



DSS Pro

User's Manual








Foreword

General

This user's manual (hereinafter referred to as "the manual") introduces the functions and operations of the DSS general surveillance management center (hereinafter referred to as "the system" or "the platform") and client operations.

Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Document Version	Software Version	Revision Content	Release Time
V1.0.5	V7.002.0000005.0	<ul style="list-style-type: none"> ● Optimized visitor management, live view, playback, face recognition, target detection, access control, business intelligence, storage configuration, thermal, event management, and entrance control functions. ● Added M+N deployment ● Optimized writing style. 	April 2020
V1.0.4	V7.002.0000003.1	<ul style="list-style-type: none"> ● Modified license strategy and radar-PTZ linkage ● Added custom event and people counting rule configuration. 	December 2019
V1.0.3	V7.002.0000003	<ul style="list-style-type: none"> ● Added visitor management, alarm controller, business intelligence, radar-PTZ smart track, electronic focus, and AI search and intelligent analysis configuration. ● Optimized instructions including authorization, device configuration, face recognition, personnel management and access control. 	October 2019

Document Version	Software Version	Revision Content	Release Time
V1.0.2	V7.002.0000002	<ul style="list-style-type: none"> Added new functions such as entrance, attendance and video intercom. Modified access control and deleted commercial functions. 	March 2019
V1.0.1	V7.002.0000001	<ul style="list-style-type: none"> Added new functions such as person management, access control management, thermal, target detection, device configuration. Modified contents such as edit device, flow analysis, plate recognition. 	December 2018
V1.0.0	V7.002.0000000	First release	September 2018

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The Manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product

updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please see our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please see our final explanation.

Table of Contents

Foreword	II
1 Overview	1
1.1 Introduction	1
1.2 Highlights	1
2 Installation and Deployment	2
2.1 Server Requirements	2
2.2 Installing Master Server	2
2.3 Installing Slave Server	6
2.4 Managing Platform Services	10
2.5 Configuring LAN or WAN	11
2.5.1 Configuring Router	11
2.5.2 Configuring DSS Platform	11
2.6 Uninstalling the platform	13
3 Basic Configurations	14
3.1 Logging in to Web Manager	14
3.2 Activating the Platform	15
3.2.1 License Capacity	15
3.2.2 Applying for a License	16
3.2.3 Activating or Updating License	16
3.3 Adding Organization	20
3.4 Managing Device	22
3.4.1 Searching for Online Devices	22
3.4.2 Initializing Devices	23
3.4.3 Modifying Device IP Address	25
3.4.4 Adding Devices	26
3.4.5 Editing Devices	32
3.4.6 Binding Resources	36
3.5 Adding Role and User	37
3.5.1 Adding User Role	37
3.5.2 Adding User	38
3.5.3 (Optional) Setting Domain User	40
3.6 Configuring Record Plan	41
3.6.1 Configuring Storage Disk	41
3.6.2 Configuring Disk Group Quota	44
3.6.3 Adding Recording Plan	46
3.6.4 Configuring Storage Backup	48
3.6.5 Adding Time Template	49
3.7 Configuring Map	51
3.7.1 Adding Map	52
3.7.2 Marking Devices	57
4 Business Functions	59
4.1 Preparations	59

4.1.1	Installing Client	59
4.1.2	Logging in to Client.....	62
4.1.3	Homepage of Control Client	64
4.1.4	Local Configuration.....	65
4.2	Live View	75
4.2.1	Typical Topology	75
4.2.2	Preparations	75
4.2.3	Viewing Live Video	76
4.2.4	Electronic Focus	84
4.2.5	Tour	86
4.2.6	View	86
4.2.7	Favorites	87
4.2.8	Region of Interest (RoI)	90
4.2.9	PTZ	91
4.3	Configuring Device Parameters.....	97
4.3.1	Configuring Camera Properties.....	97
4.3.2	Video.....	108
4.3.3	Audio	113
4.4	Event and Alarm.....	114
4.4.1	Configuring Events	115
4.4.2	Viewing Alarms	127
4.5	Intelligent Analysis	130
4.5.1	Typical Topology	130
4.5.2	Configuring Intelligent Analysis.....	131
4.6	Fisheye-PTZ Smart Track	154
4.6.1	Typical Topology	154
4.6.2	Business Flow.....	155
4.6.3	Configuring Fisheye-PTZ Smart Track.....	155
4.6.4	Applying Fisheye-PTZ Smart Track	158
4.7	Bullet-PTZ Smart Track.....	159
4.7.1	Typical Topology	160
4.7.2	Business Flow.....	160
4.7.3	Configuring Bullet-PTZ Smart Track.....	161
4.7.4	Applying Bullet-PTZ Smart Track	163
4.8	Radar-PTZ Smart Track.....	170
4.8.1	Typical Topology	170
4.8.2	Business Flow.....	171
4.8.3	Configuring Radar-PTZ Smart Track.....	171
4.8.4	Radar-PTZ Smart Track Monitoring	180
4.9	Record.....	183
4.9.1	Preparations	183
4.9.2	Playback	183
4.9.3	POS Search.....	191
4.9.4	Searching by Thumbnail.....	192
4.10	Video Wall	195
4.10.1	Typical Topology	196

4.10.2 Business Flow.....	197
4.10.3 Configuring Video Wall	197
4.10.4 Video Wall Applications	207
4.11 Traffic.....	210
4.11.1 Typical Topology.....	211
4.11.2 Business Flow	211
4.11.3 Configuring Traffic Monitoring.....	212
4.11.4 Traffic Management Applications.....	216
4.12 ANPR.....	221
4.12.1 Typical Topology	222
4.12.2 Business Flow.....	222
4.12.3 Configuring ANPR.....	223
4.12.4 ANPR Applications.....	226
4.13 Entrance.....	234
4.13.1 Typical Topology	234
4.13.2 Business Flow.....	235
4.13.3 Configuring Entrance Settings.....	236
4.13.4 Entrance Applications	247
4.14 POS.....	256
4.14.1 Typical Topology	256
4.14.2 Business Flow.....	257
4.14.3 Configuring POS Monitoring.....	257
4.14.4 POS Applications	259
4.15 Flow Analysis	263
4.15.1 Typical Topology	264
4.15.2 Business Flow.....	265
4.15.3 Configuring Flow Analysis	265
4.15.4 Flow Analysis Applications.....	279
4.16 Human Face Recognition	286
4.16.1 Typical Topology	286
4.16.2 Business Flow.....	288
4.16.3 Configuring Face Recognition	288
4.16.4 Face Recognition Applications	296
4.17 Target Detection.....	306
4.17.1 Typical Topology	307
4.17.2 Business Flow.....	307
4.17.3 Target Detection Applications	308
4.18 Thermal	314
4.18.1 Typical Topology	315
4.18.2 Business Flow.....	315
4.18.3 Thermal Applications	316
4.19 Personnel Management.....	329
4.19.1 Configuring Personnel Information.....	330
4.19.2 Configuring Door Groups.....	351
4.19.3 Configuring Admin Passwords	353
4.19.4 Configuring Time Templates.....	354

4.19.5 Configuring Holiday Schedules	356
4.20 Access Control	358
4.20.1 Typical Topology	359
4.20.2 Business Flow.....	360
4.20.3 Configuring Access Control	360
4.20.4 Access Control Applications	379
4.21 Video Intercom.....	389
4.21.1 Typical Topology	389
4.21.2 Business Flow.....	389
4.21.3 Configuring Video Intercom	390
4.21.4 Video Intercom Applications	400
4.22 Attendance Management	409
4.22.1 Typical Topology	409
4.22.2 Business Flow.....	410
4.22.3 Configuring Attendance	410
4.22.4 Viewing Attendance Report	426
4.23 Visitor Management	429
4.23.1 Preparations	430
4.23.2 Business Flow.....	430
4.23.3 Configuring Visit Settings	430
4.23.4 Visitor Appointment.....	432
4.23.5 Checking In	434
4.23.6 Checking Out	437
4.23.7 Searching for Visit Records	438
4.24 Business Intelligence	438
4.24.1 Typical Topology	439
4.24.2 Business Flow.....	440
4.24.3 Configuring Business Intelligence	440
4.24.4 Business Intelligence Applications	445
4.25 Alarm Controller	451
4.25.1 Preparations	451
4.25.2 Alarm Controller Interface.....	453
4.25.3 Updating Alarm Controller Status	455
4.25.4 Arming/Disarming	456
4.25.5 Bypassing/Isolating/Normal	459
4.26 Configuring N+M.....	462
4.27 Cascade	465
4.27.1 Typical Topology	466
4.27.2 Configuring Cascade	466
4.28 System Configuration.....	468
4.28.1 HTTPs Certificate	468
4.28.2 Setting Mail Server	468
4.28.3 Setting Device Login Mode.....	469
4.29 Server Management	469
4.29.1 Server Management	470
4.29.2 Resource Config	470

4.30 Password Maintenance.....	472
4.30.1 Modifying Password	472
4.30.2 Resetting Password.....	472
5 Maintenance.....	475
5.1 Setting System Data Retention Period	475
5.2 Updating App Certificate	475
5.3 Remote Log.....	476
5.4 Time Synchronization.....	476
5.4.1 Automatic Time Synchronization	476
5.4.2 Manual Time Synchronization	477
5.5 Backup and Restore	478
5.5.1 System Backup.....	478
5.5.2 System Restore	479
5.6 Log	482
5.7 System Maintenance	482
5.7.1 Overview	482
5.7.2 Running Status	483
5.7.3 Status Information.....	484
5.7.4 Event Information.....	485
5.7.5 Source Information	486
Appendix 1 Service Module Introduction	488
Appendix 2 Cybersecurity Recommendations	490

1 Overview

1.1 Introduction

DSS Pro is a flexible, easily-extendable, highly-reliable and professional video surveillance software. It meets the requirements of large and medium-sized projects through distributed deployment and cascade. In addition to the basic video surveillance business, it also delivers a number of AI functions such as target detection, face recognition, license plate recognition, people counting, and more. It also provides the add-on modules of transportation and business analysis, and access control. These functions enable the platform to be widely used in chain supermarket, casino, safe city, road monitoring, medium and large-sized campus surveillance and more scenarios.

1.2 Highlights

- Easily extendable
 - ◇ Supports distributed deployment for optimal system performance.
 - ◇ Supports cascading for large system management.
 - ◇ Provides Add-ons.
- More professional
 - ◇ Supports system operation and maintenance for easily acquiring information of service, system, device, time and more.
 - ◇ Supports radar-PTZ smart track, target detection, face recognition, plate recognition, people counting and other AI functions, access control, retail and transportation functions, making DSS Pro more powerful.
- Highly reliable
 - ◇ Supports hot standby and N+M deployment to guarantee system stability.
 - ◇ Supports auto and manual backup of system data to reduce loss caused by system crash.
- More open
 - ◇ Supports ONVIF protocol and active registration.
 - ◇ Provides open SDK for third party integration.

2 Installation and Deployment


DSS platform supports both single server deployment and master/slave distributed deployment.

