1' label.

Table 4-80 Parameter description

Parameter	Description
Channel	Channel of cameras from which snapshots are searched. For example, if you choose the cameras connected to the NVR800, all snapshots from these cameras will be searched.
List library	Target list to be uploaded from the iClient S100 to the NVR800.
Min Interval(s)	Interval at which two target snapshots are taken consecutively. If multiple target snapshots are taken at an interval less than the value of this parameter, the system collects statistics only once. The value ranges from 1 to 65535 (unit: second).
Similarity	Similarity between the target image captured by a camera and the target image to be searched for. A lower similarity indicates a higher false positive rate. The value ranges from 1 to 100.
Maximum Display Quantity	Maximum number of target snapshots that are displayed in the search result. When the number of search results reaches the maximum, the search stops. The value ranges from 1 to 100.

Step 3 Click a snapshot in the search result. Then, all snapshots of the person are displayed, as shown in [Figure 4-103](#).

Figure 4-103 Snapshot results



Step 4 Click **Detail** under a snapshot to view the analysis result, as shown in [Figure 4-104](#).

Figure 4-104 Snapshot details

details





Channel

CH8

Starting Time

2020-12-15 08:43:38

End Time

2020-12-15 08:43:48

face number

RhEAEOhK0T8EBAEA

Gender:

male

Age:

25

Hair:

short hair

glasses:

normal glasses

Mask:

no

hat:

no



Add People To Repo

Cancel

Step 5 (Optional) If necessary, click **Add People to Repo** to add a person in the search result to the list, as shown in [Figure 4-105](#).

Figure 4-105 Adding a person to the list

The 'Import' dialog box contains the following fields and controls:

- Device***: Dropdown menu with 'NVR800-4.154' selected.
- List library***: Dropdown menu with 'zxy' selected.
- Personnel ID***: Text input field.
- Department***: Dropdown menu with 'CX' selected.
- First Name***: Text input field.
- Birthday**: Text input field.
- Gender**: Dropdown menu with '-----' selected.
- Mobile Phone**: Text input field.
- Certificate Type**: Dropdown menu with '二代身份证' selected.
- Certificate Number**: Text input field.
- Image**: Placeholder image with a 'Browse' button next to it.
- OK**: Blue button at the bottom center.

----End

4.7.7 Appearance Frequency

Application Scenario

The iClient S100 can generate alarms for customers with high entry and exit frequency, helping merchants identify regular customers.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an NVR800 and choose **Appearance Frequency** from the shortcut menu.
- Step 3** On the **Appearance Frequency** page, select a camera channel, set alarm parameters, and configure an alarm linkage policy. [Table 4-81](#) describes the key parameters.

Figure 4-106 Appearance Frequency

Appearance Frequency

▲ **Basic Settings**

Alarm switch ☐

Channel Number CH1;CH2;CH3;CH4;CH5;CH6;CH7;C...

To improve analysis accuracy of person occurrence frequency.
You are advised to set mode of selected cameras to Facial capture!

Personnel List

Frequency interval (s) 1 86400 1800

Alarm frequency threshold 2 20 2

Alarm statistical period (days) 1 90 30

Similarity 1 100 85

Max Stranger Count 1 50000 25000

A larger value of this parameter indicates more device resources are consumed, slowing down facial recognition. Set this parameter as needed!

Nonage ☐

Filter Out Alarms for Age Under 1 18 18

OK Cancel

Table 4-81 Appearance frequency analysis parameters

Category	Parameter	Description
Basic Settings	Alarm switch	Indicates whether to enable the alarm function for appearance frequency analysis. After this function is enabled, an alarm is generated when the appearance frequency reaches the preset threshold.
	Channel Number	Channel under the current main device for appearance frequency analysis.
	Personnel List	Personnel list for appearance frequency analysis.
	Frequency interval (s)	Interval in which appearances are counted only once.
	Alarm frequency threshold	Threshold for triggering an alarm for a person with high entry and exit frequency.

Category	Parameter	Description
	Alarm statistical period (days)	Period for collecting statistics on the entry and exit frequency of regular customers.
	Similarity	Similarity threshold. If the similarity is greater than or equal to the specified value, the target in the list is matched.
	Max Stranger Count	Maximum number of strangers that can be counted. A larger value of this parameter indicates that more device resources are consumed. As a result, the target recognition speed decreases. Set this parameter based on the site requirements.
	Nonage/Filter Out Alarms for Age Under	After the underage alarm filtering function is enabled, the system filters out persons who are younger than the specified age and does not collect statistics on them.
General Setting	Buzzer(s)	Alarm duration of the buzzer. The default value is 0 .
	Alarm Show	Indicates whether to display the status icon of the camera that triggers an alarm.
	Alarm Full screen	Indicates whether to play live video from the camera that triggers an alarm in full screen mode.
	Alarm Send Email	Indicates whether to send an email to a specified email address when an alarm is generated.
Alarm Output	Alarm Output	Alarm output device.
	Output Delay (s)	Output delay, in seconds. The default value is 10 .
Video Rule	Record	Indicates whether to record video when an alarm is generated.
	Snap Shot	Indicates whether to take snapshots when an alarm is generated.
	Record Delay (s)	Recording delay. The default value is 30 .

----End

Verification

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.7.8 List-based Target Alert

Application Scenario

The target alert feature can be used to recognize targets in a detection area and generate alarms for targets. Target alert functions are usually used in scenarios such as swing gates, security gates, and building entrances and exits. Example:

A building has strict security requirements. Only trustlisted persons are allowed to enter the building. If a person not in the trustlist, for example, a resigned employee or a blocklisted person, attempts to enter the building, the system will generate an alarm, instructing the security personnel to restrict the person's access.

Prerequisites

You have created a target list on the **Personal** page, imported person information to the target list, and synchronized the target list to the NVR800. For details, see [4.7.4 Target List Management](#).

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an NVR800 and choose **Target Alerts**.
- Step 3** On the **Ended** tab page, click a target list. On the **Task Info** page shown in [Figure 4-107](#), set parameters for a target alert task. [Table 4-82](#) describes the parameters.

Figure 4-107 Enabling a target alert task

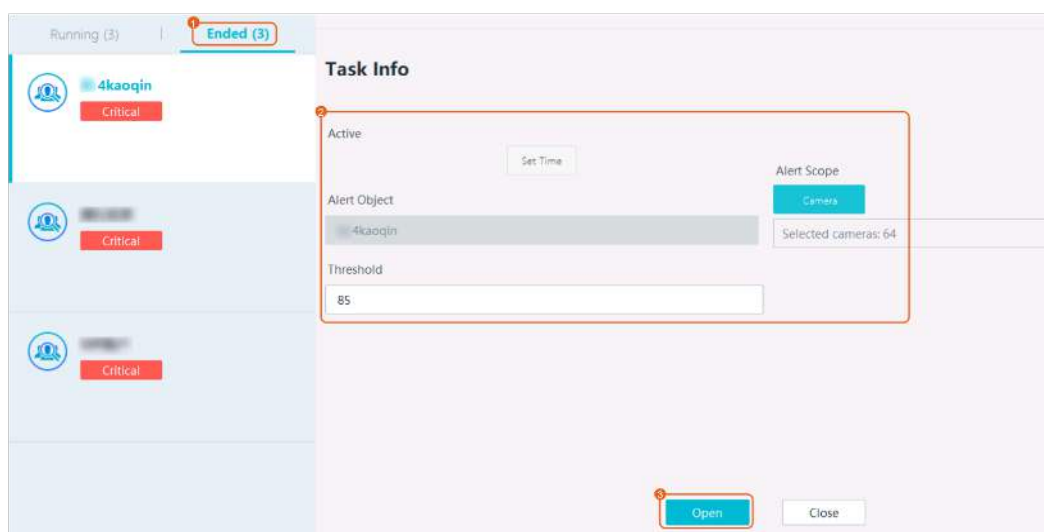


Table 4-82 Parameters for creating a target alert task

Parameter	Description
Active	Alert time range. Click Set Time to set the time segment for alert every day.
Threshold	Threshold of similarity to the target for alert.
Alert Scope	Alert scope. Click the text box under Camera and select cameras from the camera list. A maximum of 64 cameras can be selected.

Step 4 Click **Open**.

----End

Verification

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.7.9 Target Recognition Attendance

Procedure

- Step 1** Create a target list for target recognition attendance by referring to [4.7.4 Target List Management](#).
- Step 2** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 3** Create a target alert task based on the target list by referring to [4.7.8 List-based Target Alert](#).
- Step 4** Choose **Intelligent Applications > Target Recognition** and view the target recognition attendance result in real time.

If target recognition attendance has been configured for comprehensive applications, you can view the statistics on attendance data from cameras in the attendance statistics report. For details, see "Attendance Management."

----End

4.7.10 VIP Recognition

Procedure

- Step 1** Create a VIP list by referring to [4.7.4 Target List Management](#).
- Step 2** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 3** Create a target alert task based on the target list by referring to IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282866570.xml.

Step 4 Choose **Intelligent Applications > Target Recognition**. Then you can view the VIP recognition result in real time.

----End

4.7.11 Mask Detection

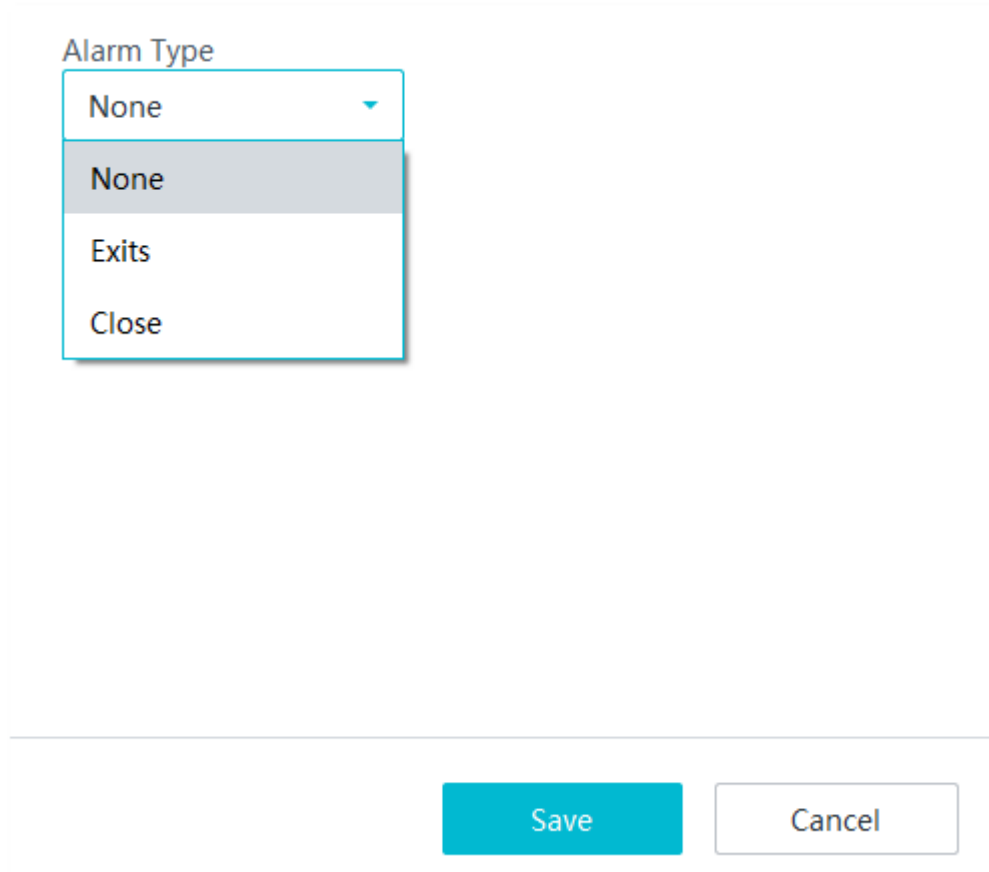
Application Scenario

In some public areas, pedestrians need to wear masks to meet health and safety requirements. In this scenario, you are advised to enable the mask detection function so that the system reports an alarm to the iClient S100 when detecting a person not wearing a mask.

Procedure

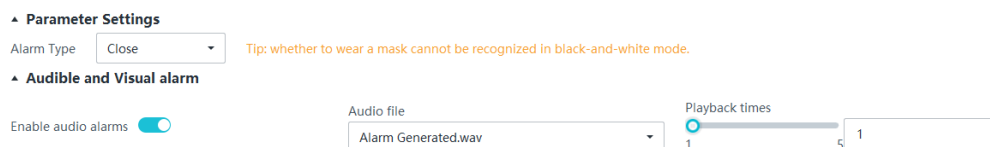
- Step 1** Choose **Maintenance Management > Smart Configuration** on the iClient S100 home page.
- Step 2** Select a camera under a main device and choose **Target Snapshot > Mask Recognition**
- Step 3** Set **Alarm Type** to **None**, as shown in [Figure 4-108](#).

Figure 4-108 Mask detection



- Step 4** After configuring audio files and selecting audio files and broadcast times, when the alarm is triggered, the front-end camera will broadcast voice.

Figure 4-109



- Step 5** Click **Save**. Choose **Intelligent Applications > Target Recognition**. Then you can view the mask detection result in real time.

----End

4.7.12 Customer Flow Analysis

Application Scenario

In densely populated areas such as business districts and restaurants, the NVR800 provides the customer flow analysis function to provide effective data support for user behavior analysis.

NOTE

Passenger flow analysis makes data statistics on the results based on the list database ratio, indicating the identification and statistical number of personnel in each list database on a certain day. Those who are not in the list database are strangers. How to distribute the list database in S100 to generate comparison data

Procedure

- Step 1** Choose **Intelligent Applications > Statistics > Target Report** on the iClient S100 home page.
- Step 2** Set the filter criteria and click **Confirm** to view the customer flow analysis result, as shown in [Figure 4-110](#). [Table 4-83](#) describes the parameters.

Figure 4-110 Customer flow analysis**Table 4-83** Parameter description

Parameter	Description
Statistical Period	Used to display statistical results in different report types. The options are Daily , Weekly , Quarterly , and Yearly .
Export	Used to export reports in different file formats. The options are EXCEL File , PDF File , and CSV File .

----End

4.7.13 Customer Flow Statistics

Application Scenario

In densely populated areas such as supermarkets entries and exits, the NVR800 provides the customer flow statistics collection function based on the list libraries and stranger dimensions to provide effective data support for user behavior analysis.

Procedure

- Step 1** Choose **Intelligent Applications > Statistics > Target Statistics** on the iClient S100 home page.
- Step 2** Set search criteria and click **OK**. You can view the crowd flow statistics result of the current device by list library and stranger, as shown in [Figure 4-111](#). [Table 4-84](#) describes the parameter and button.

Figure 4-111 Customer flow statistics

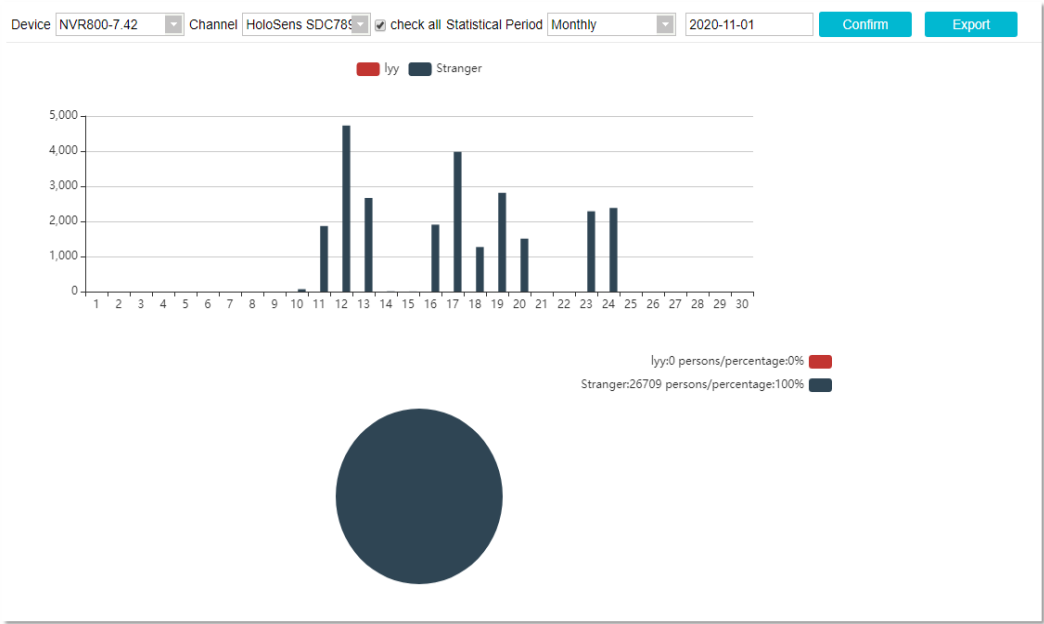


Table 4-84 Parameter/Button description

Parameter/Button	Description
Statistical Period	Used to display statistical results in different report types. The options are Daily , Weekly , Monthly , Quarterly , and Year .
Export	Used to export reports in different file formats. The options are EXCEL File , PDF File , and CSV File .

----End

4.8 Person Intelligence

4.8.1 Person Search

Application Scenario

This section describes how to search for person images captured by cameras connected to an NVR800 by criterion.

Prerequisites

The object classification service has been configured for the NVR800, and person images have been captured and stored.

Procedure

Step 1 Choose **Basic Operations > Search > Person Search** on the iClient S100 home page.

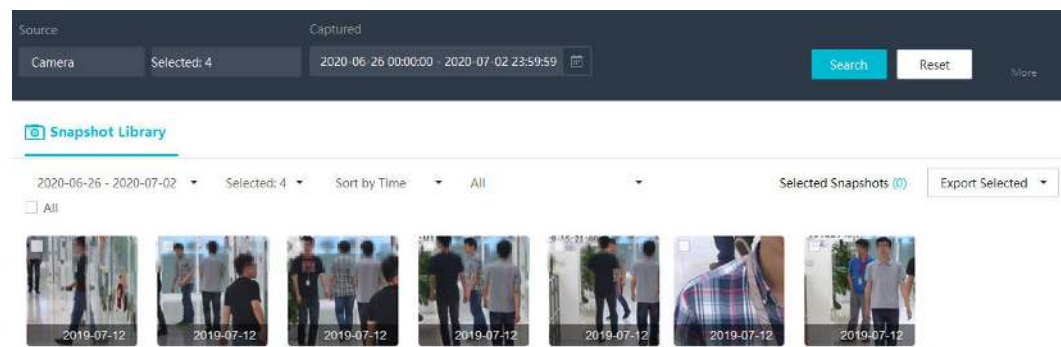
Step 2 Set search criteria. [Table 4-85](#) describes the parameters.

Table 4-85 Parameters for searching for persons by criteria

Parameter	Description
Source	Cameras from which person images are searched for. You can select multiple cameras from various main devices.
Captured	Period during which person images are captured.
Object Type	Type of the object for search, for example, Person or Cyclist . You can also set Tops Color , Backpack , Body Type , Helmet , Non-motorized Vehicle Color , and Non-motorized Vehicle Plate for accurate search.

Step 3 Click **Search**. The **Snapshot Library** tab page with the search result is displayed by default, as shown in [Figure 4-112](#). The snapshot library contains person images captured by cameras and extracted by personal feature recognition tasks or video structuring tasks.

Figure 4-112 Result of person search by criteria



Step 4 (Optional) Select multiple person images and click **Export Selected** to export the selected images. Alternatively, select **Export This Page** or **Export All** from the drop-down list box as required. [Figure 4-113](#) shows the file export dialog box.

Figure 4-113 Export Options

Export Options ✕

Encrypted Export ☒

*Password

*Confirm Password

Select export attribute. ☐ All

☐ Sex	☐ Glasses	☐ Umbrella	☐ Luggage
☐ Age	☐ Face Mask	☐ Helmet	☐ Non-motor Vehicle Shade
☐ Tops Color	☐ Match	☐ Helmet Color	☐ Shade Color
☐ Tops Style	☐ Object Type	☐ Non-motor Vehicle Type	☐ Smoking
☐ Bottoms Color	☐ Captured	☐ Non-motor Vehicle Color	☐ Hands-Free Violation
☐ Bottoms Style	☐ Camera	☐ Crossbody Bag	☐ BodySearch.colum.carryGoodsBox
☐ Tops Pattern	☐ Hat	☐ Figure	☐ Overload
☐ Backpack	☐ Orientation	☐ Non-motor Vehicle Plate	☐ Vehicle Lamp Shape
☐ Handbag	☐ Hairstyle	☐ Holding Object	☐ Non-motor Vehicle Subtype

NOTE

You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files.

-----End

4.9 Situation Analysis

4.9.1 Head Counting

Application Scenario

You can set a detection area and a detection line to collect statistics on the number of persons crossing the detection line.

When a pedestrian crosses the detection line, the system counts the number of people exiting and entering. When the sum of the two numbers reaches the preset alarm threshold, the camera reports an alarm to the main device. Then the alarm message will be displayed on the iClient S100.

Enable alarm linkage. For details, see `IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml`.

Restrictions

- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.
- This function is mutually exclusive with target capture and behavior analysis. Before enabling this function, ensure that target capture and behavior analysis are disabled.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Situation Analysis > CrossLine Statistics**.
- Step 3** Enable head counting and set parameters such as detection area parameters, as shown in [Figure 4-114](#).

Figure 4-114 Configuring head counting

Parameter Settings

Enable CrossLine Statistics ☒ Enable ZeroClear ☐ Clear Statistics

Alarm Detection Interval(s) Alarm Count

Audible and Visual alarm

Audio ☐

Area Settings

+ Area + Line Delete

Plan Settings

+ Add Delete All

No.	Execution Date	Start Time	End Time	Date	Mode	Operation
1	1970-01-01	00:00:00	23:59:59	Every Day	Weekly cycle	

Save Cancel

1. Set parameters in the **Parameter Settings** area. [Table 4-86](#) describes the parameters.

Table 4-86 Parameter description

Parameter	Description
Enable ZeroClear	Indicates whether to clear statistics on the live video viewing page at 00:00 of the next day.
Clear Statistics	Clears the current statistics immediately.
Alarm Detection Interval(s)	Interval at which alarms are checked.
Alarm Count	Alarm threshold for the number of persons who cross the detection line.

2. Set audible and visual alarm parameters. [Table 4-87](#) describes the parameters.

Table 4-87 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters. [Table 4-88](#) describes the parameters.

Table 4-88 Area setting parameters

Parameter	Description
Area	Button for drawing a maximum of one detection area.
Line	Button for drawing a maximum of one detection line.

Parameter	Description
Delete	Button for deleting a selected detection area or detection line.
Direction	Direction in which a pedestrian crosses the detection line. The options are as follows: – A->B: Collects statistics on the number of pedestrians who cross the detection line from A to B. – B->A: Collects statistics on the number of pedestrians who cross the detection line from B to A.

4. Set plan parameters. [Table 4-89](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-89 Plan settings

Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

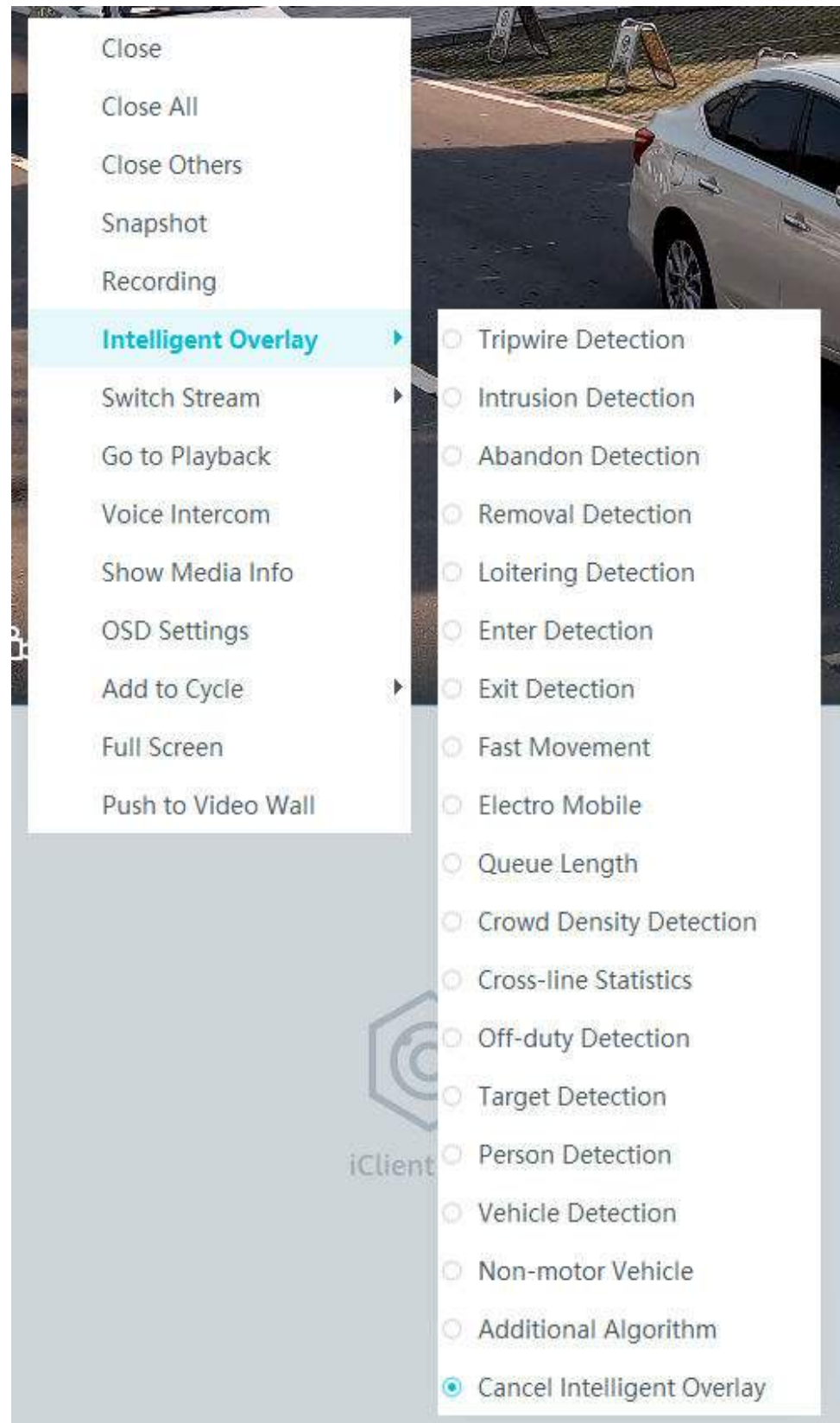
Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - On the iClient S100 home page, choose **Basic Operations > Live**.
 - Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure](#)

4-115. The real-time intelligent analysis result is superimposed on the video image.

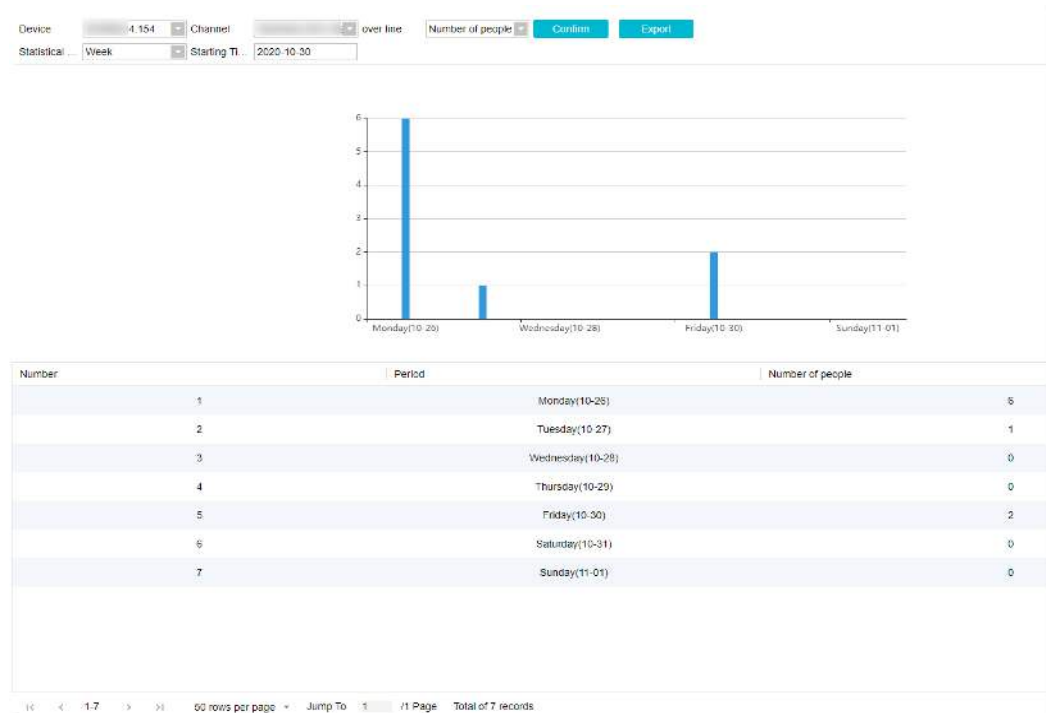
Figure 4-115 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

- Viewing statistical results
 - a. Choose **Intelligent Applications > Statistics > CrossLine Statistics** on the iClient S100 home page.
 - b. Set filter criteria and view head counting results, as shown in **Figure 4-116**.

Figure 4-116 Head counting



4.9.2 Queue Length Detection

Application Scenario

You can set a detection area to detect the queue length in the area.

You can set the service processing duration for a single person based on the service type (such as ticket check). When the predicted total processing duration (total queuing time) in the detection area exceeds the preset threshold, the camera reports an alarm to the main devices, and the alarm message will be displayed on the iClient S100.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml.

Restrictions

- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.

- This function is mutually exclusive with target capture and behavior analysis. Before enabling this function, ensure that target capture and behavior analysis are disabled.

Procedure

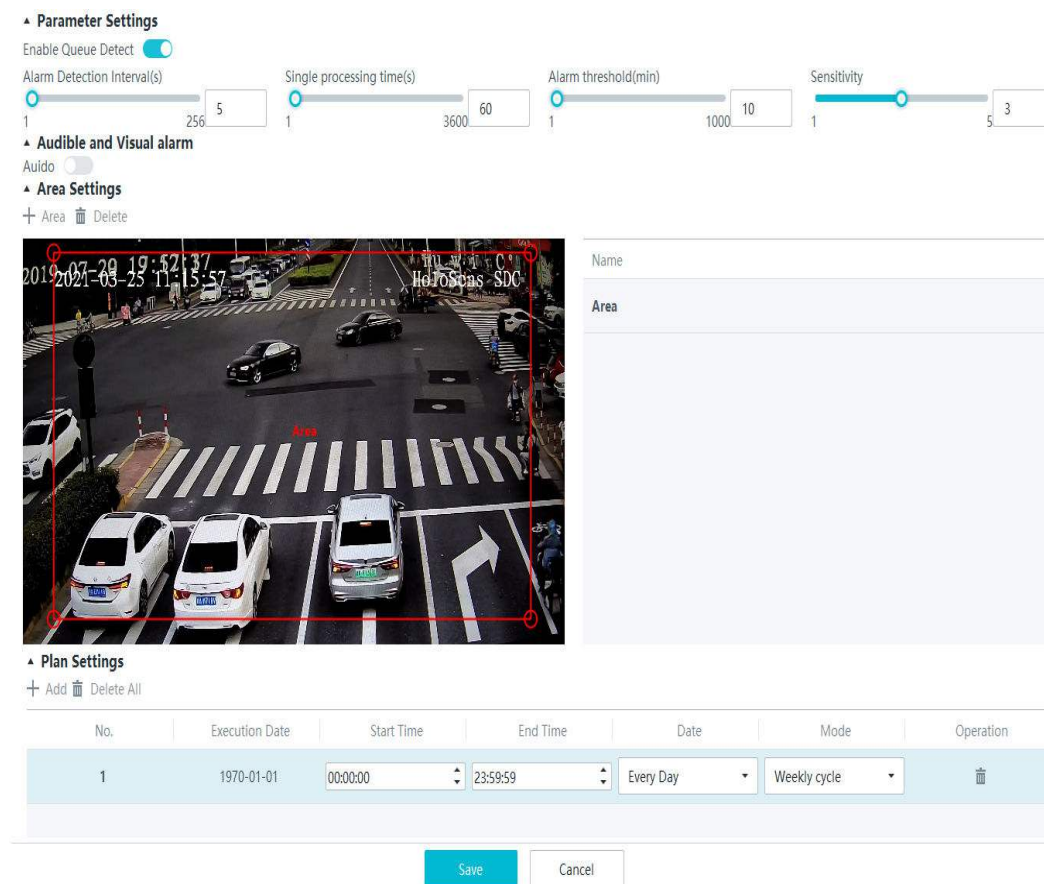
- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera under a main device.
- Step 3** **Optional:** For cameras in multi-algorithm mode, choose **Intelligent Global Configuration > Algorithm Mode** and set **Algorithm mode** to **Behavior analysis**.

NOTE

After the algorithm mode is switched, the camera will restart for the setting to take effect. Wait for 3 minutes and then set intelligent services.

- Step 4** Choose **Situation Analysis > Queue Detect**.
- Step 5** Enable queue length detection and set parameters such as detection area parameters, as shown in [Figure 4-117](#).

Figure 4-117 Configuring queue length detection



Parameter Settings

Enable Queue Detect ☒

Alarm Detection Interval(s)

Single processing time(s)

Alarm threshold(min)

Sensitivity

Audible and Visual alarm

Audio ☐

Area Settings

+ Area  Delete

Plan Settings

+ Add  Delete All

No.	Execution Date	Start Time	End Time	Date	Mode	Operation
1	1970-01-01	00:00:00	23:59:59	Every Day	Weekly cycle	

1. Set parameters in the **Parameter Settings** area. [Table 4-90](#) describes the parameters.

Table 4-90 Parameter description

Parameter	Description
Alarm Detection Interval(s)	Interval at which alarms are checked.
Single processing time (s)	Processing duration for a single person.
Alarm threshold (min)	Alarm threshold.
Sensitivity	Detection sensitivity. The value ranges from 1 to 5. A larger value indicates a higher sensitivity level.

2. Set audible and visual alarm parameters. [Table 4-91](#) describes the parameters.

Table 4-91 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	intercom support this function. You need to set parameters related to the light.
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters. [Table 4-92](#) describes the parameters.

Table 4-92 Area setting buttons

Button	Description
Area	Button for drawing a maximum of one detection area.
Delete	Button for deleting a selected detection area.

4. Set plan parameters. [Table 4-93](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-93 Plan settings

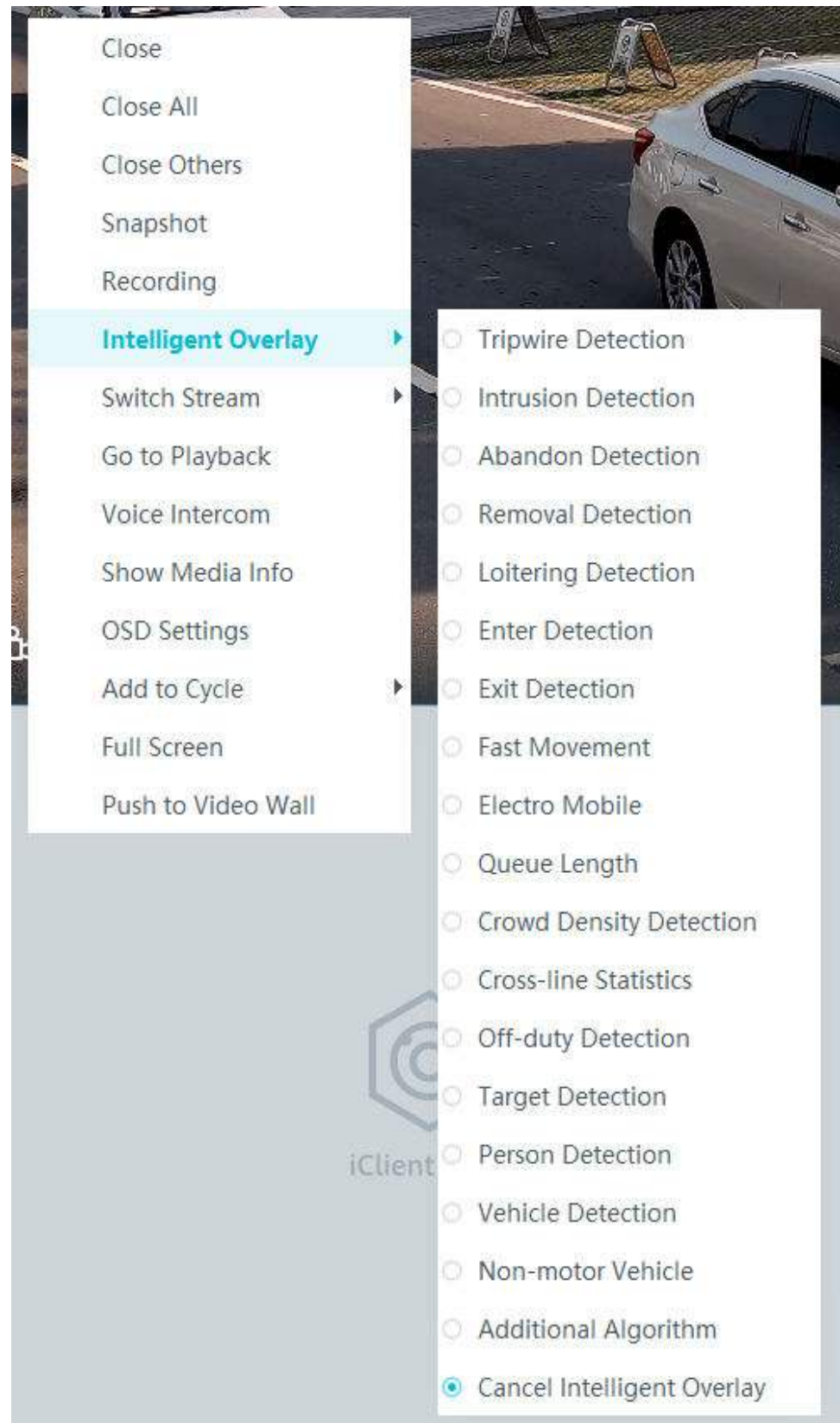
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 6 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > *Intelligent Event Name*** from the displayed menu, as shown in **Figure 4-118**. The real-time intelligent analysis result is superimposed on the video image.

Figure 4-118 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.9.3 Crowd Density Detection

Application Scenario

You can set a detection area to detect the crowd density in the area.

Once the number of persons in the detection area reaches the alarm threshold, the camera reports an alarm to the main device. Then the alarm message will be displayed on the iClient S100.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml.

Restrictions

- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.
- This function is mutually exclusive with target capture and behavior analysis. Before enabling this function, ensure that target capture and behavior analysis are disabled.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Situation Analysis > Crowd Density**.
- Step 3** Enable crowd density detection and set parameters such as detection area parameters, as shown in [Figure 4-119](#).

Figure 4-119 Configuring crowd density detection

Enable Crowd Density ☒

Alarm Check Interval (s)

Alarm threshold (Num)

Sensitivity

▲ Crowd Density

+ Add Area - Delete

2020-10-27 20:48:26 HoloSens SDC

test 333ddffessl

Name

Area

▲ Plan

☒ Daily ☐ Weekly

00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00 24:00

Save Cancel

1. Set parameters in the **Parameter Settings** area. [Table 4-94](#) describes the parameters.

Table 4-94 Parameter description

Parameter	Description
Alarm Check Interval (s)	Interval at which alarms are checked.
Alarm threshold (Num)	Alarm threshold for the number of persons in a detection area.
Sensitivity	Detection sensitivity. The value ranges from 1 to 5. A larger value indicates a higher sensitivity level.

2. Set audible and visual alarm parameters. [Table 4-95](#) describes the parameters.

Table 4-95 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an

Parameter	Description	Requirement on Cameras
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters. [Table 4-96](#) describes the parameters.

Table 4-96 Area setting buttons

Button	Description
Area	Button for drawing a maximum of one detection area.
Delete	Button for deleting a selected detection area.

4. Set plan parameters. [Table 4-97](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-97 Plan settings

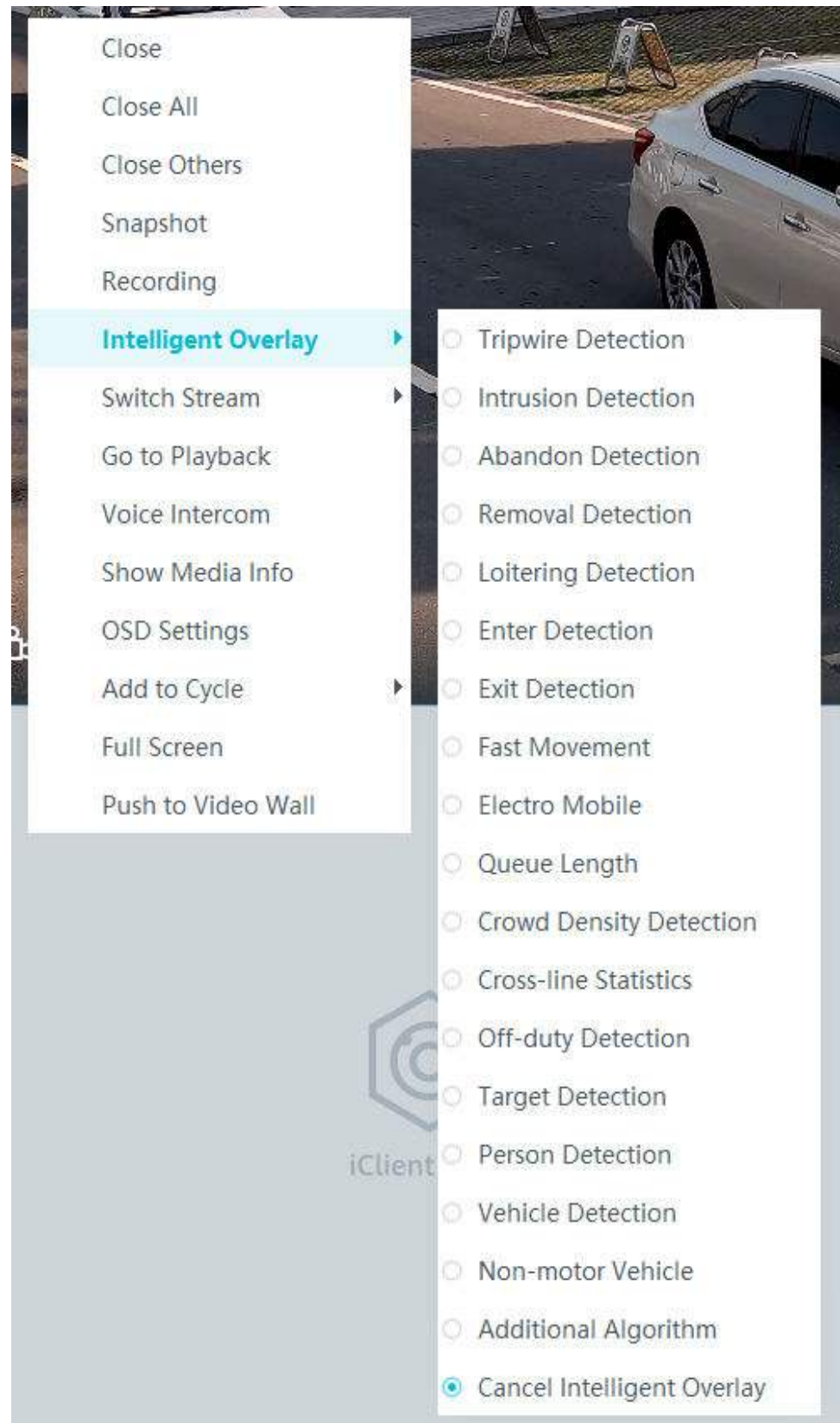
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-120](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-120 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.9.4 Heat Map

Application Scenario

You can set one or more detection areas to detect the activity degree of persons in these areas. Heat maps can be displayed by time and space.

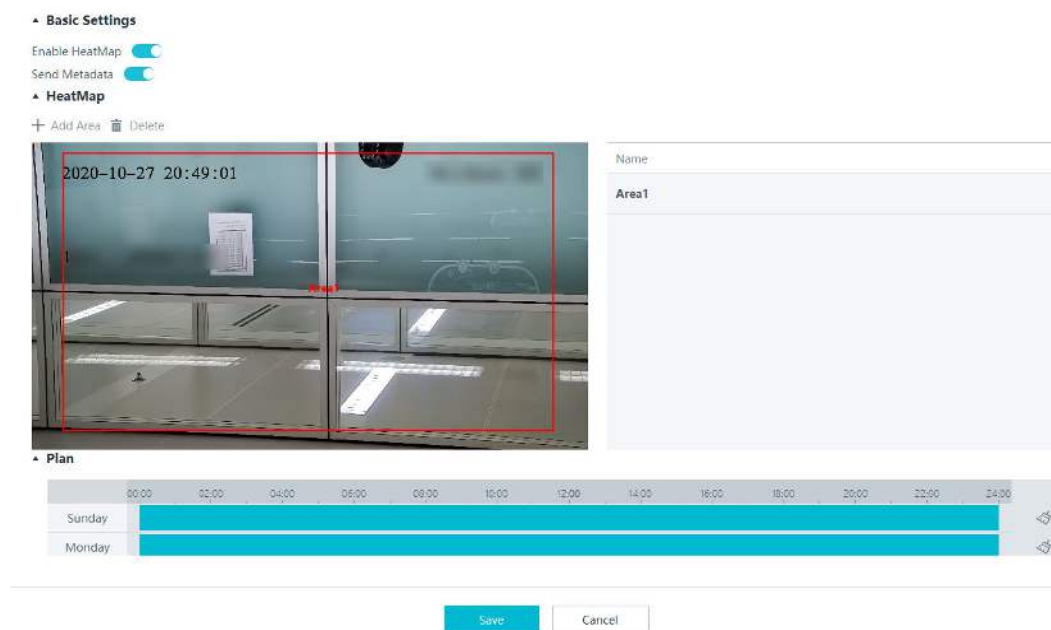
- Spatial heat map: displays the activity degree of people in different areas. The red area has the highest density and activity degree, and the blue one has the lowest density.
- Temporal heat map: displays the activity degree of people in different times. The vertical coordinate is an index calculated based on the number of people and duration of stay but does not indicate the number of persons. A larger value indicates a higher activity degree.

Restrictions

- The intelligent camera used for heat map statistics collection must be equipped with an available SD card. The heat map data will be stored in the SD card and can be stored for a maximum of one year.
- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.
- This function is mutually exclusive with behavior analysis. Before enabling this function, ensure that behavior analysis is disabled.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Situation Analysis > HeatMap**.
- Step 3** Enable heat map detection and set parameters such as detection area parameters, as shown in [Figure 4-121](#). [Table 4-98](#) describes the parameters and buttons.

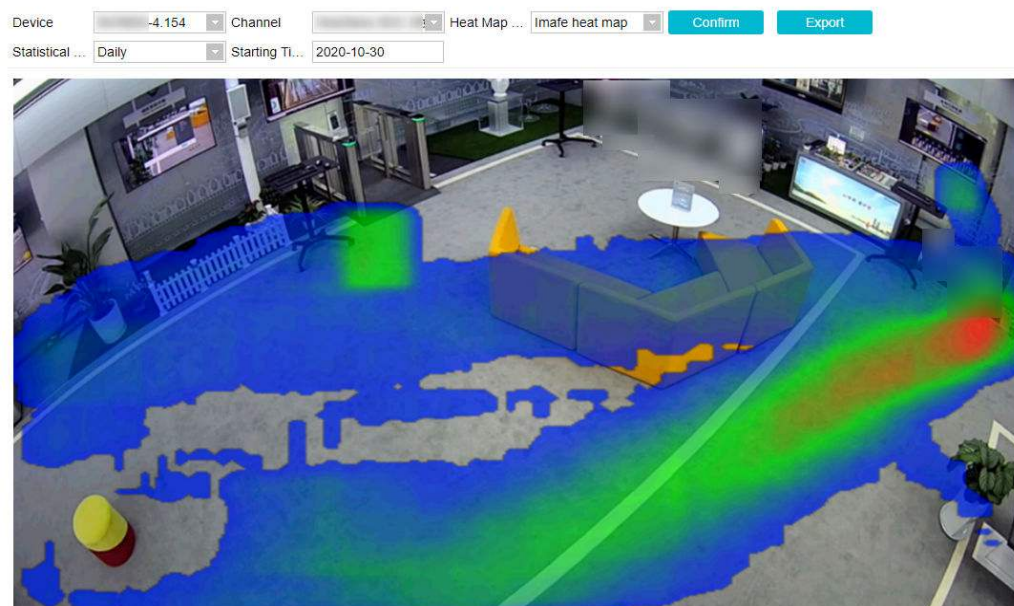
Figure 4-121 Configuring heat map**Table 4-98** Parameter/Button description

Parameter/ Button	Description
Enable HeatMap	Indicates whether to enable the heat map function for a camera
Send Metadata	Indicates whether to send metadata. After this function is enabled, the camera sends the heat map result to the iClient S100.
Add Area	Button for adding an area. A maximum of eight detection areas can be drawn.
Delete	Button for deleting a selected detection area.

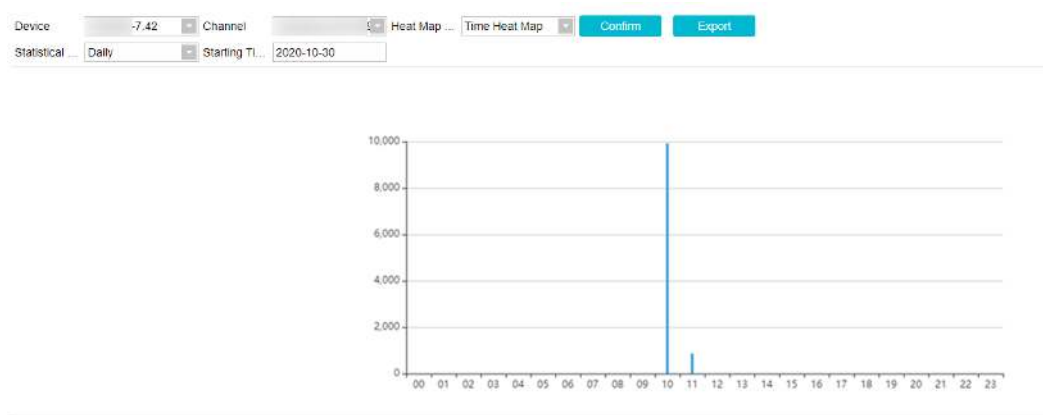
----End

Verification

- Step 1** Choose **Intelligent Applications > Statistics > HeatMap Statistics** on the iClient S100 home page.
- Step 2** Set filter criteria and view heat map statistics.
- View spatial heat map, as shown in [Figure 4-122](#).

Figure 4-122 Spatial heat map

- View temporal heat map, as shown in [Figure 4-123](#).

Figure 4-123 Temporal heat map

----End

4.9.5 Off-Duty Detection

Application Scenario

You can set a detection area to detect on-duty status in the area.

Once the off-duty duration of an employee in the detection area reaches the alarm threshold, the camera reports an alarm to the main device. Then the alarm message will be displayed on the iClient S100.

Enable alarm linkage. For details, see `IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml`.

Restrictions

- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.
- This function is mutually exclusive with target capture and behavior analysis. Before enabling this function, ensure that target capture and behavior analysis are disabled.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Situation Analysis > Off-duty Detection**.
- Step 3** Enable off-duty detection and set parameters such as detection area parameters, as shown in [Figure 4-124](#).

Figure 4-124 Configuring off-duty detection

Parameter Settings

Enable Off-duty Detection: ☐ Superimpose metadata on alarm-triggered snapshot: ☐

On-duty persons: 1 5 1

Off-duty duration(s): 1 600 1

Alarm Detection Interval(s): 1 256 1

Audible and Visual alarm

Enable audio alarms: ☐

Area Settings

+ Area - Delete

2021-05-25 Tue 15:21:57 siufffgg

osd2 OSD3

Plan Settings

+ Add - All Delete

No.	Start Time	End Time	Date	Mode	Operation
1	00:00:00	23:59:59	Every Day	Weekly cycle	

Save Cancel

1. Set parameters in the **Parameter Settings** area. [Table 4-94](#) describes the parameters.

Table 4-99 Parameter description

Parameter	Description
Superimpose metadata on alarm-triggered snapshot	Indicates whether to superimpose metadata information on alarm-triggered snapshots, such as intelligent analysis rules and results.
On-duty persons	Total number of employees that should be on duty.
Off-duty duration (s)	Interval for generating an alarm after an employee is detected off-duty.
Alarm Detection Interval(s)	Interval at which alarms are checked.

2. Set audible and visual alarm parameters. [Table 4-100](#) describes the parameters.

Table 4-100 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	- You can directly use this function when an intelligent IR/white-light camera with intercom is used. - To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	intercom support this function. You need to set parameters related to the light.
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters. [Table 4-101](#) describes the parameters.

Table 4-101 Area setting buttons

Button	Description
Area	Button for drawing a maximum of one detection area.
Delete	Button for deleting a selected detection area.

4. Set plan parameters. [Table 4-102](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 4-102 Plan settings

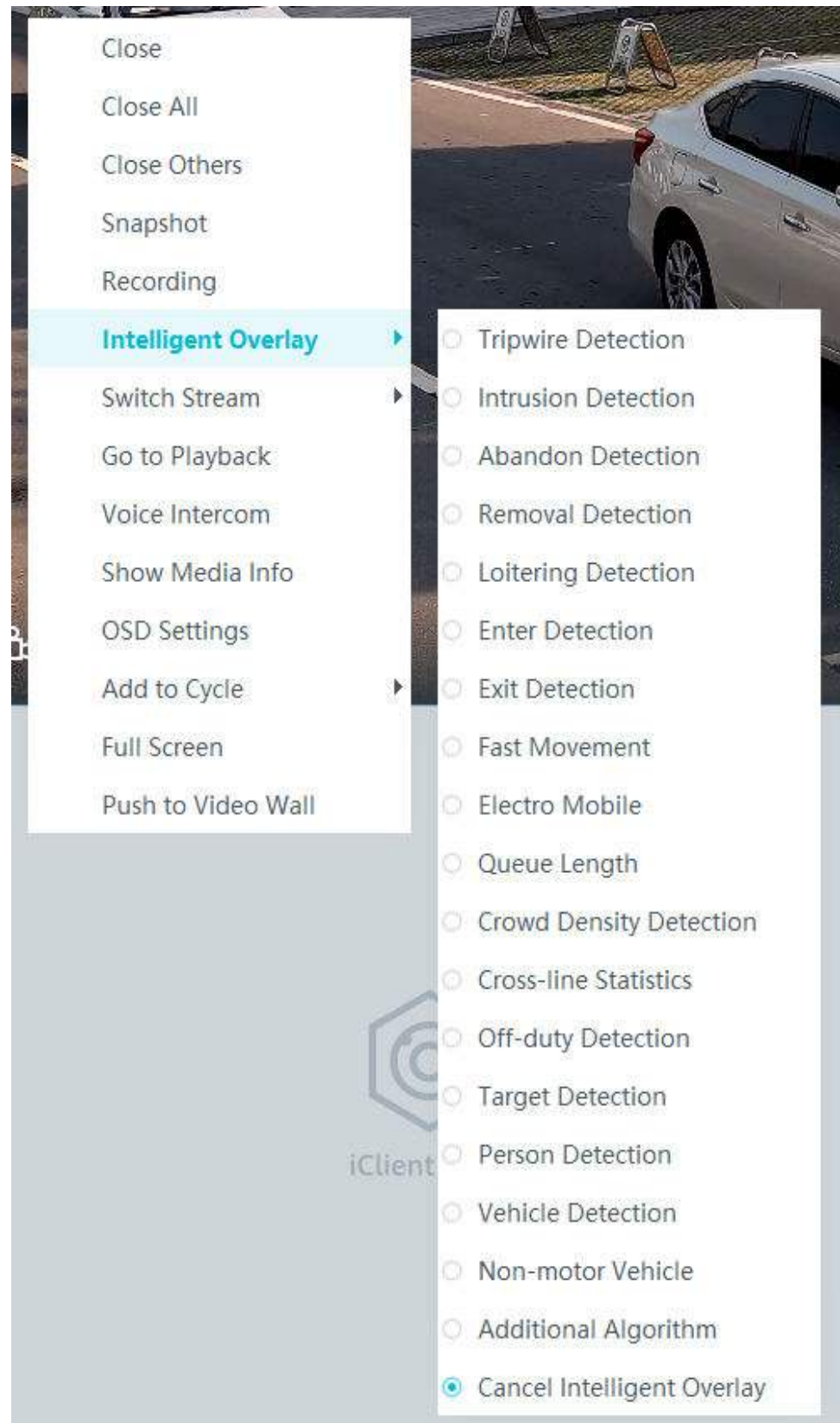
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > *Intelligent Event Name*** from the displayed menu, as shown in **Figure 4-125**. The real-time intelligent analysis result is superimposed on the video image.

Figure 4-125 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.10 Vehicle Intelligence

4.10.1 Global Configuration

Application Scenario

Before configuring vehicle intelligence on the iClient S100, complete global configuration.

Restrictions

- The NVR800 provides the vehicle intelligence function when it is connected to D2181-10-SL-PU or Dxxxx-10-SIU cameras. For details about the version mappings, see *NVR800 9.0.0 Compatibility List*.
- The object classification and motor vehicle detection functions are mutually exclusive. Ensure that only one of them is enabled at a time.

Configuring the Algorithm Mode

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Smart Global Configuration > Algorithm Mode**.

Step 3 Set **Algorithm** to **Micro checkpoint**.

NOTE

After the algorithm mode is switched, the camera will restart for the setting to take effect. Wait for 3 minutes and then set intelligent services.

Step 4 Click **Save**.

----End

Configuring Object Classification

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and click **Vehicle Intelligence > Machine Inhuman Detection**.

Step 3 Enable the object classification function, add a detection area, and set related parameters, as shown in [Figure 4-126](#). [Table 4-103](#) describes the parameters and buttons.

Figure 4-126 Configuring object classification

Parameter Settings

Enable Machine Inhuman Detection ☒

License plate compensation level

1

100

50

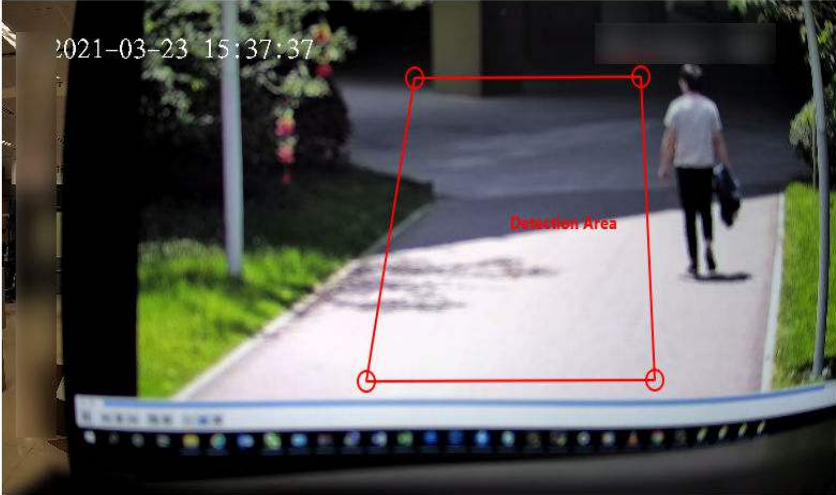
License plate brightness compensation ☒

Priority province (city)

None

Area Settings

+ Area
Delete

2021-03-23 15:37:37


Name

Detection Area

Save

Cancel

Table 4-103 Parameter/Button description

Parameter/ Button	Description
Enable Machine Inhuman Detection	Indicates whether to enable the object classification function. NOTE This function is mutually exclusive with the motor vehicle detection function and cannot take effect at the same time. Before enabling this function, ensure that motor vehicle detection function is disabled.
License plate brightness compensation	Brightness compensation for captured license plate images with too high or too low brightness.
License plate compensation level	Level of brightness compensation for captured license plate images. This parameter is available only when License plate brightness compensation is enabled. You can increase the value of the parameter when the environment is dark.
Priority province (city)	Preferential province (or city) name abbreviation used when the first character of a license plate cannot be recognized. Only one province (or city) name abbreviation can be configured.

Parameter/ Button	Description
Area	Button for adding a detection area. You can draw only one detection area.
Delete	Button for deleting a selected detection area.

Step 4 Click **Save**.

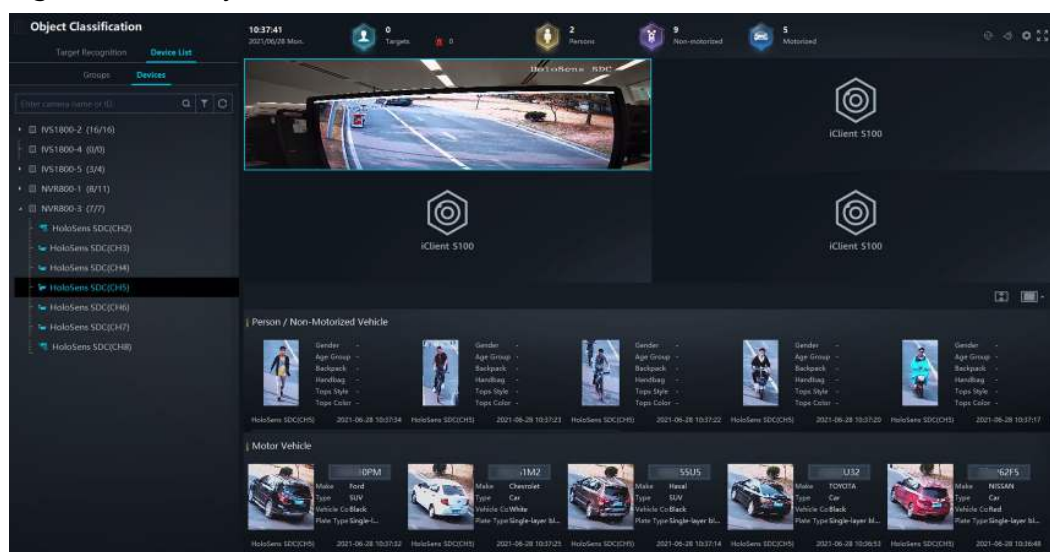
----End

Verification

Step 1 On the iClient S100 home page, choose **Intelligent Applications > Object Classification**.

Step 2 Drag the required camera to the video pane. Object classification results and snapshots will be displayed under the video pane in real time, as shown in [Figure 4-127](#).

Figure 4-127 Object classification results



----End

4.10.2 Vehicle Search

Application Scenario

You can search for vehicle images captured by cameras on the NVR800 based on search criteria.

Prerequisites

The NVR800 have captured and stored vehicle images through object classification.

Procedure

- Step 1** On the iClient S100 home page, choose **Basic Operations > Search > Vehicle Search**.
- Step 2** Configure vehicle search criteria, as shown in [Figure 4-128](#).

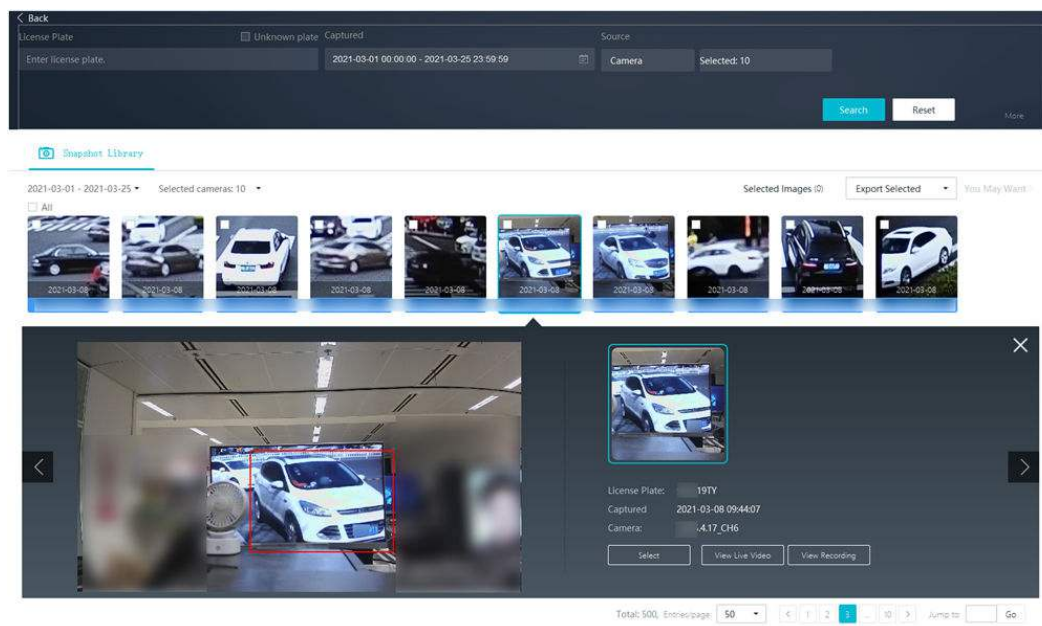
Figure 4-128 Configuring vehicle search criteria

[Table 4-104](#) describes the key parameters. Set other parameters based on the site requirements.

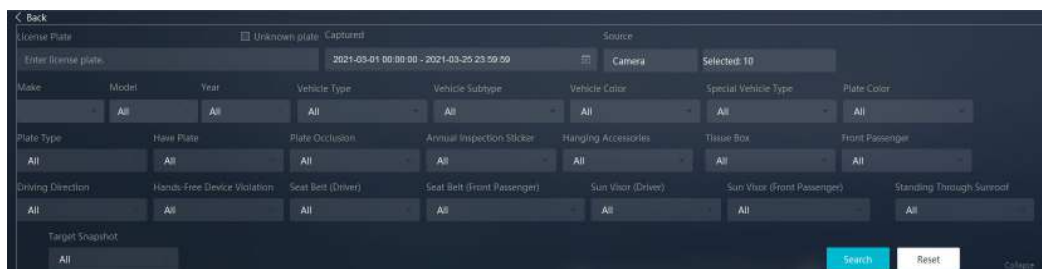
Table 4-104 Parameter description

Parameter	Setting
License Plate	License plate characters of the vehicle to be searched for. (The value is case insensitive). Fuzzy search is supported, where the question mark (?) matches exactly one character, and the asterisk (*) matches zero or more characters.
Unknown plate	Indicates whether to search for vehicles whose license plates have not been properly captured. If you select this check box, the License Plate parameter becomes unavailable, and the iClient S100 will search for vehicle images without clear license plates.
Captured	Period during which the vehicle images are captured.
Source	Cameras from which vehicle images are searched for. You can select multiple cameras from various main devices.

- Step 3** Click **Search** to search for vehicle information based on the configured search criteria. The statistics result is displayed, as shown in [Figure 4-129](#).

Figure 4-129 Vehicle search results

Step 4 Optional: For further search, click **More** to set the search criteria. [Figure 4-130](#) describes the search criteria.

Figure 4-130 More search criteria

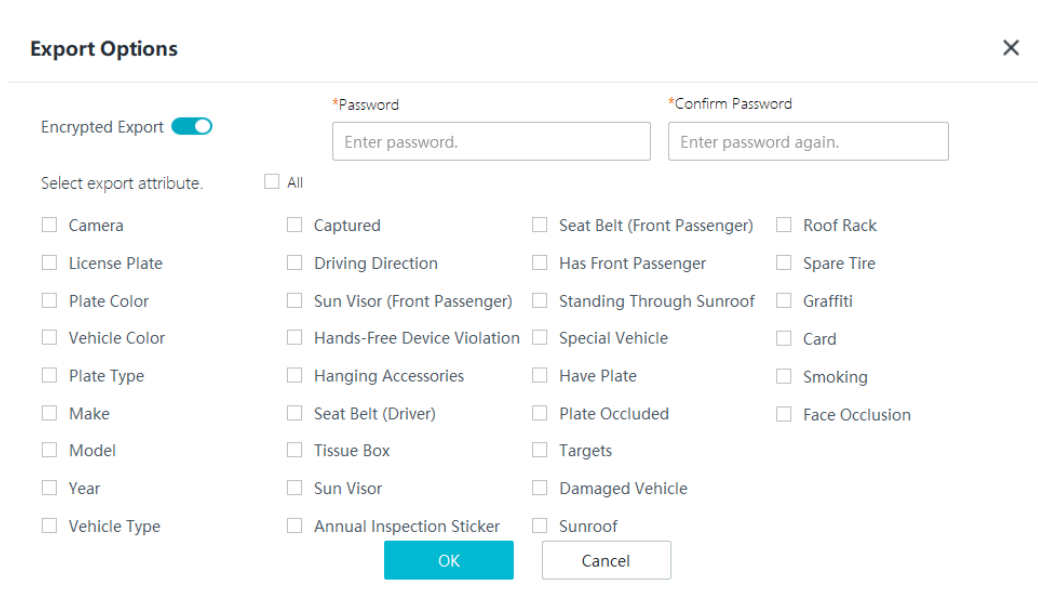
Step 5 Select multiple vehicle images and click **Export Selected** to export the selected images. Alternatively, select **Export This Page** or **Export All** from the drop-down list box as required. [Figure 4-131](#) shows the **Export Options** dialog box.

NOTE

You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files.

The password must meet the following requirements:

- Contains 10 to 16 characters.
- Contains at least two types of the following: lowercase letters, uppercase letters, digits, and special characters.
- Must be different from the user name or user name spelled backwards.
- Cannot contain space characters or Chinese characters.
- Cannot be a weak password.

Figure 4-131 Export Options dialog box


The dialog box is titled "Export Options" and has a close button (X) in the top right corner. It contains the following elements:

- Encrypted Export:** A toggle switch that is currently turned on.
- *Password:** A text input field with the placeholder text "Enter password."
- *Confirm Password:** A text input field with the placeholder text "Enter password again."
- Select export attribute:** A section with a list of checkboxes for various attributes.

Attribute	Attribute	Attribute	Attribute
☐ Camera	☐ Captured	☐ Seat Belt (Front Passenger)	☐ Roof Rack
☐ License Plate	☐ Driving Direction	☐ Has Front Passenger	☐ Spare Tire
☐ Plate Color	☐ Sun Visor (Front Passenger)	☐ Standing Through Sunroof	☐ Graffiti
☐ Vehicle Color	☐ Hands-Free Device Violation	☐ Special Vehicle	☐ Card
☐ Plate Type	☐ Hanging Accessories	☐ Have Plate	☐ Smoking
☐ Make	☐ Seat Belt (Driver)	☐ Plate Occluded	☐ Face Occlusion
☐ Model	☐ Tissue Box	☐ Targets	
☐ Year	☐ Sun Visor	☐ Damaged Vehicle	
☐ Vehicle Type	☐ Annual Inspection Sticker	☐ Sunroof	
- Buttons:** "OK" (blue) and "Cancel" (white) buttons at the bottom right.

----End

4.10.3 Object Classification Statistics

Application Scenario

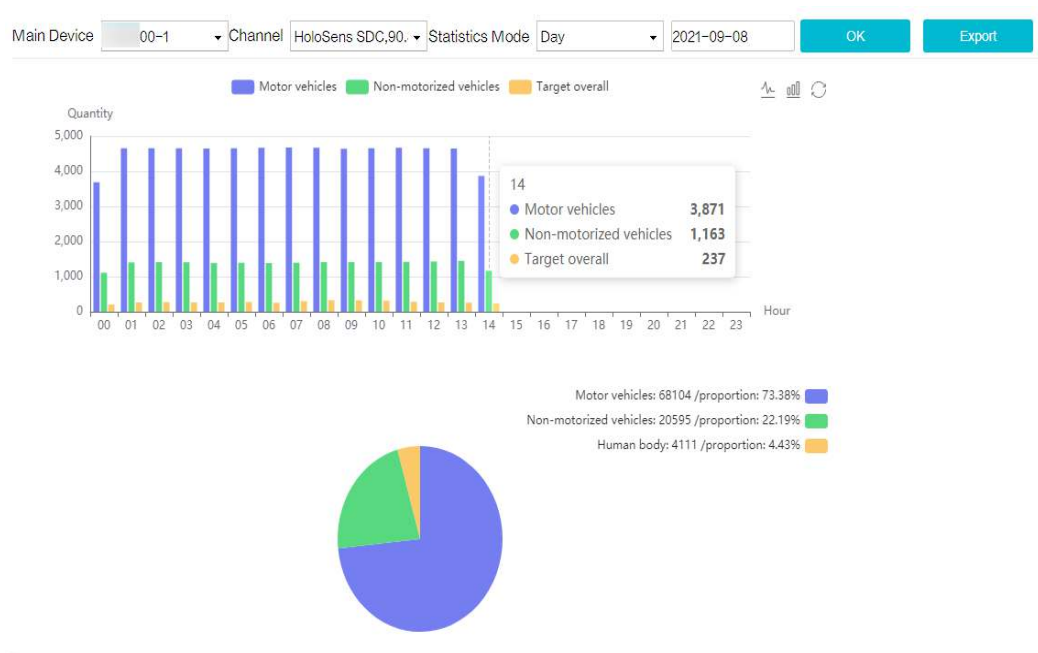
In areas with large people and vehicle traffic such as intersections, the NVR800 provides the object classification statistics collection function to provide effective data support for behavior analysis.

Prerequisites

The NVR800 have captured and stored vehicle images through object classification.

Procedure

- Step 1** Choose **Intelligent Applications > Statistics > Object Classification Statistics** on the iClient S100 home page.
- Step 2** Set search criteria and click **Confirm**. The object classification statistics result is displayed, as shown in [Figure 4-132](#). [Table 4-105](#) describes the parameters.

Figure 4-132 Object classification statistics**Table 4-105** Parameter/Button description

Parameter/Button	Description
Statistical Period	Used to display statistical results in different report types. The options are Daily , Weekly , Monthly , Quarterly , and Year .
Export	Used to export reports in different file formats. The options are EXCEL File , PDF File , and CSV File .

-----End

4.10.4 Parking Violation Detection

Application Scenario

This function can be used to detect whether motor vehicles are parked in a specified detection area. The iClient S100 reports an alarm upon detecting a motor vehicle parking in a preset detection area.

Enable alarm linkage. For details, see [4.12.2 Alarm Linkage](#).

Configuring the Algorithm Mode

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera connected to a main device and choose **Smart Global Configuration > Algorithm Mode**.

Step 3 Set Algorithm to Micro checkpoint.**NOTE**

After the algorithm mode is switched, the camera will restart for the setting to take effect. Wait for 3 minutes and then set intelligent services.

Step 4 Click Save.

----End

Settings Motor Vehicle Detection Parameters

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Vehicle Intelligent > Vehicle Parameter**.

Step 3 Enable motor vehicle detection, add a detection area, and set related parameters, as shown in [Figure 4-133](#). [Table 4-106](#) describes the parameters and buttons.

Figure 4-133 Settings motor vehicle detection parameters

Parameter Settings

Enable motor vehicle parameters ☒

License plate brightness compensation ☒

License plate compensation level

Priority province (city)

Area Settings

+ Area

2021-03-23 15:40:03

Area

Save Cancel

Table 4-106 Parameter/Button description

Parameter/ Button	Description
Enable motor vehicle parameters	Indicates whether to take snapshots of motor vehicles. NOTE This function is mutually exclusive with object classification. Before enabling this function, ensure that object classification is disabled.
License plate brightness compensation	Indicates whether to enable brightness compensation for captured license plate images with too high or too low brightness.
License plate compensation level	Level of brightness compensation for captured license plate images. This parameter is available only when License plate brightness compensation is enabled. You can increase the value of the parameter when the environment is dark.
Priority province (city)	Preferential province (or city) name abbreviation used when the first character of a license plate cannot be recognized. Only one province (or city) name abbreviation can be configured.
Area	Button for adding a detection area. A maximum of one detection area can be drawn.
Delete	Button for deleting a selected detection area.

Step 4 Click **Save**.

----End

Configuring Parking Violation Detection

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Vehicle Intelligence > Illegal Parking Detection**.

Step 3 Enable the parking violation detection function, add a detection area, and set related parameters, as shown in [Figure 4-134](#). [Table 4-107](#) describes the parameters and buttons.

Figure 4-134 Configuring parking violation detection

Parameter Settings

Enable illegal parking detection ☒

Sensitivity

Illegal parking trigger time(s)

Alarm Detection Interval(s)

Area Settings

+ Area



Name

Area 1

Area 2

Area 3

Area 4

Plan Settings

+ Add

No.	Execution Date	Start Time	End Time	Date	Mode	Operation
1	1970-01-01	00:00:00	23:59:59	Every Day	Weekly cycle	Delete

Table 4-107 Parameter/Button description

Parameter/ Button	Description
Enable illegal parking detection	Indicates whether to enable parking violation detection.
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.
Illegal parking trigger time(s)	Vehicle parking duration threshold.
Alarm Detection Interval(s)	Interval at which alarms are checked.
Area	Button for adding a detection area. A maximum of four detection areas can be drawn.
Delete	Button for deleting a selected detection area.

Step 4 Click **Save**.**----End**

Verification

For details about how to view the latest or historical alarms, see [4.12.1 Video Alarm](#).

4.11 Third-Party Algorithms

Scenario

When detecting an alarm event using a third-party algorithm, a camera reports the alarm to the main device and related alarm messages are displayed on the iClient S100.

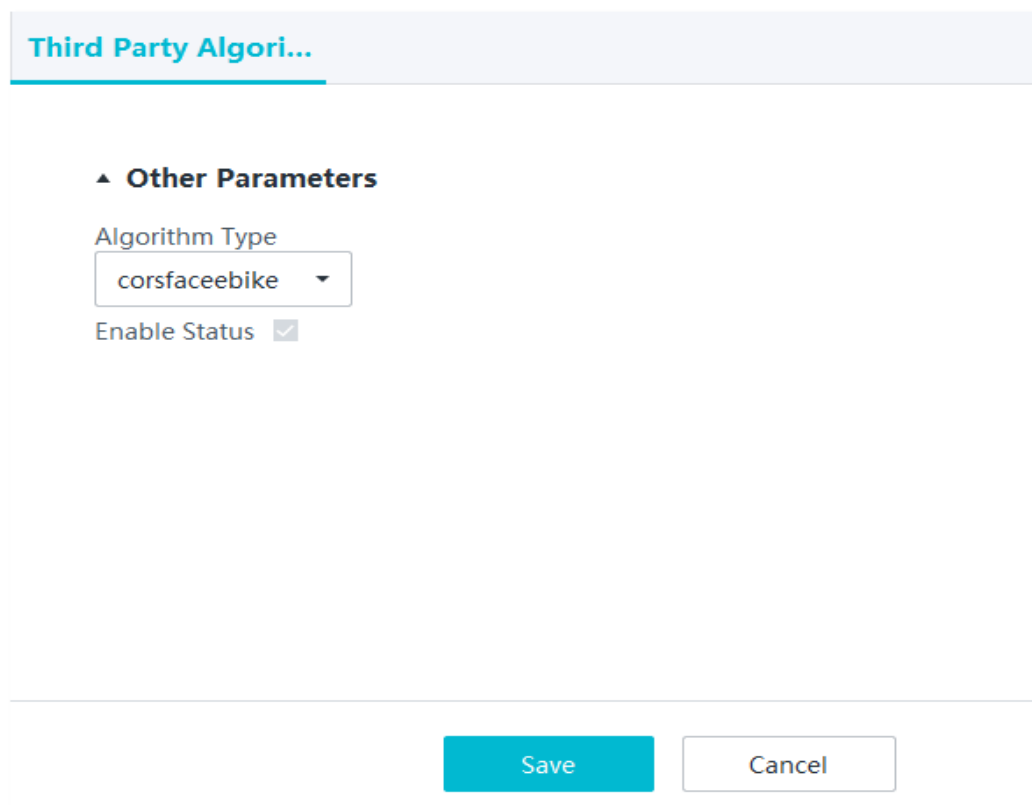
Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0282941126.xml.

Prerequisites

You have downloaded a third-party algorithm and installed and configured the third-party algorithm on the Dxxxx-10-SIU camera. For details about how to download a third-party algorithm, see the camera product documentation.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to an NVR800 and choose **Third-Party Algorithm > Third Party Algorithm**.
- Step 3** Choose a desired algorithm type in the shortcut menu. You can check the algorithm status (enabled or disabled) by checking whether **Enable Status** is selected, as shown in [Figure 4-135](#). If **Enable Status** is selected, the algorithm is enabled. If **Enable Status** is deselected, the algorithm is disabled.

Figure 4-135 Third Party Algorithm page

Third Party Algori...

▲ **Other Parameters**

Algorithm Type
corsfaceebike ▼

Enable Status ☒

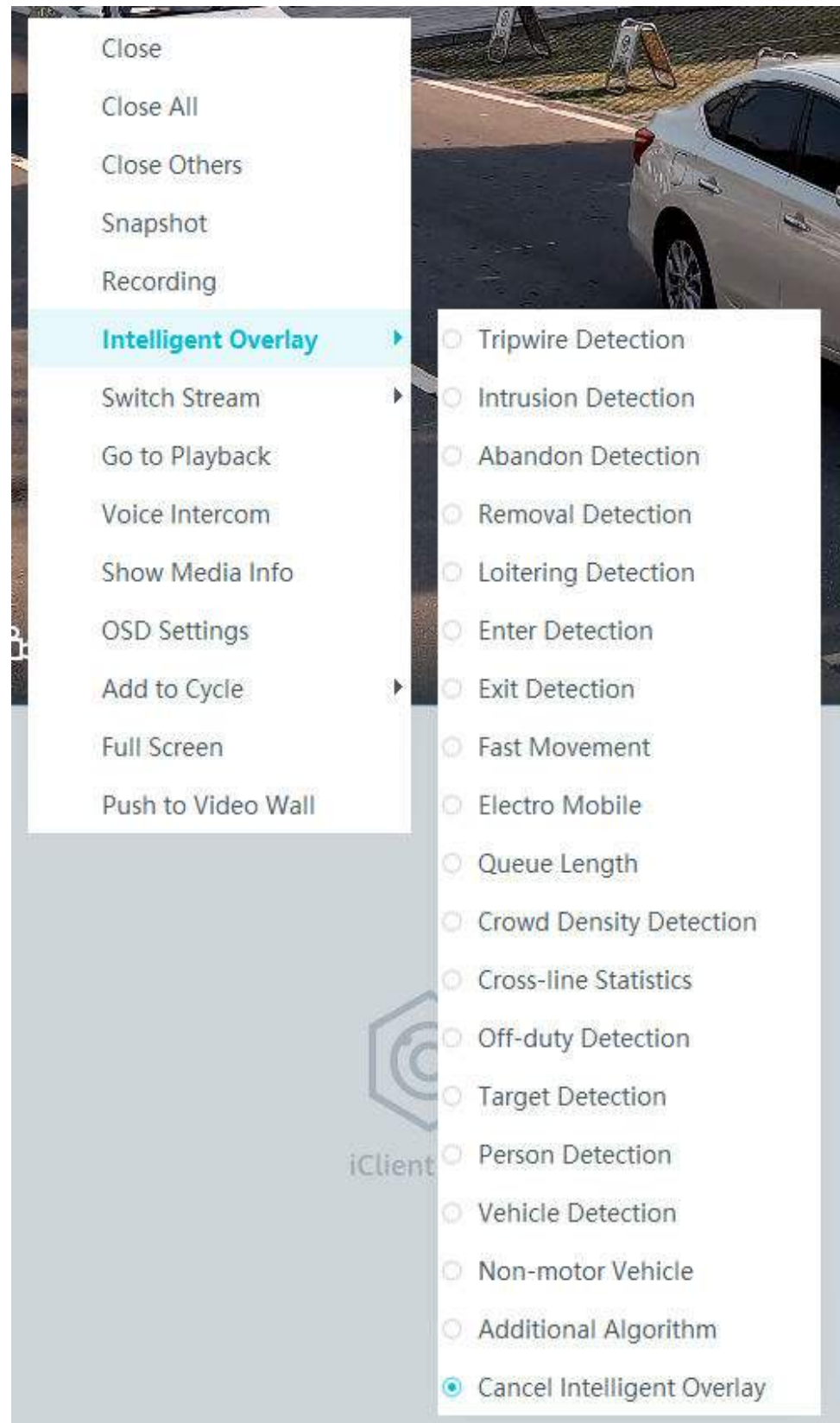
Save Cancel

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 4-136](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 4-136 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

4.12 Alarm Management

4.12.1 Video Alarm

This section describes how to view information about alarms generated by alarm linkage actions and intelligent analysis services on the iClient S100. [Table 4-108](#) describes detailed video alarms.

Table 4-108 Alarm parent types and subtypes

Parameter		Function
Latest Alarm		Displays the latest alarms of each service. On this page, alarms are displayed and updated in real time. The alarm subtypes of the latest alarms are the same as those of historical ones.
Target Alert Alarm	• Target recognition alarm • Target detection alarm • Mask detection alarm • Person detection alarm • Appearance frequency alarm (provided by the NVR800)	Displays the historical alarms of each service.
Vehicle Alert Alarm	• Vehicle recognition alarm (for motor vehicles only) • Vehicle detection alarm (for motor vehicles only) • Parking violation alarm (for motor vehicles only) • Non-motorized vehicle detection alarm	

Parameter		Function
Behavior Analysis Alarm	• Tripwire crossing detection alarm • Intrusion detection alarm • Abandoned object detection alarm • Removed object detection alarm • Loitering detection alarm • Area entry detection alarm • Area exit detection alarm • Fast movement detection alarm • Fire detection alarm • Electric bike detection alarm	
Common Business Alarm	• Motion detection alarm • Lens blocking alarm • Sudden volume increase alarm • Sudden volume decrease alarm • Video loss alarm • Micro Edge I/O alarm • Boolean value alarm	
Situation Analysis Alarm	• Human counting alarm • Queue length alarm • Crowd density alarm • Crowd gathering alarm • Off-duty detection alarm	

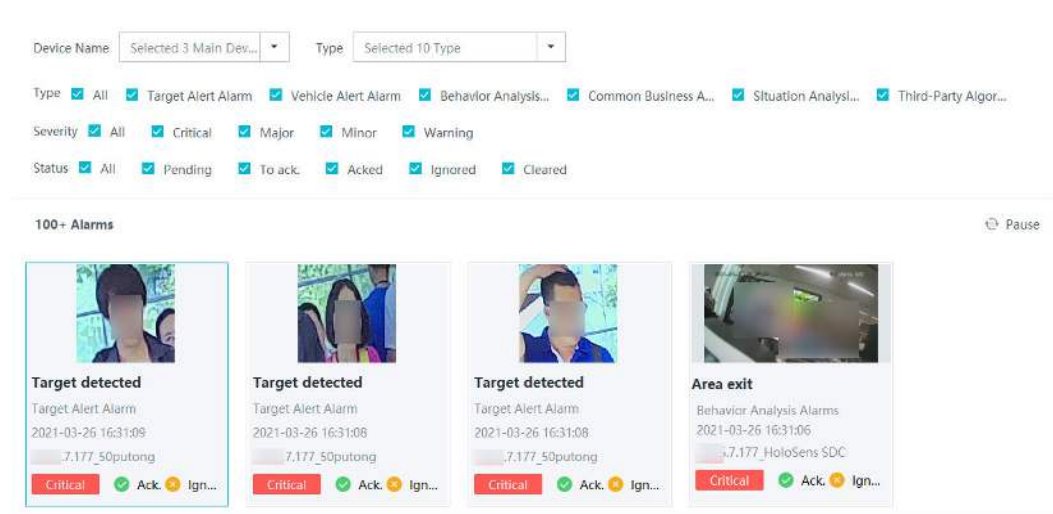
Parameter	Function
Additional Algorithm Alarm	

4.12.1.1 Latest Alarms

On the **Latest Alarm** page, you can view up to 100 latest alarms, which are updated in real time.

- Step 1** On the iClient S100 home page, choose **Complex Applications > Video Alarm > Latest Alarm**. The page shown in [Figure 4-137](#) is displayed.

Figure 4-137 Latest Alarm

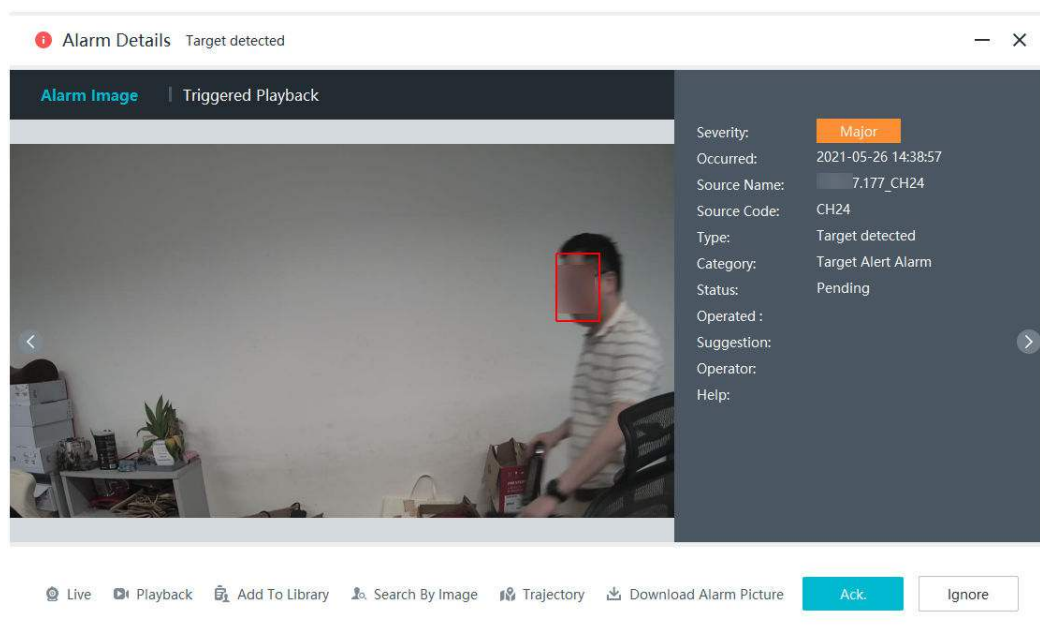


- Step 2** Select one or more main devices from the **Device Name** drop-down list as required. Then, select desired alarms subtypes from the **Type** drop-down list box as required, and all alarms of these subtypes reported by the selected main devices are automatically displayed on the page.

- Step 3** To view alarms of specified types, filter out the alarms by criteria such as the alarm type, alarm severity, and alarm status.

Alarms in the row of **Type** are of parent types. [Table 4-108](#) describes instances of alarms of parent types.

- Step 4** Click an alarm. The **Alarm Details** page is displayed, as shown in [Figure 4-138](#). [Table 4-109](#) describes the parameters on this page.

Figure 4-138 Alarm Details page**Table 4-109** Parameters/Buttons on the Alarm Details page

Type	Parameter/Button	Description
Alarm linkage	Triggered Snapshot/ Triggered Live/ Triggered Playback	Tab pages that display the results linked to the selected alarm if alarm linkage is configured for the camera.
Common functions	Live	Button for going to the Live page where you can view live video from the camera that generates the alarm.
	Playback	Button for going to the Playback page where you can play back the recording generated when the alarm is triggered.
	Downloading Alarm Picture	Button for downloading snapshots taken when the alarm is triggered.
Functions related to target recognition alarms	Add To Library	Button for going to the Target List page where you can enter list information and add the target to the target list.
	Search By Image	Button for going to the Search By Image page where you can search for similar snapshots taken by the current camera.
	Trajectory	Button for going to the Map page where you can view target trajectories on the map.

Type	Parameter/Button	Description
Alarm handling	Ack./Ignore	Button for going to the page for entering handling suggestions.

----End

4.12.1.2 Historical Alarms

You can view desired types of historical alarms on the **Target Alert Alarm**, **Vehicle Alert Alarm**, **Behavior Analysis Alarm**, **Common Business Alarm**, **Situation Analysis Alarms**, and **Third-Party Algorithm Alarms** tab pages. [Table 4-108](#) describes the alarm parent types and subtypes as well as their mappings.

This section uses **Target Alert Alarm** as an example to describe how to view historical alarms generated through a target alert or mask detection task.

- Step 1** On the iClient S100 home page, choose **Complex Applications > Video Alarm > Target Alert Alarm**.
- Step 2** Set alarm search criteria. [Table 4-110](#) describes the parameters.

Table 4-110 Parameters, buttons, and icons on the Target Alert Alarm page

Parameter/ Button/Icon	Description
Cameras	Cameras from which alarms are to be searched for. You can select cameras connected multiple main devices of the same type.
Period	Time segment during which an alarm is generated.
Type	Alarm subtype supported by the selected cameras. Only available subtypes are automatically displayed in the drop-down list.
Severity	Importance and urgency of an alert task. The Severity parameter corresponds to Alert Level of an alert task.
Search	Button for searching for alarms based on the specified criteria.
Reset	Button for restoring to initial search criteria.
All	Selects all alarms on the current page by one click.

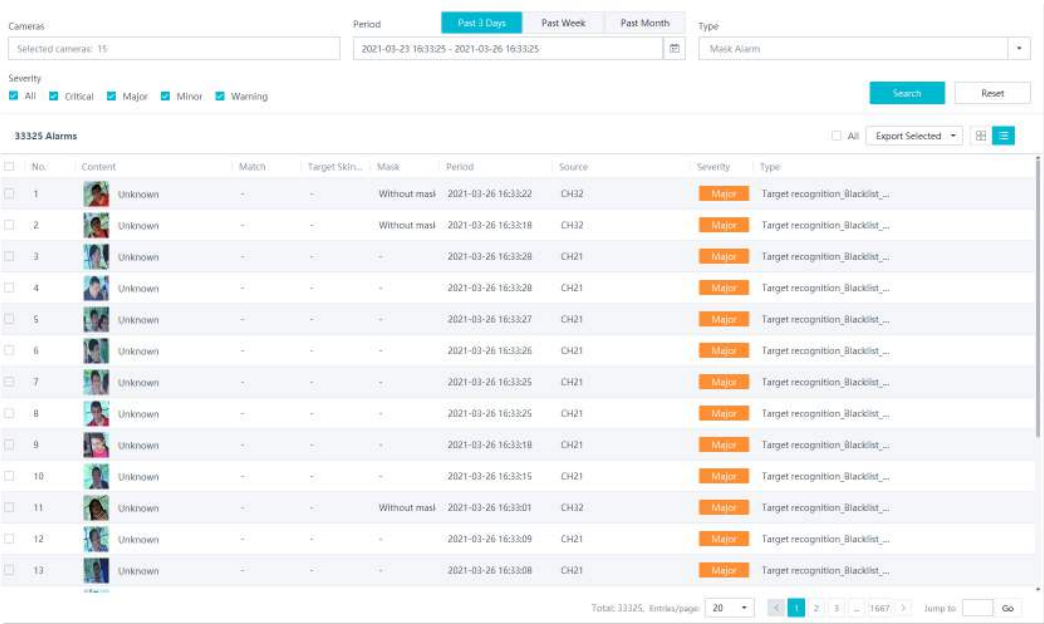
Parameter/ Button/Icon	Description	
Export Selected	Exports the selected alarms to the local computer in an Excel file.	NOTE You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files. The password must meet the following requirements: • Contains 10 to 16 characters. • Contains at least two types of the following: lowercase letters, uppercase letters, digits, and special characters. • Must be different from the user name or user name spelled backwards. • Cannot contain space characters or Chinese characters. • Cannot be a weak password.
Export This Page	Exports the alarms on the current page to the local computer in an Excel file.	
Export All	Exports all alarms in the search result to the local computer in an Excel file.	
	Switches the tile or list display mode of the alarm search result.	

NOTE

- All export and import functions can be used only in the following environments:
 - The WPS Office software is used by default.
 - The Microsoft Office software (later than Microsoft Office 2007) is installed properly. The legal license is activated and can run properly.
- You are advised to use professional video or image editing tools to shield irrelevant persons in downloaded or exported video or images and meet the HD requirements of the data subject. The recommended procedure is as follows:
 1. Download the required video to the local computer and decompress it to common video or export image data to the local computer.
 2. Use a video or an image editing tool to anonymize irrelevant targets and only retain the HD part of the data subject.
 3. Export the anonymized video or images to meet the data transfer requirements of the data subject.
 4. To ensure personal information security, delete the downloaded or exported images and recordings in a timely manner.

Step 3 Click **Search**. The search result is displayed, as shown in [Figure 4-139](#).

Figure 4-139 Target alert alarms



Step 4 Click an alarm. The **Alarm Details** page is displayed, as shown in [Figure 4-140](#). [Table 4-111](#) describes the parameters on this page.

Figure 4-140 Alarm Details page

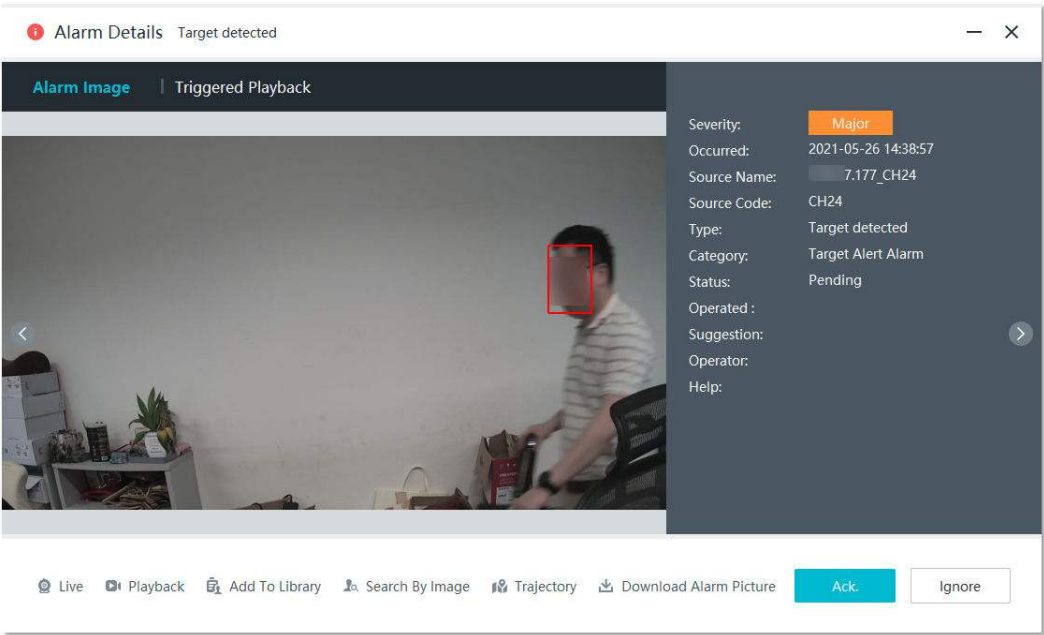


Table 4-111 Parameters/Buttons on the Alarm Details page

Type	Parameter/Button	Description
Alarm linkage	Triggered Snapshot/ Triggered Live/ Triggered Playback	Tab pages that display the results linked to the selected alarm if alarm linkage is configured for the camera.

Type	Parameter/Button	Description
Common functions	Live	Button for going to the Live page where you can view live video from the camera that generates the alarm.
	Playback	Button for going to the Playback page where you can play back the recording generated when the alarm is triggered.
	Downloading Alarm Picture	Button for downloading snapshots taken when the alarm is triggered.
Functions related to target recognition alarms	Add To Library	Button for going to the Target List page where you can enter list information and add the target to the target list.
	Search By Image	Button for going to the Search By Image page where you can search for similar snapshots taken by the current camera.
	Trajectory	Button for going to the Map page where you can view target trajectories on the map.
Alarm handling	Ack./Ignore	Button for going to the page for entering handling suggestions.

----End

4.12.2 Alarm Linkage

4.12.2.1 Application Scenario

This section describes how to configure an alarm linkage policy. After an alarm linkage policy is configured, the NVR800 performs preset linkage actions when an alarm is generated. This ensures timely alarm handling. The typical application scenario is as follows.

Some key areas raise high security requirements, and 7/24 manual detection will bring high costs. To solve this problem, the alarm linkage feature is introduced.

4.12.2.2 Configuring an Alarm Linkage Policy

Prerequisites

Alarm types such as tripwire crossing detection and intrusion detection have been configured. For details, see the links in [Table 4-112](#).

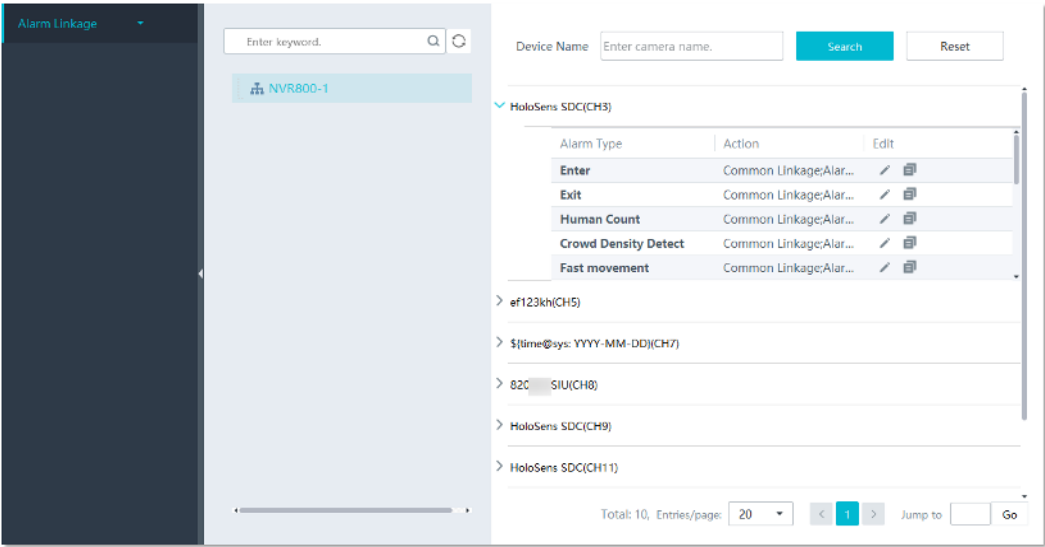
Table 4-112 Functions that support alarm linkage

Category	Subcategory
Common intelligence	4.5.1 Motion Detection
	4.5.2 Lens Blocking Detection
	4.5.3 Audio Diagnosis
Behavior analysis	4.6.4 Tripwire Crossing Detection
	4.6.5 Intrusion Detection
	4.6.8 Loitering Detection
	4.6.9 Area Entry Detection
	4.6.10 Area Exit Detection
	4.6.11 Fast Movement Detection
Crowd flow analysis	4.9.1 Head Counting
	4.9.2 Queue Length Detection
	4.9.3 Crowd Density Detection
Target intelligence	Mask detection
Vehicle intelligence	Parking violation detection
Third-party algorithm	4.11 Third-Party Algorithms

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an NVR800 and choose **Alarm Management > Alarm Linkage**.
- Step 3** Click **Camera List**, select an alarm device, and click . The page shown in [Figure 4-141](#) is displayed.

Figure 4-141 Selecting an alarm device



- Step 4** Set the alarm type, for example, **Intrusion**. Then, click  to enter the editing page.
- Step 5** Configure a policy for the alarm linkage actions, as shown in [Figure 4-142](#). [Table 4-113](#) describes the parameters for configuring a policy.

Figure 4-142 Configuring an alarm linkage policy

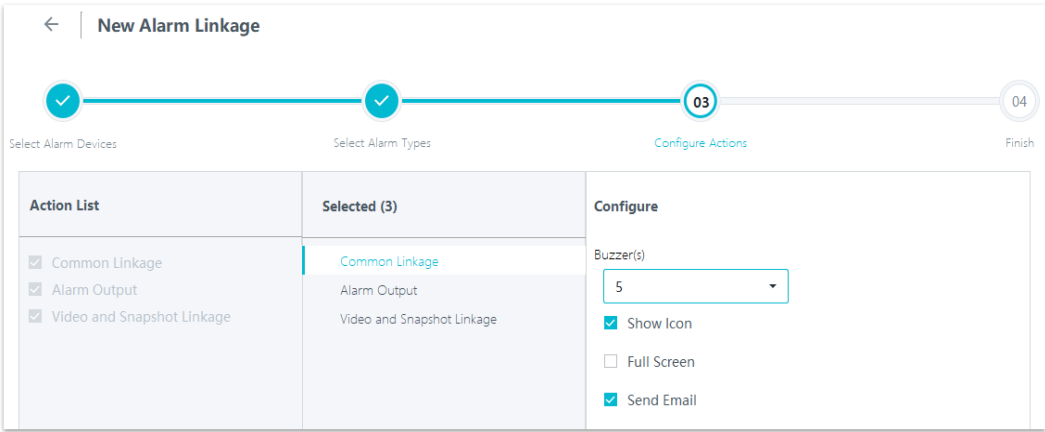


Table 4-113 Parameters for configuring an alarm linkage policy

Alarm Linkage Action	Parameter	Description
Common Linkage	Buzzer(s)	Alarm duration of the buzzer. The default value is 0.
	Show Icon	Indicates whether to display the status icon of the camera that triggers an alarm.

Alarm Linkage Action	Parameter	Description
	Full Screen	Indicates whether to play live video from the camera that triggers an alarm in full screen mode.
	Send Email	Indicates whether to send an email to a specified email address when an alarm is generated.
Alarm Output	Alarm Output	I/O alarm output device.
	Output Delay(s)	Output delay. The default value is 10 .
Video and Snapshot Linkage	Recording	Indicates whether to record video when an alarm is generated.
	Recording Channel	Recording channel.
	Recording Delay(s)	Recording duration. The default value is 30 .
	Snapshot	Indicates whether to take snapshots when an alarm is generated.

NOTE

By default, all linkage actions are selected. Configure a policy for each action and click **Next**.

Step 6 Click **Finish**.

Step 7 (Optional) To configure an alarm linkage policy for multiple cameras, click  in the **Edit** column. On the **Copy Parameters** page that is displayed, set **Parameter Type** and **Target Channel** and click **OK** to apply the settings of the current alarm linkage policy to other cameras in batches, as shown in [Figure 4-143](#).

Figure 4-143 Copy Parameters

Copy Parameters

Source Channel: HoloSens SDC(CH3)

Parameter Type:

- ☒ All
- ☒ Buzzer
- ☒ Send Email
- ☒ Recording
- ☒ Snapshot
- ☒ Show Icon
- ☒ Alarm Output
- ☒ Recording Channel
- ☒ Full Screen
- ☒ Output Delay
- ☒ Recording Delay

Target Channel: All

OK Cancel

----End

4.12.2.3 Verification

When an alarm (such as intrusion, tripwire crossing, and loitering detection alarms) is generated, the system links the camera to take snapshots and record video. You can view the alarm information on the iClient S100 client.

Procedure

- Step 1** Choose **Complex Applications > Video Alarm** on the iClient S100 home page.
- Step 2** Click a required alarm tab of the corresponding service. [Table 4-114](#) describes the parameters.

Table 4-114 Alarm parent types and subtypes

Parameter	Function
Latest Alarm	Displays the latest alarms of each service. On this page, alarms are displayed and updated in real time. The alarm subtypes of the latest alarms are the same as those of historical ones.

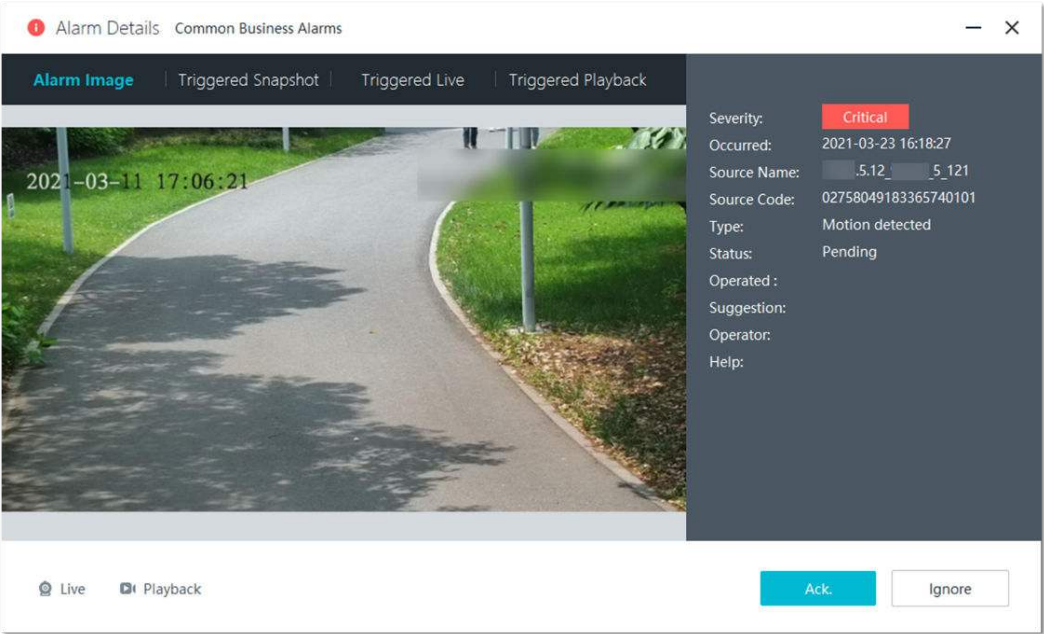
Parameter		Function
Target Alert Alarm	• Target recognition alarm • Target detection alarm • Mask detection alarm • Person detection alarm • Appearance frequency alarm (provided by the NVR800)	Displays the historical alarms of each service.
Vehicle Alert Alarm	• Vehicle recognition alarm (for motor vehicles only) • Vehicle detection alarm (for motor vehicles only) • Parking violation alarm (for motor vehicles only) • Non-motorized vehicle detection alarm	
Behavior Analysis Alarm	• Tripwire crossing detection alarm • Intrusion detection alarm • Abandoned object detection alarm • Removed object detection alarm • Loitering detection alarm • Area entry detection alarm • Area exit detection alarm • Fast movement detection alarm • Fire detection alarm • Electric bike detection alarm	

Parameter		Function
Common Business Alarm	• Motion detection alarm • Lens blocking alarm • Sudden volume increase alarm • Sudden volume decrease alarm • Video loss alarm • Micro Edge I/O alarm • Boolean value alarm	
Situation Analysis Alarm	• Human counting alarm • Queue length alarm • Crowd density alarm • Crowd gathering alarm • Off-duty detection alarm	
Additional Algorithm Alarm		

Step 3 Select the device to be queried, set alarm search criteria, and click **Search**. The found alarms are displayed in the alarm list.