2.1 Server Requirements

Table 2-1 Hardware requirement

Parameter	Hardware Requirement	Operating System
Recommended configuration	<ul style="list-style-type: none"> • CPU: Intel Xeon Silver 4114@ 2.2GHz 10 Core Processor • RAM: 16 GB • Network card: 4 Ethernet port @ 1000 Mbps • Hard drive type: HDD 1TB • DSS installation directory space: Over 500 GB 	<ul style="list-style-type: none"> • Win10-64bit • Windows server 2008 • Windows server 2012 • Windows server 2016 • Windows server 2019
Minimum configuration	<ul style="list-style-type: none"> • CPU: E3-1220 v5@2.60GHz 4 Core Processor • RAM: 8 GB • Network card: 2 Ethernet port @ 1000 Mbps • Hard drive type: HDD 1TB • DSS installation directory space: Over 500 GB 	Win10-64bit

2.2 Installing Master Server

Step 1 Double-click  .



Program name includes version number and program data, please confirm it before installation.

Figure 2-1 Agreement interface



Step 2 Click **agreement**, read the agreement, and then select the check box of **I have read and agree to the DSS agreement**. Click **Next**.

Figure 2-2 Select server type



Step 3 Select a server type, and then click **Next**.

- Select **Master** if the current server is the only server of your platform or the master server in the distributed deployment of the system.
- Select **Slave** if the current server is a slave server.

Figure 2-3 Select installation path



Step 4 Select the installation path. You can click **Browse** to customize the installation directory.

After selecting installation directory, the system displays the required space and current free space.

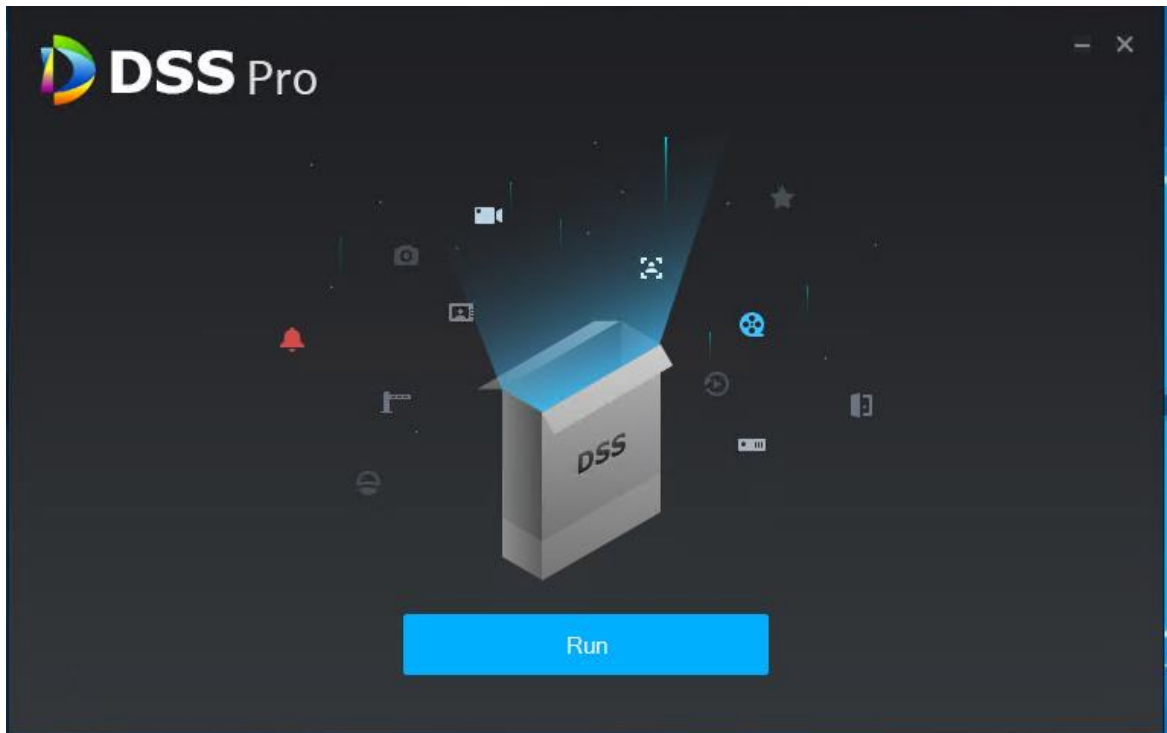


- It is not recommended that you install the platform in to Disk C because features such as face recognition require higher disk performance.
- If the **Install** button is gray, check if the installation directory is correct, or if free space is larger than the required space.

Step 5 Click **Install**.

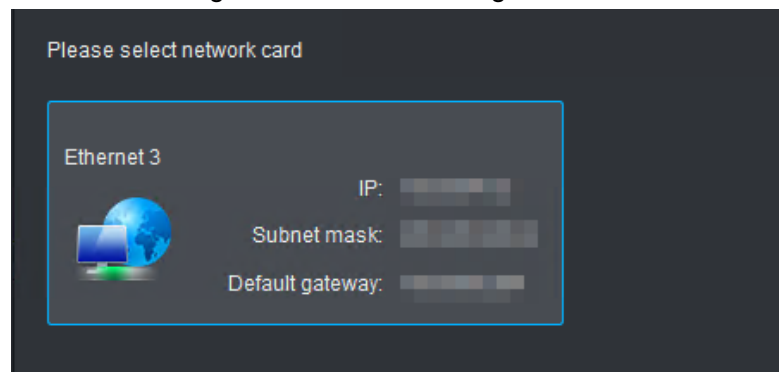
The installation process takes about 3 to 5 minutes. The **Run** interface is displayed after the installation is completed.

Figure 2-4 End of installation



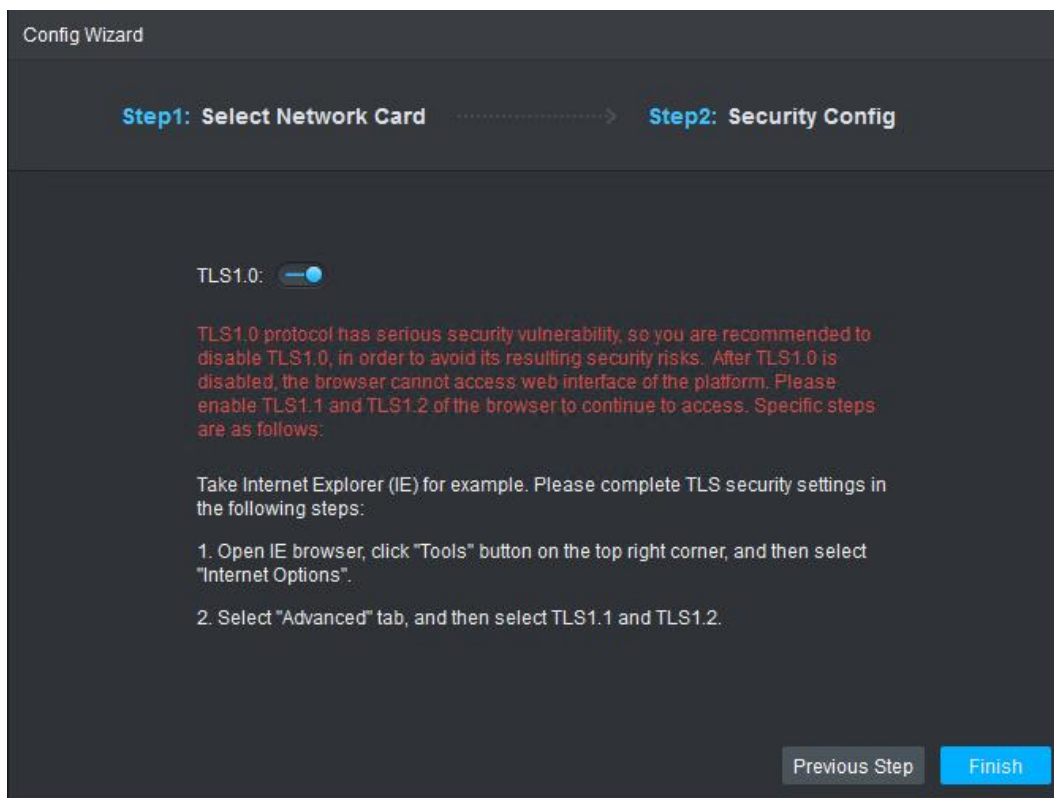
Step 6 Click **Run**.

Figure 2-5 Network config



Step 7 Select a network card, and then click **OK**.
The security setting interface is displayed.

Figure 2-6 Enable TLS1.0



Step 8 Enable or disable TLS1.0 protocol as needed.

Step 9 Click **OK**.

2.3 Installing Slave Server

Step 1 Double-click installation program



The program name includes version number and program data, please confirm it before installation.

Figure 2-7 Agreement interface



Step 2 Click the **agreement**, read and accept agreement protocol, select **I have read and agree the DSS agreement**, click **Next**.

Figure 2-8 Select server type



Step 3 Select installation mode as **Slave**, click **Next**.

Figure 2-9 Select installation path



Step 4 Select installation path, supports default installation path, click **Browse** to customize installation directory.

After selecting directory, the system displays space needed for installation and available space for selected path.

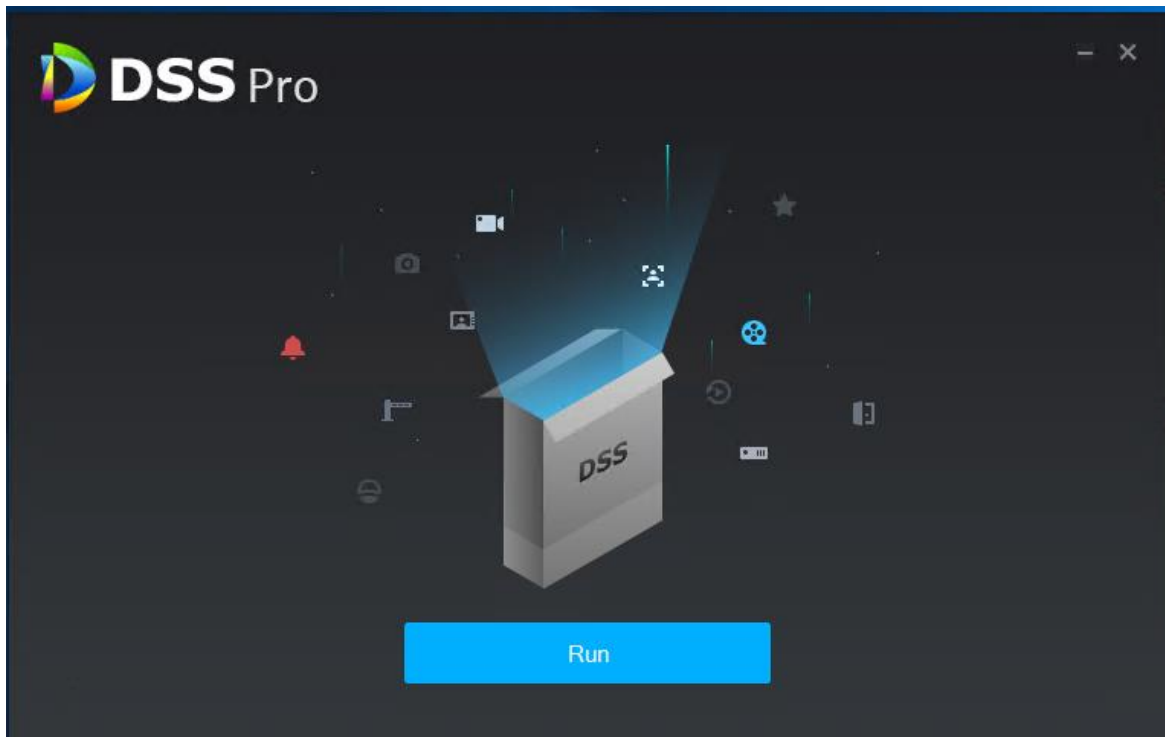


- It is not recommended that you install the platform in to Disk C because features such as face recognition require higher disk performance.
- If the Install button is gray, check if the installation directory is correct, or if free space is larger than the required space.