Step 4 Click an alarm in the search result. The alarm details are displayed. You can view information on tab pages such as **Triggered Live** and **Triggered Playback**, and click **Ack.** or **Ignore** for alarm information as required, as shown in [Figure 4-144](#).

Figure 4-144 Alarm Details



----End

4.12.3 Alarm Parameter Settings

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Personal Settings**.
- Step 2** Set alarm parameters, as shown in [Figure 4-145](#). [Table 4-115](#) describes the parameters.

Figure 4-145 Alarm Settings page

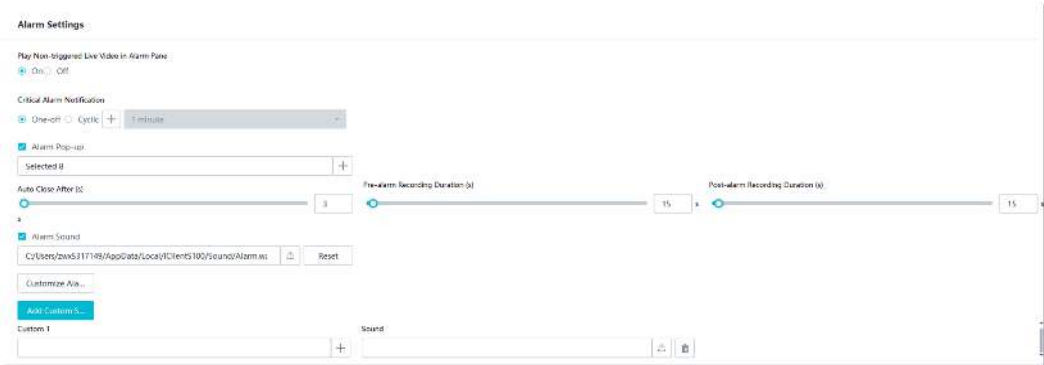


Table 4-115 Parameter description

Parameter	Description
Play Non-triggered Live Video in Alarm Pane	Indicates whether an alarm pane can play common live video. The options are as follows: • On: yes • Off: no
Auto Close After (s)	Display duration of a service or an NMS alarm notification.
Pre-alarm Recording Duration (s)	Video recording duration before an alarm is generated if the video recording linkage action is configured.
Post-alarm Recording Duration (s)	Video recording duration after an alarm is generated if the video recording linkage action is configured.
Critical Alarm Notification	You can select an alarm type as a critical alarm. When an alarm is generated, an alarm dialog box is displayed. Critical alarms are notified at the following intervals: • One-off • Cyclic notification. The interval can be set to 1 minute, 5 minutes, or 10 minutes. To set cyclic notification of critical alarms, perform the following steps: 1. Click . 2. Select Select alarm types and select an alarm type from the drop-down list box. 3. Click OK.
Alarm Pop-up	When the client receives any alarm of a specified type or severity, it displays the alarm. To enable this function, perform the following operations: 1. Select Alarm Pop-up. 2. Set Select alarm types or Select alarm severity in the dialog box. 3. Click OK. NOTE Optional operations: - Click  in the lower right corner of an alarm pop-up. Alarms will not pop up within 30 minutes. -

Parameter	Description
Alarm Sound	Audio file played when the client detects a service alarm. By default, this function is disabled. You can click  and select an audio file stored in a local directory. NOTE • Only audio files in .wav format are supported. • Click Reset to restore the system's default alarm sound. The default audio file is Alarm.wav.
Customize Alarm Sound	Click the button to add custom sounds for different alarm types. Before setting this parameter, select Alarm Sound. You can click Add Custom Sound, click Select Alarm Type, select different alarm types, and click OK. You can add different custom sounds for multiple alarm types.

Step 3 Click **Save**.

----End

5 Video Service Management (for IVS1800)

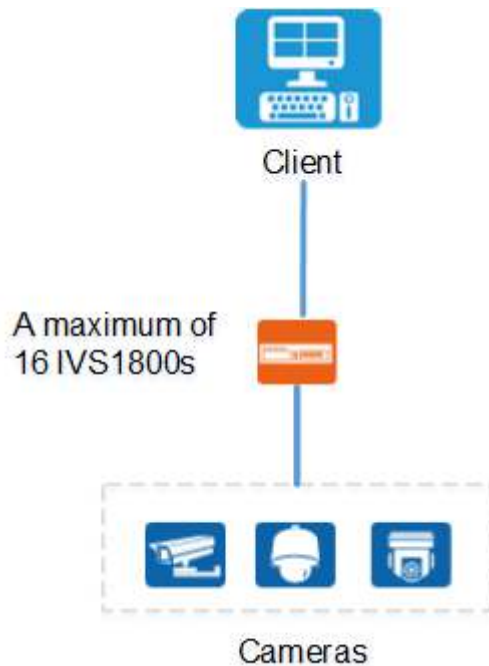
- 5.1 Device Access
- 5.2 Video Viewing
- 5.3 Recording
- 5.4 Video Wall
- 5.5 Common Intelligence
- 5.6 Behavior Analysis
- 5.7 Target Intelligence
- 5.8 Person Intelligence
- 5.9 Situation Analysis
- 5.10 Intelligent Vehicle Analysis
- 5.11 Third-Party Algorithms
- 5.12 Alarm Management
- 5.13 Media Transmission

5.1 Device Access

5.1.1 Application Scenario

This section describes how to connect multiple IVS1800s to the client and how to connect cameras to the IVS1800 so that the client can centrally manage the connected devices, for example, viewing live video and recordings from the cameras.

Figure 5-1 shows the camera access scenario. **Table 5-1** describes the access modes and protocols supported by cameras.

Figure 5-1 Camera access scenarios**NOTE**

- A camera can be connected to an IVS1800 on the iClient S100 client only through HWSDK in passive registration. That is, the IVS1800 proactively initiates an access request to the camera. After receiving the request, the camera connects to the IVS1800.
- You are advised to connect cameras to an IVS1800 through HWSDK for enabling functions such as lens blocking detection, motion detection, and behavior analysis, which are unavailable if the cameras are connected through ONVIF.
- To switch to the OMU portal of the IVS1800 on the iClient S100, perform the following operations:
Choose **Maintenance Management > Video Device > Device List > Main Devices**, right-click an IVS1800, and choose **Maintenance**.

Table 5-1 Access modes

Access Mode	Application Scenario	Supported Protocol
Automatically adding devices in batches (recommended)	If a large number of online cameras that support HWSDK or ONVIF need to connect to the IVS1800, you can use this method to quickly add the cameras. In this mode, only online cameras can be automatically added in batches, and the camera IP addresses do not need to be specified. This mode applies to scenarios where a large number of cameras need to be added. Compared with the mode of manually adding cameras in batches, this mode enables faster adding of cameras except offline cameras, and supports fewer camera protocols.	HWSDK and ONVIF
Manually adding cameras in batches	If IP addresses have been planned for a large number of cameras and the cameras need to be connected to the IVS1800, you can manually add the cameras in batches. In this mode, both online and offline cameras can be added, but the IP address of each camera must be specified.	HWSDK, ONVIF, and GB/T 28181
Manually adding cameras one by one	If only a few cameras need to be connected to the IVS1800, you can add the cameras one by one. In this mode, both online and offline cameras can be added, but the IP address of each camera must be specified.	HWSDK, ONVIF, GB/T 28181, and DHSDK

5.1.2 Device Connection

5.1.2.1 Adding IVS1800s

You can add a maximum of 16 IVS1800s and connect a maximum of 1024 video channels (including the video channels connected to the IVS1800s) to an iClient S100 server. This section describes the procedure for adding IVS1800s to an IVS1800.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** On the page that is displayed, click **Add** in the upper left corner and choose **Manual**. The page for adding a device is displayed, as shown in [Figure 5-2](#). [Table 5-2](#) describes the parameters.

Figure 5-2 Adding an IVS1800

The screenshot shows a 'New Device' dialog box with a close button (X) in the top right corner. The dialog contains several input fields: 'Device Type' is a dropdown menu with 'IVS1800' selected; 'Name' is a text box with 'IVS1800'; 'Address' is a text box with '192.168.1.10'; 'Port' is a text box with '18531'; 'User Name' is a text box with 'admin'; and 'Password' is a masked text box with 10 dots and toggle icons (X and eye) on the right. At the bottom are 'OK' and 'Cancel' buttons.

Table 5-2 Parameters for adding an IVS1800

Parameter	Description
Device Type	Type of the device to be added. Select IVS1800 from the drop-down list box.
Name	User-defined device name.
Address	IP address of the device to be added. The address is in xxx.xxx.xxx.xxx format, for example, 192.168.6.5 .

Parameter	Description
Port	Port number of the device to be added. The default port number is 18531 .
User Name	- The default user name is admin and the password is set by the user. When you log in to the IVS1800 for the first time, the system displays the page for changing the password. - Customized users need to log in to the OMU portal to change the initial password after configuring an IVS1800. Otherwise, the iClient S100 client will fail to connect to the IVS1800. - After an IVS1800 is connected to the iClient S100, if its password is changed on the IVS1800, it goes offline on the iClient S100. In this case, you can update the password of the IVS1800 on the iClient S100 and it will go online again. NOTE - If a customized user name is used, configure the user by referring to 8.1.3.1 Configuring a User Role. - To ensure that the algorithm management and algorithm store functions can be used properly, set the user role to Administrator (ISV) or O&M administrator (man-machine). - Multiple users can log in to the IVS1800 using the same account from different computers. Therefore, to ensure that functions such as system maintenance (directly opening the OMU portal on the iClient S100) can be used properly, increase the number of allowed logins to the IVS1800 using the same account as required.
Password	

Step 3 The user name and password of iClient S100 can be automatically searched and input to the same subnet as that of iClient S100. If the user names and passwords of multiple devices are consistent, batch verification can be carried out. As shown in the figure, automatic access to IVS1800.

Figure 5-3

Automatically Found Device(s)

Tip: the iClient S100 server must be in the same subnet as the searched device, and ensure that ports 9133 and 32902 of the iClient S100 server is not blocked by the firewall. It's recommended to close the firewall. To activate the device in batches, the default user name is admin, no need to configure the user name, just enter the password to activate.

User Name: Password:

Current progress 100% Search! Again

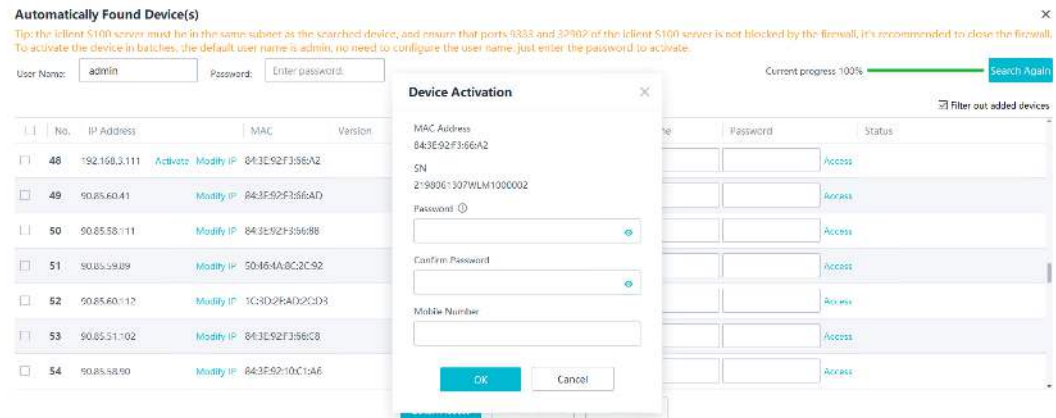
☒ Filter out added devices

No.	IP Address	MAC	Version	Device ...	Device Name	Port	User Name	Password	Status
48	192.168.3.111	843E92F366A2		IVS-B	192.168.3.111	18531	admin		Access
49	90.85.60.41	843E92F366AD		IVS-B	90.85.60.41	18531	admin		Access
50	90.85.58.111	843E92F36688		IVS-B	90.85.58.111	18531	admin		Access
51	90.85.59.89	50464A8C2C92		IVS-B	90.85.59.89	18531	admin		Access
52	90.85.60.112	1C3D2FAD2CD3		IVS-B	90.85.60.112	18531	admin		Access
53	90.85.51.102	843E92F366C8		IVS-B	90.85.51.102	18531	admin		Access
54	90.85.58.90	843E9218C1A6		IVS-B	90.85.58.90	18531	admin		Access

Batch Access Batch Activate Cancel

Step 4 If the IVS1800 is a new and inactive device, click the activate button on the searched device list to activate the device.

Figure 5-4



Step 5 If you need to modify the IP of IVS1800 equipment, you can click the modify IP button to modify the IP.

Figure 5-5

Modify IP-related Parameters ✕

Tip: After modifying the IP successfully, it will take effect in about 2 minutes.

Destination MAC Address
84:3E:92:F3:66:A2

SN
2198061307WLM1000002

Destination IP Address

Subnet Mask

Gateway Address

DNS 1

DNS 2

Step 6 Click **OK**.

----End

5.1.2.2 Adding Cameras on the IVS1800

5.1.2.2.1 Automatically Adding Cameras in Batches (Recommended)

You are advised to use this access mode to fast add cameras which can connect to the IVS1800 through HWSDK or ONVIF.

Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Select a desired IVS1800 to which the cameras to be added are mounted and click **Add** in the upper right corner of the page. Alternatively, right-click the IVS1800 and choose **Camera Access** from the shortcut menu. The **Camera Access** tab page is displayed.

Step 3 Select **Auto Batch Access (Recommended)** and click **Start**.

Step 4 Search for cameras by IP address.

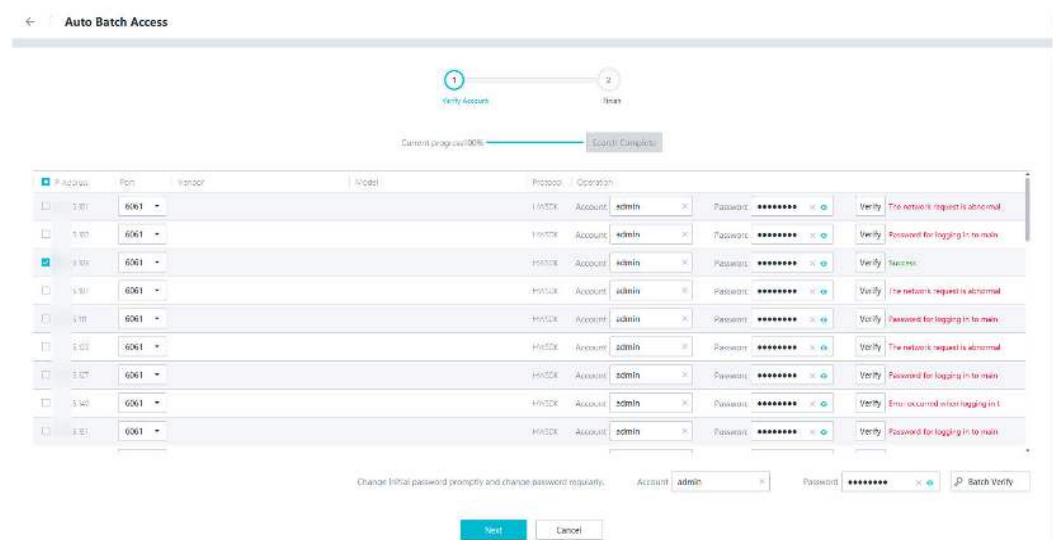
1. Select the driver supported by the device, that is, the protocol for connecting cameras (HWSDK or ONVIF, with HWSDK recommended).
2. Click **Add Network Segment** and enter the start and end IP addresses of cameras.

NOTE

- It is recommended that you specify a proper network segment to shorten the search time.
 - If a network segment is set, the system searches this network segment for cameras in unicast mode. You can set multiple network segments so that you can search multiple VLANs for cameras.
 - If you do not set a network segment, the system searches for cameras in broadcast mode. In this case, the system can only search for cameras located on the same network segment as the IP address of the local server. You are advised to search for cameras by network segment or add cameras in batches.
3. Click **Next** to search for cameras.
 4. (Optional) Click **Stop** to stop the search.

Step 5 You can use **IP Address** and **Vendor** to search for required cameras. Alternatively, you can directly select the required cameras in the camera list. Then verify accounts, as shown in [Figure 5-6](#).

Figure 5-6 Verifying accounts



Auto Batch Access

1 Verify Account 2 Finish

Current progress: 90% Search Complete

☐	IP Address	Port	Vendor	Model	Protocol	Operation	Account	Password	Verify	Message
☐	1.181	8081			HWSDK	Account	admin	*****	Verify	The network request is abnormal.
☐	1.181	8081			HWSDK	Account	admin	*****	Verify	Password for logging in is invalid.
☒	1.181	8081			HWSDK	Account	admin	*****	Verify	Success.
☐	1.181	8081			HWSDK	Account	admin	*****	Verify	The network request is abnormal.
☐	1.181	8081			HWSDK	Account	admin	*****	Verify	Password for logging in is invalid.
☐	1.181	8081			HWSDK	Account	admin	*****	Verify	The network request is abnormal.
☐	1.181	8081			HWSDK	Account	admin	*****	Verify	Password for logging in is invalid.
☐	1.181	8081			HWSDK	Account	admin	*****	Verify	Error occurred when logging in.
☐	1.181	8081			HWSDK	Account	admin	*****	Verify	Password for logging in is invalid.

Change initial password promptly and change password regularly. Account: admin Password: ***** Search Verify

Next Cancel

Table 5-3 Parameter description

Parameter	Description
Port	Port number of the camera to be added. If HWSDK is used to add cameras, the default port number is 6061 . If ONVIF is used to add cameras, the default port number is 80 . If all cameras to be added have the same port number, you can set the port number for one camera and click Apply to Others .
Account/Password	Registration user name and password used to connect the camera to the IVS1800. If all cameras to be added share the same registration user name and password, you can use the batch verification function.

NOTE

- Port number:

If you add a camera through ONVIF, you do not need to change the port number. If you add a camera through HWSDK, you are advised to set the port number to **6061**. In this case, messages are encrypted after the camera is added, improving transmission security.

- Registration user name and password of a camera:

If the registration password of a camera is changed, do not consecutively click **Verify**. If you click **Verify** for five or more consecutive times, the iClient S100 server will be locked. If the iClient S100 server is locked, you cannot add the camera again until the iClient S100 server is unlocked or the camera is restarted.

Step 6 Select the cameras to be added and click **Next**. The operation result is displayed, as shown in [Figure 5-7](#).

Figure 5-7 Camera adding result

IP Address	Camera	Driver	Vendor	Server	Result
7.10	7.10CH0	HWSDK			Successful
7.10	7.10CH1	HWSDK			Successful
7.19	7.19CH0	HWSDK			Successful
7.20	7.20CH0	HWSDK			Successful
7.20	7.21CH0	HWSDK			Successful
7.21	7.21CH0	HWSDK			Successful
7.25	7.25CH1	HWSDK			Successful
7.27	7.27CH1	HWSDK			Successful
7.29	7.29CH0	HWSDK			Successful
7.29	7.29CH1	HWSDK			Successful
7.29	7.29CH2	HWSDK			Successful

Step 7 Click **Finish**.

Step 8 Perform follow-up configurations listed in [Table 5-4](#).

Table 5-4 Follow-up configurations

Scenario	Where to Configure	Configuration
Adding cameras through ONVIF	Camera web system	Set connection parameters. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0283035578.xml.
Adding cameras to a group	Maintenance Management > Video Device > Group Device	Add cameras to a group to facilitate camera management.
Adjust Area	Maintenance Management > Video Device > Device List	Select one or multiple cameras and  Adjust Area to adjust the area to which the cameras belong on the Main Device or Camera tab page.

----End

5.1.2.2.2 Manually Adding Devices in Batches

This section describes how to manually add cameras in batches on the iClient S100 client.

Procedure

Before adding cameras in batches, you need to complete a system-provided template based on actual requirements. After importing the completed template, you can add cameras in batches on the device management page.

 NOTE

- The number of cameras to be added in batches using a template cannot exceed the maximum number of cameras supported by an IVS1800. Otherwise, the excess cameras will fail to be added.
- To import primary cameras in the 1 + N solutions by using a template, perform the following steps:

Specify the model for each primary camera in the template. The system reserves 1 + N channels for each of them. After the batch import is completed, the number of occupied channels equals the number of reported channels of online primary cameras plus the number of channels reserved for offline primary cameras.

If the number of secondary cameras connected to a primary camera is less than the threshold N, free channels will be available after these cameras go online. Then you can import more other cameras in batches.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Select a desired IVS1800 to which the cameras to be added are mounted and click **Add** in the upper right corner of the page. Alternatively, right-click the IVS1800 and choose **Camera Access** from the shortcut menu.

Step 3 Select **Manual Batch Access** and click **Start**.

Step 4 Click **Download Template** to download the **Device Batch Import.xlsx** file to the local computer.

Step 5 Open the **Device Batch Import.xlsx** file and fill in the corresponding sheets in the file by referring to [Table 5-5](#) and [Table 5-6](#).

 NOTE

In [Table 5-5](#), **M** indicates mandatory, **O** indicates optional, and **-** indicates not required or involved.

Table 5-5 Parameters in the batch import template

Parameter	HWSDK (Recommended)	ONVIF	T28181
Device Name	M	M	M
Vendor	M	O	-
Device Form Type	M	M	M
Device Model	O	O	-
Main Device Code	M	M	M
-	-	-	M
IP	M	M	-
Port	M	M	-
User Name	M	M	-
Password	M	M	M

Table 5-6 Parameters in the template for manually adding cameras in batches

Parameter	Setting
Device Name	Camera name to be displayed on the iClient S100. You are advised to enter the camera installation location or observation area.
Vendor	Camera vendor.
Device Form Type	Type of the main camera. Set this parameter to IPC .
Device Model	Actual camera model.
Main Device Code	Obtain the main device code of the current domain from the first sheet in the template.
IP	IP address of a camera.
Port	Number of the port for camera access, whose value must be the same as that set on the camera side. You are advised to use the default port number. If the port number is changed on the camera side, set this parameter based on the site requirements. NOTICE • If the HWSDK protocol is used for registration, set the port number to 6061. Messages are encrypted after the camera is added, improving transmission security. • If you change the port number after a camera is connected, the camera will be disconnected and reconnected within 1–5s. The reconnection duration depends on the network conditions.
Username/Password	Registration user name and password used for camera access. For cameras, the navigation path of the registration password on the camera web page varies depending on the protocol. • HWSDK protocol: Choose Settings > Network > Platform Connection > Password Management. On the SDK Password tab page, the value of Current password is the registration password. • ONVIF protocol: Choose Settings > Network > Platform Connection > Password Management. On the ONVIF Password tab page, the value of Current password is the registration password.

Step 6 Import the completed template file to the iClient S100. You can click **Browse** and select the file, or drag the file from the local path to the **Drag file here.** area on the **Manual Batch Access** page.

Cameras to be added are displayed on different tab pages based on their protocols.

Step 7 Click **Next**. The camera adding result is displayed.

Step 8 Click **Finish**.

Step 9 Perform follow-up configurations listed in [Table 5-7](#).

Table 5-7 Follow-up configurations

Scenario	Where to Configure	Configuration
Adding cameras through GB/T 28181	Camera web system	Set connection parameters. For details, see 5.1.2.3.1 Configuring Connection Through GB/T 28181 in the Camera Web System
Adding cameras through ONVIF	Camera web system	Set connection parameters. For details, see 5.1.2.3.2 Configuring Connection Through ONVIF in the Camera Web System .
Adding cameras to a group	Maintenance Management > Video Device > Group Device	Add cameras to a group to facilitate camera management.
Adjust Area	Maintenance Management > Video Device > Device List	Select one or multiple cameras and click  Adjust Area to adjust the area to which the cameras belong on the Main Device or Camera tab page.

----End

5.1.2.2.3 Manually Adding a Device

This section describes how to manually add a camera on the iClient S100 client.

Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Select a desired IVS1800 to which the cameras to be added are mounted and click **Add** in the upper right corner of the page. Alternatively, right-click the IVS1800 and choose **Camera Access** from the shortcut menu.

Step 3 Select **Manual Single Access** and click **Start**.

Step 4 Set the parameters for adding a camera. [Table 5-8](#) describes the parameters.

Table 5-8 Parameters for manually adding a camera

Parameter	Description
Device Name	Camera name to be displayed on the iClient S100. You are advised to enter the camera installation location or observation area.
Driver	Protocol through which the camera is connected. NOTE - Dahua cameras can be connected only through DHSDK. You can connect cameras 5 minutes after the required plug-in is installed. Otherwise, the camera cannot be connected. - You are advised to connect cameras to an IVS1800 through HWSDK for enabling functions such as lens blocking detection, motion detection, and behavior analysis, which are unavailable if the cameras are connected through ONVIF.
Area	Area to which the camera belongs. If no area is specified, the camera belongs to the default area. The value of Area has been configured under Basic Management > Basic Management > Area Settings on the iClient S100. (You can configure an area by referring to "How to Set Up an Area" under FAQs > Comprehensive Services > Basic Operations.) Only users granted permissions of an area can perform operations on devices in the current area.
Connection Code	This parameter can be set only when the device connects to the system through T28181. The value must be the same as the value of Device ID for cameras or SIP Authentication ID for Hikvision cameras. The eleventh to thirteenth digits must be 132. NOTE The connection code must be a 20-digit integer. Insufficient digits are padded with 0.
Enable RTSP	This parameter can be set only when the device connects to the system through DHSDK. After the RTSP stream obtaining function is enabled, live streams are directly transferred from cameras to the iClient S100 without being processed or forwarded by the MU, reducing the system pressure. To enable the RTSP stream obtaining function, you must set the same port (default port: 554) for the iClient S100 and the PU.

Parameter	Description
User Name/ Password	Registration user name and password used to connect the camera to the IVS1800. For cameras, the navigation path of the registration password on the camera web page varies depending on the protocol. • HWSDK protocol: Choose Settings > Network > Platform Connection > Password Management. On the SDK Password tab page, the value of Current password is the registration password. • ONVIF protocol: Choose Settings > Network > Platform Connection > Password Management. On the ONVIF Password tab page, the value of Current password is the registration password. • GB/T 28181: The registration password is the value of Password under Settings > Network > Platform Connection > Second Protocol Parameters > T28181.
IP Address	IP address of a camera.
Device Login Port	Number of the port for camera access, whose value must be the same as that set on the camera side. You are advised to use the default port number. If the port number is changed on the camera side, set this parameter based on the site requirements. NOTICE • If the HWSDK protocol is used for registration, set the port number to 6061. Messages are encrypted after the camera is added, improving transmission security. • If you change the port number after a camera is connected, the camera will be disconnected and reconnected within 1–5s. The reconnection duration depends on the network conditions.

Step 5 Click **Finish**.

Step 6 Perform follow-up configurations listed in [Table 5-9](#).

Table 5-9 Follow-up configurations

Scenario	Where to Configure	Configuration
Adding cameras through GB/T 28181	Camera web system	Set connection parameters. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268805500.xml
Adding cameras through ONVIF	Camera web system	Set connection parameters. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0283035578.xml.

Scenario	Where to Configure	Configuration
Adding cameras to a group	Maintenance Management > Video Device > Group Device	Add cameras to a group to facilitate camera management.
Adjust Area	Maintenance Management > Video Device > Device List	Select one or multiple cameras and click  Adjust Area to adjust the area to which the cameras belong on the Main Device or Camera tab page.

----End

5.1.2.3 Connecting Cameras to the IVS1800

5.1.2.3.1 Configuring Connection Through GB/T 28181 in the Camera Web System

When the GB/T 28181 protocol is used to connect a camera to the platform, you need to set the connection parameters in the camera web system.

Precautions

- The GB/T 28181 protocol uses MD5 digest authentication. The MD5 algorithm is vulnerable, and the signaling and media streams are not encrypted, which may result in security risks. Therefore, the GB/T 28181 protocol must be used on a trusted network.
- If you want to add cameras to the IVS1800 through GB/T 28181, you need to obtain the required parameter values (for example, device ID).

Setting the System Time

To connect a camera to the platform through the GB/T 28181 protocol, ensure that the camera is time-synchronized with the NTP server.

- Step 1** Open a web browser, enter the camera IP address in the address box, and press **Enter**.
- Step 2** Enter the user name and password of the camera and click the login button to log in to the camera web system.
- Step 3** Choose **Settings > System > Time**.
- Step 4** On the **Time** page, configure NTP time calibration, as shown in [Figure 5-8](#). [Table 5-10](#) describes the parameters.

Figure 5-8 Configuring NTP time calibration

Time zone: (UTC+08:00) Beijing, Hong Kong, ▾

Calibration mode: ☐ Manual ☒ NTP

NTP server: 0.0.0.0

Synchronization interval (min): 60

Device time: 2018-11-30 14:05:07

Save

Table 5-10 NTP time calibration parameters

Parameter	Description
Time zone	Select the time zone of the NTP server.
Calibration mode	Select NTP .
NTP server	IP address of the IVS1800.
Synchronization interval (min)	Time synchronization interval.

Step 5 Click **Save**.

----End

Setting GB/T 28181 Parameters

Step 1 Log in to the camera web system and choose **Settings > Network > Platform Connection**.

The **Platform Connection** page is displayed.

Step 2 Click **Second Protocol Parameters**. Click the **T28181** tab. On the tab page that is displayed, select **GB/T 28181** to enable the GB/T 28181 protocol.

Step 3 Set GB/T 28181 parameters, as shown in [Figure 5-9](#). [Figure 5-9](#) describes the GB/T 28181 parameters.

Figure 5-9 Setting GB/T 28181 parameters

☒ Enable media stream keep-alive (Note: After the function is enabled, if the IPC does not periodically receive keep-alive messages from the video surveillance platform, the IPC stops sending media streams. Set this parameter based on platform requirements.)

Keep-alive retries:

ONVIF **T28181**

☒ GB/T 28181 (Note: When all alarm input IDs and audio output IDs are empty, no IDs will be automatically generated.)

Name	12345678901324282900	Registration validity (s)	3600
Platform IP	8 . 32	Heartbeat interval (s)	60
Port number	5080	Max. timeouts	3
Device ID	12345678901324282900	Stream index	Primary stream
Server code	12345678901324282900	Lens ID	12345678901314282901
@	1234567890	Alarm input ID	12345678901344282901 Alarm input 1
Password		Audio output ID	Audio output 1

☐ GB35114

Table 5-11 Parameter description

Parameter	Description
Enable media stream keep-alive	Indicates whether to enable the keep-alive function for media streams. To enable the function, select Enable media stream keep-alive . If the keep-alive function is enabled for media streams and a camera does not receive keep-alive packets sent by the IVS1800 within a specified period, the camera stops sending media streams. If the platform supports the keep-alive function, you are advised to select Enable media stream keep-alive .
Keep-alive retries	Number of times that the camera and IVS1800 keep alive connections for media streams. The value is an integer ranging from 2 to 24. The keep-alive duration is 5s. For example, if the parameter is set to 2, the media stream keep-alive duration is 10s (2 x 5s). The camera keeps sending media streams even if it does not receive media keep-alive packets within 10s and stops sending media streams if it does not receive media keep-alive packets for more than 10s.
Name	Login name used to register a camera with the IVS1800.
Platform IP	IP address of the IVS1800.
Port number	GB/T 28181 port that the platform listens on. Use the port number 5080 when connecting the camera to the platform. If the server and camera are on different networks and NAT is performed, set this parameter to the post-NAT port number of port 5080.
Device ID	Unique ID of a device. The eleventh to thirteenth digits must be 132, and the last two digits must be 0.

Parameter	Description
Server code	GB/T 28181 server code. Enter a 20-digit number, of which the eleventh to thirteenth digits must be 200. The server code must be consistent for cameras connected to the same IVS1800.
@	User-defined domain name that consists of 10 digits.
Password	Password used to register a camera with the platform. For security purposes, the password must consist of 8 to 20 characters and contain at least two types of the following: digits, letters, and special characters.
Lens ID	Customized camera ID. The value must be a 20-digit number and the eleventh to thirteenth digits must be 131. Otherwise, live video cannot be viewed in the IVS1800 system.
Alarm input ID	Alarm input ID. The platform allocates it to a camera based on the device ID.
Audio output ID	Audio output ID. The platform allocates it to a camera based on the device ID.

Step 4 Click **Save**.

----End

5.1.2.3.2 Configuring Connection Through ONVIF in the Camera Web System

When the ONVIF protocol is used to connect a camera to the IVS1800/NVR800, you need to set the connection parameters in the camera web system.

Prerequisites

- The ONVIF protocol is used on a trusted network. Otherwise, security risks may exist. The protocol uses MD5 digest authentication. The MD5 algorithm is a weak algorithm, and media streams are not encrypted, which may result in security risks.
- The ONVIF protocol and the IVS1800/NVR800 support the H.265 encoding protocol if the ONVIF protocol needs to use the H.265 encoding protocol. cameras must be of V200R003C10 or later versions. As for the IVS1800/NVR800, contact the vendor to obtain the protocol support information. If the camera or IVS1800/NVR800 does not support H.265, set the encoding protocol (for the primary streams and secondary streams) to H.264 and then set parameters on devices. The detailed procedure is as follows: log in to the camera web system, choose **Settings > Video/Audio/Image > Video**, and set **Encoding protocol** to **H.264**.
- By default, the ONVIF protocol uses the HTTP/HTTPS transmission protocol.
- The ONVIF protocol supports only the G711U audio encoding format.
- The default port number is 80.

Procedure

Step 1 Log in to the camera web system (<https://Camera IP address>).

Step 2 Choose **Settings > Network > Platform Connection**.

The **Platform Connection** page is displayed.

Step 3 Choose **Second Protocol Parameters > ONVIF** to access the page for setting ONVIF parameters.

Step 4 Set ONVIF parameters, as shown in [Figure 5-10](#). [Table 5-12](#) describes the ONVIF parameters.

Figure 5-10 Setting ONVIF parameters

Second Protocol Parameters

☒ Enable media stream keep-alive (Note: After the function is enabled, if the SDC does not periodically receive keep-alive messages from the video surveillance platform, the SDC stops sending media streams. Set this parameter based on platform requirements.)

Keep-alive duration: 60 Save

ONVIF T28181 T28181-2 GA/T 1400 GA/T 1400-2 REST DB3311

(Note: When the video encoding format is H.265, the ONVIF protocol is not compatible with the old device on the live network. You need to change the video encoding format to H.264.)

☒ Enable ONVIF

☒ Validity period (Note: After the function is enabled, if the current SDC time is beyond the validity period specified on the platform, ONVIF messages become invalid. This parameter is valid only when the platform supports the ONVIF validity period function.)

☒ Onvif metadata flow switch (Note: Please select whether to turn on the metadata stream switch according to the requirements of the decoding platform, so as not to be unable to decode)

Stream type: Elementary stream (Note: Select a stream transmission type based on the requirements of the decoding device to prevent decoding failure.)

Authentication mode: Digest_MD5(priority)/WSSE (Note: Enabling WSSE brings security risks. Exercise caution when performing this operation.)

Version: ONVIF 16.12

ONVIF Trans Protocol Type: HTTP/HTTPS (Note: HTTP is an insecure protocol and has security risks. Exercise caution when using this protocol.)

Table 5-12 Parameter description

Parameter	Description
Enable media stream keep-alive	Indicates whether to enable the keep-alive function for media streams. To enable the function, select Enable media stream keep-alive . If the keep-alive function is enabled for media streams and a camera does not receive keep-alive packets sent by the IVS1800/NVR800 within a specified period, the camera stops sending media streams. If the platform supports the keep-alive function, you are advised to select Enable media stream keep-alive .
Keep-alive duration	Duration that the camera and IVS1800/NVR800 keep alive connections for media streams. The value is an integer ranging from 10 to 120. For example, if this parameter is set to 60s, the camera does not stop sending media streams even if it does not receive media keep-alive packets within 60s and stops sending media streams if it does not receive media keep-alive packets for more than 60s.
Enable ONVIF	To enable the ONVIF protocol, select Enable ONVIF .

Parameter	Description
Validity period	To enable the ONVIF message validity period function, select Validity period. After this function is enabled, an ONVIF message will become invalid when the specified validity period elapses. NOTE The ONVIF message validity period function is valid only when supported by the IVS1800/NVR800. If the platform does not support this function but this parameter is selected in the camera web system, the camera will fail to connect to the IVS1800/NVR800. You are advised to enable this function only when security risks exist. The ONVIF message validity period function is disabled by default.
ONVIF metadata flow switch	If this parameter is selected, the camera's metadata can be obtained. Otherwise, only video and audio streams can be obtained. This function is enabled by default.
Stream type	Select a media transmission type from the Stream type drop-down list box. The options are as follows: • Elementary stream: uses the ES compression mode. • Program stream: uses the PS compression mode. NOTE • Select the stream type based on the requirements of the decoder to prevent decoding failure. • The ONVIF media stream can be configured only when the camera is connected to the platform through the ONVIF protocol.

Parameter	Description
Authentication mode	Select a desired authentication mode from the Authentication mode drop-down list box. The options are as follows: • Digest_MD5: Digest authentication with MD5 encryption. • Digest_SHA256: Digest authentication with SHA256 encryption. • Digest_MD5/Digest_SHA256: Both Digest_MD5 and Digest_SHA256 authentication modes are supported. • Digest_MD5(priority)/WSSE: Both Digest_MD5 and WSSE authentication modes are supported, but Digest_MD5 authentication is preferred. • WSSE: indicates the Web Service Security (WSSE) authentication mode. • None: indicates that authentication is not performed. NOTE • The ONVIF WSSE authentication mode has security risks. – When some platforms to which the cameras connect support ONVIF WSSE authentication only, you are advised to enable the Digest_MD5(priority)/WSSE authentication mode. – When all platforms to which the cameras connect support ONVIF WSSE authentication only, you are advised to enable the WSSE authentication mode. – You are advised to enable the WSSE authentication mode when some platforms cannot correctly process Digest messages. • Security risks may exist when you select None. It is recommended that this authentication mode be enabled only when the platform does not support authentication. If None is selected, the system does not perform authentication if you request live video through the RTSP or ONVIF protocol.
Version	Ensure that the ONVIF version supported by the camera is consistent with that supported by the platform.
ONVIF Transmission Protocol Type	ONVIF transmission protocol. The options are as follows: • HTTP/HTTPS: Data is transmitted through HTTP or HTTPS. • HTTP: Data is transmitted through HTTP. • HTTPS: Data is transmitted through HTTPS. NOTE HTTP is an insecure protocol and has security risks. Therefore, exercise caution when using this protocol.

Parameter	Description
Password Management	Method 1: 1. In the Password Management area, click ONVIF Password. 2. On the ONVIF Password tab page, set Current password, New password, and Confirm password. 3. Click Save. Method 2: 1. Choose Settings > System > Password Management. 2. Click Protocol Password. 3. On the ONVIF Password tab page, set Current password, New password, and Confirm password. 4. Click Save. NOTE • Change the ONVIF password for data security purposes. When the camera uses the ONVIF protocol to connect to the IVS1800/NVR800, you must enter this password. Otherwise, the connection cannot be set up. If platform authentication fails for 20 consecutive times, the camera is locked for 5 minutes. After the password is changed, record and keep the new password secure. • The default user name is admin. The value of Current password must be the same as the password of the admin user who logs in to the camera web system. For security purposes, the password must consist of 8 to 20 characters and contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters. For system security purposes, the following weak passwords are not recommended: 1qaz!QAZ, admin123, admin123!, Admin123!, Administrator, datacache1, datacache2, datacache3, "datacache4", datacache5, dlsDb001, dlsDls01, guest123, LcaP2010, lcap_oracle, lcap_uoa, password1, Password, password123, PortalONE, prmt_iddeploy, Promotion, SDP Report, u+versioncode, and Change_Me.

----End

5.1.3 Verification

If a camera is added successfully, the status of the camera is **Online** and you can view live video from this camera.

Procedure

Step 1 Check the camera status.

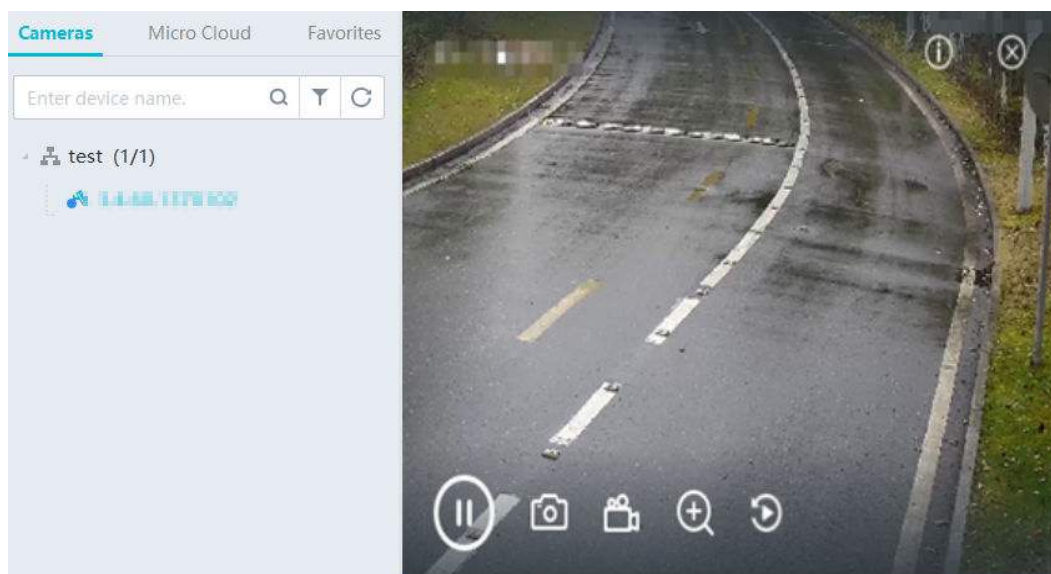
1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Select the IVS1800 to which the camera is connected and check whether the camera status is **Online** in the **Device Status** column.

NOTE

If adding a camera for the first time is successful but the camera goes offline later, no cause will be displayed on the page. You need to manually locate the cause.

Step 2 View live video from the camera.

1. Click **Live** on the iClient S100 home page.
2. Drag the added camera to the live video pane. If the live video can be properly played, the access is successful, as shown in [Figure 5-11](#).

Figure 5-11 Viewing live video from the camera**NOTE**

- If the added camera is not displayed in the **Device List**, click  to refresh the **Device List**.
- You can also drag the entire camera group to the live video layout to view the live video from all the cameras in the group. You can create camera groups as required. You can customize a camera group under **Video Device > Group Device**.
 - **Cameras**: displays all camera groups and cameras in the groups. You can view live video from a camera or a group of cameras.
 - **Micro Cloud**: displays all IVS1800s and allows users to view live video from cameras connected to each IVS1800.
 - **Favorites**: displays favorited cameras and views. You can view live video from a favorited camera and invoke a favorited view.

----End

5.2 Video Viewing

5.2.1 Live Video Viewing

NOTE

You need to strictly comply with your local laws and regulations when using video-related services, for example, recording video, recording voice, and taking snapshots. Do not use them for illegitimate purposes such as infringing on personal privacy or observing employee behaviors.

Viewing Live Video from a Single Camera

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.

----End

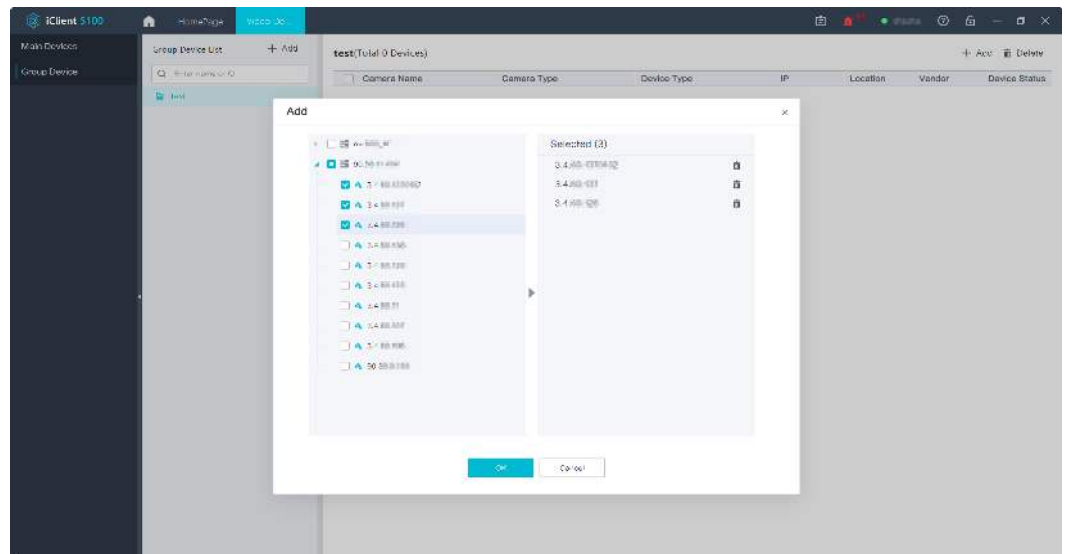
NOTE

- During live video viewing, do not overlap the video pane that is playing live video with the window or dialog box of another program. The overlap may cause artifacts or even frozen images.
- If the live network is unstable, frame freezing or artifacts may occur on the live video. In this case, you are advised to enable the bandwidth adaptation function in the camera web system. After bandwidth adaptation is enabled, the camera can reduce or increase the bit rate based on the network condition to ensure smooth live video playing.

Viewing Live Video from Grouped Cameras

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Group Device** and group cameras.

1. Click **Add** on the right of the **Group Device List**, enter the group name, and click .
2. Click the newly added camera group and click **Add** in the upper right corner. On the page that is displayed, select cameras and click **OK**, as shown in [Figure 5-12](#).

Figure 5-12 Grouping cameras

Step 2 Choose **Basic Operations > Live** on the iClient S100 home page to view live video from cameras in a group (containing more than one camera and excluding cameras in subgroups).

In the device list (for device groups or all devices):

- Hold down **Ctrl** or **Shift**, select multiple cameras from the device tree, and drag the cameras to live video panes.
- Drag a group or main device to live video panes.
- Click  next to a group or main device.

Select **Tile** or **Cycling** to start viewing live video from cameras in the group or under the main device.

- In tile mode:
 - Video from selected cameras is displayed in the camera selection sequence.
 - If the number of idle live video panes is less than the number of online cameras in the group, video from some cameras will not be played. You need to manually adjust the video pane layout and view live video.
 - Live video can be played in sequence only in the selected video pane. For example, if you drag four cameras to the fourth video pane in the layout of four video panes, live video from the cameras is played in the fourth video pane in sequence, and the first three video panes do not play live video even if they are idle.
- In cycling mode:
 - a. Click **Advanced** and set parameters. [Table 5-13](#) lists the key parameters.

Table 5-13 Key parameters

Parameter	Description
Panes	Number of cycling panes, which must be less than the number of cameras to cycle.
Arrangement	▪ Tile ▪ Custom: In the Customize Panes window that is displayed, select panes and click Start.
Interval	Dwell time for selected cameras to play live video, in seconds.
Stream Type	The default value is Primary .

- b. Click **OK** to start cycling.

----End

5.2.2 Camera Cycling

Application Scenario

You can configure a cycling policy to view live video from multiple cameras at a certain interval. For example, multiple cameras are deployed on the Tianmushan Road. However, live video panes are insufficient for playing live video from all cameras at the same time. You can configure a cycling policy to view live video from the cameras at an interval of 30 seconds.

Procedure

- Step 1** On the iClient S100 home page, choose **Basic Operations > Live**.
- Step 2** Click  in the lower right corner of the **Live** page. To add a cycle group for the first time, click +. Otherwise, click **New Group**.
- Step 3** In the **New Cycle** window, configure cycle group information, as shown in [Figure 5-13](#). [Table 5-14](#) describes the key parameters.

Figure 5-13 New Cycle window

New Cycle [X]

Name:

Pane Quantity: Must be less than camera quantity.

Camera:

Dwell Time (s): ☐ Adjustable

Up Down Delete

☐	Group ...	Name	Dwell Time (s)	Preset Position	Live Stream	Video Wall Stream
☐	Group 1		30		Locally set	Locally set
☐	Group 1		30		Locally set	Locally set
☐	Group 2		30		Locally set	Locally set

Table 5-14 Key parameters and icons for adding a cycle group

Parameter	Description
Pane Quantity	Number of cycling panes, which must be less than the number of cameras to cycle.
Dwell Time (s)	Dwell time at the selected cameras. The dwell time can be configured for cameras in batches or one by one. In this example, the dwell time is configured for a single group as an example.
Live Stream	● Locally set: The settings are the same as those in the Personal Settings area. ● Automatic: No stream is specified. After this option is selected, the stream that the camera has transmitted to the platform is preferentially used. If the camera has not transmitted any streams to the platform, the primary stream of the camera is used by default. ● Primary: The primary stream of the camera is used. The primary stream features a high bit rate, definition, and bandwidth usage. ● Secondary 1: Secondary stream 1 of the camera is used. The secondary stream features low definition and bandwidth usage. ● Secondary 2: Secondary stream 2 of the camera is used. The secondary stream features low definition and bandwidth usage. NOTE When bandwidth resources are limited, set this parameter to Secondary 1 or Secondary 2.

Parameter	Description
Video Wall Stream	• Locally set: The settings are the same as those in the Personal Settings area. • Primary: The primary stream of the camera is used. The primary stream features a high bit rate, definition, and bandwidth usage. • Secondary 1: Secondary stream 1 of the camera is used. The secondary stream features low definition and bandwidth usage. • Secondary 2: Secondary stream 2 of the camera is used. The secondary stream features low definition and bandwidth usage. NOTE When bandwidth resources are limited, set this parameter to Secondary 1 or Secondary 2.
Up/Down	Select a camera and click Up or Down to adjust the camera cycling sequence.

Step 4 Click  in the lower right corner of the **Live** page. The added cycle groups are displayed in the **Cycle Cameras** window. You can perform the following operations:

- Click . The selected pane is regarded as the first pane. The live video from corresponding cameras is played in sequence in cycling mode. For example, if pane 2 is selected, and the number of panes is three, live video is displayed in panes 2, 3, and 4 in cycling mode.
- Click  to customize panes for live video viewing in cycling mode.

----End

5.2.3 View Management

Application Scenario

Live video pane layout settings (including camera settings) and cycling settings can be stored as views to facilitate your later use.

- **View favoriting:** You are responsible for viewing live video from cameras on the Tianmushan Road (four-pane layout) and Xixi Road (nine-pane layout). You can favorite the views to quickly switch between them without repeatedly dragging cameras to live video panes.
- **View schedule configuration:** You have configured multiple views to store live video from multiple cameras on the Xixi Road. You can configure view schedules so that these views can be automatically played in the specified periods every week.

Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Select the required live video pane layout. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.

NOTE

You can store cycling views after starting viewing live video in cycling mode. For details about how to configure and start camera cycling, see [5.2.2 Camera Cycling](#). You can then configure a view schedule to perform periodic cycling as scheduled.

Step 3 Click  and set **Save as** to **New** or **Overwrite**.

- If you set **Save as** to **New**, set **View Name** and save the view.
- If you set **Save as** to **Overwrite**, the new view overwrites the existing one.

Step 4 Click **OK**.

Step 5 Repeat [Step 2](#) through [Step 4](#) to save more views.

Step 6 Click the **Favorites** tab and view the favorited views in the **Favorited Views** area.

Step 7 Click  next to **Favorited Views**. The **View Schedule** page is displayed.

Step 8 Click **New Schedule**. In the **New Schedule** window that is displayed, set view schedule parameters, as shown in [Figure 5-14](#). [Table 5-15](#) lists related parameters.

Figure 5-14 New Schedule

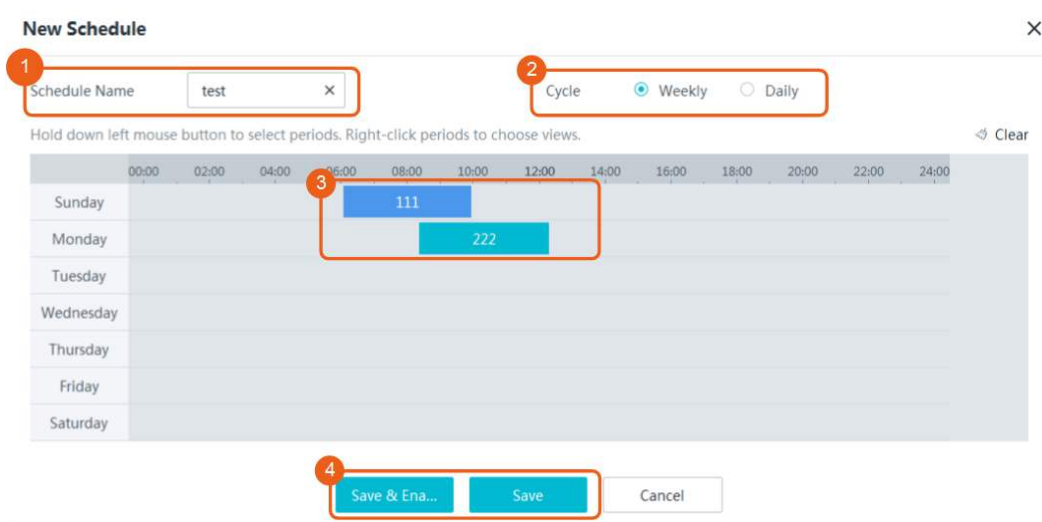


Table 5-15 Parameter description

Parameter	Description
Cycle	Cycle for executing a view schedule.

Parameter	Description
Period	Time segment for playing a view. Drag the mouse to configure a specified time segment for view playing. Right-click the time segment and choose a view from the shortcut menu. Click the time segment and set specific time points.

----End

5.2.4 PTZ Controls

Application Scenario

You can perform PTZ controls to control the camera direction and focal length and invoke preset positions. You can configure preset positions and follow-up tours to periodically view live video of specified sites.

For example, area A is a key area for video observation. To achieve better observation effect, you can use the PTZ controls function to adjust the camera direction and focal length. You can set the adjusted direction and focal length as a preset position. When you need to view live video from area A in the future, you can directly invoke the preset position to adjust the camera to the specified direction and focal length. If you have multiple key areas for video observation, you can set preset positions for each area and configure a tour to periodically view live video of these areas.

Prerequisites

The camera is a PTZ dome camera or a camera of another type providing PTZ functions.

NOTE

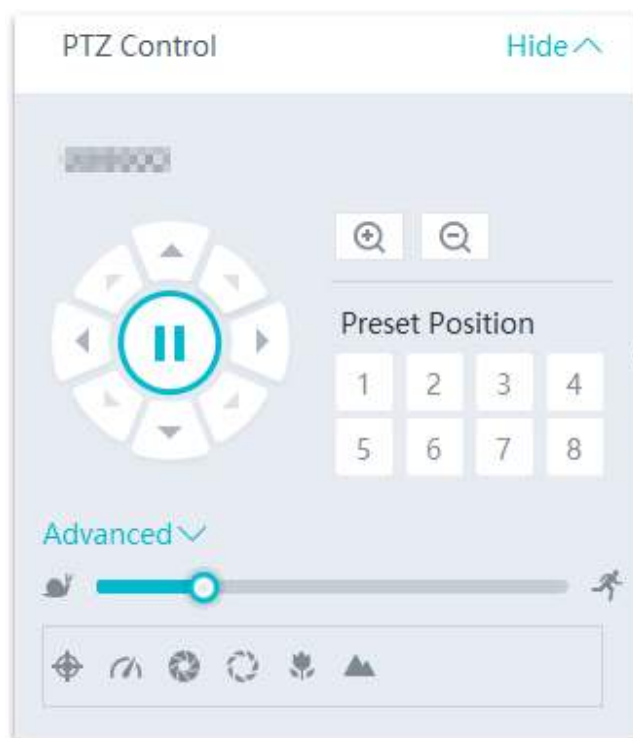
- This section uses a PTZ dome camera as an example to describe how to perform PTZ controls.
- By default, PTZ dome cameras and PTZ box cameras provide all PTZ functions, and bullet cameras and fixed dome cameras only provide some PTZ functions such as zoom in/out and focal length adjustment. The specific functions are subject to that displayed on the **PTZ Control** page of the iClient S100.
- PTZ controls results vary depending on the specific functions supported by PUs. For details, see the camera compatibility list.

Basic Operations

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Drag an online PTZ camera in the **Devices** area to a live video pane.

Step 3 Click the expand icon next to **PTZ Control** in the lower left corner, as shown in [Figure 5-15](#).

Figure 5-15 PTZ Control panel

- Use the eight arrow buttons to rotate the PTZ device to adjust the camera shooting angle.

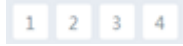
Click the expand icon next to **Advanced** and drag the slider on

   or click  or  to control the PTZ rotation speed.

- Drag the slider to the left or click  to slow down the PTZ rotation speed.
 - Drag the slider to the right or click  to increase the PTZ rotation speed.
- Click  or  to zoom in or out on the live video image.

NOTE

If you zoom in on the video image for more than 30 times, the camera will enter the digital zoom mode. If you set the current position where the camera shoots as a preset position, the camera will not record the digital zoom ratio. When you invoke the preset position, the video image is zoomed in only for 30 times.

- Click a preset position ID in  to invoke the preset position. You can set positions where the camera shoots objects as preset positions and quickly invoke a preset position to view the desired object. For details about how to set a preset position, see [Configuring Preset Positions and the Home Position](#).

- Click the expand icon next to **Advanced** and click buttons in



in the **Advanced** area to use other advanced functions of the PTZ device. [Table 5-16](#) describes the related buttons.

Table 5-16 Button description

Button	Description
3D Positioning	Automatically adjusts the PTZ camera shooting angle and focal length based on the ROI on the live video image. The procedure is as follows: - Click . Hold down the left mouse button and select an ROI on the live video image. The system automatically adjusts the shooting angle and focal length to the optimal using the ROI as the center. If you draw a frame from left to right, the video image within the frame is automatically zoomed in. If you draw a frame from right to left, the video image within the frame is automatically zoomed out. - Click  and click a position on the live video image. The system automatically rotates the PTZ camera to the position. NOTE If an ONVIF-compliant device needs to use the 3D zoom-in function, the device must implement the 3D zoom-in function in the same mode as the platform. For details about the mode used by the platform to implement the 3D zoom-in function, contact related engineers.
Horizontal Tour	Allows you to view live video from the camera that is performing a horizontal tour. The horizontal tour function allows unidirectional or back-and-forth scanning in either a clockwise or an anti-clockwise direction at a specified degree (including 360°).
Aperture-	Decreases the aperture.
Aperture+	Increases the aperture.
Focus+	Increases the focal length of the camera.
Focus-	Decreases the focal length of the camera.

- Step 4** (Optional) Click  on the toolbar of the live video pane. Then, you can use the mouse to control the PTZ rotation direction.

The operation method is specified by **Move Controls** under **Maintenance Management > Personal Settings > PTZ Settings**.

----End

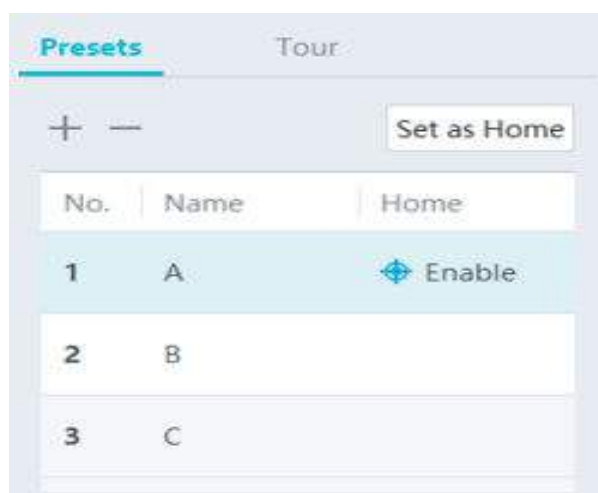
Configuring Preset Positions and the Home Position

NOTE

A home position is a special preset position to which a PTZ camera automatically rotates if users do not control the rotation direction of the camera within a specified period.

- Step 1** Click the live video pane of the selected PTZ dome camera, control the PTZ rotation direction and zoom ratio, and rotate the PTZ device to an observation site for which you want to add as a preset position.
- Step 2** Click the expand icon next to **Advanced** in the **PTZ Control** window and click the **Presets** tab. The **Presets** tab page is displayed, as shown in [Figure 5-16](#).

Figure 5-16 Presets tab page



- Step 3** Click . In the **Add Preset Position** window that is displayed, set **Preset Position Name**.

NOTE

Right-click a preset position and choose **Edit** from the shortcut menu to edit the preset position name.

- Step 4** Click **OK**.

- Step 5** Repeat [Step 1](#) through [Step 4](#) to add more preset positions.

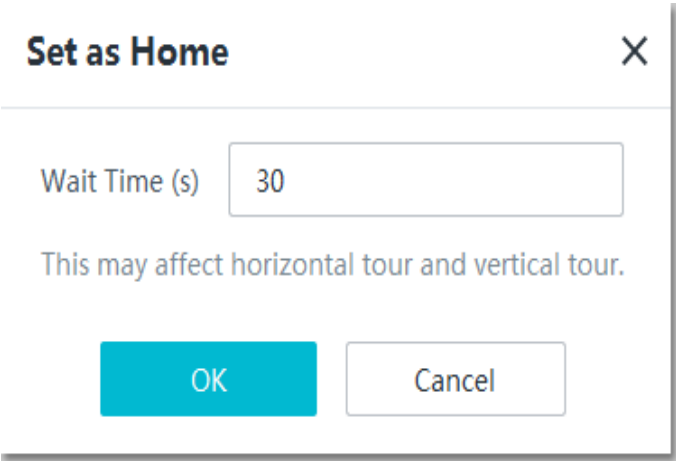
- Step 6** Click a preset position and click **Set as Home**. In the **Set as Home** window that is displayed, set **Wait Time (s)** and click **OK**, as shown in [Figure 5-17](#).

If the current position of the PTZ camera is not the home position, the PTZ camera automatically rotates to the home position if no PTZ controls are performed before the configured waiting duration elapses.

NOTE

Right-click a preset position and choose **Enable** or **Disable** from the shortcut menu to enable or disable the preset position.

Figure 5-17 Set as Home window

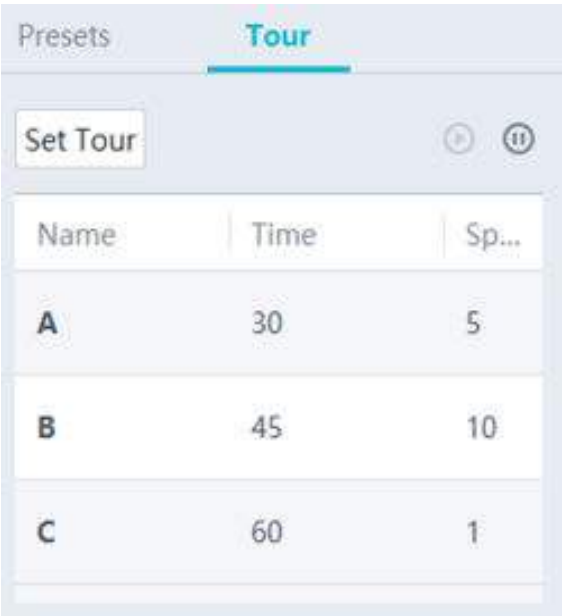


- Step 7** You can invoke a preset position in either of the following ways:
- 1. Click the preset position button on the right of the PTZ steering wheel to quickly invoke the first eight preset positions.
 - 2. Double-click a preset position in the preset position list.
- End

Tour

- Step 1** Click the expand icon next to **Advanced** in the **PTZ Control** window and click the **Tour** tab, as shown in [Figure 5-18](#).

Figure 5-18 Tour



- Step 2** Click **Set Tour** to add a tour, as shown in [Figure 5-19](#). [Table 5-17](#) describes the parameters and buttons.

Figure 5-19 Adding a tour

The 'Set Tour' dialog box contains a table with the following data:

☐	Preset Position	Dwell Time (s)	Speed Level
☐	A	30	5
☐	B	45	10
☐	C	60	1

Buttons: Up, Down, Add, Delete, OK, Cancel.

Table 5-17 Parameter/Button description

Parameter/ Button	Description
Up/Down	Select a preset position and click Up or Down to adjust the preset position sequence.
Add	Adds preset positions for the tour.
Delete	Deletes selected preset positions in batches.
Preset Position	Preset position. Each tour supports 1 to 20 preset positions.
Dwell Time (s)	Tour duration for each preset position. NOTE A short tour duration may shorten the service life of the camera motor and belt. If the preset positions do not need to be frequently switched onsite, you are advised to set the tour duration to be longer (for example, over 60 seconds).
Speed Level	Tour speed for each preset position.

Step 3 Click . The camera starts to play live video based on the tour.

-----End

5.2.5 Snapshot Taking

Manual snapshots are local snapshots. [Table 5-18](#) describes the function of local snapshots.

Table 5-18 Manual snapshot types

Snapshot Type	Function
Local snapshot	Local snapshots taken during live video viewing are stored on the computer where the iClient S100 client is located. NOTE Do not perform local snapshot taking in an alarm pane, because the alarm pane will play the alarm-triggered live video when the corresponding alarm is generated and interrupt the local snapshot taking.

Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Double-click an online camera in the **Devices** area or drag the online camera to a live video pane. Then, you can view the live video.

Step 3 Capture a snapshot and save it on the local computer.



Click  on the toolbar of the live video pane, or right-click the live video pane and choose **Snapshot** from the shortcut menu to take a snapshot of the current video image.

In this example, use the default storage directory. After the snapshot is taken, the message "Snapshot successful" is displayed in the lower right corner of the client page. You can click **Click here to open folder** to go to the snapshot storage directory.

Step 4 View the snapshot.

View the snapshot stored on the local computer.

Choose **Maintenance Management > Local Settings** on the iClient S100 home page. You can view the snapshot in the local snapshot storage directory.

----End

5.2.6 OSD Settings

Application Scenario

After setting On Screen Display (OSD) parameters, you can set whether to display the specified text and time, and whether to enable the text blinking function on the video.

Procedure

- Step 1** On the iClient S100 home page, choose **Basic Operations > Live**.
- Step 2** Double-click an online camera in the **Devices** area or drag the online camera to a live video pane. Then, you can view the live video.
- Step 3** Right-click a live video pane, choose **OSD Settings** from the shortcut menu, and set OSD parameters, as shown in **Figure 5-20**. **Table 5-19** describes the parameters.

Figure 5-20 OSD Settings page

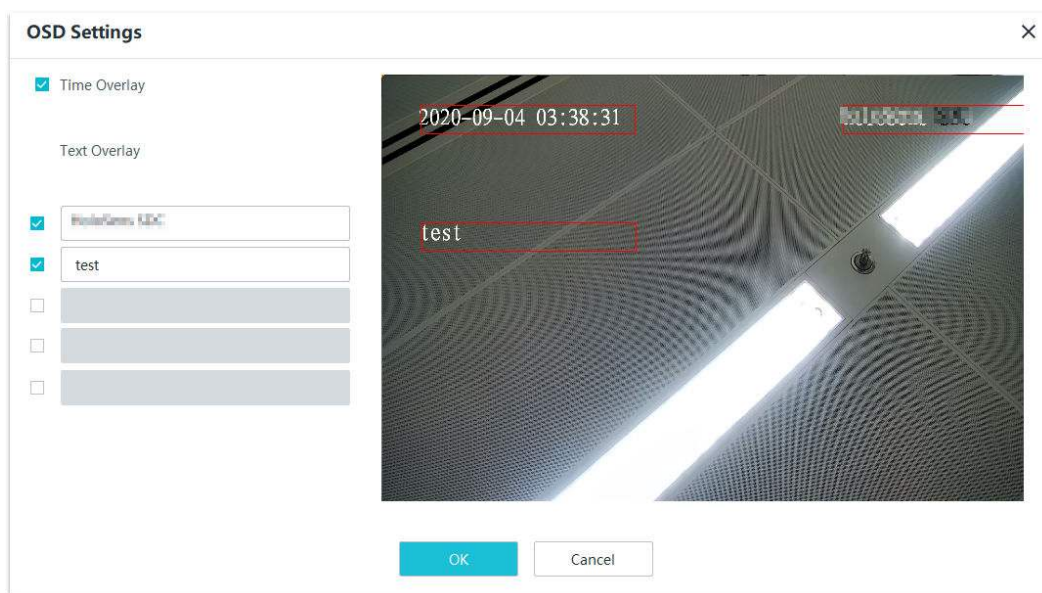


Table 5-19 OSD parameter description

Parameter	Description
Time Overlay	Indicates whether to display the current camera time on live video images.
Text Overlay	Indicates whether to display text on live video images. After this check box is selected, you can enter the text to be displayed in the text boxes. You are advised to set this parameter to the IP address or installation location of the camera. NOTE - To display multiple lines of texts on video images, select multiple check boxes under Text Overlay and enter the texts to display in the text boxes. - The maximum number of characters is determined by PU capabilities.
Red text box	Red-framed area. You can move it to adjust the display position.

----End

5.3 Recording

5.3.1 Application Scenario

You can record video after cameras are connected to the IVS1800.

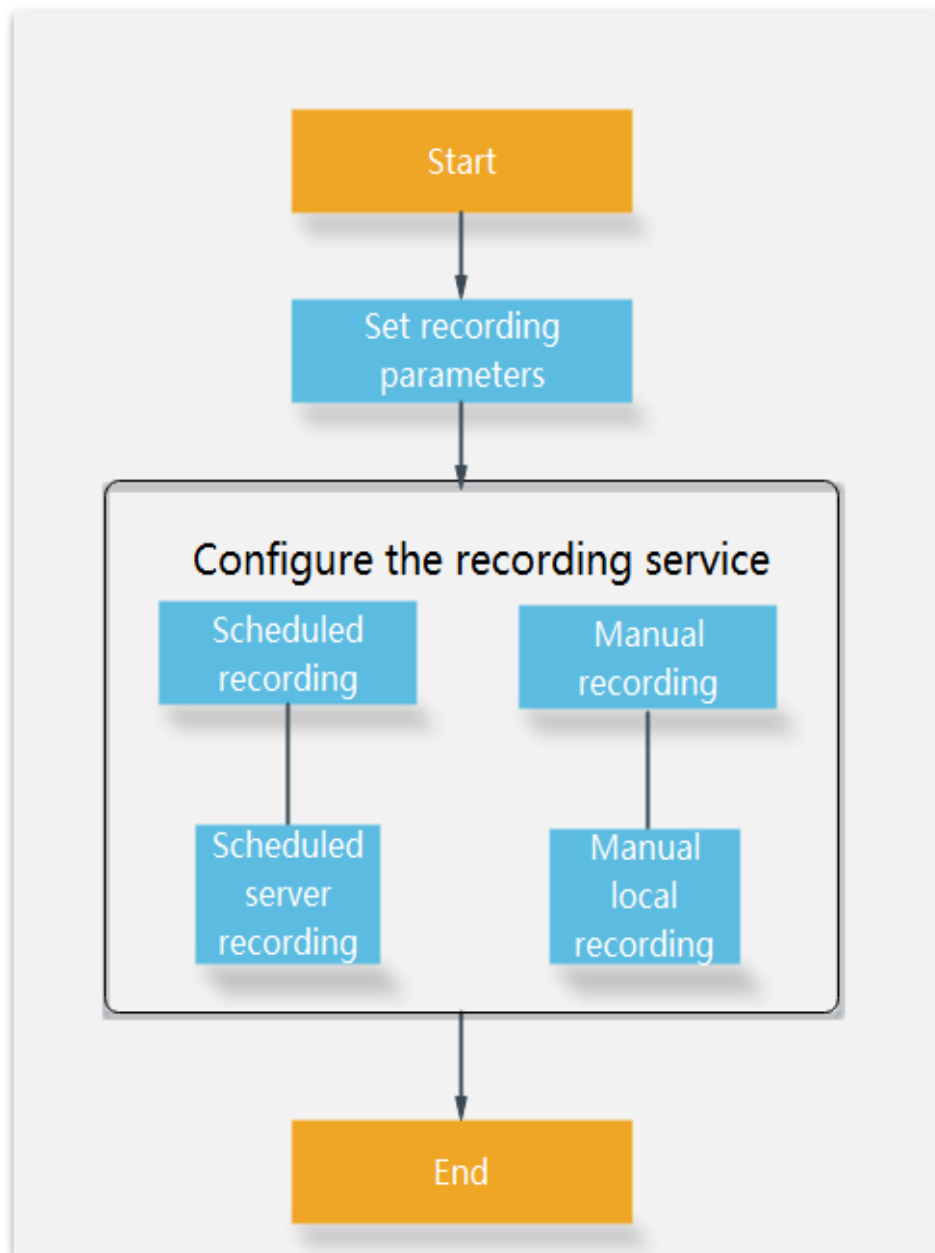
The recording function of the IVS1800 can be classified into scheduled recording and manual recording, which can be further classified into scheduled server recording, and manual local recording. [Table 5-20](#) describes the application scenarios of various recording types.

Table 5-20 Application scenarios of various recording types

Recording Type		Application Scenario
Scheduled recording	Scheduled server recording	The scheduled recording function is applicable when users need to save video of specified areas on the hard disks of the IVS1800 to facilitate analysis of incidents or abnormal situations.
Manual recording	Manual local recording	When emergencies occur in the specified area, users want to manually record the video and store it to the computer where the iClient S100 client is installed.

5.3.2 Overall Process

Before recording video, you need to determine the recording mode: scheduled recording or manual recording. In addition, you need to store recordings on the hard disk of IVS1800 or the computer running the iClient S100 client. [Figure 5-21](#) shows the configuration process.

Figure 5-21 Recording configuration process

1. Before recording video, you need to set recording parameters, such as the storage policy and video buffering.
2. Select scheduled recording or manual recording as required (For details, see [Table 5-20](#)) and start recording.

5.3.3 Recording Configuration

5.3.3.1 Setting Recording Parameters

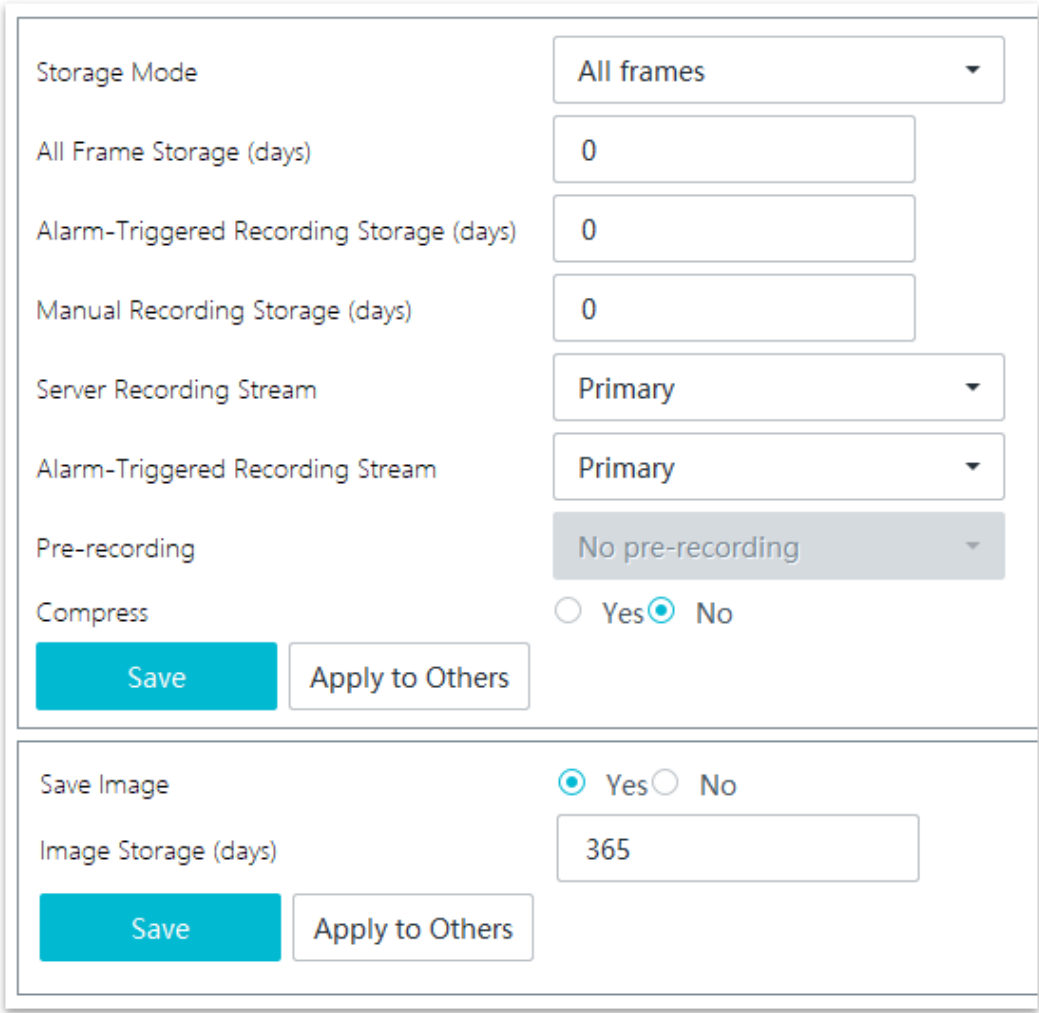
5.3.3.1.1 Configuring a Recording Storage Policy

Before configuring a recording plan or using manual recording, you need to configure a recording storage policy.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click a device in **Device List** and choose **Storage Management**.
- Step 3** Click the **Storage Policy** tab on the left of the page and select a desired camera in the camera list. Alternatively, click , set search criteria, and select the desired camera for which you want to set recording parameters. The page for configuring a storage policy is displayed, as shown in [Figure 5-22](#).

Figure 5-22 Configuring a storage policy



Storage Mode	All frames
All Frame Storage (days)	0
Alarm-Triggered Recording Storage (days)	0
Manual Recording Storage (days)	0
Server Recording Stream	Primary
Alarm-Triggered Recording Stream	Primary
Pre-recording	No pre-recording
Compress	☐ Yes ☒ No
Save Apply to Others	

Save Image	☒ Yes ☐ No
Image Storage (days)	365
Save Apply to Others	

- Step 4** Set storage policy parameters. [Table 5-21](#) describes the parameters.

Table 5-21 Recording storage policy parameters

Parameter	Description
Storage Mode	Storage mode. Select All frames in this example. The system retains the complete recordings within the all-frame storage period. When the storage period elapses and the remaining storage space is less than the threshold, the system deletes the earliest recordings. • If the remaining storage space is greater than the threshold: – If Video Recycle Policy is set to Recycle by storage space on the OMU portal, the system continues to record video. – If Video Recycle Policy is set to Recycle by expiration time on the OMU portal: ▪ If the storage period of some recordings exceeds the all-frame storage period, the system deletes these files in ascending order of their generation time until they are all deleted. ▪ If the storage period of all recordings is within the all-frame storage period, the system continues to record video. • If the remaining storage space is less than or equal to the threshold: – When Insufficient Recording Space Policy of this server is set to Stop if insufficient on the OMU portal: ▪ If the storage period of some recordings exceeds the all-frame storage period, the system deletes these files in ascending order of their generation time. ▪ If the storage period of all recordings is within the all-frame storage period, the system stops recording immediately after the storage space is used up. – When Insufficient Recording Space Policy of this server is set to Overwrite if insufficient on the OMU portal: Recordings are deleted based on the following sequence until the available storage space is greater than the threshold: recordings whose retention period expires > recordings whose retention period is not configured > earliest recordings in the retention period.
All Frame Storage (days)	Number of days for storing recordings. The value ranges from 0 to 9999. A larger value indicates a longer video storage period. The default value is 0.

Parameter	Description
Alarm-Triggered Recording Storage (days) This parameter is available for alarm-triggered recordings.	NOTE - When this parameter is set to 0, the storage period is not fixed and the storage priority is low. When the storage space is full, the recording is preferentially recycled. - Pay attention to changes of stored image data after changing any value of these parameters. If a value is reduced, data stored in the original storage period but not in the new one will be deleted. - You are advised to configure the storage period during software deployment. - You are advised not to change the storage period during upgrades, key assurance periods, or important events.
Manual Recording Storage (days) This parameter is available for manual server recording.	
Server Recording Stream	Stream type used for scheduled server recording (stored on the hard disks of IVS1800). Set this parameter based on the bandwidth and network quality. The options are as follows: Automatic: No stream is specified, and the primary stream is used by default. Primary: The primary stream of the camera is used. The primary stream features a high bit rate, definition, and bandwidth usage. Secondary: Secondary streams of the camera are used. Secondary streams feature low bit rates, definition, and bandwidth usage. If the camera has multiple secondary streams, the parameter will display multiple secondary stream options such as Secondary 1 and Secondary 2.
Alarm-Triggered Recording Stream	Stream type used for alarm-triggered recording (stored on the hard disks of IVS1800).
Pre-recording	Pre-recording mode. The options are as follows: No pre-recording (default value): The pre-recording function is disabled.

Parameter	Description
Save Image	Indicates whether to store image data captured by checkpoint cameras. The options are Yes and No .
Image Storage (days)	Duration for storing checkpoint images. The default value is 365. CAUTION • Pay attention to changes of stored image data after changing the value of this parameter. If the value is reduced, data stored in the original storage period but not in the new one will be deleted. • You are advised to configure the storage period during software deployment. • You are advised not to change the storage period during upgrades, key assurance periods, or important events.

Step 5 Click **Save**.

Step 6 (Optional) Click **Apply to Others**, select cameras to which the current camera's recording storage policy is to be copied, and click **OK** to complete the batch setting.

----End

5.3.3.1.2 (Optional) Configuring Video Buffering

When the network is disconnected, the PU can temporarily store the scheduled recordings locally based on the server recording plan. To ensure video integrity, users can use the video buffering function. After the network is recovered, the platform sends a video buffering request to the PU, and the PU sends the stored video to the server.

Prerequisites

- Cameras are equipped with SD cards, and can execute recording tasks properly.
- Time has been synchronized from the server to cameras.

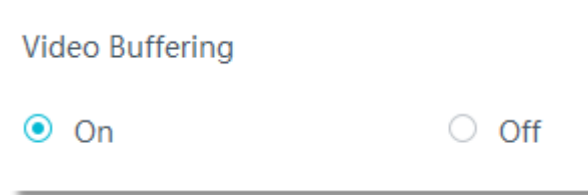
Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Double-click a camera for which video buffering needs to be configured in the camera list on the right.

Step 3 On the configuration page that is displayed, choose **Video Channel > Basic Settings**.

Step 4 Set **Video Buffering** to **On**, as shown in [Figure 5-23](#).

Figure 5-23 Setting Video Buffering to On

Step 5 Click **Save**.

Step 6 On the OMU portal, configure the number of retry days and the number of daily retry times for video buffering.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Right-click a device in **Device List** and choose **Maintenance**.
3. In the displayed dialog box, click **OK**, and the OMU portal will be automatically opened in the browser.
4. Choose **Maintenance > Unified Configuration** on the OMU portal.
5. Set **Module name** to **MU** and click **Search**.
6. Click **Edit** and set **MaxUploadRetryCountsLimit** and **MaxUploadRetryDaysLimit**, as shown in [Figure 5-24](#). [Table 5-22](#) describes the parameters.

Figure 5-24 Setting video buffering parameters

MU	No	NAT_MAPPING	NatRtpTsServerPort	Nat port to connect M...	0	A positive int...	Default port is 0. Zero ...	Edit
MU	Yes	MU recording c...	MaxUploadRetryCoun...	Record retry counts	3	A positive int...	The default value is 3	Save Cancel
MU	Yes	MU recording c...	MaxUploadRetryDays...	Record retry days	1	A positive int...	The default value is 1	Edit

Table 5-22 Parameter description

Parameter	Description
MaxUploadRetryCountsLimit	Customized number of times for a camera to send buffered video to the platform consecutively even if the sending fails. For example, set this parameter to 3. After the camera goes online again, the system triggers video buffering. If video buffering fails for three consecutive times, the system skips the current recording and proceeds with video buffering of the next recording.

Parameter	Description
MaxUploadRetryDaysLimit	Customized number of days. Buffered video recordings within this period be sent. For example, set this parameter to 3. When the camera goes online again, the system sends a request to upload buffered recordings of the last three days.

7. Click **Save**.

----End

5.3.3.2 Configuring Scheduled Recording

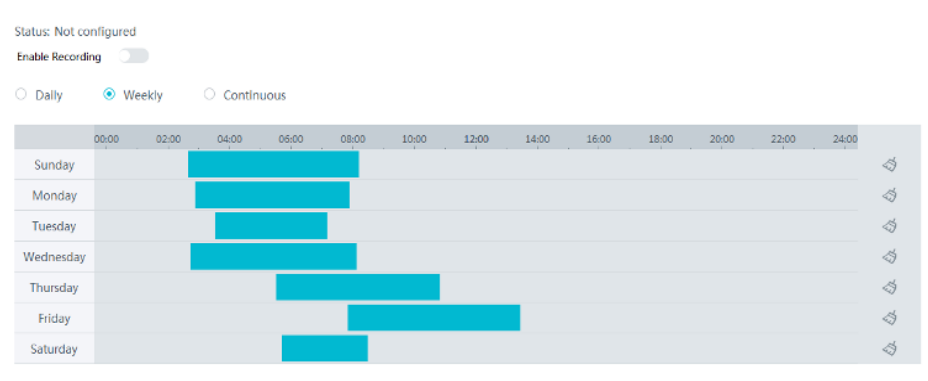
5.3.3.2.1 Configuring Scheduled Server Recording

The system can record video in a user-defined time segment and store the recorded video to server disks.

Procedure

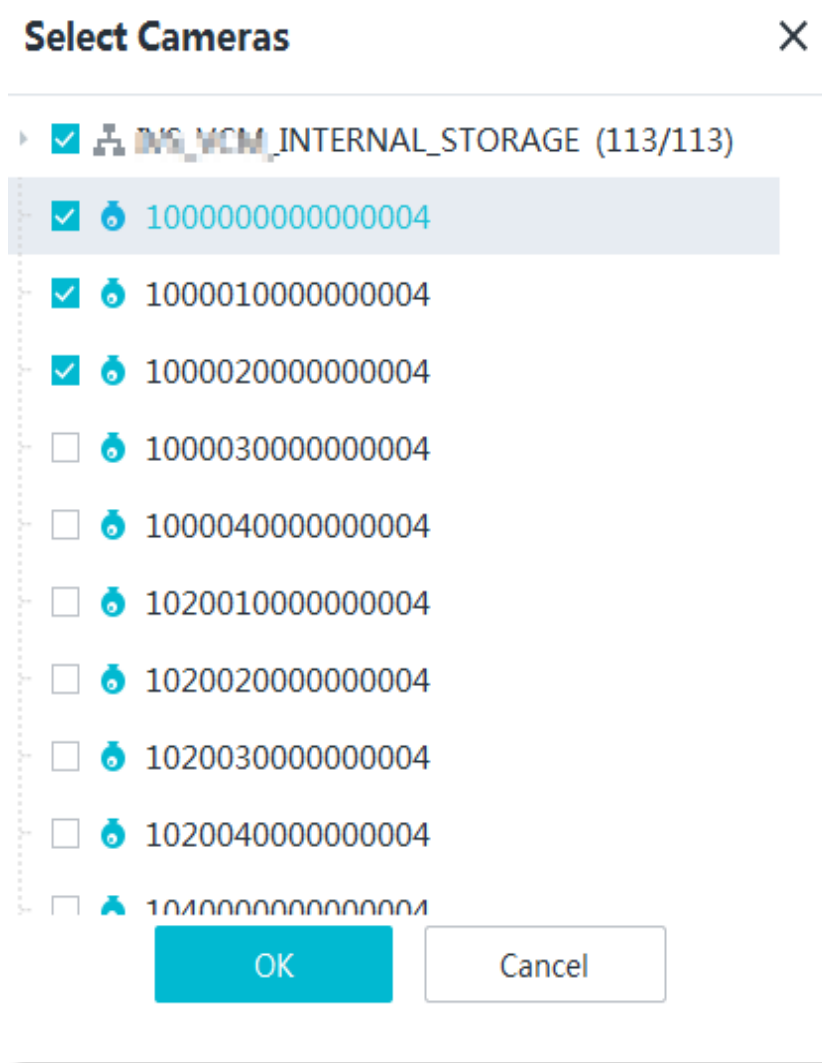
- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click a device and choose **Storage Management**.
- Step 3** Click the **Server Recording Plan** tab. The tab page for configuring a server recording plan is displayed.
- Step 4** Configure server recording plans.
 - Configure a server recording plan.
 - a. In the **Cameras** area on the left, select a camera whose recording storage policy has been configured.
 - b. In the **Server Recording Plan** area on the right, click  next to **Enable Recording**, as shown in [Figure 5-25](#).

Figure 5-25 Creating a recording plan



- c. Drag the slider on the timeline to select a time segment for executing the server recording plan.
If you click **Continuous**, you do not need to select a recording time segment.
- d. Click **Save**.
- Configure server recording plans in batches.
 - a. After configuring a server recording plan, click **Apply to Others**.
 - b. Select a batch of cameras for which you want to configure the same recording plan, as shown in [Figure 5-26](#).

Figure 5-26 Configuring server recording plans in batches



- c. Click **OK**.

----End

5.3.4 Configuring Manual Local Recording

You can manually record video during live video viewing and store the recorded video to the computer where the iClient S100 client is installed.

Prerequisites

The recording storage path has been set. For details, see [7.1 Local Settings](#).

Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Double-click an online camera in **Devices** or drag an online camera to a live video pane. The live video is played.

NOTICE

During live video viewing, ensure that no window or dialog box of another program overlaps the video pane that is playing live video. The overlap may cause artifacts or even frozen images.

Step 3 Right-click the live video pane and choose **Recording** from the shortcut menu, or click  in the live video pane. The  icon turns blue, indicating that the iClient S100 starts recording video.

Right-click the live video pane and choose  from the shortcut menu, or click . Then, the  icon turns gray, indicating that the iClient S100 stops recording video.

----End

5.3.5 Recording Playback

You can play back recordings on the iClient S100. You can also perform related operations during recording playback.

Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Playback**.

Step 2 Set recording playback parameters.

1. Select a camera whose recordings are to be played back in **Devices**.
Alternatively, click  to set search criteria, and obtain the camera whose recordings are to be played back.
2. In the recording search area, set search criteria, as shown in [Figure 5-27](#). [Table 5-23](#) describes the parameters.

Figure 5-27 Recording search

Table 5-23 Recording search parameters

Parameter	Description
Period	Time segment for recording search. The default time segment is 00:00:00-23:59:59 of the current day. Recordings in any time segment within the latest 30 days can be searched.
Scheduled/Manual/Common alarm-triggered	Recording type. - Scheduled recording: Video recorded based on a recording plan is stored on the server disk. For details about how to configure a scheduled recording plan, see 5.3.3.2 Configuring Scheduled Recording. Currently, the iClient S100 supports only scheduled recording for the IVS1800. By default, global recording is enabled on the NVR800. You do not need to enable scheduled recording on the iClient S100. - Manual recording: You can click  on the video preview page to perform manual recording (manual recordings are stored on the computer where the iClient S100 is installed) or download recordings from the server and save them to the local host during recording playback. - Common alarm-triggered recording: When the alarm linkage action is set to recording for a device and alarms are triggered, the system performs alarm-triggered recording. By default, data is stored on the hard disk of the server.

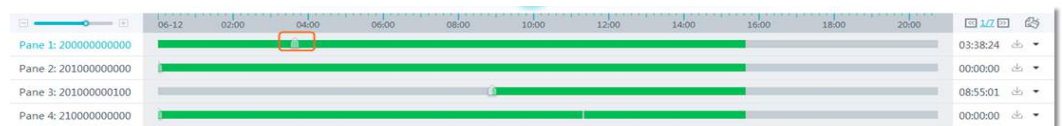
Parameter	Description
Storage Location	Recording storage location. The options are as follows: – Server: Search for video files stored on hard disks of the IVS1800/NVR800. Video files can be stored on the server after scheduled recording is performed on the iClient S100 or stored on the local host after the server is connected to cameras. – Local: Search for recordings generated during manual recording triggered on the live video viewing page and stored on the local computer.

3. Click **Search**.

The recording search result is displayed in the timeline area under the recording playback window.

4. Drag the slider on a timeline to select the playback start time, as shown in [Figure 5-28](#).

Figure 5-28 Recording playback



NOTE

- Each recording playback pane maps the timeline of a camera. If the number of cameras is greater than the number of recording playback panes, you can click the page-up or page-down button on the right of the timeline area to view the timelines of more cameras and play back their recordings.
- Play back recordings on a gigabit network. If the network bandwidth is lower than 1000 Gbit/s, artifacts or video stuttering may occur.
- If you want to change the layout of recording playback panes, select and load the video again.

5. (Optional) Cyclically play back recordings.

- In the timeline area of the search result, click  on the right and click **Loop**.
- On the timeline of the recording to be played cyclically, click the timeline and drag to select a time segment. Click . The selected recording is played cyclically in the playback window.

Click  on the right of the time line to cancel cyclic playback.

6. (Optional) Play back recordings by segment.

- Click  in the lower left corner of the live video pane.

- b. In the dialog box that is displayed, segment a recording into multiple video clips by time segment and play the video clips in multiple video panes simultaneously.

 NOTE

Enabling segment-based playback will automatically stop all recordings that are being played.

----End

5.3.6 Recording Download

5.3.6.1 Setting Recording Download Parameters

Personal Settings

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Personal Settings**.
- Step 2** Set recording download parameters. [Table 5-24](#) describes the parameters.

Table 5-24 Parameter description

Parameter	Description
Default Clip Length (5 min - 48 hours)	Default duration of a video clip that is manually recorded. This parameter applies to both manual local recording and manual server recording.
Split Files Every	Mode for splitting a single recording into several smaller data files. This parameter applies to manual local recording and recording download without encryption. The options are as follows: • Time (min): A single recording is split by time. • Capacity (MB): A single recording is split by storage space.
Reserved Space (MB)	Minimum disk space for storing recordings. To ensure that recordings can be stored correctly, the available disk space must be greater than the minimum disk space.
Space Limit Warning (MB)	Disk storage threshold for triggering an alarm. During video recording, when the available disk space is less than the value of this parameter, the system generates an alarm. In addition, the value of this parameter must be greater than that of Reserved Space .
Format	Video file storage format. The default format is MP4 .

Parameter	Description
Naming Format	Rule for naming a recording file. This parameter applies to manual local recording and recording download. The options are as follows: • Camera name_No._Time (YYYY-MM-DD-hh-mm-ss) • Camera name_Time (YYYY-MM-DD-hh-mm-ss)_No. • Time (YYYY-MM-DD-hh-mm-ss)_Camera name_No.
Download Threads	Maximum number of recordings that can be downloaded at the same time.
Download Speed (from Server)	Download speed. Server-based recordings can be downloaded at 1/4, 1/2, or 1x camera bit rate, or high speed (maximum speed that the server, client, and current network can bear). If the bit rate is 4 Mbit/s, 1/4 of it is 1 Mbit/s.
Skip Losses Under (s)	Maximum time interval for ignored interruption. During recording search, if the recording is interrupted for a specified period that is less than the value of this parameter, the recording is played as a complete recording without any interruption.

Step 3 Click **Save**.

----End

Local Settings

Step 1 On the iClient S100 home page, choose **Maintenance Management > Local Settings**.

Step 2 Set **Download Server-based Recordings to** under **Recording Directories**, and click **Save**.

----End

5.3.6.2 Configuring Recording Download

You can download recordings from the server and PUs to your local computer for later viewing. This function is sensitive. Therefore, you are advised to implement control on recording download, for example, control the content, quantity, size, and download time of recordings.

On the iClient S100, you can download recordings in either of the following ways:

- Search for recordings on the **Playback** page and download the recordings. For details, see [Downloading Recordings on Recording Playback Page](#).
- Choose **Basic Operations > Media > Recordings**, search for recordings by criteria, and download the recordings. For details, see [Downloading Recordings On the Networked Video Page](#).

NOTE

- All export and import functions can be used only in the following environments:
 - The WPS Office software is used by default.
 - The Microsoft Office software (later than Microsoft Office 2007) is installed properly. The legal license is activated and can run properly.
- You are advised to use professional video or image editing tools to shield irrelevant persons in downloaded or exported video or images and meet the HD requirements of the data subject. The recommended procedure is as follows:
 1. Download the required video to the local computer and decompress it to common video or export image data to the local computer.
 2. Use a video or an image editing tool to anonymize irrelevant targets and only retain the HD part of the data subject.
 3. Export the anonymized video or images to meet the data transfer requirements of the data subject.
 4. To ensure personal information security, delete the downloaded or exported images and recordings in a timely manner.

Downloading Recordings on Recording Playback Page

- Step 1** On the iClient S100 home page, choose **Basic Operations > Playback**.
- Step 2** Select a camera whose recordings are to be downloaded in **Devices**.
- Step 3** In the recording search area, set search criteria and click **Search**.
- Step 4** In the search result, click  on the right of a timeline and click **Download** to switch to the recording download.
- Step 5** Drag the slider on the timeline to select time segments for recording download, as shown in [Figure 5-29](#).

Figure 5-29 Selecting time segments



- Step 6** Download the recordings to a local directory.
- Recording download
 - a. Click .
 - b. Set **Video** and Click **OK** to download the recording generated in the selected time segment to the specified local directory.
 - Batch download

Click  to download recordings of multiple time segments of the current camera to the specified local directory. You can also download encrypted recordings of multiple time segments of the current camera to the specified local directory.
- Step 7** On the iClient S100 client home page, choose **Basic Operations > Media > Downloads > All** and view the recording download progress.

After the download is complete, go to the local directory to view the downloaded recordings.

 NOTE

- If the encoding format of the downloaded recording is H.265, it is recommended that the recording be played back by the VLC player.
- If the network condition is poor, the camera bit rate is high, and UDP is used for data transmission between the local domain and the external domain, packets may be lost when you download recordings from an external domain at a high speed.
- Recordings whose encoding format is MJPEG cannot be downloaded.

----End

Downloading Recordings On the Networked Video Page

Step 1 On the iClient S100 home page, choose **Basic Operations > Media > Recordings**.

Step 2 Set search criteria and click **Search**. [Table 5-25](#) describes the search parameters.

Table 5-25 Search parameters

Parameter	Description
Camera	Camera used for recording search. You can select cameras from the device list or on the map.
Period	Period used for recording search. In this case, the search result varies according to the recording type. • When Recording Type is set to Scheduled, Normal alarm triggered, or Manual, recordings whose time spans intersect with the value of Period are displayed in search results. • When Recording Type is set to Bookmarked, recording bookmarks attached during the specified recording time in Period are displayed in search results.
Recording Type	Recording type used for recording search.

Step 3 Download the recordings to a local directory.

1. On the timeline of the camera whose recordings need to be downloaded, select the recording segments to be downloaded and click .
2. Set **Video** and **Save Path**.
3. Click **OK** to download the recordings generated in the selected time segments to the specified local directory.
4. (Optional) Download recordings in batches. Select the cameras whose recordings need to be downloaded (multiple cameras can be selected), select the recording segments to be downloaded, and click  in the upper right

corner to download recordings of multiple time segments to the local computer.

 NOTE

If you do not select recording segments, all recordings from the current camera are downloaded by default.

----End

5.4 Video Wall

5.4.1 Configuring a Video Wall

5.4.1.1 Application Scenario

You can use the iClient S100 to push live or recorded video to a video wall for viewing. To display video on the video wall, you need to set decoder parameters, create a video wall layout on the iClient S100, add a decoder to the iClient S100, and bind decoder channels to panes on the video wall.

For example, if personnel in a security room need to view live video from multiple cameras in the building at the same time, they can configure a decoder and a video wall layout so that live video can be displayed on the video wall to facilitate management.

5.4.1.2 Configuring a Decoder for Video Display on a Video Wall

Prerequisites

- You have connected a decoder to the video wall.
- To ensure continuous streaming on the video wall, ensure that the network between the decoder and the IVS1800/NVR800 is normal.

 NOTE

When the iClient S100 is connected to the NVR800, only the Pearmain PEMXP70 and Jovision DEC6109 decoders can be used.

When the iClient S100 is connected to the IVS1800, supported decoders vary depending on the iClient S100 version. The details are as follows:

- When the **iClient S100 of V1.3.0 or a later version** is connected to the IVS1800, only the Pearmain PEMXP70 and Jovision DEC6109 decoders can be used.
- When the **iClient S100 of a version earlier than V1.3.0** is connected to the IVS1800, the DEC6108, Pearmain PEMXP70, and Jovision DEC6109 decoders can be used.
- If the iClient S100 is upgraded from an earlier version to V1.3.0 and the DEC6108 decoder is required, you are advised to download and use the [iClient software](#) to configure and operate the decoder. For details about the configuration and operation methods, see the iClient product documentation.

Setting the Service Parameters of a PEMXP70 Decoder

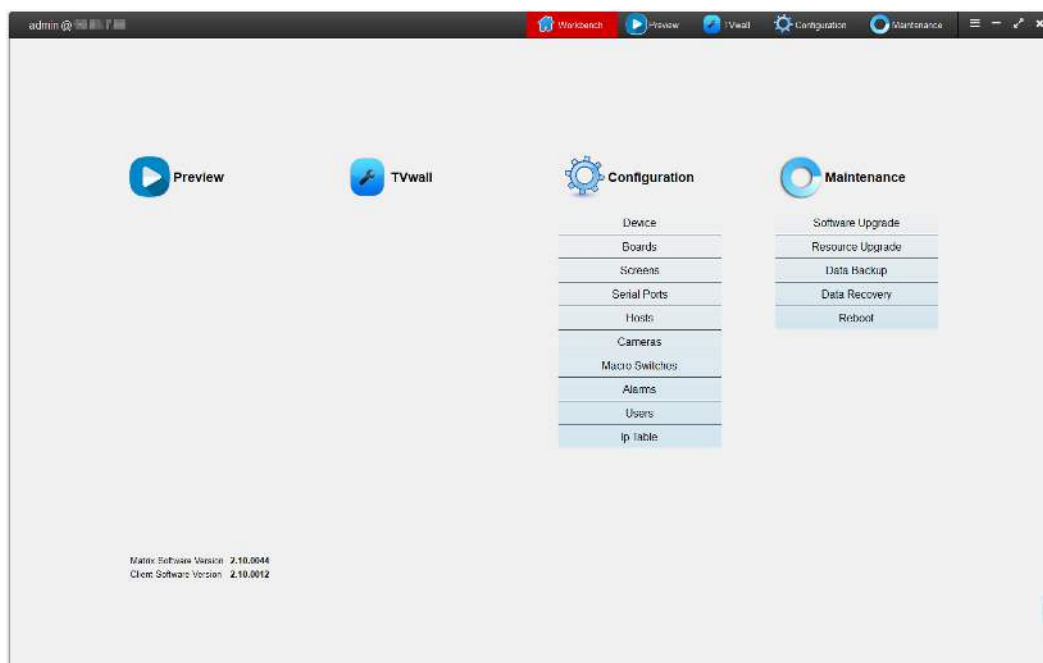
- Step 1** Start the IP MATRIX CLIENT, and enter the IP address (**192.168.0.70** by default), user name (**admin** by default), and password (**12345** by default), as shown in [Figure 5-30](#).

Figure 5-30 Login page



- Step 2** Click **LOGIN**. The home page of the client is displayed, as shown in [Figure 5-31](#).

Figure 5-31 Home page of the client



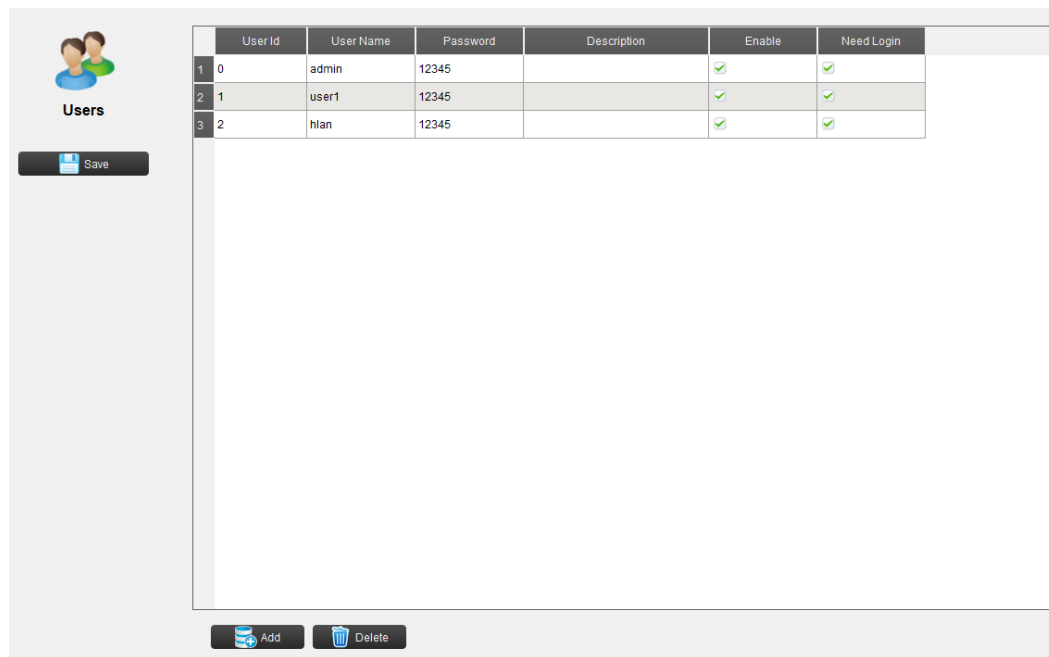
- Step 3** Choose **Workbench** > **Configuration** > **Users**. The user configuration page is displayed, as shown in [Figure 5-32](#).

On this page, you can add and delete users, and change user names and passwords.

 NOTE

- By default, the user ID of the administrator is **0**, the user name is **admin**, and the password is **12345**. The user ID and user name cannot be changed.
- For system security purposes, change the password regularly. Remember the new password after the change.

Figure 5-32 User configuration page



The screenshot shows the 'Users' configuration page. On the left, there is a sidebar with a 'Users' icon and a 'Save' button. The main area contains a table with the following data:

	User Id	User Name	Password	Description	Enable	Need Login
1	0	admin	12345		☒	☒
2	1	user1	12345		☒	☒
3	2	hlan	12345		☒	☒

At the bottom of the table, there are 'Add' and 'Delete' buttons.

Step 4 Choose **Workbench > Configuration > Ip Table**. The IP table configuration page is displayed, as shown in [Figure 5-33](#). On this page, you can set the external IP address, subnet mask, and gateway for each board in the matrix.

 NOTE

The IP addresses of all boards in the matrix must be in the same network segment. The IP address must be set for a board to connect to the network cable. Otherwise, the device will not run properly.

Figure 5-33 IP table configuration page

Ip Table

Board Id	Ip Address
1	192.168.0.70
2	
3	
4	
5	
6	
7	
8	

Mask

255.255.255.0

Gateway

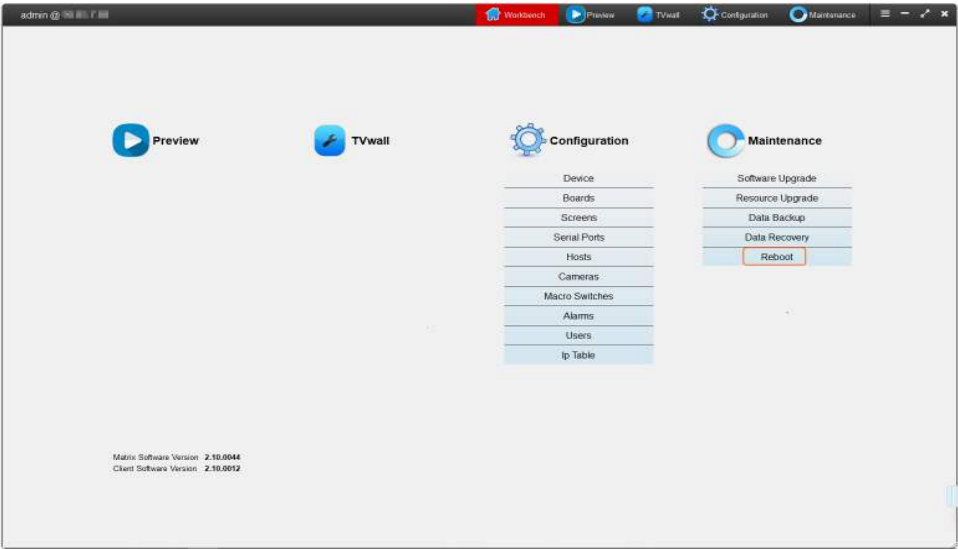
192.168.0.1

OK

Cancel

Step 5 Restart the IP MATRIX CLIENT, as shown in [Figure 5-34](#).

Figure 5-34 Restarting the client



----End

Creating a Video Wall

Step 1 Choose **Basic Operations > Video Wall** on the iClient S100 home page.

 NOTE

If decoders are stored locally, enter the passwords of all decoders.

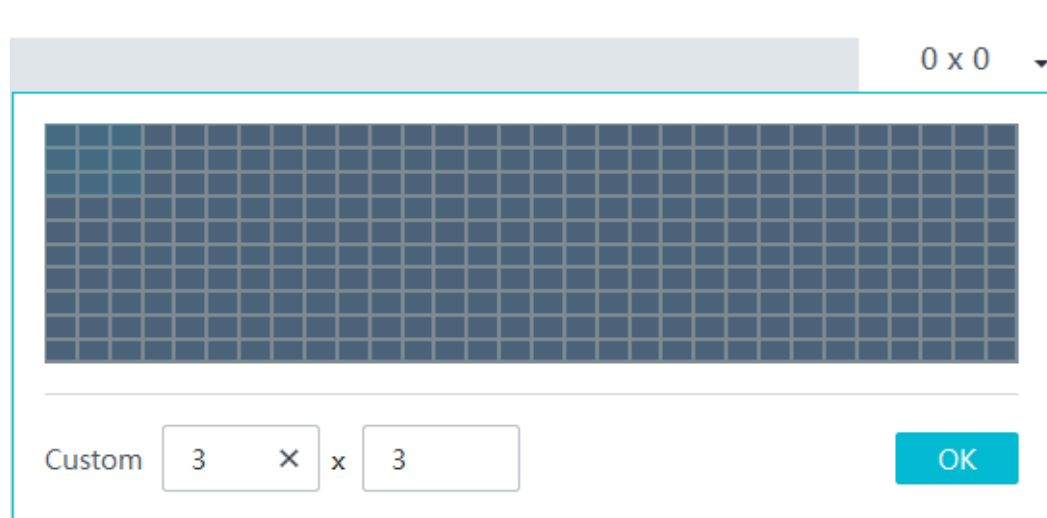
Step 2 On the page that is displayed, click **New Video Wall** or **+**. The **New Video Wall** page is displayed.

Step 3 Set **Wall Name** as required.

Step 4 Click **0 x 0** on the right of the video wall layout page. [Figure 5-35](#) shows the page that is displayed. Drag the mouse and select a layout. When you release the mouse, the layout is created.

Alternatively, you can set **Custom** to the number of columns and number of rows and click **OK** to create a layout.

Figure 5-35 Creating a video wall layout



Step 5 (Optional) If you want to customize the video wall layout on the iClient S100 to be the same as the actual one, merge panes.

To merge selected panes, drag the mouse, select several panes, and click **Merge**. To split the merged pane, select the pane and click **Split**.

Step 6 Click **Next**.

Step 7 Add decoders.

Click  next to **Decoder**. The **Add Decoders** window is displayed.

- You can add decoders one by one, as shown in [Figure 5-36](#). [Table 5-26](#) describes key parameters and buttons.

Figure 5-36 Adding decoders one by one

The 'Add Decoders' dialog box is shown. It features a table for adding decoders one by one. The table has columns for Decoder Name, IP Address, Port, Type, Verify, and Status. A red box labeled '1' points to the '+ Add' button. A red box labeled '2' points to the first row of the table, which contains 'Device 1', '192.168.1.10', '10200', 'PEMXP70', 'admin', and a password field. A red box labeled '3' points to the 'User Name', 'Password', and 'Batch Verify' fields at the bottom. A red box labeled '4' points to the 'Add' button at the bottom. Below the 'Batch Verify' field is an info message: 'Info: Remember to change the initial password and update it regularly.'

Table 5-26 Parameters and buttons for adding decoders one by one

Parameter/ Button	Description
IP Address	IP address of the decoder.
Port	Port number of the decoder. Set this parameter to 10200 (for the PEMXP70 decoder) or 28000 (for the DEC6109 decoder).
Type	Decoder model. The options are PEMXP70 (Pearmain) and DEC6109 (Jovision).
User Name	- If each decoder uses a unique service user name and password for registration, enter the service user name and password in each decoder record separately and click Verify. - If different decoders use the same service user name and password for registration, enter the service user name and password at the bottom of the window and click Batch Verify.
Password	
Verify/Batch Verify	
Add	If Verification succeeded is displayed, decoder registration is successful. Button for adding decoders. New decoders are displayed in the Decoder pane.

- You can add decoders in batches, as shown in [Figure 5-37](#). [Table 5-27](#) describes key parameters and buttons.

Figure 5-37 Adding decoders in batches

Add Decoders

Buttons: + Add, Export, Import, Delete

Decoder Name	IP Address	Port	Type	Verify	Status
device1	192.168.1.10	10200	PEMXP70	User Name: Password: Verify	Not ver
device2	192.168.1.11	10200	PEMXP	User Name: Password: Verify	Not ver
device3	192.168.1.12	10200	PEMXP	User Name: Password: Verify	Not ver

Info: Remember to change the initial password and update it regularly.

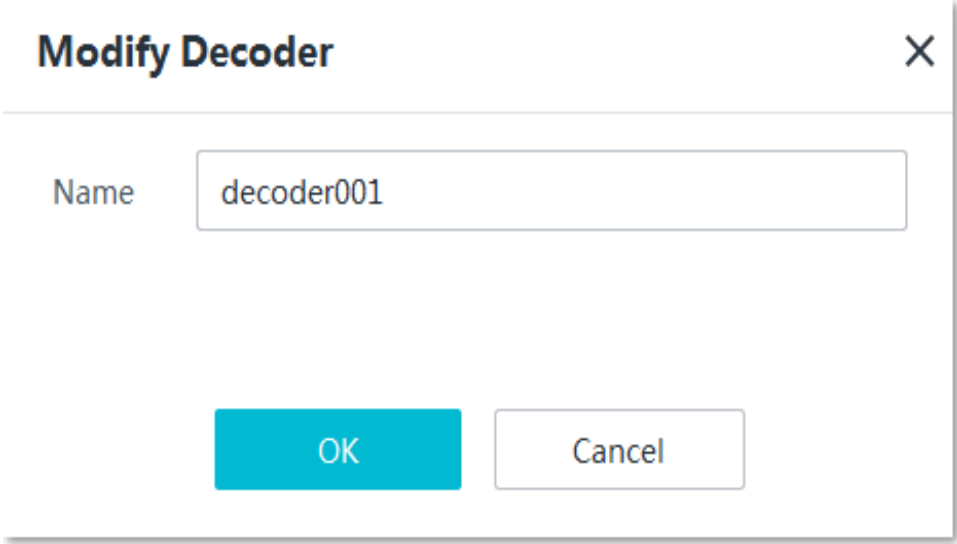
Buttons: User Name: Password:

Table 5-27 Parameters and buttons for adding decoders in batches

Parameter/ Button	Description
Export	Used to export the .csv file to the local computer. You can open the .csv file, enter decoder information, and save the file.
Import	Used to import the .csv file containing decoder information to the iClient S100.
Port	Port number of the decoder. Set this parameter to 10200 (for the PEMXP70 decoder) or 28000 (for the DEC6109 decoder).
Type	Decoder model. The options are PEMXP70 (Pearmain) and DEC6109 (Jovision).
User Name	- If each decoder uses a unique service user name and password for registration, enter the service user name and password in each decoder record separately and click Verify. - If different decoders use the same service user name and password for registration, enter the service user name and password at the bottom of the window and click Batch Verify. If Verification succeeded is displayed, decoder registration is successful.
Password	
Verify/Batch Verify	
Add	Button for adding decoders. New decoders are displayed in the Decoder pane.

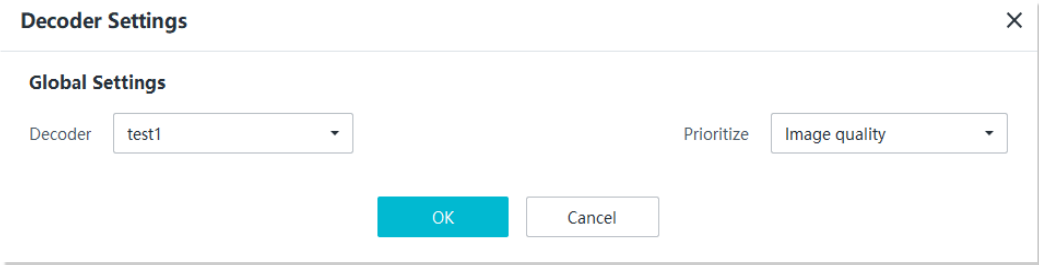
Step 8 (Optional) Change a decoder name.

1. In the **Decoder** pane, select a decoder whose name is to be changed and click . The window shown in [Figure 5-38](#) is displayed.

Figure 5-38 Modify DecoderA dialog box titled "Modify Decoder" with a close button (X) in the top right corner. It contains a text input field labeled "Name" with the value "decoder001". At the bottom, there are two buttons: "OK" (blue) and "Cancel" (white with blue border).

2. Set **Name** and click **OK**.

Step 9 Select a decoder, click  on the right of **Decoder** to configure the decoder playing mode, as shown in [Figure 5-39](#). [Table 5-28](#) describes the key parameters.

Figure 5-39 Decoder SettingsA dialog box titled "Decoder Settings" with a close button (X) in the top right corner. It has a section labeled "Global Settings". Inside this section, there is a "Decoder" dropdown menu with "test1" selected, and a "Prioritize" dropdown menu with "Image quality" selected. At the bottom, there are two buttons: "OK" (blue) and "Cancel" (white with blue border).**Table 5-28** Decoder parameters

Parameter	Description
Prioritize	• Image quality: video with more caching and a longer delay. • Smoothness: video with less caching and a shorter delay.

- Step 10** Drag decoder channels to idle video panes. To unbind channels from video panes, click **Unbind Selected** or **Unbind All** in the upper right corner.
- Step 11** (Optional) If the customized video wall layout is different from the actual physical video wall layout, you can merge or split the video wall panes to adjust their sizes.
- **Merge**: Drag the mouse to select the panes to be merged and click **Merge**.

- **Split:** Click the video pane to be split and click **Split**.

Step 12 Click **Save**.

----End

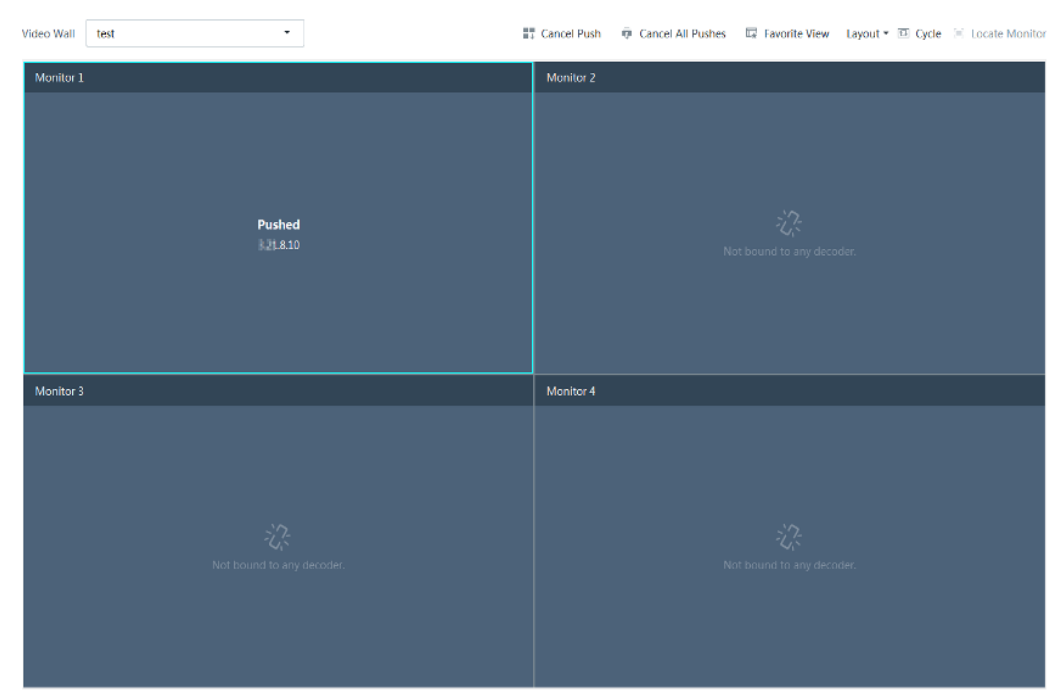
5.4.1.3 Verification

Step 1 Choose **Basic Operations > Video Wall** on the iClient S100 home page.

Step 2 On the **Set Decoder Password** page that is displayed, enter the passwords of all decoders and click **OK**.

Step 3 On the video wall page that is displayed, drag a camera whose video is to be displayed to a video pane, as shown in [Figure 5-40](#).

Figure 5-40 Video wall page



Step 4 View live video on the video wall.

----End

5.4.2 Live Video Viewing on Video Walls

Prerequisites

The administrator has created a video wall layout and connected the video wall to a decoder. For details, see [5.4.1 Configuring a Video Wall](#).

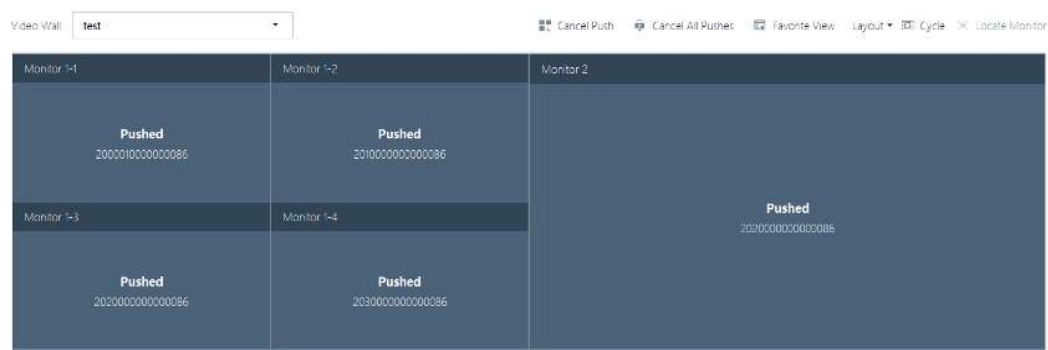
Live Video Display on the Video Wall

Step 1 On the iClient S100 home page, choose **Basic Operations > Video Wall**.

- Step 2** Double-click the created video wall to go to the **VideoWall** page.
- Step 3** Select the created video pane layout of the video wall from the **Video Wall** drop-down list box.
- Step 4** Select a video pane that is bound to a decoder channel and click **Layout**. You can select **1, 4, 8, 9, 16, 25, or 36** from the drop-down list box.

You can set **Layout** to specify the number of sub panes in a single video pane. Each sub pane can play the live video from a camera. [Figure 5-41](#) shows a 4-pane window as an example.

Figure 5-41 Layout



- Step 5** (Optional) Preview the video image of a camera if you need to know the video shot by the camera.

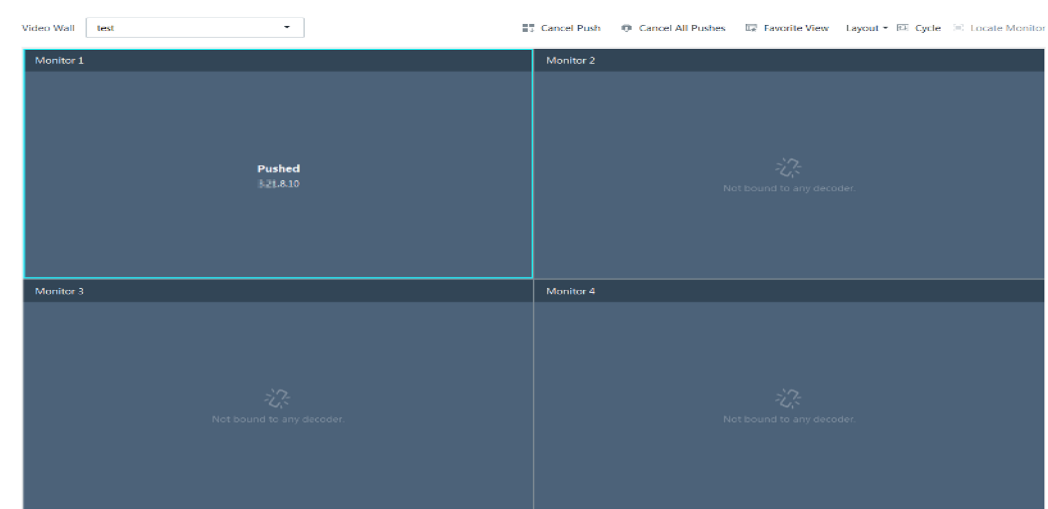
Drag the camera to **Preview Video** to view the live video shot by the camera.

Then select a video pane and click  to push the live video to the video wall.

- Step 6** Drag the camera to the video pane that has been bound to a decoder channel. [Figure 5-42](#) shows the video wall page.

You can view the live video on the video wall.

Figure 5-42 Video wall page



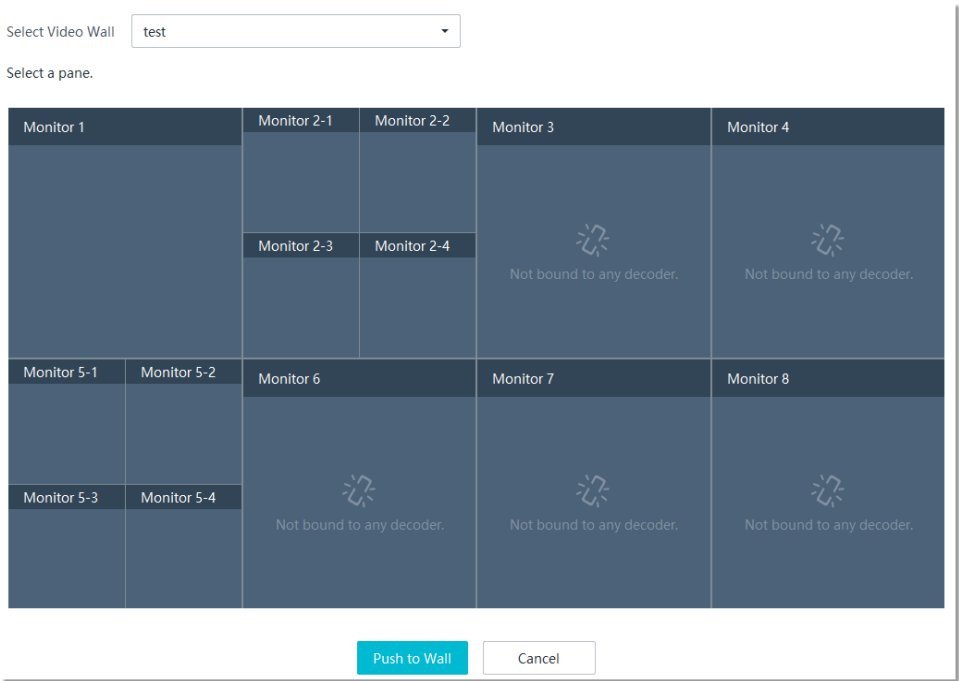
----End

Video Push to the Video Wall by One Click

- Step 1
- On the iClient S100 home page, choose **Basic Operations > Live**.
- Step 2
- Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
- Step 3
- Right-click the live video pane and choose **Push to Video Wall** from the shortcut menu.
- Step 4
- Select the created video pane layout of the video wall from the **Select Video Wall** drop-down list box.
- Step 5
- Drag the camera to the video pane that has been bound to a decoder channel.
Figure 5-43 shows the video wall page.

You can view live video from cameras on the physical video wall.

Figure 5-43 Live video display on the video wall



----End

5.4.3 Cycling on Video Walls

Prerequisites

The administrator has created a video wall layout and connected the video wall to a decoder. For details, see [5.4.1 Configuring a Video Wall](#).

Procedure

- Step 1
- On the iClient S100 home page, choose **Basic Operations > Video Wall**.
- Step 2
- On the **Set Decoder Password** page that is displayed, enter the passwords of all decoders and click **OK**.

- Step 3** Click  in the upper right corner of the page. To add a cycle group for the first time, click +. Otherwise, click **New Group**.
- Step 4** In the **Edit Cycle** window that is displayed, configure cycle group information, as shown in [Figure 5-44](#). [Table 5-29](#) describes the key parameters.

Figure 5-44 Edit Cycle window

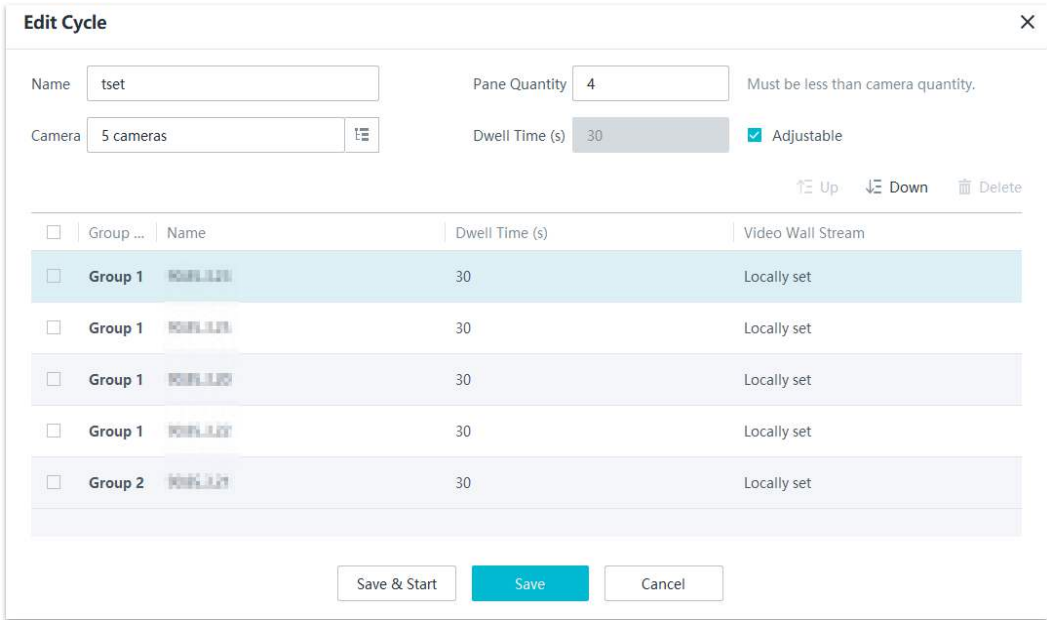
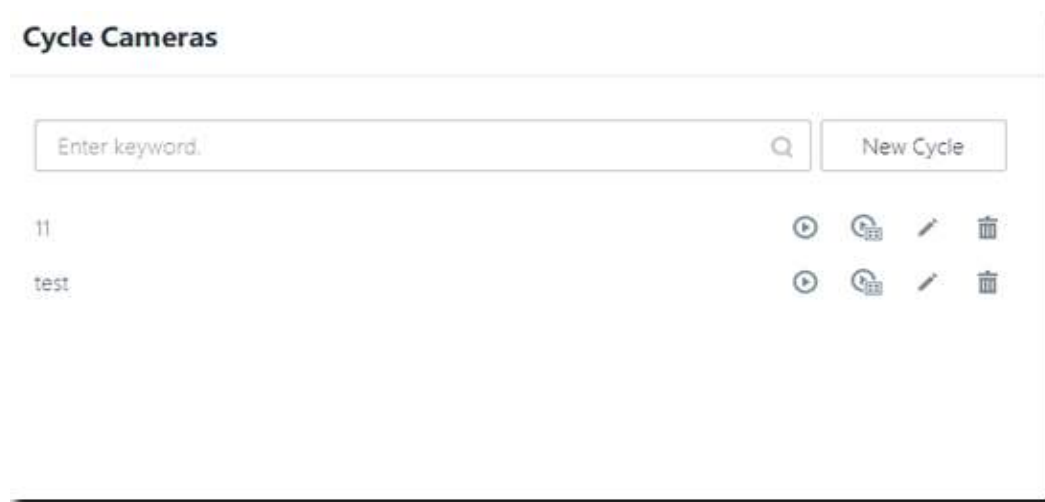


Table 5-29 Key parameters for adding a cycle group

Parameter	Description
Name	Cycle name.
Pane Quantity	Number of cycling panes, which must be less than the number of cameras to cycle.
Camera	Cameras in the cycle.
Dwell Time (s)	Dwell time at selected cameras, which can be manually adjusted. The dwell time can be configured for multiple groups in batches or for a single group. In this example, the dwell time is configured for a single group.

- Step 5** Click  in the upper right corner of the **Video Wall** tab page. The added cycle groups are displayed in the **Cycle Cameras** window, as shown in [Figure 5-45](#).

Figure 5-45 Cycle Cameras

- Click . The selected pane is regarded as the first pane. The live video from corresponding cameras is played in sequence in cycling mode. For example, if pane 2 is selected, and the number of panes is three, live video is displayed in panes 2, 3, and 4 in cycling mode.
- Click  to customize panes for live video viewing in cycling mode.

----End

5.4.4 Video Wall View Management

Application Scenario

This section describes how to configure and manage video wall views. You can add different views and view schedules and configure view cycling as planned to meet specified purposes, improving work efficiency.

Procedure

- Step 1** Choose **Basic Operations > Video Wall** on the iClient S100 home page and double-click the created video wall. The **VideoWall** tab page is displayed.

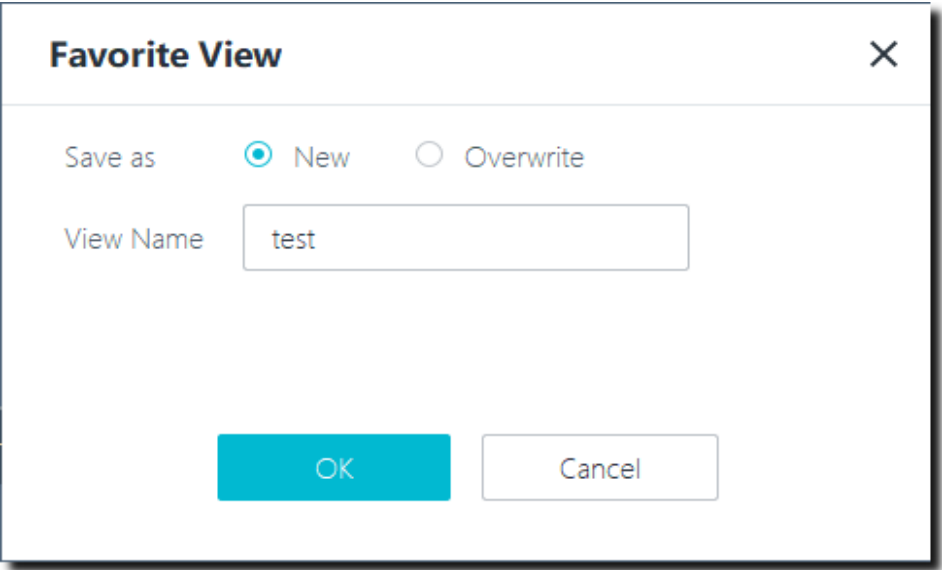
NOTE

If multiple decoders are stored locally, enter the passwords of all the decoders.

- Step 2** Add a view.

1. Choose **Favorites > Favorited Views**, click , and set **Save as** to **New** or **Overwrite**.
 - If you set **Save as** to **New**, set **View Name** and save the view.
 - If you set **Save as** to **Overwrite**, the existing view is overwritten, and the new view is saved.
2. Set **View Name** and click **OK**. The **Favorite View** window is displayed, as shown in [Figure 5-46](#).

Figure 5-46 Favorite View



3. Repeat [Step 2.1](#) and [Step 2.2](#) to save more views.

 NOTE

You can also click  Favorite View in the **Pane List** window to add a view.

Step 3 Add a view schedule.

1. Click the **Favorites** tab and view the favorited views in the **Favorited Views** panel.
2. Click  next to **Favorited Views**. The **View Schedule** page is displayed.
3. Click **New Schedule**. In the **New Schedule** window that is displayed, set view schedule parameters, as shown in [Figure 5-47](#). [Table 5-30](#) describes related parameters.

Figure 5-47 New Schedule window

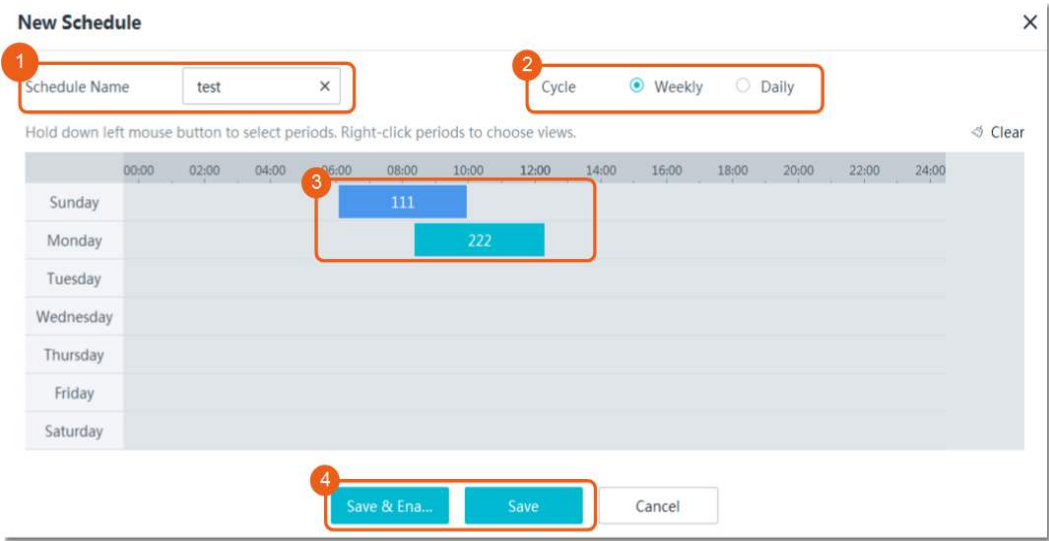
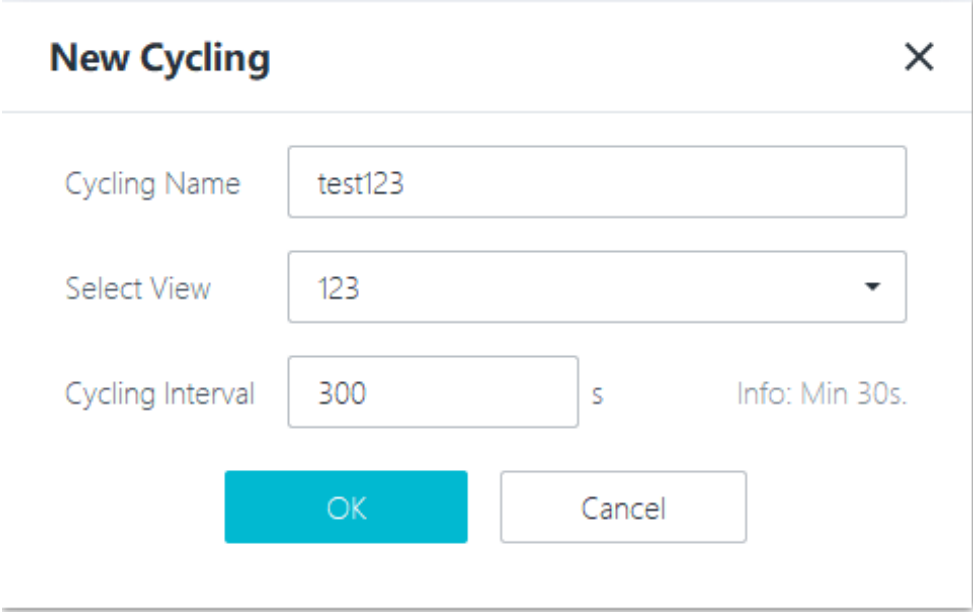


Table 5-30 Parameter description

Parameter	Description
Cycle	Cycle for executing a view schedule. In the preceding figure, this parameter is set to Weekly .
Period	Time range for playing a view. Drag the mouse to configure a specified time segment for view playing. Right-click the time segment and choose a view from the shortcut menu. Double-click the time segment and set specific time points.

Step 4 Add view cycling.

1. Click  next to **Favorited Views**. The **View Cycling** page is displayed.
2. Click **New**. In the **New Cycling** window that is displayed, set cycling parameters, as shown in [Figure 5-48](#). [Table 5-30](#) describes key parameters.

Figure 5-48 New Cycling**Table 5-31** Key parameter description

Parameter	Description
Select View	Cycling view. Select an existing view from the drop-down list box.
Cycling Interval	Video wall cycling interval.

3. Click **OK**.

----End

5.4.5 Recording Playback on the Video Wall

A recording can be played back on the video wall, facilitating historical video image viewing and unified command and dispatch.

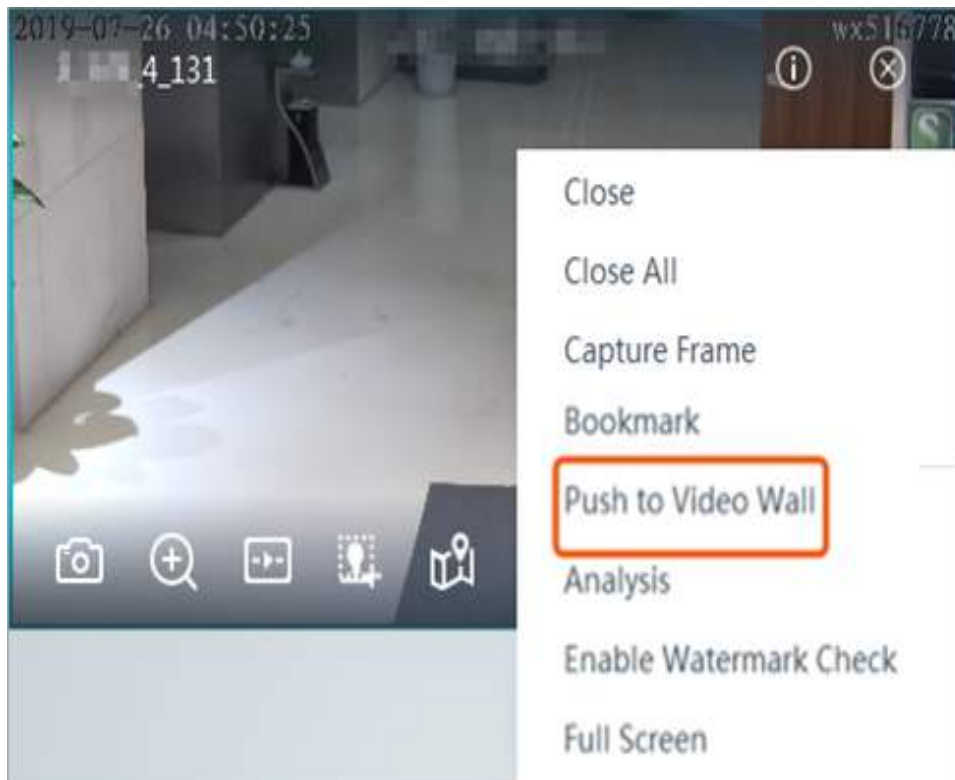
Prerequisites

The administrator has created a video wall layout and connected the video wall to a decoder. For details, see [5.4.1 Configuring a Video Wall](#).

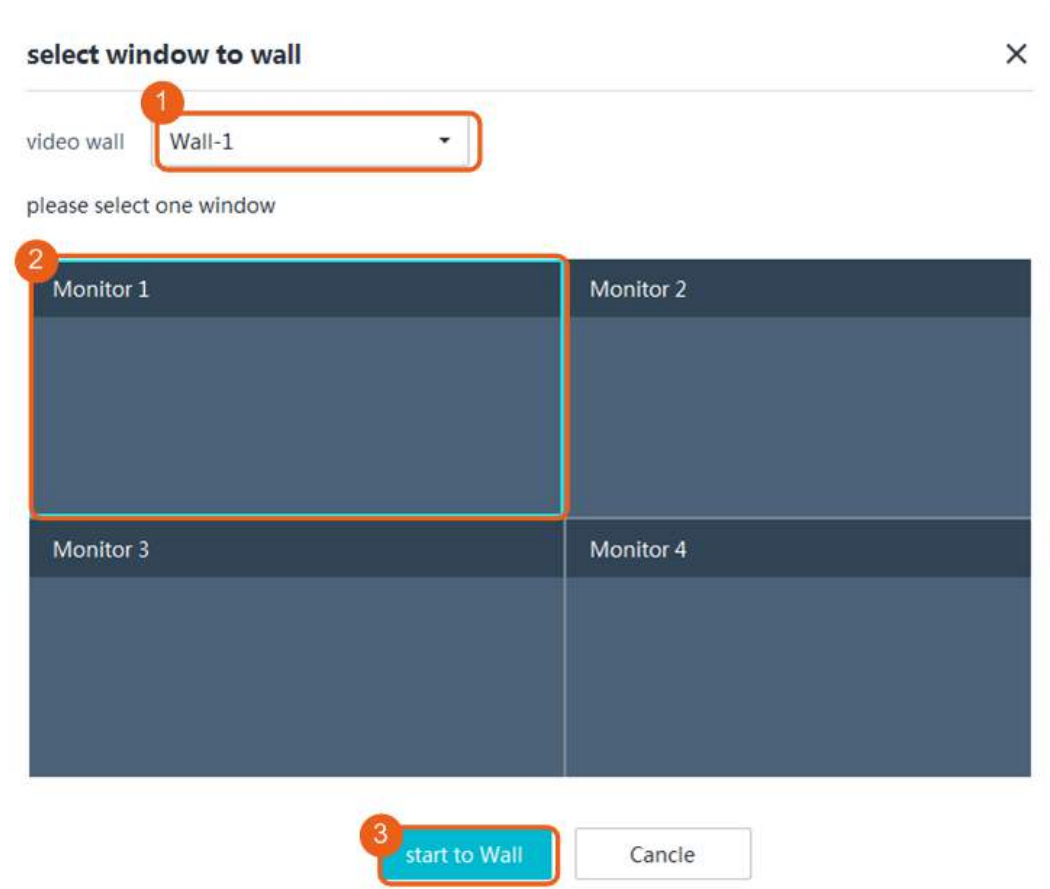
Procedure

- Step 1** On the iClient S100 home page, choose **Basic Operations > Playback**.
- Step 2** In the device list, select the camera whose recordings need to be played back on the video wall.
- Step 3** In the recording search area, set search criteria and click **Search**.
- Step 4** In the search result, drag the slider on the timeline to select the playback start time.
- Step 5** Right-click the recording playback window and choose **Push to Video Wall** from the shortcut menu, as shown in [Figure 5-49](#).

Figure 5-49 Push to Video Wall



- Step 6** On the **select window to wall** page that is displayed, select a video wall, as shown in [Figure 5-50](#).

Figure 5-50 select window to wall

If the push is successful, the recording is played back on the video wall.

Step 7 (Optional) Play back recordings from multiple cameras on the video wall at the same time.

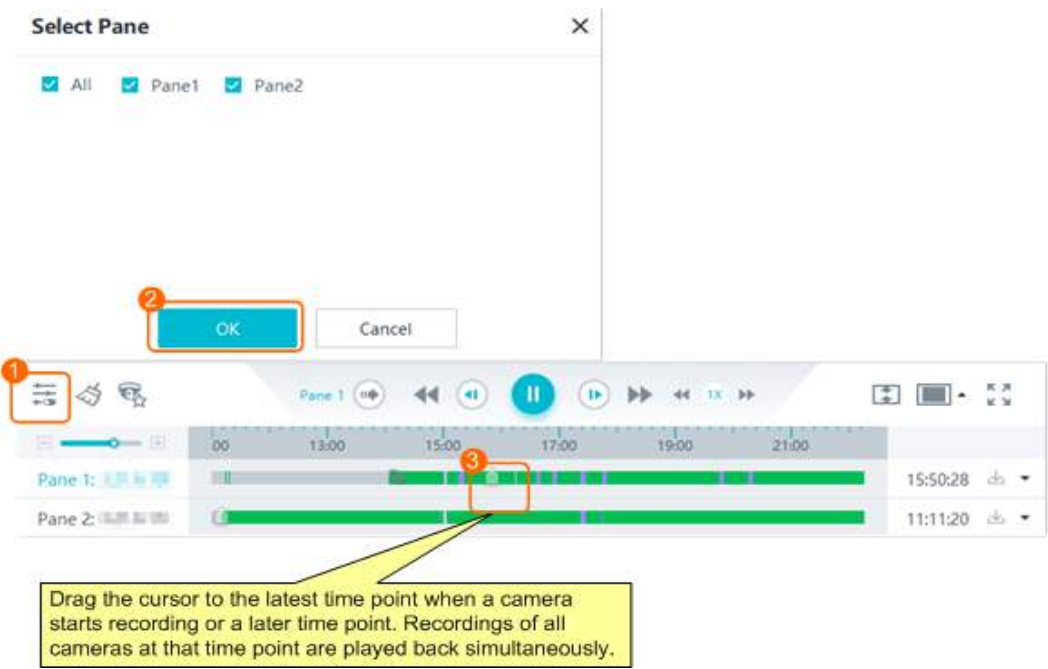
1. Repeat [Step 2](#), [Step 3](#), [Step 5](#), and [Step 6](#) to play back recordings from other cameras on the video wall.

NOTE

The video wall pane selected for each camera must be unique. Otherwise, the recordings that are being played back on the video wall will be replaced.

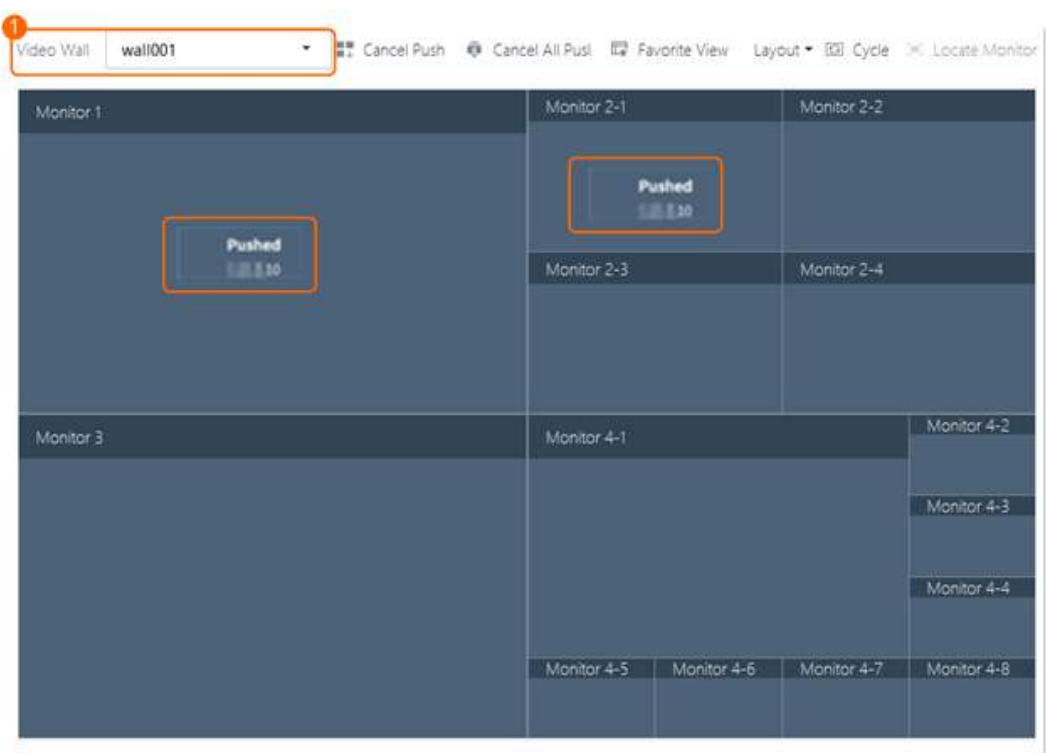
2. Configure simultaneous playback of recordings from multiple cameras, as shown in [Figure 5-51](#).

Figure 5-51 Configuring simultaneous recording playback



3. Play back recordings on the video wall.
 - a. On the iClient S100 home page, choose **Basic Operations > Video Wall**.
 - b. Play back recordings on the video wall, as shown in [Figure 5-52](#).

Figure 5-52 Playing back recordings on the video wall



On the video wall, you can view the time when the recording playback starts.

----End

5.4.6 Video Wall Window splicing

Application Scenario

Through the splicing of Video Wall windows, multiple small windows of the TV wall physical screen are combined into one large window, so as to highlight the key video pictures on the Video Wall

Prerequisites

You have created a video wall layout and connected a video wall to a decoder as an administrator. For details, see [4.4.1 Configuring a Video Wall](#).

Procedure

- Step 1** Choose **Basic Operations > Video Wall** on the iClient S100 home page and double-click the created video wall. The **VideoWall** tab page is displayed.

NOTE

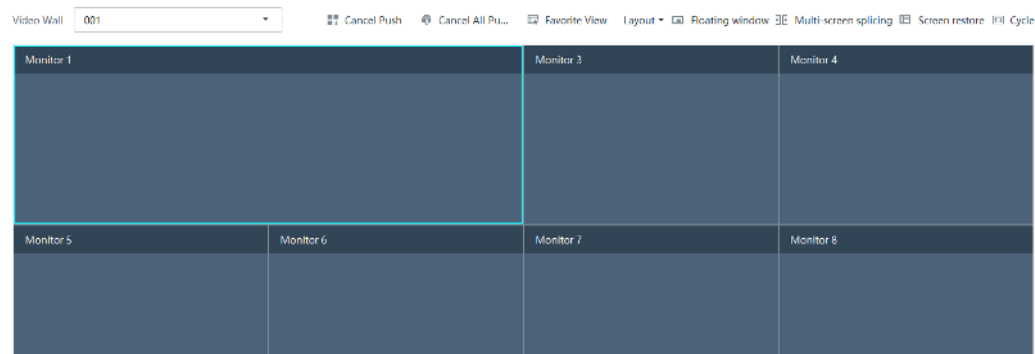
If multiple decoders are stored locally, enter the passwords of all the decoders.

- Step 2** Window splicing.

1. Create a video wall, add and bind a decoder.
2. Click **Video Wall** to enter the large screen control and select adjacent screens for splicing. Only rectangular adjacent screens can be spliced. After splicing once, it cannot be spliced again.

Figure 5-53 Before splicing window



Figure 5-54 After splicing window

-----End

5.4.7 Video Wall Floating window

Application Scenario

Open the floating window on the video wall window, and the video picture can be played on the physical screen.

Prerequisites

You have created a video wall layout and connected a video wall to a decoder as an administrator. For details, see [4.4.1 Configuring a Video Wall](#).

Procedure

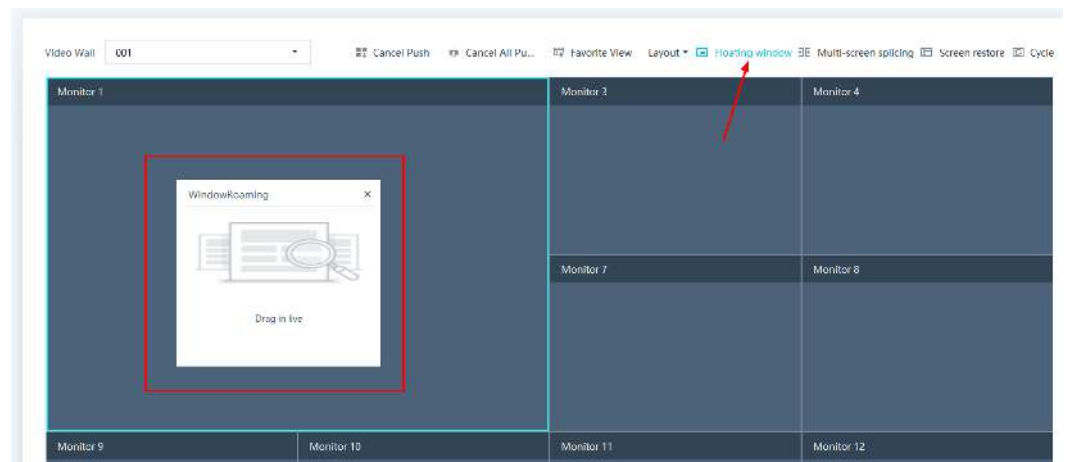
- Step 1** Choose **Basic Operations > Video Wall** on the iClient S100 home page and double-click the created video wall. The **VideoWall** tab page is displayed.

NOTE

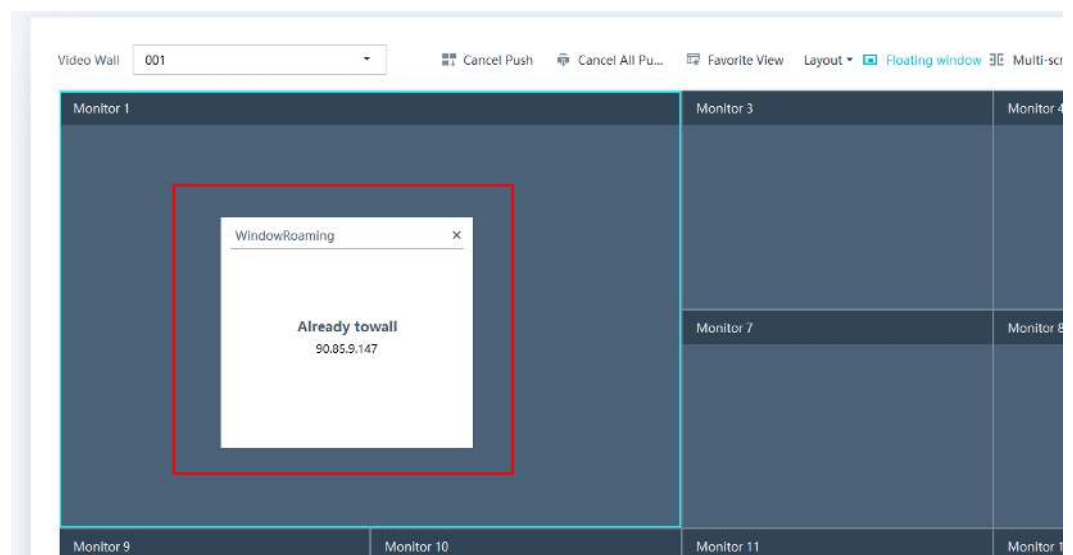
If multiple decoders are stored locally, enter the passwords of all the decoders.

- Step 2** Add a floating window.

1. Create a video wall, add and bind a decoder.
2. Click the **Floating window** to draw the floating window on the screen. When you finish drawing the floating window, you need to click **Floating window** again to restore the color of the floating window to the default color.

Figure 5-55 Draw floating window

3. After drawing the floating window, drag the left video channel to the floating window for video playback.

Figure 5-56 Play video

----End

5.4.8 Alarm linkage Video Wall

Application Scenario

For the alarm information received by the iClient S100 client, the user configures the alarm linkage on the wall according to the demand, and pops up the video channel source configured by the user on the TV wall.

Prerequisites

You have created a video wall layout and connected a video wall to a decoder as an administrator. For details, see [4.4.1 Configuring a Video Wall](#).

Procedure

Step 1 Choose **Basic Operations > Video Wall** on the iClient S100 home page and double-click the created video wall. The **VideoWall** tab page is displayed.

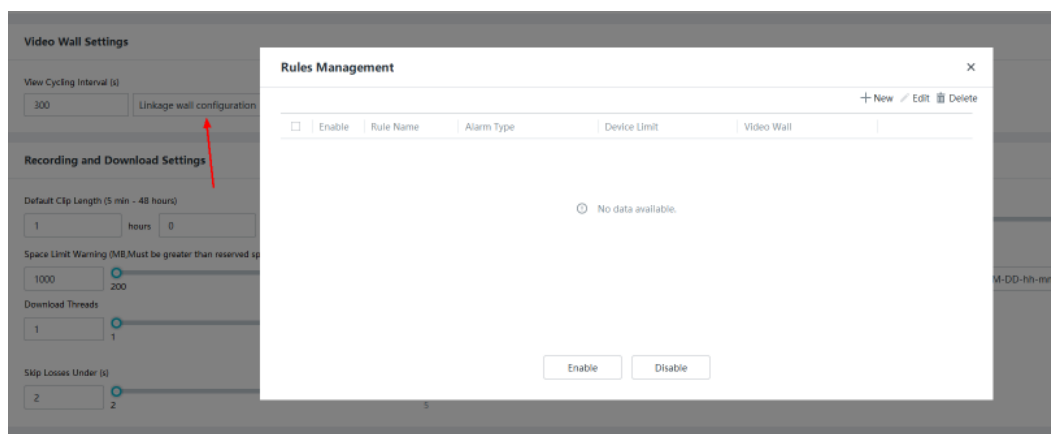
NOTE

If multiple decoders are stored locally, enter the passwords of all the decoders.

Step 2 Add one alarm linkage Video Wall rule.

1. Create a video wall, add and bind a decoder.
2. In the homepage of iclient S100, choose **Personal Configuration > Linkage wall configuration**.

Figure 5-57 Open Linkage wall configuration



3. Click New and enter the information.

Figure 5-58 Add rule

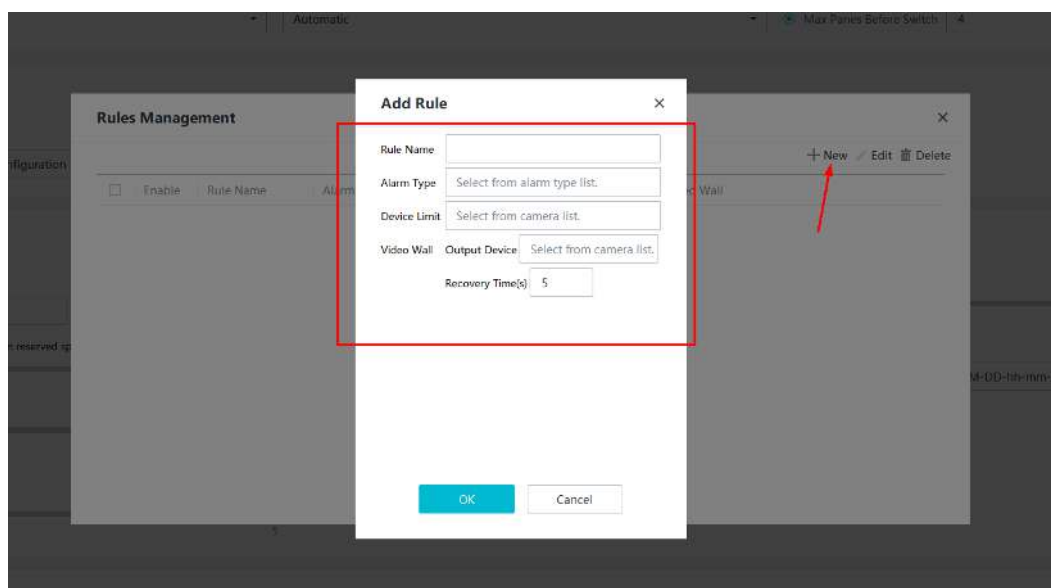
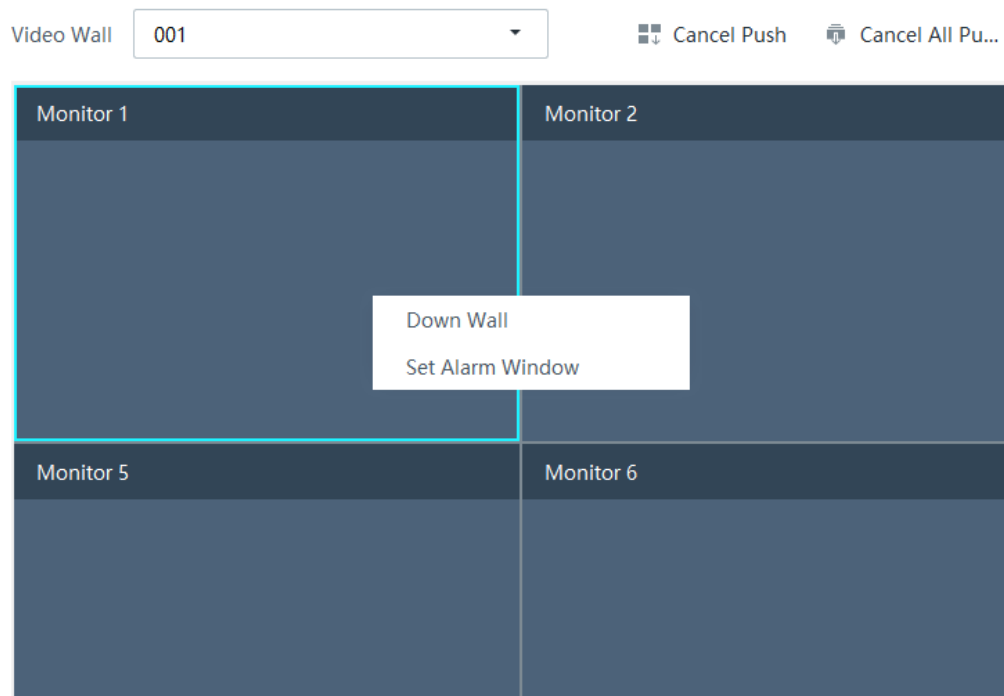


Table 5-32 Key parameter description

Parameter	Description
Rule name	User defined rule name.
Alarm Type	If the alarm type on the wall is selected, the preset alarm type on the wall will be triggered.
Device Limit	The camera managed by iClient S100 indicates that the selected camera will trigger alarm linkage to the wall.
Video Wall Output Device	The camera managed by iClient S100 indicates that after the alarm linkage is triggered, the selected output channel will be played in the TV wall alarm window in turn
Video Wall Recovery Time(s)	Indicates that after the alarm linkage video is played in the alarm window, after the recovery time, the video will automatically recover to the previously played video picture

Step 3 On the large screen control video wall page, select the video wall window and right-click to set the alarm window. After the setting is completed and the alarm linkage is triggered, the alarm output source video screen will pop up on the physical screen corresponding to the window

Figure 5-59 Set alarm window

-----End

5.5 Common Intelligence

5.5.1 Motion Detection

The system automatically generates an alarm when a motion is detected in a specified area. Security personnel can view the video image to identify harmful objects and take necessary actions.

Enable alarm linkage. For details, see [4.12.2 Alarm Linkage](#).

NOTE

- Motion detection cannot be enabled for cameras connected to main devices through ONVIF. Therefore, it is recommended that cameras be connected to main devices through HWSDK.
- The following describes the configuration on the iClient S100. For details about the configuration in the camera web system, see the camera product documentation of the required series and version.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Ordinary Intelligence > MotionDetection**.
- Step 3** Toggle-on **Enable Motion Detection**, draw a detection area, and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 5-33](#) describes the parameters.

Table 5-33 Parameter description

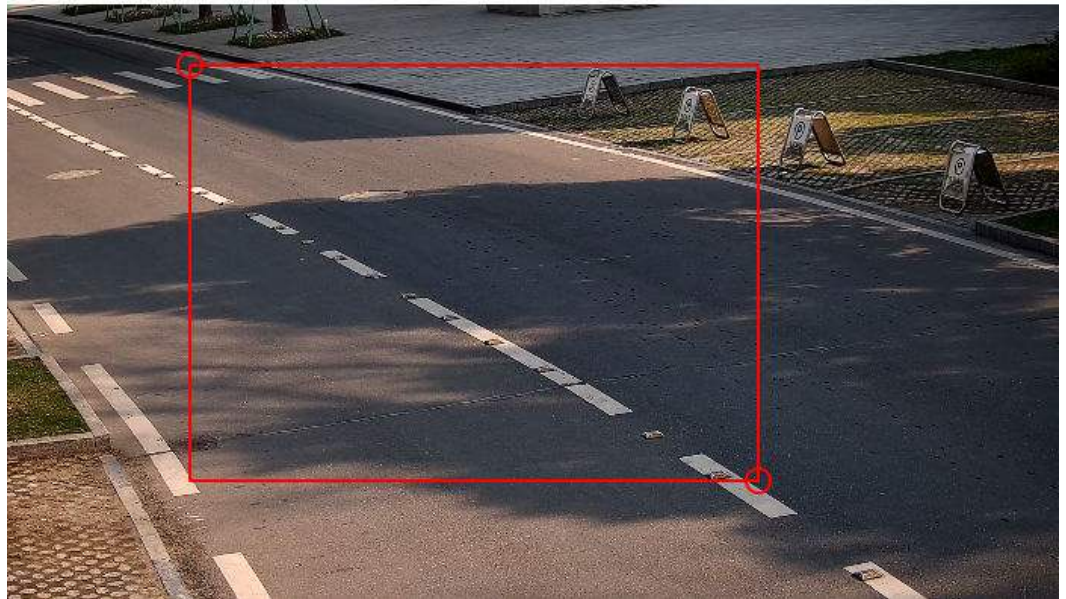
Parameter	Description
Alarm Detection Interval(s)	Interval at which the camera checks for object motion. If motion is detected, the camera reports an alarm. If an object keeps moving in the detection area, only one alarm is reported during each motion detection interval.
Sensitivity	Motion detection sensitivity. A larger value indicates a higher sensitivity. If a higher sensitivity level is used, more slight motions can be detected.

2. Set audible and visual alarm parameters. [Table 5-34](#) describes the parameters.

Table 5-34 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters, as shown in [Figure 5-60](#). [Table 5-35](#) describes the parameters.

Figure 5-60 Setting an area**▲ Area Settings**+ Area  Delete**Table 5-35** Area settings

Button	Description
+Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.

- Set plan parameters. [Table 5-36](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-36 Plan settings

Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.

Parameter/ Button	Description
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

For details about how to view the latest or historical alarms, see [4.12.1 Video Alarm](#).

5.5.2 Lens Blocking Detection

The system automatically generates an alarm when a camera lens is blocked by an object in a specified area. Security personnel can view the video image to check onsite situations and take necessary actions.

Enable alarm linkage. For details, see [4.12.2 Alarm Linkage](#).

NOTE

- Lens blocking detection cannot be enabled for cameras connected to main devices through ONVIF. Therefore, it is recommended that cameras be connected to main devices through HWSDK.
- The following describes the configuration on the iClient S100. For details about the configuration in the camera web system, see the camera product documentation of the required series and version.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Ordinary Intelligence > VideoOcclusion**.
- Step 3** Toggle-on **Enable Video Occlusion** and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 5-37](#) describes the parameters.

Table 5-37 Parameter description

Parameter	Description
Alarm Detection Interval(s)	Interval at which the camera checks for object motion. If motion is detected, the camera reports an alarm. If an object keeps moving in the detection area, only one alarm is reported during each motion detection interval.
Sensitivity	Motion detection sensitivity. A larger value indicates a higher sensitivity. If a higher sensitivity level is used, more slight motions can be detected.

2. Set audible and visual alarm parameters. [Table 5-38](#) describes the parameters.

Table 5-38 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	

Parameter	Description	Requirement on Cameras
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set plan parameters. [Table 5-39](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-39 Plan settings

Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

For details about how to view the latest or historical alarms, see [4.12.1 Video Alarm](#).

5.5.3 Privacy Mask

In scenarios where the content in some areas (such as whiteboard information in an office) may involve business secrets and should not be viewed by others (including security personnel), the privacy mask function is required. You can configure the privacy mask function in the camera web system or on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

- Step 2** Double-click a camera connected to a main device and choose **Video Channel > Privacy Mask**.
- Step 3** Set parameters for privacy mask, as shown in [Figure 5-61](#). [Table 5-40](#) describes the parameters.

Figure 5-61 Setting parameters for privacy mask

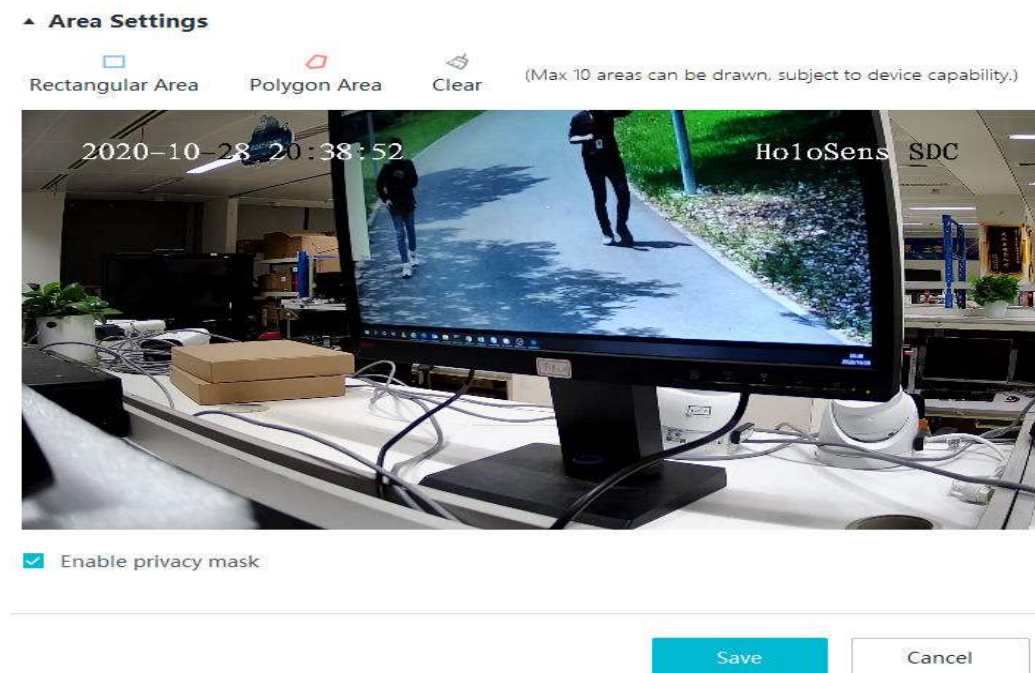


Table 5-40 Parameter description

Parameter	Description
Area Settings	You can box-select one or more rectangular areas on a video image for privacy mask. A maximum of 10 areas are allowed. NOTE You can select Polygon Area only for cameras connected through the HWSDK protocol.
Enable privacy mask	Indicates whether to enable privacy mask for the box-selected area.

- Step 4** Click **Save**.

----End

Verification

After the privacy mask is configured, you can view the result on the **Live** and **Playback** page. The following takes the **Live** page as an example.

- Step 1** On the iClient S100 home page, choose **Basic Operations > Live**.

- Step 2** View the camera image. The image in the privacy mask area cannot be viewed during live video viewing or recording playback.

----End

5.6 Behavior Analysis

5.6.1 Frontend Behavior Analysis

5.6.1.1 Function Description

The intelligent video analysis technology can be used to analyze and match the video signals captured by cameras based on preconfigured rules, decreasing the workload of observation personnel and reducing mistakes caused by negligence.

Based on the devices that execute intelligent analysis tasks, behavior analysis can be classified into frontend behavior analysis and backend behavior analysis. You can select frontend behavior analysis for a camera that supports behavior analysis and backend behavior analysis for one that does not.

- Frontend behavior analysis: Cameras themselves provide the behavior analysis function.. After you configure behavior analysis tasks on the client, the client delivers the tasks to cameras for execution.
- Backend behavior analysis: Required algorithm plug-ins should be installed on main devices to perform behavior analysis on video.

To configure frontend behavior analysis for the main device IVS1800, you need to configure behavior analysis tasks on the iClient S100 for cameras connected to the IVS1800. [Table 5-41](#) describes the frontend behavior analysis functions supported by the IVS1800.

Table 5-41 Behavior analysis functions

Behavior Analysis	Description
Tripwire crossing detection	The system automatically generates an alarm when an object crosses a tripwire from the specified direction in a specified detection area.
Intrusion detection	The system automatically generates an alarm when an object enters a specified detection area.
Abandoned object detection	The system automatically generates an alarm when an object is abandoned in a specified detection area. The system allows you to specify the shape (rectangle or polygon) of a detection area.
Removed object detection	The system automatically generates an alarm when an object is removed from a specified detection area.

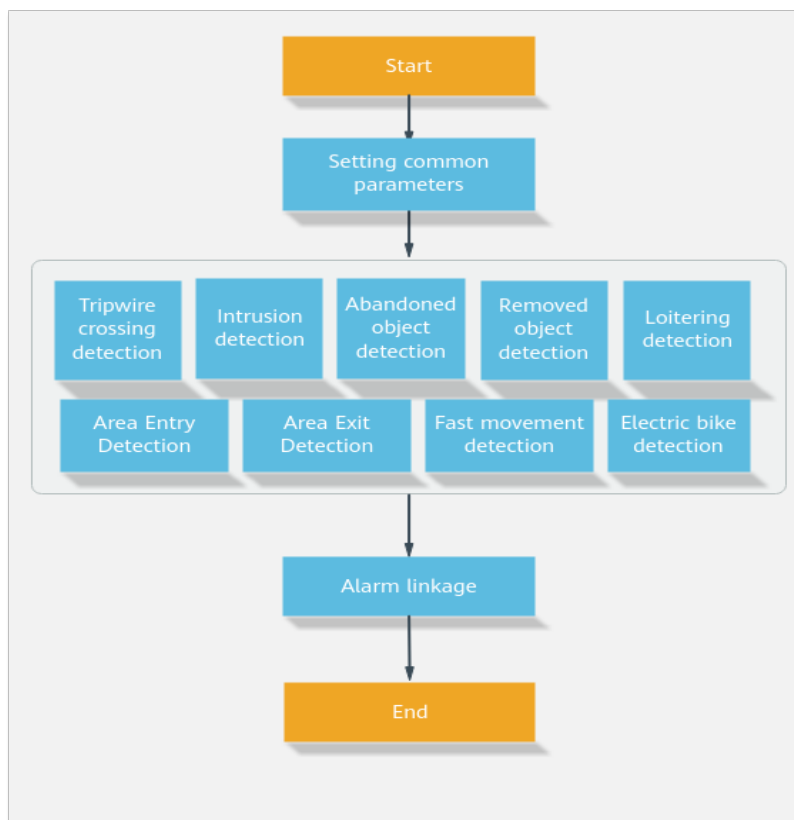
Behavior Analysis	Description
Loitering detection	The system automatically generates an alarm when a person is loitering in a specified detection area for a specified time.
Area entry detection	The system automatically generates an alarm when a person or an object enters an area that is not allowed to enter.
Area exit detection	The system automatically generates an alarm when a person or an object exits an area that is not allowed to exit.
Fast movement detection	The system automatically generates an alarm when an object moves fast to prevent security risks.
Electric bike detection	The system automatically generates an alarm when an electric bike enters a specified area.

 NOTE

- Currently, you can configure intelligent analysis tasks on the iClient S100 only for cameras that support intelligent analysis and are connected to main devices through HWSDK. In this way, alarms generated by these cameras can be reported to the iClient S100.
- This section describes the configuration on the iClient S100 as an example. For details about the configuration in the camera web system, see the camera product documentation of the corresponding series and version.

5.6.1.2 Configuration Process

Before using frontend behavior analysis, you need to configure intelligent analysis tasks for cameras that support intelligent analysis. [Figure 5-62](#) shows the configuration process.

Figure 5-62 Process for configuring frontend behavior analysis tasks**NOTE**

- Currently, you can configure intelligent analysis tasks on the iClient S100 only for cameras that support intelligent analysis and are connected to main devices through HWSDK. In this way, alarms generated by these cameras can be reported to the iClient S100.
- This section describes the configuration on the iClient S100 as an example. For details about the configuration in the camera web system, see the camera product documentation of the corresponding series and version.

5.6.1.3 Global Configuration

Before configuring behavior analysis on the iClient S100, you need to complete the global configuration.

Prerequisites

You have connected cameras that support intelligent analysis to the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Global Configuration**. The tab page shown in [Figure 5-63](#) is displayed.

Figure 5-63 Global Configuration tab page

The screenshot shows the Global Configuration tab page with the following settings:

- Enable Behavior Analysis:** Toggle switch is turned on.
- Send Metadata:** Toggle switch is turned on.
- Perimeter enhancement:** Toggle switch is turned on.
- Alarm suppression:** Toggle switch is turned on.
- Information Superimposed on Alarm Images:** Toggle switch is turned on.
- Shadow Mode:** Dropdown menu set to "Weak".
- Detection sensitivity:** Dropdown menu set to "Low".
- Background update rate:** Dropdown menu set to "Low".
- Min. object size:** Input fields set to 5 X 5.
- Max. object size:** Input fields set to 100 X 200.

1. Toggle-on **Enable Behavior Analysis** and set global parameters. [Table 5-42](#) describes the parameters.

Table 5-42 Parameter description

Parameter	Description
Send Metadata	Indicates whether to send metadata when the NVR800/IVS1800 is connected to the upper-level platform. If this function is enabled, cameras will send metadata such as snapshots and structured data to the upper-level platform. Then the upper-level platform can perform search by criteria based on the metadata sent by the main device.
Perimeter enhancement	Indicates whether to send a full image as TLV metadata.
Alarm suppression	Indicates whether to send only the alarm that is triggered for the first time.
Information Superimposed on Alarm Images	Indicates whether to superimpose the target frame and rule frame that trigger alarms on full images sent as metadata.

Parameter	Description
Shadow Mode	Shadow strength. The options are Weak , Common , and Strong .
Detection Sensitivity	Sensitivity for triggering alarms. The options are Low , Medium , and High . – A higher sensitivity indicates a higher possibility of triggering alarms, which may lead to false alarms. For example, after you set a high sensitivity for intrusion detection, a false alarm may be reported when an object passes by a sensitive area. – A lower sensitivity indicates a lower possibility of triggering alarms, which may lead to missing alarms. For example, after you set a low sensitivity for tripwire crossing detection, an alarm may not be reported when an object passes one end of a tripwire.
Background update rate	Speed of integrating an object with the background. A larger value indicates quicker object integration.
Min. object size	Minimum size of an object that can be detected on video images in the CIF (352 x 288) resolution. No alarm is generated when an object smaller than the minimum size violates the detection rules. NOTE The minimum object size supported by behavior analysis is 5 x 5 pixels (using 352 x 288 as the standard).
Max. object size	Maximum size of an object that can be detected on video images in the CIF (352 x 288) resolution. No alarm is generated when an object larger than the maximum size violates the detection rules. NOTE The maximum object size supported by behavior analysis is 200 x 200 (using 352 x 288 as the standard).

Step 4 Click **Save**.

----End

5.6.1.4 Tripwire Crossing Detection

Tripwire crossing detection is used to detect whether an object crosses the tripwire from the specified direction in a detection area. If so, an alarm is generated. Management personnel can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273283512.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see [5.6.1.3 Global Configuration](#).

Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera for which you want to configure a behavior analysis policy.

Step 3 Choose **Behavior Analysis > Tripwire** and set related parameters.

1. Set parameters in the **Parameter Settings** area. [Table 5-43](#) describes the parameters.

Table 5-43 Parameter description

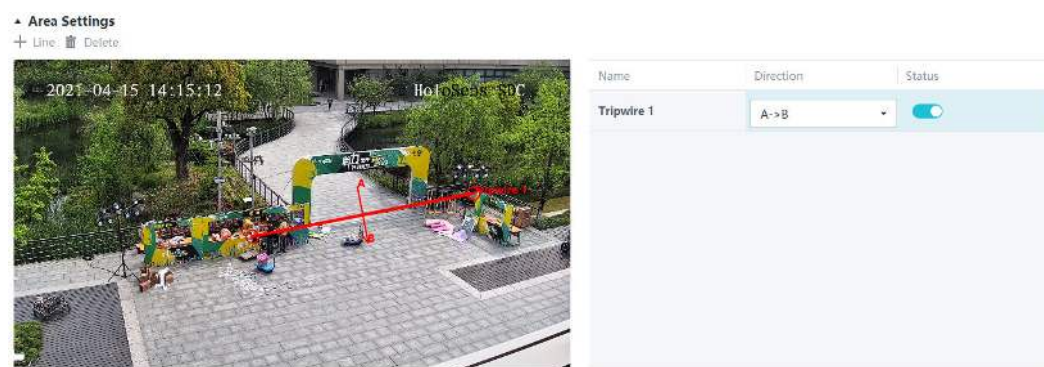
Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 5-44](#) describes the parameters.

Table 5-44 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters, as shown in [Figure 5-64](#). [Table 5-45](#) describes the parameters.

Figure 5-64 Configuring tripwire crossing detection**Table 5-45** Area settings

Parameter/ Button	Description
+ Line	Button for adding a detection line. A maximum of four detection lines are supported. You can select a detection line and drag it to change its location or change its length.
Delete	Button for deleting a selected detection area.
Direction	Specified direction in which a pedestrian crosses the detection line. The options are as follows: A<->B , A->B , and B->A
Status	- If the parameter is toggled-on, the detection line turns red and the detection takes effect. - If the parameter is toggled-off, the detection line turns white and the detection stops.

4. Set plan parameters. [Table 5-46](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-46 Plan settings

Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: - Every Day - Monday to Sunday

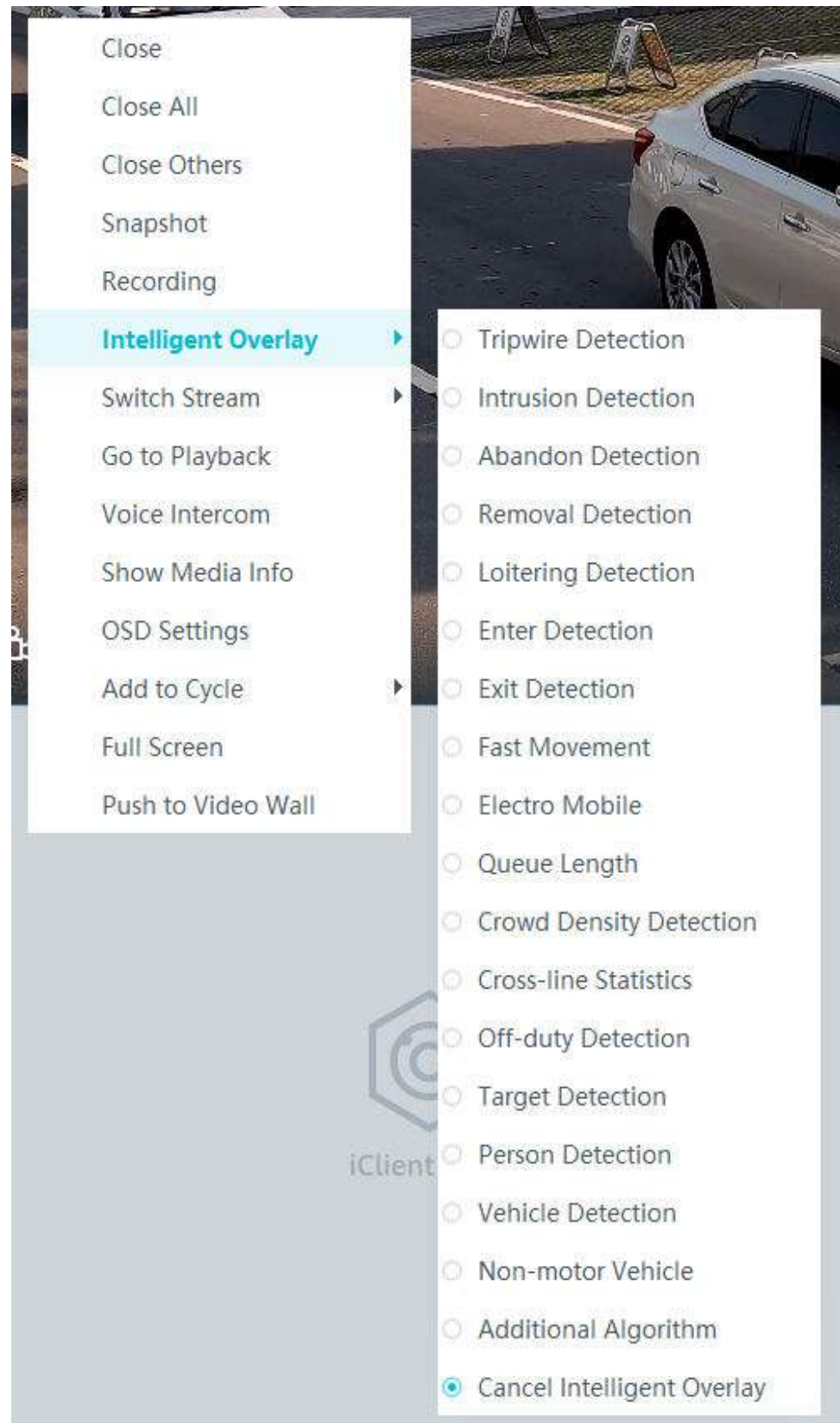
Parameter/ Button	Description
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-65](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-65 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

5.6.1.5 Intrusion Detection

Intrusion detection is used to detect whether an object enters an important detection area for which behavior analysis rules have been configured. If so, an alarm is generated. You can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273283512.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Intrusion** and set related parameters.
1. Set parameters in the **Parameter Settings** area. [Table 5-47](#) describes the parameters.

Table 5-47 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 5-48](#) describes the parameters.

Table 5-48 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 5-66](#). [Table 5-49](#) describes the parameters.

Figure 5-66 Setting detection areas

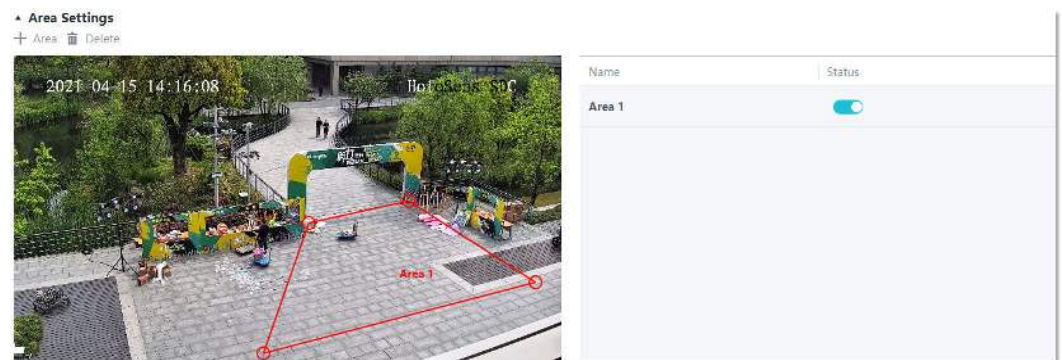


Table 5-49 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 5-50](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-50 Plan settings

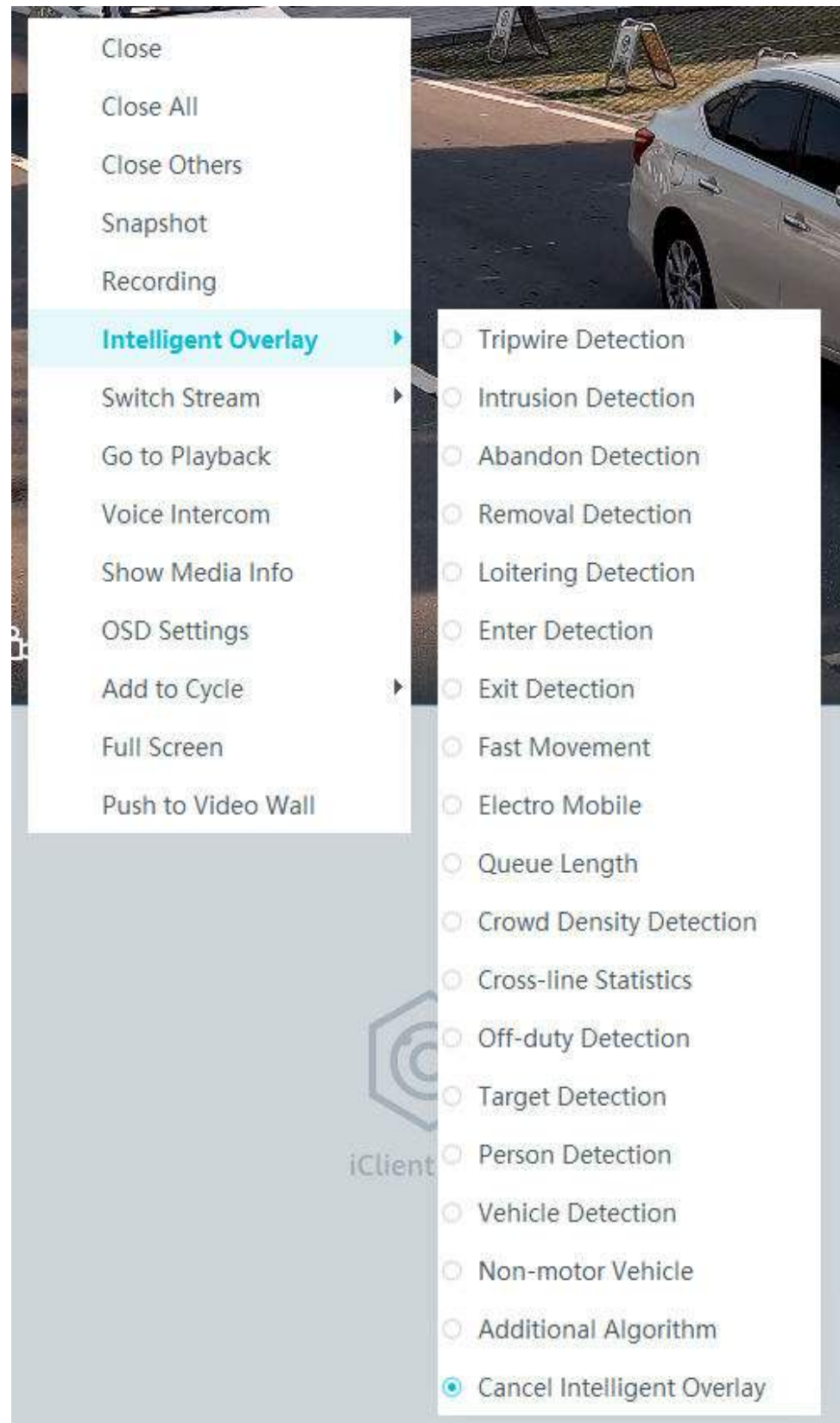
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-67](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-67 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

5.6.1.6 Abandoned Object Detection

Abandoned object detection is used to detect whether an object is abandoned in a detection area longer than the specified threshold (for example, 10 seconds). If so, an alarm is generated. Management personnel can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273283512.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Abandoned** and set related parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 5-51](#) describes the parameters.

Table 5-51 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 5-52](#) describes the parameters.

Table 5-52 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 5-68](#). [Table 5-53](#) describes the parameters.

Figure 5-68 Setting detection areas

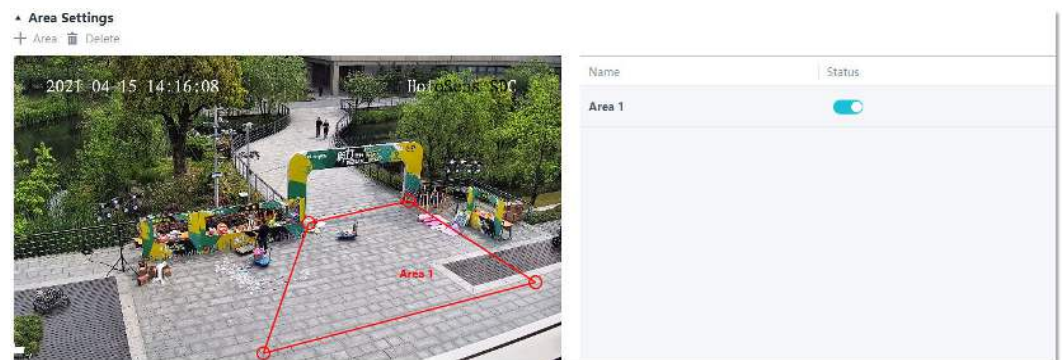


Table 5-53 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 5-54](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-54 Plan settings

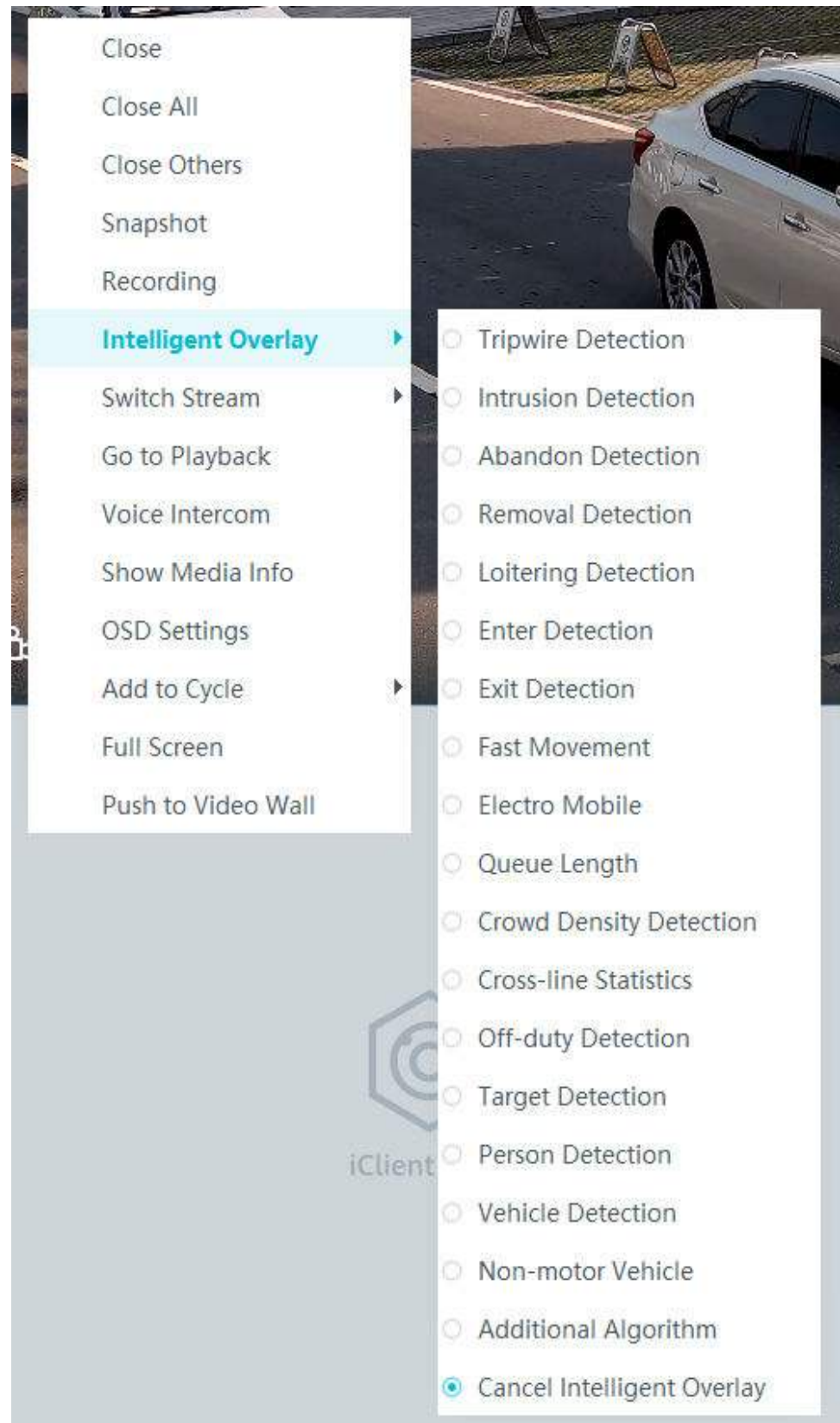
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-69](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-69 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

5.6.1.7 Removed Object Detection

Removed object detection is used to detect whether an object in a detection area is removed. If so, an alarm is generated. Management personnel can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273283512.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Removal** and set related parameters.
1. Set parameters in the **Parameter Settings** area. [Table 5-55](#) describes the parameters.

Table 5-55 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 5-56](#) describes the parameters.

Table 5-56 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 5-70](#). [Table 5-57](#) describes the parameters.

Figure 5-70 Setting detection areas

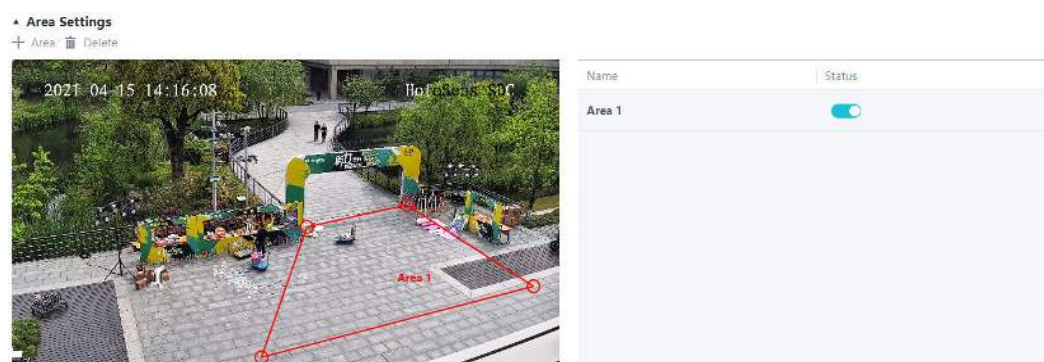


Table 5-57 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 5-58](#) describes the parameters.

NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-58 Plan settings

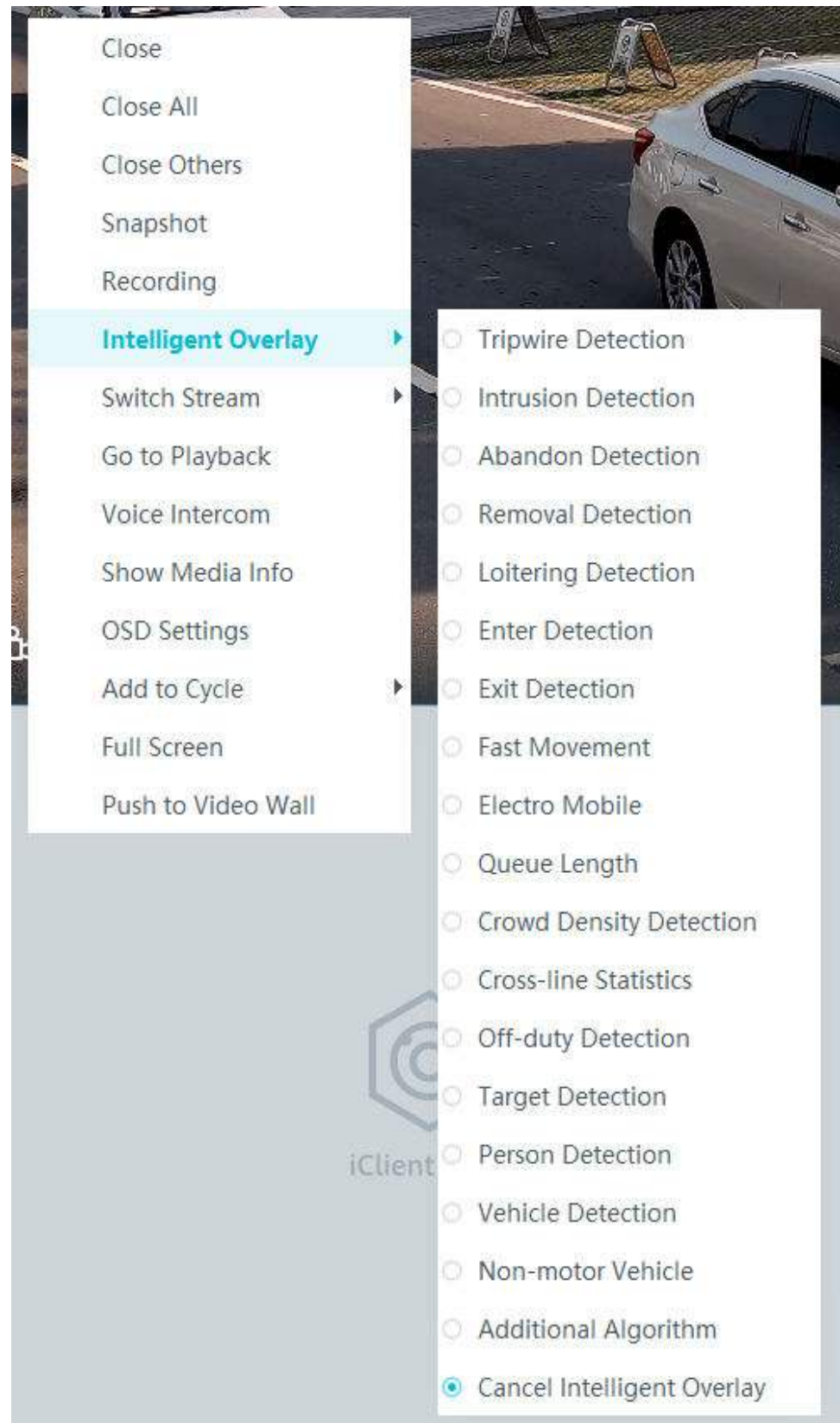
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-71](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-71 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

5.6.1.8 Loitering Detection

Loitering detection is used to detect whether an object loiters in a detection area for a duration longer than the specified threshold. If so, an alarm is generated. Management personnel can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273283512.xml.

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806249.xml.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Choose **Behavior Analysis > Loitering** and set parameters.
 1. Set parameters in the **Parameter Settings** area. [Table 5-59](#) describes the parameters.

Table 5-59 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 5-60](#) describes the parameters.

Table 5-60 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 5-72](#). [Table 5-61](#) describes the parameters.

Figure 5-72 Setting detection areas

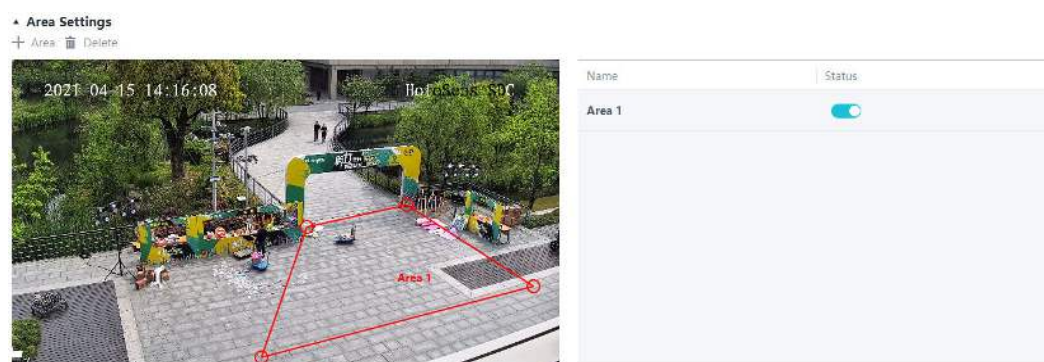


Table 5-61 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 5-62](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-62 Plan settings

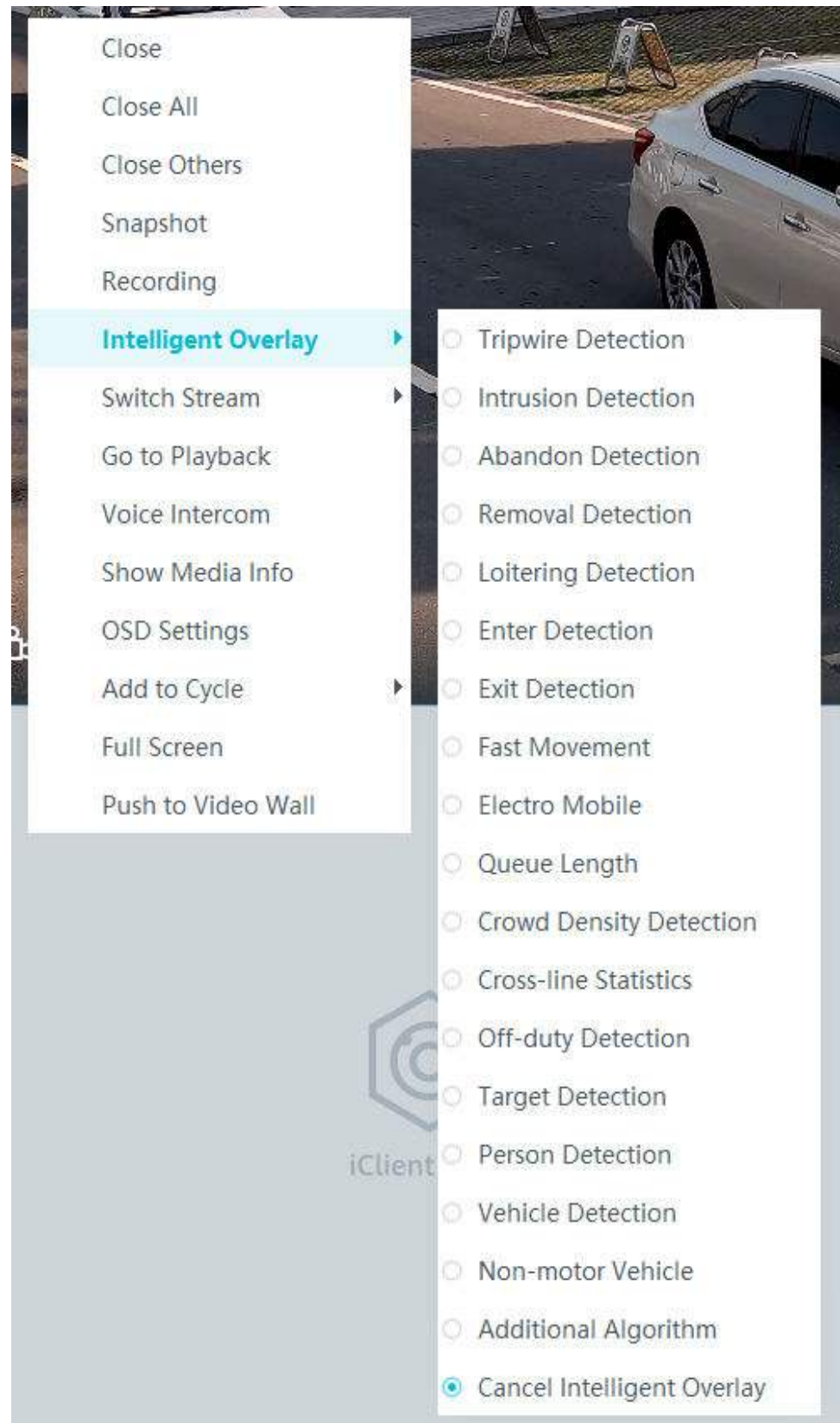
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-73](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-73 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

5.6.1.9 Area Entry Detection

Area entry detection is used to detect whether an object enters a detection area. If so, an alarm is generated. You can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see [5.6.1.3 Global Configuration](#).

Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera for which you want to configure a behavior analysis policy.

Step 3 Choose **Behavior Analysis > Area Enter** and set related parameters.

1. Set parameters in the **Parameter Settings** area. [Table 5-63](#) describes the parameters.

Table 5-63 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 5-64](#) describes the parameters.

Table 5-64 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 5-74](#). [Table 5-65](#) describes the parameters.

Figure 5-74 Setting detection areas

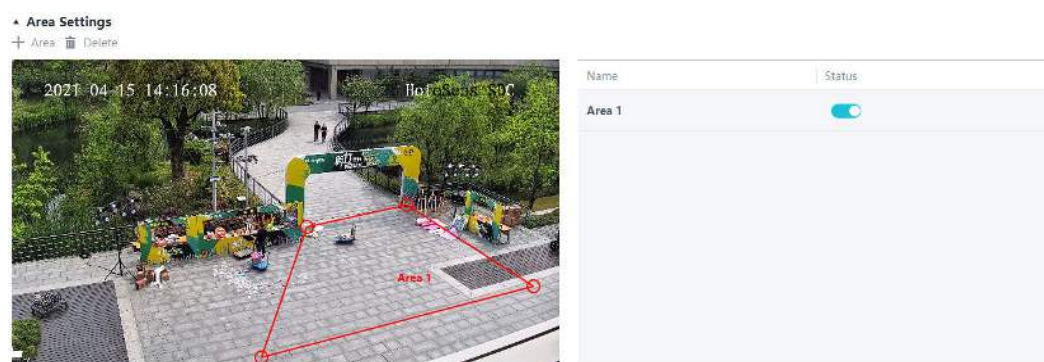


Table 5-65 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 5-66](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-66 Plan settings

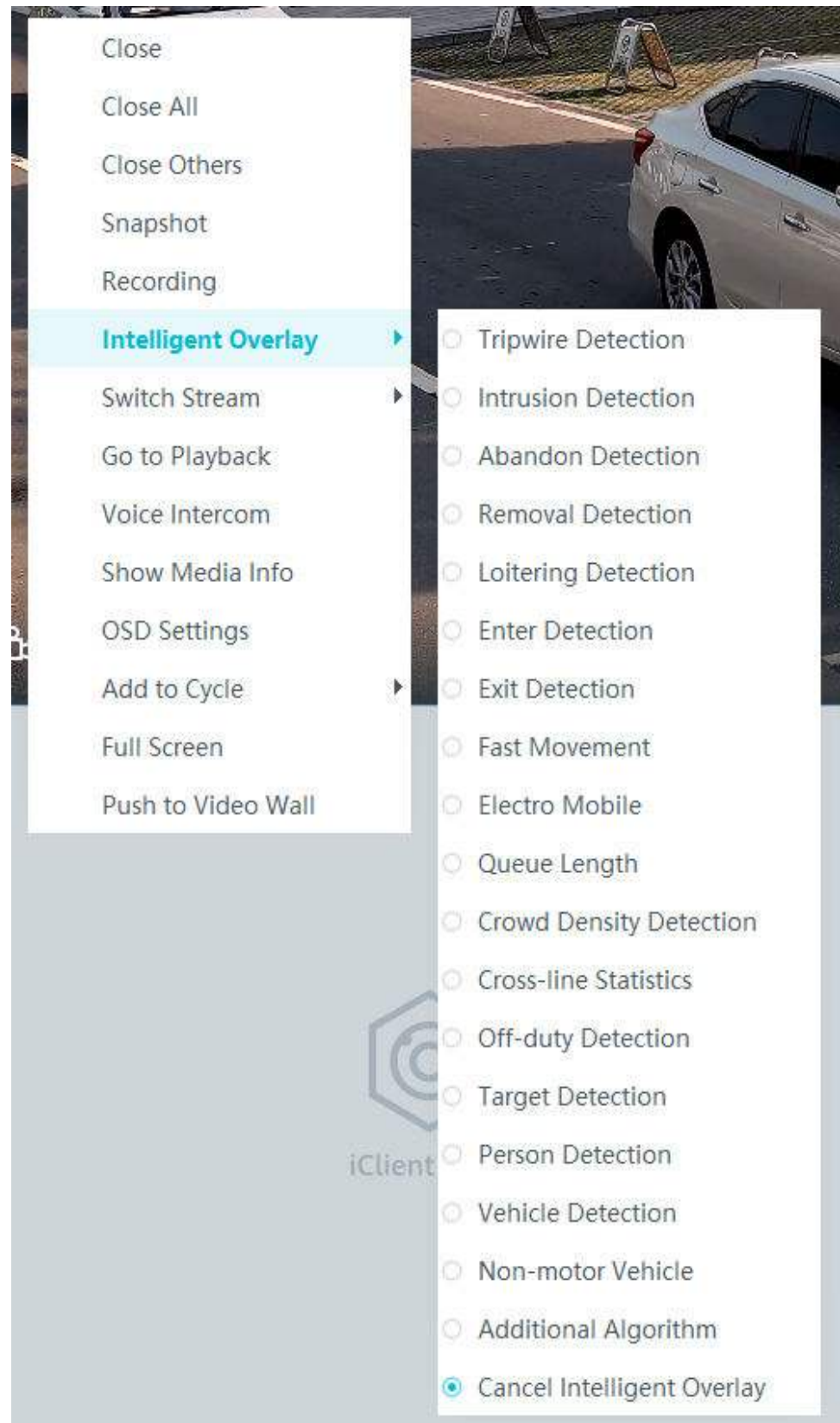
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-75](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-75 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

5.6.1.10 Area Exit Detection

Area exit detection is used to detect whether an object leaves a detection area. If so, an alarm is generated. You can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see [5.6.1.3 Global Configuration](#).

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Click the **Behavior Analysis** tab and then the **Area Exit** tab, and set related parameters.
1. Set parameters in the **Parameter Settings** area. [Table 5-67](#) describes the parameters.

Table 5-67 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 5-68](#) describes the parameters.

Table 5-68 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 5-76](#). [Table 5-69](#) describes the parameters.