Step 5 Click **Install**.

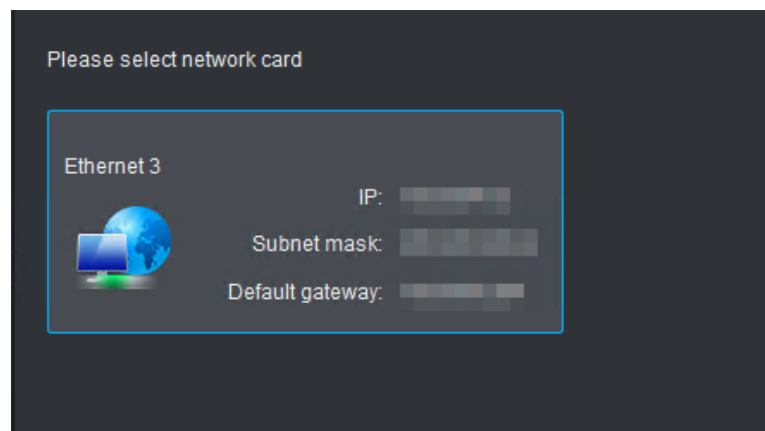
The installation process needs about 3 to 5 minutes.

Figure 2-10 Installation completed





Step 6 Click **Run**.

Figure 2-11 Select network card



Step 7 Select the network card you need and click **OK**.

Step 8 Configure master server information on the slave server.

- 1) Double-click  on the slave server.
- 2) Click  at the upper-right corner of the interface.
- 3) Set **Center IP**, **Local IP** and each port number, and then click **OK**.
 - ◇ Enter master server IP address in the **Center IP** box, and master server port numbers in the port number boxes.
 - ◇ Enter slave server IP address and WAN IP address in the **Local IP** box and **Mapping IP** box.

If the IP addresses and ports are valid, the slave server services will restart.

2.4 Managing Platform Services

View service status, start or stop services, and modify service ports.


Log in to the server, and then double-click .

Figure 2-12 Service management interface

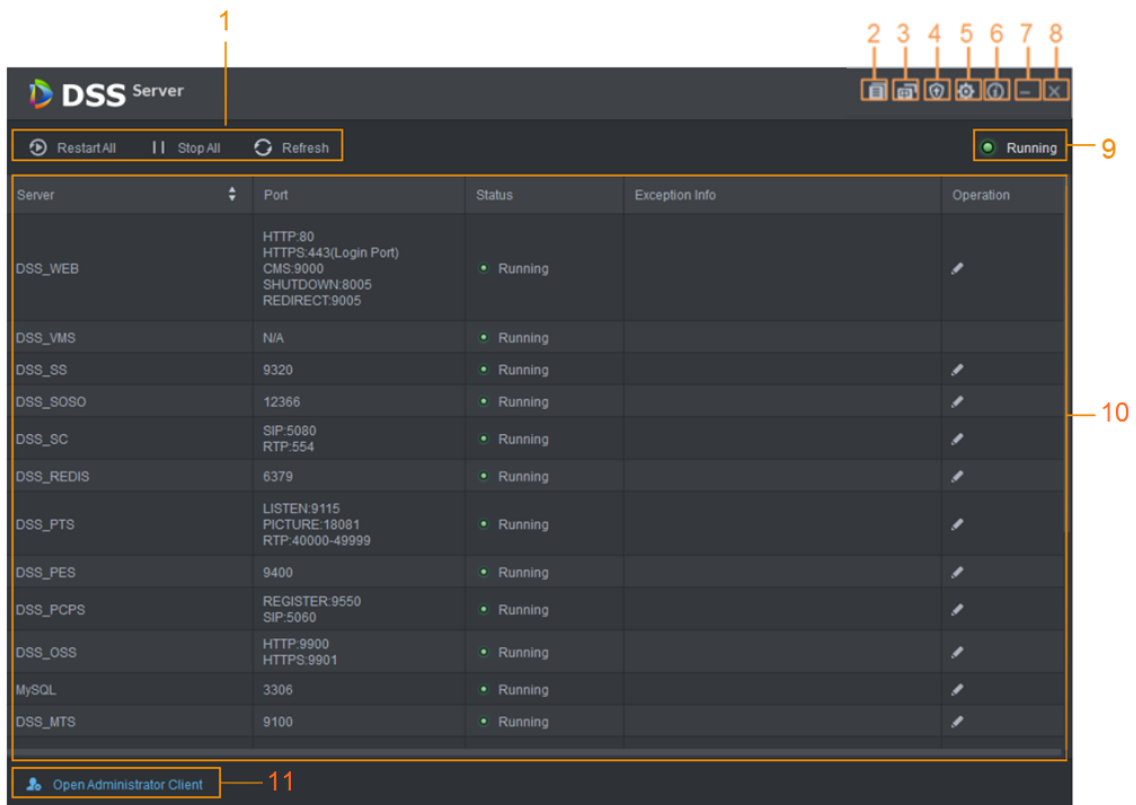
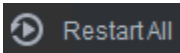
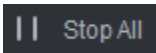
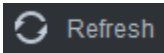

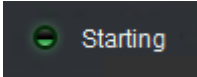
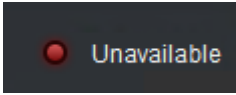
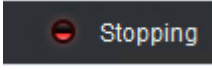
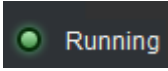
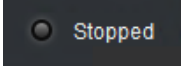



Table 2-2 Parameters

No.	Function	Description
1	Service Management	Service management, it supports following three types of operation: <ul style="list-style-type: none"> Click  to restart all services. Click  to stop all services. Click  to refresh services.
2	User's manual	User's manual.
3	Language	Switch language.
4	Security Setting	Enable or disable the TSL 1.0 protocol. TSL 1.0 protocol is a non-security protocol and is recommended to be closed. If TLS 1.0 protocol is disabled, ensure that the browser has proper access to the platform. To enable TLS1.1 and TLS 1.2, open your browser, select  > Internet Options > Advanced .

No.	Function	Description
5	Setting	Set server IP as the platform CMS IP. If the network has to go across LAN and WAN, you need to enter WAN IP in the Mapping IP box.
6	About	Software version information.
7	Minimize	Minimize the interface.
8	Close	Close.
9	Service Status	<ul style="list-style-type: none"> •  Starting •  Unavailable : Service exception •  Stopping •  Running : Service is running normally •  Stopped
10	Services	Display each service and service status. Click  to modify service port number, and then services will restart automatically after modification.
11	Open Administrator Client	Go to the Web Manager which is used by system administrators.

2.5 Configuring LAN or WAN

2.5.1 Configuring Router

If the platform is in a local network, to visit it from the public network, you need to do port mapping. For the list of the ports to be mapped, see "Appendix 1 Service Module Introduction".

2.5.2 Configuring DSS Platform

Step 1 Log in to DSS server, and then double-click .

Figure 2-13 Service status

Server	Port	Status	Exception Info	Operation
DSS_WEB	HTTP:80 HTTPS:443(Login Port) CMS:9000 SHUTDOWN:8005 REDIRECT:9005	Running		
DSS_VMS	N/A	Running		
DSS_SS	9320	Running		
DSS_SOSO	12366	Running		
DSS_SC	SIP:5080 RTP:554	Running		
DSS_REDIS	6379	Running		
DSS_PTS	LISTEN:9115 PICTURE:18081 RTP:40000-49999	Running		
DSS_PES	9400	Running		
DSS_PCPS	REGISTER:9550 SIP:5080	Running		
DSS_OSS	HTTP:9900 HTTPS:9901	Running		
MySQL	3306	Running		
DSS_MTS	9100	Running		


Step 2 Click the  on the upper-right corner.

Figure 2-14 Setting

Setting ✕

CMS IP:

Mapping IP:

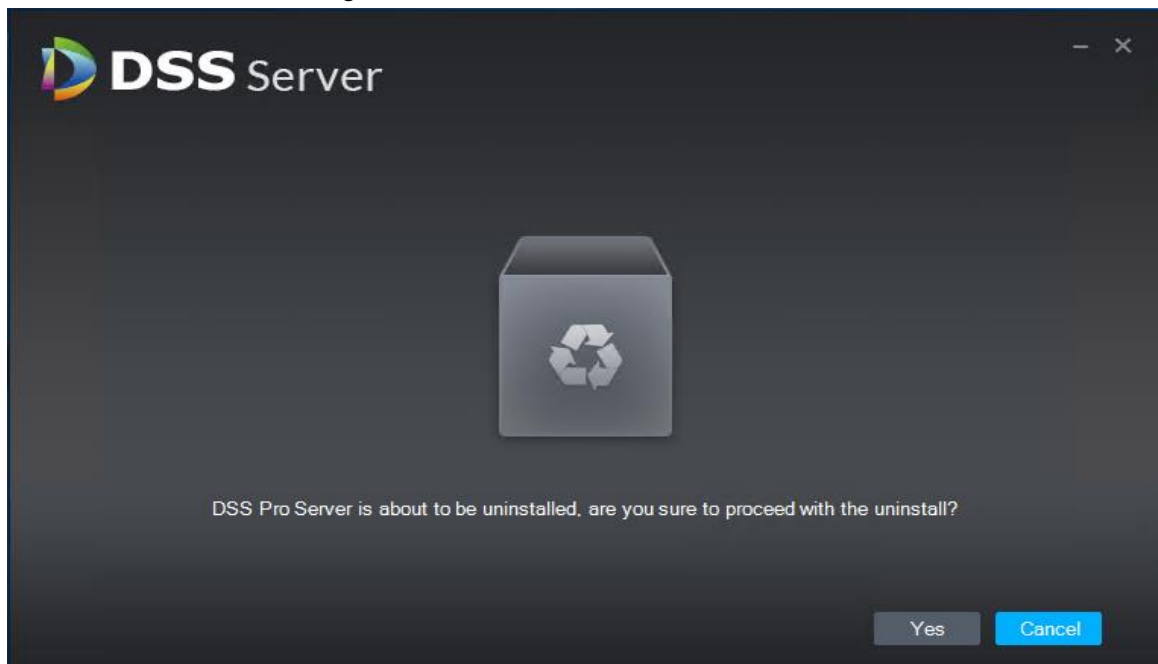
Step 3 Enter WAN address in the **Mapping IP** box, and then click **OK**.

Step 4 Click **OK** and then services restart.