Figure 5-76 Setting detection areas

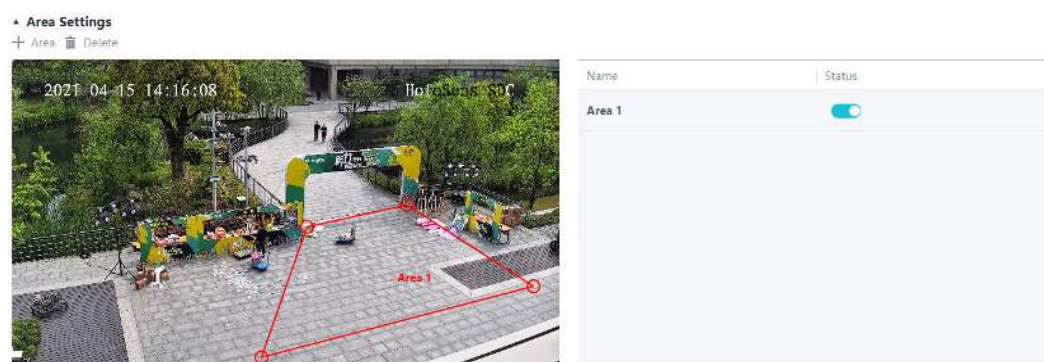


Table 5-69 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 5-70](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-70 Plan settings

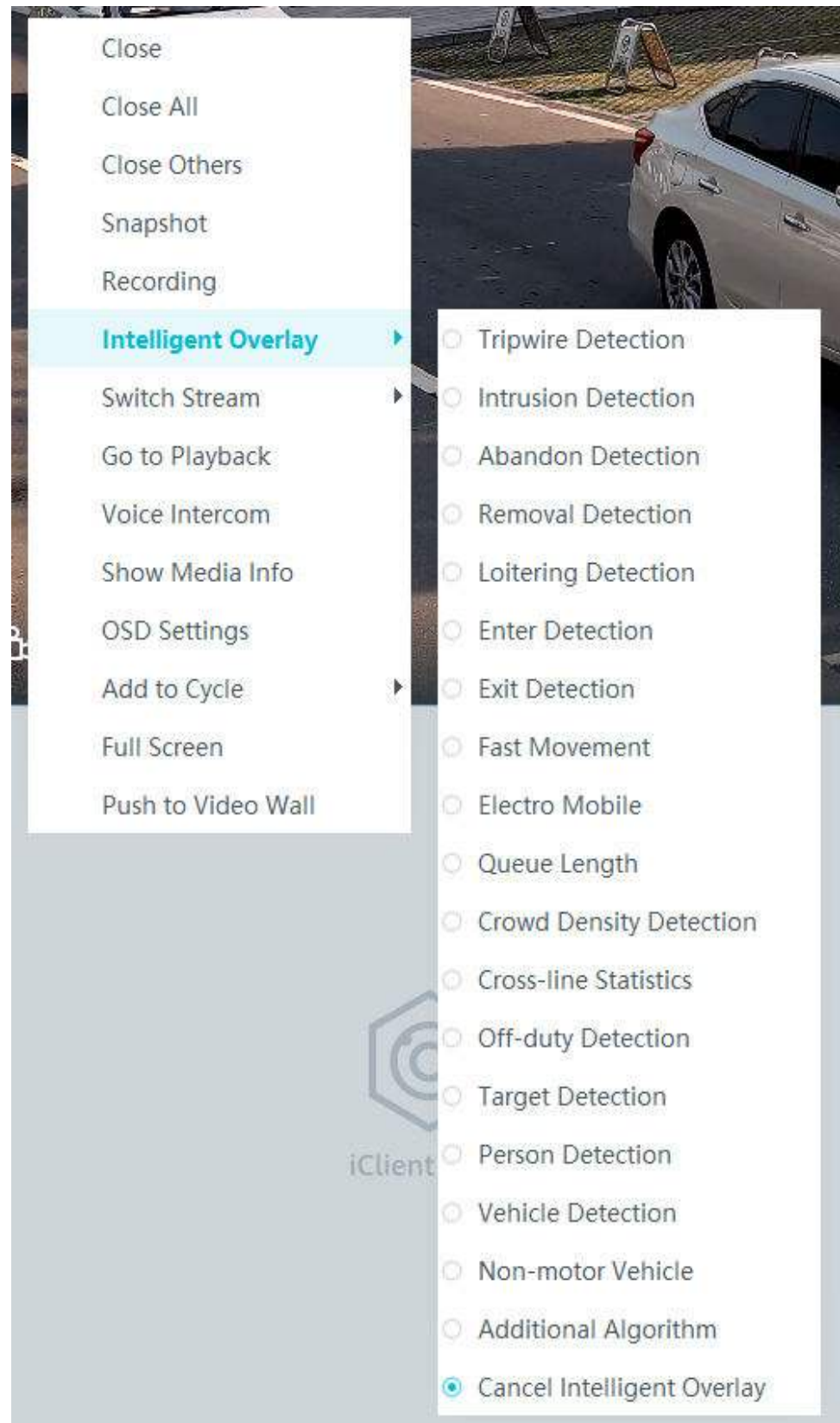
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-77](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-77 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

5.6.1.11 Fast Movement Detection

Fast movement detection is used to detect whether an object moves over in a detection area. If so, an alarm is generated. You can view the video image and dispatch personnel to the site to handle the situation.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Prerequisites

- You have connected cameras that support intelligent analysis.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see [5.6.1.3 Global Configuration](#).

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Click the **Behavior Analysis** tab and then the **Fast Movement Detection** tab, and set related parameters.
1. Set parameters in the **Parameter Settings** area. [Table 5-71](#) describes the parameters.

Table 5-71 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 5-72](#) describes the parameters.

Table 5-72 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set area parameters, as shown in [Figure 5-78](#). [Table 5-73](#) describes the parameters.

Figure 5-78 Setting detection areas

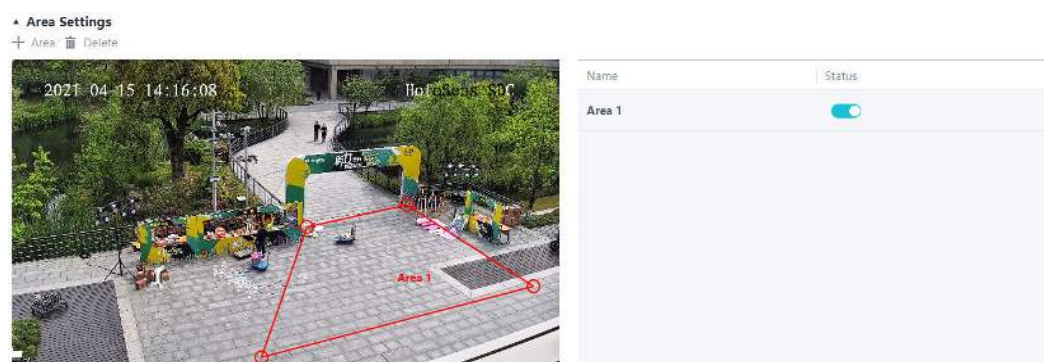


Table 5-73 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. A maximum of four detection areas can be configured for analyzing a type of behavior. A maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 5-74](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-74 Plan settings

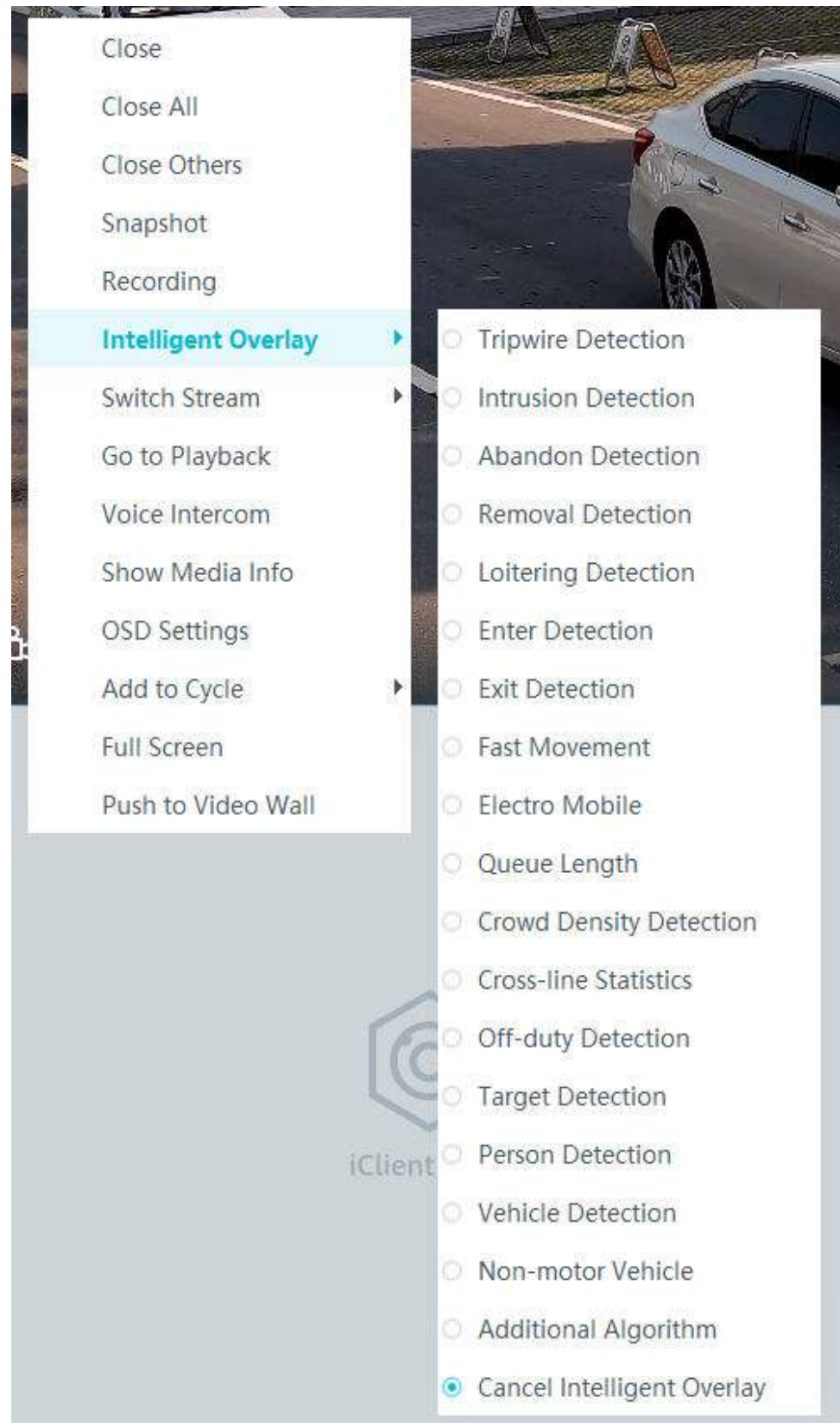
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-79](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-79 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

5.6.1.12 Electric Bike Detection

The system can generate an alarm when detecting an electric bike in areas such as elevators and corridors, where parking of electric bikes is not allowed.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Prerequisites

- You have connected cameras of the 9.0.0 version.
- You have enabled behavior analysis and set global parameters for the cameras on the iClient S100. For details, see [5.6.1.3 Global Configuration](#).

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera for which you want to configure a behavior analysis policy.
- Step 3** Click the **Behavior Analysis** tab and then the **Electric Bike Detection** tab, and set related parameters.
1. Set parameters in the **Parameter Settings** area. [Table 5-75](#) describes the parameters.

Table 5-75 Parameter description

Parameter	Description
Detection Target	Type of objects under detection. Set this parameter based on the site requirements. (This parameter is not involved when the behavior analysis type is abandoned object detection, removed object detection, or electric bicycle detection.) – Pedestrian – Motor Vehicle – Non-motor Vehicle
Alarm Detection Interval(s)	Interval at which the system checks for new alarms. If any alarm is detected, the camera reports the alarm to the iClient S100. NOTE To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.

Parameter	Description
Target Recognition Mode	Part of an object based on which the detection is performed. The options are as follows: – Center: central part of an object – Bottom: bottom part of an object – Top: top part of an object
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.

2. Set audible and visual alarm parameters. [Table 5-76](#) describes the parameters.

Table 5-76 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

- Set detection area parameters, as shown in [Figure 5-80](#). [Table 5-77](#) describes the parameters.

Figure 5-80 Setting detection areas

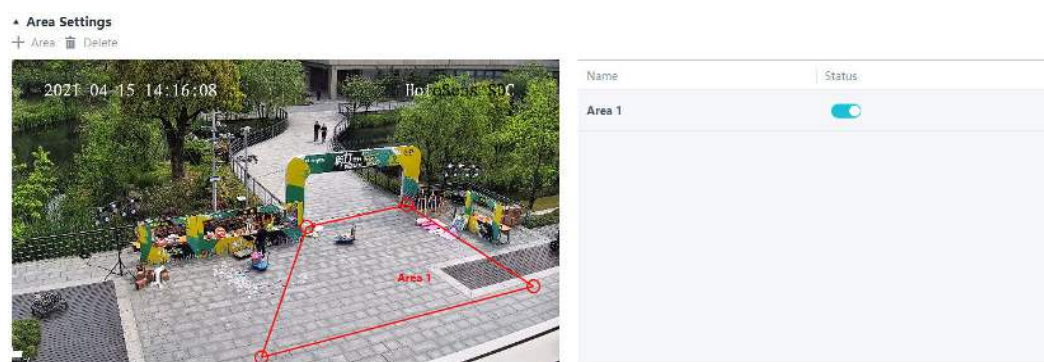


Table 5-77 Area settings

Parameter/ Button	Description
+ Area	Button for adding a detection area. Only one detection area can be configured for electric bike detection, and a maximum of 10 detection areas can be configured for all types of behavior. You can select the detection area to drag it or change its shape and size.
Delete	Button for deleting a selected detection area.
Status	- If the parameter is toggled-on, the frame of a detection area turns red and the detection takes effect. - If the parameter is toggled-off, the frame of a detection area turns white and the detection stops.

- Set plan parameters. [Table 5-78](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-78 Plan settings

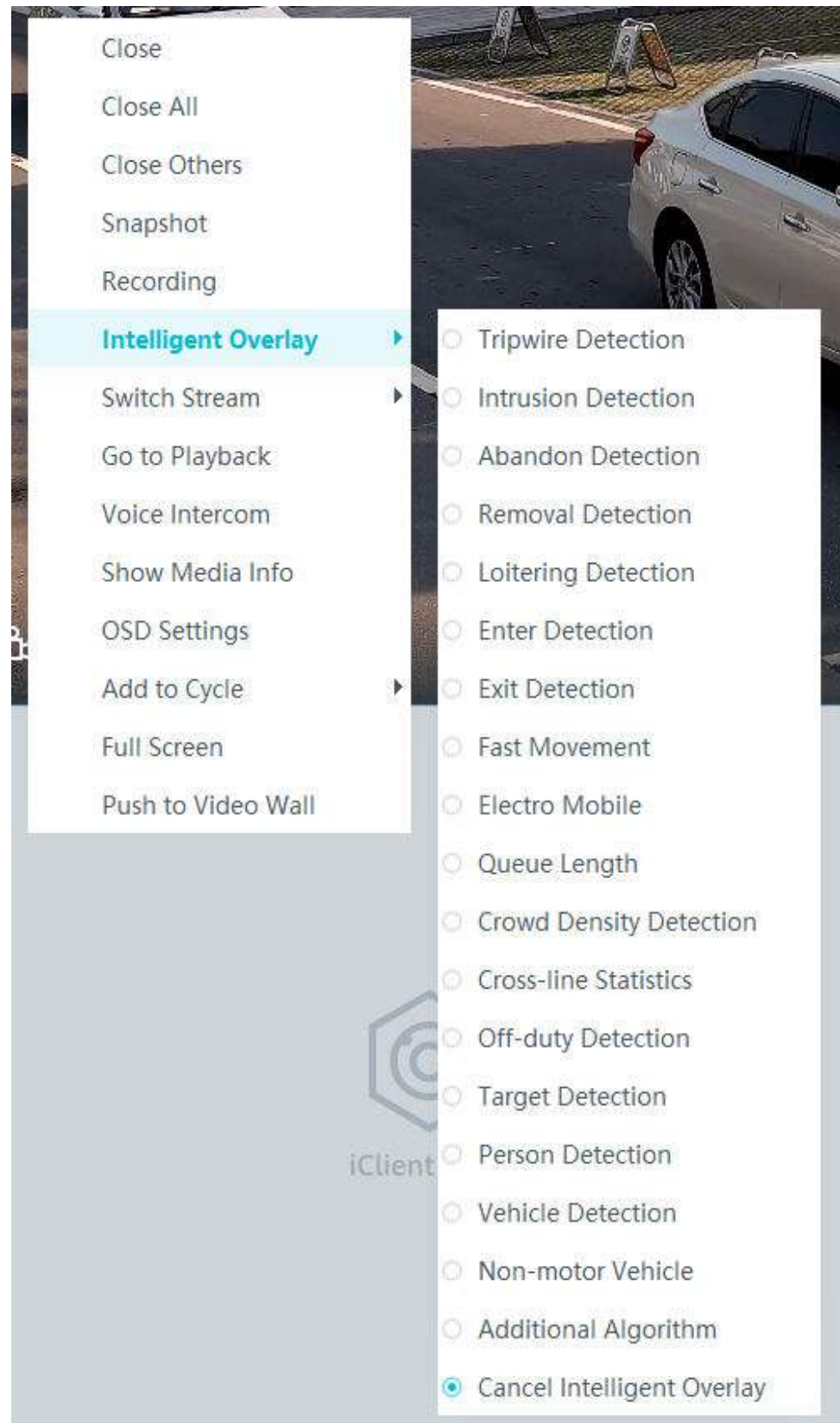
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-81](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-81 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

5.6.2 Backend Behavior Analysis

5.6.2.1 Function Description

NOTE

The IVS1800 storage model (for example, IVS1800-B08 and IVS1800-B16) does not support the backend intelligent analysis function.

After you install required algorithms in the IVS1800 and configure behavior analysis tasks on the iClient S100, the iClient S100 delivers these tasks to the IVS1800 and the IVS1800 executes the tasks on the video files from the camera.

You can configure and use behavior analysis for the IVS1800 on the iClient S100. [Table 5-79](#) lists typical application scenarios of each behavior analysis feature.

Table 5-79 Typical application scenarios

Behavior Analysis	Typical Application Scenario
Intrusion detection	You can configure intrusion detection for an area that no one is allowed to enter or approach.
Tripwire crossing detection	An alarm is generated immediately when an object crosses a predefined tripwire from a specified direction so that losses can be effectively and promptly prevented.
Area entry detection	You can configure area entry detection for an area that no object is allowed to enter.
Area exit detection	You can configure area exit detection for an area that no object is allowed to exit.
Fast movement detection	You can configure fast movement detection to prevent security risks caused by fast movement of objects.
Loitering detection	You can configure loitering detection for an area where loitering is not allowed.

5.6.2.2 (Optional) Common Configuration

Prerequisites

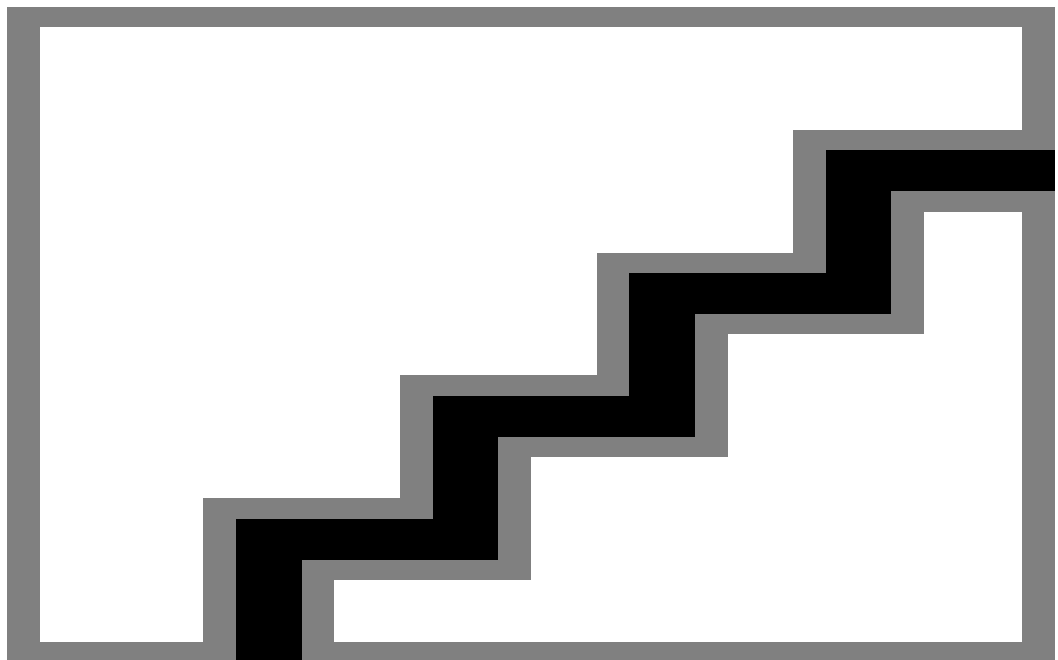
The behavior analysis algorithm plug-in has been loaded in the IVS1800. For details about how to load the plug-in, see the IVS1800 product documentation.

Common Configuration

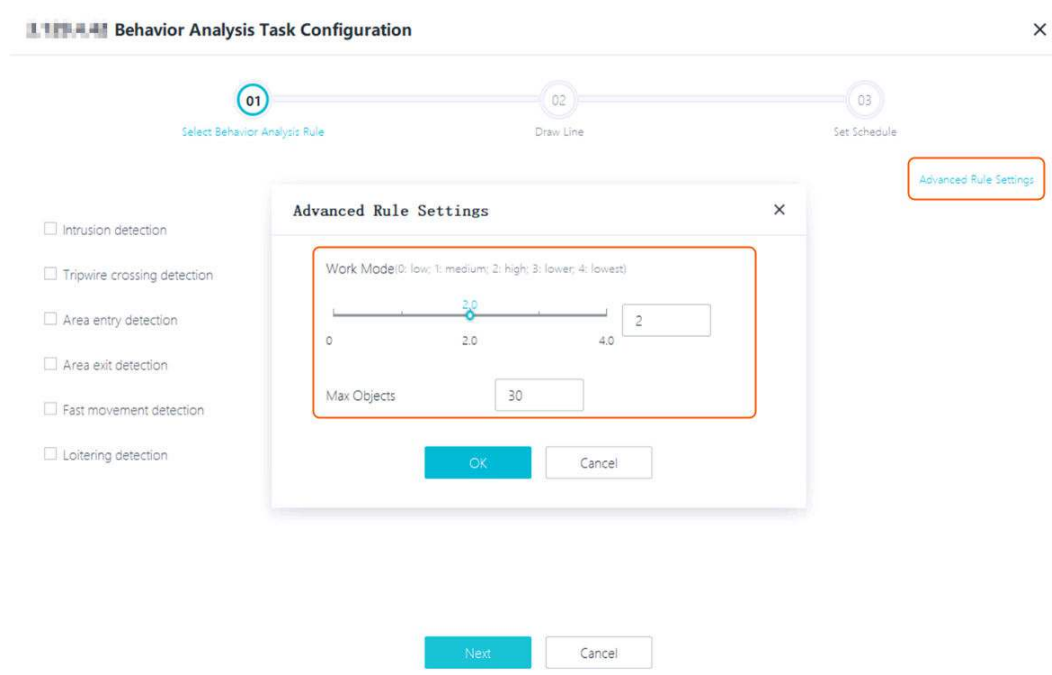
When creating a behavior analysis task, you can set advanced rule parameters based on the site requirements. The parameter settings take effect for all analysis rules of the current analysis task.

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Task Management**.
- Step 3** Click **New Task**. The **New Intelligent Analysis Task** page is displayed, as shown in **Figure 5-82**.

Figure 5-82 Creating a behavior analysis task



- Step 4** Set advanced rule parameters, as shown in [Figure 5-83](#). [Table 5-80](#) describes the parameters.

Figure 5-83 Setting advanced rule parameters**Table 5-80** Parameter description

Parameter	Setting
Work Mode	Sensitivity for detecting objects of all behavior analysis tasks in a detection area. • 0: low • 1: medium • 2: high • 3: lower • 4: lowest
Max Objects	Maximum number of objects that can be analyzed and processed in a detection area.

Step 5 Click **OK**.

Select a behavior analysis rule and configure the rule. For details, see the following sections.

-----End

5.6.2.3 Intrusion Detection

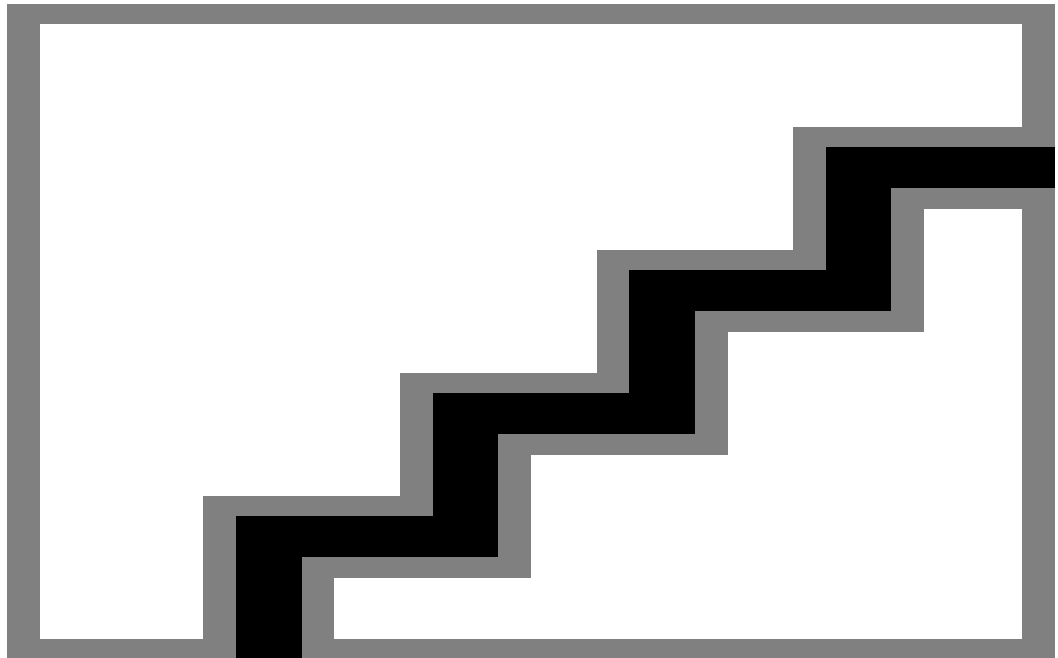
Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an IVS1800 and choose **Task Management**.

Step 3 Click **New Task**. The **New Intelligent Analysis Task** page is displayed, as shown in **Figure 5-84**.

Figure 5-84 Creating a behavior analysis task



Step 4 Select a behavior analysis rule, as shown in [Figure 5-85](#). [Table 5-81](#) describes the parameters.

Figure 5-85 Selecting a behavior analysis rule



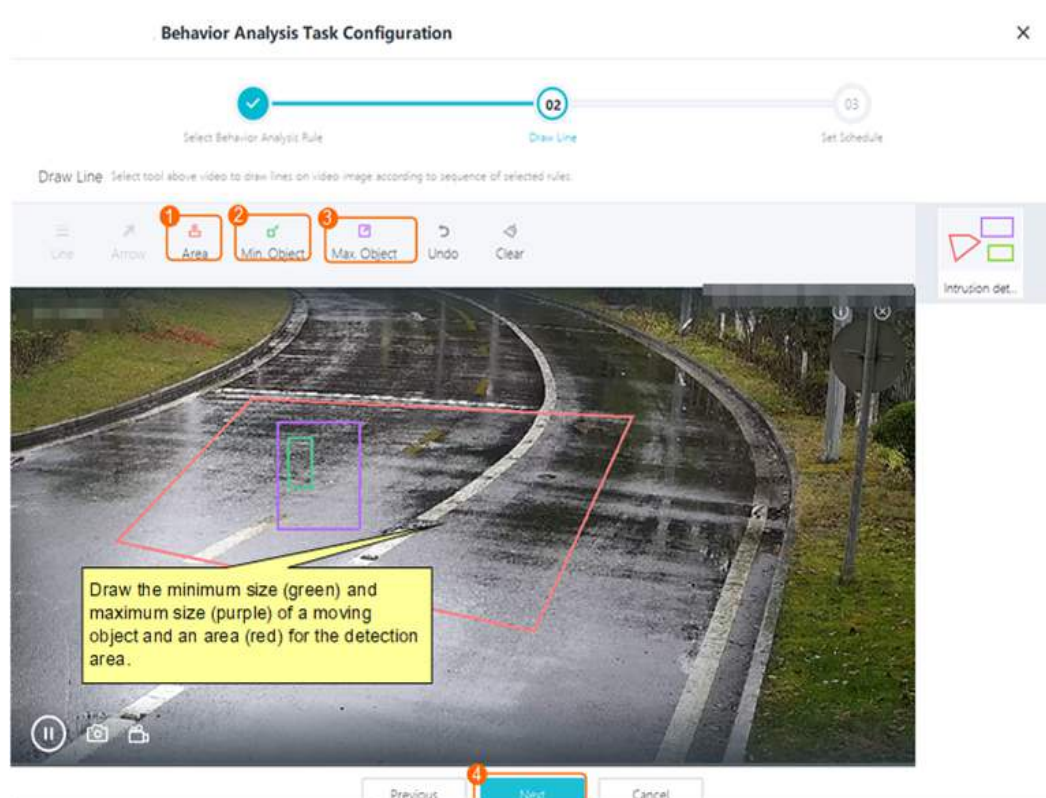
Table 5-81 Parameter description

Parameter	Setting
Select Behavior Analysis Rule	Select a behavior analysis rule.
Exclude	Select objects that do not trigger behavior analysis alarms. The options are as follows: • None • Vehicle • Person

Parameter	Setting
Alarm Interval(s)	Interval at which the system checks for new alarms.
Reference	Part of an object based on which the detection is performed. The options are as follows: • Target center: The central part of the object is used as the location reference. • Bottom center: The bottom center of an object is used as the location reference. • Top center: The top center of an object is used as the location reference. For example, if this parameter is set to Top center, an alarm is generated only when the top center of the object is in the detection area.
Sensitivity	Sensitivity for triggering alarms. Set this parameter based on the site requirements. A higher sensitivity indicates a higher probability of triggering alarms and a higher false positive rate.

Step 5 Click **Next** and draw areas, as shown in [Figure 5-86](#).

Figure 5-86 Drawing areas

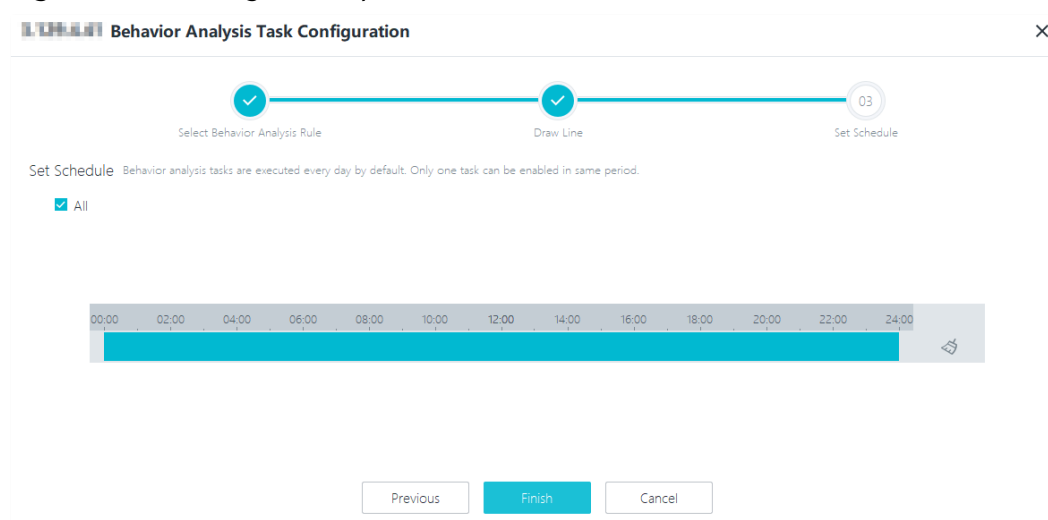


[Table 5-82](#) describes the buttons.

Table 5-82 Button description

Button	Setting
Area	Button for drawing a detection area. After drawing a detection area, double-click to finish drawing.
Min. Object	Size range of an object. An alarm is generated only when an object whose size ranges from the value of Min. Object to the value of Max. Object enters the detection area.
Max. Object	

Step 6 Click **Next** and set a time plan, as shown in [Figure 5-87](#).

Figure 5-87 Setting a time plan

Step 7 Click **Finish**.

Step 8 Click **Save**.

----End

Verification

Step 1 View the behavior analysis task status.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Right-click an IVS1800 and choose **Task Management**.
3. Set search criteria. You can click **Advanced** and set advanced search criteria. After the setting, click **Search**. Then, you can view the behavior analysis task progress and status in the task list.

Step 2 View behavior analysis alarms on the video alarm page.

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

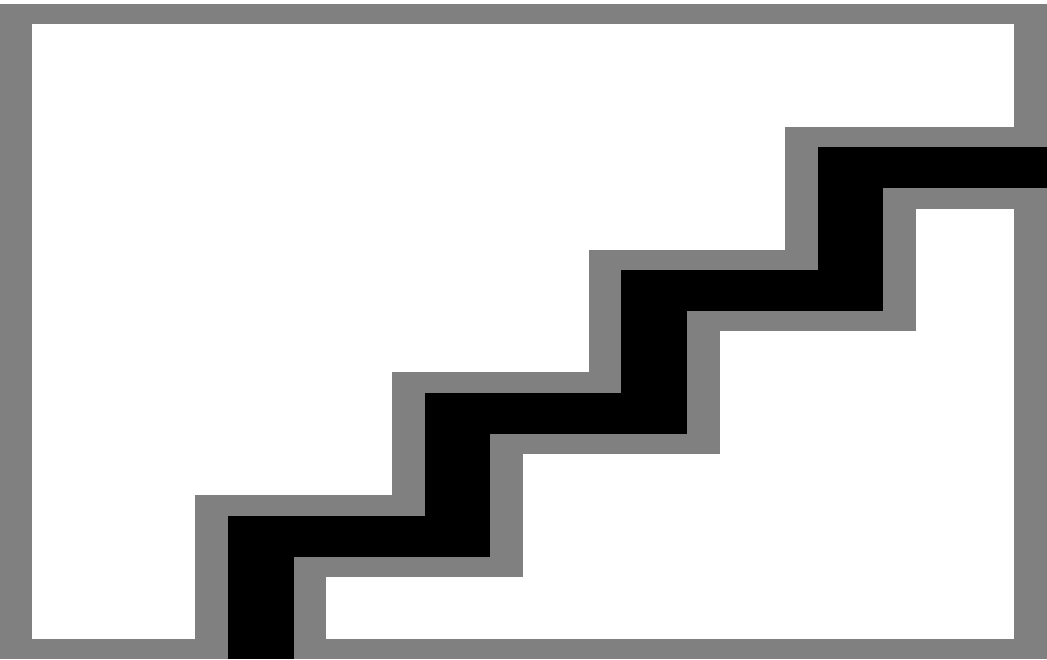
----End

5.6.2.4 Tripwire Crossing Detection

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Task Management**.
- Step 3** Click **New Task**. The **New Intelligent Analysis Task** page is displayed, as shown in [Figure 5-88](#).

Figure 5-88 Creating a behavior analysis task



- Step 4** Select a behavior analysis rule, as shown in [Figure 5-89](#). [Table 5-83](#) describes the parameters.

Figure 5-89 Selecting a behavior analysis rule

☒ Tripwire crossing detection

Exclude

None

Alarm Interval(s)

1

Reference

Target center

Sensitivity

50

Table 5-83 Parameter description

Parameter	Setting
Select Behavior Analysis Rule	Select a behavior analysis rule.

Parameter	Setting
Exclude	Select objects that do not trigger behavior analysis alarms. The options are as follows: • None • Vehicle • Person
Alarm Interval(s)	Interval at which the system checks for new alarms.
Reference	Part of an object based on which the detection is performed. The options are as follows: • Target center: The central part of the object is used as the location reference. • Bottom center: The bottom center of an object is used as the location reference. • Top center: The top center of an object is used as the location reference. For example, if this parameter is set to Top center, an alarm is generated only when the top center of the object is in the detection area.
Sensitivity	Sensitivity for triggering alarms. Set this parameter based on the site requirements. A higher sensitivity indicates a higher probability of triggering alarms and a higher false positive rate.

Step 5 Click **Next** and draw areas, as shown in [Figure 5-90](#).

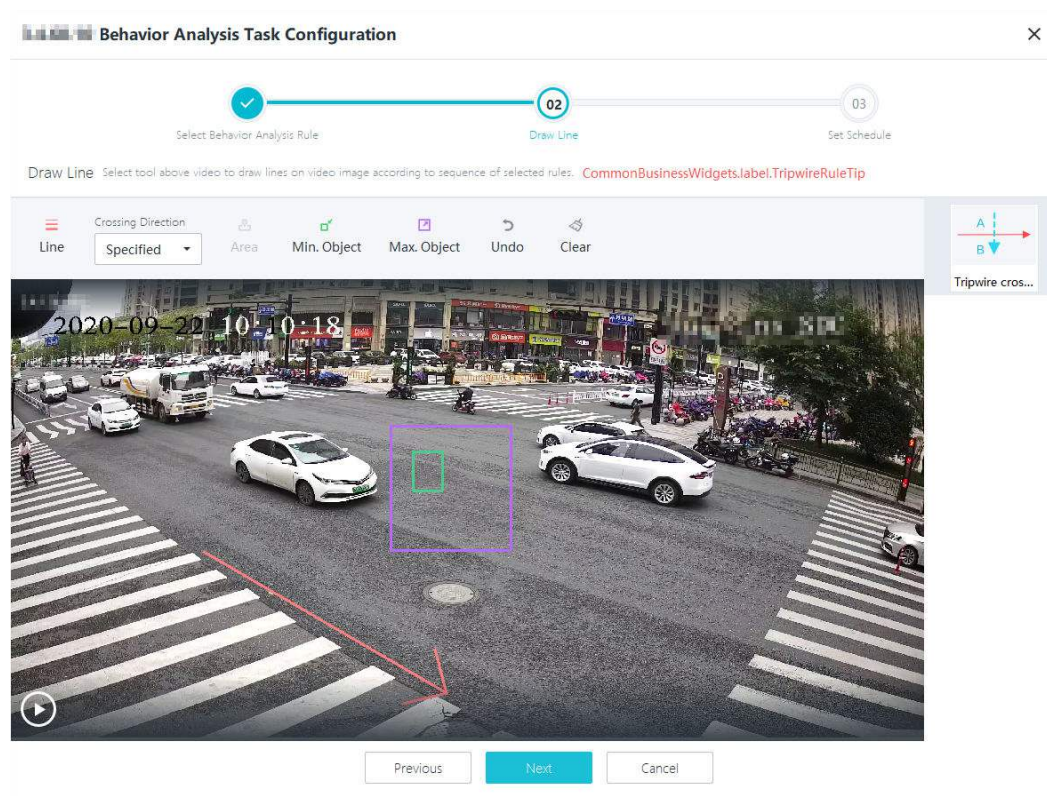
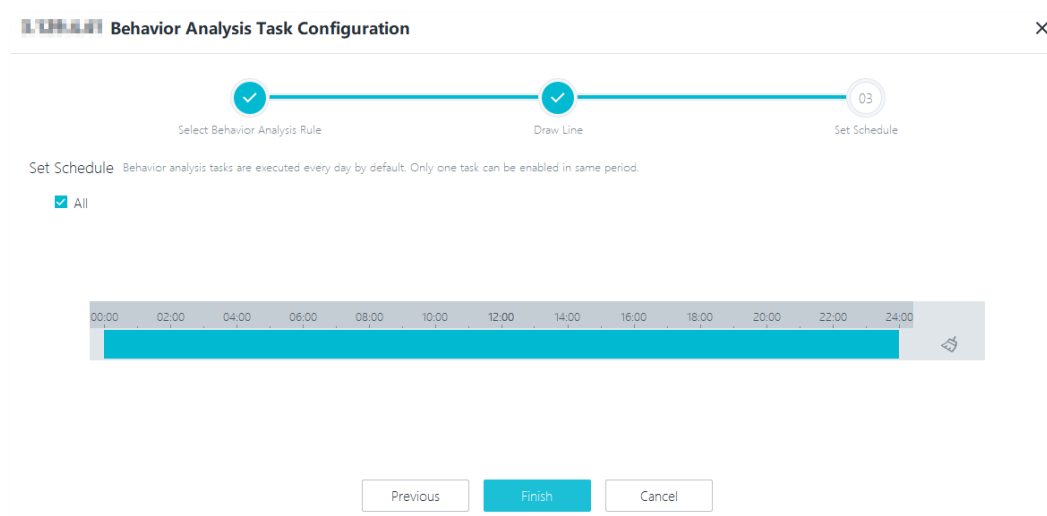
Figure 5-90 Drawing areas

Table 5-84 describes the parameters and buttons.

Table 5-84 Parameter/Button description

Parameter/Button	Setting
Min. Object	Size range of an object. An alarm is generated only when an object whose size ranges from the value of Min. Object to the value of Max. Object touches the pre-defined tripwire and continues to move in the prohibited direction.
Max. Object	
Crossing Direction	Tripwire crossing direction. The tripwire crossing direction follows the right-hand rule. That is, when you stretch your palm up with the four fingers following the tripwire drawing direction, the right thumb points to the positive direction of tripwire crossing. Set this parameter based on the site requirements. The options are as follows: - Both - Specified - The other

Step 6 Click **Next** and set a time plan, as shown in **Figure 5-91**.

Figure 5-91 Setting a time plan

Step 7 Click **Finish**.

Step 8 Click **Save**.

----End

Verification

Step 1 View the behavior analysis task status.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Right-click an IVS1800 and choose **Task Management**.
3. Set search criteria. You can click **Advanced** and set advanced search criteria. After the setting, click **Search**. Then, you can view the behavior analysis task progress and status in the task list.

Step 2 View behavior analysis alarms on the video alarm page.

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

----End

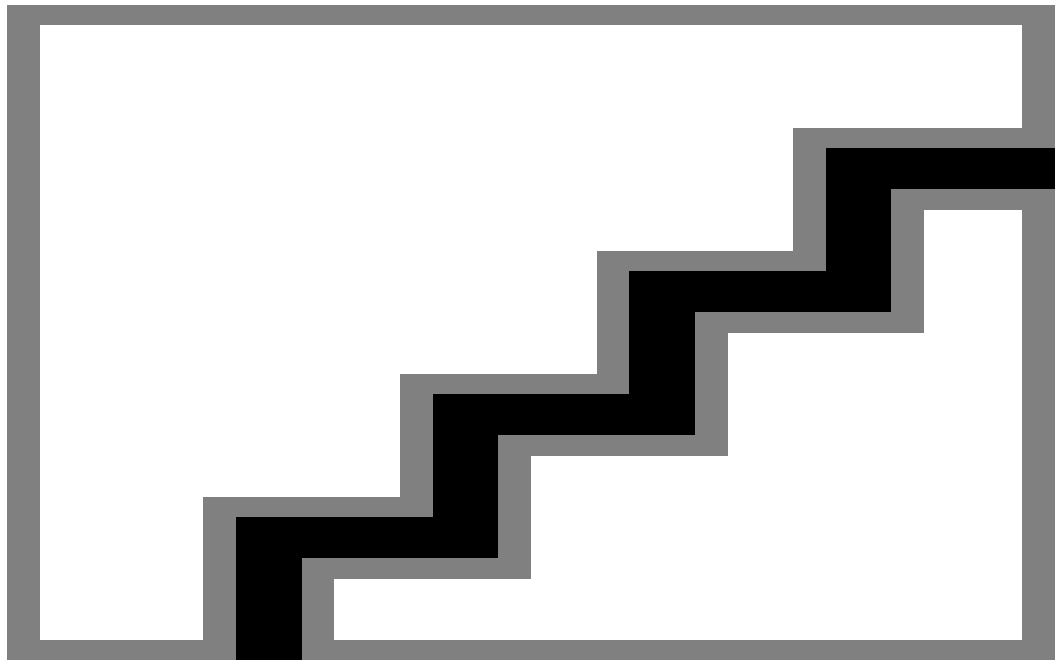
5.6.2.5 Area Entry Detection

Procedure

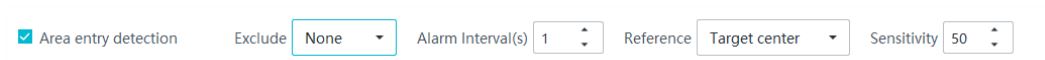
Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an IVS1800 and choose **Task Management**.

Step 3 Click **New Task**. The **New Intelligent Analysis Task** page is displayed, as shown in [Figure 5-92](#).

Figure 5-92 Creating a behavior analysis task

Step 4 Select a behavior analysis rule, as shown in [Figure 5-93](#). [Table 5-85](#) describes the parameters.

Figure 5-93 Selecting a behavior analysis rule**Table 5-85** Parameter description

Parameter	Setting
Select Behavior Analysis Rule	Select a behavior analysis rule.
Exclude	Select objects that do not trigger behavior analysis alarms. The options are as follows: • None • Vehicle • Person
Alarm Interval(s)	Interval at which the system checks for new alarms.

Parameter	Setting
Reference	Part of an object based on which the detection is performed. The options are as follows: • Target center: The central part of the object is used as the location reference. • Bottom center: The bottom center of an object is used as the location reference. • Top center: The top center of an object is used as the location reference. For example, if this parameter is set to Top center, an alarm is generated only when the top center of the object is in the detection area.
Sensitivity	Sensitivity for triggering alarms. Set this parameter based on the site requirements. A higher sensitivity indicates a higher probability of triggering alarms and a higher false positive rate.

Step 5 Click **Next** and draw areas, as shown in [Figure 5-94](#). [Table 5-86](#) describes the buttons.

Figure 5-94 Drawing areas

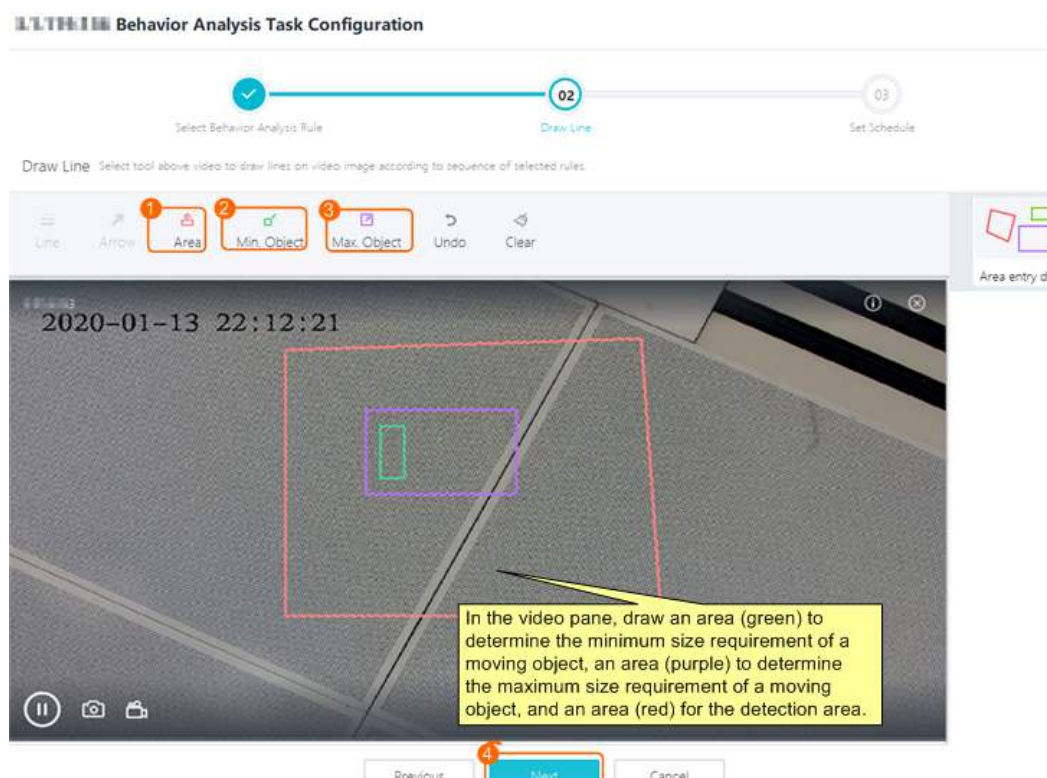
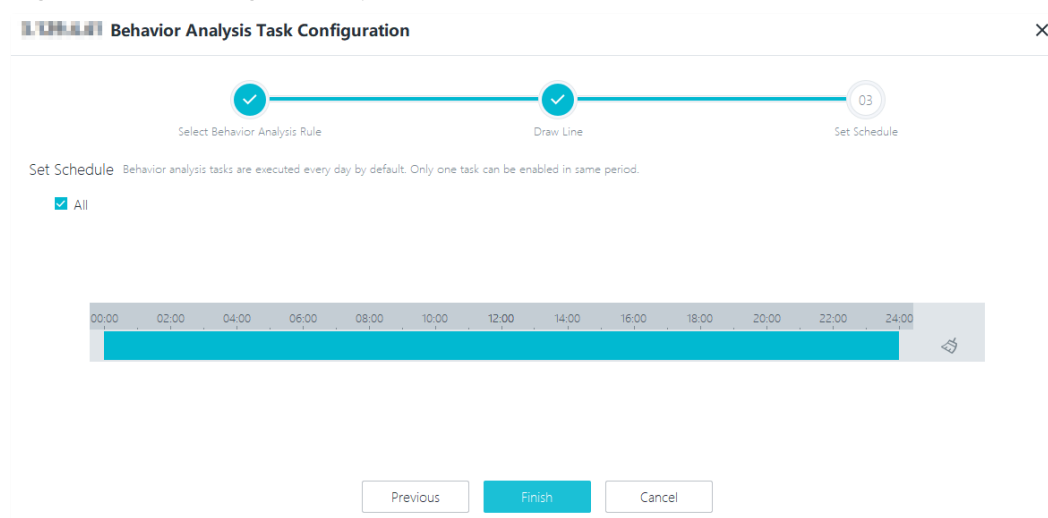


Table 5-86 Button description

Button	Setting
Min. Object	Size range of an object. An alarm is generated only when an object whose size ranges from the value of Min. Object to the value of Max. Object enters the detection area.
Max. Object	
Area	Button for drawing a detection area. After drawing a detection area, double-click to finish drawing.

Step 6 Click **Next** and set a time plan, as shown in [Figure 5-95](#).

Figure 5-95 Setting a time plan

Step 7 Click **Finish**.

Step 8 Click **Save**.

----End

Verification

Step 1 View the behavior analysis task status.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Right-click an IVS1800 and choose **Task Management**.
3. Set search criteria. You can click **Advanced** and set advanced search criteria. After the setting, click **Search**. Then, you can view the behavior analysis task progress and status in the task list.

Step 2 View behavior analysis alarms on the video alarm page.

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

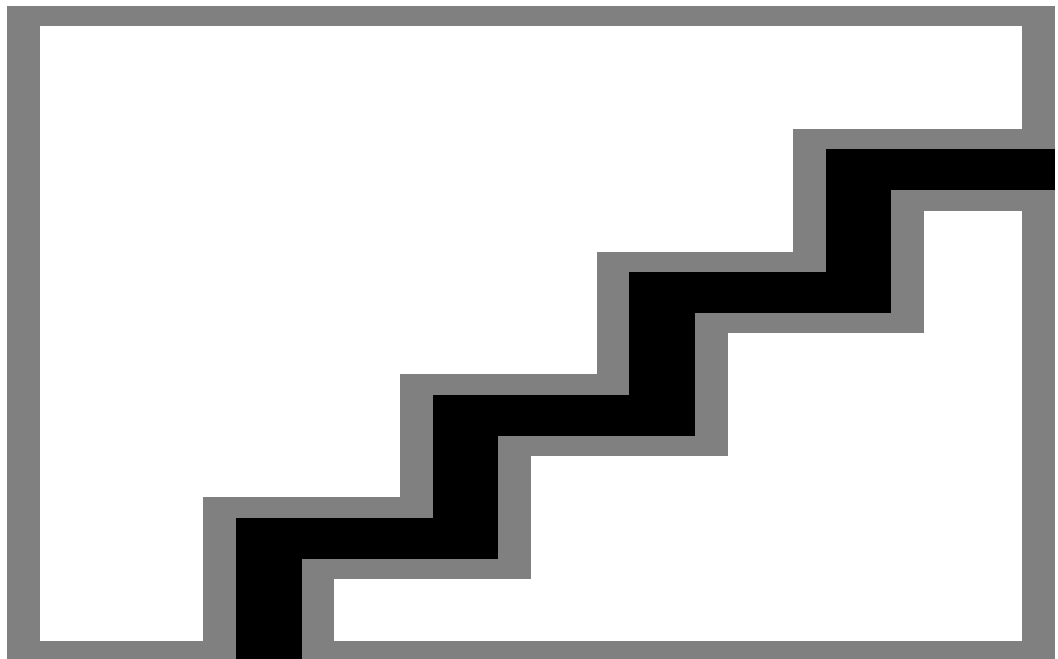
----End

5.6.2.6 Area Exit Detection

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Task Management**.
- Step 3** Click **New Task**. The **New Intelligent Analysis Task** page is displayed, as shown in [Figure 5-96](#).

Figure 5-96 Creating a behavior analysis task



- Step 4** Select a behavior analysis rule, as shown in [Figure 5-97](#). [Table 5-87](#) describes the parameters.

Figure 5-97 Selecting a behavior analysis rule



Table 5-87 Parameter description

Parameter	Setting
Select Behavior Analysis Rule	Select a behavior analysis rule.

Parameter	Setting
Exclude	Select objects that do not trigger behavior analysis alarms. The options are as follows: • None • Vehicle • Person
Alarm Interval(s)	Interval at which the system checks for new alarms.
Reference	Part of an object based on which the detection is performed. The options are as follows: • Target center: The central part of the object is used as the location reference. • Bottom center: The bottom center of an object is used as the location reference. • Top center: The top center of an object is used as the location reference. For example, if this parameter is set to Top center, an alarm is generated only when the top center of the object is in the detection area.
Sensitivity	Sensitivity for triggering alarms. Set this parameter based on the site requirements. A higher sensitivity indicates a higher probability of triggering alarms and a higher false positive rate.

Step 5 Click **Next** and draw areas, as shown in [Figure 5-98](#).

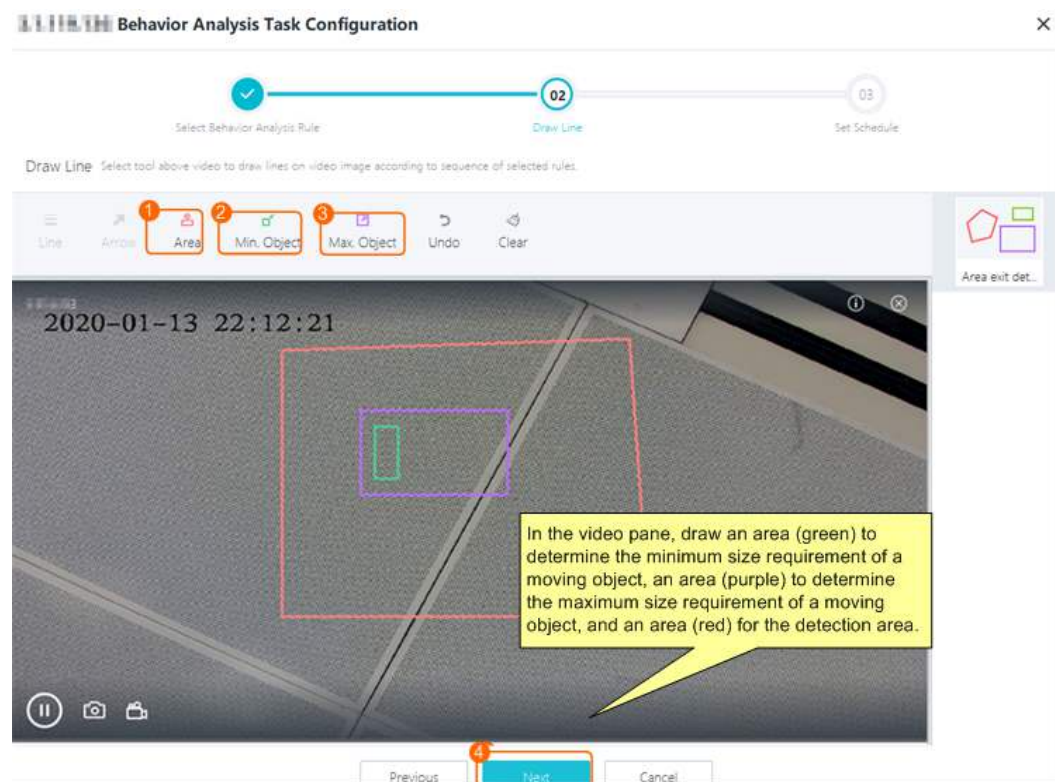
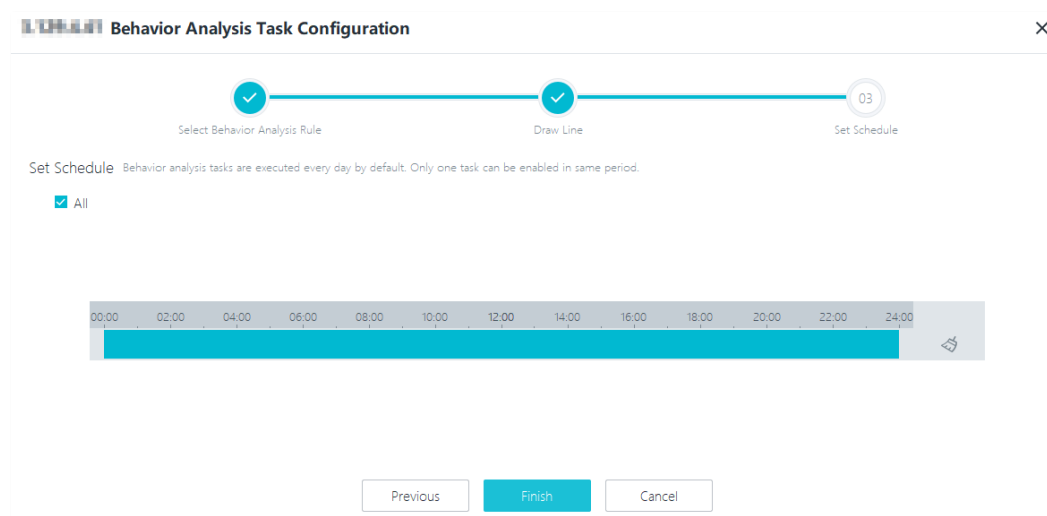
Figure 5-98 Drawing areas

Table 5-88 describes the buttons.

Table 5-88 Button description

Button	Setting
Min. Object	Size range of an object. An alarm is generated only when an object whose size ranges from the value of Min. Object to the value of Max. Object exits the detection area.
Max. Object	
Area	Button for drawing a detection area. After drawing a detection area, double-click to finish drawing.

Step 6 Click **Next** and set a time plan, as shown in **Figure 5-99**.

Figure 5-99 Setting a time plan

Step 7 Click **Finish**.

Step 8 Click **Save**.

----End

Verification

Step 1 View the behavior analysis task status.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Right-click an IVS1800 and choose **Task Management**.
3. Set search criteria. You can click **Advanced** and set advanced search criteria. After the setting, click **Search**. Then, you can view the behavior analysis task progress and status in the task list.

Step 2 View behavior analysis alarms on the video alarm page.

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

----End

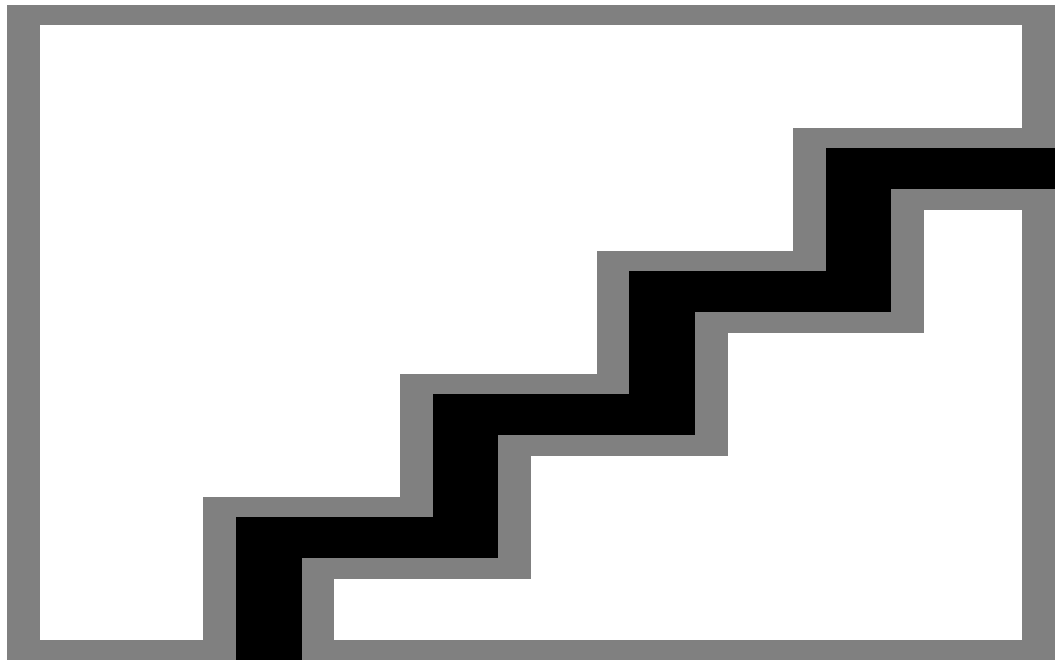
5.6.2.7 Fast Movement Detection

Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an IVS1800 and choose **Task Management**.

Step 3 Click **New Task**. The **New Intelligent Analysis Task** page is displayed, as shown in [Figure 5-100](#).

Figure 5-100 Creating a behavior analysis task

Step 4 Select a behavior analysis rule, as shown in [Figure 5-101](#). [Table 5-89](#) describes the parameters.

Figure 5-101 Selecting a behavior analysis rule

☒ Fast movement detection
 Exclude None ▼
 Alarm Interval(s) 1 ▼
 Reference Target center ▼
 Sensitivity 50 ▼

Table 5-89 Parameter description

Parameter	Setting
Select Behavior Analysis Rule	Select a behavior analysis rule.
Exclude	Select objects that do not trigger behavior analysis alarms. The options are as follows: • None • Vehicle • Person
Alarm Interval(s)	Interval at which the system checks for new alarms.

Parameter	Setting
Reference	Part of an object based on which the detection is performed. The options are as follows: • Target center: The central part of the object is used as the location reference. • Bottom center: The bottom center of an object is used as the location reference. • Top center: The top center of an object is used as the location reference. For example, if this parameter is set to Top center, an alarm is generated only when the top center of the object is in the detection area.
Sensitivity	Sensitivity for triggering alarms. Set this parameter based on the site requirements. A higher sensitivity indicates a higher probability of triggering alarms and a higher false positive rate.

Step 5 Click **Next** and draw areas, as shown in [Figure 5-102](#). [Table 5-90](#) describes the buttons.

Figure 5-102 Drawing areas

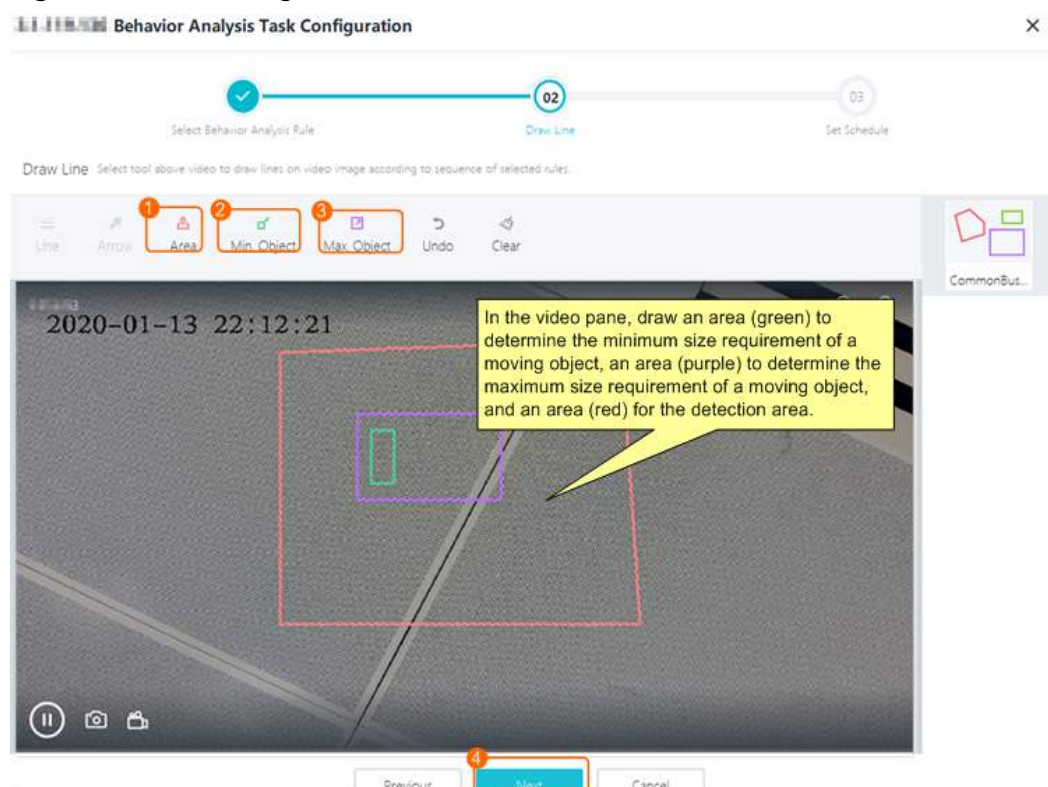
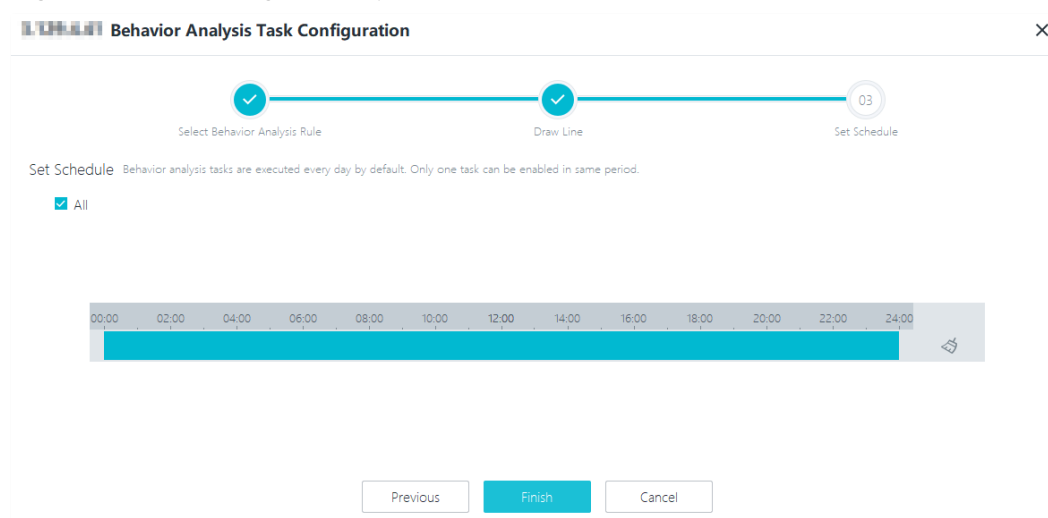


Table 5-90 Button description

Button	Setting
Min. Object	Size range of an object. An alarm is generated only when an object whose size ranges from the value of Min. Object to the value of Max. Object moves fast in the detection area.
Max. Object	
Area	Button for drawing a detection area. After drawing a detection area, double-click to finish drawing.

Step 6 Click **Next** and set a time plan, as shown in [Figure 5-103](#).

Figure 5-103 Setting a time plan

Step 7 Click **Finish**.

Step 8 Click **Save**.

----End

Verification

Step 1 View the behavior analysis task status.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Right-click an IVS1800 and choose **Task Management**.
3. Set search criteria. You can click **Advanced** and set advanced search criteria. After the setting, click **Search**. Then, you can view the behavior analysis task progress and status in the task list.

Step 2 View behavior analysis alarms on the video alarm page.

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

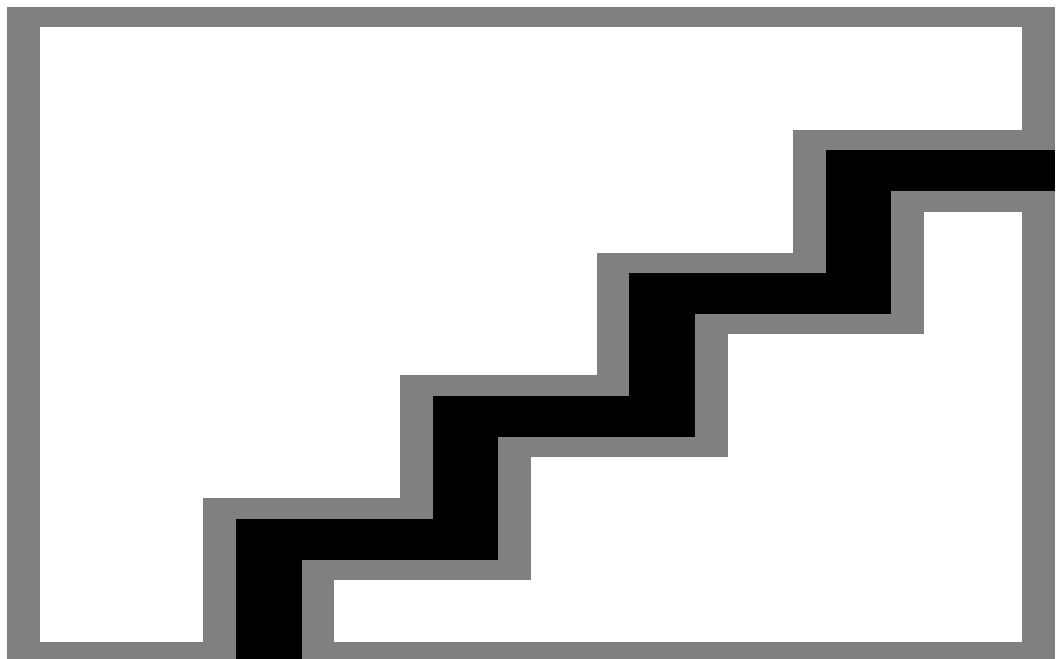
----End

5.6.2.8 Loitering Detection

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Task Management**.
- Step 3** Click **New Task**. The **New Intelligent Analysis Task** page is displayed, as shown in **Figure 5-104**.

Figure 5-104 Creating a behavior analysis task



- Step 4** Select a behavior analysis rule, as shown in [Figure 5-105](#).

Figure 5-105 Selecting a behavior analysis rule

☒ Loitering detection Exclude None Alarm Interval(s) 1 Reference Target c Sensitivity 50 Duration(s) 1

Table 5-91 describes the parameters.

Table 5-91 Parameter description

Parameter	Setting
Select Behavior Analysis Rule	Select a behavior analysis rule.

Parameter	Setting
Exclude	Select objects that do not trigger behavior analysis alarms. The options are as follows: • None • Vehicle • Person
Alarm Interval(s)	Interval at which the system checks for new alarms.
Reference	Part of an object based on which the detection is performed. The options are as follows: • Target center: The central part of the object is used as the location reference. • Bottom center: The bottom center of an object is used as the location reference. • Top center: The top center of an object is used as the location reference. For example, if this parameter is set to Top center, an alarm is generated only when the top center of the object is in the detection area.
Sensitivity	Sensitivity that is mainly used to detect the speed of a moving object. Set this parameter based on the site requirements.
Duration	Time during which an object can loiter in the detection area. This parameter is available only when Loitering detection is selected. When an object loiters in the detection area for a period longer than that specified by Duration, a behavior analysis alarm is generated.

Step 5 Click **Next** and draw areas, as shown in [Figure 5-106](#).

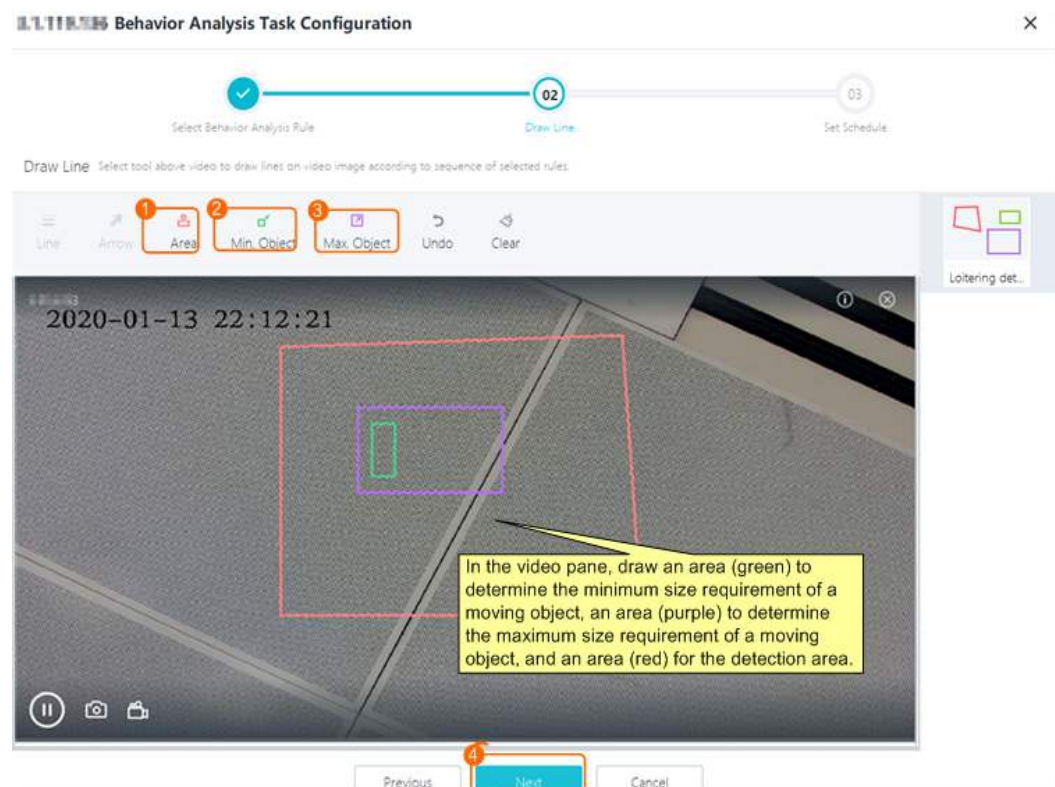
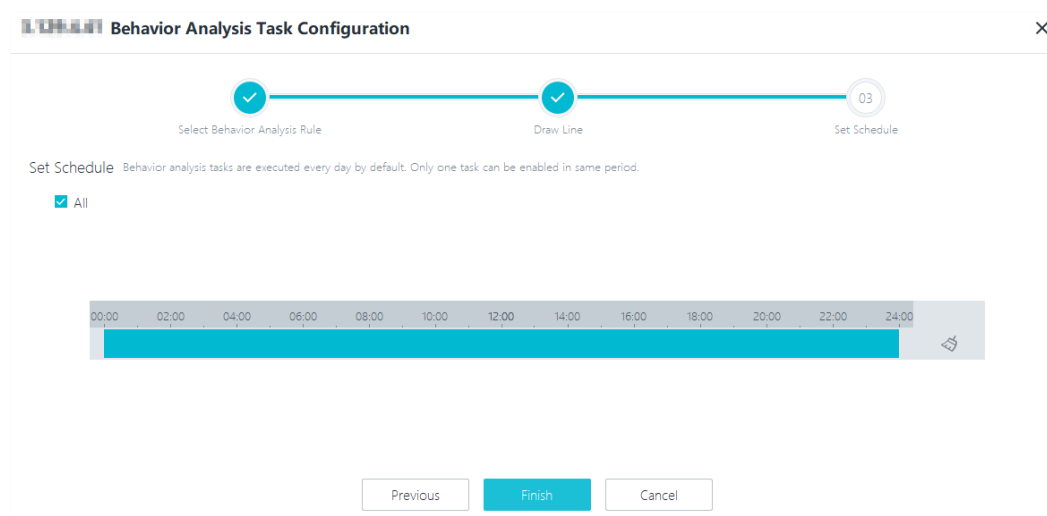
Figure 5-106 Drawing areas

Table 5-92 describes the buttons.

Table 5-92 Button description

Button	Setting
Min. Object	Size range of an object. An alarm is generated only when an object whose size ranges from the value of Min. Object to the value of Max. Object loiters in the detection area for a period longer than that specified by Duration .
Max. Object	
Area	Button for drawing a detection area. After drawing a detection area, double-click to finish drawing.

Step 6 Click **Next** and set a time plan, as shown in **Figure 5-107**.

Figure 5-107 Setting a time plan

Step 7 Click **Finish**.

Step 8 Click **Save**.

----End

Verification

Step 1 View the behavior analysis task status.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Right-click an IVS1800 and choose **Task Management**.
3. Set search criteria. You can click **Advanced** and set advanced search criteria. After the setting, click **Search**. Then, you can view the behavior analysis task progress and status in the task list.

Step 2 View behavior analysis alarms on the video alarm page.

For details about how to view the latest or historical alarms, see [IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml](#).

----End

5.7 Target Intelligence

5.7.1 Target Intelligence (Based on Cameras)

5.7.1.1 Global Configuration

Application Scenario

Before configuring target intelligence on the iClient S100, you need to complete global configuration.

Table 5-93 Global configuration for target intelligence

Procedure	Application Scenario
Turn on the target intelligent switch	This step should be started in all scenes that need to use target recognition function.
Turn on the camera target intelligent switch	This step should be started in all scenes that need to use target recognition function.
Configuring the algorithm mode	Cameras that support target recognition, such as Dxxx-10-SIU cameras
Configuring target recognition	
Setting target detection parameters	All Dxxx-10 cameras

Turn on the target intelligent switch of the main device

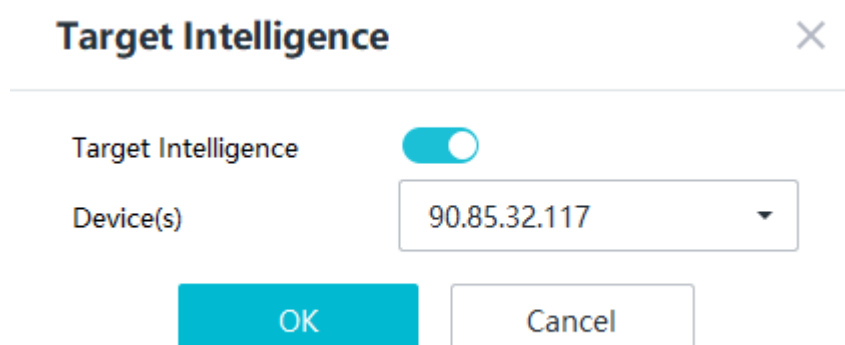
This step should be started in all scenes where the target recognition function needs to be used.

NOTE

- The use of target intelligence in business scenarios needs to be subject to legal constraints. Therefore, before starting the target intelligence function, you need to know the relevant laws and regulations, and then you can start the use of target recognition related functions with consent.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right click a main device, select the target smart switch, and turn on the target smart switch

Figure 5-108 Target Intelligence

Step 3 Click **OK**.

----End

Turn on the target intelligent switch of the main device

This step should be started in all scenes where the target recognition function needs to be used.

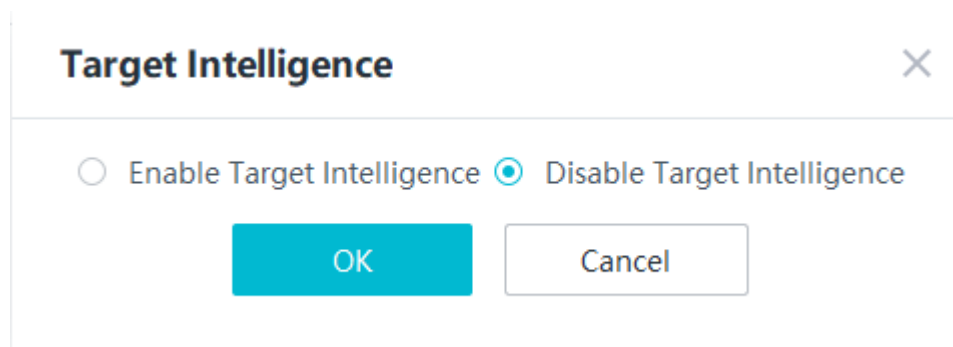
NOTE

- The use of target intelligence in business scenarios needs to be subject to legal constraints. Therefore, before starting the target intelligence function, you need to know the relevant laws and regulations, and then you can start the use of target recognition related functions with consent.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right click a video camera, select the target smart switch, and turn on the target smart switch

Figure 5-109 Target Intelligence



Step 3 Click **OK**.

----End

Configuring the Algorithm Mode

Perform the following steps only for Dxxxx-10-SIU cameras.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Smart Global Configuration > Algorithm Mode**.

Step 3 Set **Algorithm Mode** to **Target checkpoint**.

NOTE

After the algorithm mode is switched, the camera will restart for the setting to take effect. Wait for 3 minutes and then set intelligent services.

Step 4 Click **Save**.

----End

Setting Target Parameters

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera connected to a main device and choose **Target Capture > Target Parameters**.
- Step 3** Enable the target capture function and set parameters, as shown in [Figure 5-110](#). [Table 5-94](#) describes the parameters and buttons.

Figure 5-110 Setting target parameters

Table 5-94 Parameter/Button description

Parameter/Button		Description
Parameter Settings	Target Capture	Indicates whether to enable target capture. NOTE This function is mutually exclusive with behavior analysis and situation awareness. Before enabling this function, ensure that behavior analysis and situation awareness are disabled.
	Target Attributes	Indicates whether to enable target attribute recognition, which is supported by some camera models. After this function is enabled, you can view information such as the age and gender of the captured target on the target recognition page.
	Detection Mode	Detection mode. • Target detection: detects only targets. • Person detection: detects only persons. • Both: detects both targets and persons.

Parameter/Button		Description
	Capture Mode	Snapshot mode. • Optimal: When a target is in the view, the camera takes snapshots of the target and evaluates each snapshot. After the target leaves the view, the snapshot with the optimal quality is selected as the snapshot result. - This mode applies to most target capture scenarios and ensures optimal quality of snapshots. • Fast: When a target enters the detection area, the camera takes snapshots of the target and evaluates each snapshot. The target snapshot that meets the requirement is used as the snapshot result. Then the camera still detects the target but does not take snapshots of the target. • Scheduled: When a target enters the detection area, the camera takes snapshots of the target and generates a snapshot with the optimal quality at a specified interval.
	Alarm Check Interval (s)	Interval at which alarms are checked.
	Target Detection Sensitivity	Target detection sensitivity. The value ranges from 1 to 5. A larger value indicates a higher sensitivity.
	Person Detection Sensitivity	Person detection sensitivity. The value ranges from 1 to 5. A larger value indicates a higher sensitivity.
	Min Target	Maximum and minimum size of targets that can be detected.
	Max Target	
Advanced Parameters	Send Target Images	Indicates whether to send target/person cutouts and full images.
	Send Person Images	
	Send Full Images	
	Brightness Compensation	Indicates whether to enable brightness compensation. Open: Enables this function. After this function is enabled, the exposure is automatically decreased in highlight or increased in backlight to ensure ideal brightness in different environments. Close: Disables this function.

Parameter/Button		Description
	Target Snapshot Quality	Image quality of target/person snapshots and full images. The value ranges from 1 to 5. A larger value indicates higher quality. Higher image quality consumes more storage space.
	Person Snapshot Quality	
	Full Image Quality	
	Compensation Coefficient	Maximum brightness compensation coefficient. The default value is 50 . The camera will automatically adjust the compensation level within the specified range based on the image brightness. The value of this parameter can be properly increased in frontlight or backlight conditions.
	Exposure Duration (min)	Duration of target exposure, in minutes. When a target is detected, target exposure is performed for a specified period of time. You are advised to set this parameter to 10 minutes in densely populated scenarios and 5 minutes in sparsely populated scenarios.
Area Settings	Area	Button for adding areas. You can click once to add the Direction Area and click twice to add the Non-detection Area .
	Delete	Button for deleting a selected detection area or non-detection area.

Step 4 Click **Save**.

----End

Configuring Target Recognition

Perform the following steps only for Dxxx-10-SIU cameras.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Target Capture > Target Recognition**.

Step 3 Toggle-on **Enable target recognition**, as shown in [Figure 5-111](#).

Figure 5-111 Configuring target recognition

Enable target recognition ☒

Target recognition model SDC_FR V1.9.0b030s001

Target parameter model SDC TRAFFIC FACE V809

Feature Usage Mode Personal feature ▼

Personal feature

Access Control

Save Cancel

Step 4 Set **Feature Usage Mode** based on the site requirements. The following options are available:

- **Personal feature:** extracts features from an optimal target snapshot and reports the match result.

NOTE

When **Feature Usage Mode** is set to **Personal feature**, **Snapshot Mode** must be set to **Optimal**.

- **Access Control:** reports extracted features multiple times for target match, ensuring smooth access control.

NOTE

- The **Access Control** mode applies only to access control scenarios when up to four targets are queuing in the camera view.
- When **Snapshot Mode** is set to **Fast**, **Feature Usage Mode** must be set to **Access Control**.

Step 5 Click **Save**.

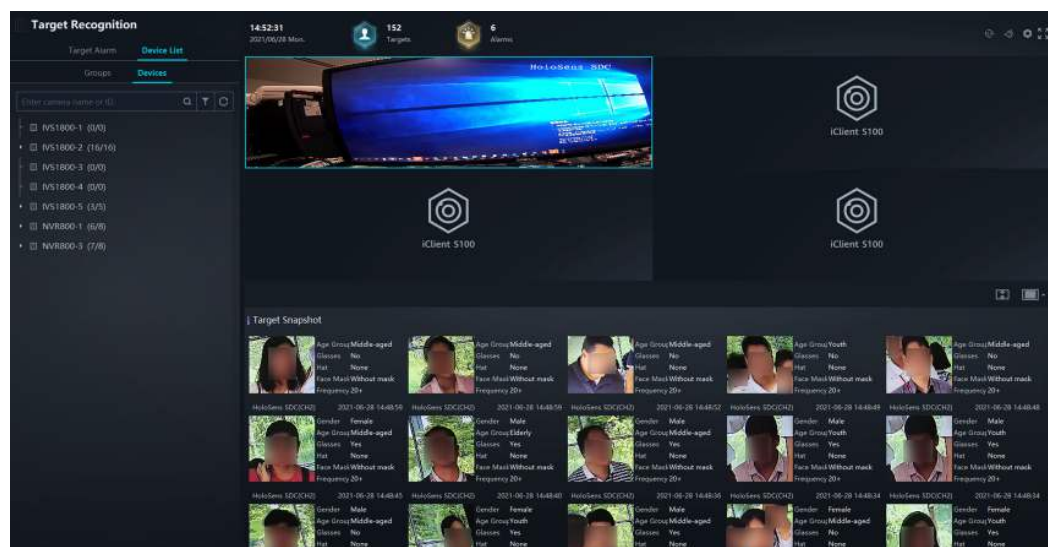
----End

Verification

Step 1 On the iClient S100 home page, choose **Intelligent Applications > Target Recognition**.

Step 2 Drag the required camera to the video pane. Target recognition results and snapshots will be displayed under the video pane in real time, as shown in [Figure 5-112](#).

Figure 5-112 Target recognition results



----End

5.7.1.2 Mask Detection

Application Scenario

In some public areas, pedestrians need to wear masks to meet health and safety requirements. In this scenario, you are advised to enable the mask detection function so that the system reports an alarm to the iClient S100 when detecting a person not wearing a mask.

Procedure

- Step 1** Choose **Maintenance Management > Smart Configuration** on the iClient S100 home page.
- Step 2** Select a camera under a main device and choose **Target Snapshot > Mask Recognition**
- Step 3** Set **Alarm Type** to **None**, as shown in [Figure 5-113](#).

Figure 5-113 Mask detection

The screenshot shows a configuration window for mask detection. At the top, there is a label 'Alarm Type' above a dropdown menu. The dropdown menu is open, displaying three options: 'None' (which is highlighted with a grey background), 'Exits', and 'Close'. Below the dropdown menu, there are two buttons: a blue 'Save' button and a grey 'Cancel' button.

Step 4 Click **Save**. Choose **Intelligent Applications > Target Recognition**. Then you can view the mask detection result in real time.

----End

5.7.2 Target Intelligence (Based on IVS1800)

5.7.2.1 Target List Management

Application Scenario

List libraries are classified into two types: **Deny List** and **Allow List**. [Table 5-95](#) describes the application scenarios and functions of these types of list libraries.

Table 5-95 List library types

List Library Type	Application Scenario
Deny list	Used in scenarios such as swing gates, security gates, and straight-through pedestrian walkways. The system generates an alarm once a blocklisted target is detected.

List Library Type	Application Scenario
Allow list	Used in scenarios such as swing gates and security gates. The system generates an alarm once an allowlisted target is detected.

Prerequisites

You have added target images for persons in a target alert task on the **Personal** page. For details, see [6.1.4 Adding Persons](#).

Creating a List Library

Step 1 Create a list library.

1. Choose **Maintenance Management > Personnel Management** on the iClient S100 home page.
2. Click the **List Library** tab.
3. On the list library page, click **New** and create a list library, as shown in [Figure 5-114](#). Click **OK**.

Figure 5-114 Adding a list library

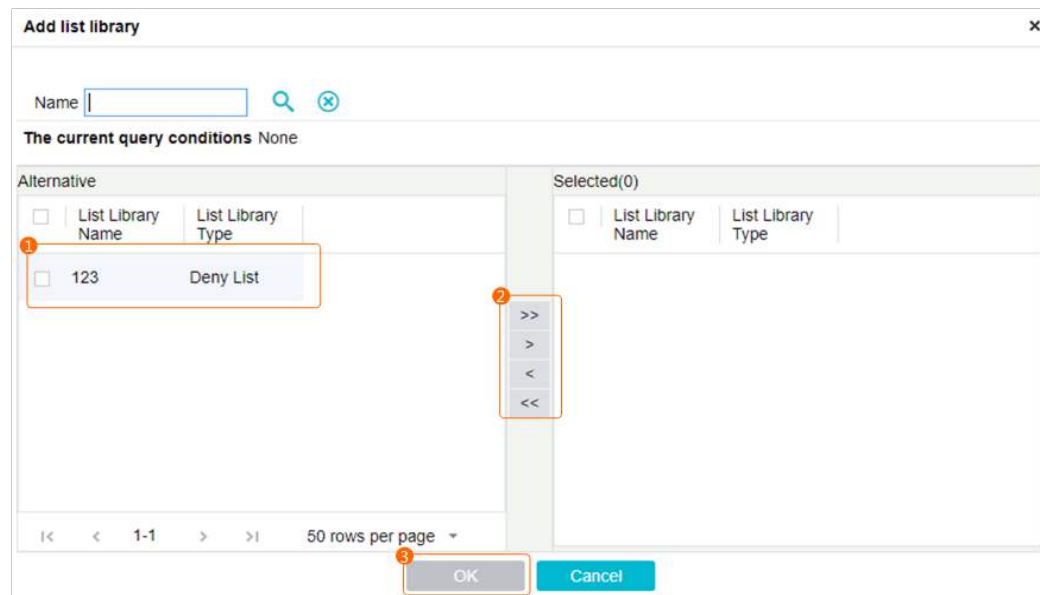
4. Click **Add People** to add the person created on the **Personal** page to the current list library.

Step 2 Synchronize the list library.

1. On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
2. Right-click a device and choose **Target Library**.

- Click **Select Personnel List** and move the list library (under **Alternative**) created on the **Personal** page to the list library (under **Selected**) on the right, as shown in [Figure 5-115](#).

Figure 5-115 Synchronizing the list library



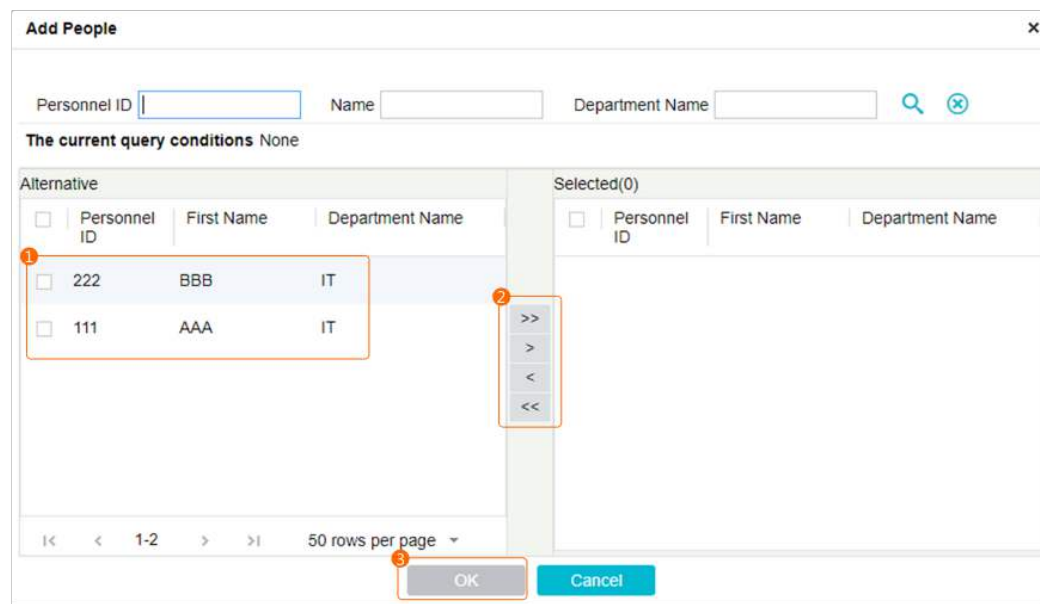
- Click **OK**.

Step 3 Synchronize person information.

- In the list library list, select the list library to which you want to add person information and click **Sync People**.
- Move the persons (under **Alternative**) created on the **Personal** page to the list library (under **Selected**) on the right, as shown in [Figure 5-116](#).

NOTE

The synchronized person information will be used for target alert. target images of such persons must be uploaded on the **Personal** page. Otherwise, the person information will fail to be synchronized.

Figure 5-116 Synchronizing person information

3. Click **OK**.

----End

5.7.2.2 Target Search

Application Scenario

You can perform target search in either of the ways listed in the following table.

Table 5-96 Target search modes

Search Mode	Description	Data Source
Search by image	After a target image is imported to the iClient S100, the system automatically extracts target features from the image and searches for targets based on the features.	Data generated by the target recognition task created for a camera.
Search by criteria	After target search criteria are entered, the system searches for matched target images based on the search criteria.	- Generic cameras: data generated by the created target recognition task. - Cameras that support target detection: metadata updates automatically subscribed by the IVS1800. No analysis task needs to be created.

This section describes how to configure target recognition tasks to extract target features and how to search for targets by image and criteria.

Prerequisites

- You have installed the target recognition algorithm plug-in for the IVS1800 on the OMU portal.
- You have added a target list and target information in it to the target library.
- You have set image storage parameters in scenarios where intelligent cameras are used. To set image storage parameters, choose **Maintenance Management > Video Device > Device List > Main Devices** on the iClient S100 home page. Right-click an IVS1800, choose **Storage Management** from the shortcut menu, and select a camera.

(Optional) Creating a Target Recognition Task

NOTE

The IVS1800 storage model (for example, IVS1800-B08 and IVS1800-B16) does not support the backend intelligent analysis function.

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Task Management**.
- Step 3** Click **New Task**.
- Step 4** Select a camera and set target recognition task parameters, as shown in [Figure 5-117](#). [Table 5-97](#) describes the parameters.

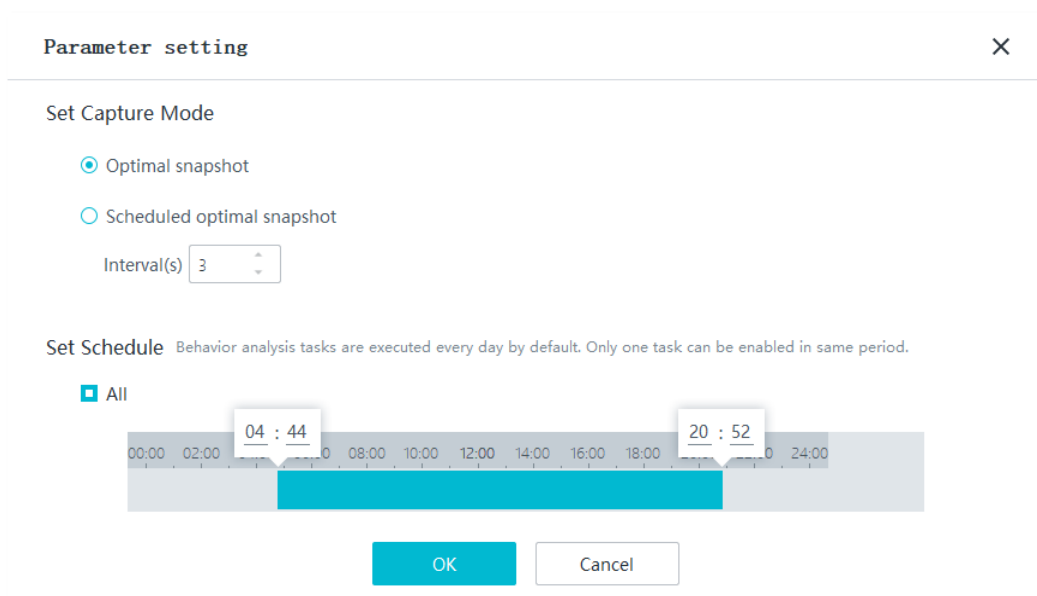
Figure 5-117 Creating a target recognition task

The screenshot displays the 'Cameras' management interface. On the left, a list of cameras is shown, with '9.49facevideo' highlighted. On the right, the configuration panel for the selected camera is visible. It includes a search bar, a 'Preview Task' button, and a 'Task Type' section where 'Target recognition' and 'Multifunc_alg_D' are selected. The 'Save' button is highlighted at the bottom.

Table 5-97 Target recognition task parameters

Parameter	Description
Video Type	Video type. The options are Live and Recorded .
Analysis Period	Recording period. Recordings generated within this period are used for target recognition. Set this parameter only when Video Type is set to Recorded .
Task Type	Task type. Select Target recognition and select an algorithm.

Step 5 In the dialog box that is displayed, set the snapshot mode and task execution plan, as shown in [Figure 5-118](#). [Table 5-98](#) describes the parameters.

Figure 5-118 Configuring a task execution plan**Table 5-98** Parameters for configuring a task execution plan

Parameter		Description
Set Capture Mode	Optimal snapshot	In this mode, this system detects targets in the video image and selects the optimal image as the snapshot result.
	Scheduled optimal snapshot	This mode is applicable to scenarios where an object stays in the image for a long period of time. In this mode, the system captures targets in the video image within the specified snapshot period (indicated by Interval) and selects the optimal image as the snapshot result.
Set Schedule		Set the time for executing the task every day.

Step 6 Click **OK**.

Step 7 Click **Save**.

----End

Search by Image

Step 1 On the iClient S100 home page, choose **Basic Operations > Search > Search By Image**.

Step 2 (Optional) Click **More** and set search criteria based on the site requirements. [Table 5-99](#) describes the parameters.

Table 5-99 Parameters for target search by image

Parameter	Description
Period	Period during which the target images are captured. • Select Past 3 Days, Past Week, or Past Month. • Alternatively, specify a period in the calendar.
Match	Threshold of similarity to the target for search.
Source	Cameras from which target images are searched for. You can select multiple cameras from various main devices.

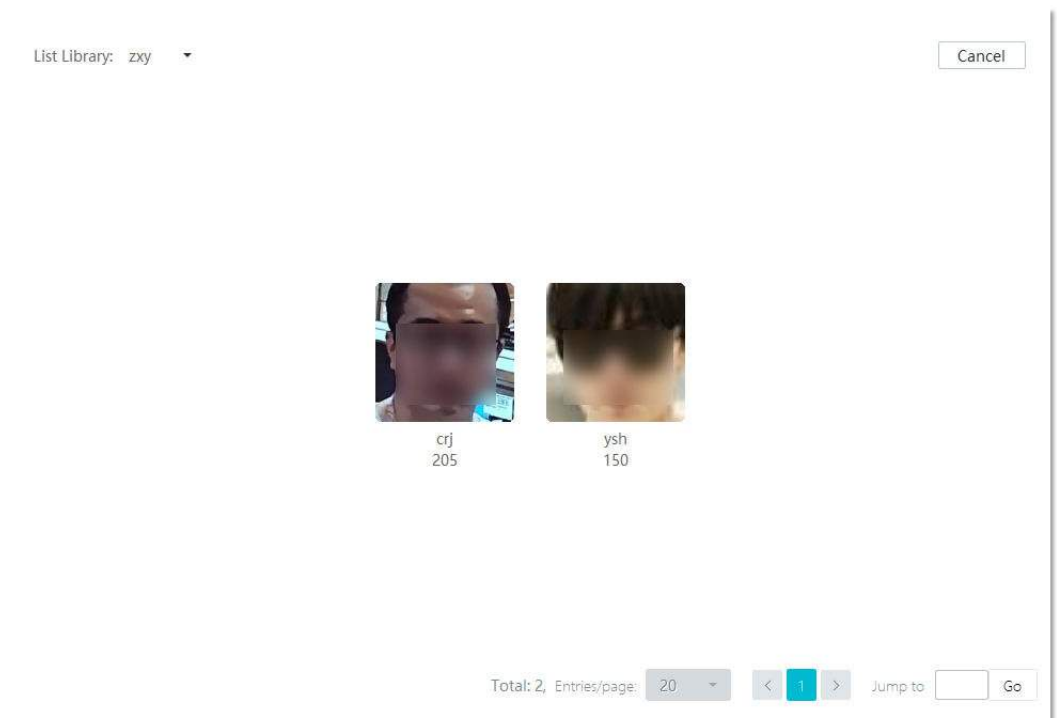
Step 3 Upload a target image for target search.

The options are as follows:

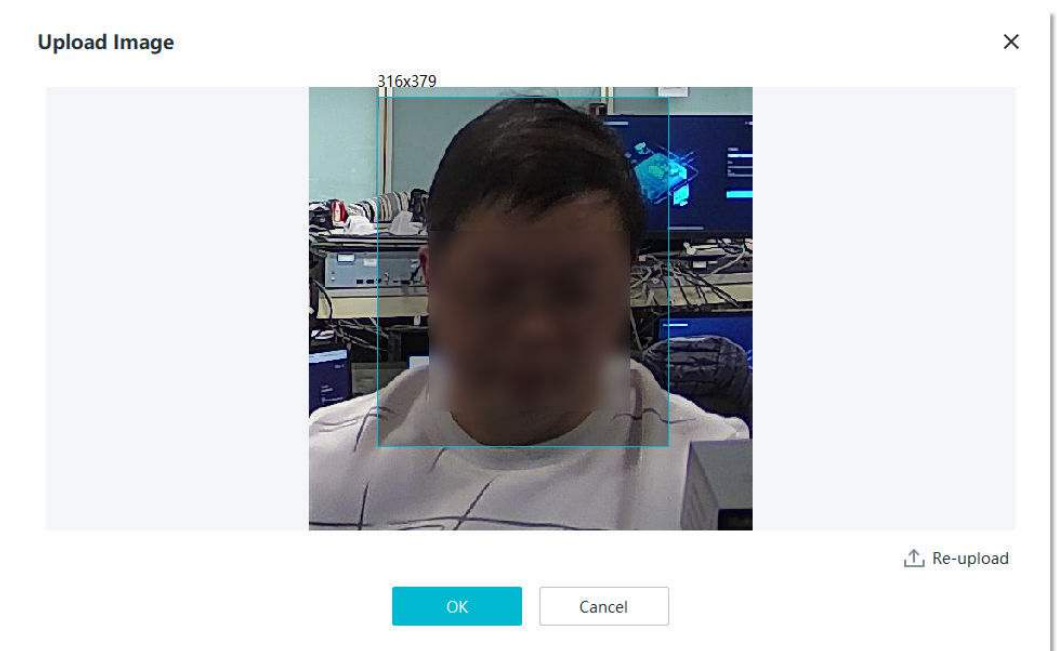
- Enter the full ID number or name in the search box and select the target image for target search from the drop-down list box.



- Click  next to the search box, and click  in the drop-down list box that is displayed. The page shown in [Figure 5-119](#) is displayed. Select a list library in the upper left corner and click a target image in the list library to start target search by image.

Figure 5-119 Search by list library

- Drag a target image to the search box. On the **Upload Image** page that is displayed, box-select the required target part and click **OK**, as shown in [Figure 5-120](#).

Figure 5-120 Box-selecting the required target part

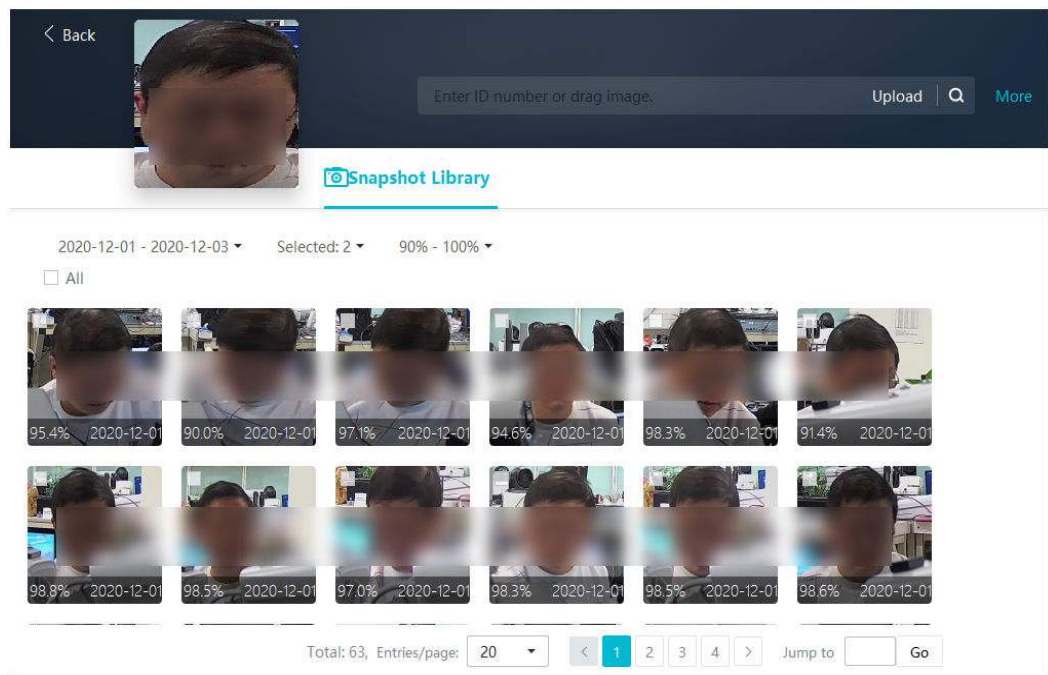
NOTE

The target image to be uploaded must meet the following requirements:

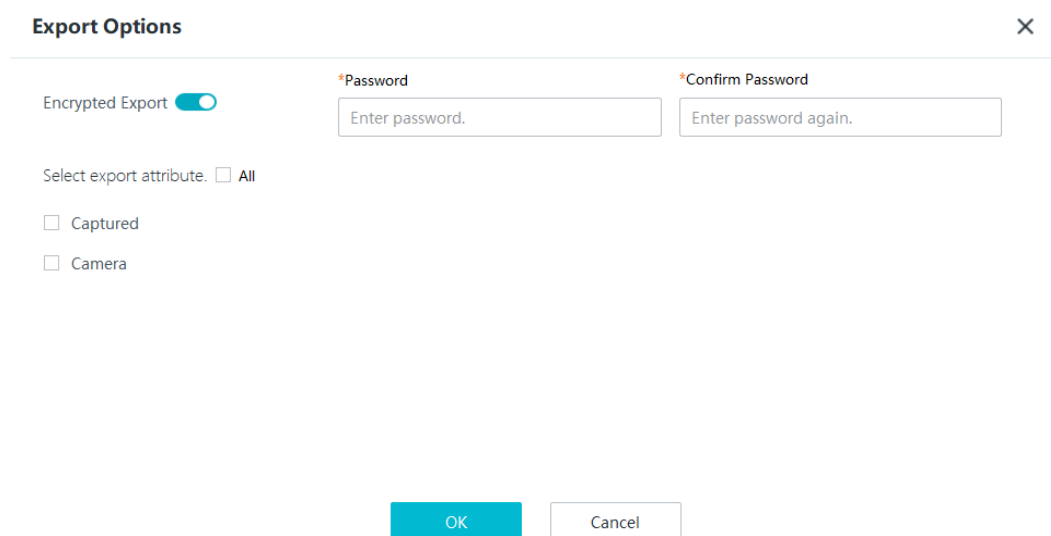
- The image file format must be .jpg, .jpeg, .jpe, .dib, .bmp, or .png.
- The image size cannot exceed 5 MB, and the image resolution cannot exceed 4096 x 3000 pixels.
- The resolution of the selected target area ranges from 60 x 60 pixels to 800 x 1200 pixels.

Step 4 Wait until the search result is displayed, as shown in [Figure 5-121](#).

Figure 5-121 Result of target search by image



Step 5 (Optional) Select **Export Selected**, **Export This Page**, or **Export All** from the **Export** drop-down list as required. [Figure 5-122](#) shows the file export dialog box.

Figure 5-122 Export OptionsThe image shows a dialog box titled "Export Options" with a close button (X) in the top right corner. Inside the dialog, there is a section for "Encrypted Export" with a toggle switch that is currently turned on. Below this, there is a label "Select export attribute." followed by a checkbox labeled "All". Underneath, there are two more checkboxes: "Captured" and "Camera". To the right of the "Encrypted Export" section, there are two input fields. The first is labeled "*Password" and contains the text "Enter password.". The second is labeled "*Confirm Password" and contains the text "Enter password again.". At the bottom of the dialog, there are two buttons: "OK" (in blue) and "Cancel" (in white with a grey border).**NOTE**

You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files.

----End

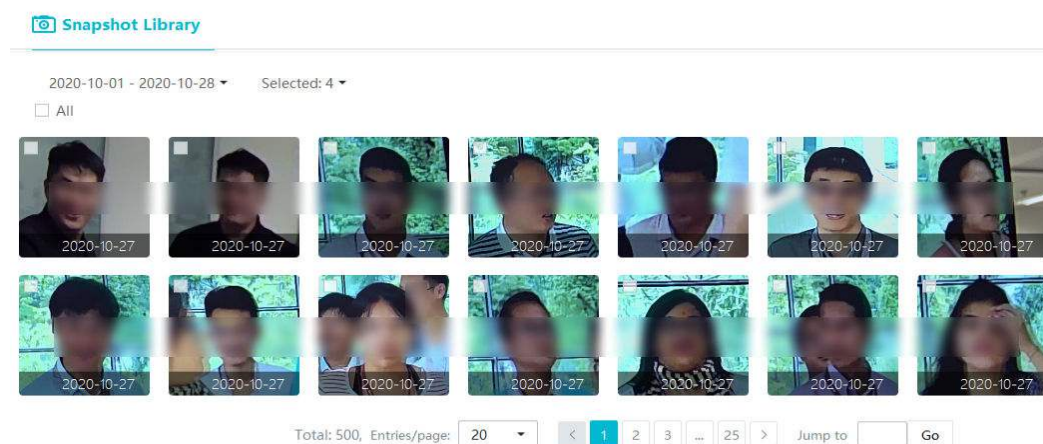
Search by Criteria

- Step 1** On the iClient S100 home page, choose **Basic Operations > Search > Target Search**.
- Step 2** Set search criteria. [Table 5-100](#) describes the parameters.

Table 5-100 Parameters for target search by criterion

Parameter	Description
Source	Cameras from which target images are searched for. You can select multiple cameras from various main devices.
Captured	Period during which the target images are captured.

- Step 3** Click **Search**. The **Snapshot Library** tab page is displayed with the search result, as shown in [Figure 5-123](#).

Figure 5-123 Result of target search by criterion

- Step 4** (Optional) Use a clear target image for secondary search to obtain more target images. Click a target image in the search result. On the details page that is displayed, click **Search**.
- Step 5** (Optional) Select **Export Selected**, **Export This Page**, or **Export All** from the **Export** drop-down list as required. [Figure 5-124](#) shows the file export dialog box.

Figure 5-124 Export Options

NOTE

You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files.

----End

5.7.2.3 1:1 Target Match

With the 1:1 target match feature, you can:

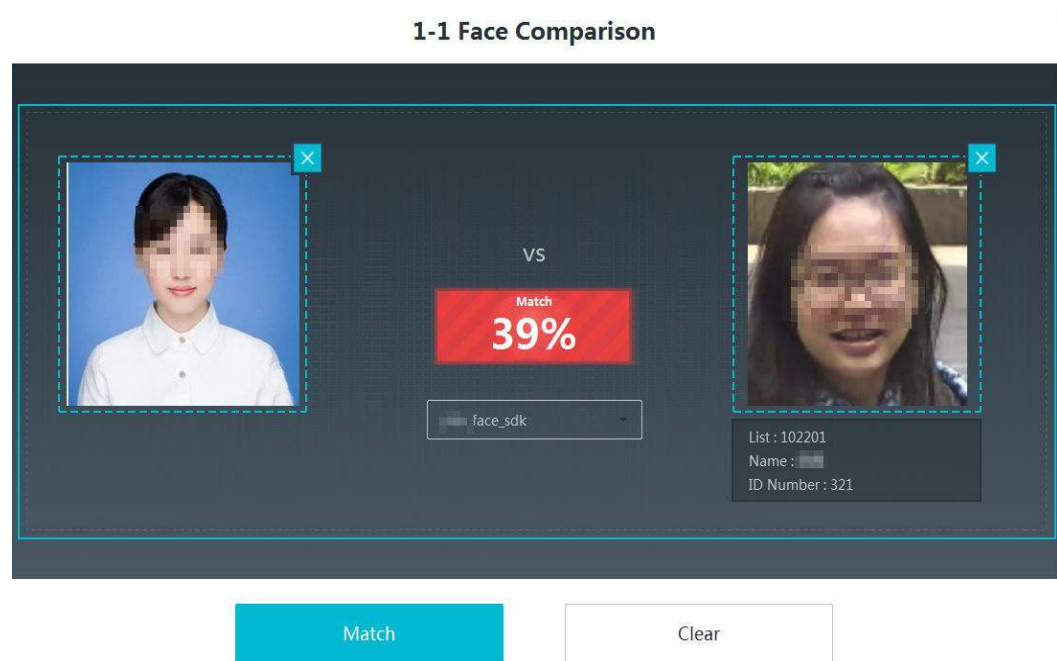
- Match two uploaded target images.
- Match an uploaded target image with target images in the target library.

The obtained similarity helps related personnel determine whether a person is the desired one. The following describes the procedure.

Procedure

- Step 1** Choose **Basic Operations > Search > 1:1 Target Match** on the iClient S100 home page.
- Step 2** Click **+** on the left, select a target image, and click **Open**.
- Step 3** Enter an ID number in the **Enter ID number** text box in the lower part and search for target images in the target library based on the ID number. Select a target image.
- Step 4** Select an algorithm and IVS1800 device used for the 1:1 target match in the box under **VS**.
- Step 5** Click **Match**. The 1:1 target match result is displayed, as shown in [Figure 5-125](#).

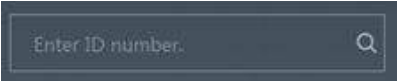
Figure 5-125 Target match



Click **Clear** to restore to the initial page. [Table 5-101](#) describes the parameters.

Table 5-101 Parameter description

Parameter/Icon	Description
	Uploads the target image to be matched.

Parameter/Icon	Description
	Specifies an ID number to search for target images in the target library.
	Selects an IVS1800 device.
	Specifies the target recognition algorithm for 1:1 target match.
Match	Starts 1:1 target match.
Clear	Deletes target images and match results and restores to the initial page.

----End

5.7.2.4 List-based Target Alert

5.7.2.4.1 Application Scenario

The target alert feature can be used to recognize targets in a detection area and generate alarms for targets. Target alert functions are usually used in scenarios such as swing gates, security gates, and building entrances and exits. Example:

A building has strict security requirements. Only trustlisted persons are allowed to enter the building. If a person not in the trustlist, for example, a resigned employee or a blocklisted person, attempts to enter the building, the system will generate an alarm, instructing the security personnel to restrict the person's access.

5.7.2.4.2 Prerequisites

- The target recognition algorithm plug-in has been installed for the IVS1800 on the OMU portal.
- You have created a target list on the **Personal** page, imported person information in the target list, and synchronized the target list to the target list of the IVS1800. For details, see [5.7.2.1 Target List Management](#).

5.7.2.4.3 Procedure

NOTE

The IVS1800 storage model (for example, IVS1800-B08 and IVS1800-B16) does not support the backend intelligent analysis function.

Creating a Target Recognition Task

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an IVS1800 and choose **Task Management**.

Step 3 Click **New Task**.

Step 4 Select a camera and set target recognition task parameters, as shown in [Figure 5-126](#). [Table 5-102](#) describes the parameters.

Figure 5-126 Creating a target recognition task

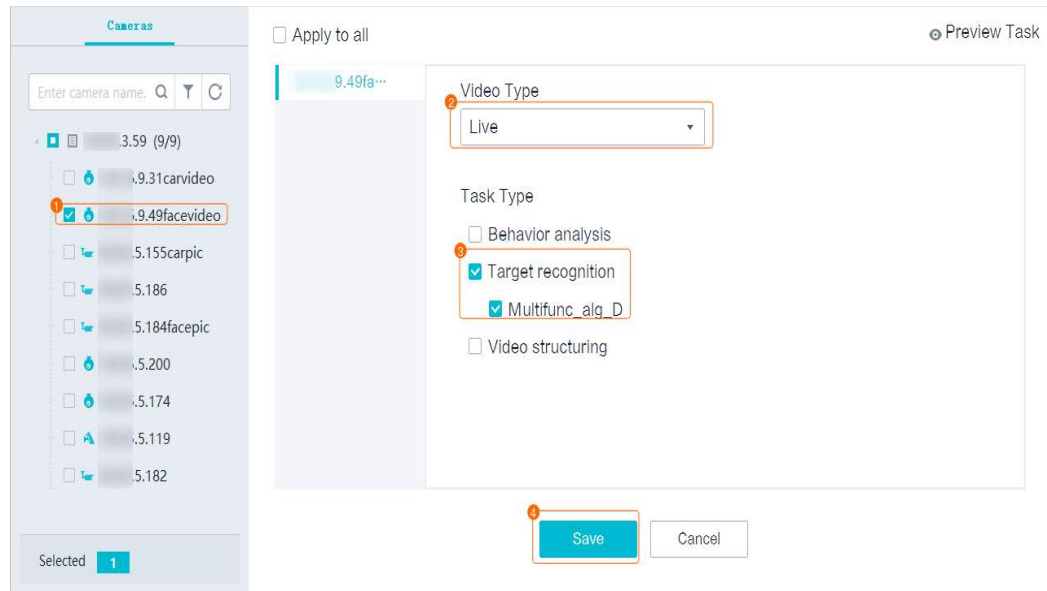


Table 5-102 Target recognition task parameters

Parameter	Description
Video Type	Video type. The options are Live and Recorded .
Analysis Period	Recording period. Recordings generated within this period are used for target recognition. Set this parameter only when Video Type is set to Recorded .
Task Type	Task type. Select Target recognition and select an algorithm.

Step 5 In the dialog box that is displayed, set the snapshot mode and task execution plan, as shown in [Figure 5-127](#). [Table 5-103](#) describes the parameters.

Figure 5-127 Configuring a task execution plan

Parameter setting

Set Capture Mode

☒ Optimal snapshot

☐ Scheduled optimal snapshot

Interval(s)

Set Schedule Behavior analysis tasks are executed every day by default. Only one task can be enabled in same period.

☒ All

00:00 02:00 04:44 08:00 10:00 12:00 14:00 16:00 18:00 20:52 22:00 24:00

OK Cancel

Table 5-103 Parameters for configuring a task execution plan

Parameter		Description
Set Capture Mode	Optimal snapshot	In this mode, this system detects targets in the video image and selects the optimal image as the snapshot result.
	Scheduled optimal snapshot	This mode is applicable to scenarios where an object stays in the image for a long period of time. In this mode, the system captures targets in the video image within the specified snapshot period (indicated by Interval) and selects the optimal image as the snapshot result.
Set Schedule		Set the time for executing the task every day.

Step 6 Click **OK**.

Step 7 Click **Save**.

----End

Creating a Target Alert Task

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an IVS1800 and choose **Target Alerts**.

Step 3 Click **New Alert Task**. On the **New Task Info** page shown in [Figure 5-128](#), set alert task parameters. [Table 5-104](#) describes the parameters.

Figure 5-128 Configuring a target alert task

Alert Basic Information

* Name

Period
☒ One Week ☐ One Month ☐ One Year ☐ Permanent 2022-04-08 - 2022-04-15

* Object ☐

Algorithm

Audio file

Playback times
 1 5

Temperature Alert
☐

Severity
☒ Critical ☐ Major ☐ Minor ☐ Warning

Alarm Type
☒ When listed detected ☐ When non-listed detected

Scope

Sequential Alert
☒ Yes ☐ No

Mask Alert
☒ Tip: whether to wear a mask cannot be recognized in black-and-white mode.

Mask Alert Type
☒ Without mask ☐ With mask

Mask alarm audio output

Mask alarm audio playback times
 1 5

Table 5-104 Parameters for creating a target alert task

Parameter	Description
Alert Task Name	Alert task name.
Active	Time range for executing a target alert task. • Select One Week, One Month, or One Year. • Specify a period in the calendar. • Click Set Hours to set the time segment for alert every day.
Alert Object	Alert target. Select a blocklist or trustlist for alert based on the site requirements.
Algorithm	Algorithm. Select For all algorithms and set Match Threshold (%) . Match Threshold (%) : When the similarity between a target detected in real time and the target in the alarm reference list is greater than or equal to the threshold, the two targets match. The value is accurate to six decimal places. • A smaller threshold indicates more matched targets, lower false negative rate, and higher false positive rate. • A higher threshold indicates fewer matched targets, lower false positive rate, and higher false negative rate.

Parameter	Description
Temperature Alert	Indicates whether to enable the temperature alarm based on the site requirements. (Optional. When this function is enabled, thermal cameras need to be installed.) Temperature Threshold: Set this parameter based on the site requirements. When the temperature of the alert target is greater than the alert threshold, an alarm is generated.
Alert Level	Importance and urgency of an alert task. Select an option based on the site requirements. The severity of alarms generated by an alert task depends on the importance and urgency of the task. For example, if this parameter is set to Critical, the severity of alarms generated by this alert task is also Critical.
Alarm Type	• When listed detected: When the recognized target matches the target specified by Alert Object, an alarm is generated. • When non-listed detected: When the recognized target does not match the target specified by Alert Object, an alarm is generated.
Alert Scope	Alert scope. Click the text box under Camera and select cameras from the camera list. A maximum of 64 cameras can be selected.
Send alarm in order	Select Yes or No. When you select multiple alert targets, the IVS1800 matches captured images with the images in the lists based on list creation time. If a target is detected in a list, the IVS1800 does not match it with the images in other lists. Set this parameter based on the site requirements.
Audio file	When the target fortification alarm is triggered, the camera will play audio files.
Playback times	When the target fortification alarm is triggered, the camera will play the corresponding number of audio files.
Mask Alert	Indicates whether to enable mask alert. You can select a mask alert type based on the site requirements. The options are as follows: • Without mask: When the system detects that the target in the target alert task does not wear a mask, an alarm is generated. • With mask: When the system detects that the target in the target alert task wears a mask, an alarm is generated. • Audio file: When the target fortification alarm is triggered, the camera will play audio files. • Playback times: When the target fortification alarm is triggered, the camera will play the corresponding number of audio files.

----End

5.7.2.4.4 Verification

Step 1 Choose **Complex Applications > Video Alarm > Target Alert Alarm** on the iClient S100 home page.

Step 2 Search for target alert alarms, as shown in [Figure 5-129](#).

Figure 5-129 Target alert alarms

You can view alarm details and export alarm information, as described in [Table 5-105](#).

Table 5-105 Operation description

Operation	Description
View alarm details	View alarm details by clicking an alarm. The following functions are available: • Live: Click this button to view the live video shot by the camera for which the alarm is generated. • Playback: Click this button to play back video recorded by the camera for which the alarm is generated. • target Search: Click this button to search for images of the target for which the alarm is generated. • Task View: Click this button to view information about the alert task that generates the alarm.
Export alarm information	Export the target alert alarms to an Excel file and save the file to the local computer. • Export Selected: Click this button to export the selected alarms. • Export This Page: Click this button to export all alarms on the current page. • Export All: Click this button to export all the found alarms.

----End

5.7.2.5 Target Recognition Attendance

Procedure

- Step 1** Create a target list for target recognition attendance by referring to [5.7.2.1 Target List Management](#).
- Step 2** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 3** Create a target alert task by referring to [5.7.2.4 List-based Target Alert](#).
- Step 4** Set related parameters on the **New Task Info** page.
1. Select a target list for target recognition attendance.
 2. Set **Alarm Type** to **When listed detected**.
 3. Set other parameters based on the site requirements.
- Step 5** Choose **Intelligent Applications > Target Recognition** and view the target recognition attendance result in real time.

If target recognition attendance has been configured for comprehensive applications, you can view the statistics on attendance data from cameras in the attendance statistics report. For details, see "Attendance Management."

----End

5.7.2.6 VIP Recognition

Procedure

- Step 1** Create a VIP list by referring to [5.7.2.1 Target List Management](#).
- Step 2** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 3** Create a target alert task by referring to IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0268806719.xml.
- Step 4** Set related parameters on the **New Task Info** page.
1. Select a list for VIP recognition.
 2. Set **Alarm Type** to **When listed detected**.
 3. Set other parameters based on the site requirements.
- Step 5** Choose **Intelligent Applications > Target Recognition**. Then you can view the VIP recognition result in real time.

----End

5.7.3 Customer Flow Analysis

Scenario

In densely populated areas such as business districts and restaurants, the IVS1800 provides the customer flow analysis function to provide effective data support for user behavior analysis.

NOTE

Passenger flow analysis makes data statistics on the results based on the list database ratio, indicating the identification and statistical number of personnel in each list database on a certain day. Those who are not in the list database are strangers. How to distribute the list database in S100 to generate comparison data

Procedure

- Step 1** Choose **Intelligent Applications > Statistics > Target Report** on the iClient S100 home page.
- Step 2** Set the filter criteria and click **Confirm** to view the customer flow analysis result, as shown in [Figure 5-130](#). [Table 5-106](#) describes the parameters.

Figure 5-130 Customer flow analysis



Table 5-106 Parameter description

Parameter	Description
Statistical Period	Used to display statistical results in different report types. The options are Daily , Weekly , Quarterly , and Yearly .

Parameter	Description
Export	Used to export reports in different file formats. The options are EXCEL File , PDF File , and CSV File .

-----End

5.7.4 Customer Flow Statistics

Scenario

In densely populated areas such as supermarkets and campus entries and exits, the IVS1800 provides the customer flow statistics collection function to provide effective data support for user behavior analysis.

Procedure

- Step 1** Choose **Intelligent Applications > Statistics > Target Statistics** on the iClient S100 home page.
- Step 2** Set search criteria and click **OK**. You can view the crowd flow statistics result of the current device by list library and stranger, as shown in [Figure 5-131](#). [Table 5-107](#) describes the parameter and button.

Figure 5-131 Customer flow statistics

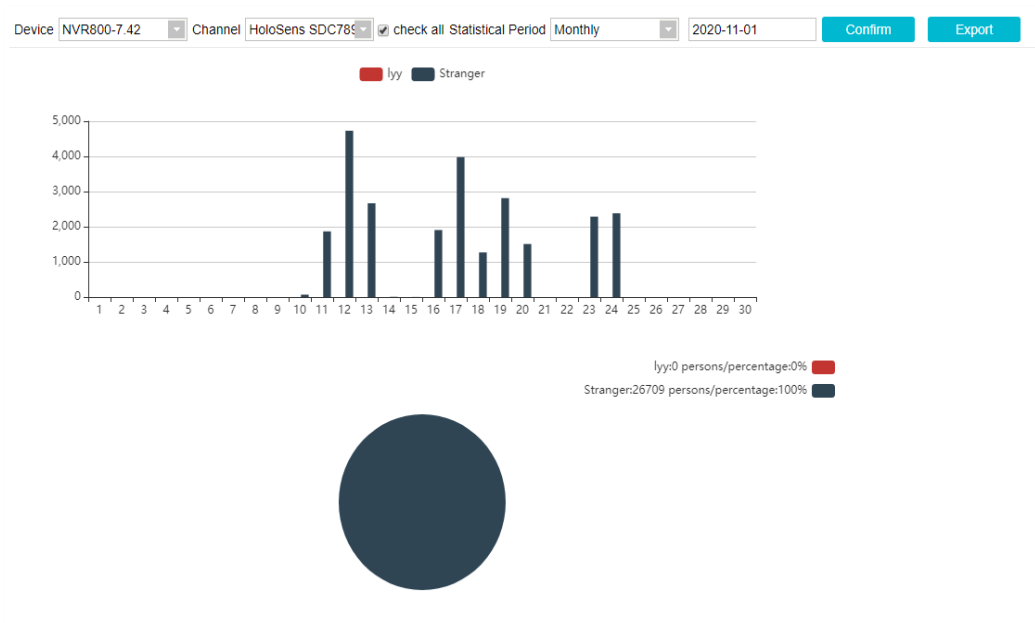


Table 5-107 Parameter/Button description

Parameter/Button	Description
Statistical Period	Used to display statistical results in different report types. The options are Daily , Weekly , Monthly , Quarterly , and Year .
Export	Used to export reports in different file formats. The options are EXCEL File , PDF File , and CSV File .

----End

5.8 Person Intelligence

5.8.1 Person Search

5.8.1.1 Application Scenario

Table 5-108 describes the person search mode.

Table 5-108 Person search mode

Search Mode	Description	Data Source
By criteria	After person search criteria are entered, the system searches for person images based on the search criteria.	- Generic cameras: data generated by the video structuring tasks created for these cameras. - Target checkpoint cameras/Object classification cameras: metadata updates automatically subscribed by the IVS1800 from these cameras. No analysis task needs to be created.

This section describes how to configure person recognition tasks to extract personal features and how to search for persons by criteria.

5.8.1.2 Prerequisites

- You have installed object classification and target recognition algorithm plug-ins for the IVS1800 on the OMU portal. For details about how to install the plug-ins, see the IVS1800 product documentation.
- You have set image storage parameters in scenarios where intelligent cameras are used. To set image storage parameters, choose **Maintenance Management > Video Device > Device List > Main Devices** on the iClient S100 home page. Right-click an IVS1800, choose **Storage Management** from the shortcut menu, and select a camera.

5.8.1.3 (Optional) Configuring a Person Recognition Task

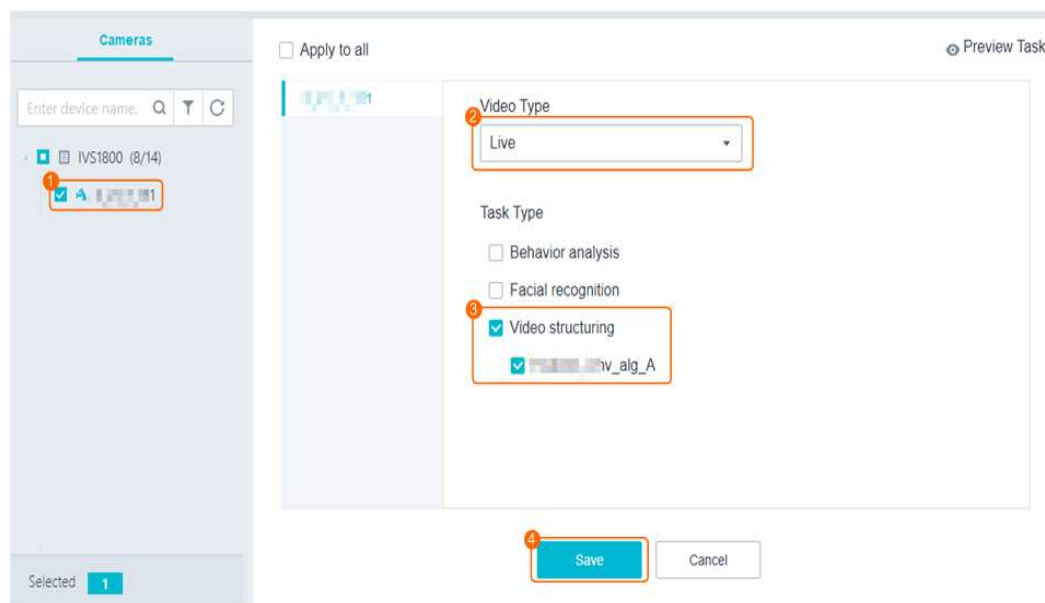
NOTE

The IVS1800 storage model (for example, IVS1800-B08 and IVS1800-B16) does not support the backend intelligent analysis function.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Task Management**.
- Step 3** Click **New Task**.
- Step 4** Create a video structuring task, as shown in [Figure 5-132](#).

Figure 5-132 Creating a video structuring task



[Table 5-109](#) describes the parameters.

Table 5-109 Parameter description

Parameter	Setting
Video Type	Video type. The options are Live and Recorded .
Analysis Period	Time range. The default value is the past 24 hours. Set this parameter only when Video Type is set to Recorded .
Task Type	Task type. Select Video structuring and select an algorithm.

----End

5.8.1.4 Verification

Filter by Criteria

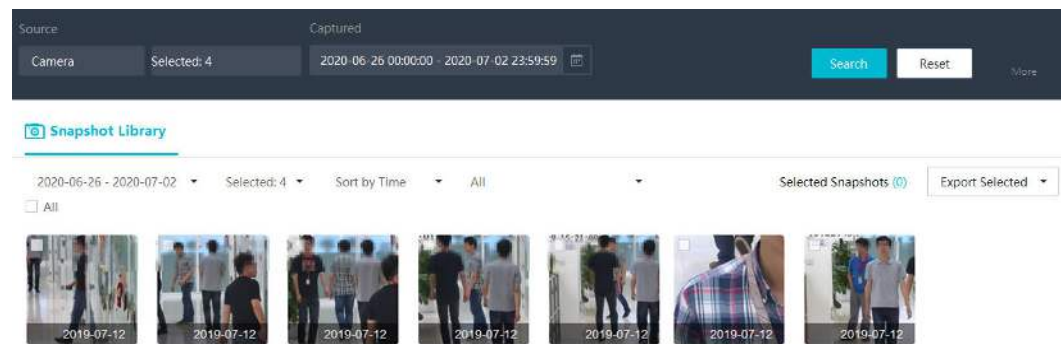
- Step 1** Choose **Basic Operations > Search > Person Search** on the iClient S100 home page.
- Step 2** Set search criteria. [Table 5-110](#) describes the parameters.

Table 5-110 Parameters for searching for persons by criteria

Parameter	Description
Source	Cameras from which person images are searched for. You can select multiple cameras from various main devices.
Captured	Period during which person images are captured.
Object Type	Type of the object for search, for example, Person or Cyclist . You can also set Tops Color , Backpack , Body Type , Helmet , Non-motorized Vehicle Color , and Non-motorized Vehicle Plate for accurate search.

- Step 3** Click **Search**. The **Snapshot Library** tab page with the search result is displayed by default, as shown in [Figure 5-133](#). The snapshot library contains person images captured by cameras and extracted by personal feature recognition tasks or video structuring tasks.

Figure 5-133 Result of person search by criteria



- Step 4** (Optional) Select multiple person images and click **Export Selected** to export the selected images. Alternatively, select **Export This Page** or **Export All** from the drop-down list box as required. [Figure 5-134](#) shows the file export dialog box.

Figure 5-134 Export Options

NOTE

You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files.

----End

5.9 Situation Analysis

5.9.1 Head Counting

Application Scenario

You can set a detection area and a detection line to collect statistics on the number of persons crossing the detection line.

When a pedestrian crosses the detection line, the system counts the number of people exiting and entering. When the sum of the two numbers reaches the preset alarm threshold, the camera reports an alarm to the main device. Then the alarm message will be displayed on the iClient S100.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Restrictions

- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.
- This function is mutually exclusive with target capture and behavior analysis. Before enabling this function, ensure that target capture and behavior analysis are disabled.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Situation Analysis > CrossLine Statistics**.
- Step 3** Enable head counting and set parameters such as detection area parameters, as shown in [Figure 5-135](#).

Figure 5-135 Configuring head counting

Parameter Settings

Enable CrossLine Statistics ☒ Enable ZeroClear ☐ Clear Statistics

Alarm Detection Interval(s) Alarm Count

Audible and Visual alarm

Audio ☐

Area Settings

+ Area + Line Delete

Plan Settings

+ Add Delete All

No.	Execution Date	Start Time	End Time	Date	Mode	Operation
1	1970-01-01	00:00:00	23:59:59	Every Day	Weekly cycle	

Save Cancel

1. Set parameters in the **Parameter Settings** area. [Table 5-111](#) describes the parameters.

Table 5-111 Parameter description

Parameter	Description
Enable ZeroClear	Indicates whether to clear statistics on the live video viewing page at 00:00 of the next day.
Clear Statistics	Clears the current statistics immediately.
Alarm Detection Interval(s)	Interval at which alarms are checked.
Alarm Count	Alarm threshold for the number of persons who cross the detection line.

2. Set audible and visual alarm parameters. [Table 5-112](#) describes the parameters.

Table 5-112 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters. [Table 5-113](#) describes the parameters.

Table 5-113 Area setting parameters

Parameter	Description
Area	Button for drawing a maximum of one detection area.
Line	Button for drawing a maximum of one detection line.

Parameter	Description
Delete	Button for deleting a selected detection area or detection line.
Direction	Direction in which a pedestrian crosses the detection line. The options are as follows: – A->B: Collects statistics on the number of pedestrians who cross the detection line from A to B. – B->A: Collects statistics on the number of pedestrians who cross the detection line from B to A.

4. Set plan parameters. [Table 5-114](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-114 Plan settings

Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

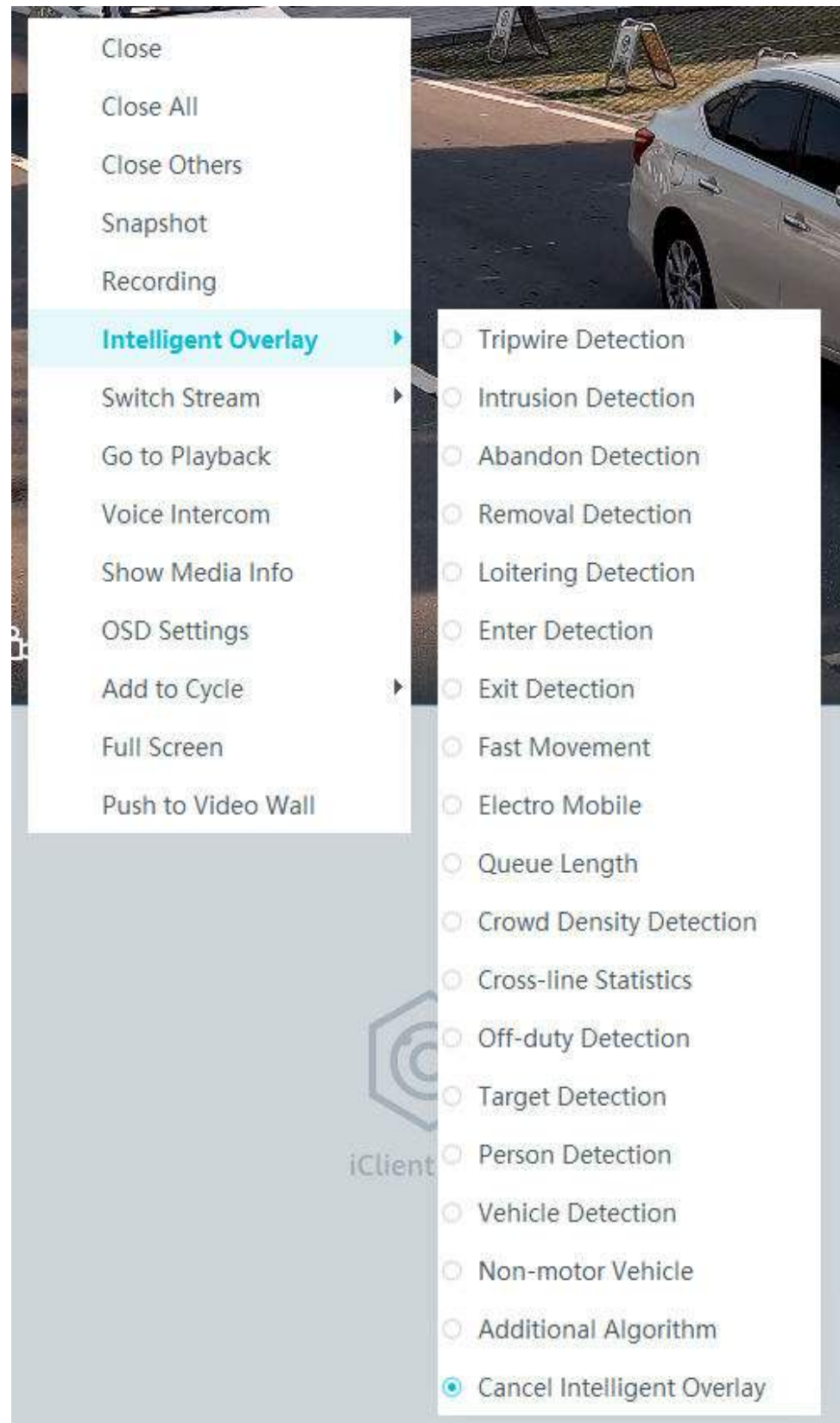
Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#))
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure](#)

5-136. The real-time intelligent analysis result is superimposed on the video image.

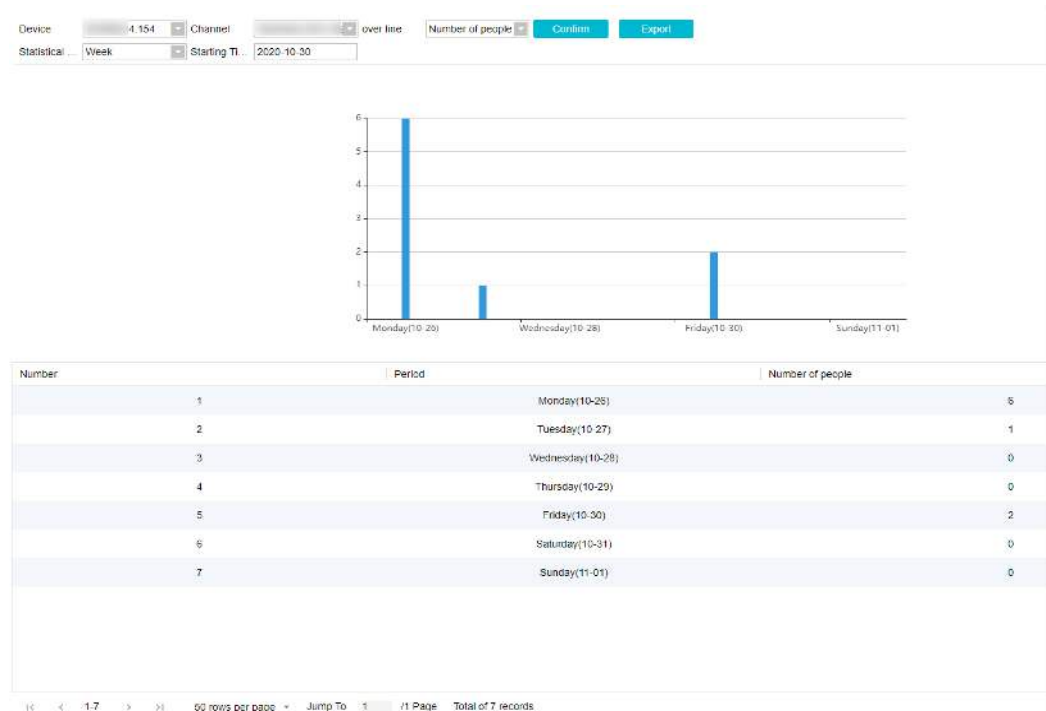
Figure 5-136 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

- Viewing statistical results
 - a. Choose **Intelligent Applications > Statistics > CrossLine Statistics** on the iClient S100 home page.
 - b. Set filter criteria and view head counting results, as shown in [Figure 5-137](#).

Figure 5-137 Head counting



5.9.2 Queue Length Detection

Application Scenario

You can set a detection area to detect the queue length in the area.

You can set the service processing duration for a single person based on the service type (such as ticket check). When the predicted total processing duration (total queuing time) in the detection area exceeds the preset threshold, the camera reports an alarm to the main devices, and the alarm message will be displayed on the iClient S100.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Restrictions

- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.

- This function is mutually exclusive with target capture and behavior analysis. Before enabling this function, ensure that target capture and behavior analysis are disabled.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera under a main device.
- Step 3** **Optional:** For cameras in multi-algorithm mode, choose **Intelligent Global Configuration > Algorithm Mode** and set **Algorithm mode** to **Behavior analysis**.

NOTE

After the algorithm mode is switched, the camera will restart for the setting to take effect. Wait for 3 minutes and then set intelligent services.

- Step 4** Choose **Situation Analysis > Queue Detect**.
- Step 5** Enable queue length detection and set parameters such as detection area parameters, as shown in [Figure 5-138](#).

Figure 5-138 Configuring queue length detection

Parameter Settings

Enable Queue Detect ☒

Alarm Detection Interval(s) Single processing time(s) Alarm threshold(min) Sensitivity

Audible and Visual alarm

Audio ☐

Area Settings

+ Area

Plan Settings

+ Add

No.	Execution Date	Start Time	End Time	Date	Mode	Operation
1	1970-01-01	00:00:00	23:59:59	Every Day	Weekly cycle	Delete

1. Set parameters in the **Parameter Settings** area. [Table 5-115](#) describes the parameters.

Table 5-115 Parameter description

Parameter	Description
Alarm Detection Interval(s)	Interval at which alarms are checked.
Single processing time (s)	Processing duration for a single person.
Alarm threshold (min)	Alarm threshold.
Sensitivity	Detection sensitivity. The value ranges from 1 to 5. A larger value indicates a higher sensitivity level.

- Set audible and visual alarm parameters. [Table 5-116](#) describes the parameters.

Table 5-116 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	- You can directly use this function when an intelligent IR/white-light camera with intercom is used. - To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	intercom support this function. You need to set parameters related to the light.
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters. [Table 5-117](#) describes the parameters.

Table 5-117 Area setting buttons

Button	Description
Area	Button for drawing a maximum of one detection area.
Delete	Button for deleting a selected detection area.

4. Set plan parameters. [Table 5-118](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-118 Plan settings

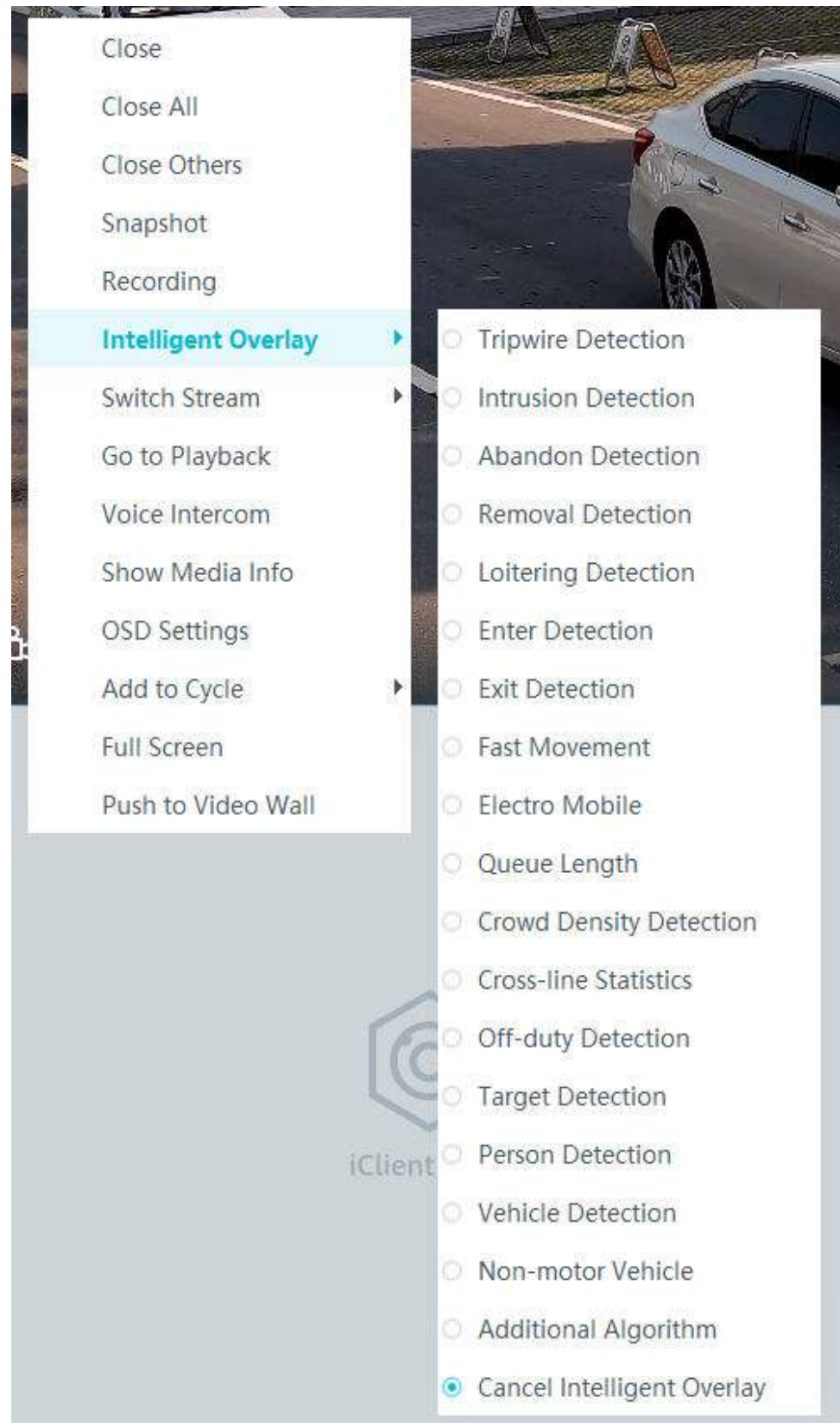
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 6 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > *Intelligent Event Name*** from the displayed menu, as shown in [Figure 5-139](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-139 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

5.9.3 Crowd Density Detection

Application Scenario

You can set a detection area to detect the crowd density in the area.

Once the number of persons in the detection area reaches the alarm threshold, the camera reports an alarm to the main device. Then the alarm message will be displayed on the iClient S100.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Restrictions

- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.
- This function is mutually exclusive with target capture and behavior analysis. Before enabling this function, ensure that target capture and behavior analysis are disabled.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Situation Analysis > Crowd Density**.
- Step 3** Enable crowd density detection and set parameters such as detection area parameters, as shown in [Figure 5-140](#).

Figure 5-140 Configuring crowd density detection

1. Set parameters in the **Parameter Settings** area. [Table 5-119](#) describes the parameters.

Table 5-119 Parameter description

Parameter	Description
Alarm Check Interval (s)	Interval at which alarms are checked.
Alarm threshold (Num)	Alarm threshold for the number of persons in a detection area.
Sensitivity	Detection sensitivity. The value ranges from 1 to 5. A larger value indicates a higher sensitivity level.

2. Set audible and visual alarm parameters. [Table 5-120](#) describes the parameters.

Table 5-120 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	– You can directly use this function when an

Parameter	Description	Requirement on Cameras
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	intelligent IR/white-light camera with intercom is used. – To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	Currently, only intelligent IR/white-light cameras with intercom support this function. You need to set parameters related to the light.
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters. [Table 5-121](#) describes the parameters.

Table 5-121 Area setting buttons

Button	Description
Area	Button for drawing a maximum of one detection area.
Delete	Button for deleting a selected detection area.

4. Set plan parameters. [Table 5-122](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-122 Plan settings

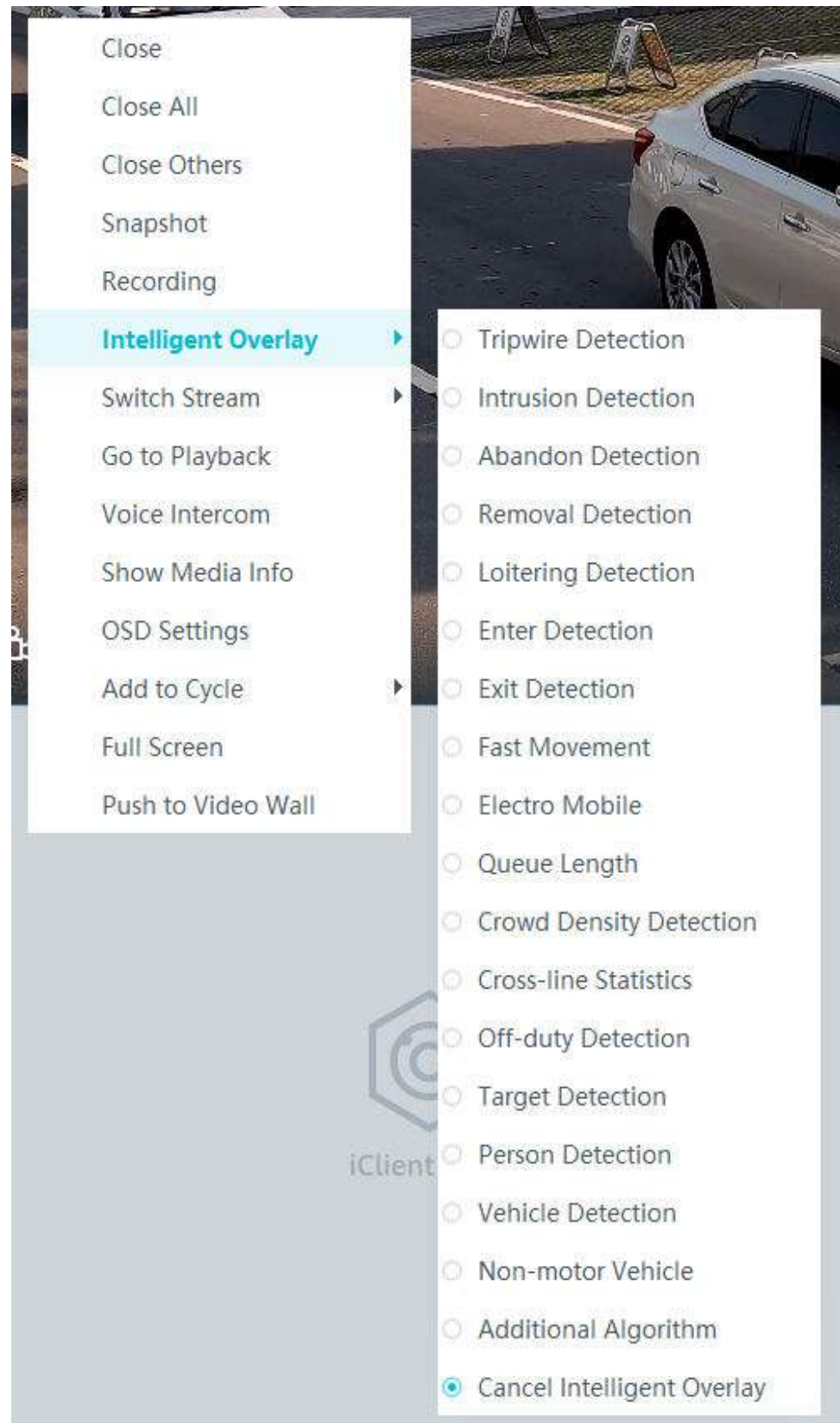
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > Intelligent Event Name** from the displayed menu, as shown in [Figure 5-141](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-141 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [5.12.1 Video Alarm](#).

5.9.4 Heat Map

Application Scenario

You can set one or more detection areas to detect the activity degree of persons in these areas. Heat maps can be displayed by time and space.

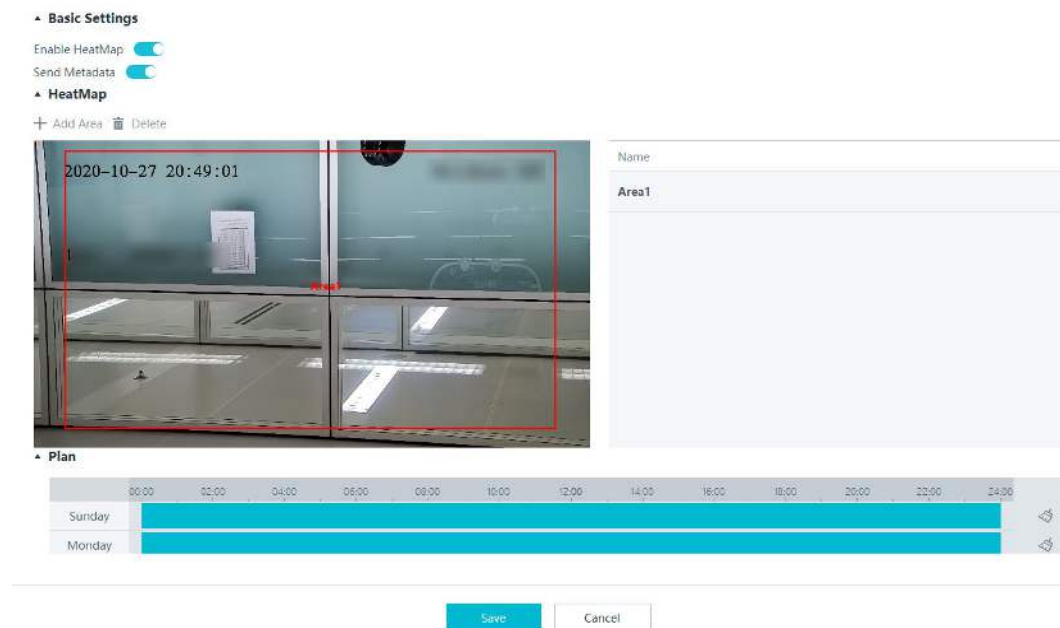
- Spatial heat map: displays the activity degree of people in different areas. The red area has the highest density and activity degree, and the blue one has the lowest density.
- Temporal heat map: displays the activity degree of people in different times. The vertical coordinate is an index calculated based on the number of people and duration of stay but does not indicate the number of persons. A larger value indicates a higher activity degree.

Restrictions

- The intelligent camera used for heat map statistics collection must be equipped with an available SD card. The heat map data will be stored in the SD card and can be stored for a maximum of one year.
- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.
- This function is mutually exclusive with behavior analysis. Before enabling this function, ensure that behavior analysis is disabled.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Situation Analysis > HeatMap**.
- Step 3** Enable heat map detection and set parameters such as detection area parameters, as shown in [Figure 5-142](#). [Table 5-123](#) describes the parameters and buttons.

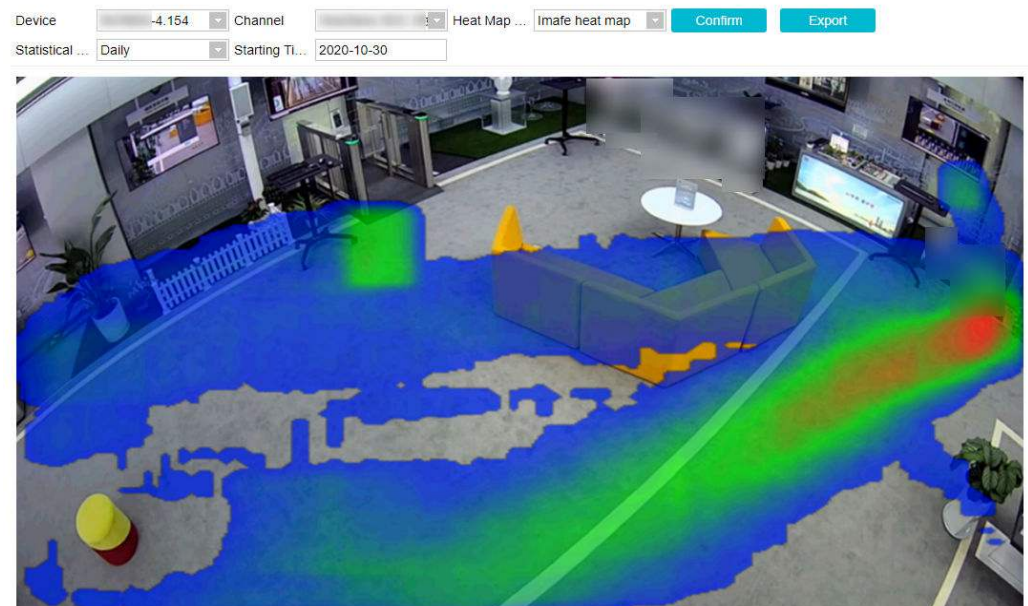
Figure 5-142 Configuring heat map**Table 5-123** Parameter/Button description

Parameter/ Button	Description
Enable HeatMap	Indicates whether to enable the heat map function for a camera
Send Metadata	Indicates whether to send metadata. After this function is enabled, the camera sends the heat map result to the iClient S100.
Add Area	Button for adding an area. A maximum of eight detection areas can be drawn.
Delete	Button for deleting a selected detection area.

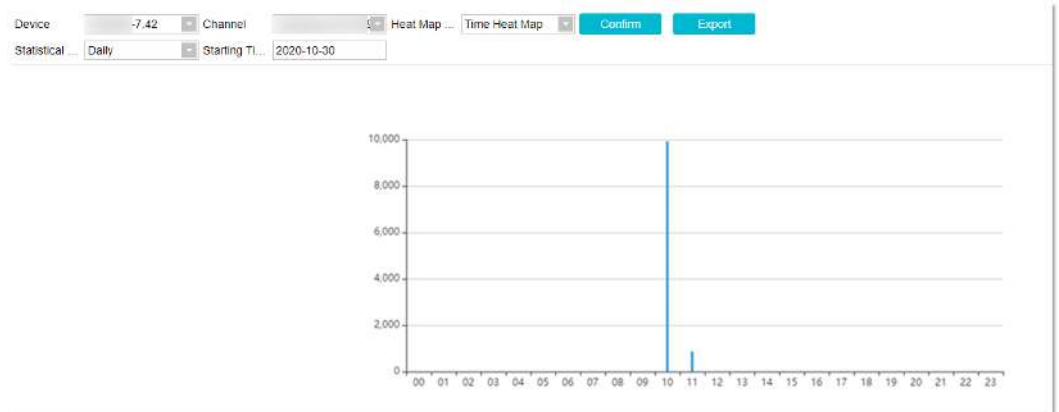
----End

Verification

- Step 1** Choose **Intelligent Applications > Statistics > HeatMap Statistics** on the iClient S100 home page.
- Step 2** Set filter criteria and view heat map statistics.
- View spatial heat map, as shown in [Figure 5-143](#).

Figure 5-143 Spatial heat map

- View temporal heat map, as shown in [Figure 5-144](#).

Figure 5-144 Temporal heat map

----End

5.9.5 Off-Duty Detection

Application Scenario

You can set a detection area to detect on-duty status in the area.

Once the off-duty duration of an employee in the detection area reaches the alarm threshold, the camera reports an alarm to the main device. Then the alarm message will be displayed on the iClient S100.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Restrictions

- The NVR800 can provide the situation analysis function only after being connected to cameras. For details about the version mappings, see the compatibility list of the required product.
- This function is mutually exclusive with target capture and behavior analysis. Before enabling this function, ensure that target capture and behavior analysis are disabled.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Click a camera connected to a main device and choose **Situation Analysis > Off-duty Detection**.
- Step 3** Enable off-duty detection and set parameters such as detection area parameters, as shown in [Figure 5-145](#).

Figure 5-145 Configuring off-duty detection

Parameter Settings

Enable Off-duty Detection: ☐ Superimpose metadata on alarm-triggered snapshot: ☐

On-duty persons: 1 5 1

Off-duty duration(s): 1 600 1

Alarm Detection Interval(s): 1 256 1

Audible and Visual alarm

Enable audio alarms: ☐

Area Settings

+ Area - Delete

2021-05-25 Tue 15:21:57 siufffgg

osd2 OSD3

Plan Settings

+ Add - All Delete

No.	Start Time	End Time	Date	Mode	Operation
1	00:00:00	23:59:59	Every Day	Weekly cycle	

Save Cancel

1. Set parameters in the **Parameter Settings** area. [Table 4-94](#) describes the parameters.

Table 5-124 Parameter description

Parameter	Description
Superimpose metadata on alarm-triggered snapshot	Indicates whether to superimpose metadata information on alarm-triggered snapshots, such as intelligent analysis rules and results.
On-duty persons	Total number of employees that should be on duty.
Off-duty duration (s)	Interval for generating an alarm after an employee is detected off-duty.
Alarm Detection Interval(s)	Interval at which alarms are checked.

2. Set audible and visual alarm parameters. [Table 5-125](#) describes the parameters.

Table 5-125 Audible and visual alarm parameters

Parameter	Description	Requirement on Cameras
Audio	Indicates whether to enable the function of generating an audible alarm when an alarm is triggered.	- You can directly use this function when an intelligent IR/white-light camera with intercom is used. - To use this function when a non-intelligent IR/white-light camera with intercom is used, audio parameters must be configured for the camera and an external audio device must be connected to the camera.
Audio file	Select the audio file to be played when an alarm is triggered. To import an audio file to the iClient S100, perform the following operations: choose Maintenance Management > Video Device > Device List > Main Devices on the home page, double-click a camera that supports audible alarms and is mounted to a main device, and add an audio file on the Audio Channel tab page.	
Playback times	Number of times for playing an audio file when an alarm is triggered.	
White light illuminator	Indicates whether to enable the function of blinking light when an alarm is triggered.	

Parameter	Description	Requirement on Cameras
White light illuminator	Frequency at which the light blinks when an alarm is triggered. You can set this parameter to Low frequency , Intermediate frequency , High frequency , or Steady on as required.	intercom support this function. You need to set parameters related to the light.
Flash duration (s)	Light blinking duration when an alarm is triggered.	

3. Set area parameters. [Table 5-126](#) describes the parameters.

Table 5-126 Area setting buttons

Button	Description
Area	Button for drawing a maximum of one detection area.
Delete	Button for deleting a selected detection area.

4. Set plan parameters. [Table 5-127](#) describes the parameters.

 NOTE

When the iClient S100 and a main device are in different time zones, the time set in the **Plan Settings** area refers to the time of the main device.

Table 5-127 Plan settings

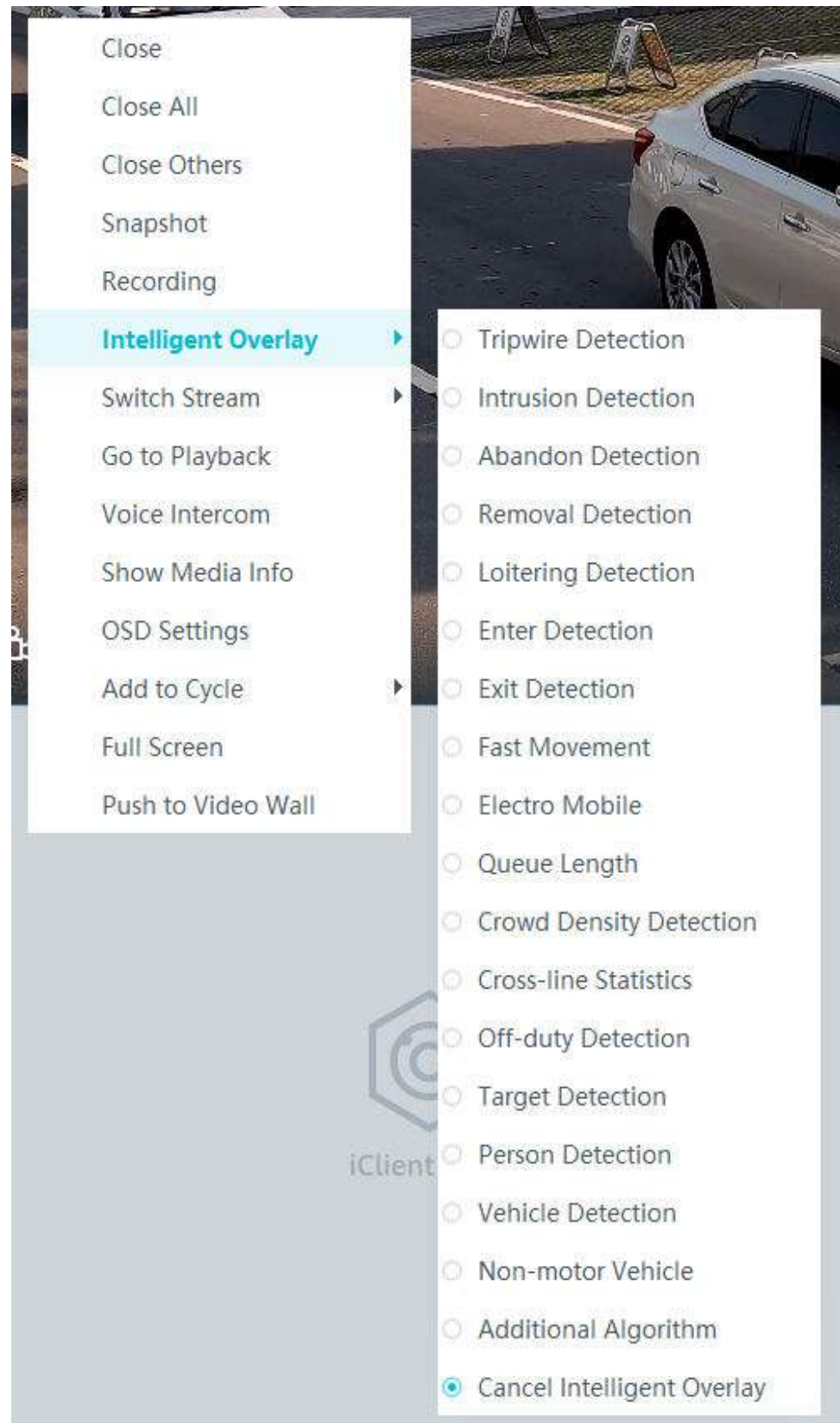
Parameter/ Button	Description
Add	Button for adding an alert plan. A maximum of eight alert plans can be added.
Date	Date on which an alert plan is to be executed. The options are as follows: – Every Day – Monday to Sunday
Mode	Indicates whether to cyclically execute an alert plan. The options are as follows: – Weekly cycle – Do not loop

Step 4 Click **Save**.

----End

Verification

- Viewing real-time results (For details, see [8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?](#).)
 - a. On the iClient S100 home page, choose **Basic Operations > Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay > *Intelligent Event Name*** from the displayed menu, as shown in [Figure 5-146](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-146 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see [4.12.1 Video Alarm](#).

5.10 Intelligent Vehicle Analysis

5.10.1 Vehicle Intelligence (Based on Cameras)

5.10.1.1 Global Configuration

Application Scenario

Before configuring vehicle intelligence on the iClient S100, complete global configuration.

Restrictions

- The NVR800 provides the vehicle intelligence function when it is connected to D2181-10-SL-PU or Dxxxx-10-SIU cameras. For details about the version mappings, see *IVS1800 9.0.0 Compatibility List*.
- The object classification and motor vehicle detection functions are mutually exclusive. Ensure that only one of them is enabled at a time.

Configuring the Algorithm Mode

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Smart Global Configuration > Algorithm Mode**.

Step 3 Set **Algorithm** to **Micro checkpoint**.

NOTE

After the algorithm mode is switched, the camera will restart for the setting to take effect. Wait for 3 minutes and then set intelligent services.

Step 4 Click **Save**.

----End

Configuring Object Classification

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and click **Vehicle Intelligence > Machine Inhuman Detection**.

Step 3 Enable the object classification function, add a detection area, and set related parameters, as shown in [Figure 5-147](#). [Table 5-128](#) describes the parameters and buttons.

Figure 5-147 Configuring object classification

Parameter Settings

Enable Machine Inhuman Detection ☒

License plate brightness compensation ☒

License plate compensation level
 1 100 50

Priority province (city)

Area Settings

+ Area Delete

2021-03-23 15:37:37

Name

Detection Area

Save

Cancel

Table 5-128 Parameter/Button description

Parameter/ Button	Description
Enable Machine Inhuman Detection	Indicates whether to enable the object classification function. NOTE This function is mutually exclusive with the motor vehicle detection function and cannot take effect at the same time. Before enabling this function, ensure that motor vehicle detection function is disabled.
License plate brightness compensation	Brightness compensation for captured license plate images with too high or too low brightness.
License plate compensation level	Level of brightness compensation for captured license plate images. This parameter is available only when License plate brightness compensation is enabled. You can increase the value of the parameter when the environment is dark.
Priority province (city)	Preferential province (or city) name abbreviation used when the first character of a license plate cannot be recognized. Only one province (or city) name abbreviation can be configured.

Parameter/ Button	Description
Area	Button for adding a detection area. You can draw only one detection area.
Delete	Button for deleting a selected detection area.

Step 4 Click **Save**.

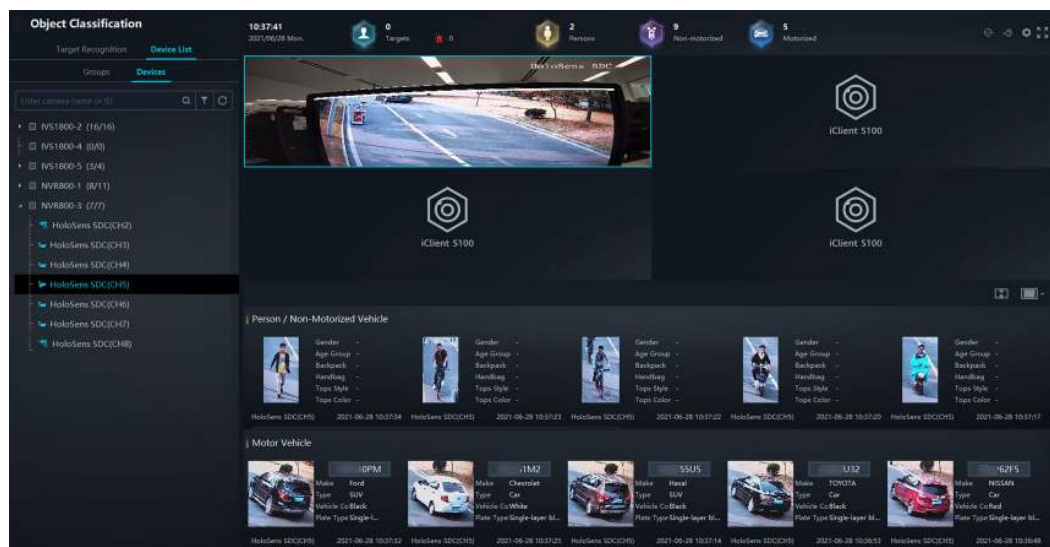
----End

Verification

Step 1 On the iClient S100 home page, choose **Intelligent Applications > Object Classification**.

Step 2 Drag the required camera to the video pane. Object classification results and snapshots will be displayed under the video pane in real time, as shown in [Figure 5-148](#).

Figure 5-148 Object classification results



----End

5.10.1.2 Parking Violation Detection

Scenario Description

This function can be used to detect whether motor vehicles are parked in a specified detection area. The iClient S100 reports an alarm upon detecting a motor vehicle parking in a preset detection area.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

Configuring the Algorithm Mode

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera connected to a main device and choose **Smart Global Configuration > Algorithm Mode**.
- Step 3** Set **Algorithm** to **Micro checkpoint**.

NOTE

After the algorithm mode is switched, the camera will restart for the setting to take effect. Wait for 3 minutes and then set intelligent services.

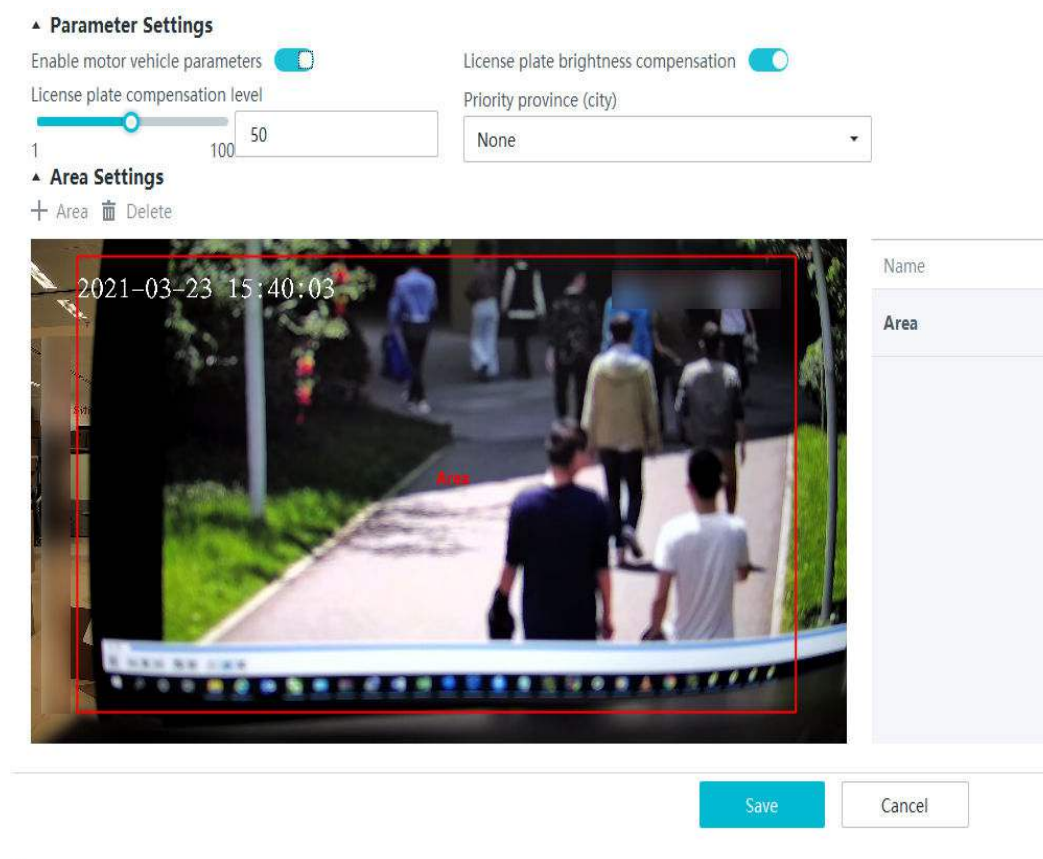
- Step 4** Click **Save**.

----End

Settings Motor Vehicle Detection Parameters

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.
- Step 2** Select a camera connected to a main device and choose **Vehicle Intelligent > Vehicle Parameter**.
- Step 3** Enable motor vehicle detection, add a detection area, and set related parameters, as shown in [Figure 5-149](#). [Table 5-129](#) describes the parameters and buttons.

Figure 5-149 Settings motor vehicle detection parameters



Parameter Settings

Enable motor vehicle parameters ☒

License plate compensation level

License plate brightness compensation ☒

Priority province (city)

Area Settings

+ Area

2021-03-23 15:40:03

Area

Save Cancel

Table 5-129 Parameter/Button description

Parameter/ Button	Description
Enable motor vehicle parameters	Indicates whether to take snapshots of motor vehicles. NOTE This function is mutually exclusive with object classification. Before enabling this function, ensure that object classification is disabled.
License plate brightness compensation	Indicates whether to enable brightness compensation for captured license plate images with too high or too low brightness.
License plate compensation level	Level of brightness compensation for captured license plate images. This parameter is available only when License plate brightness compensation is enabled. You can increase the value of the parameter when the environment is dark.
Priority province (city)	Preferential province (or city) name abbreviation used when the first character of a license plate cannot be recognized. Only one province (or city) name abbreviation can be configured.
Area	Button for adding a detection area. A maximum of one detection area can be drawn.
Delete	Button for deleting a selected detection area.

Step 4 Click **Save**.

----End

Configuring Parking Violation Detection

Step 1 On the iClient S100 home page, choose **Maintenance Management > Smart Configuration**.

Step 2 Select a camera connected to a main device and choose **Vehicle Intelligence > Illegal Parking Detection**.

Step 3 Enable the parking violation detection function, add a detection area, and set related parameters, as shown in [Figure 5-150](#). [Table 5-130](#) describes the parameters and buttons.

Figure 5-150 Configuring parking violation detection

Parameter Settings

Enable illegal parking detection ☒

Sensitivity

Illegal parking trigger time(s)

Alarm Detection Interval(s)

Area Settings

+ Area Delete

2021-03-23 15:46:29

Area 1

Area 2

Area 3

Area 4

Name

Area 1

Area 2

Area 3

Area 4

Plan Settings

+ Add Delete All

No.	Execution Date	Start Time	End Time	Date	Mode	Operation
1	1970-01-01	00:00:00	23:59:59	Every Day	Weekly cycle	

Save Cancel

Table 5-130 Parameter/Button description

Parameter/ Button	Description
Enable illegal parking detection	Indicates whether to enable parking violation detection.
Sensitivity	Detection sensitivity. The value ranges from 1 to 100. A larger value indicates a higher sensitivity.
Illegal parking trigger time(s)	Vehicle parking duration threshold.
Alarm Detection Interval(s)	Interval at which alarms are checked.
Area	Button for adding a detection area. A maximum of four detection areas can be drawn.
Delete	Button for deleting a selected detection area.

Step 4 Click **Save**.

----End

Verification

For details about how to view the latest or historical alarms, see [4.12.1 Video Alarm](#).

5.10.2 Vehicle Intelligence (Based on IVS1800)

5.10.2.1 Vehicle Library

5.10.2.1.1 Application Scenario

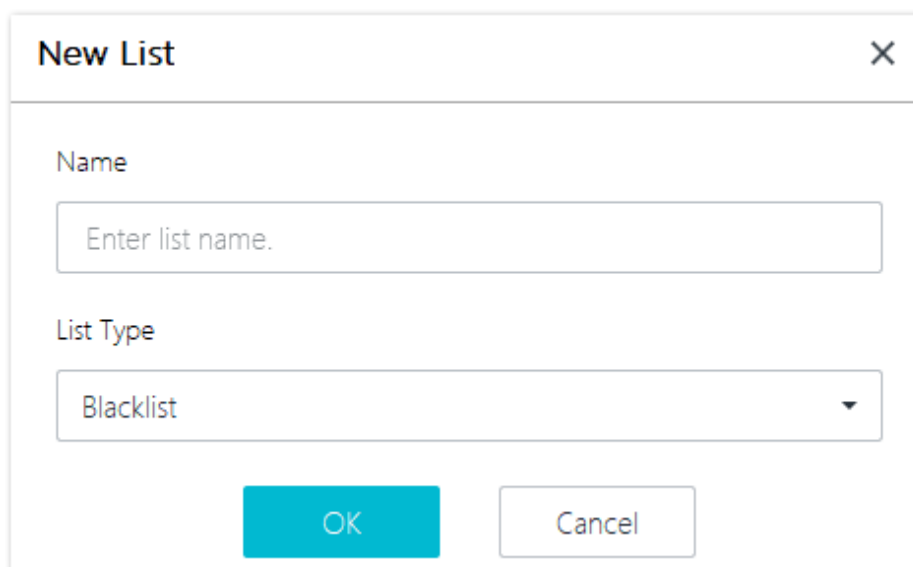
The vehicle library contains vehicle blocklists, which are used in scenarios such as intersections and highways. When a blocklisted vehicle is detected, an alarm is generated in real time.

5.10.2.1.2 Adding a Vehicle List

Adding a Vehicle Blocklist

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 device and choose **Vehicle Library**.
- Step 3** Click **New List**. On the **New List** page that is displayed, set **Name** and **List Type** and click **OK**, as shown in [Figure 5-151](#).

Figure 5-151 Creating a new list



The image shows a 'New List' dialog box. It has a title bar with the text 'New List' and a close button (X). Below the title bar, there are two main sections. The first section is labeled 'Name' and contains a text input field with the placeholder text 'Enter list name.'. The second section is labeled 'List Type' and contains a dropdown menu with 'Blacklist' selected. At the bottom of the dialog, there are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

- Step 4** Click **OK** again.

-----End

5.10.2.1.3 Adding Vehicle Records to a Vehicle List

You can use either of the following methods to add vehicle records to a vehicle blocklist: [Adding a Vehicle Record](#) and [Importing Vehicle Records](#).

Table 5-131 Entries for adding information about a single vehicle

Entry for Adding Information About a Single Vehicle	Application Scenario
Through the Vehicle Library page	You can directly add information about a vehicle whose image and information are available on the Vehicle Library page.
Capturing a vehicle image from a vehicle search result	During vehicle search, if you want to add a found vehicle to a vehicle list, you can view the vehicle details and add the vehicle to the vehicle list.

Adding a Vehicle Record

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an IVS1800 device and choose **Vehicle Library**.

Step 3 Select a vehicle list and click **New**.



Step 4 (Optional) Click . In the dialog box that is displayed, draw a box to select the vehicle in the uploaded image for alert task creation, and click **OK**.

NOTE

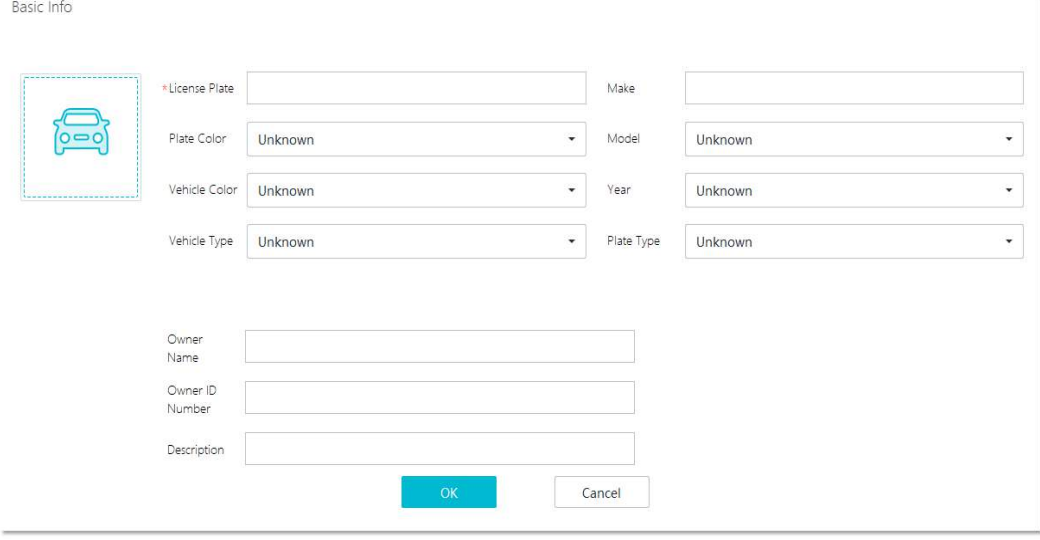
The supported image formats are as follows: .jpg, .jpeg, .jpe, .dib, .bmp, and .png. The size of each image cannot exceed 5 MB.

Step 5 Enter basic vehicle information, as shown in [Figure 5-152](#).

The **License Plate** parameter is mandatory. You can use an asterisk (*) to indicate zero, one, or multiple unknown characters. Set other parameters based on the actual available information.

Figure 5-152 Basic vehicle information

Basic Info



License Plate
 Make

Plate Color
 Model

Vehicle Color
 Year

Vehicle Type
 Plate Type

Owner Name

Owner ID Number

Description

Step 6 Click **OK**.

----End

Importing Vehicle Records

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an IVS1800 device and choose **Vehicle Library**.

Step 3 Select a vehicle list and click **Import**.

Step 4 Set **Import Method** to **Template import**, **Batch import**, or **Quick import**.

- **Template import**

- Click **Download Template** or **Download Template (No Image)** to download either template to the local computer.

If you click **Download Template (No Image)**, you cannot fill in vehicle images in the downloaded template. Download either template based on the site requirements.

- Decompress the downloaded package, open **Image Batch Import Tool.xlsm**, and fill in vehicle information in the template.

 NOTE

- If you click **Download Template**, you can click **Read All Files in Target Folder** in the downloaded template to automatically read image names. Vehicle images must be stored in the same folder as the **Image Batch Import Tool.xlsm** template and the .csv file generated later.
 - You must set the **License Plate** parameter in the template. Otherwise, the .csv file cannot be generated.
 - The supported image formats are as follows: .jpg, .jpeg, .jpe, .dib, .bmp, and .png.
 - The size of each image cannot exceed 5 MB.
 - A maximum of 10,000 vehicle records can be imported at a time.
 - If you select **Allow duplicates**, you can import records that already exist in the vehicle list.
- c. Click **Generate CSV File** in the template.
- d. Click  on the right of **List File**, select a local .csv file, and upload the file.
- **Batch import**
- Click  on the right of **List File** and select the directory for storing vehicle images.

 NOTE

- You can select a folder to upload all images in the folder.
 - The supported image formats are as follows: .jpg, .jpeg, .jpe, .dib, .bmp, and .png.
 - The size of each image cannot exceed 5 MB.
 - An image file (.jpg file in this example) must be named in the following format: *Characters of the license plate_Vehicle color_Vehicle type_License plate color_License plate type_Vehicle make_Vehicle model_Model year_Vehicle owner name_Vehicle owner ID number.jpg* The *Characters of the license plate* field is mandatory.
 - Use underscores (`_`) to separate fields in the name of an image file. The values of *Vehicle color*, *Vehicle type*, *License plate color*, *License plate type*, *Vehicle make*, and *Vehicle model* must be numerical enumerated values. For details, see **Image Batch Import Tool.xlsm** that is locally extracted in [Step 4.b](#).
 - If a field between two other fields needs to be ignored, you do not need to set the field and use an underscore (`_`) to replace the field. For example, if only the license plate characters and vehicle type can be identified for a vehicle image, the vehicle image can be named in the format *Characters of the license plate_Vehicle type.jpg*.
 - If an end field needs to be ignored, delete it directly.
 - If you select **Allow duplicates**, you can import records that already exist in the vehicle list.
- **Quick import**

Click  on the right of **List File** and select the directory for storing vehicle images.

 NOTE

The supported image formats are as follows: .jpg, .jpeg, .jpe, .dib, .bmp, and .png. The size of each image cannot exceed 5 MB.

The iClient S100 extracts fields from image names. Therefore, images must meet the following requirements:

- An image must be named after the license plate.
- Characters of a license plate consist of 1 to 255 characters, including letters and digits.
- If you select **Allow duplicates**, you can import records that already exist in the vehicle list.

Step 5 Click **Import**.

----End

Searching for Vehicle Information in a Vehicle List

- Select a vehicle list on the left, select the **License Plate**, **Owner ID Number**, or **Owner Name** parameter, enter a value in the search box, and click  to search for the vehicle.
- Select a vehicle list on the left, click **Advanced**, set search criteria, and click **Search** to search for the vehicle, as shown in [Figure 5-153](#).
- Double-click a record in the search result to view the vehicle details.

Figure 5-153 Searching for vehicle information by criteria

Make	Model	Year	Vehicle Color	Plate Color
	All ▾	All ▾	All ▾	All ▾
Vehicle Type		Created		
All ▾		All 	Search	Reset

5.10.2.2 Vehicle Search

5.10.2.2.1 Application Scenario

This section describes how to search the snapshot list for vehicle information. The vehicle information in the snapshot list is generated by intelligent analysis tasks on the IVS1800. [Table 5-132](#) describes the vehicle search modes.

Table 5-132 Vehicle search modes

Search Mode	Description	Data Source
Vehicle filter by criteria	The system searches for matched vehicle images based on the specified search criteria.	- Common cameras: The IVS1800 creates video structuring tasks for the cameras and searches for vehicles based on the analysis result. - Vehicle checkpoint cameras/object classification cameras: The IVS1800 automatically subscribes to the metadata from the cameras and directly uses the metadata for search. Analysis tasks do not need to be configured.

5.10.2.2.2 Prerequisites

- Vehicle lists and corresponding vehicle information have been added to the vehicle library.
- The video structuring algorithm plug-in package has been installed. The video structuring algorithm can extract structured data of persons, vehicles, and cyclists. For details about how to install the plug-in package, see the operations for loading the algorithm plug-in.
The video structuring algorithm plug-in package varies depending on the device model. Install the plug-in package based on the site requirements. To check the device model, view the electronic label attached to the chassis or choose **Local Configuration > Basic Configuration** on the OMU portal.
- You have set image storage parameters in scenarios where intelligent cameras are used. To set image storage parameters, choose **Maintenance Management > Video Device > Device List > Main Devices** on the iClient S100 home page. Right-click an IVS1800, choose **Storage Management** from the shortcut menu, and select a camera.

5.10.2.2.3 (Optional) Creating a Video Structuring Task

NOTE

The IVS1800 storage model (for example, IVS1800-B08 and IVS1800-B16) does not support the backend intelligent analysis function.

Procedure

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an IVS1800 and choose **Task Management**.

Step 3 Click **New Task**.

Step 4 Select a camera. The page for creating a video structuring task is displayed, as shown in [Figure 5-154](#). [Table 5-133](#) describes the parameters.

Figure 5-154 Creating a video structuring task

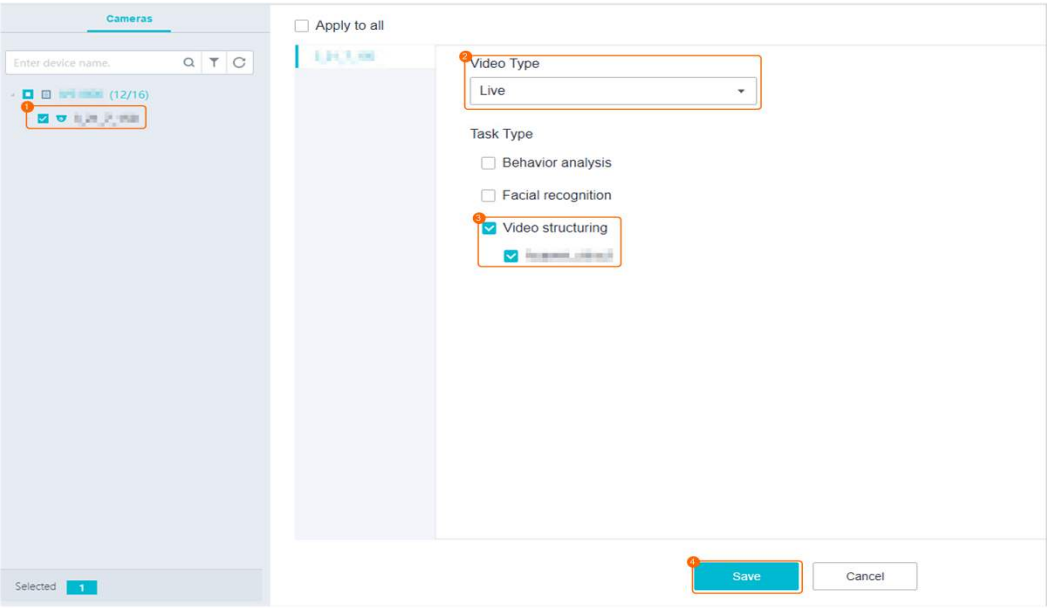
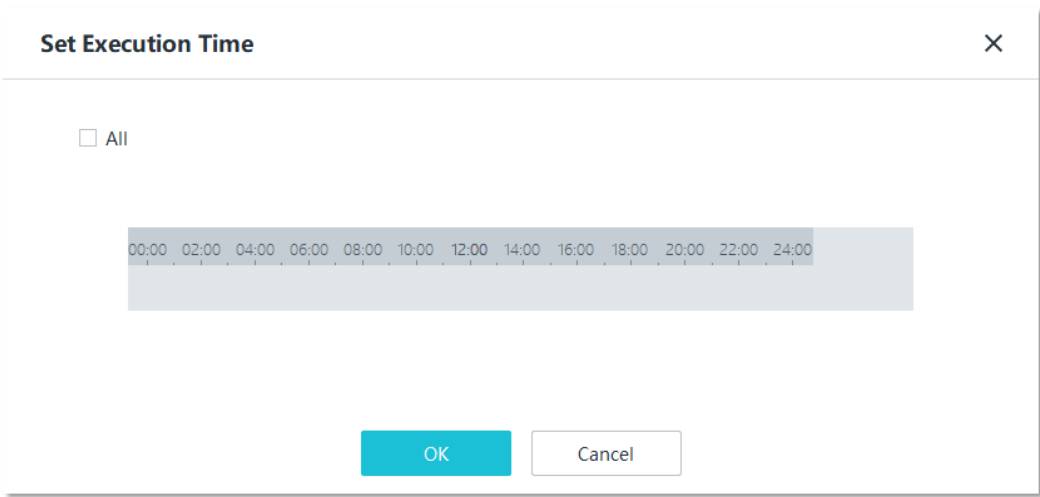


Table 5-133 Parameters for creating a video structuring task

Parameter	Setting
Video Type	Video type. The options are Live and Recorded .
Analysis Period	Recording period. Recordings generated within this period are used for video structuring. Set this parameter only when Video Type is set to Recorded .
Task Type	Task type. Select Video structuring and select an algorithm.

Step 5 In the **Set Execution Time** dialog box, set the time for executing the task every day, as shown in [Figure 5-155](#).

Figure 5-155 Set Execution Time dialog box



Step 6 Click **OK**.

Step 7 Click **Save**.

----End

5.10.2.2.4 Verification

Step 1 On the iClient S100 home page, choose **Basic Operations > Search > Vehicle Search**.

Step 2 Configure vehicle search criteria, as shown in [Figure 5-156](#).

Figure 5-156 Configuring vehicle search criteria

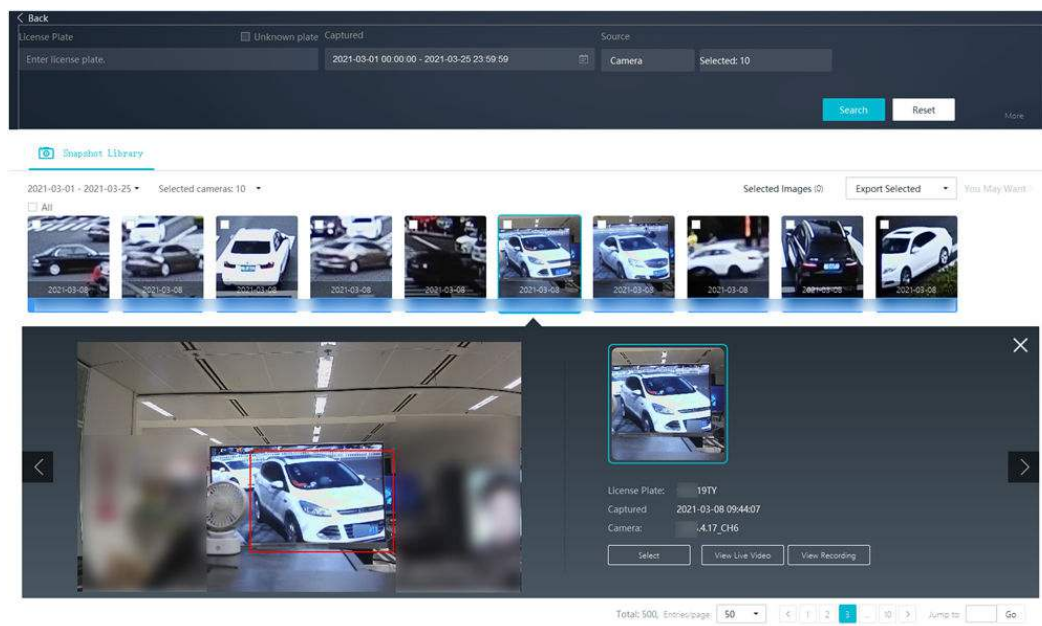
[Table 5-134](#) describes the key parameters. Set other parameters based on the site requirements.

Table 5-134 Parameter description

Parameter	Setting
License Plate	License plate characters of the vehicle to be searched for. (The value is case insensitive). Fuzzy search is supported, where the question mark (?) matches exactly one character, and the asterisk (*) matches zero or more characters.
Unknown plate	Indicates whether to search for vehicles whose license plates have not been properly captured. If you select this check box, the License Plate parameter becomes unavailable, and the iClient S100 will search for vehicle images without clear license plates.
Captured	Period during which the vehicle images are captured.
Source	Cameras from which vehicle images are searched for. You can select multiple cameras from various main devices.

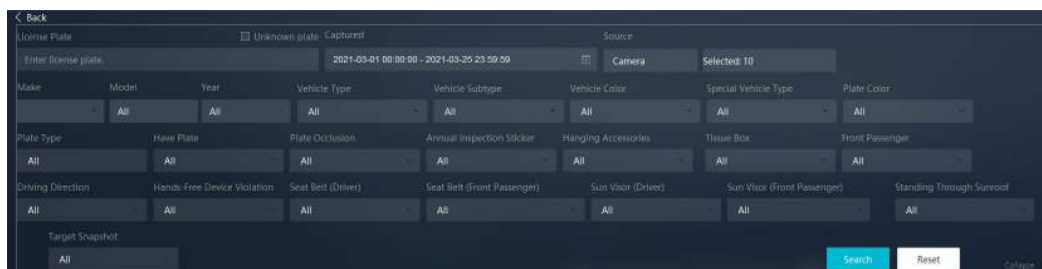
Step 3 Click **Search** to search for vehicle information based on the configured search criteria. The statistics result is displayed, as shown in [Figure 5-157](#).

Figure 5-157 Vehicle search results



Step 4 Optional: For further search, click **More** to set the search criteria. [Figure 5-158](#) describes the search criteria.

Figure 5-158 More search criteria



Step 5 Select multiple vehicle images and click **Export Selected** to export the selected images. Alternatively, select **Export This Page** or **Export All** from the drop-down list box as required. [Figure 5-159](#) shows the **Export Options** dialog box.

NOTE

You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files.

The password must meet the following requirements:

- Contains 10 to 16 characters.
- Contains at least two types of the following: lowercase letters, uppercase letters, digits, and special characters.
- Must be different from the user name or user name spelled backwards.
- Cannot contain space characters or Chinese characters.
- Cannot be a weak password.

Figure 5-159 Export Options dialog box

----End

5.10.2.3 Vehicle Alert

5.10.2.3.1 Application Scenario

This section describes how to configure a vehicle alert task. After creating an intelligent analysis task on the iClient S100, you can configure a vehicle alert task.

A typical application scenario of vehicle alert is as follows: When information about the target vehicle is not clear, you need to search for the vehicle first to identify it, and then create an alert task to detect the vehicle.

5.10.2.3.2 Prerequisites

- The video image resolution is within the range from 768 x 432 to 4096 x 3000 (or 8,847,360) pixels. If the resolution is out of the range, no vehicle or license plate recognition result can be obtained on the iClient S100.
- The video structuring algorithm plug-in package has been installed. The video structuring algorithm can extract structured data of persons, vehicles, and cyclists. For details about how to install the plug-in package, see the operations for loading the algorithm plug-in.

The video structuring algorithm plug-in package varies depending on the device model. Install the plug-in package based on the site requirements. To check the device model, view the electronic label attached to the chassis or choose **Local Configuration > Basic Configuration** on the OMU portal.

- A vehicle library has been configured. For details, see [5.10.2.1 Vehicle Library](#).
- Before performing vehicle alert on common cameras, ensure that video structuring tasks have been configured for the cameras. For details, see [5.10.2.2.3 \(Optional\) Creating a Video Structuring Task](#).

5.10.2.3.3 Creating a Vehicle Alert Task

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Vehicle Alerts**.
- Step 3** Click **New Alert Task**.
- Step 4** Configure a vehicle alert task, as shown in [Figure 5-160](#).

Figure 5-160 Configuring a vehicle alert task

[Table 5-135](#) describes the parameters.

Table 5-135 Parameter description

Parameter	Setting
Alert Task Name	Alert task name.
Active	Time range for executing a vehicle alert task. - Select One Week, One Month, or One Year. - Specify a period in the calendar. - Click Set Hours to set the time segment for alert every day.
Alert Object	Vehicle list for alert. You can select multiple vehicle lists.
Alert Level	Alert level. The options are Critical , Major , Minor , and Warning . The alert level is the same as the severity of alarms generated by the alert task.
Alarm Type	Alarm type. The options are as follows: When listed detected: When the recognized vehicle matches the alerted vehicle, an alarm is generated. When non-listed detected: When the recognized vehicle does not match the alerted vehicle, an alarm is generated.

Parameter	Setting
Alert Scope	Alert scope. Click the text box under Camera and select cameras from the camera list. A maximum of 64 cameras can be selected.

----End

5.10.2.3.4 Viewing Vehicle Alert Results

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0273281878.xml.

5.10.3 Object Classification Statistics

Application Scenario

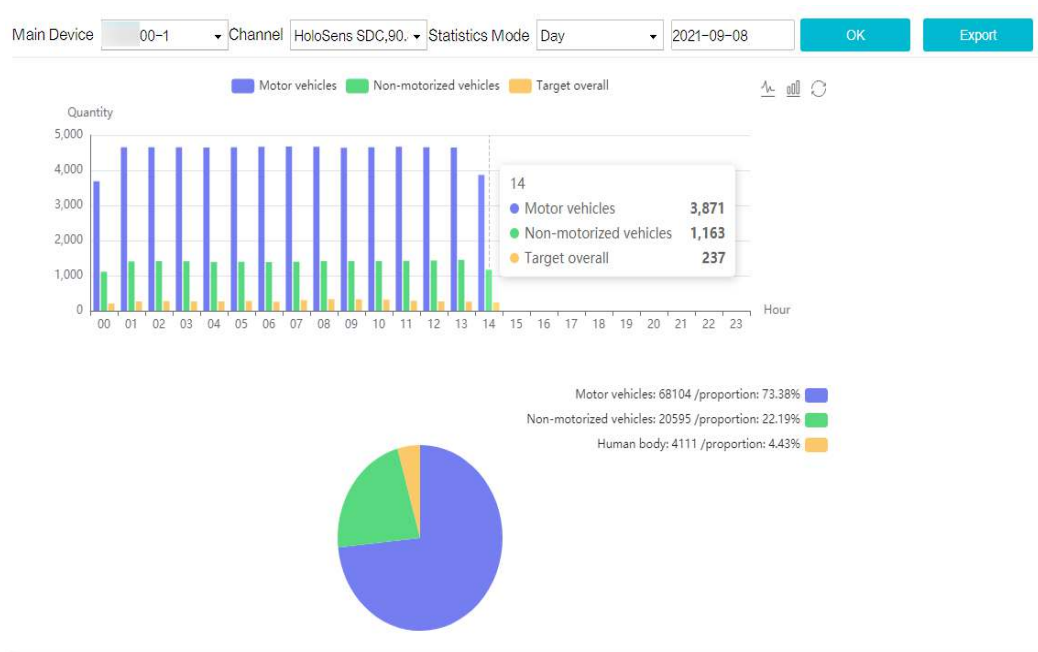
In areas with a large flow of people and vehicles such as intersections, the IVS1800 provides the object classification statistics function to provide valid data for behavior analysis.

Prerequisites

The object classification service has been configured for the IVS1800, and vehicle images have been captured and stored.

Procedure

- Step 1** Choose **Intelligent Applications > Statistics > Object Classification Statistics** on the iClient S100 home page.
- Step 2** Set search criteria and click **Confirm**. The object classification statistics result is displayed, as shown in [Figure 5-161](#). [Table 5-136](#) describes the parameters.

Figure 5-161 Object classification statistics**Table 5-136** Parameter/Button description

Parameter/Button	Description
Statistical Period	Used to display statistical results in different report types. The options are Daily , Weekly , Monthly , Quarterly , and Year .
Export	Used to export reports in different file formats. The options are EXCEL File , PDF File , and CSV File .

----End

5.11 Third-Party Algorithms

5.11.1 Context

On the iClient S100, you can install download third-party algorithms on the IVS1800, or you can upload local installation packages of third-party algorithms to the IVS1800. Additionally, you can activate licenses of, configure, upgrade, and uninstall these algorithms on the iClient S100.

After a third-party algorithm is installed and activated on the IVS1800 and configured on a camera, when the camera detects an alarm event, it reports the alarm to the IVS1800, and the alarm is displayed on the iClient S100.

Enable alarm linkage. For details, see [5.12.2 Alarm Linkage](#).

5.11.2 Third-Party Algorithm Installation

5.11.2.1 Offline Installation

Prerequisites

- The IVS1800 is of 9.1.0 or a later version. For versions earlier than 9.1.0, third-party algorithm plug-ins must be installed on the OMU portal of the IVS1800.

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Algorithm Management**. The **Algorithm Management** page is displayed, as shown in [Figure 5-162](#). [Table 5-137](#) describes the parameters.

Figure 5-162 Algorithm Management page

Device Name	IP	Hardware ID	Host CPU	Host Memory	Algorithm Storage	All Total Power	Number	Platform Type	Operate
IVS1800-2	192.168.1.10	2188001214001000000	30%	4372.4MB Available (Algorithm 6...)	27803.0MB Available (Algorithm ...)	0%	0	Accord100	Local Algorithm install
IVS1800-2	192.168.1.11	2182411810171000000	34%	4305.9MB Available (Algorithm 6...)	27803.0MB Available (Algorithm ...)	0%	0	Accord100	Local Algorithm install
IVS1800-3	192.168.1.12	2188001218001000000	37%	3633.2MB Available (Algorithm 6...)	26672.2MB Available (Algorithm 2...)	30%	2	Accord100	Local Algorithm install

Algorithm Status	Algorithm Version	Source Type	Operating status	Operate
Hardware	6.0	Local Install	☒	License Configuration Upgrade Uninstall
Software	2.7.3	Local Install	☒	License Configuration Upgrade Uninstall

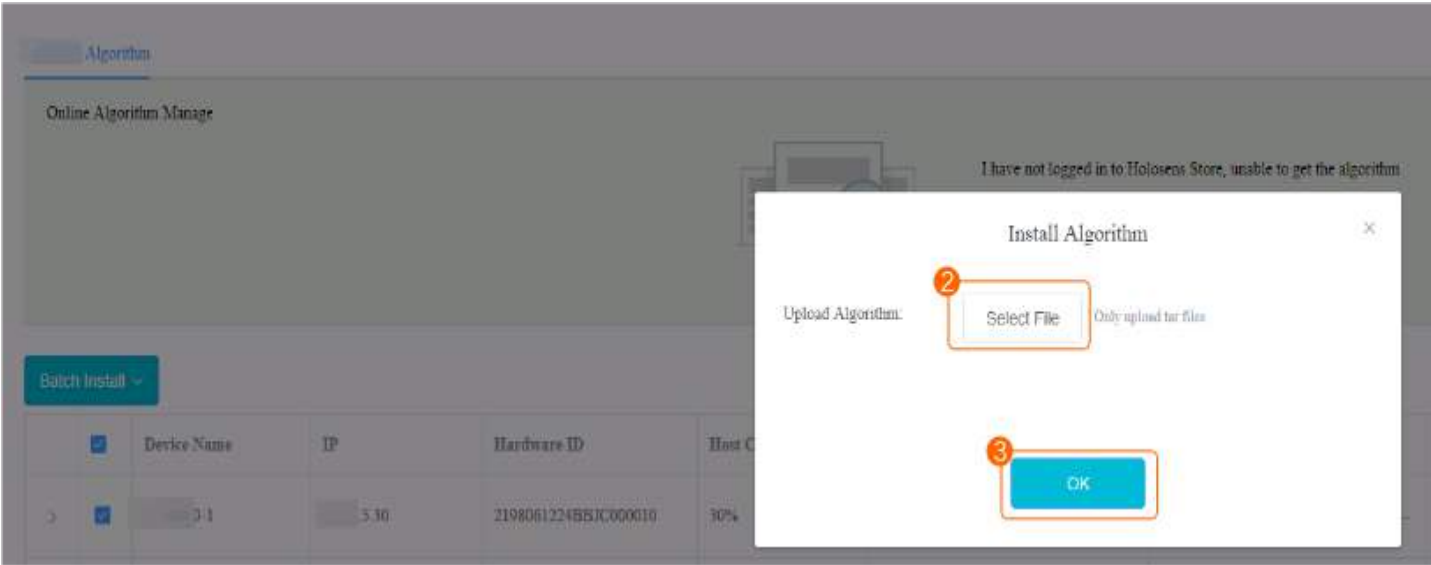
Device Name	IP	Hardware ID	Host CPU	Host Memory	Algorithm Storage	All Total Power	Number	Platform Type	Operate
IVS1800-6	192.168.1.13	2188001218001000000	27%	8134.0MB Available (Algorithm 6...)	10548.18MB Available (Algorithm ...)	0%	0	Accord100	Local Algorithm install
IVS1800-7	192.168.1.14	2188001218001000000	30%	4372.2MB Available (Algorithm 6...)	27778.0MB Available (Algorithm ...)	0%	1	Accord100	Local Algorithm install
IVS1800-8	192.168.1.15	2188001218001000000	26%	3123.2MB Available (Algorithm 6...)	18043.0MB Available (Algorithm 10...)	0%	1	Accord100	Local Algorithm install

Table 5-137 Algorithm management parameters

Parameter	Description
Batch Install	Installs algorithms online or uploads local algorithm installation packages for multiple cameras.
Operating status 	- Toggled-on (default): The third-party algorithm is enabled. You can create analysis tasks based on the algorithm and manage these tasks. - Toggled-off: You are not allowed to create analysis tasks based on the third-party algorithm, and all intelligent analysis tasks based on this algorithm are disabled.
License	Uploads the license of the algorithm.
Configuration	Modifies configurations of the algorithm.
Upgrade	Uploads an upgrade package to upgrade the third-party algorithm.
Uninstall	For a disabled algorithm, you can click Uninstall to uninstall it.

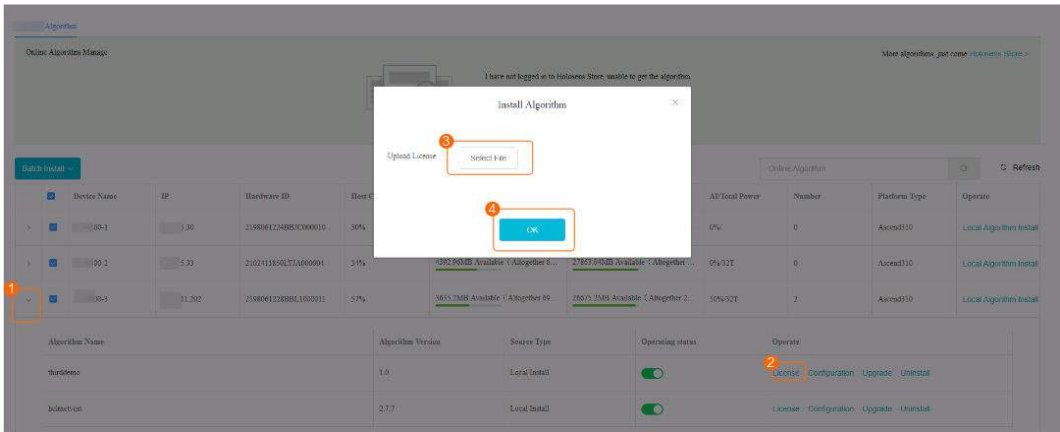
Step 2 Select a device and click **Local Algorithm Install** to upload and install a local algorithm installation package, as shown in [Figure 5-163](#).

Figure 5-163 Uploading and installing an algorithm



Step 3 Click **License** in the **Operation** column of the algorithm and upload the license, as shown in [Figure 5-164](#).

Figure 5-164 Uploading a license



----End

5.11.3 Third-Party Algorithm Configuration

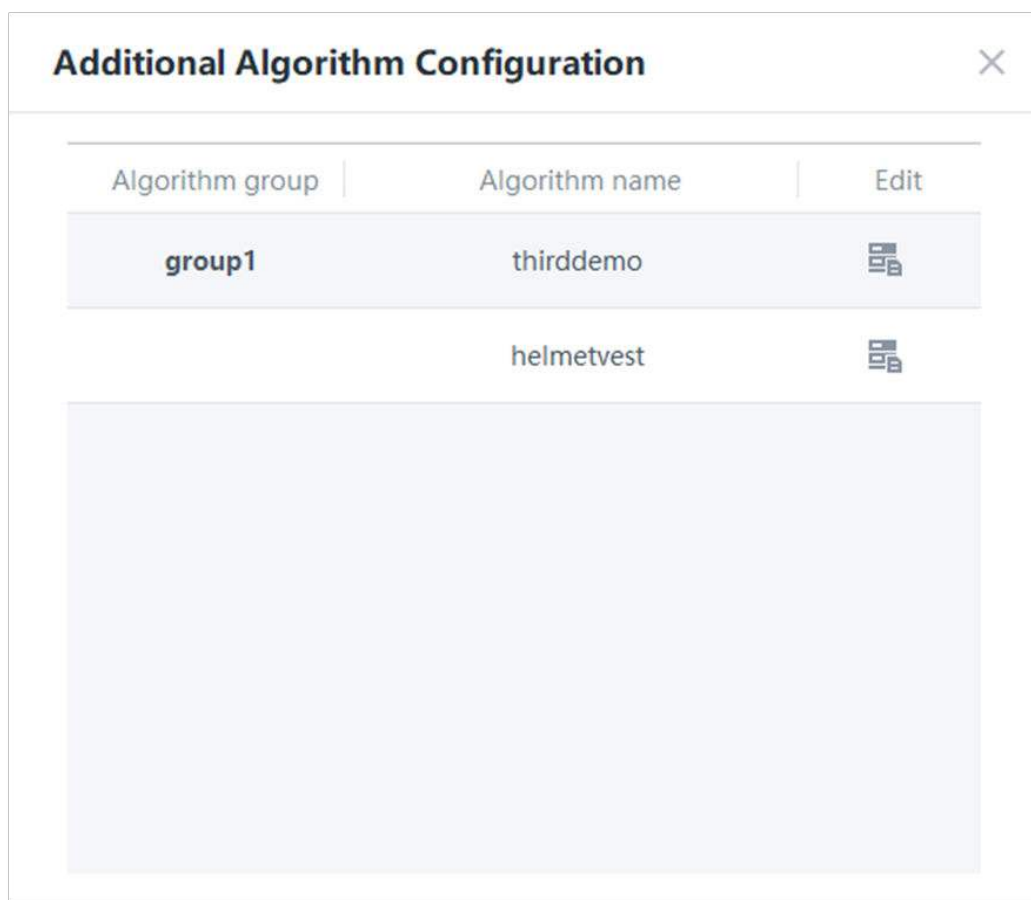
Prerequisites

You have installed a third-party algorithm plug-in on the IVS1800 or the **Algorithm Management** page of the iClient S100, and activated the license.