2.6 Uninstalling the platform

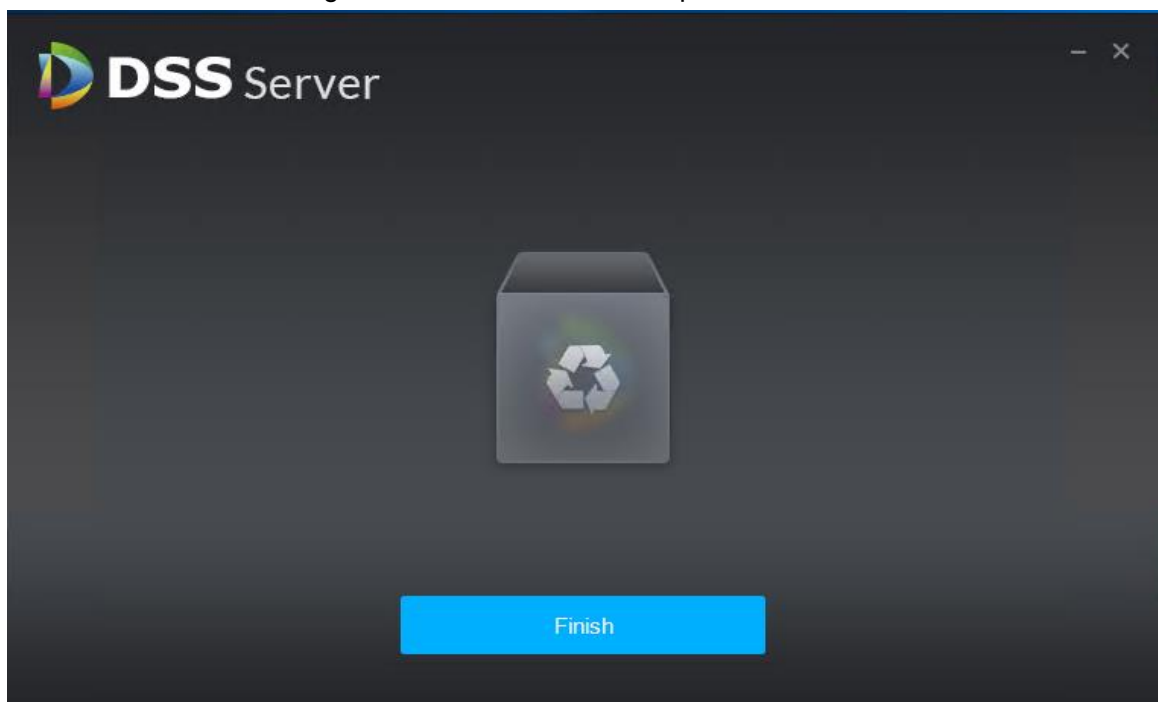
Step 1 On the server, go to the service directory "..\DSS Pro\Server\Uninstall", and then double-click "uninst.exe".

Figure 2-15 Confirm uninstallation



Step 2 Click **Yes**.

Figure 2-16 Uninstallation completed



Step 3 Click **Finish**.

3 Basic Configurations

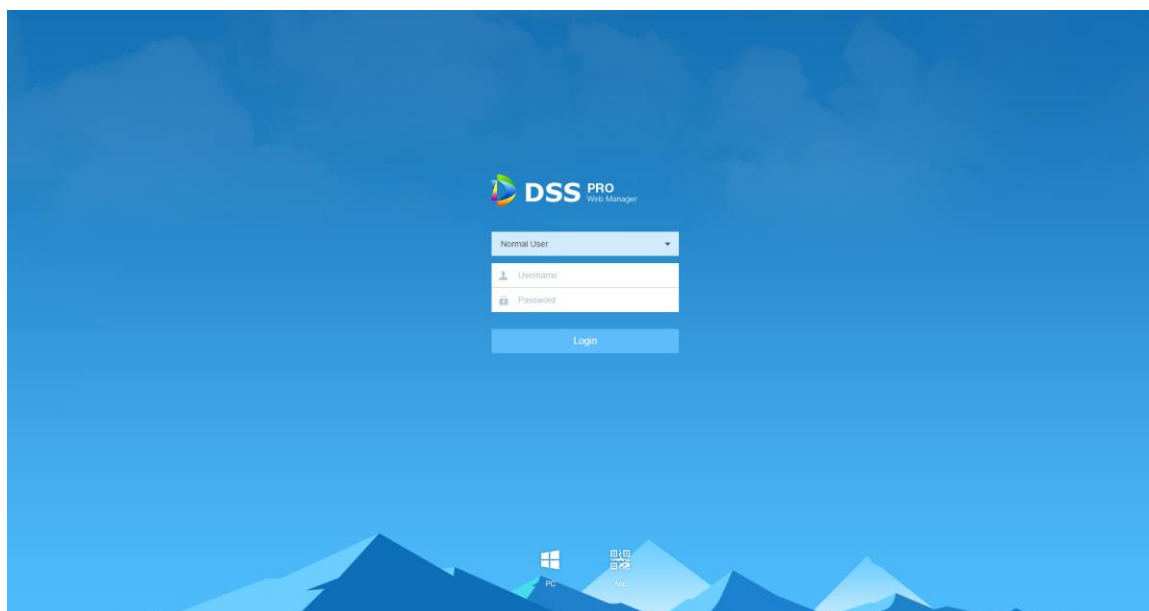
Configure basic settings of the system functions before you can use them, such as system activation, organization and device management, user creation, storage and recording planning, and event rules configuration. The basic configurations are made on Web Manager, the web client of DSS Pro. To log in to Web Manager, you are recommended to use Google Chrome 70 and later, and Firefox 56 and later, and IE 11.

3.1 Logging in to Web Manager

Log in to the Web Manager via browser to perform remote configuration of the system.

Step 1 Enter platform IP address in the browser, and then press Enter.

Figure 3-1 Log in to the Web Manager



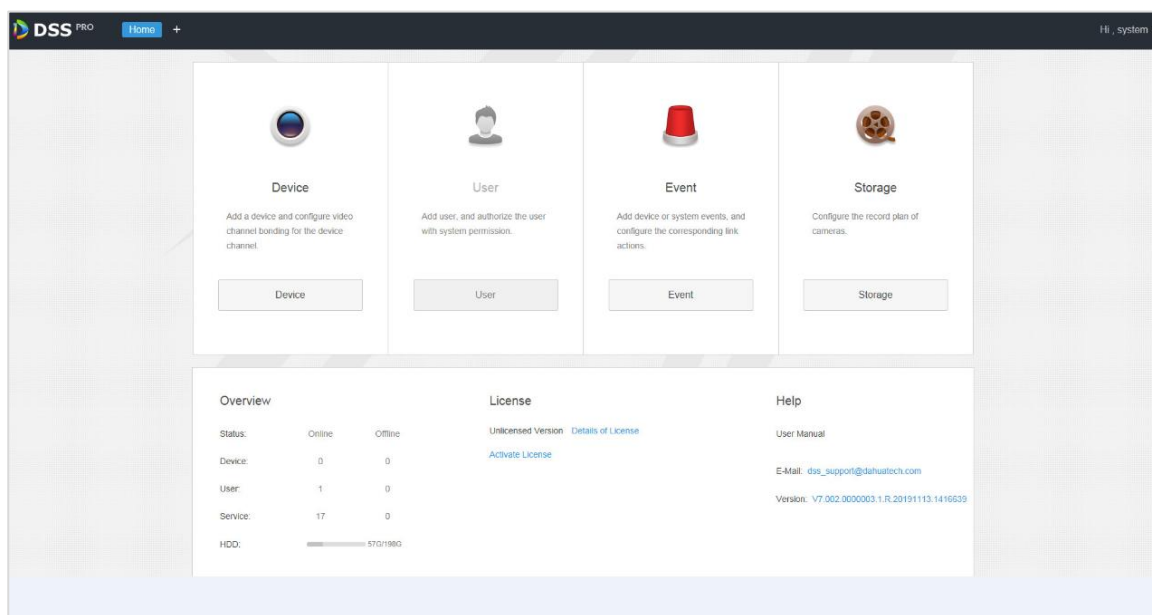
Step 2 Enter username and password, and then click **Login**.


The default username is *system*.



- The system will pop out the interface of modifying password if it is the first time to log in system. It can continue to log in system after the password is modified in time.
- Please add the platform IP address into the trusted sites of browser if it is your first time to log in DSS Web Manager.

Figure 3-2 Homepage



- Place the mouse pointer on the username of upper-right corner, and then you can modify password or log out current user.
- The shortcut access of general modules is displayed on the top of interface, click  on the homepage to present all the modules and open new modules.
- Overview: It displays the online/offline status of device, user and service, and the usage proportion of hard drive.
- License: Activate or update license, and check license details.
- Help: Check user's manual and version information.

3.2 Activating the Platform

Activate the platform with a trial or paid license the first time you log in to it. Otherwise you cannot use it.

This section introduces license capacity, how to apply for a license, how to use license to activate the platform, and how to renew your license.

3.2.1 License Capacity

- A trial license provides limited capacity and expires in 90 days.
- To acquire full capacity and permanent use, you shall buy a formal license.
- After activating the first paid license, if you want to increase your license capacity, you can buy more license codes. For example, if you have 500 channels currently, you can buy another 500 channels. After activating the new 500 channels, you will have 1,000 channels in total.
- The activated official version cannot be downgraded to the trail version.

3.2.2 Applying for a License

To get a formal license, contact the sales personnel.

To apply for a trial license, see the following instructions.

Step 1 Go to <https://www.dahuasecurity.com/products/productDetail/35647>.

Step 2 Click **Apply for DEMO**, and then follow the onscreen guide to complete and submit the application.

In 2 or 3 days after the application, you will receive a system email that contains your trial license.

3.2.3 Activating or Updating License

Activate the platform with a trial or formal license for first-time login. Otherwise you cannot use the platform.

During use of the platform, you can also update your trial or formal license with a new one, so as to achieve greater capacity or longer use.

To activate or update your license, see the following procedures.



The license activation and update procedures are the same. This section takes license activation as an example. The actual interface shall prevail.

Step 1 On the **Home** interface of the Web Manager, click **Activate License**.

Figure 3-3 Update license

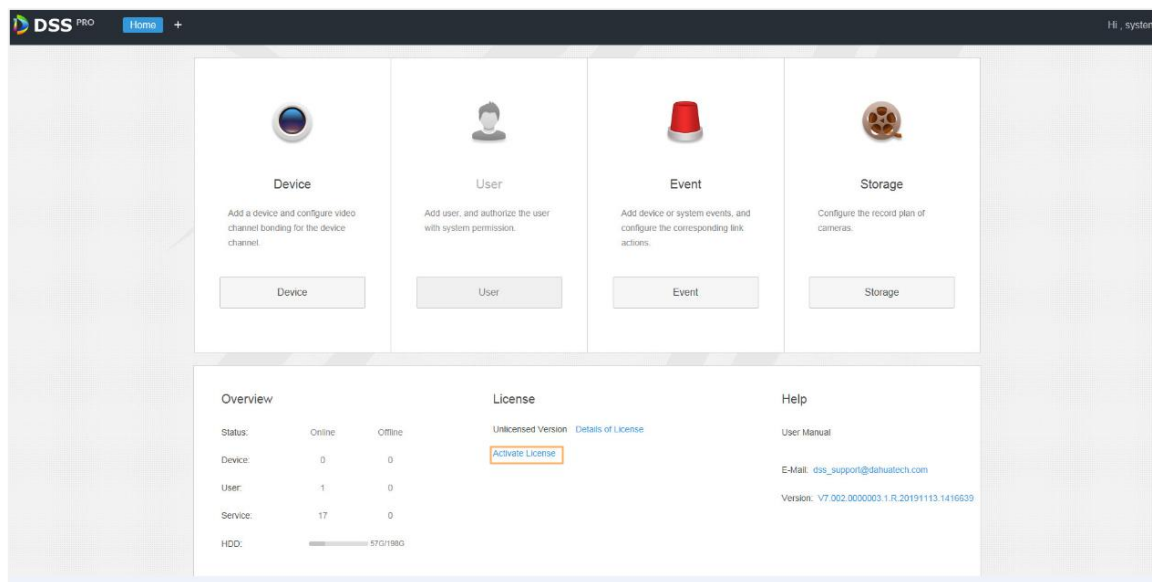
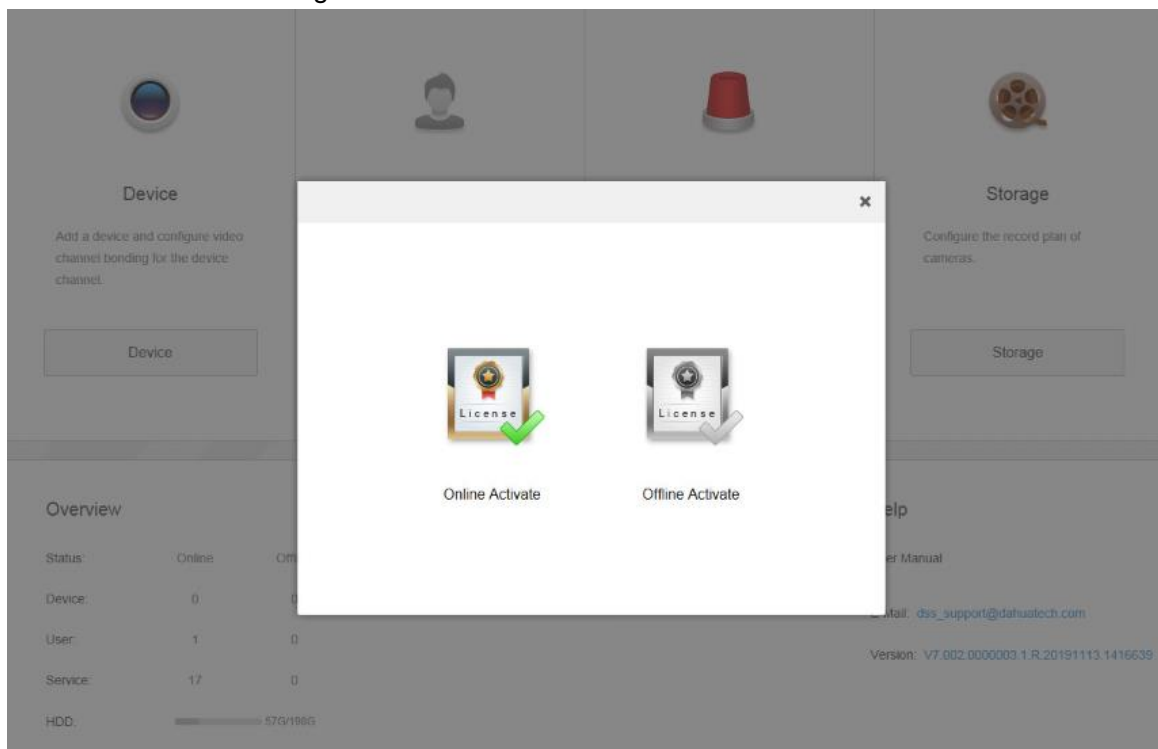


Figure 3-4 Activation method selection



Step 2 Select an activation method.

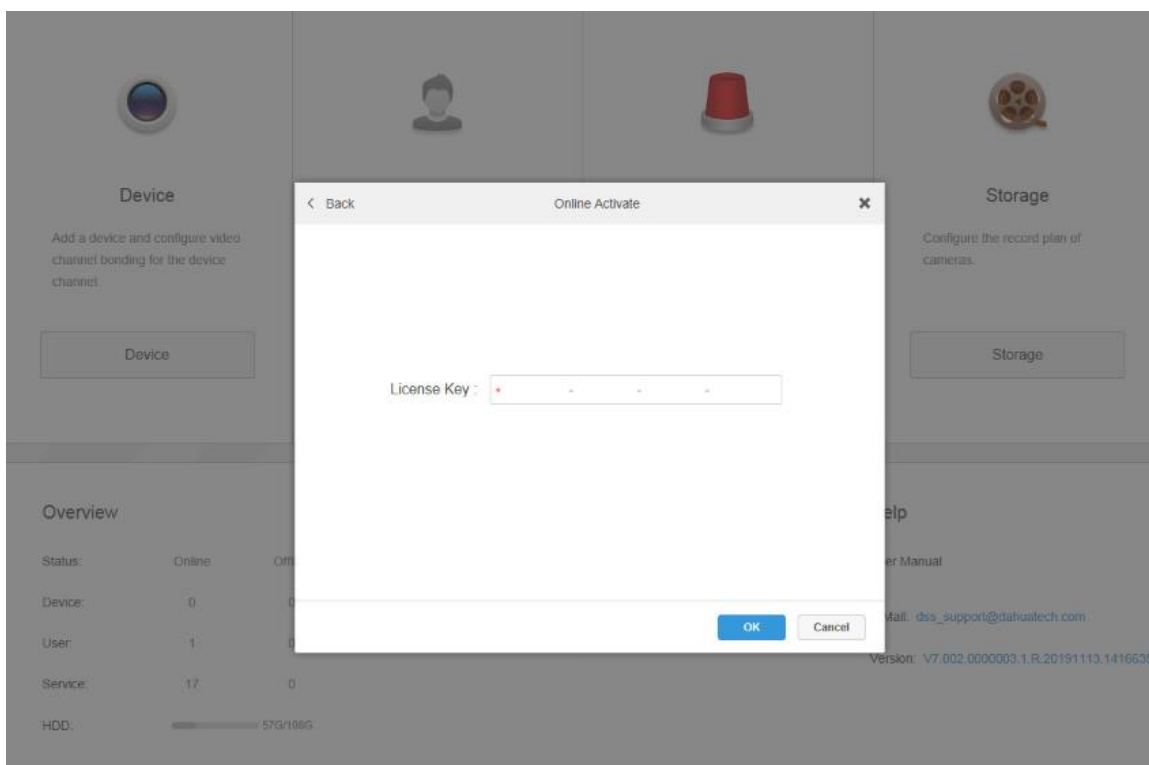
There are two ways to activate the license.

- Online activation
 - Select **Online Activate** if the platform server is connected to the Internet.
- Offline activation
 - Select **Offline Activate** if the platform server is disconnected from the Internet.

◇ Online activation

- 1) On the activation method interface, select **Online Activate**.

Figure 3-5 Online activate

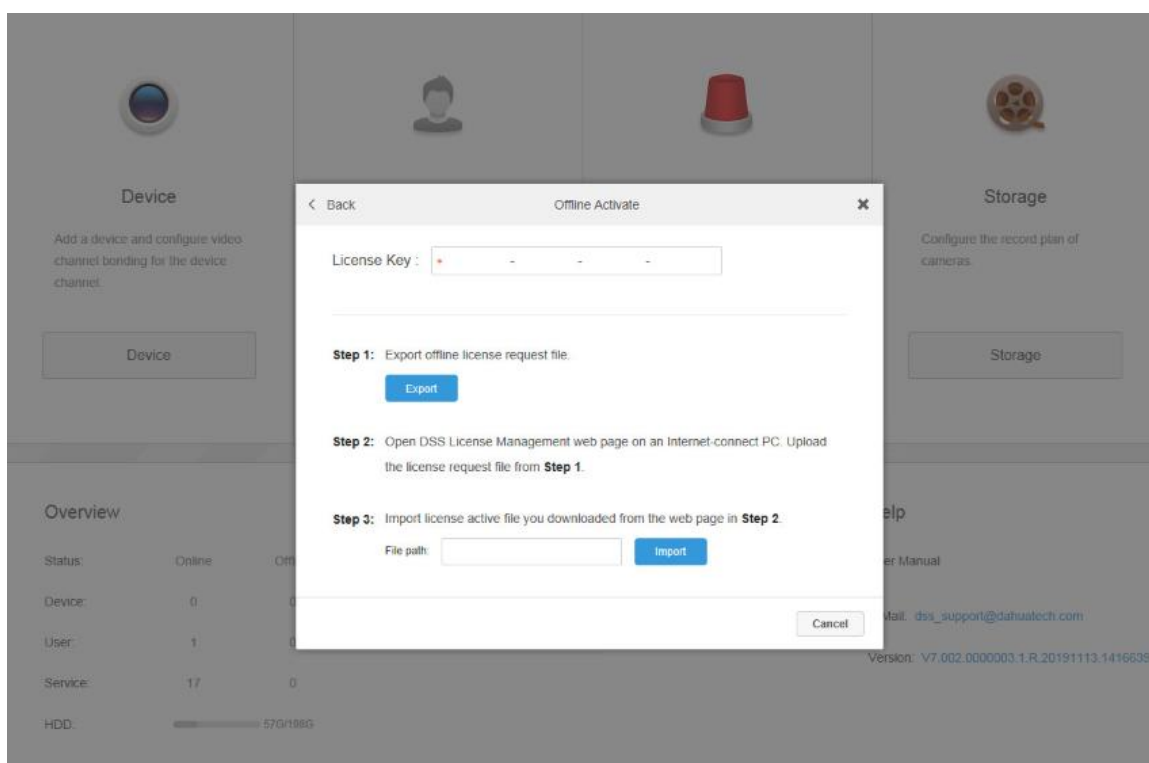


- 2) Enter the new license key, and then click **OK**.
After the license is activated successfully, you can click **Details of License** to view the details of your license capacity.