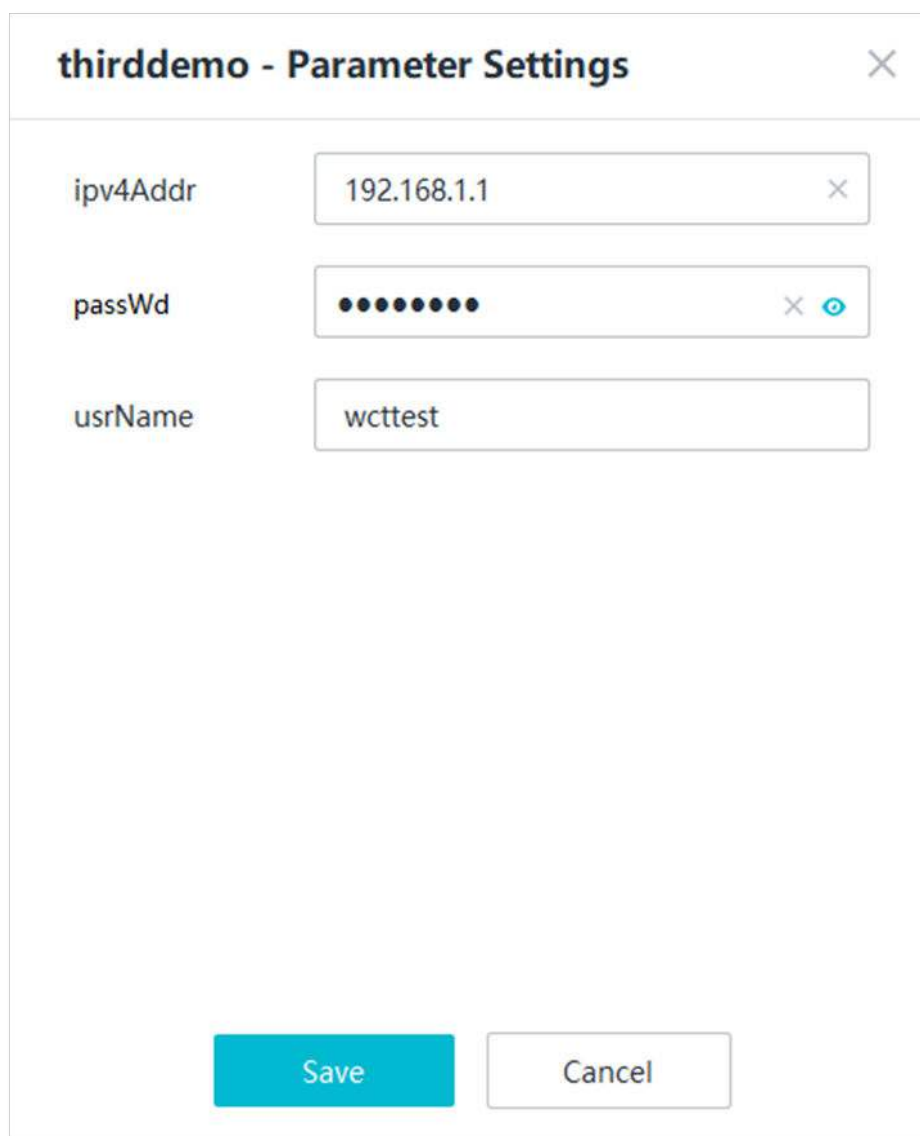
Configuring Third-Party Algorithms (For IVS1800 of Versions Earlier Than 9.1.0)

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Algorithm Config** from the shortcut menu. In the dialog box that is displayed, some of the third-party algorithm plug-ins installed on the device are displayed, as shown in [Figure 5-165](#).

Figure 5-165 Installed third-party algorithms



- Step 3** Click  in the **Edit** column of the required algorithm. In the dialog box that is displayed, enter the IP address, user name, and password of the camera to which the algorithm is to be assigned, as shown in [Figure 5-166](#).

Figure 5-166 Setting third-party algorithm parameters

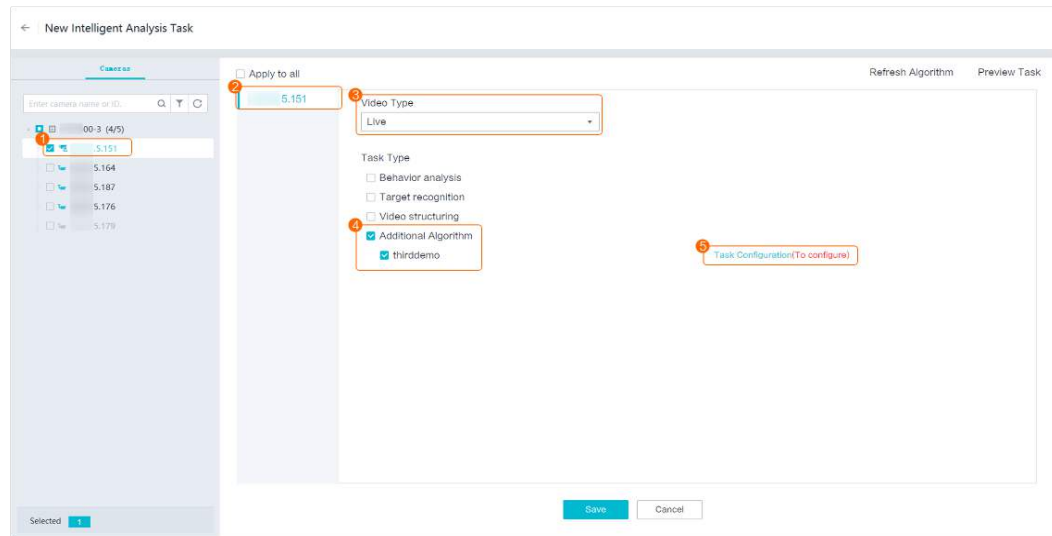
The screenshot shows a dialog box titled "thirddemo - Parameter Settings". It has three input fields: "ipv4Addr" containing "192.168.1.1", "passWd" containing masked characters and a toggle icon, and "usrName" containing "wcttest". At the bottom are "Save" and "Cancel" buttons.

Step 4 Click **Save**.

----End

Configuring Third-Party Algorithms (For IVS1800 of 9.1.0 and Later Versions)

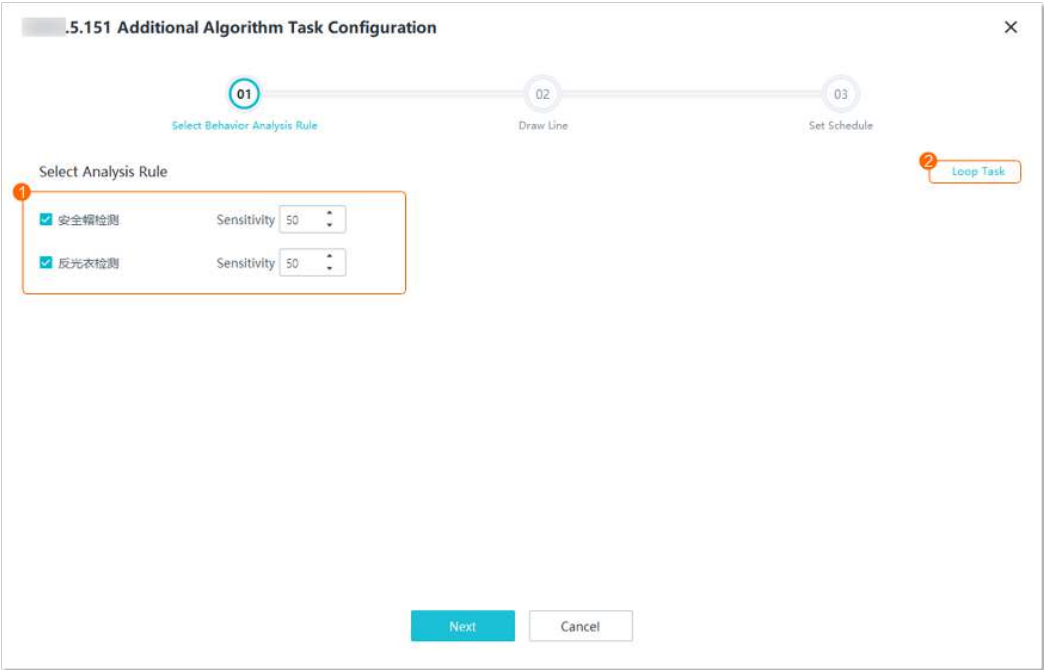
- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Task Management** from the shortcut menu.
- Step 3** Click **New Task**.
- Step 4** Select a camera and create an intelligent analysis task based on a third-party algorithm, as shown in [Figure 5-167](#). [Table 5-138](#) describes the parameters.

Figure 5-167 Creating an intelligent analysis task based on a third-party algorithm**Table 5-138** Parameters for creating an intelligent analysis task based on a third-party algorithm

Parameter	Description
Video Type	Type of the video used for intelligent analysis. Select Live or Recorded as required.
Analysis Period	Recording period. Recordings generated within this period are used for intelligent analysis. Set this parameter only when Video Type is set to Recorded .
Task Type	Type of an intelligent analysis task. Select Additional Algorithm and select an algorithm as required.

Step 5 Configure a task execution plan, as shown in [Figure 5-168](#). Detection rules are required for some third-part algorithms.

Figure 5-168 Configuring a task execution plan



Step 6 Optional: If the computing power of the IVS1800 is insufficient to support concurrent execution of selected tasks, you can configure time-based computing power reuse for tasks that do not require real-time analysis, as shown in [Figure 5-169](#). In this way, the computing power can be used to analyze tasks in a polling group alternatively within a specified period.

Figure 5-169 Configuring time-based computing power reuse

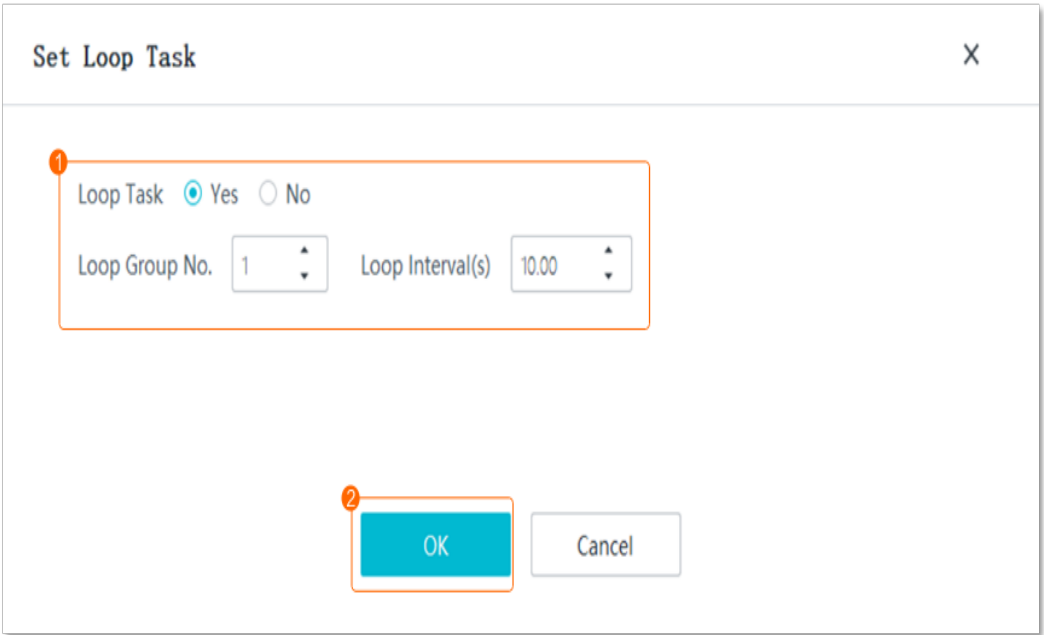
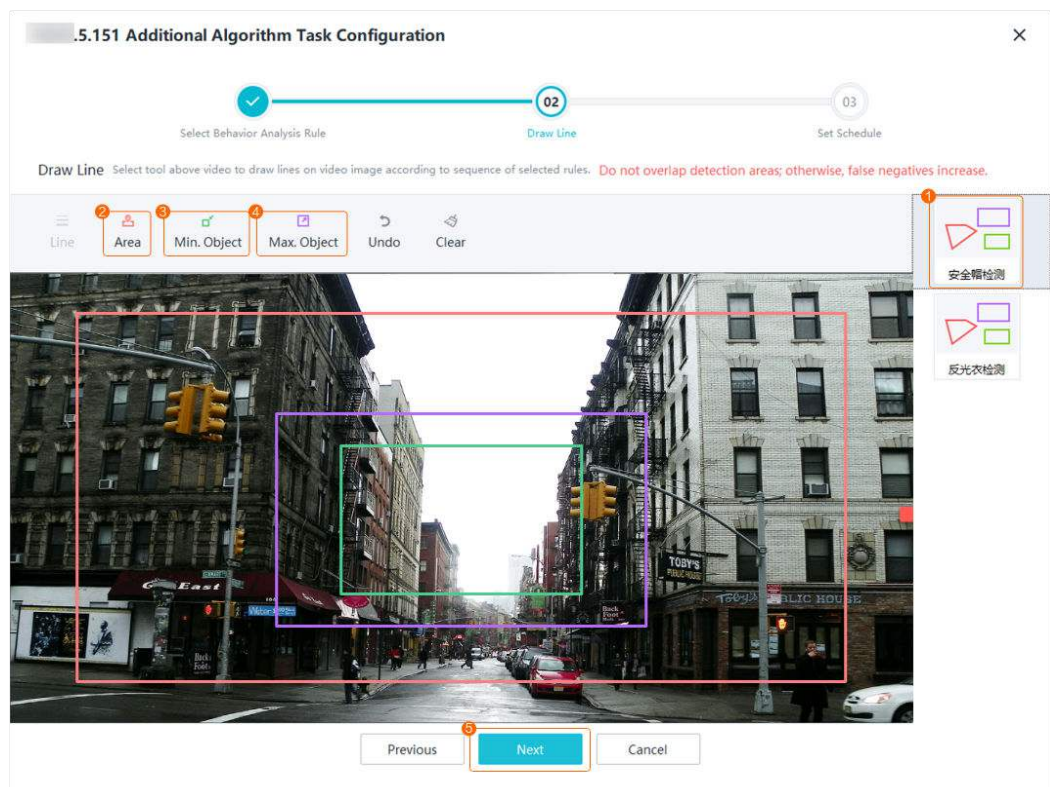


Table 5-139 Time-based computing power reuse parameters

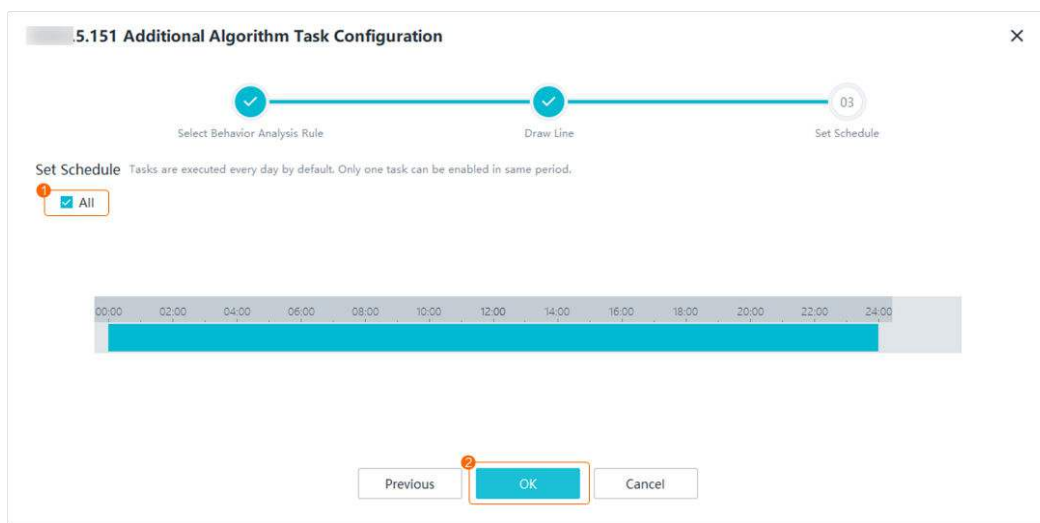
Parameter	Description
Loop Task	Indicates whether to enable time-based computing power reuse.
Loop Group No.	ID of the polling group to which a third-party algorithm-based analysis task belongs. - IVS1800-CXX-16T supports a maximum of eight polling groups. - IVS1800-CXX-32T supports a maximum of 16 polling groups.
Loop Interval	Execution time of all tasks in a polling group. For details, see the capability of the third-party algorithm.

Step 7 Configure detection rules. [Figure 5-170](#) shows detection rules for safe helmet detection.

Figure 5-170 Configuring detection rules

You can configure detection rules for reflective cloth detection by referring to the figure above.

Step 8 Configure a time plan, as shown in [Figure 5-171](#).

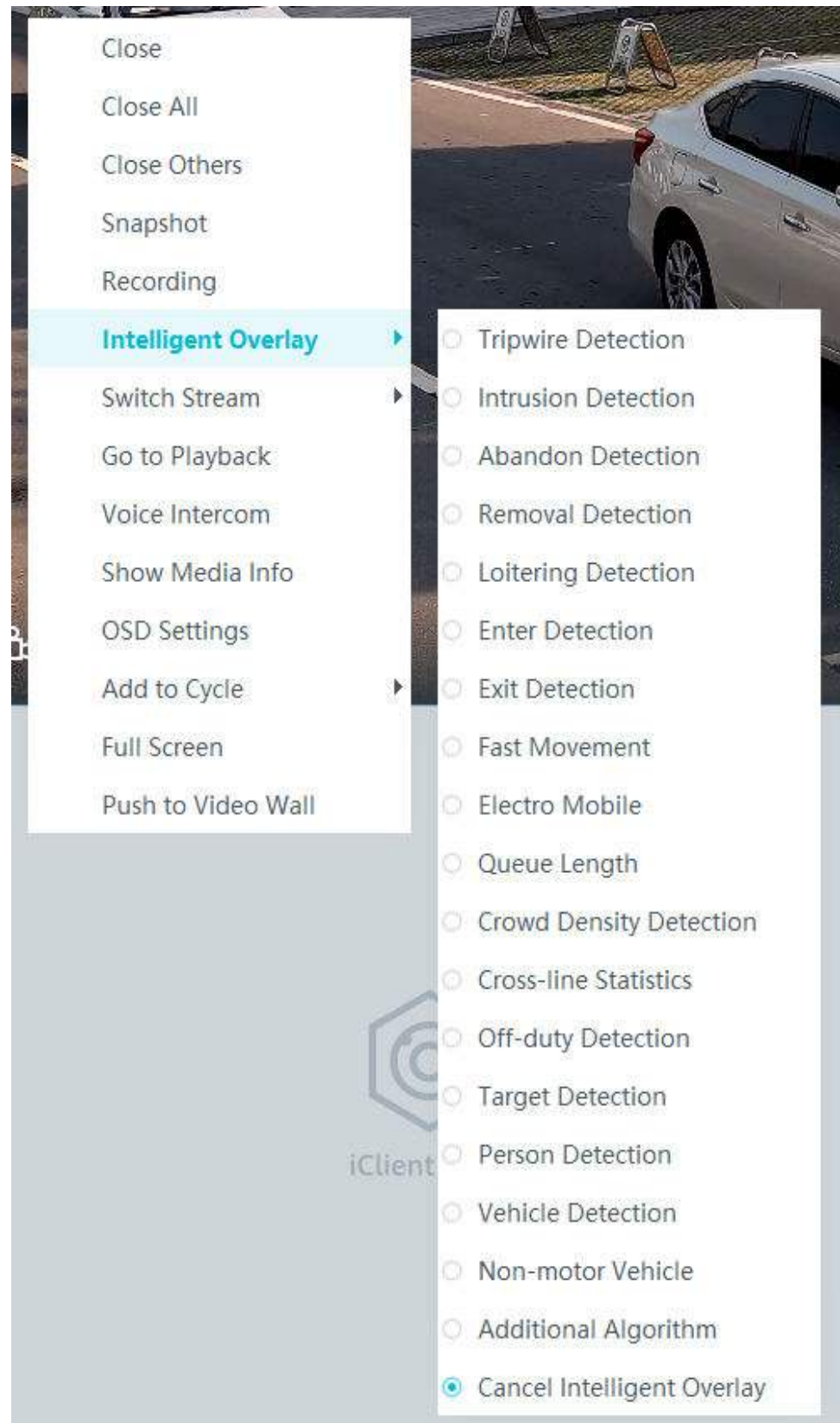
Figure 5-171 Configuring a time plan**Step 9** Click **OK**.

If the status of the task is **Analyzing** on the **Task Management** page, the task is successfully created.

-----End

Verification

- Viewing real-time results (For details, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0301260441.xml.)
 - a. On the iClient S100 home page, choose **Basic Operations** > **Live**.
 - b. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.
 - c. Right-click a live video pane and choose **Intelligent Overlay** > **Intelligent Event Name** from the displayed menu, as shown in [Figure 5-172](#). The real-time intelligent analysis result is superimposed on the video image.

Figure 5-172 Options under Intelligent Overlay

- Viewing alarms

For details about how to view the latest or historical alarms, see IDP-CMS-TEMP-LINK-EXTENAL=en-us_topic_0000001088143994.xml.

5.12 Alarm Management

5.12.1 Video Alarm

This section describes how to view information about alarms generated by alarm linkage actions and intelligent analysis services on the iClient S100. [Table 5-140](#) describes detailed video alarms.

Table 5-140 Alarm parent types and subtypes

Parameter		Function
Latest Alarm		Displays the latest alarms of each service. On this page, alarms are displayed and updated in real time. The alarm subtypes of the latest alarms are the same as those of historical ones.
Target Alert Alarm	• Target recognition alarm • Target detection alarm • Mask detection alarm • Person detection alarm • Appearance frequency alarm (provided by the NVR800)	Displays the historical alarms of each service.
Vehicle Alert Alarm	• Vehicle recognition alarm (for motor vehicles only) • Vehicle detection alarm (for motor vehicles only) • Parking violation alarm (for motor vehicles only) • Non-motorized vehicle detection alarm	

Parameter		Function
Behavior Analysis Alarm	• Tripwire crossing detection alarm • Intrusion detection alarm • Abandoned object detection alarm • Removed object detection alarm • Loitering detection alarm • Area entry detection alarm • Area exit detection alarm • Fast movement detection alarm • Fire detection alarm • Electric bike detection alarm	
Common Business Alarm	• Motion detection alarm • Lens blocking alarm • Sudden volume increase alarm • Sudden volume decrease alarm • Video loss alarm • Micro Edge I/O alarm • Boolean value alarm	
Situation Analysis Alarm	• Human counting alarm • Queue length alarm • Crowd density alarm • Crowd gathering alarm • Off-duty detection alarm	

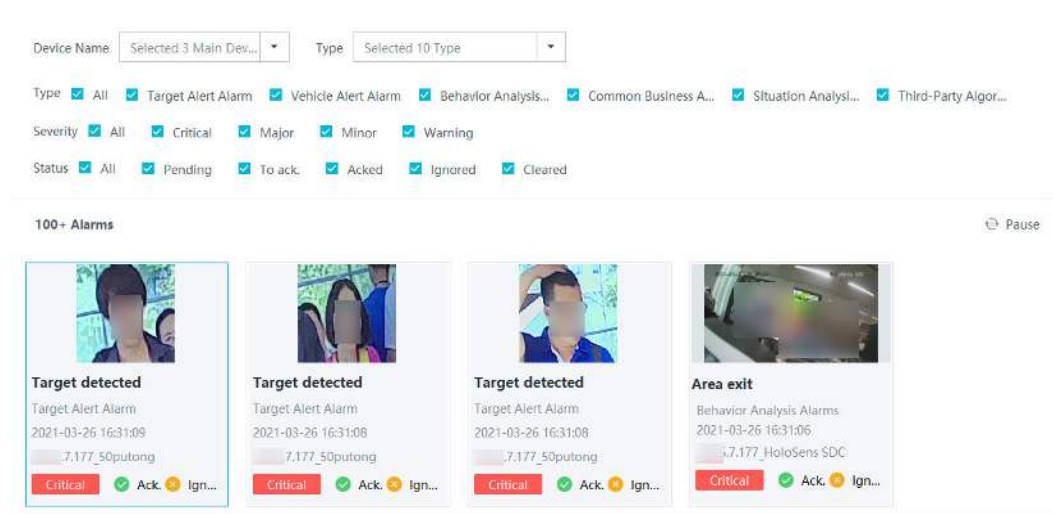
Parameter	Function
Additional Algorithm Alarm	

5.12.1.1 Latest Alarms

On the **Latest Alarm** page, you can view up to 100 latest alarms, which are updated in real time.

- Step 1** On the iClient S100 home page, choose **Complex Applications > Video Alarm > Latest Alarm**. The page shown in [Figure 5-173](#) is displayed.

Figure 5-173 Latest Alarm

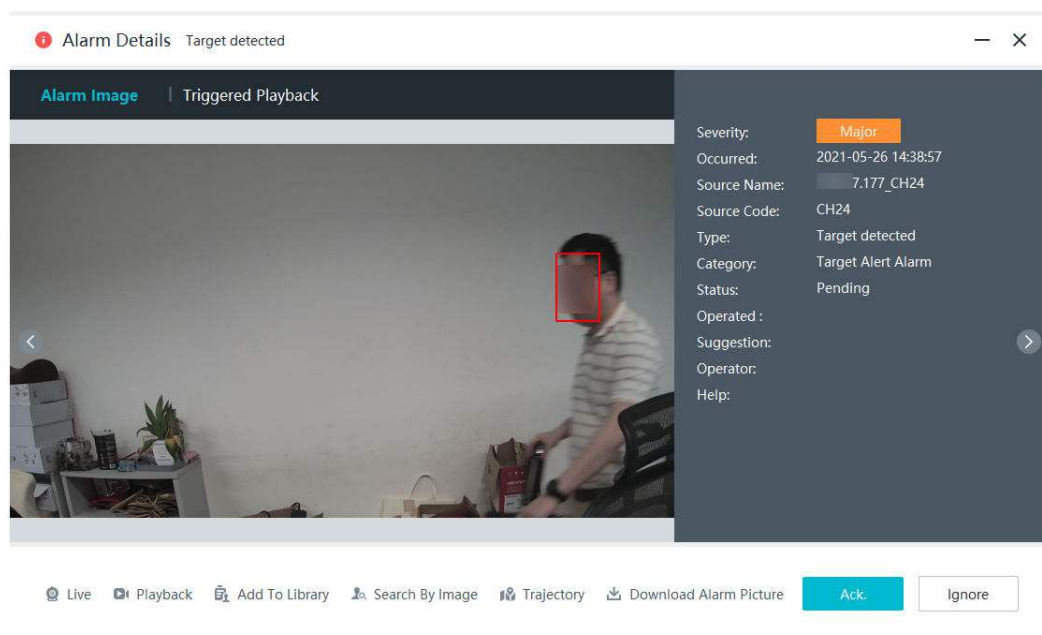


- Step 2** Select one or more main devices from the **Device Name** drop-down list as required. Then, select desired alarms subtypes from the **Type** drop-down list box as required, and all alarms of these subtypes reported by the selected main devices are automatically displayed on the page.

- Step 3** To view alarms of specified types, filter out the alarms by criteria such as the alarm type, alarm severity, and alarm status.

Alarms in the row of **Type** are of parent types. [Table 5-140](#) describes instances of alarms of parent types.

- Step 4** Click an alarm. The **Alarm Details** page is displayed, as shown in [Figure 5-174](#). [Table 5-141](#) describes the parameters on this page.

Figure 5-174 Alarm Details page**Table 5-141** Parameters/Buttons on the Alarm Details page

Type	Parameter/Button	Description
Alarm linkage	Triggered Snapshot/ Triggered Live/ Triggered Playback	Tab pages that display the results linked to the selected alarm if alarm linkage is configured for the camera.
Common functions	Live	Button for going to the Live page where you can view live video from the camera that generates the alarm.
	Playback	Button for going to the Playback page where you can play back the recording generated when the alarm is triggered.
	Downloading Alarm Picture	Button for downloading snapshots taken when the alarm is triggered.
Functions related to target recognition alarms	Add To Library	Button for going to the Target List page where you can enter list information and add the target to the target list.
	Search By Image	Button for going to the Search By Image page where you can search for similar snapshots taken by the current camera.
	Trajectory	Button for going to the Map page where you can view target trajectories on the map.

Type	Parameter/Button	Description
Alarm handling	Ack./Ignore	Button for going to the page for entering handling suggestions.

----End

5.12.1.2 Historical Alarms

You can view desired types of historical alarms on the **Target Alert Alarm**, **Vehicle Alert Alarm**, **Behavior Analysis Alarm**, **Common Business Alarm**, **Situation Analysis Alarms**, and **Third-Party Algorithm Alarms** tab pages. [Table 5-140](#) describes the alarm parent types and subtypes as well as their mappings.

This section uses **Target Alert Alarm** as an example to describe how to view historical alarms generated through a target alert or mask detection task.

- Step 1** On the iClient S100 home page, choose **Complex Applications > Video Alarm > Target Alert Alarm**.
- Step 2** Set alarm search criteria. [Table 5-142](#) describes the parameters.

Table 5-142 Parameters, buttons, and icons on the Target Alert Alarm page

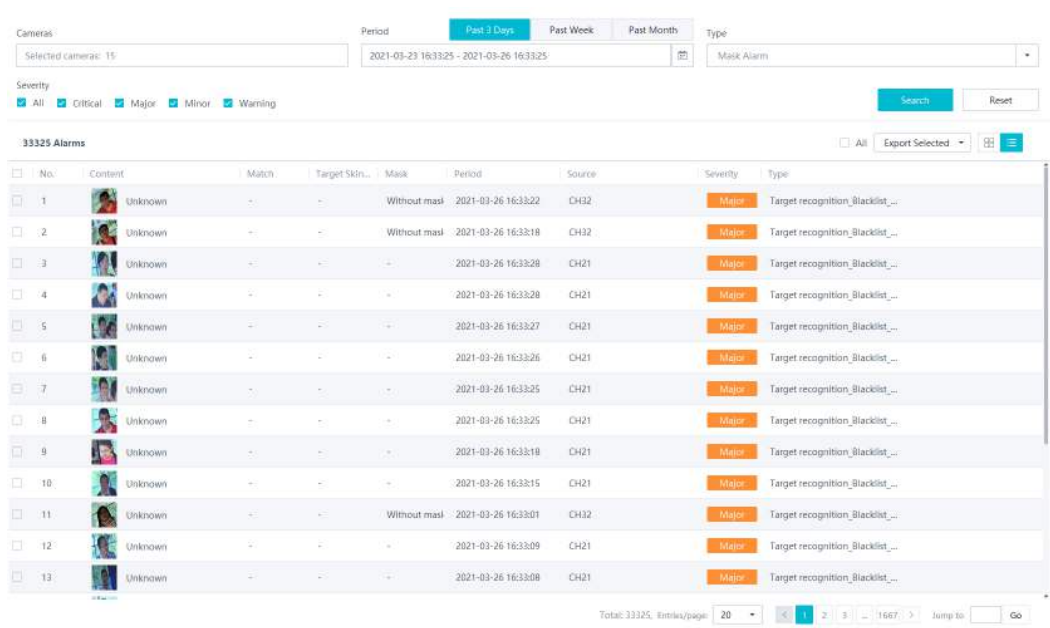
Parameter/ Button/Icon	Description
Cameras	Cameras from which alarms are to be searched for. You can select cameras connected multiple main devices of the same type.
Period	Time segment during which an alarm is generated.
Type	Alarm subtype supported by the selected cameras. Only available subtypes are automatically displayed in the drop-down list.
Severity	Importance and urgency of an alert task. The Severity parameter corresponds to Alert Level of an alert task.
Search	Button for searching for alarms based on the specified criteria.
Reset	Button for restoring to initial search criteria.
All	Selects all alarms on the current page by one click.

Parameter/ Button/Icon	Description	
Export Selected	Exports the selected alarms to the local computer in an Excel file.	NOTE You can enable the encrypted download function when exporting files to the local computer. After this function is enabled, you need to enter the preset password to open the exported files. The password must meet the following requirements: • Contains 10 to 16 characters. • Contains at least two types of the following: lowercase letters, uppercase letters, digits, and special characters. • Must be different from the user name or user name spelled backwards. • Cannot contain space characters or Chinese characters. • Cannot be a weak password.
Export This Page	Exports the alarms on the current page to the local computer in an Excel file.	
Export All	Exports all alarms in the search result to the local computer in an Excel file.	
	Switches the tile or list display mode of the alarm search result.	

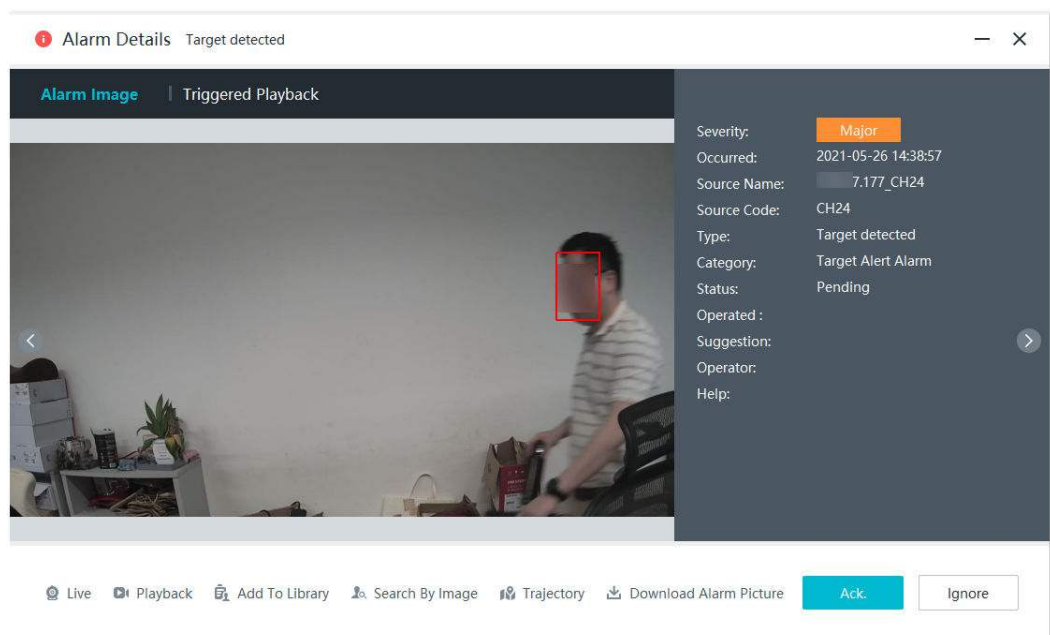
NOTE

- All export and import functions can be used only in the following environments:
 - The WPS Office software is used by default.
 - The Microsoft Office software (later than Microsoft Office 2007) is installed properly. The legal license is activated and can run properly.
- You are advised to use professional video or image editing tools to shield irrelevant persons in downloaded or exported video or images and meet the HD requirements of the data subject. The recommended procedure is as follows:
 1. Download the required video to the local computer and decompress it to common video or export image data to the local computer.
 2. Use a video or an image editing tool to anonymize irrelevant targets and only retain the HD part of the data subject.
 3. Export the anonymized video or images to meet the data transfer requirements of the data subject.
 4. To ensure personal information security, delete the downloaded or exported images and recordings in a timely manner.

Step 3 Click **Search**. The search result is displayed, as shown in [Figure 5-175](#).

Figure 5-175 Target alert alarms

Step 4 Click an alarm. The **Alarm Details** page is displayed, as shown in [Figure 5-176](#). [Table 5-143](#) describes the parameters on this page.

Figure 5-176 Alarm Details page**Table 5-143** Parameters/Buttons on the Alarm Details page

Type	Parameter/Button	Description
Alarm linkage	Triggered Snapshot/ Triggered Live/ Triggered Playback	Tab pages that display the results linked to the selected alarm if alarm linkage is configured for the camera.

Type	Parameter/Button	Description
Common functions	Live	Button for going to the Live page where you can view live video from the camera that generates the alarm.
	Playback	Button for going to the Playback page where you can play back the recording generated when the alarm is triggered.
	Downloading Alarm Picture	Button for downloading snapshots taken when the alarm is triggered.
Functions related to target recognition alarms	Add To Library	Button for going to the Target List page where you can enter list information and add the target to the target list.
	Search By Image	Button for going to the Search By Image page where you can search for similar snapshots taken by the current camera.
	Trajectory	Button for going to the Map page where you can view target trajectories on the map.
Alarm handling	Ack./Ignore	Button for going to the page for entering handling suggestions.

-----End

5.12.2 Alarm Linkage

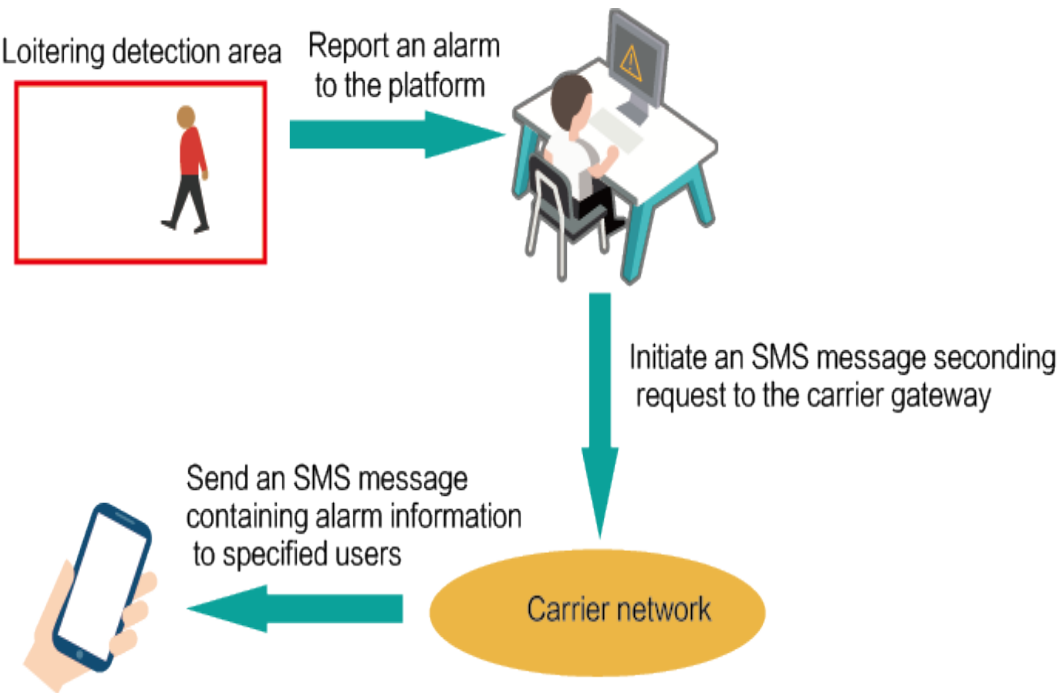
5.12.2.1 Application Scenario

This section describes how to configure the alarm linkage feature. After alarm linkage is configured, the IVS1800 performs preset linkage actions when an alarm is generated. This ensures timely alarm handling. The typical application scenario is as follows:

Some key areas raise high security requirements, and 7/24 manual detection will bring high costs. To solve this problem, the alarm linkage feature is introduced.

Exhibition hall A is a key area. To prevent theft, a series of security plans (such as intrusion detection plans, tripwire crossing detection plans, and loitering detection plans) are set. You want cameras to take snapshots, record video, or send them to employees when an exception occurs (for example, intrusion, tripwire crossing, or loitering) so that employees can handle exceptions promptly and effectively and record evidence. To achieve this goal, you need to configure alarm linkage for cameras in the exhibition hall. When detecting an abnormal person loiters in the detection area, the device reports the alarm to the iClient S100 client, as shown in [Figure 5-177](#).

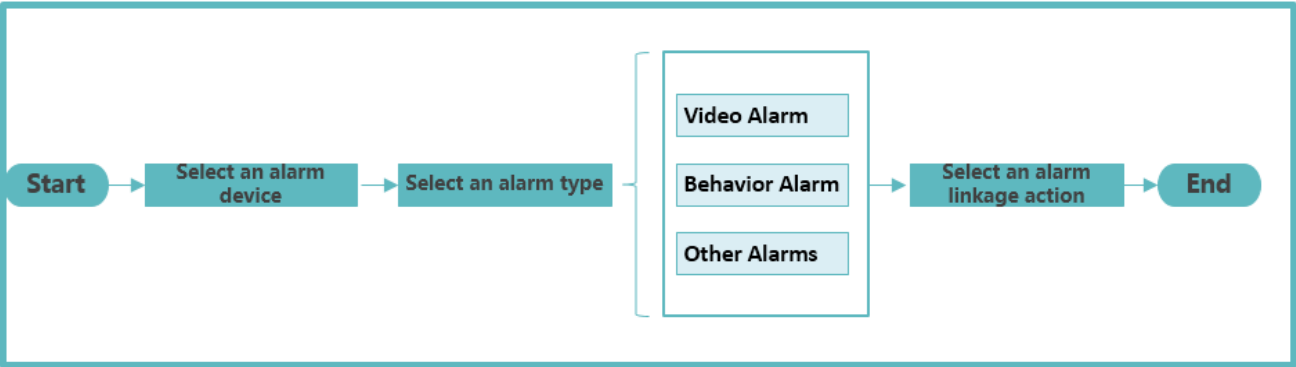
Figure 5-177 Scenario



5.12.2.2 Configuration Process

Figure 5-178 shows the alarm linkage configuration process.

Figure 5-178 Configuration process



5.12.2.3 Prerequisites

Table 5-144 Prerequisites for configuring alarm linkage

Alarm Action	Prerequisites
Live video display on video wall	The video wall has been configured. For details, see 5.4.1 Configuring a Video Wall .

Alarm Action	Prerequisites
Boolean value output	The alarm input and output parameters of the camera have been set. For details, see 8.1.4.1 How Do I Set Alarm Input and Output Parameters for a Camera? . NOTE The IVS1800 9.0.0 supports Boolean value output alarms but not Boolean value input alarms.
Preset position display	The preset position and home position have been configured.

5.12.2.4 Configuring an Alarm Linkage Policy

Procedure

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Right-click an IVS1800 and choose **Alarm Management > Alarm Linkage**.
- Step 3** Add an alarm linkage policy. The following uses the **Camera List** menu as an example. For details about the parameters for selecting alarm devices, see [Table 5-145](#).

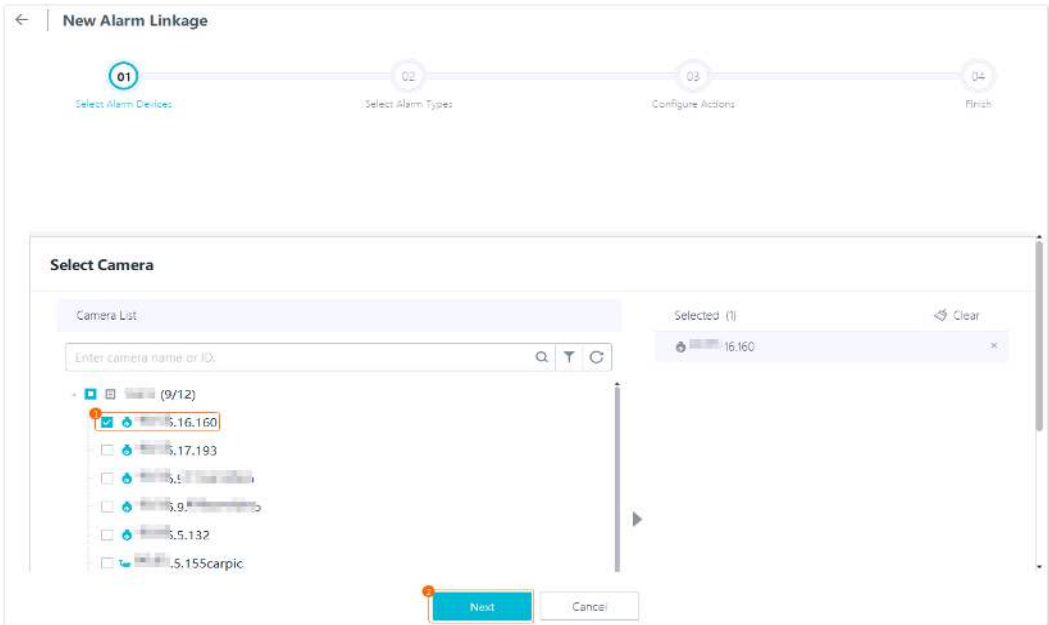
Table 5-145 Parameters for selecting alarm devices

Parameter	Description
Camera List	You can configure alarm linkage for video devices.
Alarm Source List	You can select alarm devices, for example, alarm bells to configure alarm linkage.
Protection Zone List	You can select protection zones to configure alarm linkage.

- Step 4** Select alarm devices, as shown in [Figure 5-179](#).

For a protection zone list, select the protection zone for which you want to configure alarm linkage.

Figure 5-179 Selecting alarm devices



Step 5 Select an alarm type, for example, video loss alarm.
For the alarm source list, you can select only Boolean value device alarms.

Step 6 Select an alarm action and configure the corresponding rule, as shown in [Figure 5-180](#). [Table 5-146](#) describes the alarm actions and corresponding rules.

Figure 5-180 Selecting an alarm linkage action

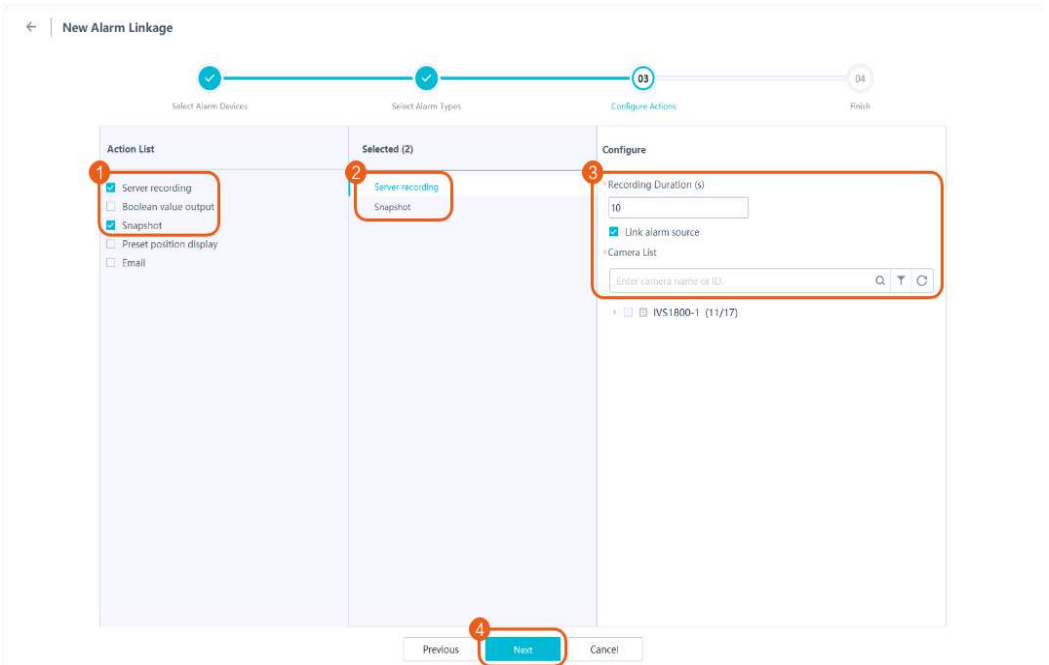


Table 5-146 Alarm action rule description

Alarm Action	Parameter	Configuration Rule
Server recording/ Snapshot	Camera List	You can select a maximum of eight cameras to be linked.
	Link alarm source	If Link alarm source is selected, you do not need to select a camera for linkage. The camera selected in Step 4 is linked by default.
Live video	Camera List	- Select a maximum of eight cameras to be linked. - After you select multiple cameras, the user list displays all users who have permissions on the selected cameras.
	User List	- Select users as required. - After the configuration is complete, if a user is online when such an alarm is generated, the iClient S100 of the user automatically switches to the Live tab page and plays live video from the specified camera.
Live video display on video wall	Camera List	- Select a maximum of eight cameras to be linked. - After you select multiple cameras, the user list displays all users who have permissions on the video wall and selected cameras.
	User List	- Select users as required. - After the configuration is complete, if the linked user is online when such an alarm is generated, the iClient S100 of the user plays the video related to the alarm on the video wall. NOTE If you have not set the screen for playing the alarm-triggered video, the video is displayed on screen 1-1 by default.
Boolean value output	Alarm Output List	You can select a maximum of eight alarm output devices.
Preset position display	Camera List	- Select a maximum of eight cameras to be linked. - You must select cameras with preset positions. For details about how to configure a preset position, see sections about preset position and home position.
	Preset Position	Select a preset position to link. If multiple cameras are selected, you must select a preset position to link for each selected camera.
Email	Email Address	Enter users' email addresses.

Alarm Action	Parameter	Configuration Rule
	Email Body	Enter the email content to be sent to the specified users after alarms are triggered.
	Add snapshot/ Select device	If you select this parameter, select a camera. When an alarm is triggered, snapshots taken by the selected camera will be sent to the specified users.
Stop server recording	Camera List	You can select a maximum of eight cameras to be linked.

NOTE

You can select multiple actions. Configure a rule for each action and click **Next**.

Only some of the GB/T 28181-compliant cameras support the alarm-triggered snapshot function. For details about cameras supporting this function, see the *IVS1800 9.0.0 Compatibility List*.

Step 7 Click **Finish**.

----End

5.12.2.5 Verification

When an alarm (such as intrusion, tripwire crossing, and loitering detection alarms) is generated, the system links the camera to take snapshots and record video. You can view the alarm information on the iClient S100 client.

Procedure

Step 1 Choose **Complex Applications > Video Alarm** on the iClient S100 home page.

Step 2 Click a required alarm tab of the corresponding service. [Table 5-147](#) describes the parameters.

Table 5-147 Alarm parent types and subtypes

Parameter	Function
Latest Alarm	Displays the latest alarms of each service. On this page, alarms are displayed and updated in real time. The alarm subtypes of the latest alarms are the same as those of historical ones.

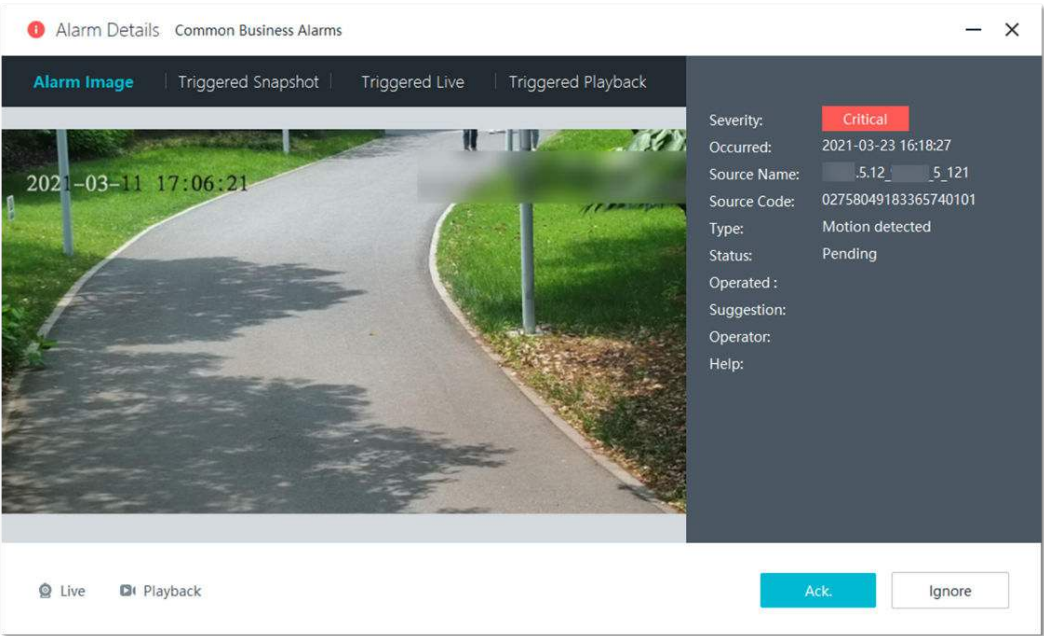
Parameter		Function
Target Alert Alarm	• Target recognition alarm • Target detection alarm • Mask detection alarm • Person detection alarm • Appearance frequency alarm (provided by the NVR800)	Displays the historical alarms of each service.
Vehicle Alert Alarm	• Vehicle recognition alarm (for motor vehicles only) • Vehicle detection alarm (for motor vehicles only) • Parking violation alarm (for motor vehicles only) • Non-motorized vehicle detection alarm	
Behavior Analysis Alarm	• Tripwire crossing detection alarm • Intrusion detection alarm • Abandoned object detection alarm • Removed object detection alarm • Loitering detection alarm • Area entry detection alarm • Area exit detection alarm • Fast movement detection alarm • Fire detection alarm • Electric bike detection alarm	

Parameter		Function
Common Business Alarm	• Motion detection alarm • Lens blocking alarm • Sudden volume increase alarm • Sudden volume decrease alarm • Video loss alarm • Micro Edge I/O alarm • Boolean value alarm	
Situation Analysis Alarm	• Human counting alarm • Queue length alarm • Crowd density alarm • Crowd gathering alarm • Off-duty detection alarm	
Additional Algorithm Alarm		

Step 3 Select the device to be queried, set alarm search criteria, and click **Search**. The found alarms are displayed in the alarm list.

Step 4 Click an alarm in the search result. The alarm details are displayed. You can view information on tab pages such as **Triggered Live** and **Triggered Playback**, and click **Ack.** or **Ignore** for alarm information as required, as shown in [Figure 5-181](#).

Figure 5-181 Alarm Details



----End

5.12.3 Alarm Management Configuration

5.12.3.1 Alarm Parameter Settings

- Step 1
- On the iClient S100 home page, choose **Maintenance Management > Personal Settings**.
- Step 2
- Set alarm parameters, as shown in **Figure 5-182**. **Table 5-148** describes the parameters.

Figure 5-182 Alarm Settings page

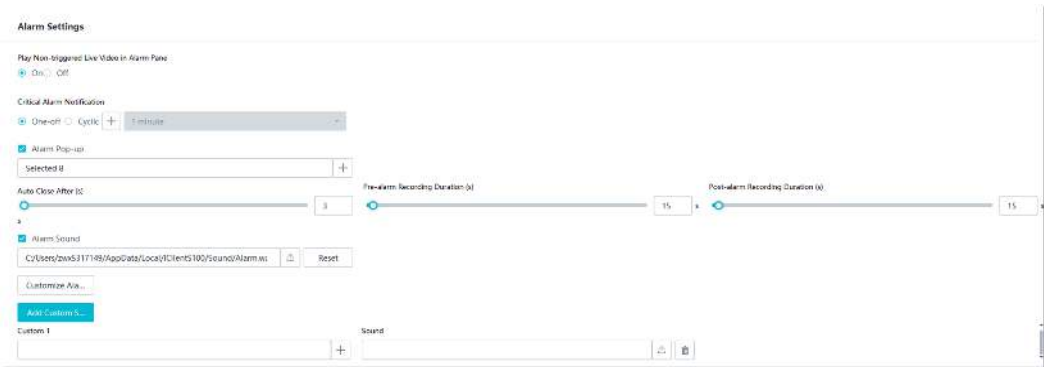


Table 5-148 Parameter description

Parameter	Description
Play Non-triggered Live Video in Alarm Pane	Indicates whether an alarm pane can play common live video. The options are as follows: ● On: yes ● Off: no
Auto Close After (s)	Display duration of a service or an NMS alarm notification.
Pre-alarm Recording Duration (s)	Video recording duration before an alarm is generated if the video recording linkage action is configured.
Post-alarm Recording Duration (s)	Video recording duration after an alarm is generated if the video recording linkage action is configured.
Critical Alarm Notification	You can select an alarm type as a critical alarm. When an alarm is generated, an alarm dialog box is displayed. Critical alarms are notified at the following intervals: ● One-off ● Cyclic notification. The interval can be set to 1 minute, 5 minutes, or 10 minutes. To set cyclic notification of critical alarms, perform the following steps: 1. Click . 2. Select Select alarm types and select an alarm type from the drop-down list box. 3. Click OK.
Alarm Pop-up	When the client receives any alarm of a specified type or severity, it displays the alarm. To enable this function, perform the following operations: 1. Select Alarm Pop-up. 2. Set Select alarm types or Select alarm severity in the dialog box. 3. Click OK. NOTE Optional operations: – Click  in the lower right corner of an alarm pop-up. Alarms will not pop up within 30 minutes. –

Parameter	Description
Alarm Sound	Audio file played when the client detects a service alarm. By default, this function is disabled. You can click  and select an audio file stored in a local directory. NOTE - Only audio files in .wav format are supported. - Click Reset to restore the system's default alarm sound. The default audio file is Alarm.wav.
Customize Alarm Sound	Click the button to add custom sounds for different alarm types. Before setting this parameter, select Alarm Sound. You can click Add Custom Sound, click Select Alarm Type, select different alarm types, and click OK. You can add different custom sounds for multiple alarm types.

Step 3 Click **Save**.

----End

5.12.3.2 Alarm Severity

You can set the alarm severity, for example, set the severity of the most concerned alarm types to critical. This enables users to quickly handle alarms based on alarm severities.

Step 1 On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.

Step 2 Right-click an IVS1800, choose **Alarm Management > Alarm Severity**, and click **New**.

Step 3 Add an alarm severity, as shown in [Figure 5-183](#).

Figure 5-183 Adding an alarm severity

New Severity

*Severity Name

Loitering

*Weight

60

Alarm Type

Enter alarm type name.

All

Critical

Loitering

Removed object

Abandoned object

Intrusion

Motion detected

VCN Boolean value input

Lens blocking

Selected (1)

Loitering

Clear

Color

Description

OK

Cancel

Table 5-149 describes the parameters.

Table 5-149 Parameter description

Parameter	Description
Severity Name	Name of an alarm severity. The default alarm severities are as follows: • Critical • Major • Minor • Warning You can change the name of a customized alarm severity based on the site requirements.

Parameter	Description
Weight	Weight of an alarm severity. The default alarm severity weights are as follows: • Critical: 100 • Major: 80 • Minor: 50 • Warning: 1 You can change the weight of a customized alarm severity based on the site requirements. The weight of a customized alarm severity must be different from those of default alarm severities.
Alarm Type	Alarm type.
Color	Color of an alarm severity. Click  to select a color.
Description	Description of an alarm severity.

Step 4 Click **OK**.

----End

5.13 Media Transmission

5.13.1 Feature Description

Definition

To ensure reliable transmission of packets, the IVS1800 provides multiple function items to ensure service continuity and availability when the network condition is poor.

Bandwidth adaptation can be configured on the iClient S100 only. FEC and SEC can be configured on the LDU of the IVS1800.

Benefits

[Table 5-150](#) lists the benefits of reliable transmission.

Table 5-150 Benefits of reliable transmission

Function Item	Benefits
FEC	• The system ensures service continuity in special cases and ensures system availability. • Users can modify FEC parameters to balance the bandwidth increase caused by FEC and the actual video effect to meet the mission-critical requirements of customers.
SEC	• The system ensures service continuity in special cases and ensures system availability. • Users can modify SEC parameters to balance the bandwidth increase caused by SEC and the actual video effect to meet the mission-critical requirements of customers.
Bandwidth adaptation	• The system ensures service continuity in special cases and ensures system availability. • The system balances the bandwidth pressure and video effect to meet the mission-critical requirements of customers.

Application Scenarios

Reliable transmission involves multiple functions. [Table 5-151](#) shows the application scenarios of these functions.

Table 5-151 Application scenarios of reliable transmission

Function Item	Application Scenario
FEC	When a lot of data packets are lost or incorrect due to poor network performance, error correction packets and FEC can be used to improve video availability and quality.
SEC	When a lot of data packets are lost or incorrect due to poor network performance, error correction packets and SEC can be used to improve video availability and quality.
Bandwidth adaptation	This feature can reduce video quality to ensure video timeliness and availability when the network conditions are poor.

Functions

[Table 5-152](#) lists the functions of this feature.

Table 5-152 Feature functions

Function	Description
FEC	Supports FEC-enabled media transmission, ensuring that the video is played smoothly even with a 5% packet loss. The FEC parameters are configurable.
SEC	Supports SEC-enabled media transmission, ensuring that the video is played smoothly even with a 20% packet loss. The SEC parameters are configurable.
Bandwidth adaptation	Works with PUs to detect the network bandwidth. Based on the network bandwidth, the PUs dynamically adjust the bit rate to ensure smooth video.

5.13.2 Setting Bandwidth Adaptation Parameters

Prerequisites

This function is valid only when the following conditions are met:

- The stream type is set to **Primary**.
- The encoding protocol is set to **H.264** or **H.265**.
- The bit rate type is set to **Constant bit rate**.
- The dynamic bit rate function is disabled.
- The bandwidth adaptation parameters have been set on the camera.

Setting Bandwidth Adaptation Parameters

- Step 1** On the iClient S100 home page, choose **Maintenance Management > Video Device > Device List > Main Devices**.
- Step 2** Double-click a camera connected to a main device.
- Step 3** On the configuration page that is displayed, choose **Video Channel > Video**.
- Step 4** On the **Primary** tab page, configure the constant bit rate, as shown in [Figure 5-184](#).

Figure 5-184 Configuring a constant bit rate

The screenshot shows the configuration page for the Primary video channel. The 'Primary' tab is selected. The configuration fields are as follows:

- Encoding Format:** H264
- Transmission Protocol:** RTP over TCP
- Bit Rate Type:** Constant bit rate (selected), Variable bit rate (unselected)
- Packing Protocol:** ES (selected), PS (unselected)
- Profile:** MP
- Bit Rate:** 2048
- I-Frame Interval:** 25
- Resolution:** 1280*720
- Frame Rate:** 25
- Image Quality:** High
- Intelligent Encoding:** ☐ (unchecked)
- Set video parameter for alarm-triggered:** ☐ (unchecked)

A 'Save' button is located at the bottom right of the configuration area.

Table 5-153 describes the parameters.

Table 5-153 Parameter description

Parameter	Description
Encoding Format	Select H.264 or H.265 .
Constant bit rate	Constant bit rate indicates that the rate at which a codec's output data should be consumed is stable. If the bit rate is incorrectly configured for images with fast encoding and compression speed but great dynamic changes, the images will be unclear.
Variable bit rate	The bit rate varies depending on the image complexity to ensure that large dynamic images are clear. However, the compression speed is low. The bit rate is low if the image is simple or static.

----End

Verification

- When the camera is in an environment with high bandwidth:
Click  on the **Live** tab page and view the current video bit rate. The bit rate is high.
- When the camera is in an environment with low bandwidth:
Click  on the **Live** tab page and view the current video bit rate. The bit rate is low.

6 Comprehensive Services

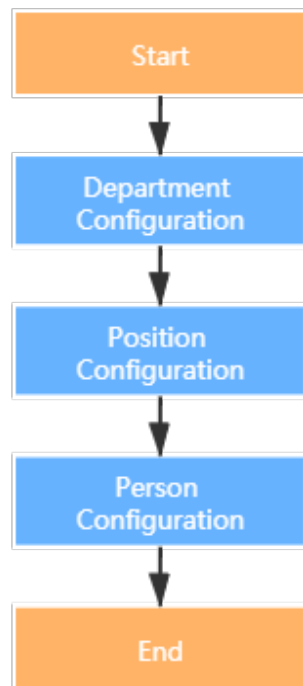
- 6.1 Personnel Management
- 6.2 Access Control Management
- 6.3 Configuring Electronic Maps
- 6.4 Attendance Management Service Configuration
- 6.5 Configuring Epidemic Prevention Management
- 6.6 Configuring User Permission Management

6.1 Personnel Management

6.1.1 Configuration Process

This section describes how to configure and manage personnel organizations after the iClient S100 is installed. The configurations will be used for scenario-specific applications such as access control, attendance, and epidemic prevention.

Figure 6-1 shows the process of configuring a personnel organization.

Figure 6-1 Configuration process

Personnel organization configurations include department, position, and person configurations. [Table 6-1](#) describes these configurations by type.

Table 6-1 Personnel organization configurations

Type	Description
Department configuration	Describes and manages the organization structure of a department.
Position configuration	Adds positions to clarify position levels and approval processes and establish a standard HR structure.
Person configuration	Adds persons on the iClient S100 or through devices. When adding persons on the iClient S100, you can add them one by one or import them in batches from other software or information centers.

6.1.2 Adding Departments

You can import departments in batches or add them one by one. [Table 6-2](#) describes the two methods.

Table 6-2 Methods of adding departments

Method	Description
Importing departments in batches	If a department organization structure has been planned, you can import departments in batches.
Adding departments one by one	If only a small number of departments need to be added, you can add them one by one.

6.1.2.1 Importing Departments in Batches

This section describes how to import departments in batches on the iClient S100.

This method applies to scenarios where a large number of departments need to be added. It is more efficient than the method of manually adding departments one by one. To use the batch import method, you need to plan a department organization in advance and fill in the import template.

Procedure

Before importing departments in batches, you need to fill in a built-in template file. Then you can use the template file to import departments in batches on the **Department** page.

NOTE

- The parent department parameters specify a company's organization structure that is displayed in a department tree on the iClient S100.
- Before importing departments in batches, ensure that each department has a unique ID. Duplicate department IDs will cause batch import failure.

Step 1 Choose **Personnel Management > Personnel > Department** on the iClient S100 home page.

Step 2 On the **Department** page that is displayed, choose **Export > Download Department Import Template** and download the **Department Import Template.xls** file to the local computer.

Step 3 Open the template file and fill it in as required. [Table 6-3](#) describes the parameters.

Table 6-3 Parameter description

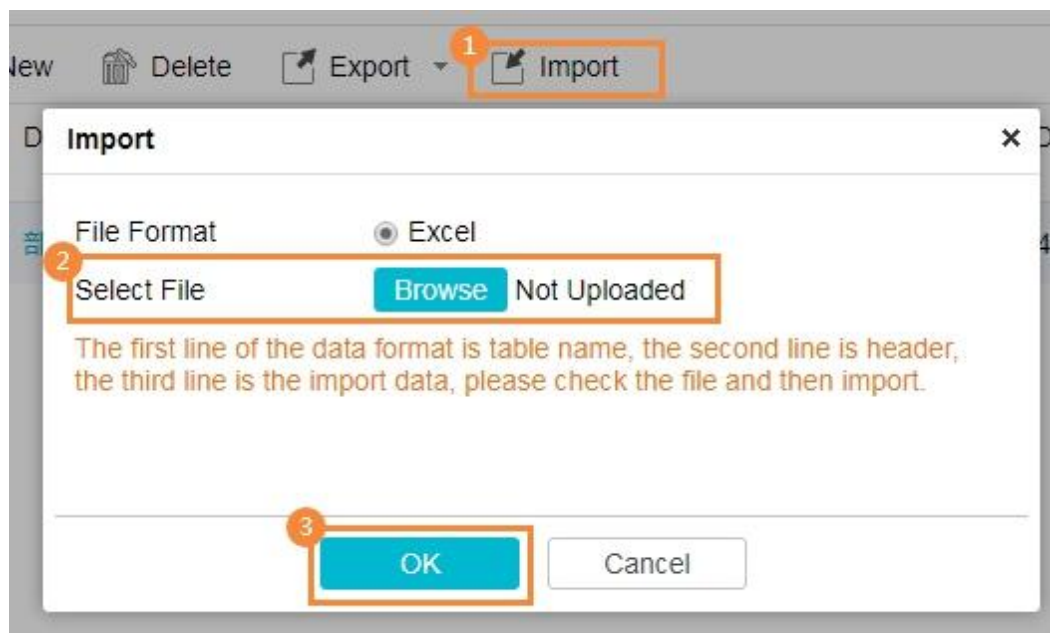
Parameter	Description
Department Number	Department ID, which can contain letters and digits.
Department Name	Department name.

Parameter	Description
Parent Department Number	ID of the parent department.
Parent Department Name	Name of the parent department.

Step 4 On the **Department** page, click **Import**.

Step 5 Click **Browse** and select the template file to be imported, as shown in [Figure 6-2](#).

Figure 6-2 Importing departments



Step 6 Click **OK**. The import result is displayed.

Step 7 Click **Close**.

----End

6.1.2.2 Adding Departments One by One

This section describes how to manually add departments one by one on the iClient S100.

This method applies to scenarios where a small number of departments need to be added.

Procedure

Step 1 Choose **Personnel Management > Personnel > Department** on the iClient S100 home page.

Step 2 Click **New**. The page for adding a department is displayed.

Step 3 Set parameters as required, as shown in [Figure 6-3](#). [Table 6-4](#) describes the parameters.

Figure 6-3 Adding a department

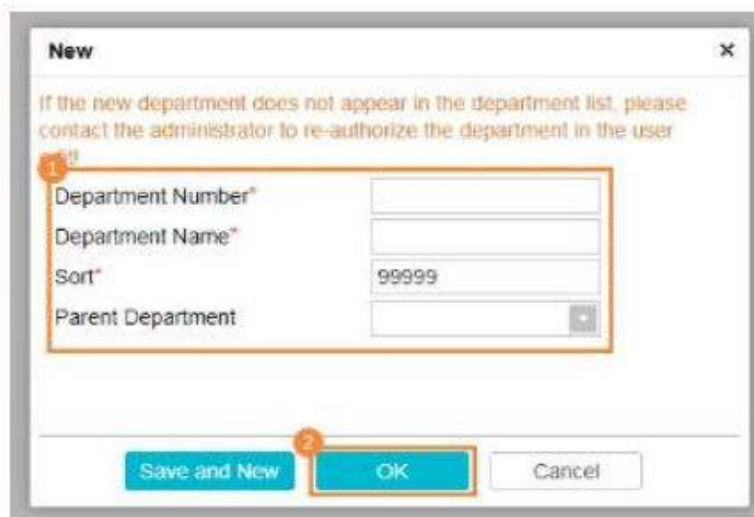


Table 6-4 Parameter description

Parameter	Description
Department Number	Department ID.
Department Name	Department name.
Sort	Department sequence number, which can contain only digits.
Parent Department	Parent department of the department to be added. Select an option from the drop-down list box.

Step 4 Click **OK**.

----End

6.1.3 Position Configuration

In this, new positions can be added manually. The parameter settings of newly add positions is shown in [6.1.3.1 Adding Positions One by One](#).

6.1.3.1 Adding Positions One by One

This section describes how to manually add positions one by one on the iClient S100. The positions will be used for adding persons.

Procedure

- Step 1** Choose **Personnel Management > Personnel > Position** on the iClient S100 home page.
- Step 2** Click **New**. The page for adding a position is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-4](#). [Table 6-5](#) describes the parameters.

Figure 6-4 Adding a position

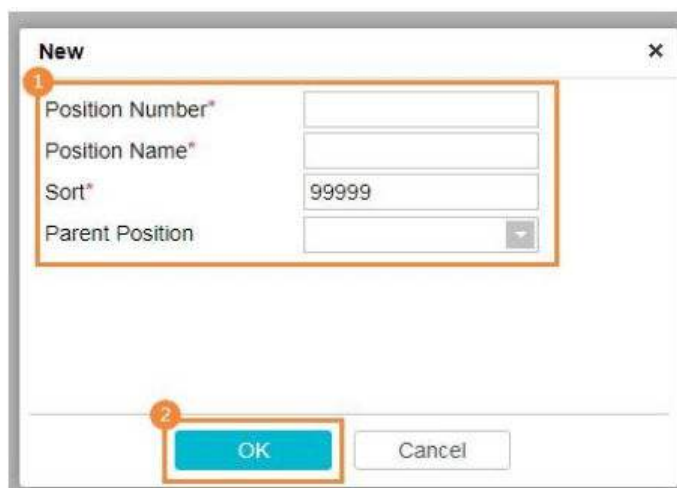


Table 6-5 Parameter description

Parameter	Description
Position Number	Position ID.
Position Name	Position name.
Sort	Position sequence number, which can contain only digits.
Parent Position	Parent position of the position to be added. Select an option from the drop-down list box. To cancel the selection, click the selected option.

- Step 4** Click **OK**.

----End

6.1.4 Adding Persons

You can add persons in batches (by importing them from other software or information centers) or one by one on the iClient S100 or through devices. [Table 6-6](#) describes the three methods.

Table 6-6 Methods of adding persons

Method	Description
Importing persons in batches on the iClient S100	When a large number of persons with electronic profiles need to be added, you can import persons in batches. The import process includes importing person information, importing biometric recognition data (optional), and importing person photos (optional).
Adding persons one by one on the iClient S100	When a small number of persons need to be added, you can add persons one by one on the iClient S100.
Adding person through devices	When a small number of persons need to be added, you can add person information on devices that support the manual adding function and then synchronize the information to the iClient S100.

6.1.4.1 Importing Persons in Batches on the iClient S100

This section describes how to import persons in batches on the iClient S100.

This method applies to scenarios where a large number of persons need to be added. It is more efficient than the method of manually adding persons one by one.

NOTE

- The import process includes importing person information, importing biometric recognition data (optional), and importing person photos (optional).
- Before importing persons in batches, ensure that each person has a unique personnel ID. Duplicate personnel IDs will cause import failure.

6.1.4.1.1 Importing Person Information

Before adding persons in batches, you need to download and fill in a template file as required. Then you can use the template to add persons in batches on the **Personnel** page.

Procedure

- Step 1** Choose **Personnel Management > Personnel > Person** on the iClient S100 home page.
- Step 2** On the **Person** page that is displayed, choose **Export > Download Personnel Import Template**, select the parameters to be set, and download the **Personnel Import Template.xls** file to the local computer. [Figure 6-5](#) describes the parameters.

Figure 6-5 Download Personnel Import Template

Step 3 Open the template file and fill it in as required.

Step 4 On the **Person** page, choose **Import > Import Personnel**. On the **Import Personnel** page that is displayed, click **Browse** and import the template file, as shown in [Figure 6-6](#).

Figure 6-6 Import Personnel page

Step 5 Click **OK**. The import result is displayed.

Step 6 Click **Close**.

----End

6.1.4.1.2 (Optional) Importing Biometric Recognition Data

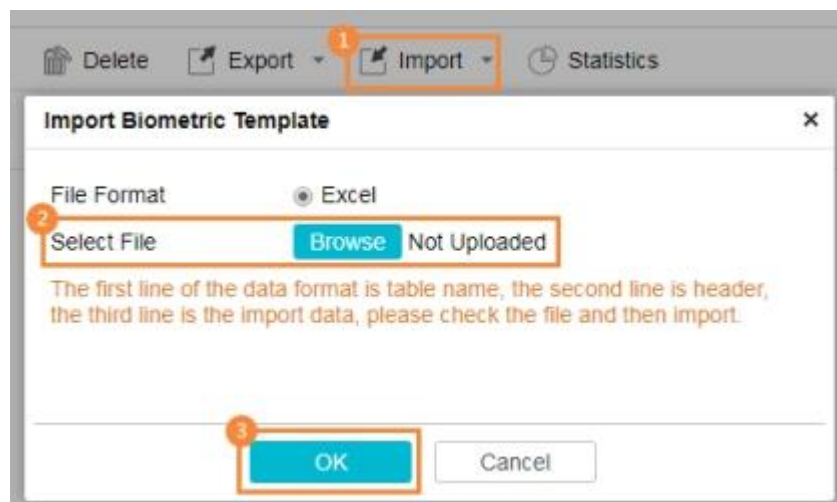
Prerequisites

1. You have added basic person information to the iClient S100.
2. You have obtained the template file containing biometric recognition data of the target person.

Procedure

- Step 1** Choose **Personnel Management > Personnel > Person** on the iClient S100 home page.
- Step 2** On the **Person** page, choose **Import > Import Biometric Template**. On the page that is displayed, click **Browse** and import the biometric template file, as shown in [Figure 6-7](#).

Figure 6-7 Import Biometric Template



- Step 3** Click **OK**. The import result is displayed.

- Step 4** Click **Close**.

----End

6.1.4.1.3 (Optional) Importing Person Photos

Prerequisites

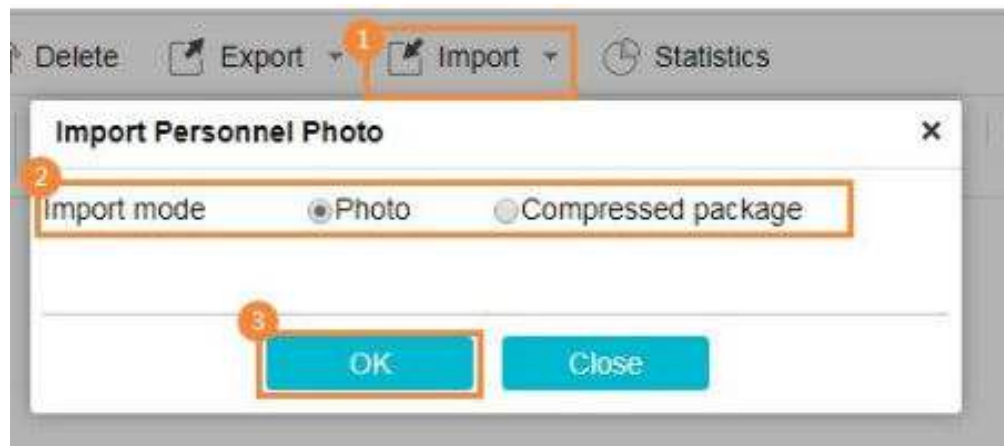
1. You have added basic person information to the iClient S100.
2. You have obtained photos of the target person and named the photos by personnel ID.
3. The photos must meet the following requirements:
 - Image format: .jpg or .png
 - Size of an image: 35 KB to 200 KB (recommended); 5 MB (maximum)
 - Image quality: clear and recognizable; grayscale image with a bit depth ≥ 8

- Resolution: target cutout: 80 x 80 pixels to 200 x 200 pixels (recommended); eye spacing: at least 60 pixels (≥ 90 pixels being recommended)
- Brightness and contrast: ambient illumination: ≥ 300 lux; diffuse lighting (for the best effect); moderate contrast and exposure; no shadow, backlight or light reflection on targets
- Posture: proper posture; look straight ahead; angle range: -10° to $+10^\circ$ (for yaw angles, pitch angles, and roll angles)
- Occlusion: features (such as eyebrows, eyes, mouths, noses, and target contours): not covered by occluders such as hair, masks, accessories, or glasses; glass lens: clear, colorless, and non-reflective (for the best effect)
- target: completely captured, well-defined, unretouched, and with light or no makeup
- Countenance: neutral and unposed expression with eyes open and natural mouth gestures

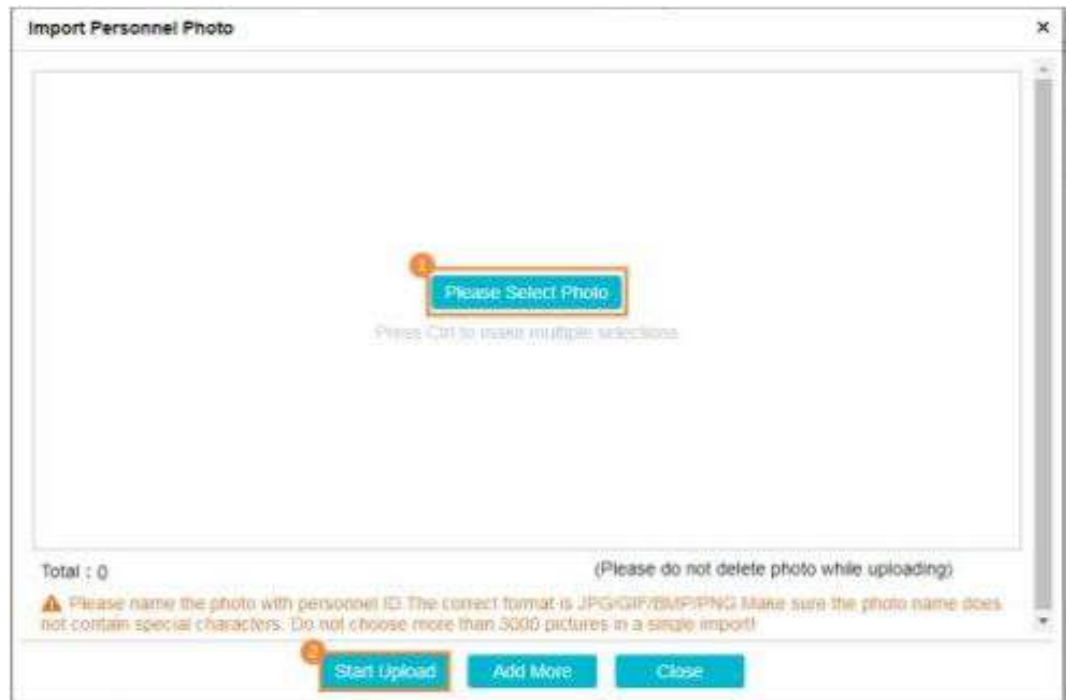
Procedure

- Step 1** Choose **Personnel Management > Personnel > Person** on the iClient S100 home page.
- Step 2** On the **Person** page that is displayed, choose **Import > Import Personnel Photo**, as shown in [Figure 6-8](#).

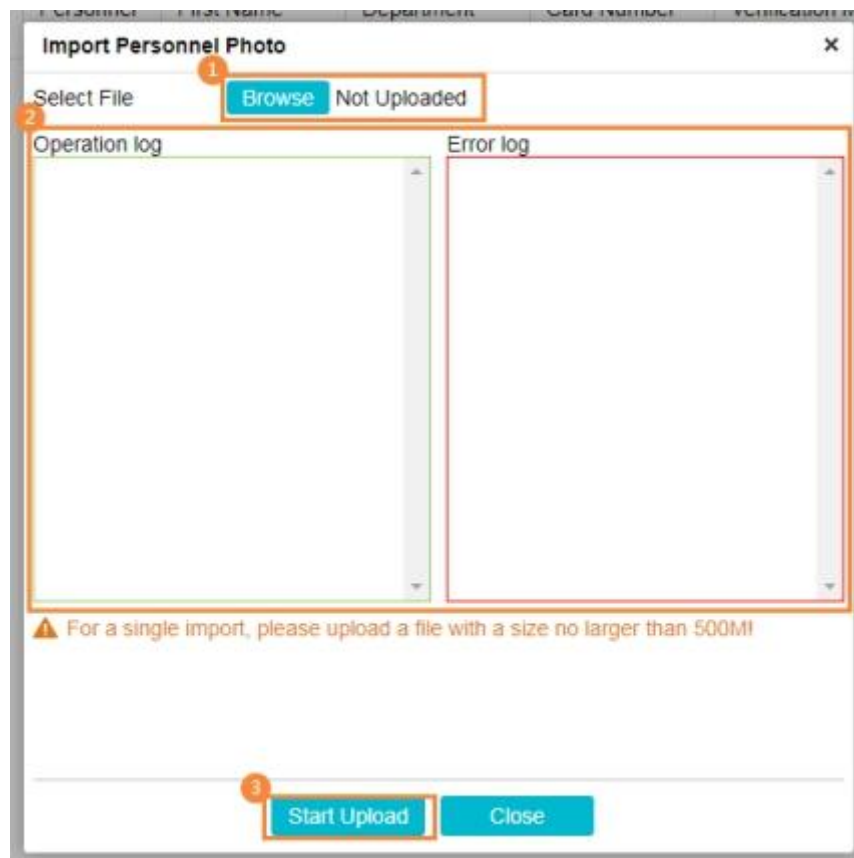
Figure 6-8 Import Personnel Photo



- Step 3** (Optional) Upload photos using either of the following methods:
1. Set **Import mode** to **Photo** and click **OK**. On the **Import Personnel Photo** page that is displayed, click **Please Select Photo**, select a photo, and click **Start Upload**, as shown in [Figure 6-9](#).

Figure 6-9 Photo - Import Personnel Photo

2. Set **Import mode** to **Compressed package** and click **OK**. On the **Import Personnel Photo** page that is displayed, click **Browse**, select a package, and click **Start Upload**, as shown in [Figure 6-9](#).

Figure 6-10 Compressed package - Import Personnel Photo

3. Wait until the upload is complete. The import result is displayed.
4. Click **Close**.

----End

6.1.4.2 Manually Adding Persons One by One on the iClient S100

This section describes how to manually add persons one by one on the iClient S100.

This method applies to scenarios where a small number of persons need to be added. In this method, you need to import person information and biometric recognition data.

6.1.4.2.1 Adding Person Information

This section describes how to manually add person information one by one on the iClient S100.

Procedure

- Step 1** Choose **Personnel Management > Personnel > Person** on the iClient S100 home page.
- Step 2** Click **New**. The page for adding person is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-11](#). [Table 6-7](#) describes the parameters.

Figure 6-11 Adding persons

New

1

Personnel ID*

First Name

Gender

Certificate Type

Birthday

Hire Date

Device Verification

Password

Biometrics Type

Department*

Last Name

Mobile Phone

Certificate Number

Email

Position Name

Card Number

Department Name

Browse

2

Access Control

Time Attendance

Personnel Detail

Levels Settings

General

Add

Select All

Unselect All

Superuser

Device Operation Role

Disabled

Set Valid Time

No

Ordinary User

3

Save and New

OK

Cancel

Table 6-7 Parameter description

Parameter	Description
Basic person information	Basic person information, including the personnel ID, name, department, position, and photo. • Device Verification: password used for verification through access control devices. • Biometrics Type: type of biometric templates (fingerprint, target, finger vein, palm print, and photo) that have been imported. The biometric recognition data is used for verification and recognition through access control and attendance devices. For details about how to import biometric recognition data, see 6.1.4.2.2 Importing Biometric Recognition Data. NOTE target photos must meet the following requirements: - Image format: .jpg or .png - Size of an image: 35 KB to 200 KB (recommended); 5 MB (maximum) - Image quality: clear and recognizable; grayscale image with a bit depth ≥ 8 - Resolution: target cutout: 80 x 80 pixels to 200 x 200 pixels (recommended); eye spacing: at least 60 pixels (≥ 90 pixels being recommended) - Brightness and contrast: ambient illumination: ≥ 300 lux; diffuse lighting (for the best effect); moderate contrast and exposure; no shadow, backlight or light reflection on targets - Posture: proper posture; look straight ahead; angle range: -10° to $+10^\circ$ (for yaw angles, pitch angles, and roll angles) - Occlusion: features (such as eyebrows, eyes, mouths, noses, and target contours): not covered by occluders such as hair, masks, accessories, or glasses; glass lens: clear, colorless, and non-reflective (for the best effect) - target: completely captured, well-defined, unretouched, and with light or no makeup - Countenance: neutral and unposed expression with eyes open and natural mouth gestures
Access Control	Person access permission.
Time Attendance	Attendance information such as the area and mode.
Personnel Detail	Other required information.

Step 4 Click **OK**.

----**End**

6.1.4.2.2 Importing Biometric Recognition Data

This section describes how to import biometric recognition data on the iClient S100 for verification and recognition through access control and attendance devices.

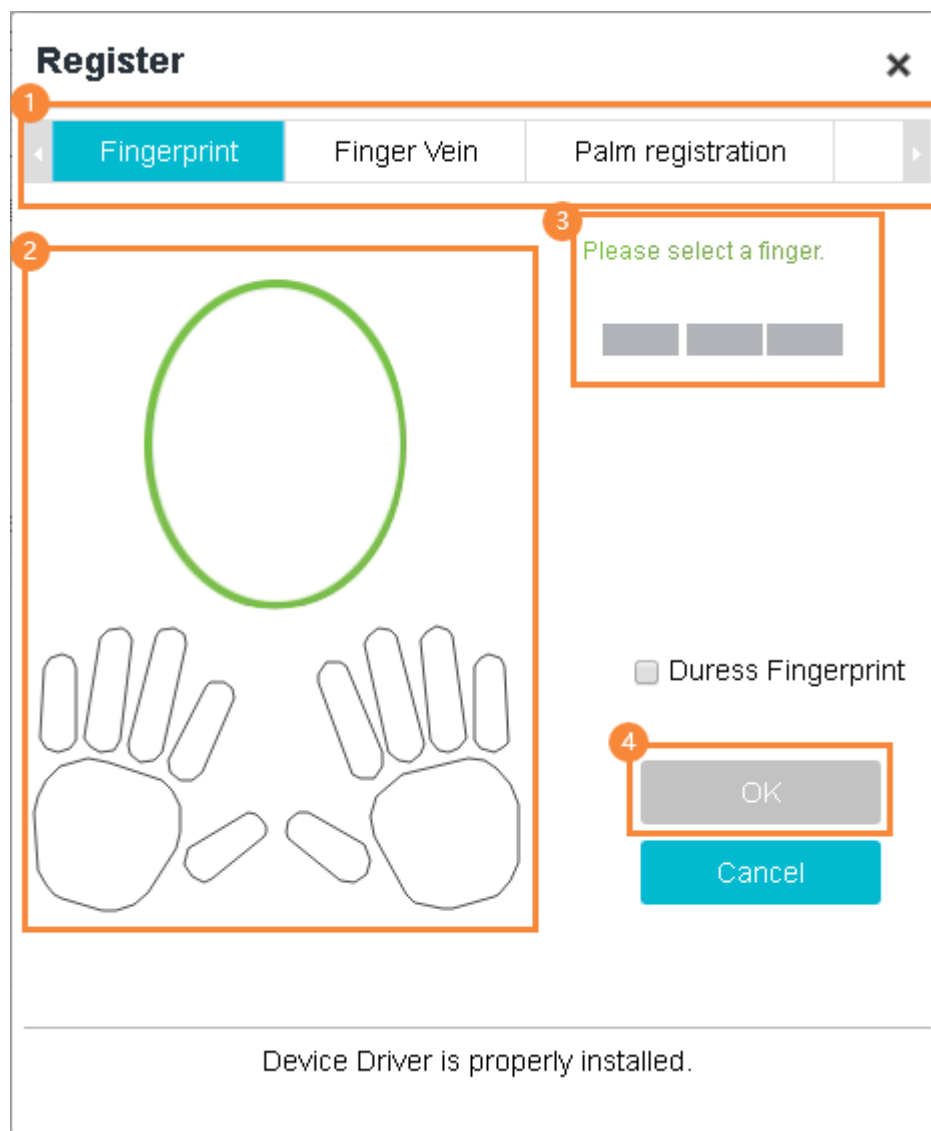
Biometric recognition data includes fingerprints, finger veins, and palm veins. The following describes how to import fingerprints. You can follow the same instructions to import finger veins and palm veins.

Prerequisites

You have added person information on a computer as an administrator and connected the computer to a fingerprint reader through a USB port.

Procedure

- Step 1** Choose **Personnel Management > Personnel > Person** on the iClient S100 home page.
- Step 2** Click **New**.
- Step 3** On the **New** page that is displayed, click .
- Step 4** (Optional) If no driver is installed, download and install one by following the instructions in the dialog box displayed upon clicking .
- Step 5** Import fingerprints after the driver is installed, as shown in [Figure 6-12](#).

Figure 6-12 Importing fingerprints

Step 6 Press a finger on the fingerprint reader for three consecutive times. Then the system displays a message indicating that the fingerprint is imported successfully.

Step 7 Click **OK**, save the data, and close the fingerprint import page.

----End

6.1.4.3 Adding Persons Through Devices

This section describes how to manually add persons through devices connected to the iClient S100.

This method applies to scenarios where a small number of persons need to be added. You can register person and biometric recognition data to connected devices and then synchronize the data to the iClient S100.

Multiple types of devices support manual registration. The following describes how to register data on an access control tablet.

Prerequisites

You have connected the iClient S100 to an access control tablet that supports manual registration.

Procedure

Step 1 (Optional) Set the access control tablet as the registration device on the iClient S100.

1. Choose **Access > Device > Device** on the iClient S100 home page.
2. Select the access control tablet and choose **Set up > Set as Registration Device**. The **Set as Registration Device** page is displayed.
3. Set registration parameters, as shown in [Figure 6-13](#).

Figure 6-13 Set as Registration Device



4. Click **OK**, save the settings, and close the page.

Step 2 Add person on the access control tablet. For details, see [8.2.5.1 How Can I Add Person Information on a Device?](#)

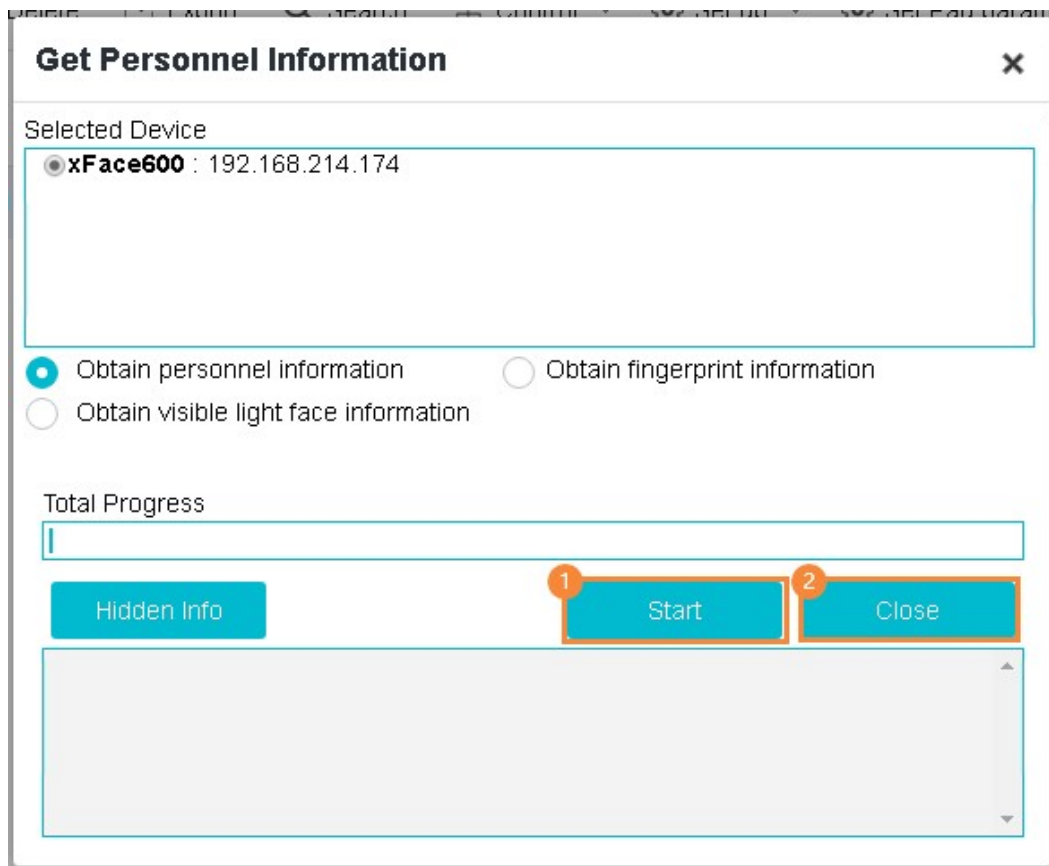
Step 3 (Optional) Manually synchronize persons to the iClient S100.

NOTE

- If you have set the tablet as a registration device in [Step 1](#) and the network connection is normal, the persons added on the tablet will be automatically synchronized to the iClient S100.
 - If you do not set the tablet as a registration device in [Step 1](#) or the network is disconnected, the persons added on the tablet may fail to be synchronized to the iClient S100. In this case, you can perform this step to synchronize the persons.
1. Choose **Access > Device > Device** on the iClient S100 home page.
 2. Select the tablet and choose **View/Get > Get Personnel Information**. The **Get Personnel Information** page is displayed.

3. Click **Start** to obtain person information, as shown in [Figure 6-14](#).

Figure 6-14 Get Personnel Information page



4. Click **Close** when the progress is complete.

----End

6.2 Access Control Management

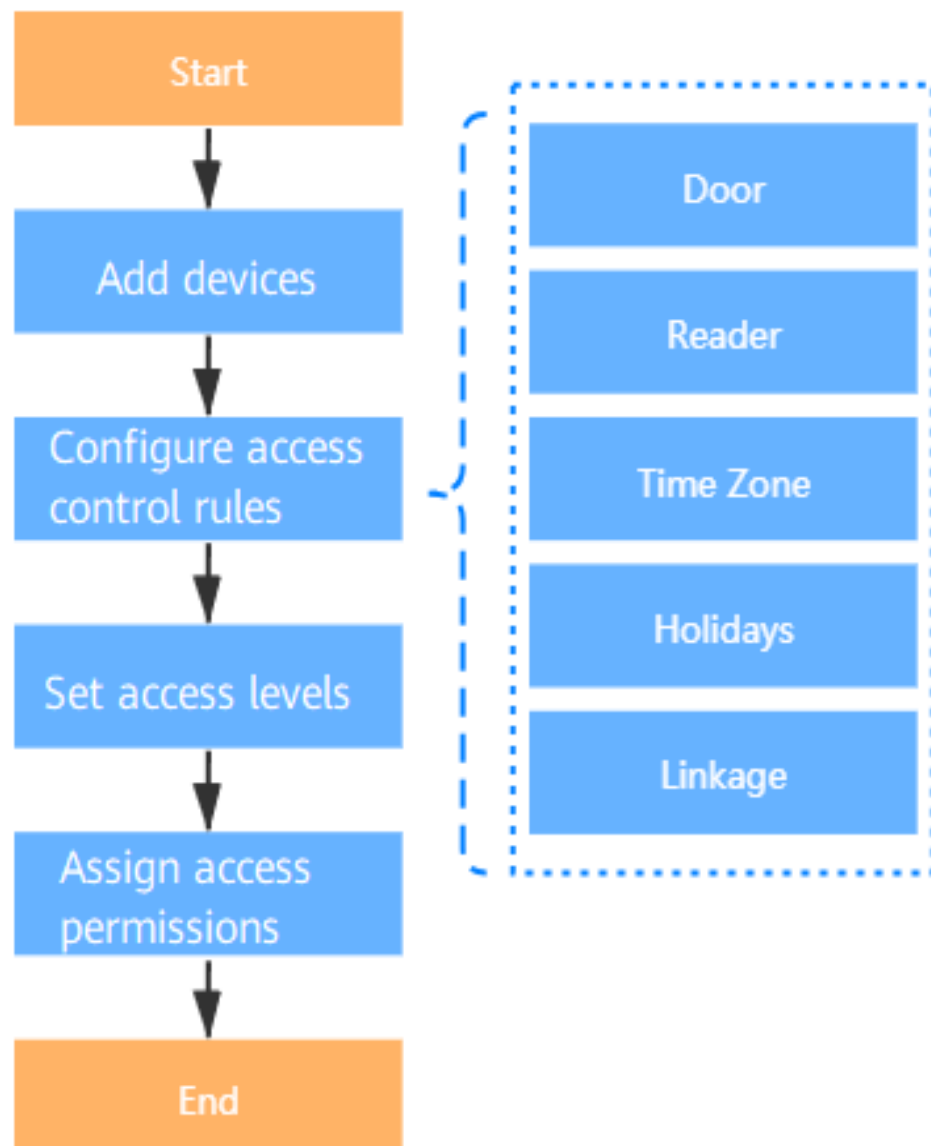
6.2.1 Application Scenario

Access control management allows you to configure access control devices and permission groups to centrally manage person entry and exit.

Access control is used to detect the access person, time, medium, and door.

6.2.2 Configuration Process

This section describes the configuration process of access control management, as shown in [Figure 6-15](#).

Figure 6-15 Configuration process

6.2.3 Adding Devices

This section describes how to search for and add access control devices on the iClient S100.

6.2.3.1 Prerequisites

1. You have assigned IP addresses to access control devices before adding these devices. For details, see [8.2.3.1 How Can I Set or Change the IP Address of an Access Control Device Using a Tool?](#).
2. You have performed the following substeps to configure the IP address and port number of the iClient S100 for access control devices:

- a. Log in to an access control device with power supply and network connected.
- b. Choose **Main Menu** > **COMM**, as shown in [Figure 6-16](#).

Figure 6-16 Communication setting



- c. On the server connection setting page, enter the IP address and port number of the iClient S100 for connection between the device and the iClient S100.

6.2.3.2 Adding Access Control Devices

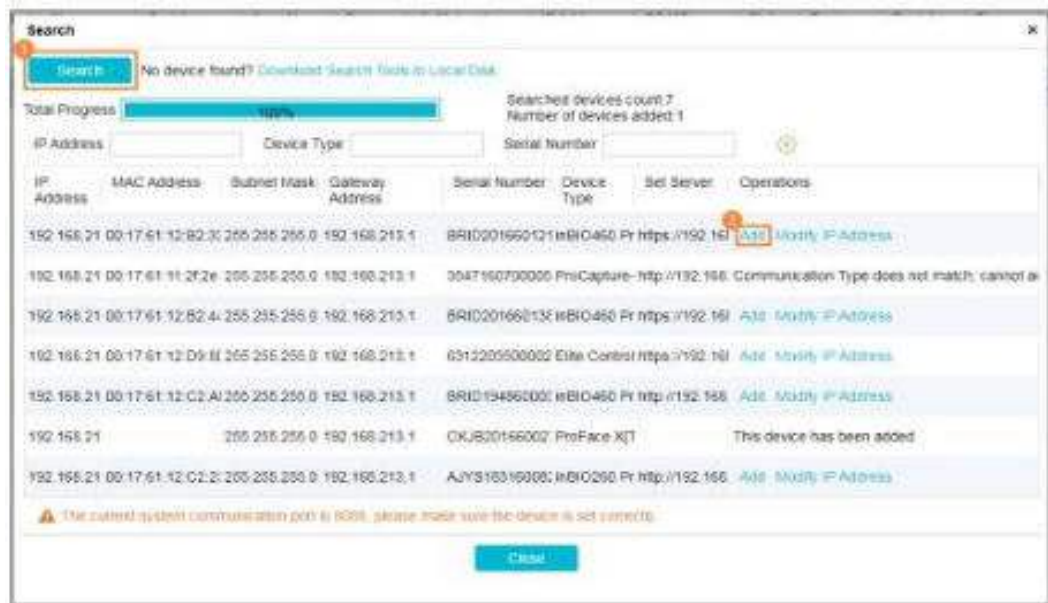
This section describes how to search for and add access control devices on the iClient S100.

You can directly add the found access control devices whose connection settings take effect on the iClient S100.

Procedure

- Step 1** Choose **Access** > **Device** > **Device** on the iClient S100 home page.
- Step 2** On the **Device** page that is displayed, click **Search**. The search box is displayed.
- Step 3** Click **Search**. Access control devices that can be added are displayed, as shown in [Figure 6-17](#).

Figure 6-17 Search



- Step 4** (Optional) To change the IP address of the access control device, click **Modify IP Address**. After the IP address is changed, the device restarts for the setting to take effect.
- Step 5** Select a found access control device, click **Add** in the **Operation** column, and set parameters on the page shown in Figure 6-18 to add the device. Table 6-8 describes the parameters.

Figure 6-18 Device adding page

Table 6-8 Parameter description

Parameter	Description
Device Name	Device name.
New Server Address/ Port	IP address and communication port of the iClient S100 server. The default communication port is 8088 .
Communication Password	Communication password of an access control device. If no password is available, leave this parameter empty. A device can be added only after the password (if any) is verified successfully. The communication password is empty for newly delivered devices and initialized devices. To prevent unauthorized users from using the device, you can enter the device IP address on the web page, log in to the server, and customize the communication password.
Icon Type	Type of the device icon on the real-time observation page. The type can be door or aisle.
Area	Home area of the device to be added. For details about how to configure an area, see 8.2.1.4 How Can I Set Up an Area? .
Add to Level	Permission group to which a device is automatically added. For details about how to configure a permission group, see 6.2.5 Setting Access Levels .
Clear Data in the Device when Adding	Indicates whether to automatically clear the original access control data in the device after the device is added.

Step 6 Click **OK**. The device restarts for the setting to take effect.

Step 7 Click **Close**.

----End

6.2.4 Configuring Access Control Rules

Access control rules are the core control logic of the access control system, including the settings of door parameters, valid time periods, and linkage.

6.2.4.1 Setting Door Parameters

The setting of door parameters affects the verification logic of the access control system.

Door parameters vary according to the device firmware. The following describes how to set door parameters for a device.

Procedure

- Step 1** Choose **Access > Device > Door** on the iClient S100 home page.
- Step 2** On the **Door** page, click **Edit** in the **Operations** column of a door. The **Edit** dialog box is displayed.
- Step 3** In the **Edit** dialog box, set door parameters as required, as shown in [Figure 6-19](#). [Table 6-9](#) describes the parameters.

Figure 6-19 Setting door parameters

NOTE

Different access control device firmware supports different door parameters. You need to set the parameters based on the actual GUI. For details about the parameters, see [Table 6-9](#).

Table 6-9 Door parameter description

Parameter	Description
Device Name/ Door Number	Basic information about the door. These two parameters cannot be modified after being set.
Door Name	Customized name of the door.
Active Time Zone	Valid time period of the door. During the time that is not within the validity period, the door cannot be opened even if a person has the access permission.
Authentication Mode	Authentication mode supported by the device. You can select an authentication mode as required.

Parameter	Description
Lock Open Duration	Duration during which a door can be opened after access is granted. For example, if this parameter is set to 5 (unit: second), a person can open the door within 5s after the verification. If the person does not open the door within 5s, the door is automatically locked and the person can open the door only after re-verification.
Wiegand Format	Format of the Wiegand card that can be recognized by the Wiegand reader at the door. If a card of a different format is used for verification, the door cannot be opened. The software has built-in nine formats. By default, this parameter is set to Automatic Identification . This means that the system can recognize Wiegand cards of all the formats embedded in the software.
REX Mode	Status of the door exit button, which can be locked or unlocked. If this parameter is set to Lock , the door is still locked after you press the exit button. If this parameter is set to Unlock , the door is unlocked after you press the exit button.
REX Delay	Delay between the time when you press the exit button and the door opening. This parameter is available when you set REX Mode to Lock .
Operate Interval	Interval between two verifications.
REX Time Zone	Valid time period of the exit button.
Door Sensor Type	Door sensor type. The options are None (default), Normal Open , and Normal Close .
Close and Reverse State	Indicates whether to lock the door after it is closed.
Door Sensor Delay	Delay time for checking the door status after the door is opened. In the scenario where Door Sensor Type is not set to Normal Open and the door is opened, after the time period specified by this parameter elapses, the door status sensor generates an alarm. Such an alarm will be cleared when the door is closed.
Anti-Passback Duration of Entrance	Time period in which a person can enter for a time.
Duress Password	The system generates an alarm after you enter the duress password. You can use this password when you are coerced.

Parameter	Description
Emergency Password	Password used in emergencies. This password is valid during any time period and in any authentication mode. Generally, it is used by the administrator.
Passage Mode Time Zone	Time segment during which the door is always open.
Passage Delay	Additional time period added on the original door opening period. It is often used to extend the passage time for persons with disabilities and persons who are inconvenient to pass.
Open Door Delay	Delay for opening the door after the verification succeeds.
Disable Alarm	Indicates whether to play an alarm sound on the real-time detection page when an alarm is generated at the door.
Allow super users to pass when the door is locked	Indicates whether to allow super users to pass after verification when the door is locked.
The above settings are copied to	Doors to which the preceding door parameters apply. The options are All doors of the current device and All doors of all devices .

Step 4 Click **OK**.

----End

6.2.4.2 Binding Reader/Auxiliary Input Devices to Cameras

This section describes how to bind readers to cameras on the iClient S100.

Application Scenario

After a reader or an auxiliary input device is bound to a camera and linkage actions are configured, the video (snapshot) linkage will be performed once the corresponding event is triggered by the reader/auxiliary input.

The method for binding a camera to a reader is the same as that to an auxiliary input device. The following uses the reader as an example.

Prerequisites

A camera has been added on the **Video Device** page.

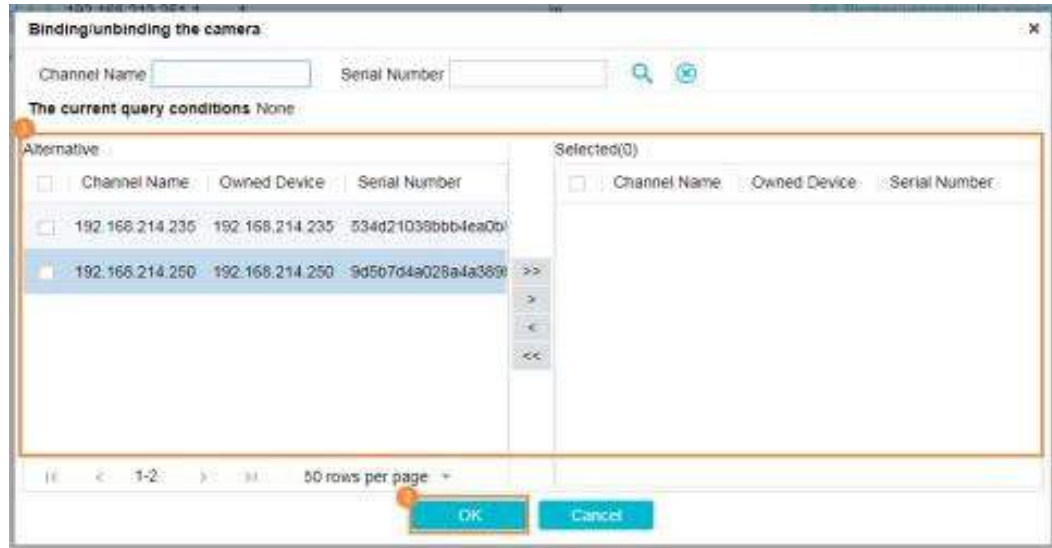
Procedure

Step 1 On the iClient S100 home page, choose **Access > Device > Reader**.

Step 2 On the page of selecting the reader, select the reader and set the corresponding reader as required.

- Step 3** In the **Operations** column of the corresponding reader, click **Binding/unbinding the camera**. The **Binding/unbinding the camera** dialog box is displayed, as shown in [Figure 6-20](#).

Figure 6-20 Binding a reader to a camera



- Step 4** Double-click the camera to be bound and click **OK**.

----End

6.2.4.3 Setting Valid Time Periods

In access control, valid time period is a basic concept. It is used to set the use time of a door and specify the available time of specified access control rules.