◇ Offline activate

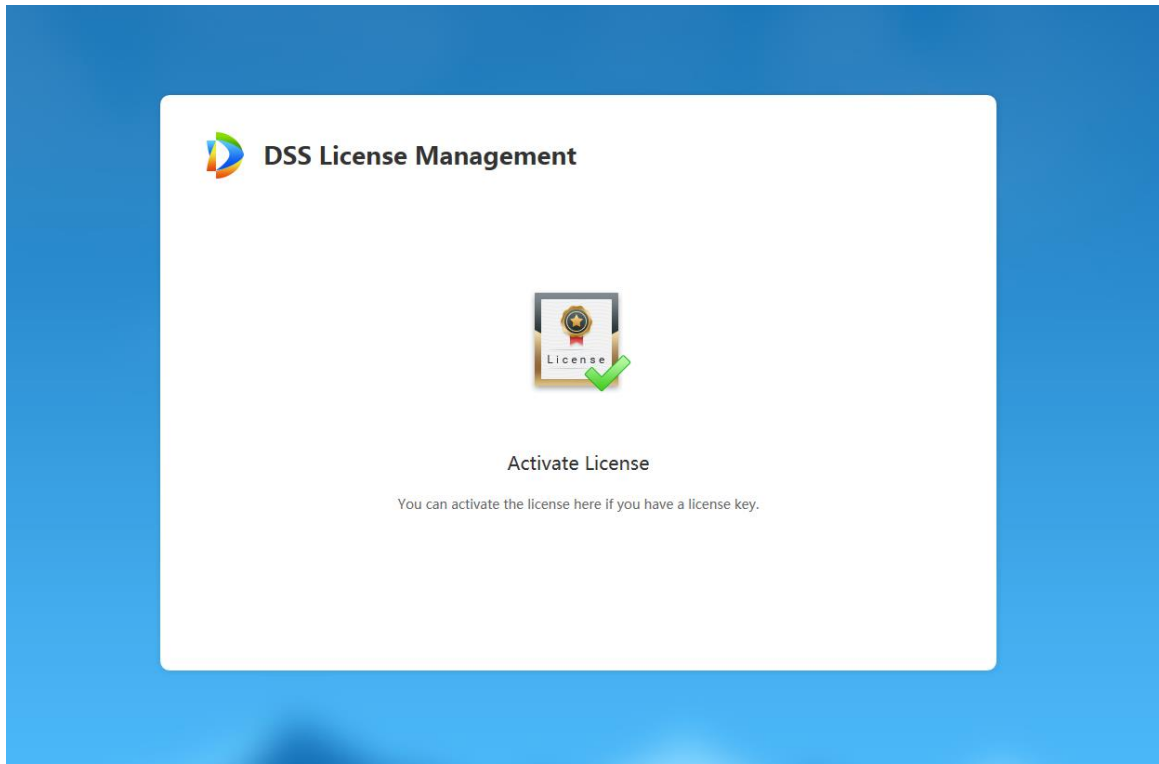
- 1) On the activation method interface, select **Offline Activate**.

Figure 3-6 Offline activate



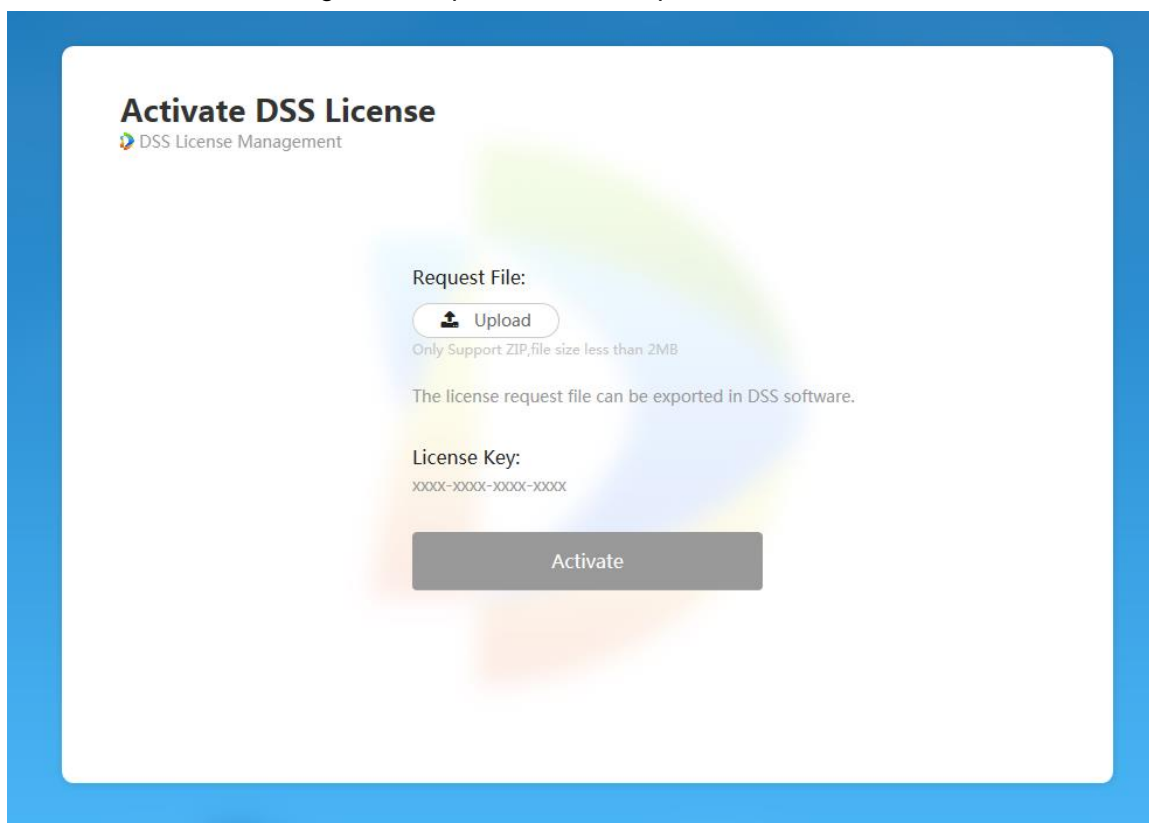
- 2) Enter the license code in the **License Key** box.
- 3) Click **Export** to export the license request file.
- 4) Move the request file to a computer that is connected to the Internet. On that computer, open the system email that contains your license, and then click the web page address to go to the license management page.

Figure 3-7 License management web page



- 5) Click **Activate License**.

Figure 3-8 Upload license request file



- 6) Click **Upload**, select the license request file, and then when you are prompted **uploaded successfully**, click **Activate**.
The success interface is displayed, where a download prompt is displayed asking you to save the license activation file.
- 7) On the success interface, click **Save** to save the file, and then move the file to back to the computer where you exported the license request file.
- 8) On the **Offline Activate** interface, click **Import**, and then follow the onscreen instructions to import the license activation file.
After you are prompted that the platform license is activated, you can click **Details of License** to view license capability details.

3.3 Adding Organization

Classify devices by logical organization for the ease of management.


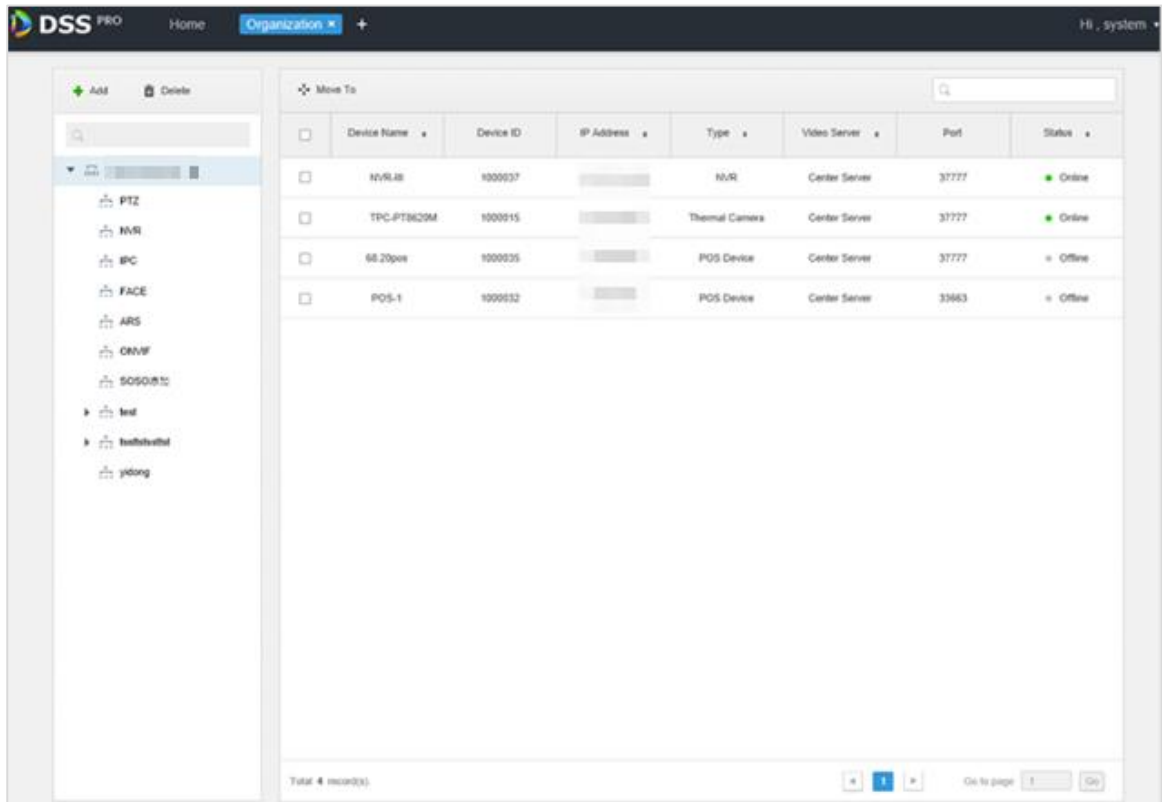
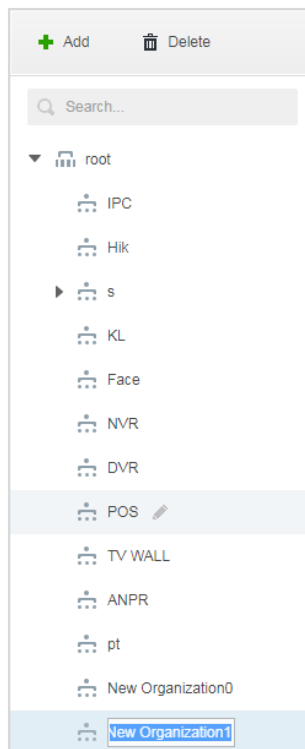
Step 1 Log in to the Web Manager. Click , and then select **Organization** on the **New Tab** interface.

Figure 3-9 Device organization






Step 2 Select the root node of the device tree on the left, and then click **Add** to add new organizations under the root node.

Figure 3-10 Add an organization



Step 3 Enter organization name, and then press Enter.

Operations


- Move device: Select the device under the root organization, click  **Move To**, select **New Organization 1**, and then click **OK**.
- Edit: Click the  next to the organization and modify the organization name.
- Delete: Select an organization, and then click  **Delete**.

3.4 Managing Device

Add devices before you can use them for video monitoring. This section introduces how to add, initialize, and edit devices and how to modify device IP address.

3.4.1 Searching for Online Devices

Search for devices on the same LAN with the platform before you can add them to the platform.

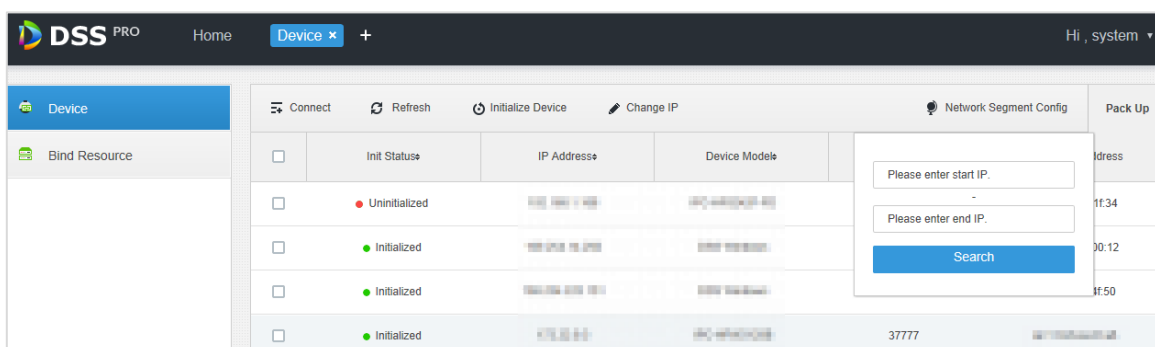
Step 1 Log in to the Web Manager. Click , and then select **Device**.



- The platform searches for and displays devices on the same LAN with the platform server during first-time use.
- The platform searches for and displays devices according to the network segment as defined last time if it is not the first-time use.

Step 2 Click **Network Segment Config**.

Figure 3-11 Set network segment



Step 3 Enter the start IP and end IP, and then click **Search**.

Figure 3-12 Search results

<input type="checkbox"/>	Init Status	IP Address	Device Model	Port	MAC Address
<input type="checkbox"/>	Uninitialized	192.168.1.100	DS-3A2204-01	37777	88:88:88:88:88:88
<input type="checkbox"/>	Initialized	192.168.1.101	DS-3A2204-01	37810	88:88:88:88:88:88
<input type="checkbox"/>	Initialized	192.168.1.102	DS-3A2204-01	37810	88:88:88:88:88:88
<input type="checkbox"/>	Initialized	192.168.1.103	DS-3A2204-01	37777	88:88:88:88:88:88

3.4.2 Initializing Devices

You need to initialize the uninitialized devices before you can add them to the platform.

Step 1 Log in to the Web Manager. Click , and then select **Device**.

Step 2 Search for devices. See "3.4.1 Searching for Online Devices".

Figure 3-13 Search results

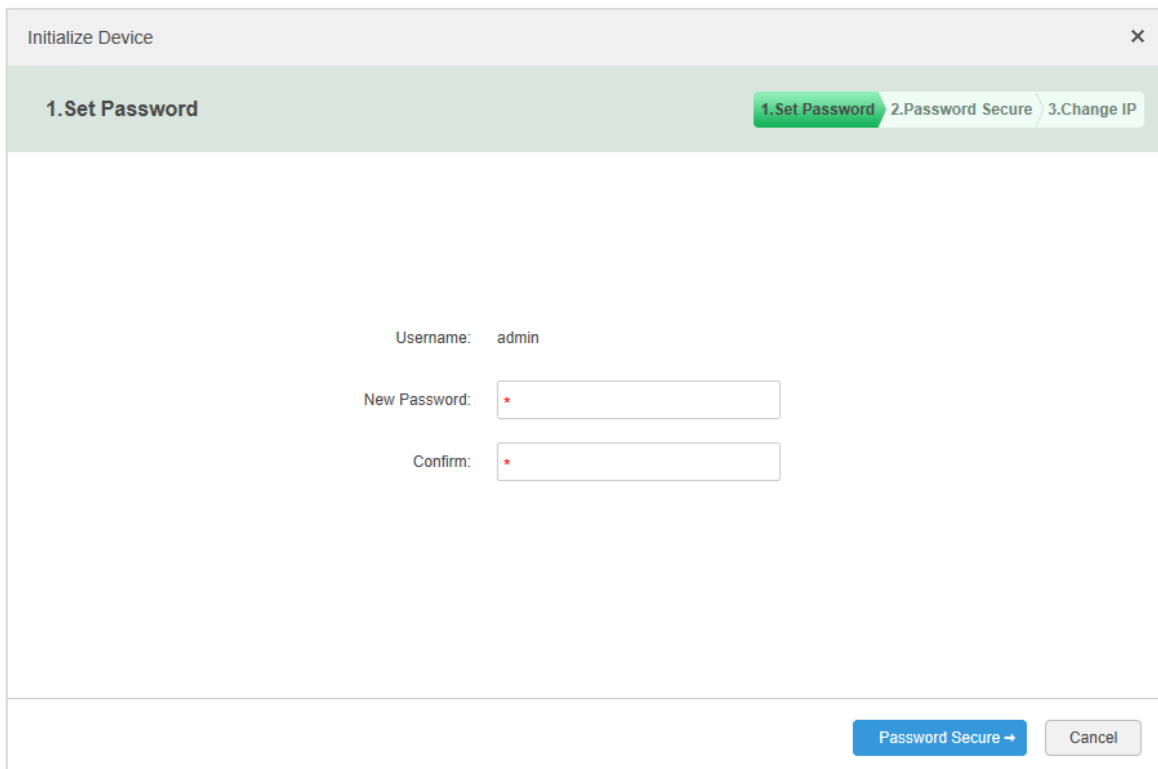
<input type="checkbox"/>	Init Status	IP Address	Device Model	Port	MAC Address
<input type="checkbox"/>	Uninitialized	192.168.1.100	DS-3A2204-01	37777	88:88:88:88:88:88
<input type="checkbox"/>	Initialized	192.168.1.101	DS-3A2204-01	37810	88:88:88:88:88:88
<input type="checkbox"/>	Initialized	192.168.1.102	DS-3A2204-01	37810	88:88:88:88:88:88
<input type="checkbox"/>	Initialized	192.168.1.103	DS-3A2204-01	37777	88:88:88:88:88:88

Step 3 Select an uninitialized device, and then click **Initialize**.



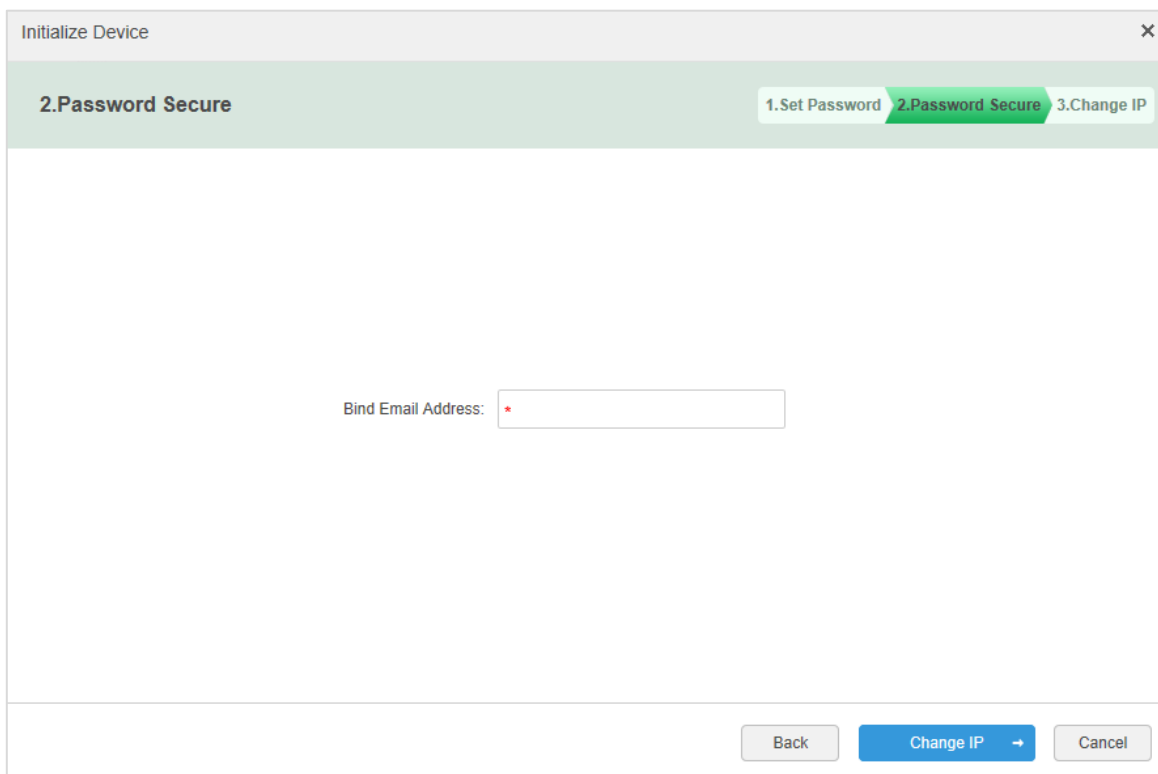
- You can select multiple devices to initialize them in batches. Make sure that the selected devices have the same username, password and email information.
- Click ▲ or ▼ next to **Init Status** to quickly sort out the status column, and then you can see all the uninitialized devices.

Figure 3-14 Set password



Step 4 Enter the password, and then click **Password Secure**.

Figure 3-15 Password security



Step 5 Enter the email address, and then click **Change IP**.




The email is used to receive security code for resetting password.

Figure 3-16 Change IP

Step 6 Enter the IP address, and then click **OK**.

3.4.3 Modifying Device IP Address

You can modify IP addresses of the devices that have not been added to the platform yet.

Step 1 Log in to the Web Manager. Click , and then select **Device**.

Step 2 Search for devices. See "3.4.1 Searching for Online Devices".

Figure 3-17 Search results

Init Status	IP Address	Device Model	Port	MAC Address
Uninitialized	192.168.1.1	DS-3A2008-01	37777	88-8E-46-04-00-00
Initialized	192.168.1.2	DS-3A2008-01	37810	88-8E-46-04-00-01
Initialized	192.168.1.3	DS-3A2008-01	37810	88-8E-46-04-00-02
Initialized	192.168.1.4	DS-3A2008-01	37777	88-8E-46-04-00-03

Step 3 Select a device, and then click **Change IP**.



For devices that have the same username and password, you can select and modify their IP addresses in batches.

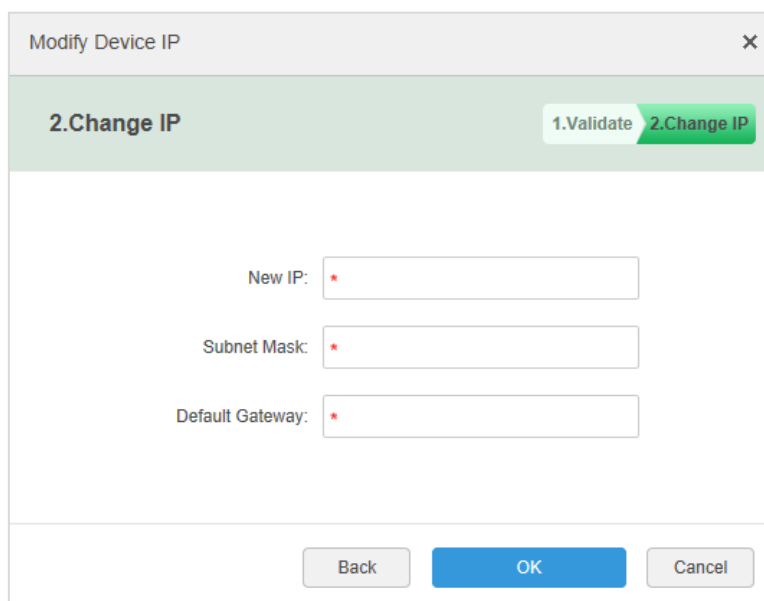
Step 4 Modify the IP address, and then click **OK**.