This section describes how to manually add valid time periods one by one on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Access > Access Control > Time Zones**.
- Step 2** Click **New**. The **New** dialog box is displayed.
- Step 3** In the **New** dialog box, set the parameters based on the site requirements, as shown in [Figure 6-21](#). [Table 6-10](#) describes the parameters.

Figure 6-21 Adding valid time periods

Date	Time	Interval 1		Interval 2		Interval 3	
		Start Time	End Time	Start Time	End Time	Start Time	End Time
Monday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Tuesday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Wednesday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Thursday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Friday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Saturday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Sunday		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Holiday Type 1		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Holiday Type 2		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00
Holiday Type 3		00 : 00	00 : 00	00 : 00	00 : 00	00 : 00	00 : 00

Copy Monday's Setting to Others Weekdays: ☐

Buttons: Save and New, OK, Cancel

Table 6-10 Parameters for adding valid time periods

Parameter	Description
Time Zone Name	Customized name of the valid time period.
Remark	Description of the time period.
Interval	Start time and end time of each time period. You can set time periods from Monday to Sunday and for three holidays.
Copy Monday's Setting to Others Weekdays	After this check box is selected, the settings of Monday are copied to other weekdays.

Step 4 Click **OK**.

----End

6.2.4.4 Setting Holidays

The access control time on holidays may be different from that on other days. To simplify operations, the system allows you to set the access control time on holidays separately.

This section describes how to manually add holidays on the iClient S100.

Procedure

Step 1 On the iClient S100 home page, choose **Access > Access Control > Holidays**.

- Step 2** Click **New**. The dialog box for adding holidays is displayed.
- Step 3** In the dialog box for adding holidays, set the parameters based on the site requirements, as shown in [Figure 6-22](#). For details about the parameter description, see [Table 6-11](#).

Figure 6-22 Adding holidays

Table 6-11 Parameters for adding holidays

Parameter	Description
Holiday Name	Customized name of the holiday.
Holiday Type	Type of a holiday. The options are Holiday Type 1 , Holiday Type 2 , and Holiday Type 3 . You can set holiday types under Time Zones > New .
Start/End Date	Time range of the holiday.
Recurring	Whether the holiday is cycled by year. The options are Yes and No . For holidays that are always on the same day like New Year's Day, you can set this parameter to Yes . For holidays that are not always on the same day like Mother's Day, set this parameter to No .
Remark	Description of the remarks.

- Step 4** Click **OK**.

----End

6.2.4.5 Configuring Linkage Policies

6.2.4.5.1 Application Scenario

You can configure different linkage policies in various scenarios as required. If a linkage policy is configured for a specific event, for example, door opening, alarming, or abnormal events, after the event is triggered at an input point in the access control system, the corresponding action is performed at the specified output point.

6.2.4.5.2 Prerequisites

You need to perform the following operations before adding a linkage policy.

- Step 1** Add access control devices, input points, and output points, and bind a reader to the camera.
- Step 2** (Optional) Set email parameters under **Basic Management > E-mail Management**.
1. On the iClient S100 home page, choose **Basic Management > Basic Management > E-mail Management**.
 2. Click **Email Parameter Settings**, then, the **Email Parameter Settings** dialog box is displayed.
 3. In the **Email Parameter Settings** dialog box, set related parameters, as shown in [Figure 6-23](#). [Table 6-12](#) describes the parameters.

Figure 6-23 Setting email parameters

Email Parameter Settings

1 Email Parameter Settings

Email Sending Server* (smtp.xxx.xxx)

Port* 25 ☐ SSL ☐ TLS

Email Account* (xxx@xxx.xxx)

Password*

Sender Name

2 Test Connection

3 OK Close

Table 6-12 Email parameters

Parameter	Description
Email Sending Server/Port	IP address and port number of a mail server. You can set these two parameters based on the IP address and port number of an SMTP-based server provided by a mailbox. For details about related configurations, contact for the mailbox provider, such as Netease (163 Mail), Tencent (QQ Mail), and Foxmail.
Email Account/Password	Email address and sign-in password.
Sender Name	Email sender name.

4. After the setting is complete, click **Test Connection**. If an email is received by the preconfigured email account, the setting is successful.
5. Click **OK**.

----End

6.2.4.5.3 Adding Linkage Policies

This section describes how to add linkage policies on the iClient S100.

Procedure

- Step 1** Choose **Access > Access Control > Linkage** on the iClient S100 home page.
- Step 2** On the **Linkage** page, click **New**. The **New** dialog box is displayed, as shown in [Figure 6-24](#).

Figure 6-24 New dialog box

Table 6-13 Linkage policy parameters

Parameter	Description
Linkage Name	Customized name of the linkage policy.
Device	Access control device.
Linkage Trigger Condition	Condition for triggering the linkage action, that is, action performed on the selected access control device.
Input Point	Input point of the device.
Output Point	Output point of the device.
Linkage action settings	In the lower part of the dialog box, you can set linkage actions, including output point operation, video linkage, and email linkage. Table 6-14 describes the configurations of these linkage actions.

Table 6-14 Linkage action parameters

Parameter	How to Set
Output Point	Set Action type to Close , Open , or Normally Open .
	If Action type is set to Open , you need to set Action time delay .
Video Linkage	Decide whether to select Capture . If snapshot is enabled, you need to set In the detection page immediately pop up and Display time .
E-mail	Set the email address for receiving the linkage information when a linkage event occurs.

Example:

- Set **Linkage Trigger Condition** to **Normal Verify Open**, **Input Point** to **192.168.214.167-1**, **Output Point** to **192.168.214.167-1**, **Action type** to **Open**, **Action time delay** to **60**, and select **Capture** under **Video Linkage**. For details, see [Figure 6-25](#).

Figure 6-25 Configuring linkage

The screenshot shows the 'New' dialog box for configuring linkage. The 'Linkage Name' is 'Test Linkage' and the 'Device' is '192.168.214.205'. The 'Linkage Trigger Conditions' are set to 'Normal Verify Open'. The 'Input Point' is set to '192.168.214.205-1'. The 'Output Point' tab is selected, showing a list of IP addresses: '192.168.214.205-1', '192.168.214.205-2', '192.168.214.205-3', and '192.168.214.205-4'. The 'Door' section shows a list of IP addresses: '192.168.214.205-1', '192.168.214.205-2', '192.168.214.205-3', and '192.168.214.205-4'. The 'Action type' is set to 'Open' and the 'Action time delay' is set to 60. The 'Auxiliary Output' section shows a list of IP addresses: '192.168.214.205-1', '192.168.214.205-2', '192.168.214.205-3', and '192.168.214.205-4'. The 'Save and New' button is highlighted.

- Effect: After someone opens the door 192.168.214.167-1 after successful verification, the door is opened and remains open for 60 seconds, and the system takes snapshots.

Step 3 Click **OK**.

----End

6.2.5 Setting Access Levels

Access levels are used to classify doors in the system to facilitate subsequent permission assignment.

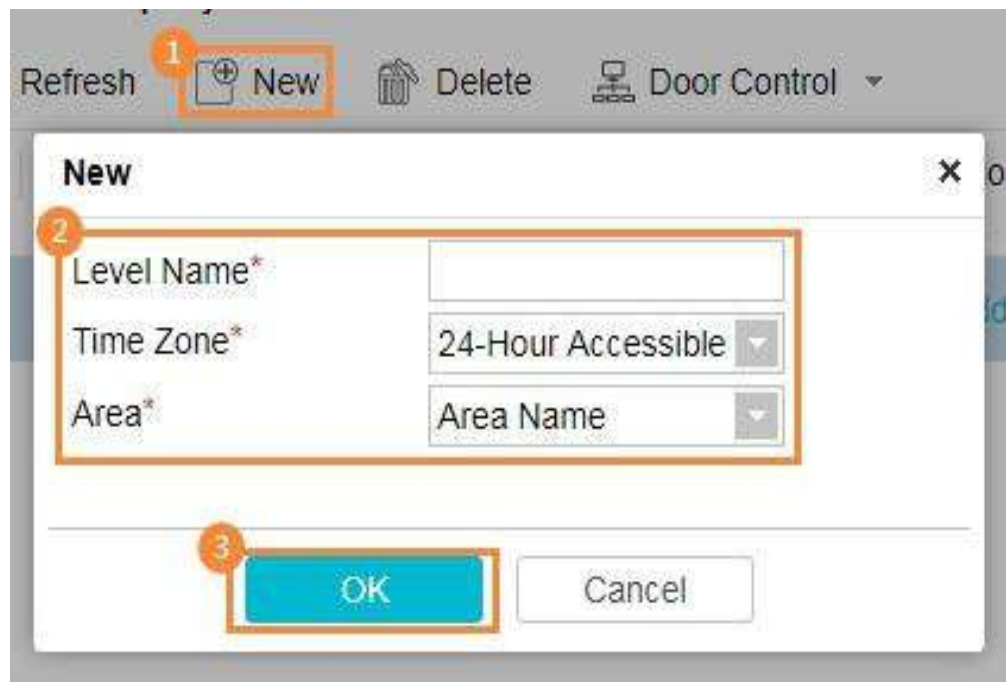
The settings include creating access levels and adding doors to the access levels.

6.2.5.1 Creating Access Levels

This section describes how to create and configure access levels on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Access > Access Control > Access Levels**.
- Step 2** Click **New** in the left pane. The **New** dialog box is displayed.
- Step 3** In the **New** dialog box, set the parameters for adding access levels, as shown in [Figure 6-26](#). [Table 6-15](#) describes the parameters.

Figure 6-26 Adding access levels**Table 6-15** Access level parameters

Parameter	Description
Level Name	Name of the access level.
Time Zone	Valid time period of the access level. Select a preconfigured access control time period from the drop-down list box.
Area	Area to which the access level belongs. Select an area preconfigured under Basic Management > Basic Management > Area Setting . For details about how to configure an area, see 8.2.1.4 How Can I Set Up an Area?

Step 4 Click **OK**.

----End

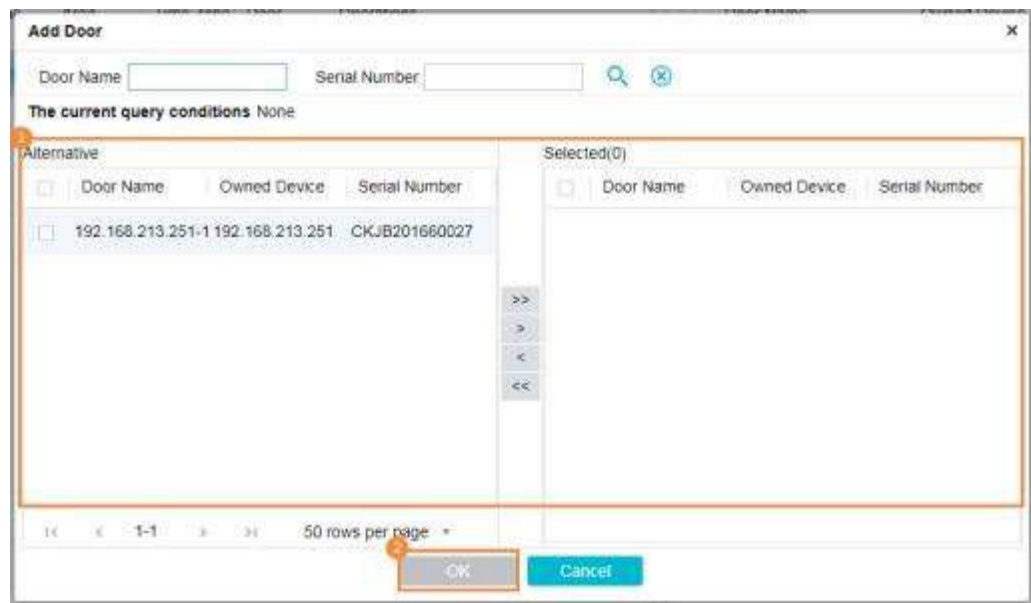
6.2.5.2 Adding Doors to Access Levels

This section describes how to add doors to access levels on the iClient S100.

Procedure

Step 1 On the iClient S100 home page, choose **Access > Access Control > Access Levels**.

Step 2 Click **Add Door**. In the **Add Door** dialog box that is displayed, add a door as required, as shown in [Figure 6-27](#).

Figure 6-27 Adding doors

Step 3 Click **OK**.

----End

6.2.6 Assigning Access Permissions

A person can open a door only after being granted the corresponding access permission from the administrator. You can assign the access permissions either by access level or by person.

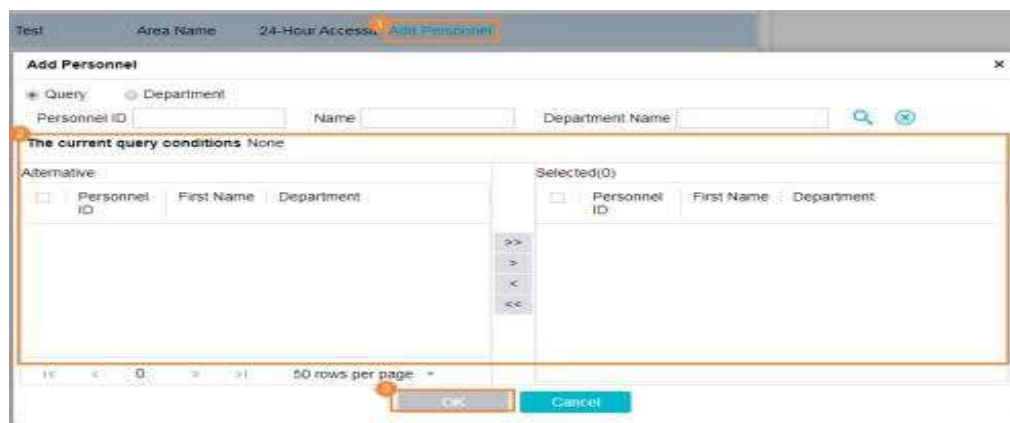
6.2.6.1 Assigning Access Permissions by Access Level

You can assign the access permission of an access level to a specific group of persons.

This section describes how to assign access permissions by access level on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Access > Access Control > Set Access by Levels**.
- Step 2** Click **Add Personnel** in the **Operations** column of the corresponding access level. In the displayed **Add Personnel** dialog box, select persons to which you want to assign the permission of the access level, as shown in [Figure 6-28](#).

Figure 6-28 Assigning access permissions by access level

Step 3 Click **OK**.

----End

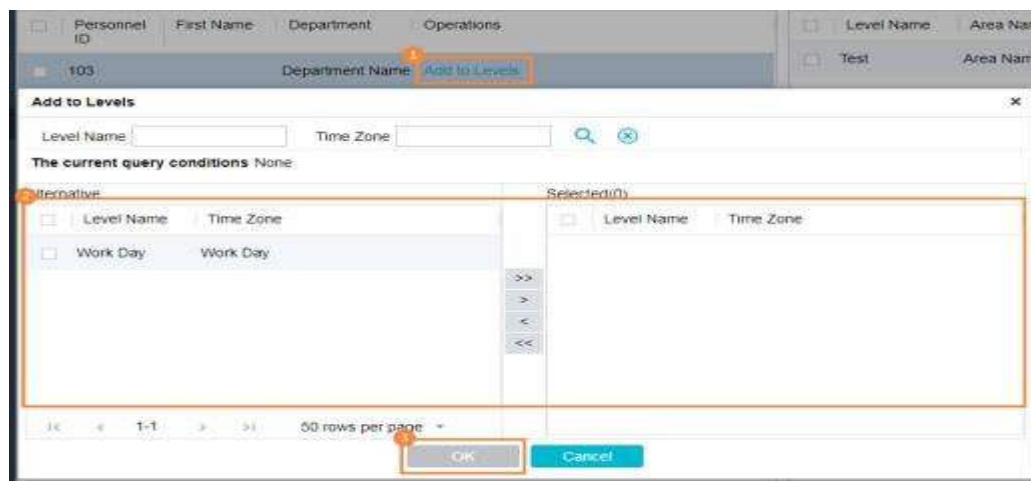
6.2.6.2 Assigning Access Permissions by Person

You can assign the access permissions of multiple access levels to a specific person.

This section describes how to assign access permissions by person on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Access > Access Control > Set Access by Person**.
- Step 2** Click **Add to Levels** in the **Operations** column of the corresponding person. In the displayed **Add to Levels** dialog box, select access levels whose access permissions you want to assign to the person, as shown in [Figure 6-29](#).

Figure 6-29 Assigning access permissions by person

Step 3 Click **OK**.

----End

6.2.7 Verification

On the real-time management page, check whether the added door is online and can be opened and closed properly and observe real-time events. If the door can be opened after a successful verification, and the corresponding linkage action is performed, the access control management service is configured successfully.

Procedure

Step 1 Check whether the added door is online.

1. Choose **detection** on the iClient S100 home page.
2. Check whether the added door is online according to the status icon. For details about the icons, see [Table 6-16](#).

Table 6-16 Door status icons

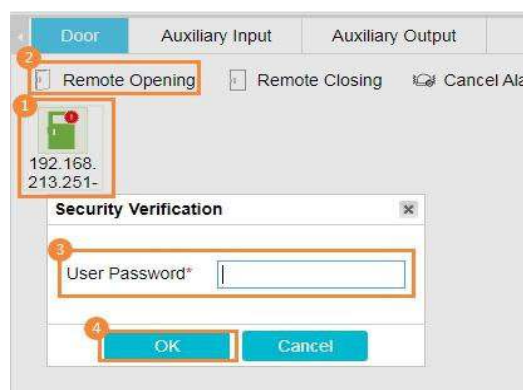
Icon	Status	Icon	Status
	Disabled		Offline
	Door status sensor unset, and relay turned off/no relay status		Door status sensor unset, and relay turned on/no relay status
	Door closed and relay turned off/no relay status in online mode		Door closed and relay turned on/no relay status in online mode
	Door opened and the relay turned off/no relay status in online mode		Door opened and relay turned on/no relay status in online mode
	Door opening alarm with the relay turned off		Door opening alarm with relay turned on
	Door opening timeout alarm with relay turned off/no relay status, and door status sensor turned on		Door opening timeout alarm with relay turned on/no relay status, and door status sensor turned on

Icon	Status	Icon	Status
	Door opening timeout alarm with relay turned off/door status sensor turned off		Door opening timeout alarm with relay turned on/door status sensor turned off
	Door closing alarm with relay turned off/no relay status		Door closing alarm with relay turned on/no relay status
	Door status sensor unset with door alarms and relay turned off		Door status sensor unset with door alarms and relay turned on
	Door opening timeout alarm with no relay status/door status sensor turned off		Door locked
Note: If there is no relay status, the current firmware does not support the relay status detection function.			

Step 2 Verify remote door opening and closing. The following uses remote door opening as an example.

1. Choose **detection** on the iClient S100 home page.
2. Select an online door and click **Remote Opening**. In the displayed **Security Verification** dialog box, enter the user password and click **OK**, as shown in [Figure 6-30](#).

Figure 6-30 Remote door opening



3. On the **Remote Opening** page, enter the time to open the door and click **OK**.
4. If the message "Operation Successful" is displayed, the setting is successful and the door will be opened at the specified time.

Step 3 Verify access permissions.

1. Choose **detection** on the iClient S100 home page.
2. Verify access permissions of an added door.
3. On the **detection** page, check whether the access permission is correctly assigned to a person based on the displayed real-time events. If the person assigned with the access permission opens the door, and **Normal Verify Open** is displayed in the **Event Description** column of the corresponding event, the access permission service is configured successfully, as shown in [Figure 6-31](#).

Figure 6-31 Real-time event

Time	Area	Device	Event Point	Event Description	Card Number	Person	Reader Name	Verification Mode
2023-10-16 09:57:21	168	192	192	Normal Verify Open	101	192	192	192

Total Received: 1 Normal: 1 Exception: 0 Alarm: 0 Clear Data Rows Event Description

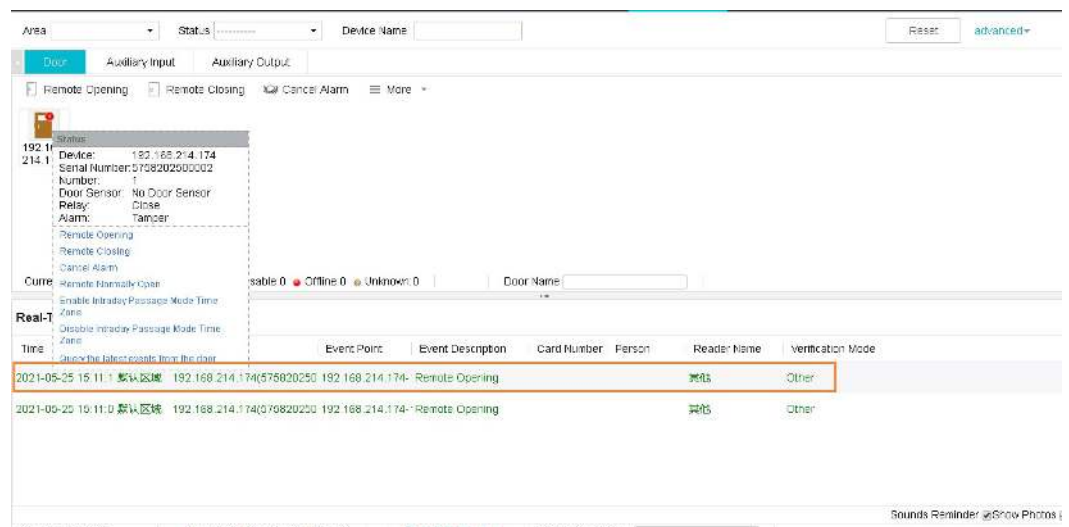
Step 4 Verify the linkage policies.

1. Choose **detection** on the iClient S100 home page.
2. Verify the linkage policies at the input point that has been configured as a linkage device.
3. On the **detection** page, check whether the corresponding linkage event and linkage action are displayed. If so, the linkage policy is configured successfully, as shown in [Figure 6-32](#).

Example:

- Set **Linkage Trigger Condition** to **Remote Opening**, **Input Point** to **Door 2**, **Output Point** to **Door Lock 1**, **Action type** to **Open** and **Action time delay** to **60**.
- Effect: After someone remotely opens door 1, door 1 opens and remains open for 60 seconds.

Figure 6-32 Linkage results



----End

6.3 Configuring Electronic Maps

6.3.1 Adding Maps

This section describes how to configure electronic maps on the iClient S100.

Application Scenario

You can upload a local map image to the iClient S100 to serve as the electronic map. After you add icons of doors and cameras to the corresponding positions, the system automatically reads the related settings and position parameters.

The electronic map clearly displays detection points, events, and alarms, and provides a unified entry for you to learn about the overall situation, remotely open and close doors, clear alarms, and view live video. As a result, you can obtain real-time and effective data to work more efficiently.

Prerequisites

1. Access control devices and cameras have been added on the **Device** tab page under **Access**.
2. You have obtained the electronic map file to be added and saved it to the local server.

NOTE

- The maps can be in .jpe, .jpg, .jpeg, .gif, .png, .bmp, .ico, .svg, .svgz, .tif, .tiff, .ai, .drw, .pct, .psp, .xcf, .psd, .raw, or .webp format.
- The resolution of a map image is no more than 1120 x 380 pixels.

Procedure

- Step 1** Choose **Complex Applications > Map** on the iClient S100 home page.
- Step 2** Click **New**.
- Step 3** In the **New** dialog box, set related parameters, as shown in [Figure 6-33](#). [Table 6-17](#) describes the parameters and icon.

Figure 6-33 Adding a map

Edit [X]

Map Name*

Area Name* [v] [+]

Map Path* Not Uploaded

⚠ Please upload pictures with suffixes of jpg, png, gif, bmp, and the size is between 0 and 10MB!

Table 6-17 Map adding parameters and icon

Parameter/Icon	Description
Map Name	Customized name of the map.
Area Name	Name of the area that the map shows. Select an area preconfigured under Basic Management > Basic Management > Area Setting . For details about how to configure an area, see 8.2.1.4 How Can I Set Up an Area? . Only one map can be uploaded for an area. Areas for which maps have been uploaded cannot be selected.
Map Path	Path storing the map to be added. Select a map from the local server.
	Icon for quickly adding an area on the current page.

- Step 4** Click **OK**.
- End

6.3.2 Adding Devices

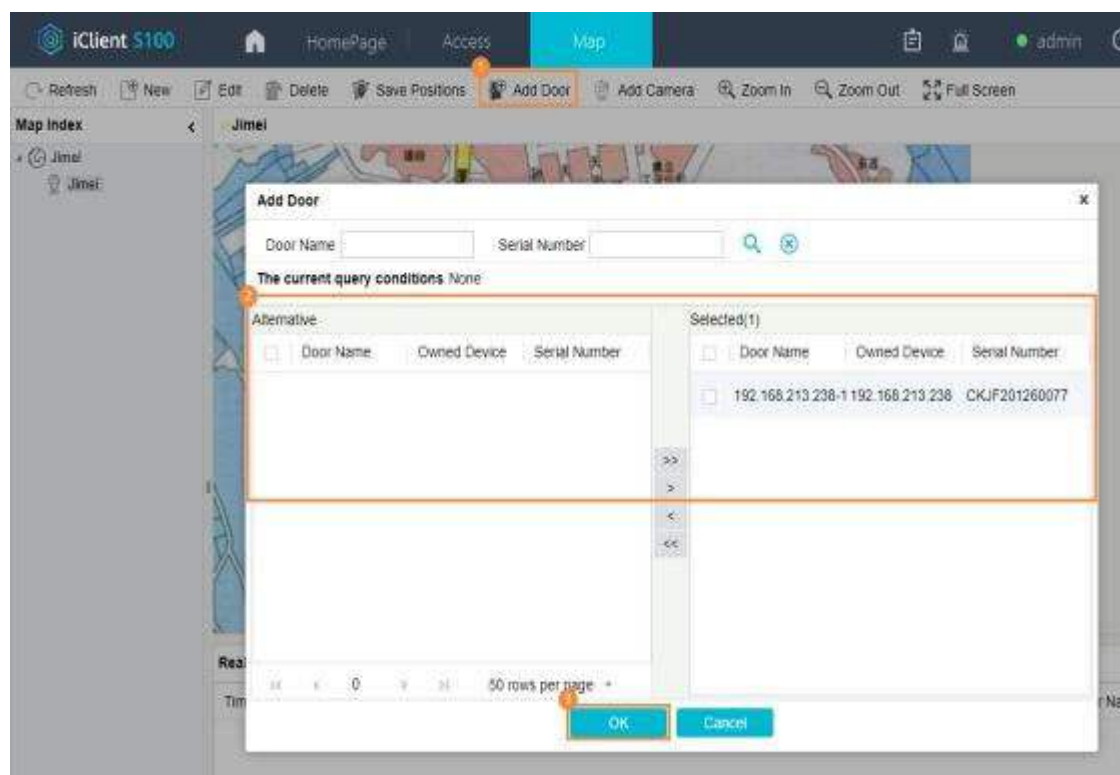
This section describes how to add devices to the electronic map on the iClient S100.

Devices include doors and cameras, and the procedures for adding these two types of devices are the same. The following describes how to add doors.

Procedure

- Step 1** Choose **Complex Applications > Map** on the iClient S100 home page.
- Step 2** Click an added electronic map in the left pane and click **Add Door**. The **Add Door** dialog box is displayed.
- Step 3** In the **Add Door** dialog box, select doors to be observed, as shown in [Figure 6-34](#).

Figure 6-34 Selecting doors



- Step 4** Click **OK**. The doors are added to the map and displayed in the upper left corner of the map.
- Step 5** Drag the door icons to the corresponding positions.
- Step 6** Click **Save Location** in the operation column.

----End

6.3.3 Verification

On the **Map** page, if the added electronic map and icons of the added doors and cameras are displayed and you can remotely open and close doors, view live video, and check events in real time, the electronic map is configured successfully.

Procedure

Step 1 Verify the function of adding electronic maps.

1. Choose **Complex Applications > Map** on the iClient S100 home page.
2. Click a map in the map list and check whether the map is displayed properly.

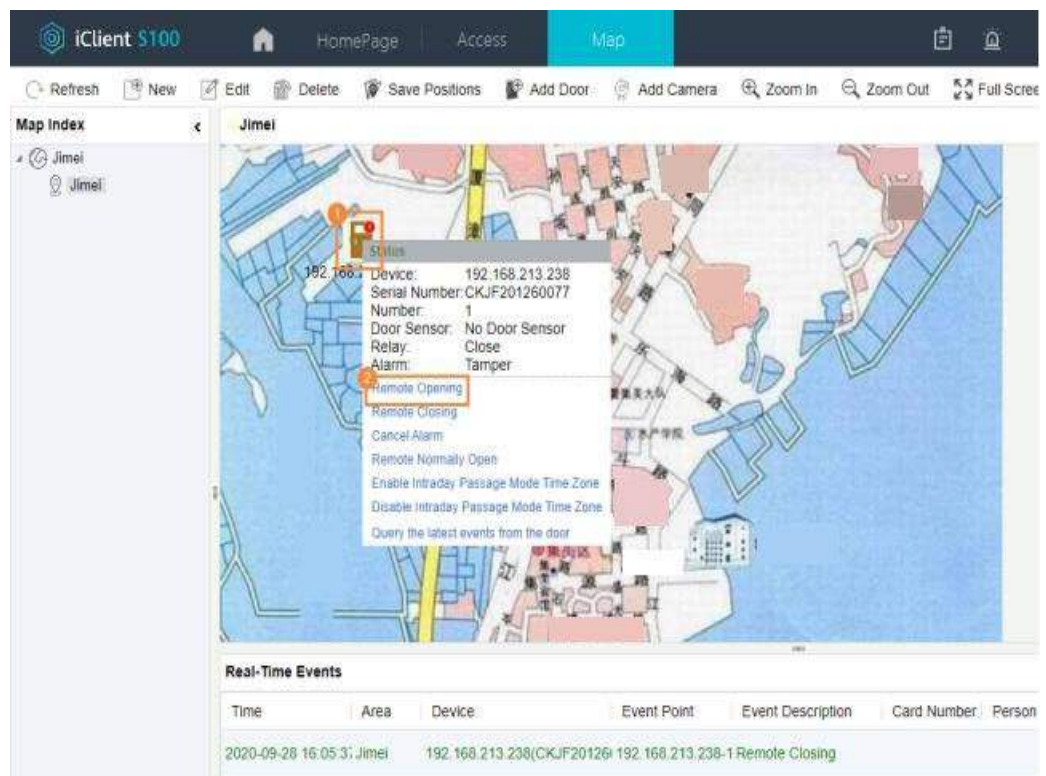
Step 2 Verify that the device position is configured successfully.

1. Choose **Complex Applications > Map** on the iClient S100 home page.
2. Click a map in the map list and check whether all icons on the map are displayed properly.

Step 3 Verify that doors have been configured. The following uses remote door opening as an example.

1. Choose **Complex Applications > Map** on the iClient S100 home page.
2. Right-click an online door device and click **Remote Opening**, as shown in [Figure 6-35](#).

Figure 6-35 Remote door opening



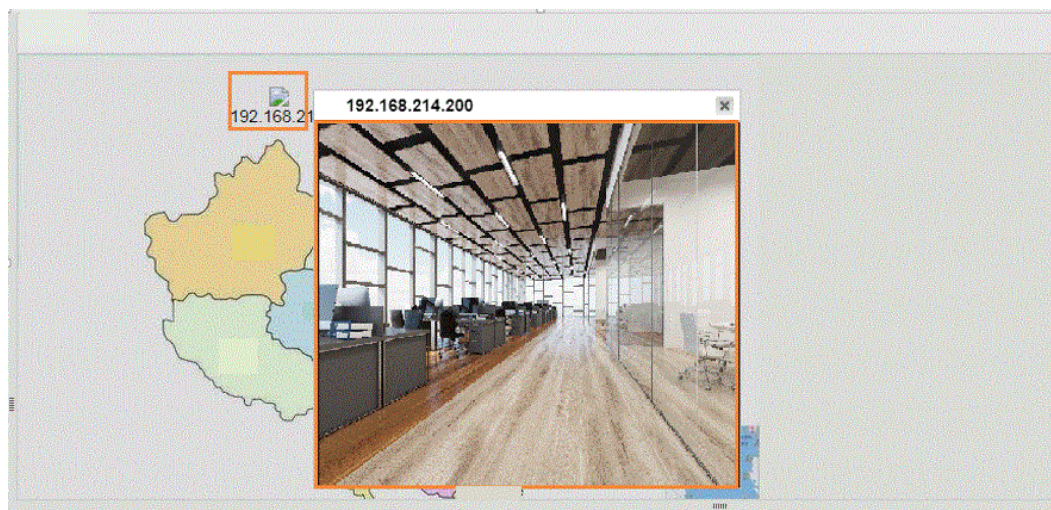
3. In the security verification dialog box that is displayed, enter the user password and click **OK**.

4. On the **Remote Opening** page, enter the time to open the door and click **OK**.
5. If the message "Operation Successful" is displayed, the setting is successful and the door will be opened at the specified time.

Step 4 Verify the camera configuration.

1. Choose **Complex Applications** > **Map** on the iClient S100 home page.
2. Double-click an online camera. The live video from the camera is displayed, as shown in [Figure 6-36](#).

Figure 6-36 Live video viewing



3. If the live video from the camera is displayed properly, the camera is configured successfully.

 NOTE

- Currently, a maximum of four live video viewing channels are supported.
- If the camera support PTZ controls, you can perform PTZ controls in the live video pane.

Step 5 Verify the electronic map access observation function.

1. Choose **Complex Applications > Map** on the iClient S100 home page.
2. Click a map in the map list and arrange a person to verify on the access control device.
3. If an event is displayed in the **Real-Time Event** area, the electronic map observation function is configured successfully, as shown in [Figure 6-37](#).

Figure 6-37 Real-time event

Real-Time Events										Message Tip						
Time	Area	Device	Event Point	Event Description	Card Number	Person	Reader Name	Verification Mode								
2020-10-16 12:30:11	Area Name	102	363	213	1996	CJR20126-100	363	213	1996-1	Normal Verify Open	101	192	363	213	1996-1	Only Pin
2020-10-16 14:10:41	Area Name	192	363	213	1996	CJR20126-165	363	213	1996-1	Normal Verify Open	101	192	363	213	1996-1	Only Pin
Total Received: 2										Normal: 2	Exception: 0	Alarm: 0	Clear Data Item			
																
										101						
										Normal Verify Open						
										2020-10-16 12:00:12						

Step 6 Verify the person trajectory search function.

1. Choose **Complex Applications** > **Map** on the iClient S100 home page.
2. Arrange a person to verify the recognition and snapshot functions of the added camera.
3. Click **Personnel trends**. The page for setting person trajectory search is displayed.
4. Set search criteria, upload a person image, and click **Search**, as shown in [Figure 6-38](#).

Figure 6-38 Personnel trends

5. Click **OK**. The system automatically returns to the **Map** page.
6. Wait until the person trajectories are displayed on the electronic map, as shown in [Figure 6-39](#).

Figure 6-39 Person trajectories



Step 7 Verify the multi-layer hotspot function.

1. Choose **Complex Applications** > **Map** on the iClient S100 home page.
2. (Optional) If the map tree on the left contains multi-layer maps, move the hotspot icon (which is automatically generated on the map of the upper-level area in this case) of the lower-level area to the corresponding position on the map. [Figure 6-40](#) shows the effect of multi-layer hotspots.

Figure 6-40 Effect of multi-layer hotspots

3. Double-click the hotspot icon to go to the map of the lower-level area.
4. Click **Upper map** to go to the map of the upper-level area.

----End

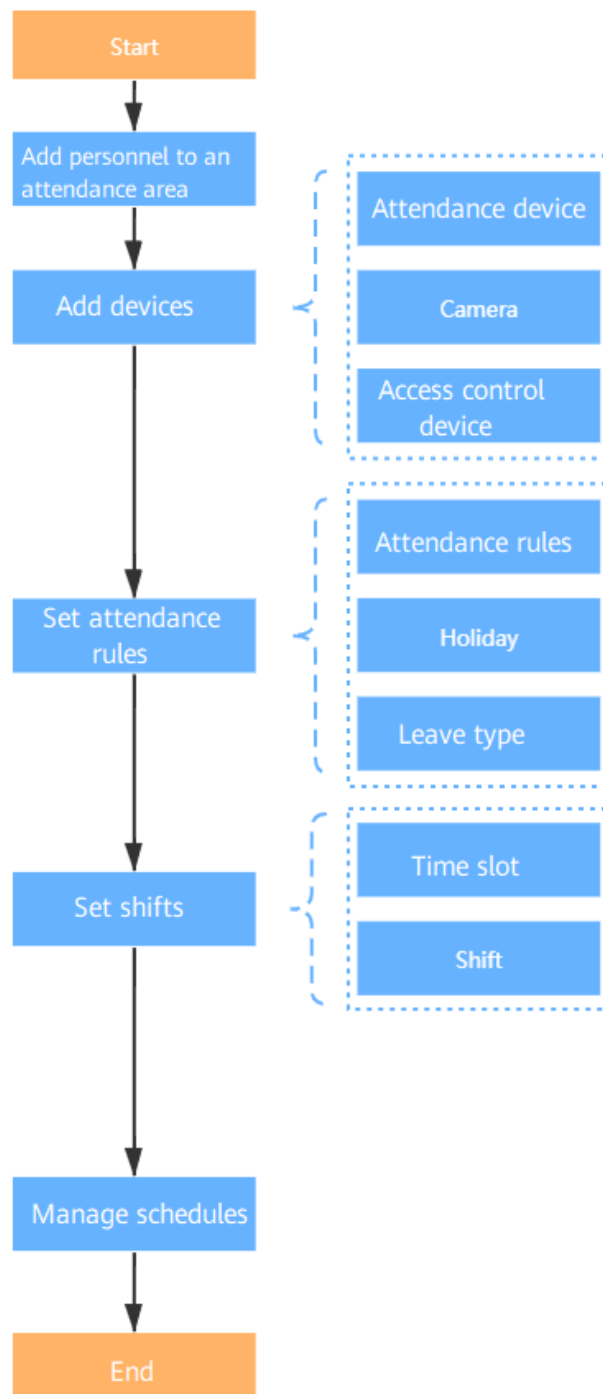
6.4 Attendance Management Service Configuration

6.4.1 Application Scenario

Attendance, also known as time management, helps enterprises to effectively collect personnel attendance data, input attendance exception data, and calculate attendance results used as the basis for payroll.

6.4.2 Configuration Process

This section describes the configuration process of attendance management, as shown in [Figure 6-41](#).

Figure 6-41 Configuration process

6.4.3 Adding Personnel to an Attendance Area

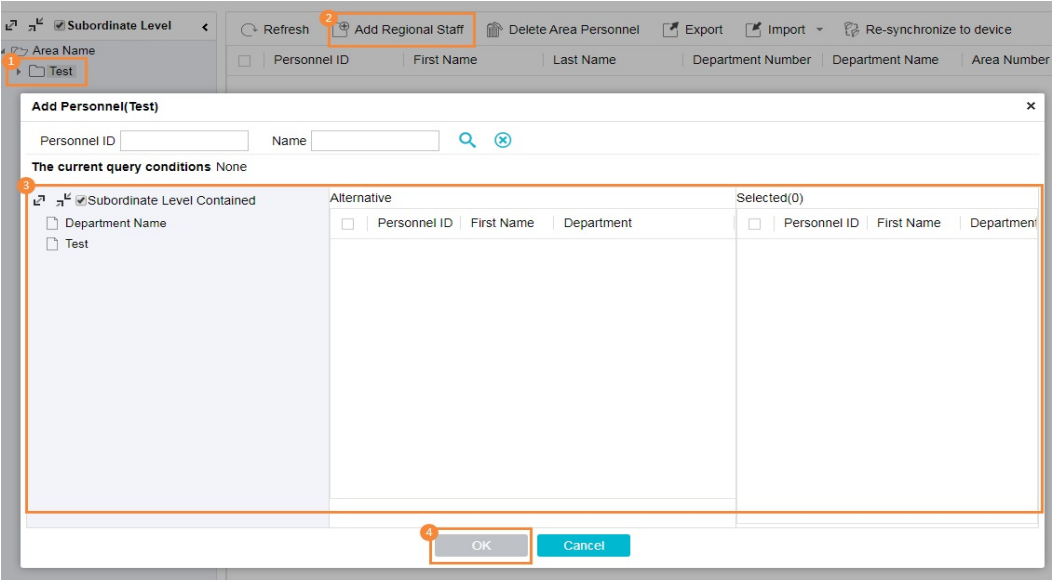
You need to add personnel to an attendance area so that personnel attendance data can be collected.

This section describes how to manually add personnel to an attendance area on the iClient S100.

Procedure

- Step 1** Choose **Attendance > Attendance Device > By Region** on the iClient S100 home page.
- Step 2** Select a required area and click **Add Regional Staff**. The **Add Personnel** dialog box is displayed.
- Step 3** Select personnel as required, as shown in **Figure 6-42**.

Figure 6-42 Add Personnel



- Step 4** Click **OK**.
- End

6.4.4 Adding Devices

6.4.4.1 Attendance Device Description

Attendance devices, cameras, and access control devices can generate attendance data. For details about the application scenarios of the preceding three types of devices, see **Table 6-18**.

 NOTE

The three devices can be used separately or together.

Table 6-18 Attendance Device Description

Attendance Device	Application Scenario
Attendance device	Users have purchased dedicated attendance devices for daily attendance. For details about how to configure an attendance device, see 6.4.4.2 Using an Attendance Device as the Attendance Data Source .
Camera	Users attempt to use cameras instead of attendance devices to implement seamless attendance. The iClient S100 can use installed cameras as the attendance data source. After a person is recognized by a camera, the attendance system obtains the recognition record and automatically takes the record as an attendance record. For details about how to configure a camera, see 6.4.4.3 Using a Camera as the Attendance Data Source.
Access control device	Users attempt to use access control devices instead of attendance devices to implement attendance. The iClient S100 can use the installed access control device as the attendance data source. After a person is recognized by an access control device, the attendance system obtains the recognition record and automatically takes the record as an attendance record. For details about how to configure an access control device, see 6.4.4.4 Using an Access Control Device as the Attendance Data Source.

6.4.4.2 Using an Attendance Device as the Attendance Data Source

6.4.4.2.1 Prerequisites

1. You have performed operations described in [8.2.3.1 How Can I Set or Change the IP Address of an Access Control Device Using a Tool?](#) to assign an IP address to the attendance device to be added.
2. You have performed the following steps to configure the IP address and port number of the iClient S100 server before adding the attendance device:
 - a. Log in to the attendance device with power supply and network connected and go to the configuration page.
 - b. Perform cloud server configuration under communication configuration.
 - c. On the server connection setting page, enter the IP address and port number of the iClient S100 server for connection between the device and the iClient S100.

6.4.4.2.2 Automatically Adding an Attendance Device

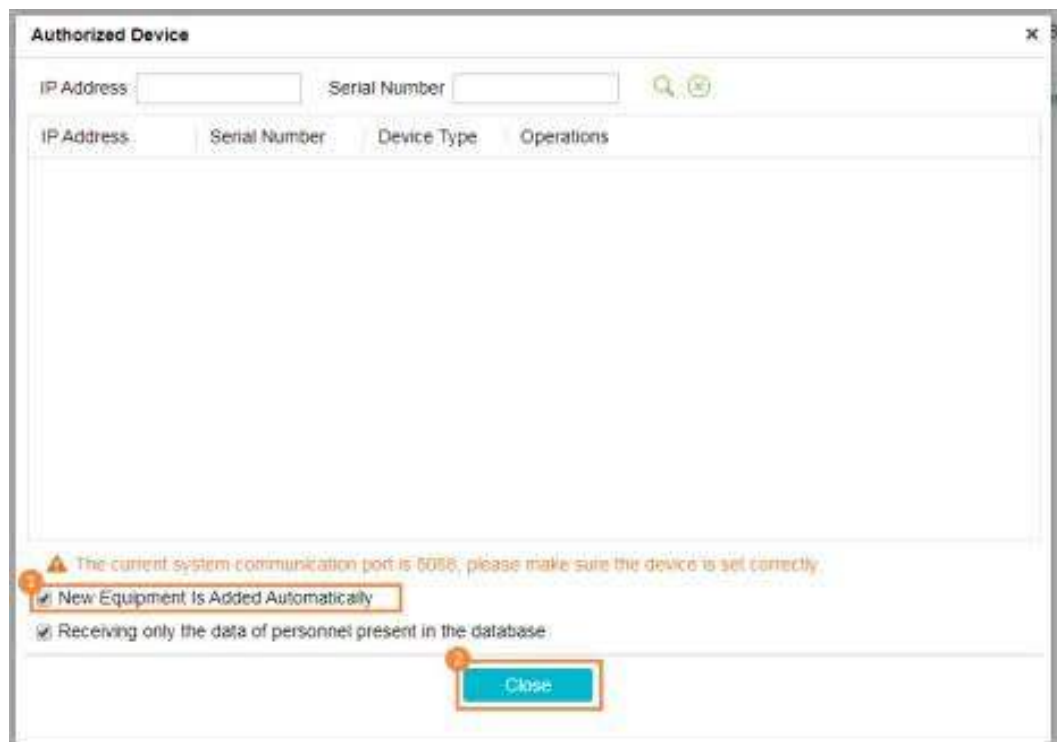
This section describes how to automatically add an attendance device on the iClient S100.

You can directly add the attendance device for which the IP address and port number of the iClient S100 have been configured, which is quick and convenient.

Procedure

- Step 1** Choose **Attendance > Attendance Device > Device** on the iClient S100 home page.
- Step 2** Click **Authorized Device**. The **Authorized Device** page is displayed.
- Step 3** Select **New equipment is Added Automatically**, as shown in [Figure 6-43](#).

Figure 6-43 Authorized Device



- Step 4** Click **Close**.
- Step 5** Wait until the attendance device for which the IP address and port number of the iClient S100 have been configured is automatically added.

----End

6.4.4.2.3 Adding an Attendance Device by Authorization

This section describes how to add an attendance device by authorization on the iClient S100.

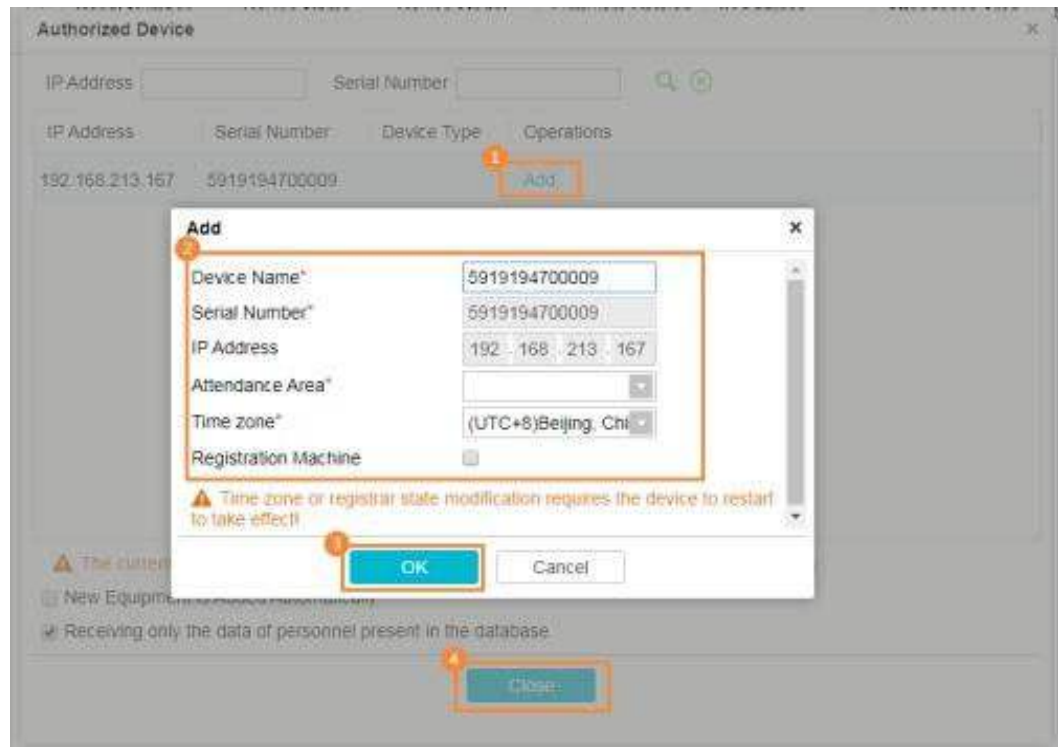
When the **New Equipment Is Added Automatically** parameter is deselected, you can add an attendance device by authorization.

Procedure

- Step 1** Choose **Attendance > Attendance Device > Device** on the iClient S100 home page.

- Step 2** On the **Device** page that is displayed, click **Authorized Device**. The attendance devices for which the IP address and port number of the iClient S100 have been configured are displayed on the **Authorized Device** page. Click **Add** for a required device.
- Step 3** Set parameters as required, as shown in [Figure 6-44](#).

Figure 6-44 Device adding page



- Step 4** Click **OK**.
- Step 5** Click **Close** after all required attendance devices are added by authorization.
- End

6.4.4.3 Using a Camera as the Attendance Data Source

This section describes how to use a camera as the attendance data source on the iClient S100.

Prerequisites

- You have performed the following operations to add required information on the **Personnel Management** page:
 - Add personnel information. Normal and available target images must be uploaded for personnel. For details, see [6.1.4 Adding Persons](#).
 - Add other relevant information.
- You have performed the following operations to configure required information on the **Video Device** page:
 - Use a camera as the attendance data source. The camera requirements are as follows:

- The camera connected to the IVS1800 must support target recognition and has been configured with functions related to target recognition. Alternatively, the camera needs to be connected to the IVS1800 that is loaded with target recognition algorithms.
 - The camera connected to the NVR800 must support target recognition and has been configured with functions related to target recognition.
- b. Add the camera to the NVR800 or IVS1800. For details, see [4.1 Device Access](#) or [5.1 Device Access](#).
 - c. Add personnel to corresponding lists and synchronize the lists to the NVR800 or IVS1800. For details, see [4.7.4 Target List Management](#).
 - d. Configure target alert tasks. You need to set the alarm type to the listed target detection alarm for the target alert tasks configured on the IVS1800. For details, see [4.7.9 Target Recognition Attendance](#) or [5.7.2.5 Target Recognition Attendance](#).

Procedure

- Step 1** Choose **Attendance > Attendance Device > Attendance Point** on the iClient S100 home page.
- Step 2** Click **New**. The page for adding an attendance site is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-45](#). [Table 6-19](#) describes the parameters.

Figure 6-45 Page for adding a camera as an attendance site

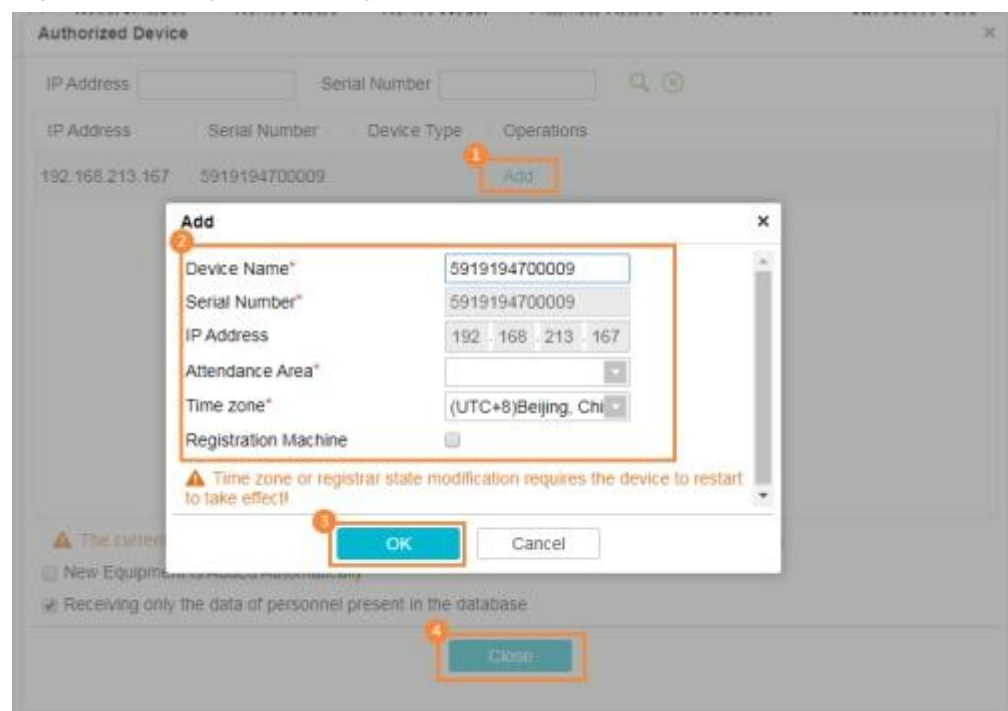


Table 6-19 Attendance site parameters

Parameter	Description
Attendance Point Name	Attendance site name.
Device Module	Type of the attendance data source. The type can be access control or video. If the type is video, the device list will display cameras.
Area Name	Name of the area configured under Basic Management > Basic Management > Area Settings . For details about how to configure an area, see 8.2.1.4 How Can I Set Up an Area? .
Camera List	List of cameras that belong to the area configured under Basic Management > Basic Management > Area Settings . Select a camera that can be used as the attendance data source.

Step 4 Click **OK**.

Step 5 Wait until the camera is successfully added as the attendance data source. Then the records that are successfully verified and recognized by the camera will automatically become the attendance records in the attendance system.

----End

6.4.4.4 Using an Access Control Device as the Attendance Data Source

This section describes how to use an access control device as the attendance data source on the iClient S100.

Prerequisites

- You have performed the following operations to add required information on the **Personnel Management** page:
 - a. Add personnel information. You need to configure personnel data that supports device verification, such as card number, target image, and fingerprint. For details, see [6.1.4 Adding Persons](#).
 - b. Add other relevant information.
- You have performed the following operations to configure required information on the **Access** page:
 - a. Add access control devices. For details about how to add access control devices, see [6.2.3 Adding Devices](#).
 - b. Assign access permission groups to personnel. For details about how to configure access permission groups, see [6.2.6 Assigning Access Permissions](#).

Procedure

- Step 1** Choose **Attendance > Attendance Device > Attendance Point** on the iClient S100 home page.
- Step 2** Click **New**. The page for adding an attendance site is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-46](#). [Table 6-20](#) describes the parameters.

Figure 6-46 Page for adding an access control device as the attendance site

Table 6-20 Attendance site parameters

Parameter	Description
Attendance Point Name	Attendance site name.
Device Module	Type of the attendance data source. The type can be access control or video. If the type is access control, the device list will display access control devices.
Area Name	Name of the area configured under Basic Management> Basic Management> Area Settings . For details about how to configure an area, see 8.2.1.4 How Can I Set Up an Area? .
Door List	List of access control devices that belong to the area configured under Basic Management> Basic Management> Area Settings . Select an access control device that can be used as the attendance data source.

- Step 4** Click **OK**.
- Step 5** Wait until the access control device is successfully added as the attendance data source. Then the records that are successfully verified and recognized by the access control device will automatically become the attendance records in the attendance system.

----End

6.4.5 Attendance Setting

Attendance setting affects attendance results and functions as the core of the attendance calculation logic. The setting includes the setting of the attendance rules, holiday, and leave type.

6.4.5.1 Setting the Attendance Rules

Attendance rules refer to attendance parameters which are used to demonstrate a company's attendance system. The attendance parameters function as system global variables and their settings can ensure the accuracy of the final attendance data calculation.

This section describes how to configure the attendance rule on the iClient S100.

Procedure

- Step 1** Choose **Attendance > Attendance Setting > Attendance Rules** on the iClient S100 home page.
- Step 2** On the page that is displayed, set attendance rules, as shown in [Figure 6-47](#). [Table 6-21](#) describes the parameters for setting basic rules. [Table 6-22](#) describes the parameters for setting non-leave calculation. [Table 6-23](#) describes the parameter for setting frequency of obtaining attendance records from the attendance site.

Figure 6-47 Page for setting attendance rules

1Basic Rule Setting

Check-In RuleThe Earliest Rule

The minimum time period should be greater than (minimum 10 minutes)120

Check-Out RuleThe Latest Rule

The maximum time period should be less than (maximum 1,440 minutes)600

Attendance calculation result for cross-day shiftFirst Day

Overtime StatisticsYes

Late and Early Leave Counted as AbsentNo

Single shortest overtime (minutes)5

Exact digits of the decimal point1

Missing Check-In count asAbsent0 Minutes

Missing Check-Out count asAbsent0 Minutes

2Non-leave calculation setting

Expected/Actual

Early

Late

No Check-Out

No Check-In

Overtime

Minimum unit*1minute

Rounding Control*Up (carry)

Report display symbol*√

3Time attendance point obtains record frequency regularly

frequency10 seconds/time

4OK

Table 6-21 Parameters for setting basic rules

Parameter	Description
Clock-In Rule/Clock-Out Rule	Attendance rule. The options are The Earliest Rule , The Latest Rule , and The Proximity Rule .
Attendance calculation result for cross-day shift	Day to which the cross-day shift belongs. The options are First Day and Second Day .
Late and Early Leave Counted as Absent	Rule for determining whether the late and early leave are regarded as absenteeism.
Missing Check-In count as	Rule for setting the text displayed in the report for missing check-in and clock-out. The options are Absent , Late , and Incomplete . If this parameter is set to Late , the number of late minutes is mandatory.
The minimum time period should be greater than (minimum 10 minutes)	Minimum valid attendance duration.
The maximum time period should be less than (maximum 1,440 minutes)	Maximum valid attendance duration.
Overtime Statistics	Rule for determining whether to calculate overtime data into attendance.
Single shortest overtime (minutes)	Minimum overtime duration per time.
Exact digits of the decimal point	Number of decimal places for attendance calculation. The options are 1 and 2 .

Table 6-22 Parameters for setting non-leave calculation

Parameter	Description
Status	Attendance status.
Minimum unit	Minimum unit of the current attendance state. The options are minute , hour(s) , and Work day .
Rounding Control	Rounding control method for the time segment that is not equal to the unit. The options are Up (carry) , Down (discard) , and rounding .
Report display symbol	Symbol of the current attendance status displayed in the report.

Table 6-23 Parameter for setting the record obtaining frequency

Parameter	Description
frequency	Frequency of obtaining attendance records from the configured attendance site. The options are 10 seconds/time , 20 seconds/time , 30 seconds/time , 1 minute/time , 2 minute/time , 3 minute/time , 4 minute/time , 5 minute/time , and 8 minute/time .

Step 3 Click **OK**.

----End

6.4.5.2 Adding a Holiday

This section describes how to manually add a holiday on the iClient S100.

Procedure

- Step 1** Choose **Attendance > Attendance Setting > Holiday** on the iClient S100 home page.
- Step 2** Click **New**. The page for adding a holiday is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-48](#). [Table 6-24](#) describes the parameters.

Figure 6-48 Page for adding a holiday

The screenshot shows a 'New' dialog box with a close button (X) in the top right corner. The dialog contains four input fields: 'Name*' (empty), 'Start Time*' (2020-10-16), 'Number of Days*' (empty), and 'Remark' (empty). A red box labeled '1' highlights the input fields. At the bottom, there are three buttons: 'Save and New' (blue), 'OK' (blue), and 'Cancel' (gray). A red box labeled '2' highlights the 'OK' button.

Table 6-24 Parameters for adding a holiday

Parameter	Description
Name	User-defined holiday name.
Start Time	Start time of a holiday.
Number of Days	Number of days in a holiday.
Remarks	Description of the remarks.

Step 4 Click **OK**.

----End

6.4.5.3 Adding a Leave Type

This section describes how to add a leave type on the iClient S100.

Procedure

- Step 1** Choose **Attendance > Attendance Setting > Leave Type** on the iClient S100 home page.
- Step 2** Click **New**. The page for adding a leave type is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-49](#). [Table 6-25](#) describes the parameters.

Figure 6-49 Page for adding a leave type

New [X]

1

Name* [Text Box]

Whether to subtract work hours* [Yes ▼]

Minimum unit* [Text Box] [minute ▼]

Rounding Control* [Down (discard) ▼]

Report display symbol* [Text Box]

2

[Save and New] [OK] [Cancel]

Table 6-25 Parameters for adding a leave type

Parameter	Description
Name	User-defined name of the leave type.
Whether to subtract work hours	Indicates whether to deduct the leave duration from the work time.
Minimum unit	Minimum unit of the current leave state. The options are minute , hour(s) , and Work day .
Rounding Control	Rounding control method for the time segment that is not equal to the unit. The options are Up (carry) , Down (discard) , and rounding .
Report display symbol	Symbol of the current leave status displayed in the report.

Step 4 Click **OK**.

----End

6.4.6 Regular Shift Setting

You can add a regular shift that consists of one or more normal time slots that are added. The regular shift is usually used in scenarios that feature regular work, such as companies, governments, and banks.

6.4.6.1 Add a Normal Time Slot

This section describes how to add a normal time slot for regular shift on the iClient S100.

Procedure

- Step 1** Choose **Attendance > Schedule > Timetable** on the iClient S100 home page.
- Step 2** Click **Add normal time slot**. The page for adding a normal time slot is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-50](#). [Table 6-26](#) describes the parameters.

Figure 6-50 Page for adding a normal time slot

New

Name*

Check-In Time* 09 : 00 (HH.MM) Check-Out Time* 18 : 00 (HH.MM)

Before going to work* 60 Check-in is valid within minutes Before going off duty* 60 Check-in is valid within minutes

After work* 60 Check-in is valid within minutes After work* 60 Check-in is valid within minutes

Allow Late(minutes) 0 Allow Early Leave(minutes) 0

Must Check-In* Yes Must Check-Out* Yes

Auto Deduct Break Time* No Work Time (minutes)* 540

☐ On duty 0 Sign in minutes ago for overtime , Minimum overtime minutes 30 , Limit the maximum overtime hours 0

☐ Off duty 0 Start counting overtime minutes later , Minimum overtime minutes 30 , Limit the maximum overtime hours 0

Save and New OK Cancel

Table 6-26 Parameters for adding a normal time slot

Parameter	Description
Name	User-defined name of a time slot.
Check-In Time/Check-Out Time	Work time.
Before going to work/ After work Before going off/After work	Check-in and check-out time range.
Allow Late(minutes)/ Allow Early Leave(minutes)	Allowed time range for late arrival and early leave.
Must Check-In/Must Check-Out	Indicates whether check-in or check-out is mandatory.

Parameter	Description
Auto Deduct Break Time	Indicates whether to deduct the rest duration from the work time. If this parameter is set to Yes , the start time and end time of the rest duration are required.
Work Time	Work time, which is automatically calculated based on the above settings.

Step 4 Click **OK**.

----End

6.4.6.2 Adding a Regular Shift

Procedure

Step 1 Add a regular shift.

1. Choose **Attendance > Schedule > Shift** on the iClient S100 home page.
2. Click **Add Regular Shift**. The page for adding a regular shift is displayed.
3. Set parameters as required, as shown in [Figure 6-51](#). [Table 6-27](#) describes the parameters.

Figure 6-51 Page for adding a regular shift

The screenshot shows a 'New' dialog box with the following fields and values:

- Schedule Type:** (empty)
- Name:** (empty)
- Unit:** Day
- Period start type:** Period start date
- Period start date:** (empty)
- Cycle Start Date:** 2020-10-16
- Number:** (empty)
- Cycle(1-99):** (empty)
- Cycle Shift in one Month:** Yes
- Schedule Name:** (empty)
- Work Type:** Normal Work
- Attendance Mode:** (empty)
- Punch Card According to:** (empty)
- Overtime Mode:** Computer Automatic

At the bottom, there are three buttons: 'Save and New', 'OK' (highlighted with a red box), and 'Cancel'.

Table 6-27 Parameters for adding a regular shift

Parameter	Description
Name/Number	User-defined name and number of the regular shift.

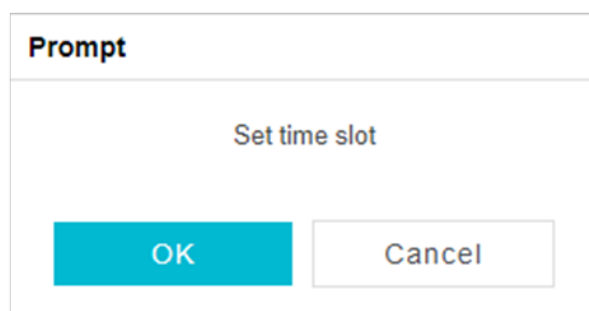
Parameter	Description
Unit	Shift unit. The options are Day , Week , and Month .
Cycle	Shift cycle.
Period start type/Cycle Start Date	Period start type and cycle start date, which are displayed only when Unit is set to Day . The options of Period start type are Period start date and Shift start date . After Period start type is set, Cycle Start Date is mandatory.
Cycle Shift in one Month	Indicates whether to cycle the shift by month. If this parameter is set to Yes , the shift restarts when a new month begins. This parameter is displayed only when Unit is set to Day .
Work Type	Work type. The options are Normal Work , Rest Day OT , and Holiday OT .
Attendance Mode	Attendance calculation method for the shift. The options are Punch Card According to Normal Shift , Punch once at any Time in a Day , and Free Punch .
Overtime Mode	Overtime calculation method. The options are Computer Automatic Calculation , Overtime Must Apply , and Not Calculated as Overtime .

4. Click **OK**.

Step 2 Set a time slot for the shift.

1. Click **OK** in the dialog box that is displayed after the shift is added successfully, as shown in [Figure 6-52](#). Alternatively, you can click **Set time slot** in the **Operations** column of the shift. The page for setting a time slot is displayed.

Figure 6-52 Set time slot



2. Select a time slot and set **Timetable Details**, as shown in [Figure 6-53](#).

Figure 6-53 Set time slot

Set time slot

1

Timetable

Please select the time slot

2

Timetable Details

Cycle

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

3

OK Close

3. Click **OK**.

----End

6.4.7 Schedule Setting

After setting the attendance time slot and shift, you can schedule personnel.

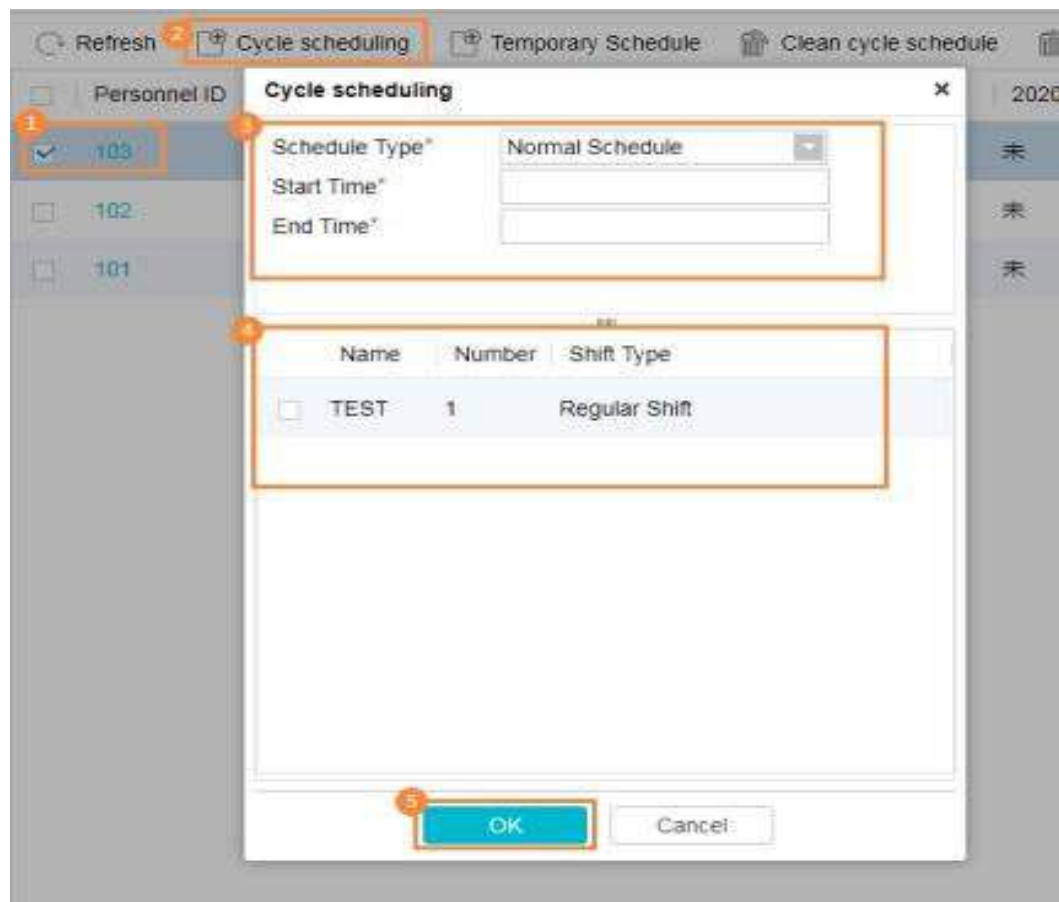
There are two schedule methods: personnel schedule and group schedule.

6.4.7.1 Personnel Schedule

This section describes how to configure personnel schedule on the iClient S100.

Procedure

- Step 1** Choose **Attendance > Schedule > Personnel Schedule** on the iClient S100 home page.
- Step 2** Select the personnel to be scheduled and click **Cycle Scheduling**. On the page that is displayed, set parameters as required, as shown in [Figure 6-54](#).

Figure 6-54 Personnel schedule page

Step 3 Click **OK**.

----End

6.4.7.2 Group Schedule

Group schedule refers to the process of grouping personnel and scheduling personnel in batches by group.

This section describes how to configure group schedule on the iClient S100.

Procedure

Step 1 Create a group.

1. Choose **Attendance > Schedule > Group Schedule** on the iClient S100 home page.
2. On the **Group Schedule** page, click **New** on the left. The page for adding a group is displayed.
3. Set parameters as required, as shown in [Figure 6-55](#).

Figure 6-55 Page for adding a group

New

1

Name*

Remark

2

Save and New

OK

Cancel

4. Click **OK**.

Step 2 Add personnel to the group.

1. On the **Group Schedule** page, click **Add personnel** next to the group.
2. On the **Add Personnel** page that is displayed, select a department on the left and select personnel in the department, as shown in [Figure 6-56](#).

Figure 6-56 Page for adding personnel

Add Personnel

Personnel ID

Name

The current query conditions

Department:(Department Name)

1

Subordinate Level Contained

Department Name

2

Alternative	Selected(1)
☐ Personnel ID	☒ Personnel ID
First Name	First Name
Department Name	Department Name
☒ 103	☒ 103
☐ 102	
☐ 101	

OK

Cancel

3. Click **OK**.

Step 3 Configure group schedule.

1. Select the group or in-group personnel to be scheduled and click **Cycle Scheduling**. The **Cycle scheduling** page is displayed.
2. Set parameters as required. For details, see [6.4.7.1 Personnel Schedule](#).
3. Click **OK**.

----End

6.4.8 Verification

This section describes how to check the status of an added device, the function of clocking on and out, and the attendance status and data. If all these elements are normal, the attendance service is configured successfully.

Procedure

Step 1 Check whether an added device is online.

1. Choose **Attendance > Attendance Device > Device** on the iClient S100 home page.
2. Check whether the status of the added device is online, as shown in [Figure 6-57](#).

Figure 6-57 Device list page

Serial Number	Device Name	Device Model	Firmware Version	IP Address	Attendance Area	Status	Registration Machine	Commands to be Executed
5919194700009	5919194700009	G3 Pro	ZMM720-NF-Ver1.1	192.168.213.167	Area Name	Online		0

Step 2 Verify the function of clocking in and out.

1. Arrange a system personnel to clock in and out on the added attendance device.
2. Choose **Attendance > Calculate Report > Transactions** on the iClient S100 home page.
3. Check whether the clock-in and out records of the personnel are correctly displayed in the original record table, as shown in [Figure 6-58](#).

Figure 6-58 Original record table

Personnel ID	First Name	Last Name	Department Name	Attendance Area	Serial Number	Device Name	Attendance Point Name	Attendance time
2947			Department Name	Area Name	5347183600058	5347183600058		2020-10-29 14:36:
80809				Area Name	5347183600058	5347183600058		2020-10-29 14:35:
80809				Area Name	5347183600058	5347183600058		2020-10-29 14:34:
2947			Department Name	Area Name	CK37194900039			2020-10-29 14:10:
2947			Department Name	Area Name	CK37194900039			2020-10-29 14:10:
2947			Department Name					2020-10-29 09:00:
6464				Area Name	5347183600058	5347183600058		2020-10-28 11:35:
6464				Area Name	5347183600058	5347183600058		2020-10-28 11:35:
6464				Area Name	5347183600058	5347183600058		2020-10-28 11:35:

Step 3 Verify the function of using a camera to record attendance.

1. Arrange an added system personnel to clock in and out on a camera added as the attendance site.
2. Choose **Attendance > Calculate Report > Transactions** on the iClient S100 home page.

3. Check whether the clock-in and out records of the personnel are correctly displayed in the original record table, as shown in [Figure 6-59](#).

Figure 6-59 Original record table

Refresh Export Import U disk record Synchronize attendance records								
Personnel ID	First Name	Last Name	Department Name	Attendance Area	Serial Number	Device Name	Attendance Point Name	Attendance time
2947			Department Name	Area Name	5347183600058	5347183600058		2020-10-29 14:36:
80809				Area Name	5347183600058	5347183600058		2020-10-29 14:35:
80809				Area Name	5347183600058	5347183600058		2020-10-29 14:34:
2947			Department Name	Area Name	CK37194900039			2020-10-29 14:10:
2947			Department Name	Area Name	CK37194900039			2020-10-29 14:10:
2947			Department Name					2020-10-29 09:00:
6464				Area Name	5347183600058	5347183600058		2020-10-28 11:35:
6464				Area Name	5347183600058	5347183600058		2020-10-28 11:35:
6464				Area Name	5347183600058	5347183600058		2020-10-28 11:35:

Step 4 Verify the function of clocking in and out on an access control device.

1. Choose **Attendance > Calculate Report > Transactions** on the iClient S100 home page.
2. Arrange an added system personnel to clock in and out on an access control device added as the attendance site.
3. Check whether the clock-in and out records of the personnel are correctly displayed in the original record table, as shown in [Figure 6-60](#).

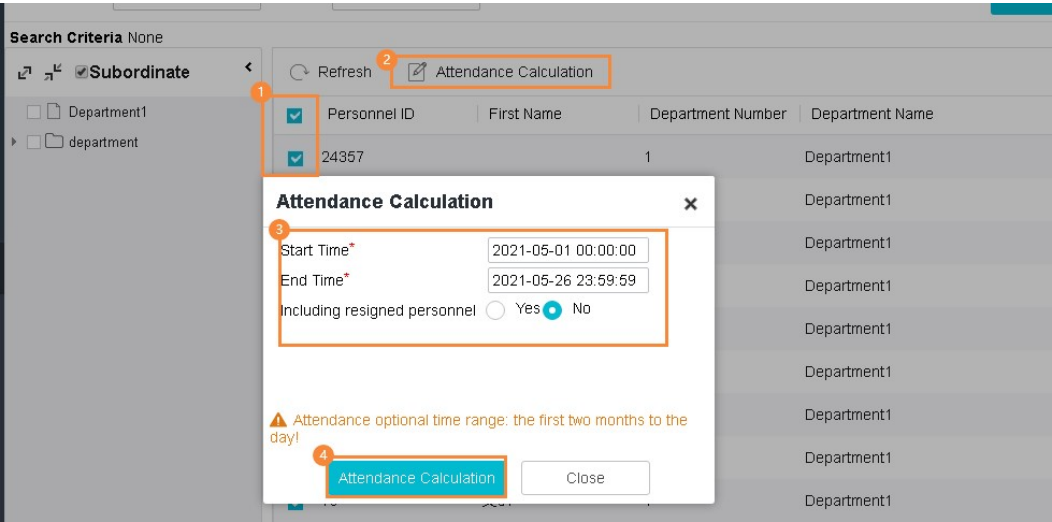
Figure 6-60 Original record table

Refresh Export Import U disk record Synchronize attendance records								
Personnel ID	First Name	Last Name	Department Name	Attendance Area	Serial Number	Device Name	Attendance Point Name	Attendance time
2947			Department Name	Area Name	5347183600058	5347183600058		2020-10-29 14:36:
80809				Area Name	5347183600058	5347183600058		2020-10-29 14:35:
80809				Area Name	5347183600058	5347183600058		2020-10-29 14:34:
2947			Department Name	Area Name	CK37194900039			2020-10-29 14:10:
2947			Department Name	Area Name	CK37194900039			2020-10-29 14:10:
2947			Department Name					2020-10-29 09:00:
6464				Area Name	5347183600058	5347183600058		2020-10-28 11:35:
6464				Area Name	5347183600058	5347183600058		2020-10-28 11:35:
6464				Area Name	5347183600058	5347183600058		2020-10-28 11:35:

Step 5 Verify schedule setting.

1. After a system personnel clocks in and out within the specified attendance duration, choose **Attendance > Calculate Report > Manual Calculate** on the iClient S100 home page.
2. Select a personnel whose attendance statistics are to be calculated and click **Attendance Calculation**, as shown in [Figure 6-61](#).

Figure 6-61 Clicking Attendance Calculation



3. After the attendance calculation is complete, choose **Attendance > Calculate Report > Monthly Detail Report** on the iClient S100 home page.
4. Check whether the attendance status and data are consistent with results of the set schedule, as shown in [Figure 6-62](#).

Figure 6-62 Monthly Detail Report

Personnel			Department	2020-09-20	2020-09-21	2020-09-22	2020-09-23	2020-09-24	2020-09-25	Expected/Actual/Minute		
ID	First Name	Last Name	Name							Should	Actual	Valid
100	Sale			NS	NS	NS	NS	NS	NS	0.0	0.0	0.0
101	Department A			NS	NS	NS	NS	NS	NS	0.0	0.0	0.0

----End

6.5 Configuring Epidemic Prevention Management

6.5.1 Application Scenario

To prevent and control epidemic, devices are used to measure the skin temperature of personnel in real time, alarms are generated upon detecting abnormal skin temperatures, and these abnormal skin temperatures are recorded and summarized. In this case, management personnel can take measures in a timely manner.

6.5.2 Prerequisites

You have performed the operations described in [6.2.3 Adding Devices](#) to add devices that support skin temperature detection on the **Access** page.

6.5.3 Setting Epidemic Prevention Parameters

This section describes how to set epidemic prevention parameters on the iClient S100.

Procedure

- Step 1** Choose **Access > Device > Device** on the iClient S100 home page.
- Step 2** Select a required device and choose **Set up > Set Hep parameters**. The page for setting epidemic prevention parameters is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-63](#).

Figure 6-63 Page for setting epidemic prevention parameters

Set Hep parameters

Selected Device

The following devices are online, please operate!
192.168.213.238

Temperature detection attribute*

Max temperature* 37.30 Temperature Unit* Degree centigrade

Temperature Deviation 0.00 Verify temperature value display* ☒

Correction* Infrared temperature measurement distance* Far Show thermal image* ☒

Mask detection attribute* Mask detection ☒ Please take off your mask* ☒

Trigger External Alarm* ☐ External alarm delay* 10 Second

OK Cancel

- Step 4** Click **OK**.

----End

6.5.4 Verification

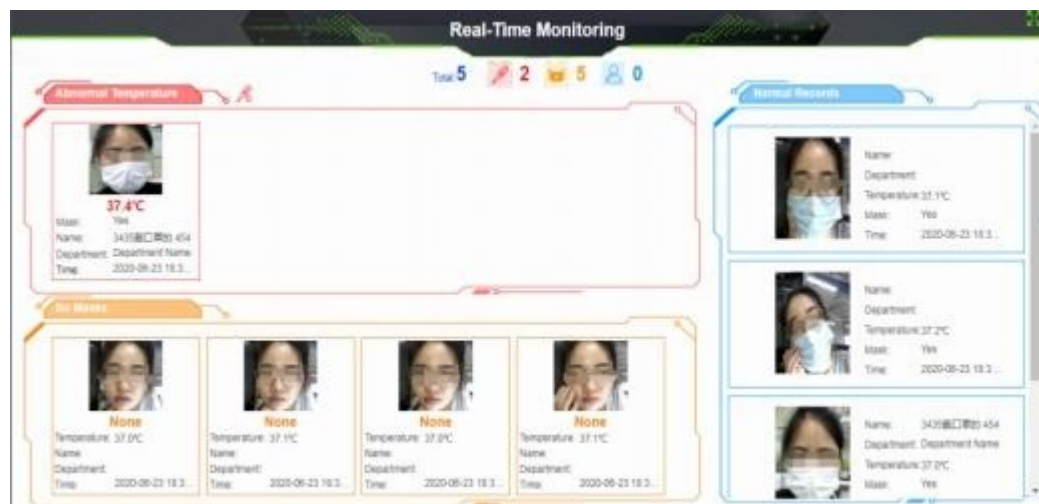
This section describes how to verify the epidemic prevention configuration.

Procedure

- Step 1** Choose **Antiepidemic > Temperature Management > Real-Time detection** on the iClient S100 home page.

- Step 2** On the **Real-Time detection** page that is displayed, perform temperature measurement configuration verification on the required device.
- Step 3** Check whether events of temperature measurement and epidemic prevention are obtained in real time and data is correctly displayed. If so, the epidemic prevention service is configured successfully, as shown in [Figure 6-64](#).

Figure 6-64 Real-time epidemic prevention observation page



----End

6.6 Configuring User Permission Management

6.6.1 Application Scenario

During usage, the superuser needs to add some users with different levels of permissions. To avoid repeated operations of assigning permissions to each user, the superuser can configure roles with different permissions on the role management page and directly assign a role with required permissions to a user to be added.

The superuser has all the permissions and can assign roles (permissions) to users to be added.

6.6.2 Adding a Role

This section describes how to add a role on the iClient S100.

Procedure

- Step 1** Choose **Basic Management > Authority Management > Role** on the iClient S100 home page.
- Step 2** Click **New**. The page for adding a role is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-65](#). [Table 6-28](#) describes the parameters.

Figure 6-65 Page for adding a role

New

1 Role Code*

Role Name*

2 Assign Permissions*

Video Application Complex Application Public Application Maintenance And Management

☐ Video Preview

☐ Video Playback

☐ Search

☐ Statistics

☐ Intelligent

☐ TV Wall

☐ Media Information

☐ Select All

3 Save and New OK Cancel

Table 6-28 Parameters for adding a role

Parameter	Description
Role Code/Role Name	User-defined name and code of the role.
Assign Permissions	Permissions of the role. Select required modules and assign permissions to the role. You can add multiple roles for users at different levels.

Step 4 Click **OK**.

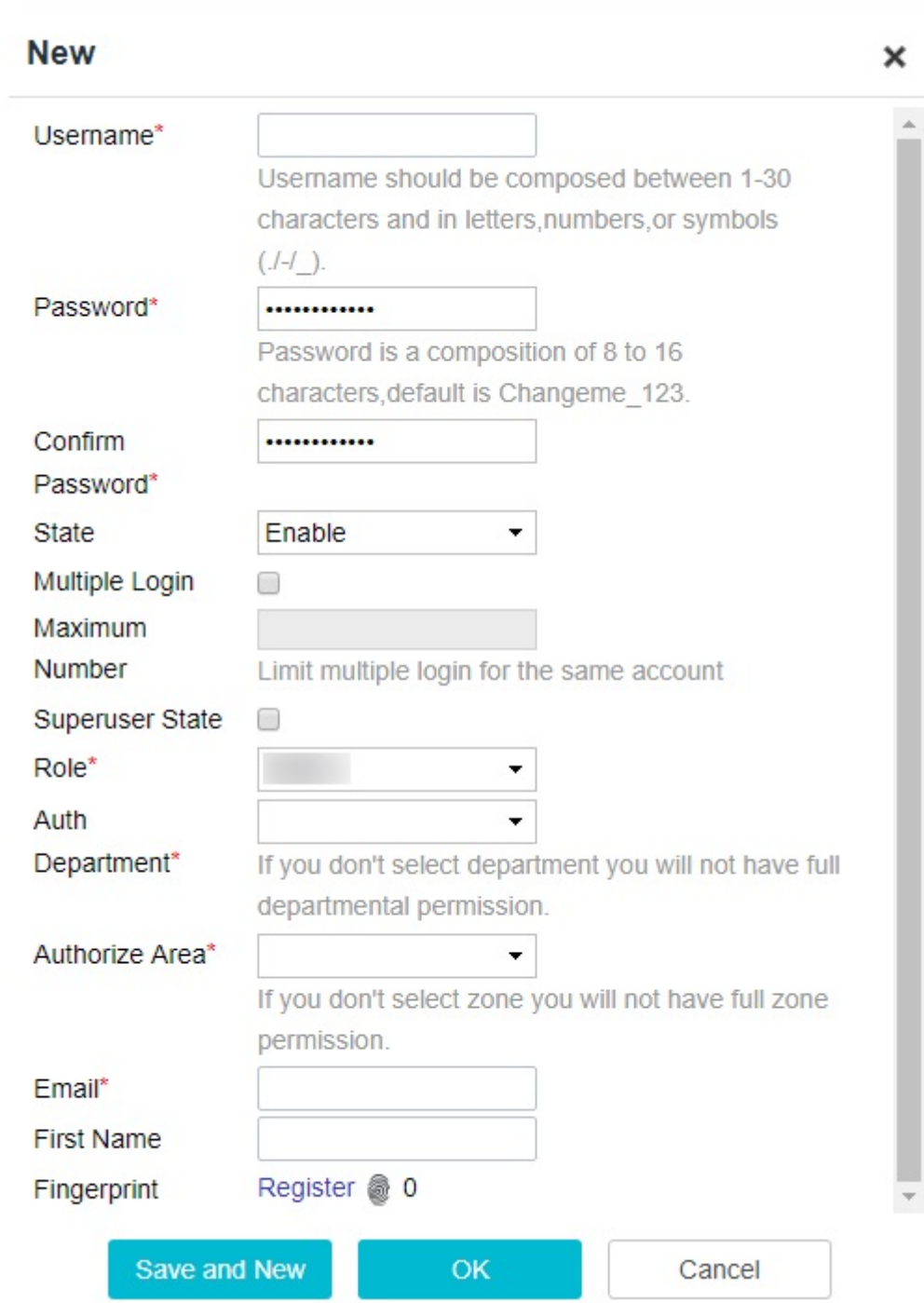
----End

6.6.3 Adding a User

This section describes how to add a user on the iClient S100.

Procedure

- Step 1** Choose **Basic Management > Authority Management > User** on the iClient S100 home page.
- Step 2** Click **New**. The page for adding a user is displayed.
- Step 3** Set parameters as required, as shown in [Figure 6-66](#). [Table 6-29](#) describes the parameters.

Figure 6-66 Page for adding a user


New [Close]

Username*
Username should be composed between 1-30 characters and in letters,numbers,or symbols (/./_).

Password*
Password is a composition of 8 to 16 characters,default is Changeme_123.

Confirm Password*

State

Multiple Login ☐

Maximum Number
Limit multiple login for the same account

Superuser State ☐

Role*

Auth

Department*
If you don't select department you will not have full departmental permission.

Authorize Area*
If you don't select zone you will not have full zone permission.

Email*

First Name

Fingerprint [Register](#) 0

[Save and New](#) [OK](#) [Cancel](#)

Table 6-29 Parameters for adding a user

Parameter	Description
Username/Password	User name and password for logging in to the iClient S100.

Parameter	Description
State	Indicates whether a user can log in to and operate the iClient S100.
Multiple Login	Indicates whether a user is allowed to log in to the iClient S100 on multiple computers at the same time.
Maximum Number	Maximum number of computers where a user can log in to the iClient S100 at the same time.
Superuser State	Indicates whether the user has all permissions by default. If the parameter is selected, the user is a superuser and you do not need to assign a role to the user.
Role	Role of the user. The user has all the operation permissions of the selected role.
Auth Department	Department authorized to the user.
Authorize Area	Area authorized to the user.
Email	User-defined email address, which can be used to retrieve the password.
First Name	First name of the user.
Fingerprint	Fingerprint of the user.

Step 4 Click **OK**.

----End

6.6.4 Verification

This section describes how to check whether the user is added and role permissions are assigned successfully.

Procedure

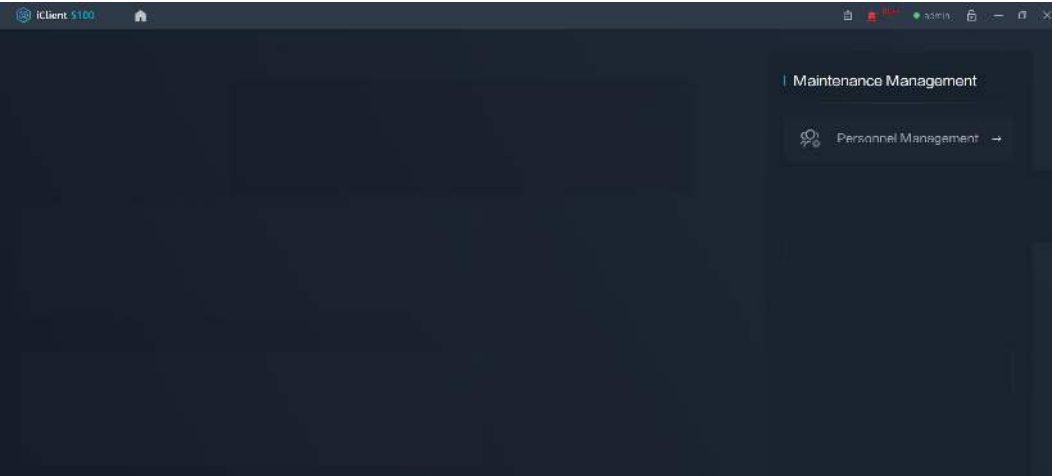
Step 1 Check whether the user is added successfully.

1. Log in to the iClient S100 using the name and password of the added user.
2. If the login is successful, the user is added successfully.

Step 2 Check whether role permissions are assigned successfully.

1. Assign the entry role and required permissions (such as access observation and video alarming) to the user, re-log in to the iClient S100, and view the home page.
2. Check whether only assigned permissions of the role are displayed on the home page. If so, the role is assigned successfully, as shown in [Figure 6-67](#).

Figure 6-67 Role permissions displayed on the home page



----End

7 Local/Personal Configuration

[7.1 Local Settings](#)

[7.2 Personal Settings](#)

7.1 Local Settings

This section describes how to configure local settings and store the settings to the local computer. For example, user A and user B can both use account C to modify local settings and store the settings to each one's local computer, respectively. The local settings of user A and user B do not affect each other. You can set the following parameters on the **Local Settings** page:

- Recording directories
- Snapshot directories
- Other parameters, such as GPU acceleration

Table 7-1 Parameter description

Parameter		Description
Recording Directories	Save Local Recordings to	Local path for storing recordings generated on the iClient S100.
	Download Server-based Recordings to	Local path for storing recordings downloaded from the iClient S100 server.
Snapshot Directories	Save Local Snapshots to	Local path for storing snapshots taken on the iClient S100.
Others	Enable IVS Debug Log	Indicates whether to enable the IVS debug log function. This function is enabled by default.

Parameter		Description
	Enable Local Debug Log	Indicates whether to enable the local debug log function. You can click Open Log Directory to go to the directory for storing client logs on the local computer.
	GPU Acceleration	Indicates whether to enable the function for GPU acceleration. To use GPU decoding, enable GPU acceleration.
	Decode Only I-Frames for Live Video If CPU Usage Exceeds 90%	Indicates whether to enable the function of decoding only I-frames for live video viewing to reduce the CPU and memory usage.
	Decode Only I-Frames for Playback If CPU Usage Exceeds 90%	Indicates whether to enable the function of decoding only I-frames for recording playback to reduce the CPU and memory usage.
	Decoding Format	HME and FFmpeg decoding formats are supported.
	Auto-Lock Screen	Indicates whether to automatically lock the screen when no operation is performed within the configured interval. This function is enabled by default.
Diagnoses	Client Log Export	Button for exporting iClient S100 client logs, CUServer logs, and ZKBioSecurity service logs with one click.

7.2 Personal Settings

This section describes how to perform personal settings. Personal settings are bound to accounts. For example, if user_b uses account_c to log in to the iClient S100 after user_a uses account_c to modify personal settings, the personal settings of user_a are synchronized for user_b. You can set the following parameters on the **Personal Settings** page:

- Set network parameters.
- Set video wall and snapshot parameters.
- Set recording and download parameters.

Network Settings

Table 7-2 Parameter description

Parameter	Description
Video Wall Stream	The options are as follows: • Primary: The primary stream of the camera is used. The primary stream features a high bit rate, definition, and bandwidth usage. • Secondary 1: Secondary stream 1 of the camera is used. Secondary stream 1 features low definition and bandwidth usage. • Automatic: No stream is specified. After this option is selected, the stream that has been transmitted by the camera to the platform is preferentially used. If the camera has not transmitted any stream to the platform, the primary stream of the camera is used by default. NOTE When bandwidth resources are limited, set this parameter to Secondary 1 or Secondary 2.
Live Stream	The options are as follows: • Primary: The primary stream of the camera is used. The primary stream features a high bit rate, definition, and bandwidth usage. • Secondary 1: Secondary stream 1 of the camera is used. Secondary stream 1 features low definition and bandwidth usage. • Secondary 2: Secondary stream 2 of the camera is used. Compared with secondary stream 1, secondary stream 2 features lower definition and bandwidth usage. • Automatic: No stream is specified. After this option is selected, the stream that has been transmitted by the camera to the platform is preferentially used. If the camera has not transmitted any stream to the platform, the primary stream of the camera is used by default. NOTE When bandwidth resources are limited, set this parameter to Secondary 1 or Secondary 2.
Stream Switch	If Live Stream is not set, you can set this parameter. The options are as follows: • Max 960 x 540 Pixels Before Switch • Max Panes Before Switch: You can customize a threshold ranging from 2 to 63.

Video Wall Settings

Table 7-3 Parameter description

Parameter	Description
View Cycling Interval (s)	After this parameter is set, when you choose Favorites > Favorited Views and click  on the VideoWall page to configure view cycling, the default value of Interval (s) is the value of View Cycling Interval (s) .

Recording and Download Settings

Table 7-4 Parameter description

Parameter	Description
Default Clip Length (5 min to 48 hours)	Default duration of a video clip that is manually recorded. This parameter applies to both manual local recording and server-based manual recording.
Split Files Every	Mode for splitting a single recording into several smaller data files. This parameter applies to local manual recording and recording download without encryption. The options are as follows: • Time (minutes): A single recording is split by time. • Capacity (MB): A single recording is split by storage space.
Reserved Space (MB)	Minimum disk space for storing recordings. To ensure that recordings can be stored correctly, the available disk space must be greater than the minimum disk space.
Space Limit Warning (MB)	During video recording, if the disk capacity is less than the value of this parameter, the system generates an alarm. In addition, the disk storage threshold capacity must be greater than the minimum disk storage capacity.
Format	Video file storage format. The default format is MP4.

Parameter	Description
Naming Format	Rule for naming a recording file. This parameter applies to local manual recording and recording download. The options are as follows: • Camera name_No._Time (YYYY-MM-DD-hh-mm-ss) • Camera name_Time (YYYY-MM-DD-hh-mm-ss)_No. • Time (YYYY-MM-DD-hh-mm-ss)_Camera name_No.
Download Threads	Maximum number of recordings that can be downloaded at the same time.
Download Speed (from Server)	Server-based recordings can be downloaded at 1/4, 1/2, or 1x camera bit rate, or high speed (maximum speed that the server, client, and current network can bear). If the bit rate is 4 Mbit/s, 1/4 of it is 1 Mbit/s.
Skip Losses Under (s)	During recording search, if the recording is interrupted for a specified period that is less than the value of this parameter, the recording is played as a complete recording without any interruption.

Snapshot Settings

Table 7-5 Parameter description

Parameter	Description
Shooting Mode	Mode of taking snapshots on the local computer. The options are as follows: • Single: Only one snapshot is taken at a time. • Continuous: Multiple snapshots are taken consecutively at a specified interval.
Format	Format in which local snapshots are stored. The options are as follows: • .jpg: a method of lossy compression. Images saved in .jpg format occupy less space but are easily distorted. • .bmp: a method of lossless compression. Images saved in .bmp format occupy larger space but feature good image quality.
Naming Format	Rule for naming local snapshots.

Alarm Settings

Table 7-6 Parameter description

Parameter	Description
Play Non-triggered Live Video in Alarm Pane	Indicates whether an alarm pane can play common live video. The options are as follows: • On: yes • Off: no
Auto Close After (s)	Display duration of a service or an NMS alarm notification.
Pre-alarm Recording Duration (s)	Video recording duration before an alarm is generated if the video recording linkage action is configured.
Post-alarm Recording Duration (s)	Video recording duration after an alarm is generated if the video recording linkage action is configured.
Critical Alarm Notification	You can select an alarm type as a critical alarm. When an alarm is generated, an alarm dialog box is displayed. Critical alarms are notified at the following intervals: • One-off • Cyclic notification. The interval can be set to 1 minute, 5 minutes, or 10 minutes. To set cyclic notification of critical alarms, perform the following steps: 1. Click . 2. Select Select alarm types and select an alarm type from the drop-down list box. 3. Click OK.
Alarm Pop-up	When the client receives any alarm of a specified type or severity, it displays the alarm. To enable this function, perform the following operations: 1. Select Alarm Pop-up. 2. Set Select alarm types or Select alarm severity in the dialog box. 3. Click OK. NOTE Optional operations: • Click  in the lower right corner of an alarm pop-up. Alarms will not pop up within 30 minutes. •

Parameter	Description
Alarm Sound	Audio file played when the client detects a service alarm. By default, this function is disabled. You can click  and select an audio file stored in a local directory. NOTE - Only audio files in .wav format are supported. - Click Reset to restore the system's default alarm sound. The default audio file is Alarm.wav.
Customize Alarm Sound	Click the button to add custom sounds for different alarm types. Before setting this parameter, select Alarm Sound. You can click Add Custom Sound, click Select Alarm Type, select different alarm types, and click OK. You can add different custom sounds for multiple alarm types.

Other Settings

Table 7-7 Parameter description

Parameter	Description
Optimize Images	Indicates whether to optimize images. If you set this parameter to Yes , blank screen issues caused by network faults will be decreased. Instead, just frame freezing may occur.
Max Packet Loss Rate in Image Quality Optimization (%)	If Optimize Images is set to Yes , the frames with artifacts are automatically discarded to ensure the video definition when the packet loss rate exceeds the threshold specified by this parameter.
Resume Default Scene	Indicates whether to resume the default scene. If you set this parameter to Yes , the last scene is displayed when you reopen the video wall or live video page.
Enable Seamless Switch for Cycling	Select Yes to enable this function. When camera cycling is enabled, video played in the video panes can be seamlessly switched.

Parameter	Description
Anonymize Data	If this function is enabled, sensitive personal information (such as the name, date of birth, and certificate number) in system modules can be processed. NOTE • If the server of the platform is upgraded from an earlier version, this function is disabled by default. • If the server of the platform is newly installed and configured, this function is enabled by default. • If you modify the anonymization configuration, you will be logged out of the system and need to log in again.
Update Key	Updates the key in one-click mode.

8 FAQs

[8.1 Video Service](#)

[8.2 Comprehensive Services](#)

8.1 Video Service

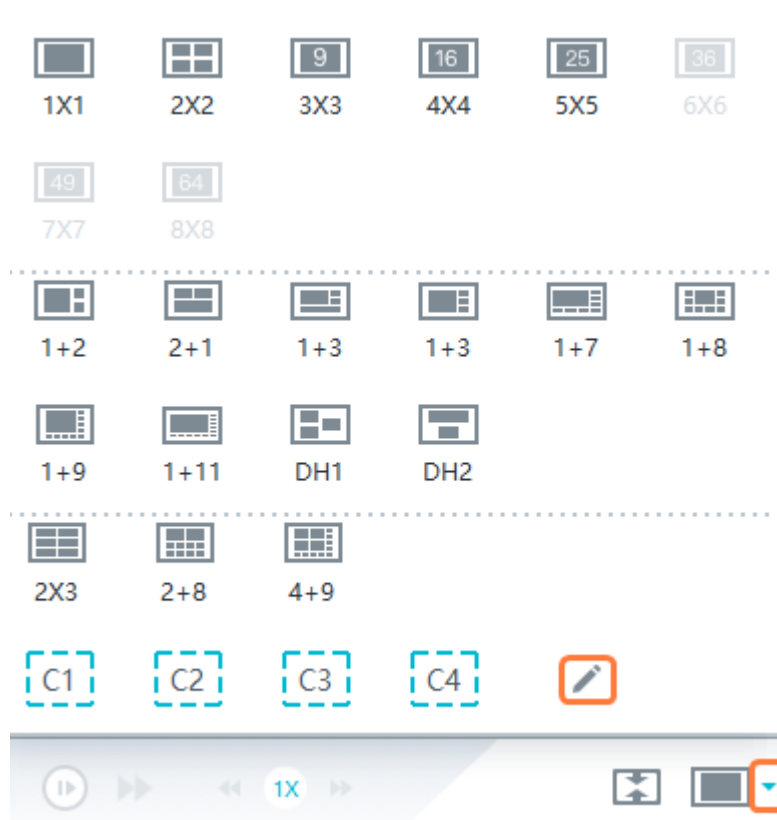
8.1.1 Viewing Live Video

8.1.1.1 How Do I Define the Layout for Live Video Viewing or Recording Playback?

This section describes how to define the layout for recording playback. The method of defining the layout for live video viewing is similar.

Step 1 On the iClient S100 home page, choose **Basic Operations > Playback**.

Step 2 Click ▲ on the right of  above the timeline area, as shown in [Figure 8-1](#).

Figure 8-1 Setting a layout

Step 3 Select a system default layout. Alternatively, click  to customize a layout. A maximum of four layouts (C1, C2, C3, and C4) can be customized.

Step 4 Repeat [Step 2](#) and select a customized layout, for example, C1. The customized layout is used for recording playback.

----End

8.1.1.2 How Do I Add Cameras to a Favorites Folder?

Application Scenario

This section describes how to add frequently used cameras to a camera favorites folder so that you can quickly locate these cameras whenever you want to use them. For example, you spend most time every day observing key area A every day. Therefore, you want to add all the cameras deployed on this road to a favorites folder.

Procedure

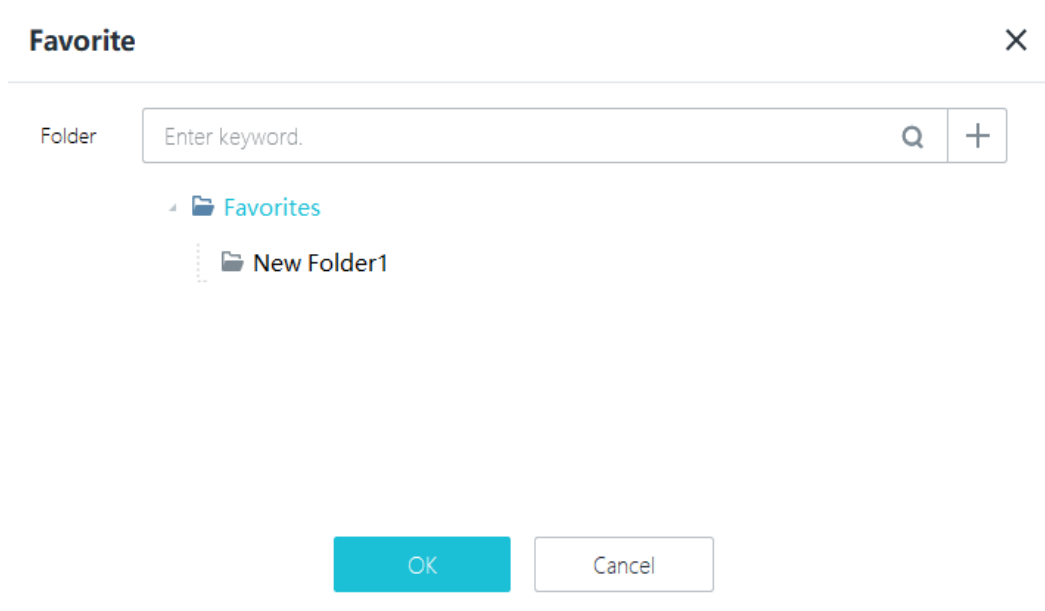
Step 1 Choose **Basic Operations** > **Live** on the iClient S100 home page.

Step 2 You can use either of the following methods to add a camera to the favorites folder:

- Click the corresponding icon on a live video image.

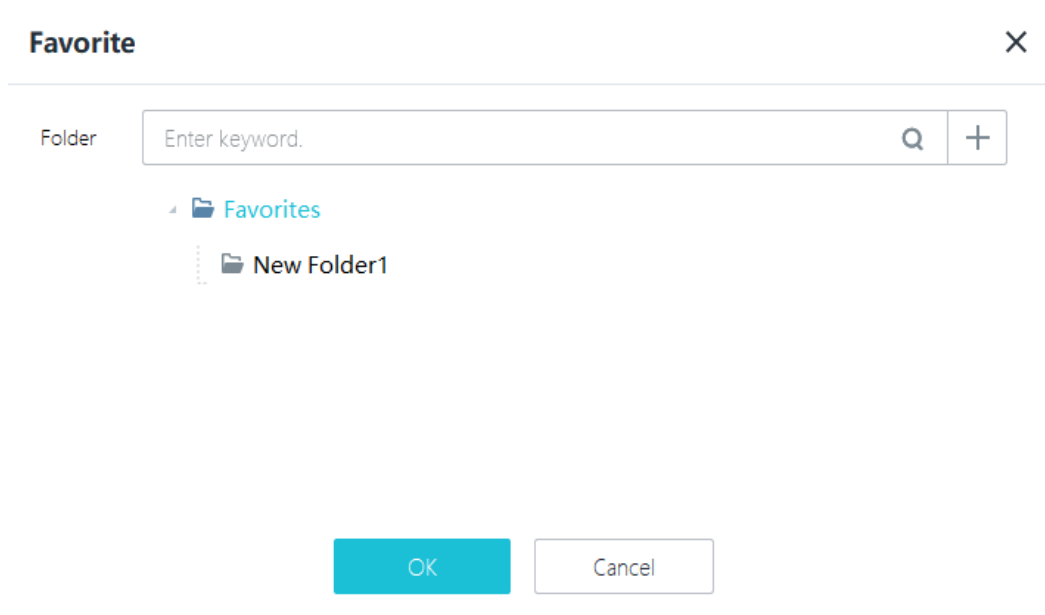
- a. Double-click an online camera in the **Devices** area or drag the online camera to a live video pane. Then, you can view the live video.
- b. Click . In the **Favorite** dialog box that is displayed, enter a folder name or select **Favorites**, as shown in [Figure 8-2](#).

Figure 8-2 Adding cameras to a favorites folder



- c. Click **OK**.
- Select a device on the device tree.
 - a. Right-click a device and choose **Favorite**.
 - b. In the **Favorite** dialog box that is displayed, enter a folder name or select **Favorites**, as shown in [Figure 8-3](#).

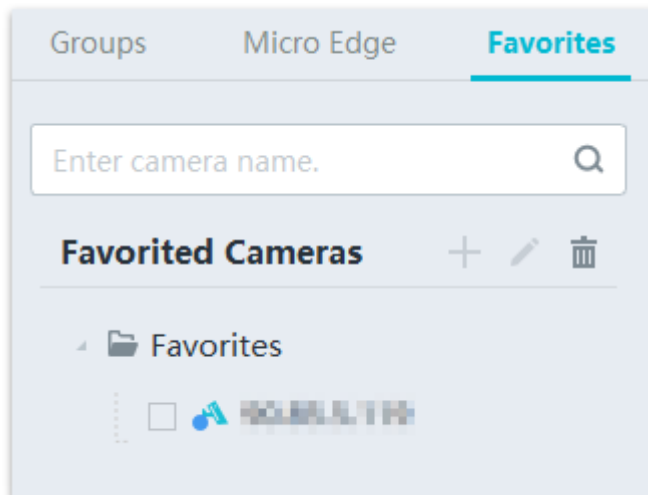
Figure 8-3 Adding cameras to a favorites folder



c. Click **OK**.

Step 3 Choose **Favorites > Favorited Cameras** and click **Favorites**. Favorited cameras are displayed, as shown in [Figure 8-4](#).

Figure 8-4 Viewing favored cameras



Step 4 Manage the **Favorites** folder and its subfolders. To add a subfolder for the folder, right-click the folder and choose **Add Subfolder**. To add a peer folder or a subfolder for a subfolder and edit or delete a subfolder, select the subfolder, right-click and choose **Add Peer Folder**, **Add Subfolder**, **Edit**, or **Delete** from the shortcut menu.

NOTE

You can drag a favorites folder under **Favorited Cameras** to its upper-level favorites folder and drag a single favorited device from one favorites folder to another.

----End

8.1.1.3 How Do I Use Voice Intercom?

Prerequisites

- A camera with a built-in microphone or audio ports is available.
- You have connected the speaker and microphone.
 - You have connected the microphone to the AUDIO_IN port on the camera, and the speaker to the AUDIO_OUT port on the camera. The ports vary depending on the camera model.
 - You have connected the microphone to the LINE IN port on the rear panel of the device, and the speaker to the LINE OUT port on the rear panel of the device.
- You have enabled the voice intercom function for the camera. For details, see the camera product documentation.

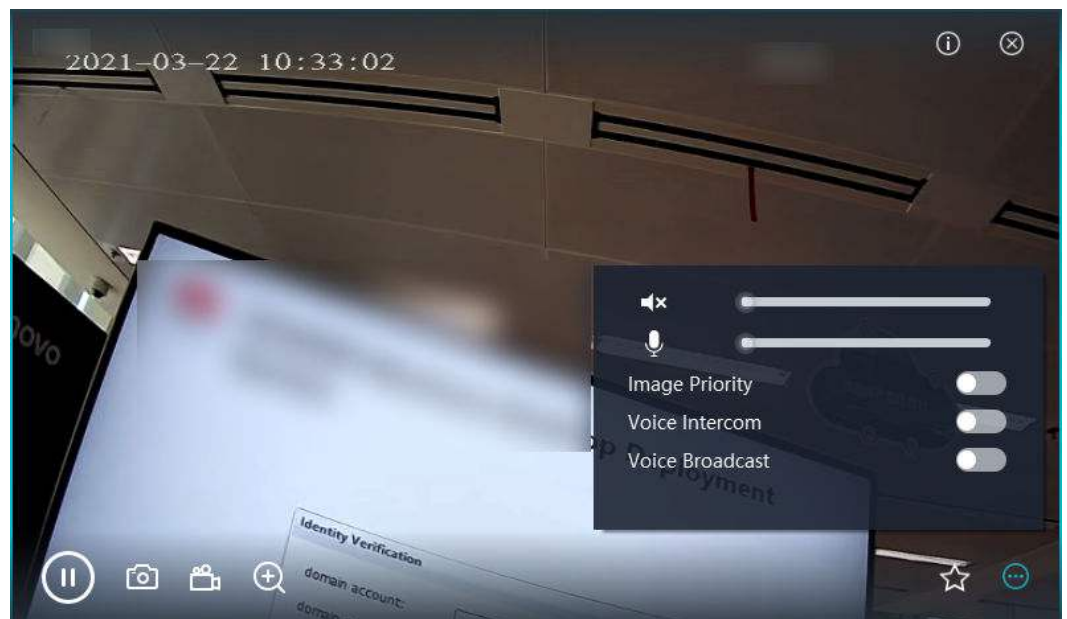
Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 You can enable voice intercom in one of the following ways:

- Move the pointer to a video pane that is playing live video. The toolbar is displayed at the bottom of the video pane. Click  to expand the functions and toggle-on  next to **Voice Intercom** to enable voice intercom, as shown in [Figure 8-5](#).

Figure 8-5 Voice intercom



- Right-click a live video pane and choose **Voice Intercom** from the shortcut menu.

----End

8.1.1.4 How Do I Use Voice Broadcast?

Prerequisites

- A camera with a built-in microphone or audio ports is available.
- You have connected the speaker.
 - You have connected the speaker to the AUDIO_OUT port on the camera.
 - You have connected the speaker to the LINE OUT port on the rear panel of the device.

NOTE

Currently, this feature is available only for the IVS1800.

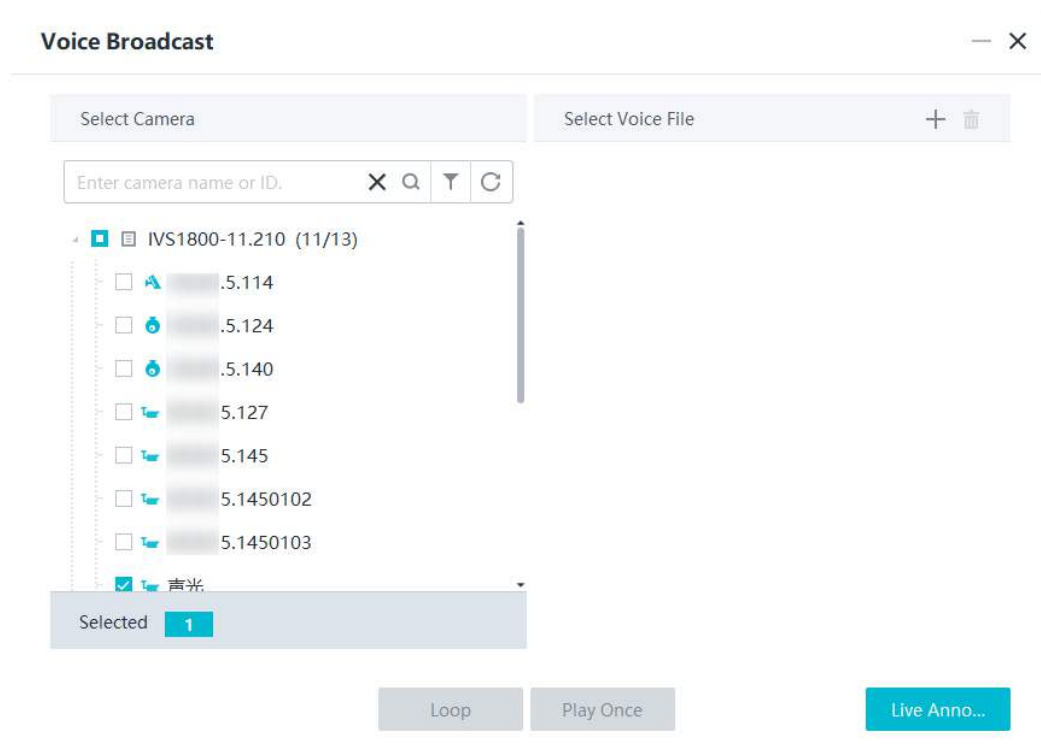
Procedure

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 You can enable voice broadcast in either of the following ways:

1. Move the pointer to a video pane that is playing live video. The toolbar is displayed at the bottom of the video pane. Click  to expand the functions and click  next to **Voice Broadcast**. In the **Voice Broadcast** window that is displayed, click **Live Announcement**, as shown in [Figure 8-6](#).

Figure 8-6 Voice broadcast



2. Right-click a live video pane and choose **Voice Broadcast** from the shortcut menu. In the **Voice Broadcast** window that is displayed, click **Live Announcement**.

Step 3 To stop manual broadcast, click **Stop**.

Step 4 Click + next to **Select Voice File**, add a local audio file, and click **Play Once** or **Loop**. To stop the broadcast, click **Stop**.

NOTE

- Only the .wav and .wave local audio files in PCM encoding format can be broadcast.
- If a local audio file fails to be broadcast, you can use the VLC player to check the encoding format of the audio file and determine whether the broadcast failure is caused by the encoding format.

----End

8.1.1.5 How Do I Superimpose a Behavior Analysis Task on Live Video?

Application Scenario

For a camera that supports intelligent analysis functions such as behavior analysis and situation analysis, you can configure intelligent overlay on the **Live** or **Playback** page of the iClient S100 to superimpose detection lines or frames on the video image from the camera (only the IVS1800 supports intelligent overlay on the **Playback** page). Then you can view the detection result in real time.

Prerequisites

You have configured camera functions on the iClient S100 or in the camera web system.

- For details about how to configure intelligent analysis functions in the camera web system, see the camera product documentation.
- The functions supported by the iClient S100 vary according to the connection mode of a camera. [Table 8-1](#) describes the functions supported for each connection mode.

Table 8-1 Camera parameter settings

Connection Mode	Supported Function	Configuration Description
Cameras connected through the IVS1800	• Frontend behavior analysis: tripwire crossing detection, intrusion detection, abandoned object detection, removed object detection, loitering detection, area entry/exit detection, fast movement detection, and electric bike detection • Situation analysis: head counting, queue length detection, and crowd density detection • Target recognition: target detection and person detection • Vehicle recognition: vehicle detection and non-motorized vehicle detection	• For details about frontend behavior analysis parameters, see 5.6.1 Frontend Behavior Analysis. • For details about situation analysis parameters, see 5.9 Situation Analysis. • For details about intelligent target analysis parameters, see 5.7 Target Intelligence. • For details about intelligent person analysis parameters, see 5.8 Person Intelligence. • For details about intelligent vehicle analysis parameters, see 5.10 Intelligent Vehicle Analysis.

Connection Mode	Supported Function	Configuration Description
Cameras connected through the NVR800	• Behavior analysis: tripwire crossing detection, intrusion detection, abandoned object detection, removed object detection, loitering detection, area entry/exit detection, fast movement detection, and electric bike detection • Situation analysis: head counting, queue length detection, crowd density detection, and off-duty detection • Target detection • Vehicle recognition: vehicle detection and non-motorized vehicle detection	• For details about behavior analysis parameters, see 4.6 Behavior Analysis. • For details about situation analysis parameters, see 4.9 Situation Analysis. • For details about intelligent target analysis parameters, see 4.7 Intelligent target Analysis. • For details about intelligent vehicle analysis parameters, see 4.10 Vehicle Intelligence. • For details about third-party algorithm parameters, see 4.11 Third-Party Algorithms.

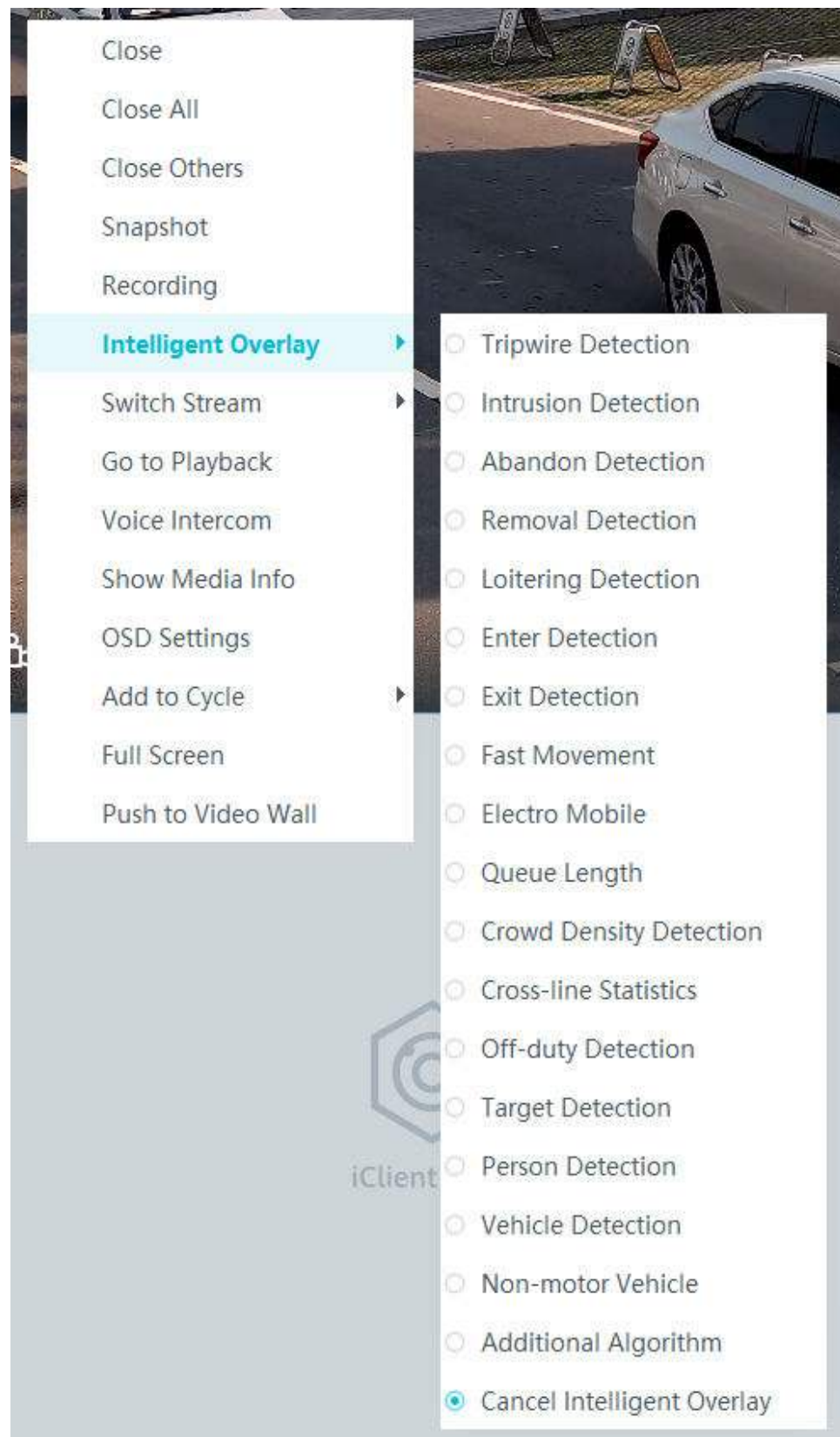
Procedure

You can superimpose an intelligent analysis task of a camera on live video from the camera to detect related behavior in real time.

Step 1 On the iClient S100 home page, choose **Basic Operations > Live**.

Step 2 Double-click an online camera in the **Devices** area or drag the online camera to a live video pane.

Step 3 Right-click the live video pane. Choose **Intelligent Overlay > Intelligent event name**. The real-time intelligent analysis result is superimposed on the video image, as shown in [Figure 8-7](#).

Figure 8-7 Options under Intelligent Overlay

The information displayed varies depending on the selected intelligent overlay type. **Figure 8-8** shows the intrusion detection result, which displays trajectories of pedestrians. Pedestrians in the detection area are framed in yellow and those outside the detection area are framed in blue in the video image.

Figure 8-8 Intrusion detection



Step 4 To cancel the intelligent overlay, click **Cancel Intelligent Overlay**.

----End

8.1.1.6 How Do I Adjusting the Video Grouping Sequence

Video groups are sorted by group creation time by default. To adjust the grouping sequence, perform the following steps

Step 1 On the iClient S100 home page, choose **Video Device > Group Device**.

Step 2 In the Group Device List area, select the group whose sequence needs to be adjusted, drag it to a new position, and release the mouse pointer. Repeat this step until the grouping sequence is adjusted.

Step 3 Manually refresh the device tree status in the video live area, show as in **Figure 8-9**.

Figure 8-9 refresh device tree

----End

8.1.2 Client

8.1.2.1 How Do I Use the Multiple Windows Function?

Drag a function tab on the top of the iClient S100 from the main window to secondary windows.

NOTE

- Each tab can be dragged to only **one secondary window**, and the tab cannot be opened on the main window of the client at the same time.
- The multiple windows function supports a maximum of four windows.

8.1.2.2 What Is the Default Password for Logging in to the Client?

The default password of the iClient S100 is **Changeme_123**. You need to change the password upon the first login.

8.1.2.3 How Do I Set the System Time and Time Zone?

The system time and time zone of the computer running the server and clients must be the same as those of the main device (NVR800/IVS1800).

You can set the system time and time zone on the computer under **Start > Control Panel > Clock, Language, and Region**.

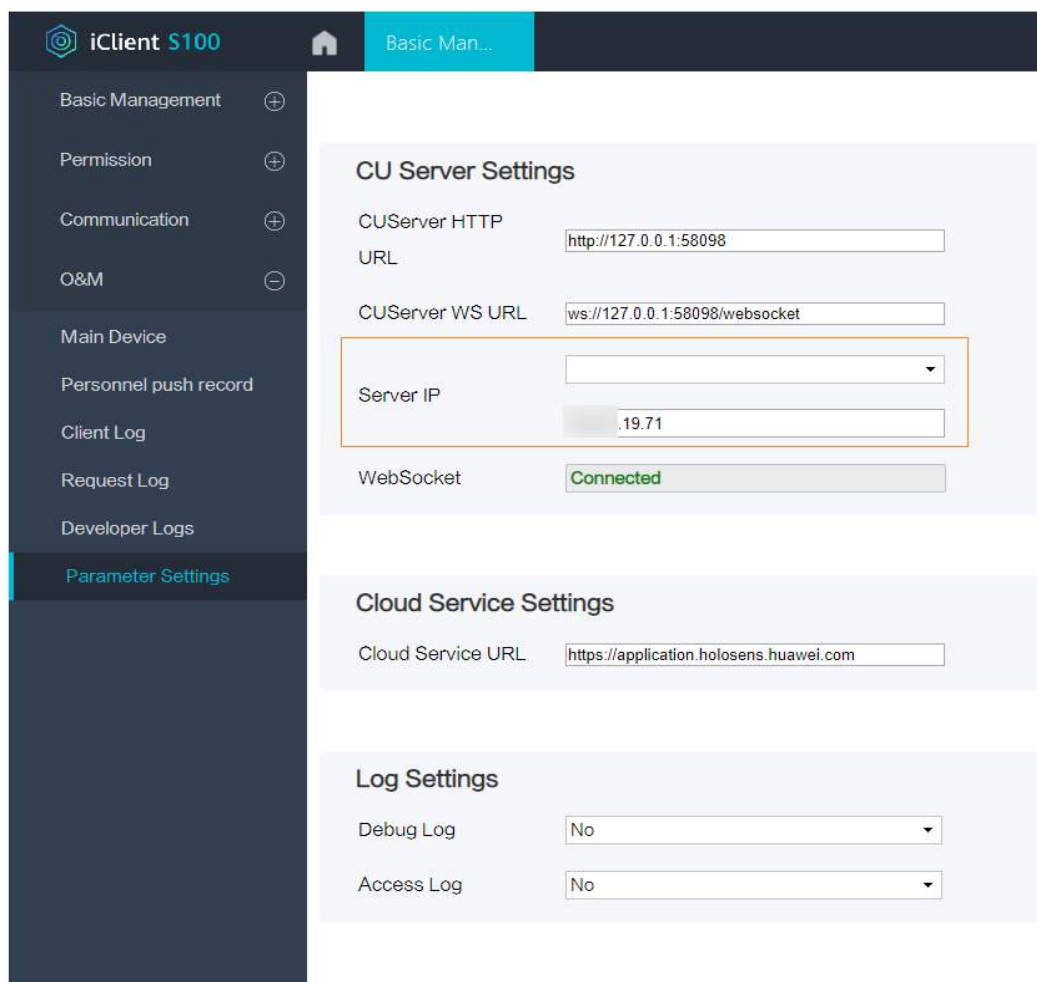
8.1.2.4 How Do I Set the Server IP Address When the Computer Running the iClient S100 Server Has Two Network Adapters?

- Step 1** Check the IP addresses of the two network adapters on the computer running the iClient S100 server and select an IP address as required.

Step 2 Configure the IP address on the iClient S100 server.

Choose **Maintenance Management > Basic Management > O&M > Parameter Settings**. In the **CU Server Settings** area, set **Server IP**, as shown in [Figure 8-10](#).

Figure 8-10 Changing the IP address of the server



----End

8.1.3 User Management

8.1.3.1 Configuring a User Role

Context

On the OMU portal of the IVS1800, the **admin** user can define general users and assign a proper built-in role to each user based on user information. The configurable built-in roles are as follows: **System Operator**, **General Operator**, **System Operator (ISV)**, **General Operator (ISV)**, and **System O&M**.

- The **admin** user is a system-predefined role with full permissions on the system. The role and name of the **admin** user are specified by default and unconfigurable.

- The **System Operator** and **System Operator (ISV)** roles have the same permissions in differing application scenarios.
 - The **System Operator** role is used to log in to the iClient S100 or OMU portal.
 - The **System Operator (ISV)** role is used to connect a third-party VIID or an integrated video and image application platform to the IVS1800.
- The **General Operator** and **General Operator (ISV)** roles have the same permissions in differing application scenarios.
 - The **General Operator** role is used to log in to the iClient S100 or OMU portal.
 - The **General Operator (ISV)** role is used to connect a third-party VIID or an integrated video and image application platform to the IVS1800.
 - The **General Operator** role cannot use video services, import target lists, or manage algorithms on the iClient S100.
- The **System O&M** role is used to log in to the iClient OM to perform operations such as device upgrade and preventive maintenance inspection (PMI).

Procedure

User roles are configured in akin procedures. This section uses the procedure of configuring a user with the **System Operator** role as an example.

- Step 1** Log in to the OMU portal as the **admin** user.
- Step 2** Choose **User Management > AddUser**.
- Step 3** Configure a user with the **System Operator** role, as shown in [Figure 8-11](#).

Figure 8-11 Configuring a user role

1

*Role System Operator

*User Name test001

Weak Medium Strong

*Password

*Confirm password

*MaxLoginSession 1

*CloudControlLevel 1 32 min, 1 Max

*Enable account validity ☒

*ValidDateStart 2020-09-04 11:33:43

*ValidDateEnd 2020-09-06 11:33:43

*Enable all domain to look ☒

*UserDescription

2 Save

Table 8-2 describes the parameters.

Table 8-2 Parameter description

Parameter	Description
Role	Role type. Select System Operator .
User Name	Customized user name and password. You need to set a complex password by referring to "Password Maintenance Suggestions" in the <i>IVS1800 Product Documentation</i> .
Password	
Confirm password	

Parameter	Description
Multi-point Logins	Maximum number of servers with the same system environment where a user account can be used. That is, the user account can be used to connect an IVS1800 to a specified number of iClient S100 servers at most and used to log in to the OMU portal on a specified number of computer servers at most in the same predetermined period of time. This will not cause cross-system login congestion. For example, if this parameter is set to a value N, a user account can be used to connect an IVS1800 to N iClient S100s at most and log in to the OMU portal on N computers at most in the same predetermined period of time.
PTZ Control Priority	Precedence order of PTZ controls. The value ranges from 1 to 32 in descending order of precedence.
Validity Period	- Selected: only valid in the validity period of a user account - Deselected: permanently valid If Validity Period is deselected, a message indicating the account vulnerability is displayed. For security purposes, you are advised to select this check box.
Effective Time/Expiration Time	
View All Devices	Indicates whether the user can view all connected cameras on the IVS1800.
Description	User description.

Step 4 (Optional) Grant the camera viewing permission to the user.

1. In the **Manage User** area, click **Set Permission** in the row of the newly added user.
2. Grant the camera viewing permission to the user assigned with a role, as shown in [Figure 8-12](#).

Figure 8-12 Granting camera viewing permission

The user cannot view cameras newly added to the IVS1800 by default even being granted with the camera viewing permission. To view new cameras, select **View All Devices** listed in [Step 3](#).

Step 5 (Optional) If there are multiple IVS1800s, perform [Step 1](#) through [Step 4](#) to add users for each IVS1800.

-----End

Verification

Step 1 Click **Log Out** to log out the **admin** user.

Step 2 Log in to the OMU portal as the new user, as shown in [Figure 8-13](#).

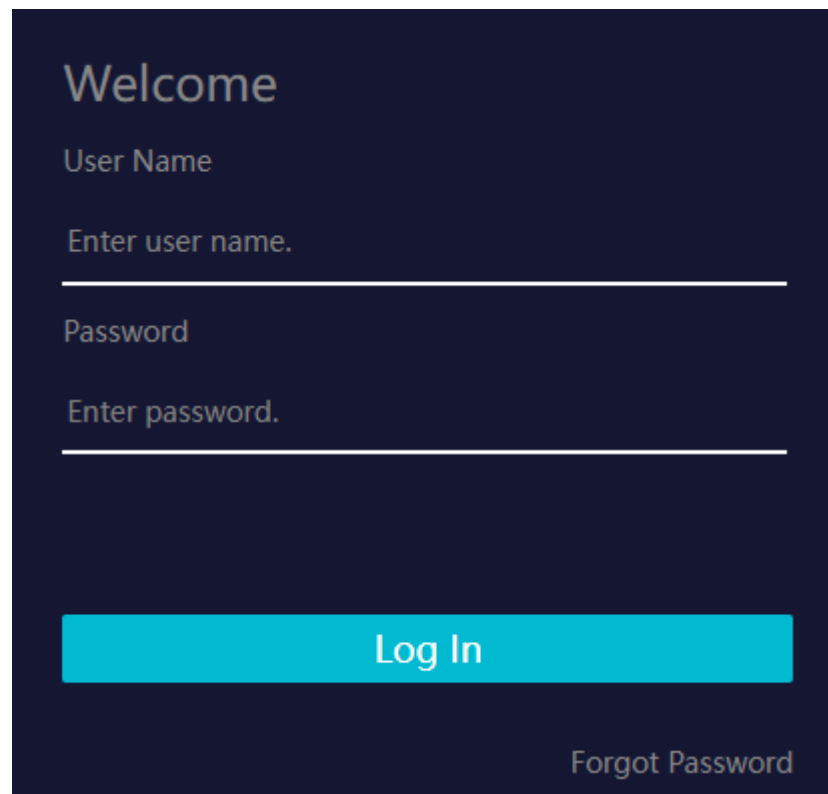
Figure 8-13 Logging in as a new userA login form with a dark blue background. At the top, the word "Welcome" is displayed in a large, light blue font. Below it, the text "User Name" is followed by a light blue input field with the placeholder text "Enter user name.". Below that, the text "Password" is followed by a light blue input field with the placeholder text "Enter password.". At the bottom, there is a large, bright blue rectangular button with the text "Log In" in white. To the right of the button, the text "Forgot Password" is displayed in a smaller, light blue font.

Table 8-3 describes the parameters.

Table 8-3 Parameter description

Parameter	Description
User name	The user name and password must be the same as those set in Figure 8-11 .
Password	

Step 3 Click **OK** when the system displays "The first time you log in, please change your password".

Step 4 Change the password, as shown in [Figure 8-14](#).

Figure 8-14 Changing the password

The screenshot shows a 'Change Password' dialog box with a close button (X) in the top right corner. It contains three input fields: 'Old password', 'New password', and 'Confirm password'. The 'New password' field has a strength indicator with three tabs: 'Weak', 'Medium', and 'Strong'. The 'Strong' tab is selected and highlighted in green. Below the input fields are two buttons: 'Save' and 'Cancel'. A red box highlights the input fields, and a red circle with the number 1 is next to the 'Old password' label. A red circle with the number 2 is next to the 'Save' button.

Table 8-4 describes the parameters.

Table 8-4 Parameter description

Parameter	Setting
Old password	Enter the password set in Figure 8-11 .
New password	Customize a complex password by referring to "Password Maintenance Suggestions" in the <i>IVS1800 Product Documentation</i> .
Confirm password	

Step 5 Use the new password to relog in to the OMU portal.

----End

8.1.4 Camera

8.1.4.1 How Do I Set Alarm Input and Output Parameters for a Camera?

1. Open Internet Explorer, enter the IP address of the camera in the address box, and press **Enter**.
2. Enter the user name and password of the camera and click **Login**.
3. In the camera web system, choose **Settings > Alarms > Alarms > Device Setup**.

4. Set alarm input and output parameters, as shown in [Figure 8-15](#). [Table 8-5](#) describes the parameters.

Figure 8-15 Setting alarm input and output parameters

Alarm Input

☐ Enable

Device ID

Alarm input 1

Name

input1

Type

Normally closed

Alarm check interval (s)

1

Alarm Output

Device ID

Alarm output 1

Enable

Name

Output1

Duration (s)

10

Save

Table 8-5 Parameter/Button description

Parameter/Button		Description
Alarm Input	Enable	Indicates whether to enable the alarm input function.
	Device ID	ID of the alarm input device. You can select a value from the drop-down list box.
	Name	User-defined device name.

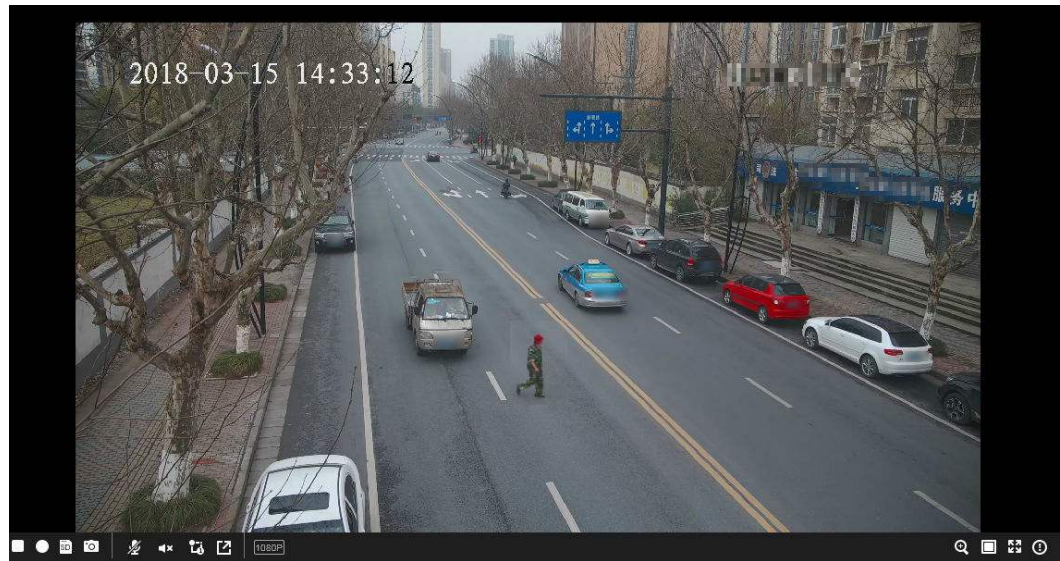
Parameter/Button		Description
	Type	Type. Select either Normally open or Normally closed based on the device status.
	Alarm check interval (s)	Interval at which the system checks for new alarms.
Alarm Output	Device ID	ID of the alarm output device.
		Manual control of the output device status. Do not enable the device when the alarm linkage function is in use. Otherwise, the alarm linkage actions will be affected.
	Name	User-defined device name.
	Duration (s)	Duration of an alarm. If Duration (s) is set to 0 , the alarm persists permanently.

8.1.5 Others

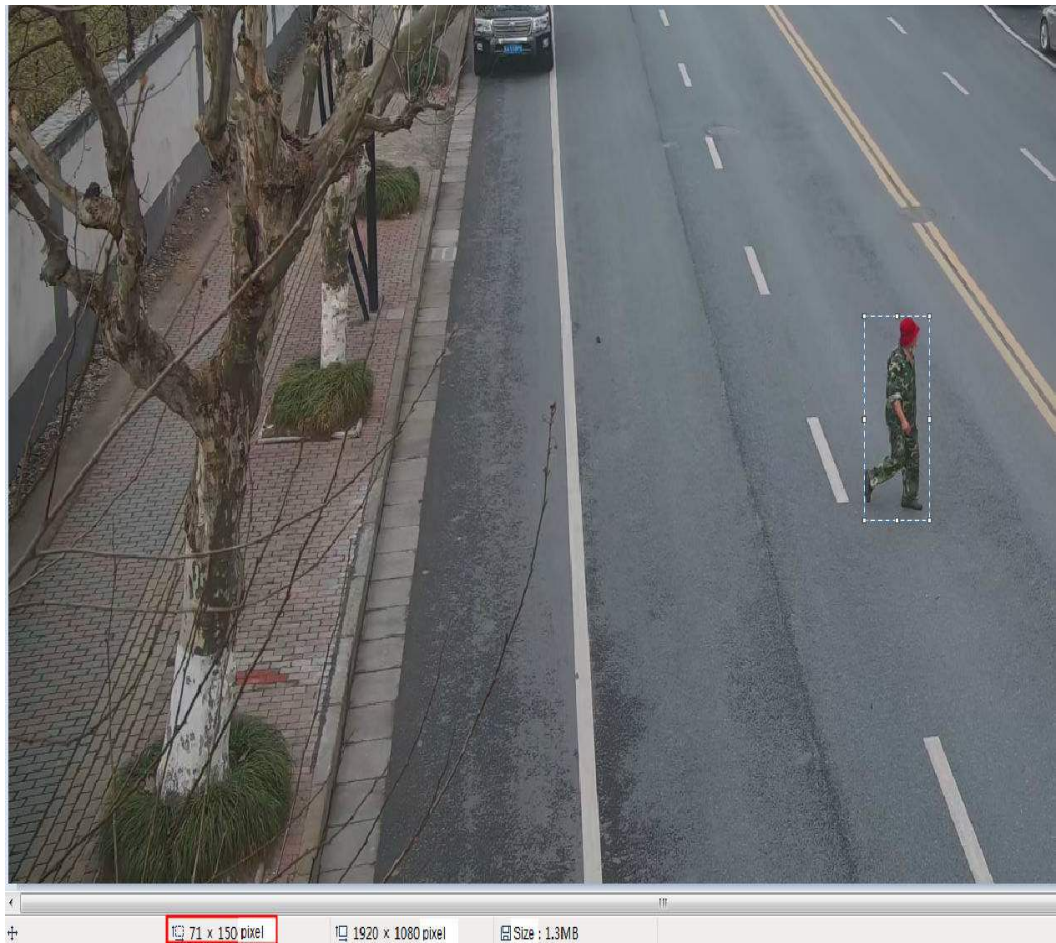
8.1.5.1 How Do I Check the Target Image Resolution?

Step 1 Log in to the camera web system as the **admin** user.

Step 2 On the video preview page, click **Snapshot** in the lower left corner when a person appears in the center of the image, as shown in [Figure 8-16](#).

Figure 8-16 Snapshot taking

- Step 3** In the dialog box that is displayed in the lower right corner, check the path for storing snapshots and find the snapshot in the path.
- Step 4** Use the Microsoft Paint software on the Windows operating system to open the snapshot, and use a rectangle to frame the target in the image. The resolution of the area covered by the rectangle is displayed in the lower left corner of the window, as shown in [Figure 8-17](#).

Figure 8-17 Checking the resolution of the target image

In the example, the height of the target image is 150 pixels, which meets the requirements of the long shot mode.

If the height of the target image does not meet the requirements, you need to adjust the installation height, angle, distance, and focal length of the camera to ensure the image clarity.

----End

8.2 Comprehensive Services

8.2.1 Basic Management

8.2.1.1 How Can I View Logs Recording My Operations on the iClient S100?

This section describes the procedure for viewing and exporting logs recording your operations on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Basic Management > Basic Management > Operation Log**.
- Step 2** On the page that is displayed, view all logs recording your in-system operations, or search for required operation records by criteria such as the operator and operation time period, as shown in [Figure 8-18](#).

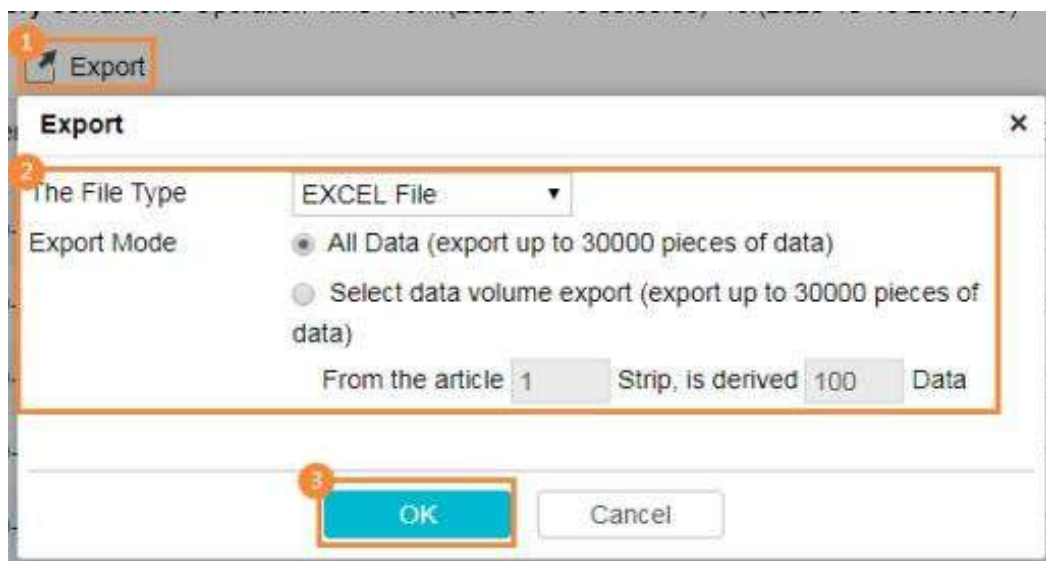
Figure 8-18 Viewing logs

Operation User	Operation Time	Operation IP	Module	Operating Object	Operation Type	Operation Content	Result	Time (ms)
test	2020-09-30 09:32:37	192.168.213.11	System	User	User Login	User Login: test	Success	359
admin	2020-09-30 09:13:48	192.168.213.19	Business	Main device Search		Get the parent device	Success	7
admin	2020-09-30 09:13:48	192.168.213.19	Business	File	Download	Download personnel config	Success	17
admin	2020-09-30 09:13:48	192.168.213.19	System	User	User Login	User Login: admin	Success	251
admin	2020-09-29 14:21:08	192.168.213.19	Business	Main device Search		Get the parent device	Success	1
admin	2020-09-29 14:20:25	192.168.213.19	Business	Main device Search		Get the parent device	Success	2
admin	2020-09-29 14:19:42	192.168.213.19	Business	Main device Search		Get the parent device	Success	2
admin	2020-09-29 14:19:42	192.168.213.19	Business	File	Download	Download personnel config	Success	1
admin	2020-09-29 14:19:42	192.168.213.19	System	User	User Login	User Login: admin	Success	34
admin	2020-09-29 14:15:03	192.168.213.19	Business	Main device Search		Get the parent device	Success	1
admin	2020-09-29 14:10:56	192.168.213.19	Business	Main device Search		Get the parent device	Success	2
admin	2020-09-29 14:08:47	0.0.0.0.0.0.1	System	User	User Login	User Login: admin	Success	48

- Step 3 Optional:** Export the logs from the system.

1. Click **Export**. The **Export** dialog box is displayed.
2. Set the file format in which logs are exported and the mode for exporting log records, as shown in [Figure 8-19](#).

Figure 8-19 Exporting logs



3. Click **OK**.

----End

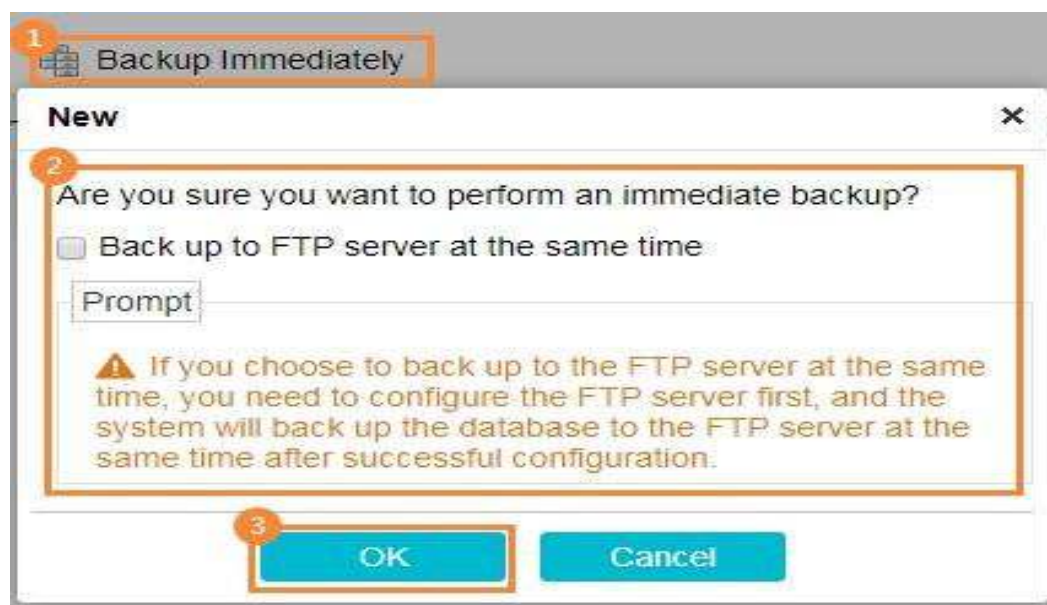
8.2.1.2 How Can I Back Up a Database?

This section describes the procedure for database backup on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Basic Management > Basic Management > Database Management**.
- Step 2** Click **Backup Immediately**. The **New** dialog box is displayed.
- Step 3** Complete related settings based on actual requirements, as shown in [Figure 8-20](#).

Figure 8-20 Backing up a database



Step 4 Click **OK**.

----End

8.2.1.3 How Can I Restore a Database?

This section describes the procedure for database restoration on the iClient S100.

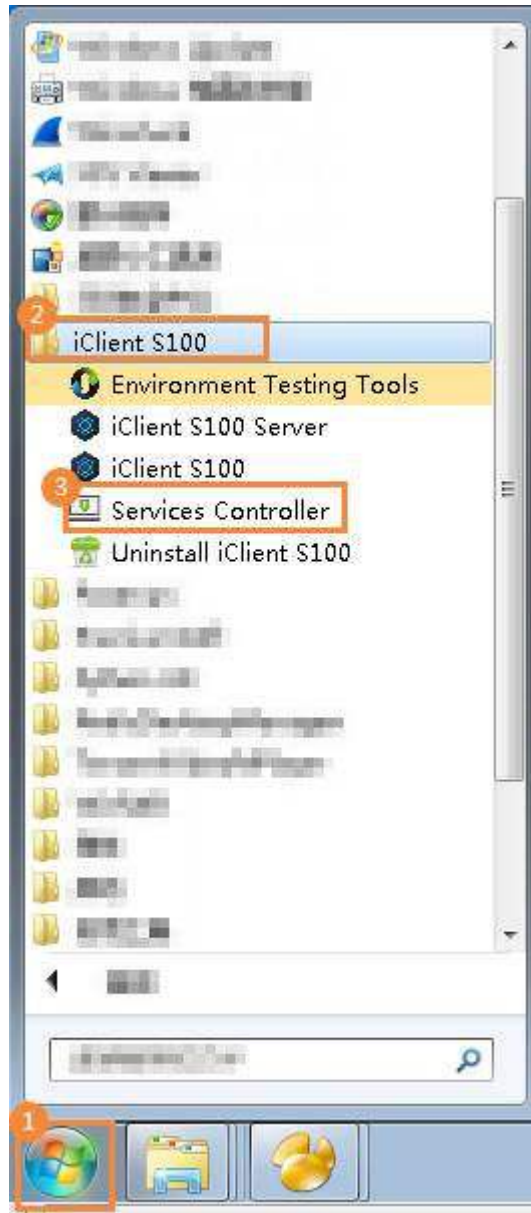
Prerequisites

- You have backed up the database, and the backup file has been stored on the local server. For details about the procedure for database backup, see [8.2.1.2 How Can I Back Up a Database?](#)
- The iClient S100 server has been started in running status.

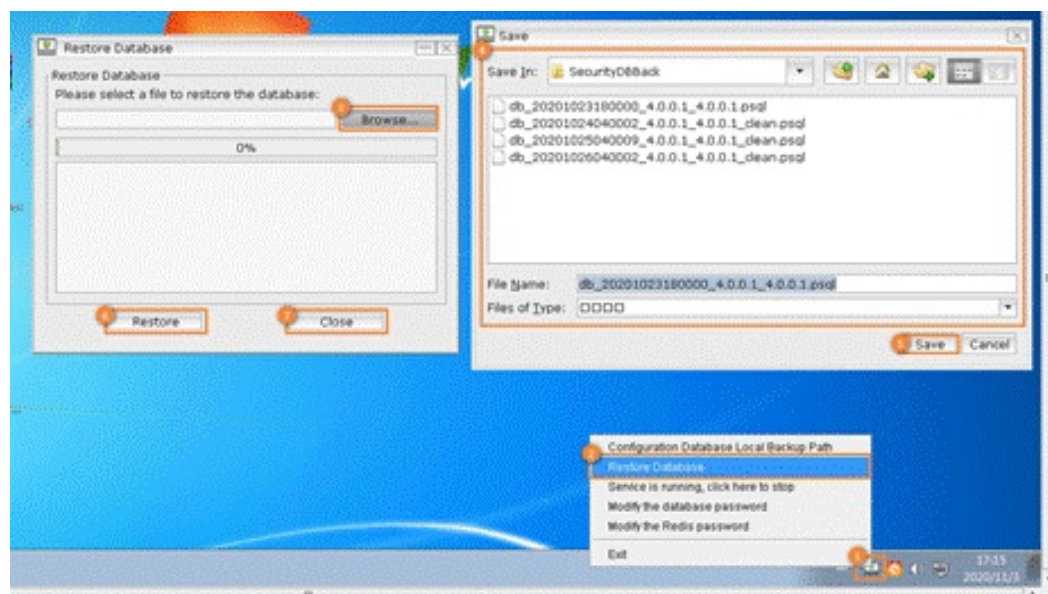
Procedure

- Step 1** In the lower left corner of the desktop of the computer where the iClient S100 is installed, click the Windows icon ("Start" menu) and choose **iClient S100 > Services Controller** to start the service console, as shown in [Figure 8-21](#).

Figure 8-21 Starting the service console



- Step 2** In the lower right corner of the Windows taskbar, right-click the service console icon and choose **Restore Database** from the displayed menu. The **Restore Database** dialog box is displayed, as shown in [Figure 8-22](#).

Figure 8-22 Restore Database

- Step 3** Click **Browse**. In the dialog box that is displayed, select the database backup file from the local path and click **Save**.
- Step 4** In the **Restore Database** dialog box, click **Restore**. The restoration progress is displayed.
- Step 5** Click **Close** after the restoration progress reaches 100%. Then, the iClient S100 server will be restarted. After the restart is complete, the database is restored.

----End

8.2.1.4 How Can I Set Up an Area?

This section describes the procedure for setting up an area on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Basic Management > Basic Management > Area Settings**.
- Step 2** Click **New**. The **New** dialog box is displayed.
- Step 3** Complete related settings based on actual requirements, as shown in [Figure 8-23](#).

Figure 8-23 Setting up an area

New [X]

If the new area failed to show in the area list, please contact the administrator to re-authorize the user to edit the area!

Area Number*

Area Name*

Parent Area* ▼

Remark

OK Cancel

Step 4 Click **OK**.

----End

8.2.1.5 How Can I Configure Support for Sending Emails?

This section describes the procedure for configuring support for sending emails on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Basic Management > Basic Management > E-mail Management**.
- Step 2** Click **Email Parameter Settings**. The **Email Parameter Settings** dialog box is displayed.
- Step 3** Complete related settings based on actual requirements, as shown in [Figure 8-24](#). [Table 8-6](#) describes the parameters.

Figure 8-24 Email Parameter Settings

Email Parameter Settings

1 Email Parameter Settings

Email Sending Server* (smtp.xxx.xxx)

Port* 25 ☐ SSL ☐ TLS

Email Account* (xxx@xxx.xxx)

Password*

Sender Name

2 Test Connection

3 OK Close

Table 8-6 Email parameters

Parameter	Description
Email Sending Server/ Port	IP address and port number of a mail server. You can set these two parameters based on the IP address and port number of an SMTP-based server provided by a mailbox. For details about related configurations, contact for the mailbox provider, such as Netease (163 Mail), Tencent (QQ Mail), and Foxmail.
Email Account/ Password	Email address and sign-in password.
Sender Name	Name of the sender involved in the email.

Step 4 After the setting is completed, click **Test Connection**. If an email is received by the preconfigured email account, the setting is successful.

Step 5 Click **OK**.

----End

8.2.2 Communication Management

8.2.2.1 How Can I View Records of Commands Issued by the Server?

This section describes the procedure for viewing and exporting records of commands issued by the server on the iClient S100.

Procedure

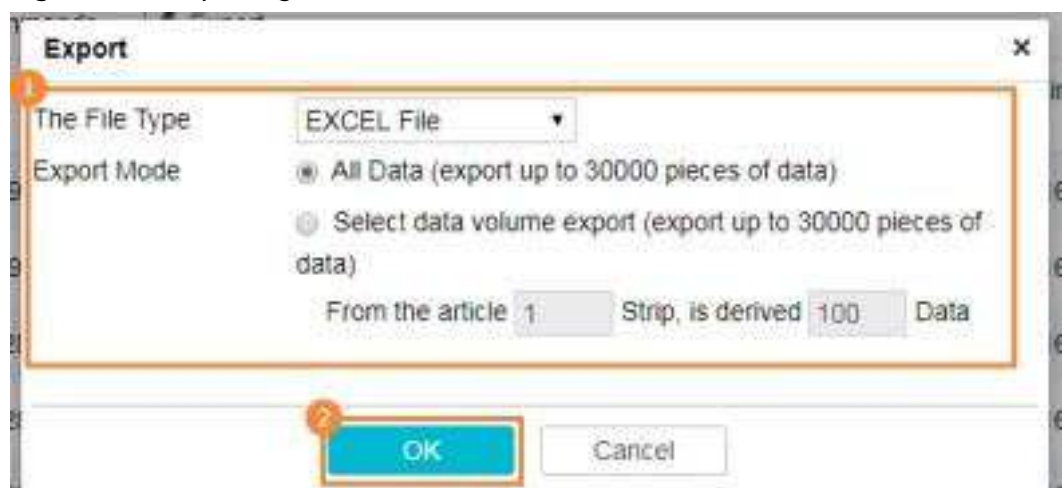
- Step 1** On the iClient S100 home page, choose **Basic Management > Communication > Device Commands**.
- Step 2** On the page that is displayed, view all issued server command records, or search for desired command records by criteria such as submission time period and serial number, as shown in [Figure 8-25](#).

Figure 8-25 Viewing command records

ID	Serial Number	Content	Immediate Cmd	Submit Time	Return Time	Returned Value
39	3547160700005	SET OPTIONS Door1MultiCardOpenDoor=0		2020-09-29 10:03:4	2020-09-29 10:03:50	
38	3547160700005	DATA DELETE multimcard *		2020-09-29 10:03:4	2020-09-29 10:03:50	
37	3547160700005	SET OPTIONS Door1MaskFlag=0		2020-09-29 10:03:4	2020-09-29 10:03:50	
36	3547160700005	SET OPTIONS UserWithMulCardOn=1		2020-09-29 10:03:4	2020-09-29 10:03:50	
35	3547160700005	DATA UPDATE CardFormat CardBit=34 SiteCode=0 FmtName=		2020-09-29 10:03:4	2020-09-29 10:03:50	
34	3547160700005	DATA DELETE CardFormat *		2020-09-29 10:03:4	2020-09-29 10:03:50	
33	3547160700005	SET OPTIONS WGFmtWithSitecodeOn=1		2020-09-29 10:03:4	2020-09-29 10:03:50	
32	3547160700005	SET OPTIONS DateTime=666698529		2020-09-29 10:03:4	2020-09-29 10:03:50	
31	3547160700005	SET OPTIONS MachineTZ=+0800		2020-09-29 10:03:4	2020-09-29 10:03:50	
30	3547160700005	DATA DELETE holiday *		2020-09-29 10:03:4	2020-09-29 10:03:50	
29	3547160700005	DATA UPDATE timezone TimezoneId=1 SunTime1=2359 SunTi		2020-09-29 10:03:4	2020-09-29 10:03:50	

- Step 3** (Optional) Export records of commands issued by the server.
1. Click **Export**. The **Export** dialog box is displayed.
 2. Set the file format in which records are exported and the mode for exporting records, as shown in [Figure 8-26](#).

Figure 8-26 Exporting command records



3. Click **OK**.

----End

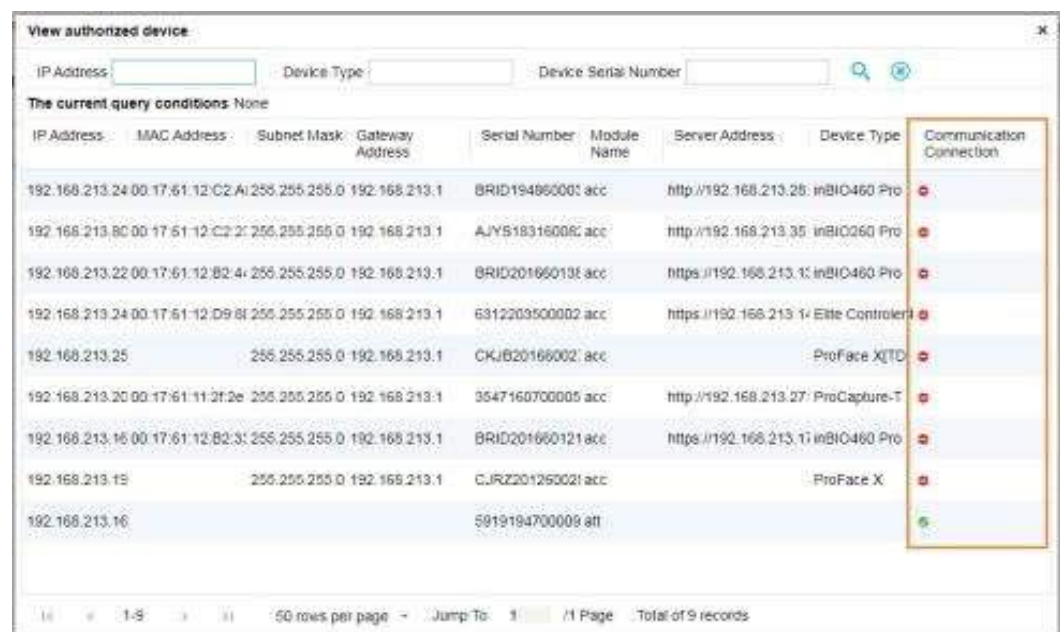
8.2.2.2 How Can I Check Communication Status of Devices Added to the iClient S100?

This section describes the procedure for checking communication status of added devices on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Basic Management > Communication > Communication Device**.
- Step 2** Click **View authorized device**. On the **View authorized device** page that is displayed, obtain current communication status of devices in the **Communication Connection** column, as shown in [Figure 8-27](#).

Figure 8-27 Viewing authorized devices



The screenshot shows a web interface titled "View authorized device". It contains a search bar with fields for IP Address, Device Type, and Device Serial Number. Below the search bar, it says "The current query conditions: None". A table lists authorized devices with columns: IP Address, MAC Address, Subnet Mask, Gateway Address, Serial Number, Module Name, Server Address, Device Type, and Communication Connection. The Communication Connection column shows status icons (red for disconnected, green for connected). At the bottom, there is a pagination bar showing "50 rows per page", "Jump To: 1 / 1 Page", and "Total of 9 records".

IP Address	MAC Address	Subnet Mask	Gateway Address	Serial Number	Module Name	Server Address	Device Type	Communication Connection
192.168.213.24	00:17:61:12:C2:A1	255.255.255.0	192.168.213.1	BRID194860001	acc	http://192.168.213.25	inBIO460 Pro	Disconnected
192.168.213.80	00:17:61:12:C2:21	255.255.255.0	192.168.213.1	AJY518316008	acc	http://192.168.213.35	inBIO260 Pro	Disconnected
192.168.213.22	00:17:61:12:82:41	255.255.255.0	192.168.213.1	BRID201660131	acc	https://192.168.213.11	inBIO460 Pro	Disconnected
192.168.213.24	00:17:61:12:D9:81	255.255.255.0	192.168.213.1	6312203500002	acc	https://192.168.213.14	Elite Controler	Disconnected
192.168.213.25		255.255.255.0	192.168.213.1	CKJB201660002	acc		ProFace X(TD	Disconnected
192.168.213.20	00:17:61:11:2F:2e	255.255.255.0	192.168.213.1	9547160700005	acc	http://192.168.213.27	ProCapture-T	Disconnected
192.168.213.16	00:17:61:12:82:31	255.255.255.0	192.168.213.1	BRID201660121	acc	https://192.168.213.11	inBIO460 Pro	Disconnected
192.168.213.15		255.255.255.0	192.168.213.1	CJRW201250001	acc		ProFace X	Disconnected
192.168.213.16				5919194700009	att			Connected

----End

8.2.2.3 How Can I Check Communication Status of the Server?

This section describes the procedure for checking communication status of the server on the iClient S100.

Procedure

- Step 1** Choose **Basic Management > Communication > Communication Monitor** on the iClient S100 home page.
- Step 2** On the page that is displayed, check current communication status of the server, as shown in [Figure 8-28](#).

Figure 8-28 Checking current communication status of the server

----End

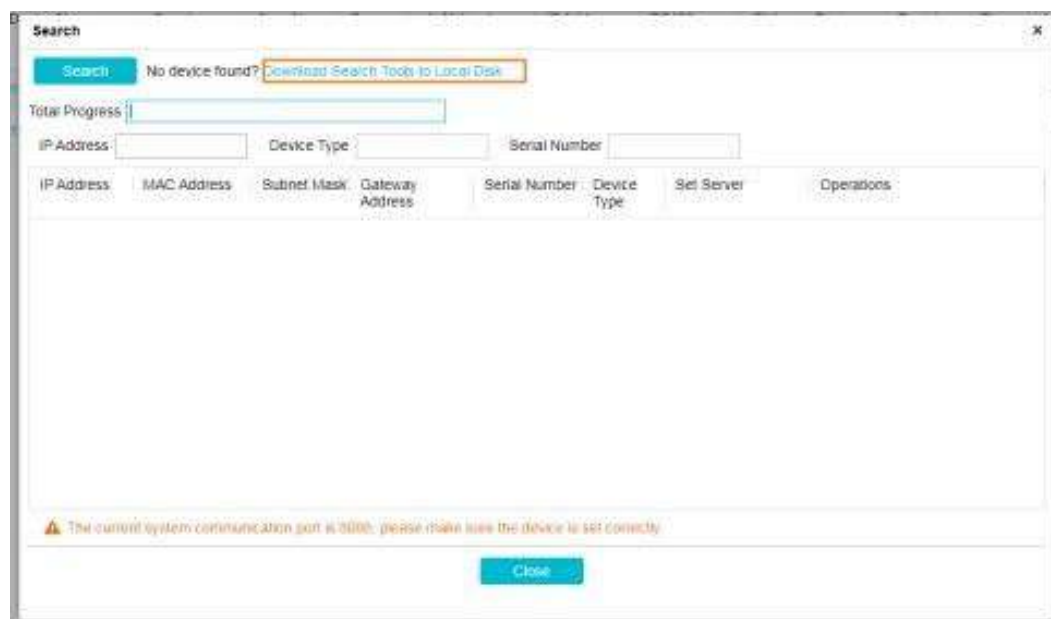
8.2.3 Device Addition

8.2.3.1 How Can I Set or Change the IP Address of an Access Control Device Using a Tool?

This section describes the procedure for setting or changing the IP address of an access control device before adding the device to the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Access > Device > Device**.
- Step 2** On the page for device management, click **Search**. On the **Search** page that is displayed, click **Download Search Tools to Local Disk**, as shown in [Figure 8-29](#).

Figure 8-29 Downloading search tools

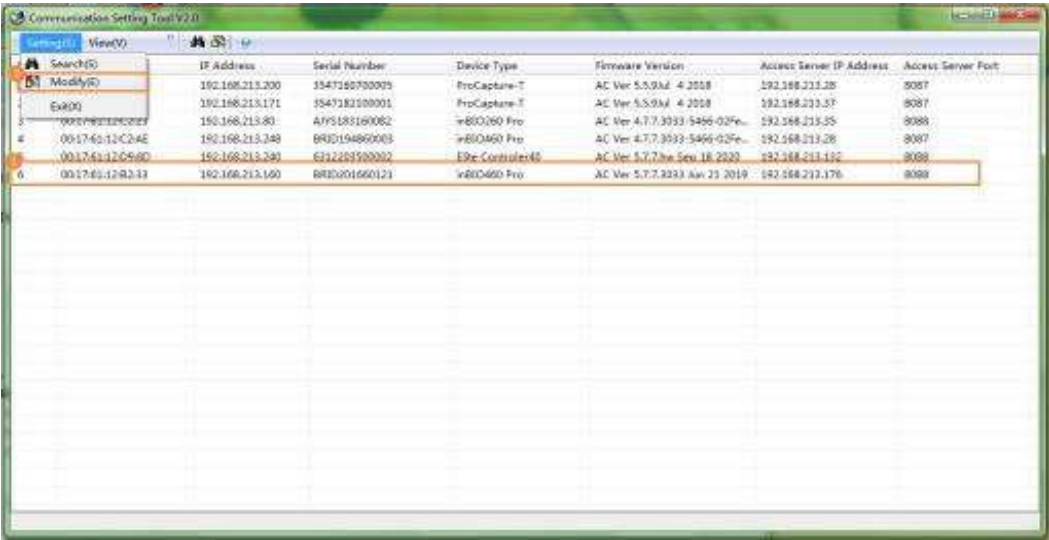
- Step 3** After the download is complete, find the **deviceSetting Tool.exe** file in the local path. [Figure 8-30](#) shows the icon of the file.

Figure 8-30 deviceSetting Tool.exe

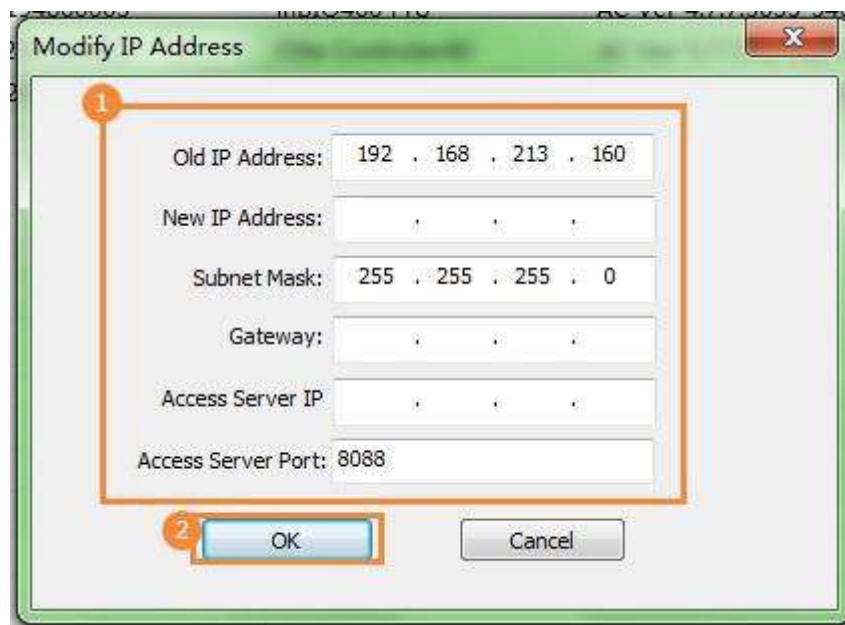


- Step 4** Double-click the **deviceSetting Tool.exe** file to run the tool and click  for device search. The list of devices in the local network is displayed.
- Step 5** Click a device whose IP address needs to be changed, click the **Settings** tab in the upper right corner of the page, and choose **Modify** in the drop-down list, as shown in [Figure 8-31](#).

Figure 8-31 Modifying parameters for device communication



- Step 6** In the **Modify IP Address** dialog box, complete related settings based on the requirements, as shown in [Figure 8-32](#).

Figure 8-32 Modify IP Address

Step 7 Click **OK**.

Step 8 Optional: Repeat the preceding operations for other devices if needed and close the tool. The IP address change is completed.

-----End

8.2.4 Tablet Source Management

8.2.4.1 How Can I Customize the Image Display of Specific Pages on a Tablet Device?

Tablet devices support the image display customization of specific pages. To implement this function, you need to add and allocate related resources.

8.2.4.1.1 Resource Addition

This section describes the procedure for adding a resource on the iClient S100.

Procedure

Step 1 On the iClient S100 home page, choose **Access > Pad related > Resource**.

Step 2 Click **New**. The **New** dialog box is displayed.

Step 3 Complete related settings based on actual requirements, as shown in [Figure 8-33](#). [Table 8-7](#) describes the parameters.

Figure 8-33 Adding a resource

Table 8-7 Parameters for adding a resource

Parameter	Setting
Resource Name	Customize the name of a resource.
Resource Type	Set Resource Type to Image .
Resource Type Name	Set Resource Type Name to a desired page to which the image resource is applied. The options are as follows: Startup Screen , Welcome Page , Screensaver Page , and Disable Page .
File Upload	Click Browse and select an image file that has been stored from the local path. The image must be in .png format, and the size must be 800 x 1280 pixels.

Step 4 Click **OK**.

----End

8.2.4.1.2 Resource Allocation

This section describes the procedure for allocating added resources on the iClient S100.

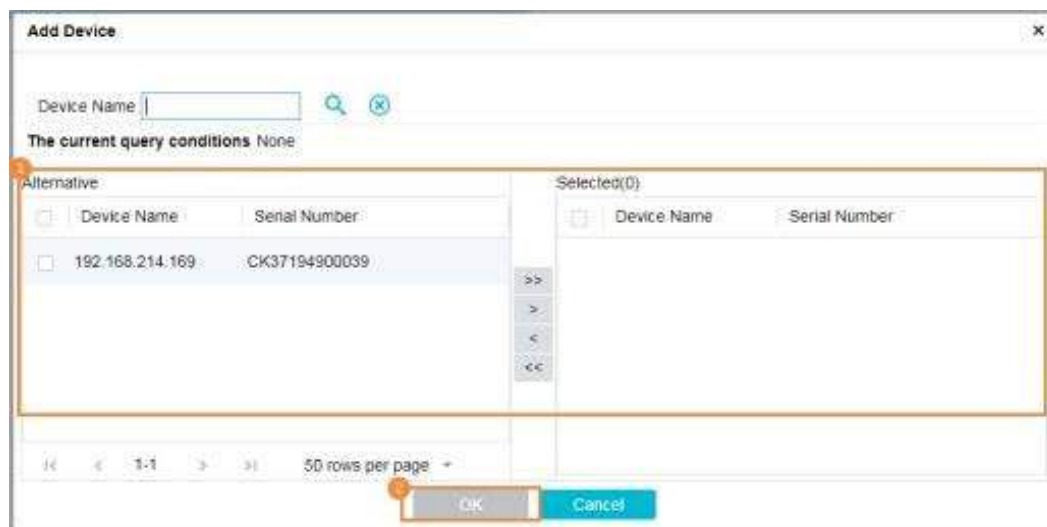
Procedure (Set by Resource)

Step 1 On the iClient S100 home page, choose **Access > Pad related > Set By Resource**.

Step 2 On the page that is displayed, add devices in the operation column.

- Step 3** On the page that is displayed for device addition, select desired devices to which resources are allocated, as shown in [Figure 8-34](#).

Figure 8-34 Adding devices



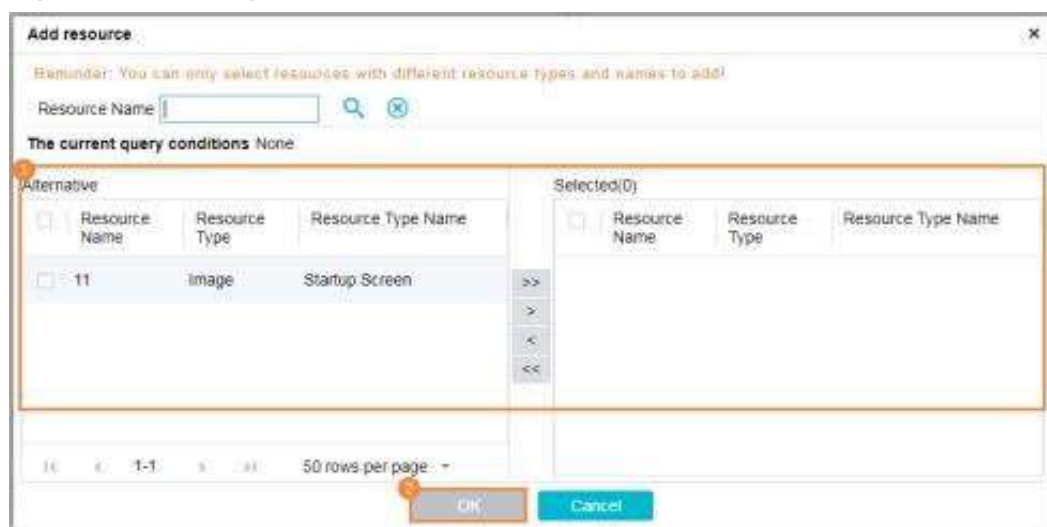
- Step 4** Click **OK**.

----End

Procedure (Set by Device)

- Step 1** On the iClient S100 home page, choose **Access > Pad related > Set By Device**.
- Step 2** On the page that is displayed, add resources in the operation column.
- Step 3** On the page that is displayed for resource addition, select resources required by devices, as shown in [Figure 8-35](#).

Figure 8-35 Adding resources



- Step 4** Click **OK**.

----End

8.2.4.2 How Can I Set a Customized Message Prompting an Event to Occur on a Tablet Device?

Tablet devices support the customization of messages that prompt device events to occur. To implement this function, you need to add and allocate related resources.

8.2.4.2.1 Resource Addition

This section describes the procedure for adding a resource on the iClient S100.

Procedure

- Step 1** On the iClient S100 home page, choose **Access > Pad related > Resource**.
- Step 2** Click **New**. The **New** dialog box is displayed.
- Step 3** Complete related settings based on actual requirements, as shown in [Figure 8-36](#). [Table 8-8](#) describes the parameters.

Figure 8-36 Adding a resource

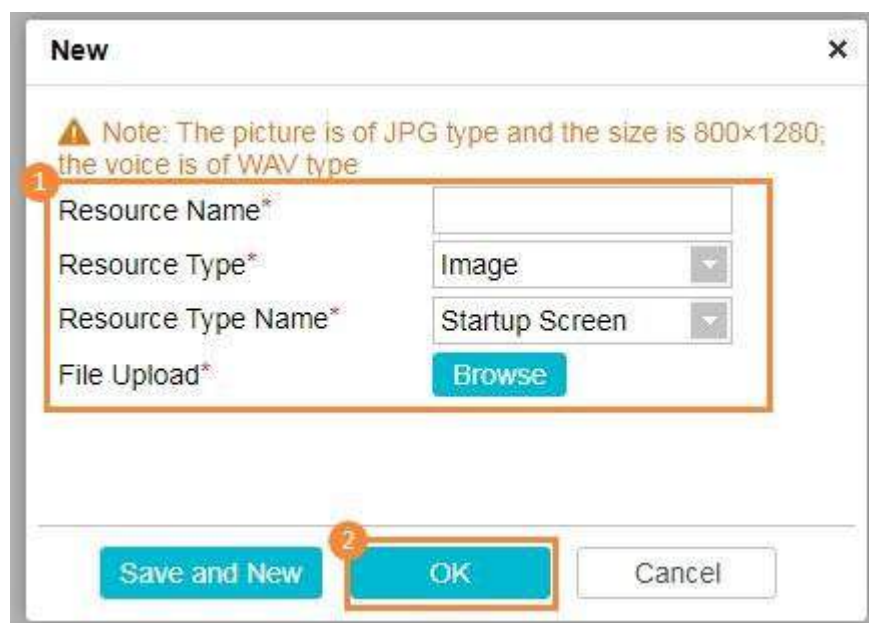


Table 8-8 Parameters for adding a resource

Parameter	Setting
Resource Name	Customize the name of a resource.
Resource Type	Set Resource Type to Voice or Text .

Parameter	Setting
Resource Type Name	Set Resource Type Name to an event to which an audio or a text resource is applied to notify the event occurrence. The options are as follows: Successful Comparison , Illegal Time , Personnel Not Registered , Personnel Not Authorized , System Service Exception (text resource only), target Comparison Failed (text resource only), and target Similarity Not Standard (text resource only).
File Upload/Hint	• Voice: Click Browse and select a stored WAV audio file from the local path. • Hint: Enter the message content to be displayed when an event occurs.

Step 4 Click **OK**.

----End

8.2.4.2.2 Resource Allocation

This section describes the procedure for allocating added resources on the iClient S100.

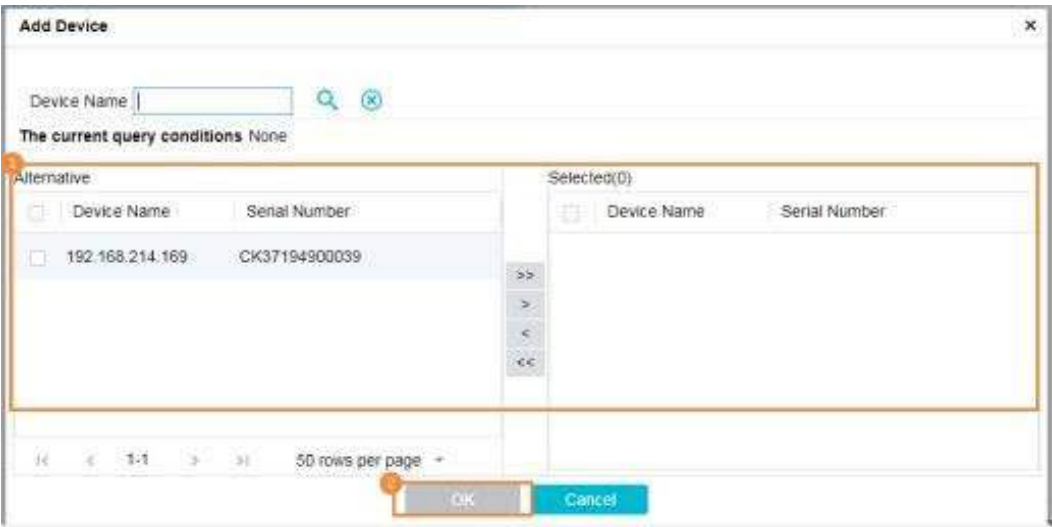
Procedure (Set by Resource)

Step 1 On the iClient S100 home page, choose **Access > Pad related > Set By Resource**.

Step 2 On the page that is displayed, add devices in the operation column.

Step 3 On the page that is displayed for device addition, select desired devices to which resources are allocated, as shown in [Figure 8-37](#).

Figure 8-37 Adding devices



Step 4 Click OK.

----End

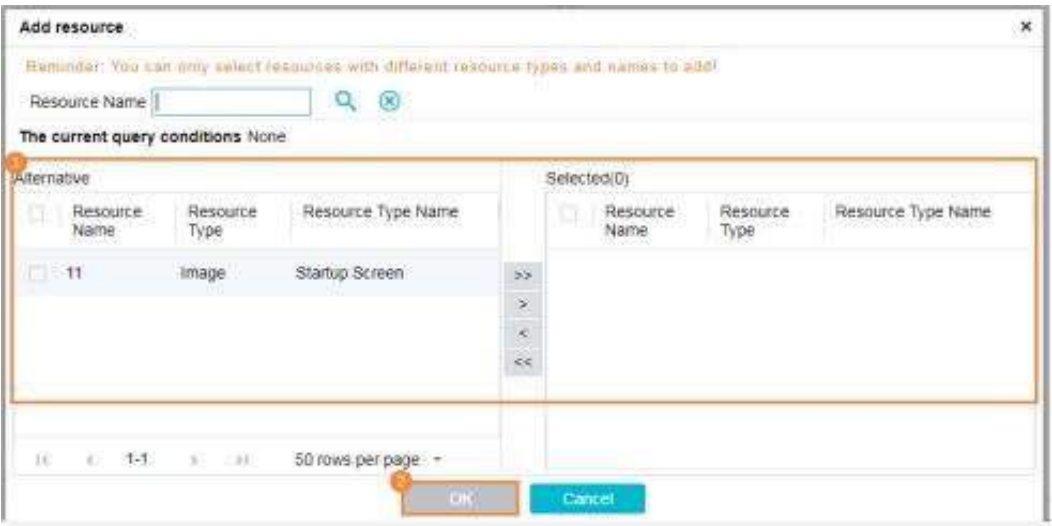
Procedure (Set by Device)

Step 1 On the iClient S100 home page, choose **Access > Pad related > Set By Device**.

Step 2 On the page that is displayed, add resources in the operation column.

Step 3 On the page that is displayed for resource addition, select resources required by devices, as shown in [Figure 8-38](#).

Figure 8-38 Adding resources



Step 4 Click OK.

----End

8.2.5 Person Addition

8.2.5.1 How Can I Add Person Information on a Device?

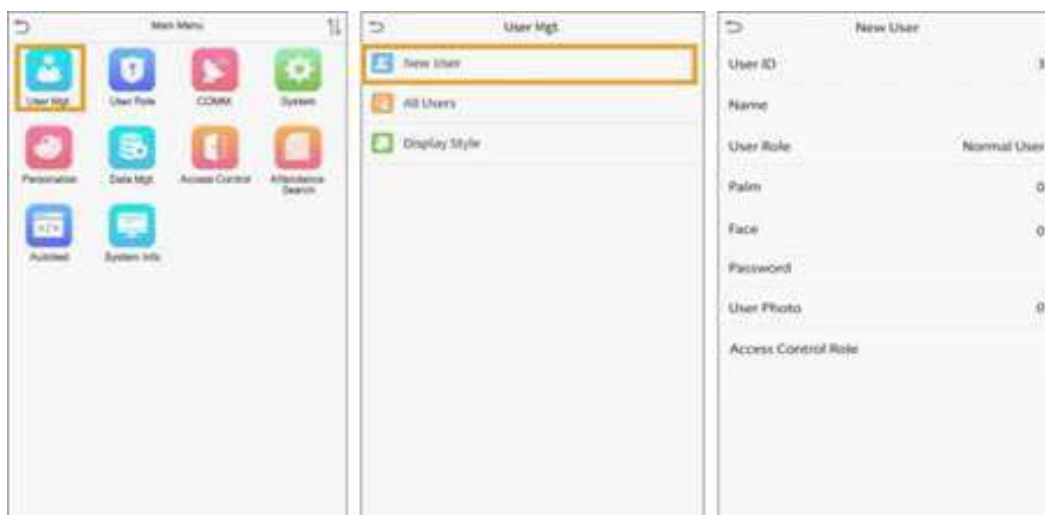
In addition to adding person information on the iClient S100, you can also directly add person information on device, for example, access control tablets.

This section uses the access control tablet as an example to describe the procedure for adding person information.

Procedure

- Step 1** On the home page of an access control device, tap . The main menu page is displayed.
- Step 2** On the main menu, tap **User Mgt. > New User**. The page for adding users is displayed.
- Step 3** Complete related settings for adding users based on the actual requirements, as shown in [Figure 8-39](#).

Figure 8-39 New User



- Step 4** Tap  to return to the previous page. Person information addition is completed.
- End

9 Troubleshooting

[9.1 Client](#)

[9.2 Video Devices](#)

[9.3 Basic Operations](#)

[9.4 Intelligent Applications](#)

[9.5 Comprehensive Services](#)

9.1 Client

9.1.1 Login Fails After the iClient S100 Is Installed

Symptom

After the iClient S100 is installed, login to the iClient S100 fails.

Possible Causes

The iClient S100 is installed in **Client** mode, but the server IP address is set to the local IP address **127.0.0.1** for login.

The process of the iClient S100 server that you want to log in to from the iClient S100 is not started.

Solution

- Step 1** Check whether the iClient S100 installation mode complies with the application scenario. For details about the installation modes and scenarios, see [Table 9-1](#).

Table 9-1 Installation modes

Installation Mode	Scenario and Restrictions
Server+Client	- One iClient S100 server must be installed in an iClient S100 system. - When only one client is required for service configuration and operations, you only need to complete the installation in this mode. - In this mode, you can enter the local IP address 127.0.0.1 to log in to the local iClient S100 server, or enter the IP address of another iClient S100 server to log in to that server.
Client	- To configure and operate multiple clients, you need to install the iClient S100 in Server+Client mode on the local computer and install it in Client mode on other computers. - Currently, an iClient S100 server can connect to a maximum of 16 clients (including the clients installed on the computer in Server+Client mode). - To log in this mode, enter the IP address of the computer where the server is located.

- If the **Server+Client** mode is used, go to [Step 2](#).
- If the **Client** mode is used, go to [Step 3](#).

Step 2 Check whether the server IP address entered for login is correct in the **Server+Client** mode.

To log in to the local server, enter the local IP address **127.0.0.1**. To log in to the other servers, enter the IP addresses of the computers where the servers are located.

- If the server IP address is incorrect, enter a correct one and log in again.
- If the server IP address is correct, wait for about 2 minutes until all services start after the software is installed on the server.

Step 3 Check whether the server IP address entered for login is correct in the **Client** mode.

Ensure that the server IP address must be the IP address of the computer where the client installed in **Server+Client** mode is located.

- If the server IP address is incorrect, enter a correct one and log in again.
- If the server IP address is correct, wait for about 2 minutes until all services start after the software is installed on the server.

Step 4 Check whether the login is successful. If so, no further action is required. If not, contact technical support.

----End

9.1.2 An Error Message Is Displayed During Login to the iClient S100

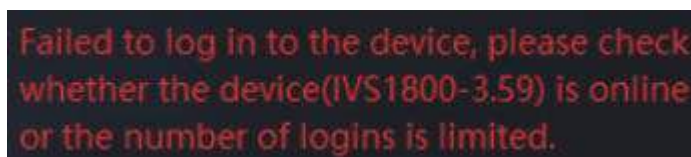
NOTE

This problem occurs only when the version of the iClient S100 is earlier than V1.3.0 and the IVS1800 8.1.0 is used.

Symptom

An error message shown in [Figure 9-1](#) is displayed during login to the iClient S100.

Figure 9-1 Device login failure



Possible Causes

The IVS1800 is offline or disconnected from the computer where the iClient S100 client is located.

The number of concurrent logins using an account for adding the IVS1800, has reached the upper limit.

Solution

- Step 1** Verify that the IVS1800 mentioned in the error message is online, and that the computer where the iClient S100 client is located is properly connected to the IVS1800. Then log in to the iClient S100 client again.
- Step 2** If the login still fails, check whether the IVS1800 is added to other iClient S100 servers on the LAN or whether the **admin** user has logged in to the web client of the IVS1800 using a browser. Ensure that the **admin** account of the IVS1800 is idle, and then log in again.

NOTE

The **admin** account supports one concurrent login for adding the IVS1800 by default. If the number of concurrent logins using the **admin** account has reached the upper limit, the **admin** account cannot be used to add the IVS1800 to the iClient S100 server.

- Step 3** After the re-login is successful, create a system administrator account on the IVS1800 and set the number of concurrent logins using this account to a value greater than five, to avoid this error.

-----End

9.1.3 File Loss Error Displayed When Running the iClient S100 Client

Symptom

When you run the iClient S100 client, an error message is displayed, indicating that the **VCRUNTIME140_1.dll** or **opencv_world348.dll** file cannot be found.

Possible Causes

The **VCRUNTIME140_1.dll** or **opencv_world348.dll** file is lost.

The iClient S100 client version is outdated.

Solution

Upgrade the iClient S100 client to V1.2.0 or a later version.

Manually install **vc_redist.x64.exe**, which can be obtained from the Microsoft technical support website for free.

9.1.4 iClient S100 Server Fails to Be Started

Symptom

After you log in to the iClient S100, a message is frequently displayed, indicating that the server does not respond or is starting and asking you to try again 1 minute later.

Possible Causes

On the iClient S100 of a version earlier than V1.1.2, the disk where the installation directory is located may be used up by cached snapshots, causing service process startup failure.

Solution

Check whether the disk where the installation directory is located is used up by snapshots. If so, install the software of the latest version. The cached snapshots will be automatically deleted when the iClient S100 starts.

9.1.5 Login to the iClient S100 Server Fails Occasionally After the Computer Where the iClient S100 Server Is Located Restarts Unexpectedly

Symptom

After the computer where the iClient S100 server is located restarts unexpectedly, the login to the iClient S100 fails and the message is continuously displayed, indicating that the iClient S100 service is being started. In the system services, it is

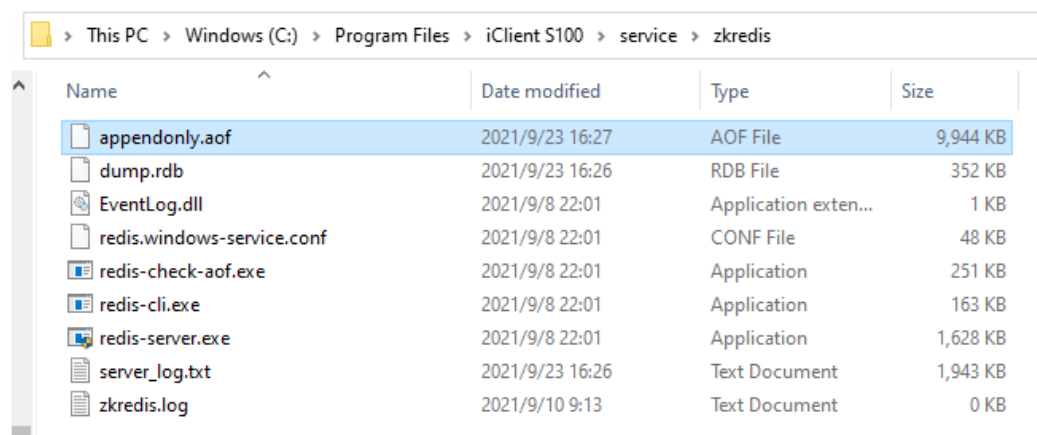
found that the cache service of the iClient S100 is stopped and cannot be restarted manually.

Possible Causes

The unexpected restart of the computer may corrupt the cache service of the iClient S100. As a result, the service cannot be started.

Solution

1. Delete the iClient S100 cache file **appendonly.aof** under **iClient S100 installation directory\service\zkredis**.



2. Restart the cache and core services of the iClient S100. After the services are restarted, log in to the iClient S100 again.

9.1.6 The iClient S100 Suddenly Shuts Down During Service Running and Fails to Be Re-logged in

Symptom

The iClient S100 suddenly shuts down during service running and fails to be re-logged in.

Possible Causes

The database backup occupies a large amount of storage space. As a result, the space of the disk where the iClient S100 stores data (or where the iClient S100 installation directory is located) is almost used up. Logs need to be written during the running of the iClient S100. However, services cannot run due to insufficient disk space.

Solution

1. It is recommended that the disk for storing manually downloaded recordings and manually captured images be different from the disk where the iClient S100 installation directory is located. In addition, you are advised to periodically delete historical recordings.
2. For the iClient S100, the database is automatically backed up by default, and the backed-up database files are stored for six months by default. You are

advised to change the database file storage duration under **Home > Basic Management > Data Clearance > Database backup files** depending on your needs.

9.1.7 A Specific Recording Can Be Played Back on a Client But Cannot Be Played on the Other Client

Symptom

When you log in to two iClient S100 clients to play back a specific recording, one can properly play back the recording but the other cannot.

Possible Causes

To play back a recording from a device, you must specify the start time and end time on the client. If the time zone where an iClient S100 client is located is different from that where the IVS1800 and NVR800 device is located, the recording time range sent from the iClient S100 client to the device will fail to be parsed by the device, leading to the recording playback anomalies on the client.

Solution

Before site deployment, synchronize the time zone and time settings of the iClient S100 client with those of the NVR800 and IVS1800 by referring to [8.1.2.3 How Do I Set the System Time and Time Zone?](#)

9.1.8 The iClient S100 Fails to Receive Messages (Such as Alarms) from the IVS1800 Due to the Change of the IP Address of the Computer Where the iClient S100 Server Is Located

Symptom

The IP address of the computer where the iClient S100 server is located changes. As a result, messages (such as alarms) from the IVS1800 cannot be received by the iClient S100.

Possible Causes

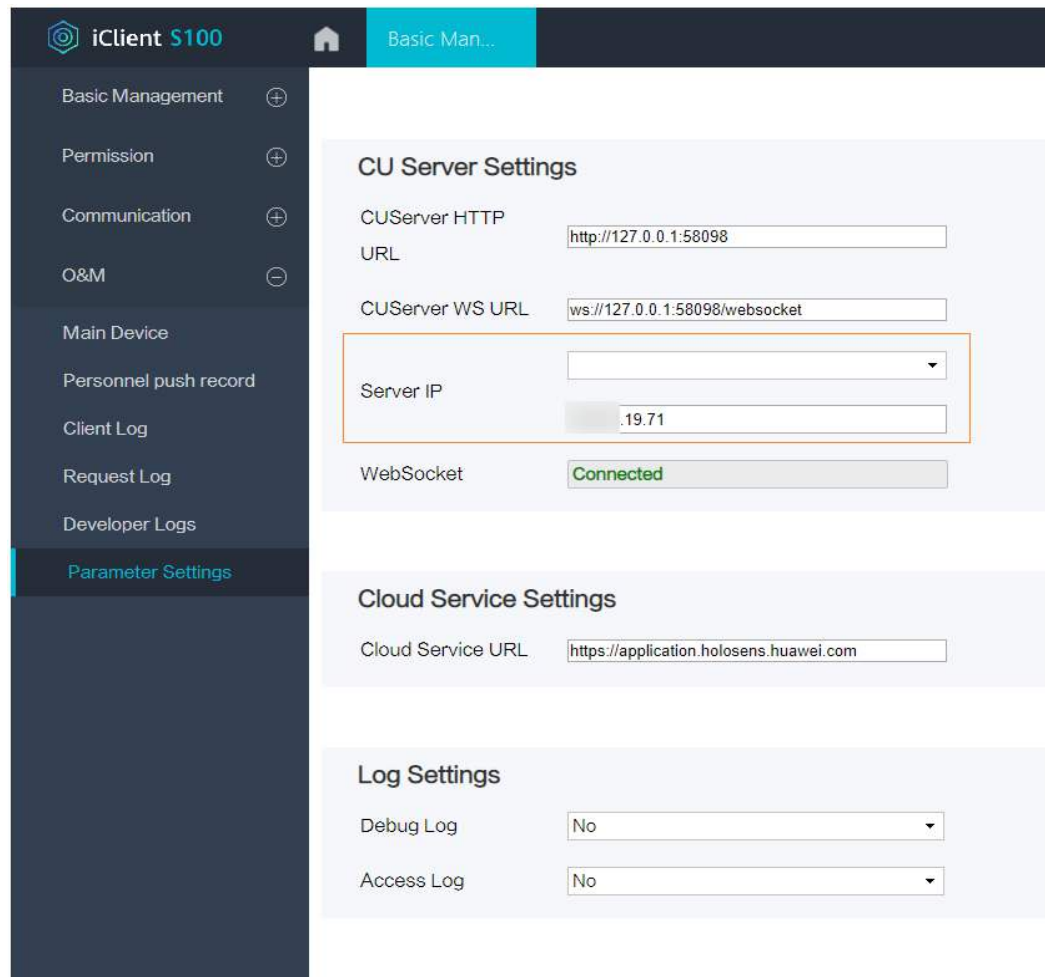
Messages including IVS1800 alarms and camera search results, are proactively sent from the IVS1800 to the iClient S100 server through the subscription channel. After the IP address of the computer where the iClient S100 server is located changes, the IVS1800 still pushes messages to the original IP address of the iClient S100. Consequently, the iClient S100 cannot receive the messages.

Solution

The iClient S100 server requires a fixed IP address instead of the DHCP floating IP address. When the iClient S100 server IP address changes, you need to change the server IP address under **Maintenance Management > Basic Management >**

O&M > Parameter Settings on the iClient S100, as shown in [Figure 9-2](#), to request a new subscription.

Figure 9-2 Changing the IP address of the server

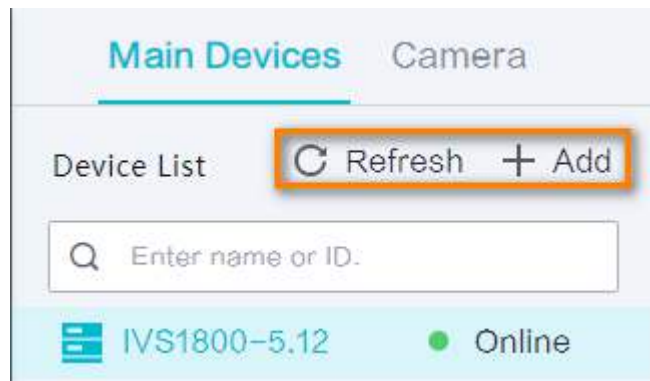


9.2 Video Devices

9.2.1 No Refresh and Add Buttons in the Device List

Symptom

The **Refresh** and **Add** buttons are not displayed in the device list on the client.



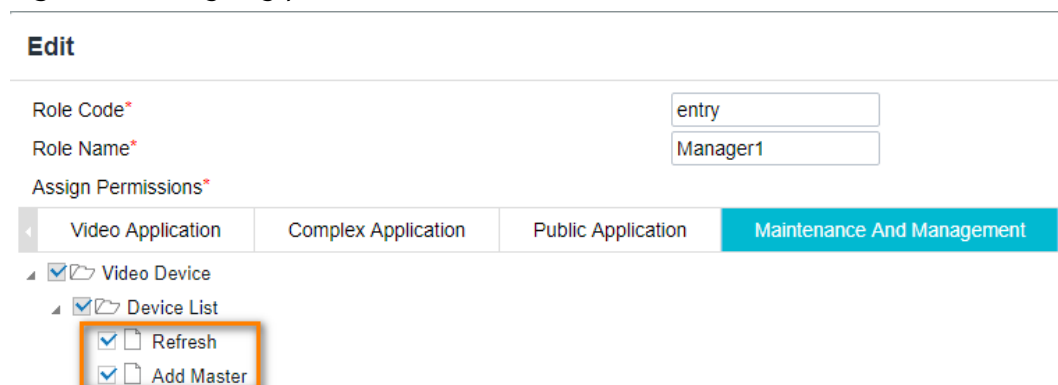
Possible Causes

The function permissions of the iClient S100 whose version is V1.2.0 and later is refined. After the iClient S100 is upgraded to V1.2.0 or a later version, non-administrator accounts created in versions earlier than V1.2.0 do not have permissions of adding and refreshing main devices.

Solution

Choose **Basic Management > Authority Management > Role**, click **Edit** in the **Operations** column corresponding to the current role, and add permissions for adding and refreshing main devices to the role, as shown in [Figure 9-3](#). After the configuration is complete, log out and then log in to the client again using the account with this role.

Figure 9-3 Assigning permissions



9.2.2 Failure to Connect an IVS1800/NVR800 to the iClient S100

Symptom

The connection of an IVS1800/NVR800 to the iClient S100 fails and **connect timed out** is displayed.

Possible Cause

During the iClient S100 installation, the antivirus software of the computer blocks the installation of the iClient S100 CU server, which is responsible for signaling

exchanges with devices such as the NVR800 and IVS1800. As a result, signaling exchanges between the iClient S100 and devices are abnormal.

Solution

Close the antivirus software installed on the PC or delivered with the Windows operating system, and reinstall the iClient S100.

After the installation is complete, enable the antivirus software in a timely manner to ensure security.

9.2.3 After You Connect Cameras to a Registered IVS1800 on the iClient S100, None of the Cameras Is Displayed; When You Connect Them Again, a Message Is Displayed Indicating Connection Failure Due to Duplicate IP Addresses

Symptom

After you connect cameras to a registered IVS1800 on the iClient S100, none of the cameras is displayed under **Maintenance Management > Video Device > Device List > Main Devices**; when you connect them again, a message is displayed indicating connection failure due to duplicate IP addresses.

Possible Causes

1. On the iClient S100 earlier than V1.2.0, cameras that fail to be connected to the IVS1800 (due to incorrect passwords or other causes) are not displayed in the camera list. On the iClient S100 of V1.2.0 and later versions, cameras are displayed in the camera list even when they fail to be connected.
2. The user account used to register the iClient S100 with the IVS1800 has no permission on the cameras to be added.

Solution

- Step 1** Log in to the OMU portal of the IVS1800 and select the required cameras in the **Assign View Permission** area, as shown in [Figure 9-4](#).

Figure 9-4 Set Permission

Set Permission

Multi-point Logins

32

PTZ Control Priority

1

▼

Validity Period

☐

Deselecting this item will cause security risks.

Description

Save

Assign View Permission

☒ DeviceName

☒ .5.17

☒ .5.108

☒ .5.160

☒ .5.167

☒ .5.208

☒ .5.206

☒ .5.168

☒ .5.205

☒ .5.2050102

☒ .5.102

☒ .5.188

Step 2 Select **View All Devices** when creating the user account, as shown in [Figure 9-5](#).

Figure 9-5 Selecting View All Devices when creating the user account

Add User

*Role

▼

*User Name

*Password

Enter password.

Weak

Medium

Strong

*Confirm Password

Enter password again.

*Multi-point Logins

1

An integer from 1 to 32.

*PTZ Control Priority

1

▼

An integer from 1 to 32 in descending order of priority.

Validity Period

☐

Deselecting this item will cause security risks.

View All Devices

☒

Description

Save

----End

2022-09-27

645

9.2.4 When You Attempt to Connect or Log In to an NVR800 on the iClient S100, a Message Is Displayed Indicating that the Account Has Logged In Elsewhere

Symptom

When you attempt to connect or log in to an NVR800 on the iClient S100, a message is displayed indicating that the account has logged in elsewhere.

Possible Causes

An NVR800 account can log in to either the iClient S100 or the NVR800 web system at the same time.

Solution

Enable the **apiadmin** account in the NVR800. Use this account to connect to the NVR800 on the iClient S100, and use another account to log in to the NVR800 on the NVR800 web system.

9.2.5 After an IVS1800 Is Upgraded Through Reinstallation, Some of Its Functions Are Unavailable on the iClient S100

Symptom

After an IVS1800 is upgraded through reinstallation, some of its functions are unavailable on the iClient S100. For example, video and audio channels fail to be obtained, backend analysis tasks fail to be created, and historical alarms reported by the IVS1800 fail to be found.

Possible Causes

Before being reinstalled, the IVS1800 has been connected to the iClient S100 and its device code has been stored in the **Store Code** field in the iClient S100 database. After the IVS1800 is reinstalled, the storage code of the IVS1800 is changed.

When the iClient S100 invokes the IVS1800 intertarget, the value of **Store Code** (device code) stored in the database is carried. The intertarget invoking fails due to inconsistency between the device code and storage code.

Solution

- Step 1** Among the IVS1800 devices connected to the iClient S100, right-click the IVS1800 that functions improperly and select **View Information** from the shortcut menu. In the **View Information** dialog box that is displayed, check whether the storage code is the same as the device code. If not, go to the next step.

View Information		×
Device Name	IVS1800	
Model	IVS1800	
AI Power	16T	
Max Channels	16	
Version	9.1.RC1	
Store Code	b42	:85
Device Code	9ef4	3e
IP		5.33

Step 2 After reinstalling the IVS1800, delete it and then connect it again on the iClient S100.

 CAUTION

You are advised to upgrade the IVS1800 on the OMU portal. In this case, the device code of the IVS1800 will not be changed.

----End

9.3 Basic Operations

9.3.1 Video from an IVS1800/NVR800 Pushed to the Video Wall Through the iClient S100 Is Abnormal

Symptom

- The video from an IVS1800/NVR800 is pushed to the video wall through the iClient S100 successfully. However, the video display becomes abnormal after several days.
- After the camera is powered off and restarted, the decoder fails to decode video and no video is displayed on the video wall.

Possible Causes

The IVS1800/NVR800 directly pushes video streams to the decoder without passing through the iClient S100 server. After the camera is restarted or the network is disconnected, the token for transferring media streams from the IVS1800/NVR800 to the decoder becomes invalid.

Solution

- If an NVR800 is connected, send the user name, password, and URLs to the decoder. After the token expires, the decoder obtains streams again. For iClient S100 V1.2.1 and earlier versions, you can upgrade the client to solve

this problem. This problem has been resolved in iClient S100 V1.2.2 and later versions.

- If an IVS1800 is connected, log in to the OMU portal of the IVS1800, choose **System > Advanced Configuration**, select **MU** from the **Module** drop-down list box, and set **IsConstantUrl** to **1** to enable static URL, as shown in [Figure 9-6](#).

Figure 9-6 Enabling static URL

[illegible]

9.3.2 The Intelligent Overlay Function on the Live Video Viewing Page and Regular Customer Detection Are Unavailable After an NVR800 Is Connected to the iClient S100

Only the NVR800 of 9.X and later versions support intelligent data overlay on the live video viewing page of cameras connected to the NVR800 and regular customer detection.

9.3.3 Video Streams Are Interrupted and Then Being Reconnected When You Attempt to View Live Video from Cameras Connected to an NVR800 or IVS1800 on Multiple Clients

Symptom

When you attempt to play live video from cameras connected to an NVR800 or IVS1800 on some clients concurrently, the playing is normal on the clients that first request the live stream and fails on other clients. On the clients where the playing fails, a message is displayed, asking you to wait for the video stream, and then the client stays in the status of reconnecting the video stream.

Possible Causes

The forwarding bandwidth and the number of connections used for requesting video streams on the client cannot exceed the maximum specified for the NVR800 or IVS1800.

Solution

1. Reduce the video bit rate to lower the forwarding bandwidth.
2. Reduce the number of connections used for requesting video streams. For details, see the NVR800 or IVS1800 specification list.

9.4 Intelligent Applications

9.4.1 No Snapshot Alarm Is Displayed on the Target Recognition or Object Classification Page of the iClient S100

Symptom

Target snapshot alarms cannot be displayed on the target recognition or object classification page of the iClient S100, but can be displayed on the NVR800 LDU.

Possible Causes

- The target lists are imported on the NVR800 LDU, instead of the iClient S100.
- The alarm function of the corresponding target list is not enabled on the NVR800. As a result, the NVR800 does not push target alarms to the iClient S100.

Solution

1. Add and import target lists on the iClient S100.
2. Enable the alarm function of the required target list on the NVR800 LDU under **Intelligence > Intelligent Settings > Target Recognition > List-based Alarm > Alarming**. Alternatively, you can enable target alert of the corresponding target list on the iClient S100.

You can configure only target list-based alert on the iClient S100. To enable stranger snapshot and alarm, you need to configure the function on the NVR800 LDU.

9.4.2 Failure to Import Dynamic Lists to the NVR800

Symptom

When you attempt to import a dynamic list to the NVR800 on the iClient S100, the system displays a message indicating that the device API fails to be invoked.

Possible Causes

The NVR800 account used to log in to the iClient S100 does not have the required permission.

Solution

Log in to the iClient S100 as the **admin** or **apiadmin** user of the NVR800 and obtain administrator permissions by referring to [4.1.2.1 Adding NVR800s](#).

9.4.3 Target Snapshot Alarms Cannot Be Displayed on the Intelligent Recognition Page of the iClient S100, But Can Be Displayed on the NVR800 LDU

Symptom

Target snapshot alarms cannot be displayed on the intelligent recognition page of the iClient S100, but can be displayed on the NVR800 LDU.

Possible Causes

1. The alarm function of the corresponding target list is not enabled on the NVR800. As a result, the NVR800 does not push target alarms to the iClient S100.
2. The target lists are imported on the NVR800 LDU, instead of the iClient S100.

Solution

1. Add and import target lists on the iClient S100.
2. Enable the alarm function of the required target list on the NVR800 LDU under **Intelligence > Intelligent Settings > Target Recognition > List-based Alarm > Alarming**. Alternatively, you can enable target alert of the corresponding target list on the iClient S100.

9.5 Comprehensive Services

9.5.1 Personnel Management

What Can I Do If the System Displays a Message Indicating That an Employee Fails to Be Recognized During Real-Time Observation Because the Employee Is Not Registered?

Check whether the employee has been added to the permission group and whether the employee information has been synchronized to the access device. If not, add the employee to the permission group and synchronize the employee information to the access device again.

What Can I Do If I Fail to View a Department After I Successfully Add It as a System Administrator?

Check whether you added the department as a non-super administrator. If so, you can view and manage the department as the non-super administrator only after you are assigned permissions to manage the department by the super administrator.

9.5.2 Access Control

What Can I Do If the Exported Access Control Report Contains Garbled Characters?

Open the report using WPS or Excel. If the problem persists, open the report on another computer.

What Can I Do if I Fail to Add an Integrated Access Control Device to the iClient S100 After I Click the Device Adding Button and Set Device Information?

Check whether the device is added manually. If so, configure the IP address and port number of the iClient S100 on the device and scan for the device on the iClient S100 client to add it. The device cannot be added manually.

What Can I Do If I Fail to Use the iClient S100 Because the Administrator of an Integrated Access Control Device Fails to Be Deleted?

- If the device password is obtained,
 1. Log in to the iClient S100 client, mount the device to the server, and delete the administrator.
 2. Re-log in to the iClient S100 and run the `cd mnt/mtdblock/service` command to start the device.
- If the device password is not obtained,

Register an account at the device official website, use the serial number to obtain the cracking password, and perform operations under the condition that the device password is obtained.

What Can I Do If the TA1200 Search Result Contains Two Records with the Same Serial Number 0123456?

Contact technical support to set `IsSupportPull` to `0` on the device.

9.5.3 Attendance

What Can I Do If I Fail to Add an Attendance Device or Integrated Access Control Device to the iClient S100 (Where the IP Address of the Device Has Been Changed but the Device Cannot Be Found)?

Check whether the device firmware version is normal. If not, contact technical support to set `IsSupportSSL` and `IsSupportHttps` to `1`.

What Can I Do If the Employee Information Recorded on an Attendance Device Fails to Be Automatically Uploaded to the iClient S100?

Check whether the attendance device has been set as the registration device. If not, set the attendance device as the registration device.

10 Reference

[10.1 Password Maintenance Suggestions](#)

[10.2 Communication Matrix](#)

10.1 Password Maintenance Suggestions

Only authenticated users can log in to the application system. You must configure account and password complexity and password validity periods based on security requirements.

During password maintenance:

- The password of a new iClient S100 user must meet the following requirements:
 - The password must contain 8 to 16 characters.
 - The password cannot be the same as the user account or the user account in reverse order.
 - The password must contain digits and lowercase letters.
 - The password cannot be a weak password.
- Passwords must be encrypted before transmission and cannot be transferred by email.
- Passwords must be encrypted for storage.
- Passwords must be changed for system handover.

10.2 Communication Matrix

Table 10-1 Communication matrix of the client

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plane	Version
iClient S100 client IP	Random port	iClient S100 server IP	8098	TCP	Port for RESTful API-based communication and web page access between the iClient S100 client and iClient S100 server. If the port number is not changed during installation, the default port number 8098 is used.	Yes	Password	HTTPS	User plane	All versions

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plan	Version
iClient S100 client IP	Random port	iClient S100 server IP	58098	TCP	Enabled when required CU Server WebSocket port, which is used to push data to the client in real time.	No	N/A	N/A	User plan	All versions
IP addresses of access control and attendance devices	Random port	iClient S100 server IP	8088	TCP	Port for communication between the iClient S100 server and access control and attendance devices. If the port number is not changed during installation, the default port number 8088 is used.	Yes	Password	HTTPS	User plan	All versions

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plan	Version
iClient S100 server IP	Random port	NVR800 IP	443	TCP	Normally enabled 1. The iClient S100 accesses the northbound APIs of the NVR800. 2. The iClient S100 accesses the NVR800 web system.	Yes	Password	HTTPS	User plan	All versions
iClient S100 client IP	Random port	NVR800 IP	10000–12000	TCP	Normally enabled The iClient S100 obtains RTSP video streams from the NVR800.	No	Password	N/A	User plan	All versions

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plan	Version
iClient S100 client IP address	Random port	NVR800 IP	80	TCP	Enabled when required HTTP access port, which is used to redirect the browser to the corresponding HTTPS port.	No	N/A	N/A	User plan	All versions
iClient S100 server IP address	Random port	255.255.255.255	9333	UDP	Normally enabled Port for proprietary protocol-based search, which is used to search for NVR800s on the iClient S100.	No	N/A	N/A	User plan	All versions

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plan	Version
iClient S100 client IP	Random port	IVS1800 IP	9910	TCP	Normally enabled Port for the iClient S100 to access the SMU NSS TLS encryption channel of the IVS1800.	Yes	Password	TLS1.2	User plan	All versions
iClient S100 client IP	Random port	IVS1800 IP	9900	TCP	Normally enabled Port for the iClient S100 to access the IVS1800 SMU NSS.	Yes	Password	N/A	User plan	All versions
iClient S100 server IP	Random port	IVS1800 IP	18531	HTTPS	Normally enabled Port for the iClient S100 CUServer to access the IVS1800 northbound intertarget.	Yes	Password	TLS1.2	User plan	All versions

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plane	Version
iClient S100 server IP address	Random port	IVS1800 IP address	31943	HTTPS	Northbound API service (original SDKService HTTPS and XML intertarget).	Yes	Password	TLS1.2	Service plane	9.0.0
IVS1800 IP	Random port	iClient S100 server IP	58097	TCP	Enabled when required iClient S100 CUServer HTTPS service port, which is used by the IVS1800 data callback intertarget to send requests.	No	N/A	N/A	User plane	All versions
iClient S100 client IP	Random port	IVS1800 IP	554	RTSP	Normally enabled Port for the iClient S100 to obtain RTSP media streams from the IVS1800.	Yes	Dynamic password authentication	N/A	User plane	All versions

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plan	Version
iClient S100 client IP	Random port	IVS1800 IP	TCP: 11400~11465 UDP: 21200~21719	TCP and UDP	Normally enabled 1. Support live video forwarding of the MU. 2. Support voice intercom and broadcast. Only UDP ports are involved in this scenario.	Yes	Enabled based on the negotiation result	AES 256 (optional)	User plan	All versions

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plan	Version
iClient S100 server IP	Random port	IVS1800 IP	9554	TCP	Normally enabled Image media port.	Yes	Dynamic password authentication	A security mechanism based on the principle of AES 256-bit encryption after RSA 2048 key negotiation is provided for image upload and download.	User plan	All versions

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plan	Version
iClient S100 server IP	Random port	IVS1800 IP	8443	HTTPS	Normally enabled Port used by the iClient S100 to access the IVS1800 OMU portal and manage algorithms.	Yes	Password	TLS1.2	User plan	All versions
iClient S100 client IP	Random port	Peer main decoder IP address	10200	TCP	Enabled when required The iClient S100 configures the decoder to split the pane and screen and bind the playback stream address.	No	Username/Password	N/A	User plan	All versions

Source IP	Source Port	Destination IP	Destination Port (Listening)	Protocol	Port Description	Listening Port Changeable (Yes/No)	Authentication Mode	Encryption Mode	Plan	Version
iClient S100 client IP	Random port	DEC 6108 decoder IP address	9900	TCP	Enabled when required Port used by the iClient S100 to configure the decoder to split the pane and screen and bind the playback stream address.	No	Username/Password	N/A	User plan	All versions
iClient S100 client IP address	Random port	DEC 6109 decoder IP address	28000	TCP	Enabled when required Port used by the iClient S100 to configure the decoder to split the video pane and screen and bind the playback stream address.	No	Username/Password	N/A	User plan	All versions