Figure 3-18 Verification



Step 5 Enter the username and password for logging in to the device, and then click **Change IP**.

Figure 3-19 Change IP



Step 6 Enter the IP address, and then click **OK**.

Step 7 Click **OK**.

3.4.4 Adding Devices

You can add different types of devices, such as encoder, decoder, ANPR device, access control, LED, video intercom and emergency assistance device. In this chapter, take adding encoder as an example. For other devices, the actual configuration interface shall prevail.

3.4.4.1 Adding Devices One by One

Step 1 Click **+** and select **Device** on the **New Tab** interface.

Figure 3-20 Device

The screenshot shows the 'Device' management interface. At the top, there are action buttons: Connect, Refresh, Initialize Device, and Change IP. Below these is a table of initialized devices with columns for Init Status, IP Address, Type, Port, and MAC Address. The table contains four rows, all with 'Initialized' status.

Below the table is a toolbar with '+ Add', 'Delete', 'Mod...', and 'Imp...' buttons, along with an 'Org:' dropdown menu set to 'root' and a search field.

At the bottom, there are tabs for different device categories: All, Encoder, Decoder, Video Wall, ANPR, Matrix, Access Control, Led Device, Video Intercom, and Emergency. Below the tabs is a detailed table of devices with columns for Device ID, IP/Domain, Home Server, Device Name, Type, Org, Status, Offline Cause, and Operation.

Device ID	IP/Domain	Home Server	Device Name	Type	Org	Status	Offline Cause	Operation
1001886		Center Server		Access Snapsho...	root	Offline	Network anomaly.	✎ ✕
1001880		Center Server		EVS	root	Offline	Network anomaly.	✎ ✕
1001878		Center Server		VTH	root	Offline	Network anomaly.	✎ ✕
1001875		Center Server		Access Snapsho...	root	Offline	Network anomaly.	✎ ✕
1001874		Center Server		NVR	root	Offline	Network anomaly.	✎ ✕
1001873		Center Server		Unit VTO		Offline	Network anomaly.	✎ ✕
1001872		Center Server		VTH		Offline	Network anomaly.	✎ ✕

Step 2 Click **Add**.

Figure 3-21 Add a device (1)

Step 3 Set parameters.



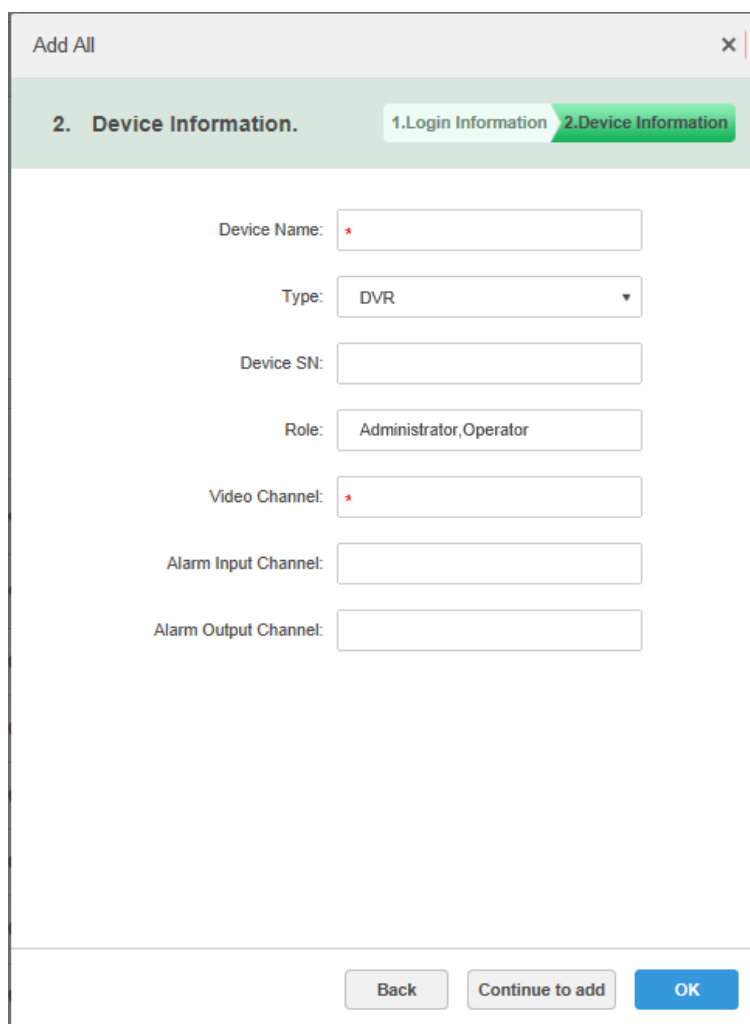
The parameters vary with the selected protocols. The actual interface shall prevail.

In the **Add Type** drop-down list,

- When **Auto Register** is selected, enter device registration ID. The auto register method is only for adding encoders and emergency alarm devices. The ID of auto register has to be in accordance with the registered ID configured at encoder. The port number must be the same on the platform and on the device. The auto register port is 9500 on the platform by default. To modify, open the system configuration tool to modify the DSS_ARS port number.
- When **Domain Name** is selected, the options are from the configured domain during deployment.

Step 4 Click **Add**.

Figure 3-22 Add a device (2)



Step 5 Set parameters.

Step 6 Click **OK**.

Click **Continue to add** more devices.

3.4.4.2 Adding Devices through Searching

Devices on the same LAN with the platform server can be added using the automatic search function.

Step 1 Click  and select **Device** on the **New Tab** interface.

Step 2 Search for online devices.

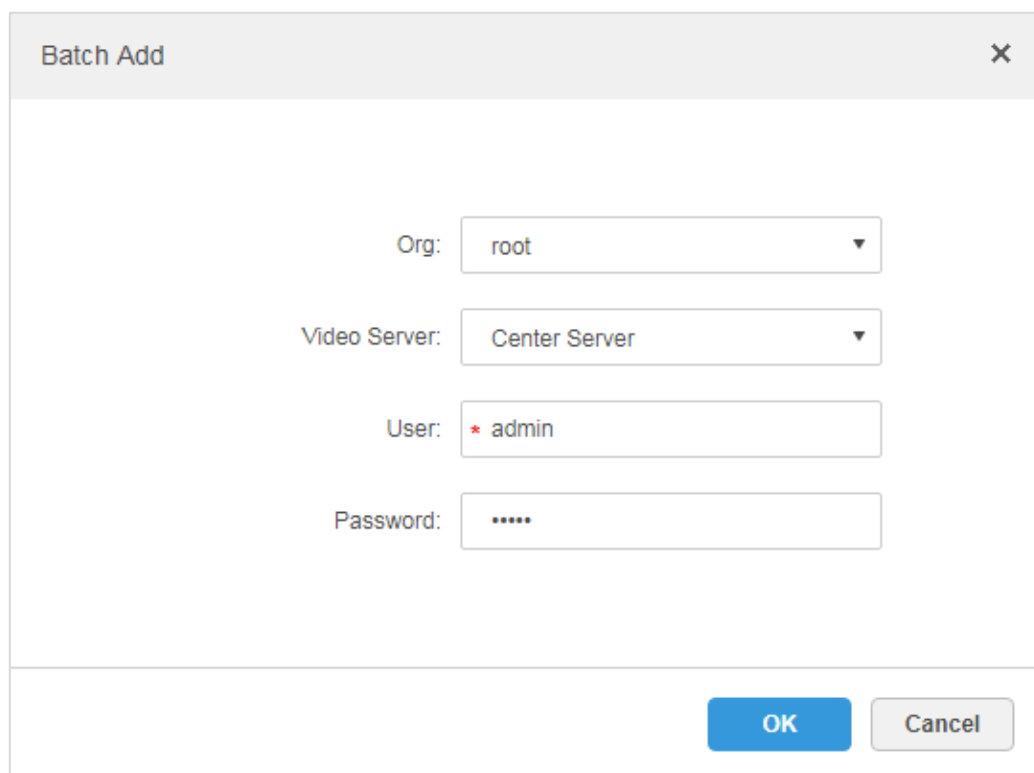
The search results are displayed.

Step 3 Select the device which needs to be added, and click **Connect**.



You can select multiple devices to add them in batches if they have the same username and password.

Figure 3-23 Batch add



Step 4 Set parameters, and then click **OK**.

The device is added into corresponding organization.

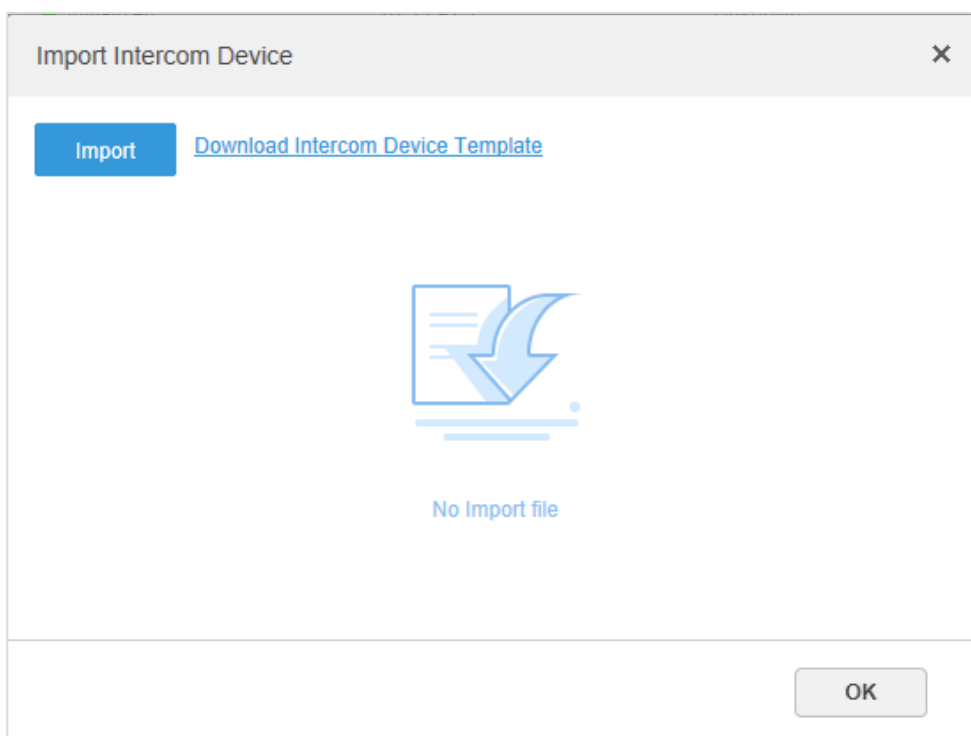
3.4.4.3 Importing Video Intercom Device

Fill in intercom device template, and then you can add intercom devices in batches.

Step 1 Click  and select **Device** on the interface of **New Tab**.

Step 2 Click **Import**.

Figure 3-24 Import video intercom devices (1)



Step 3 Click **Download Intercom Device Template** and save the template to PC according to interface tips.

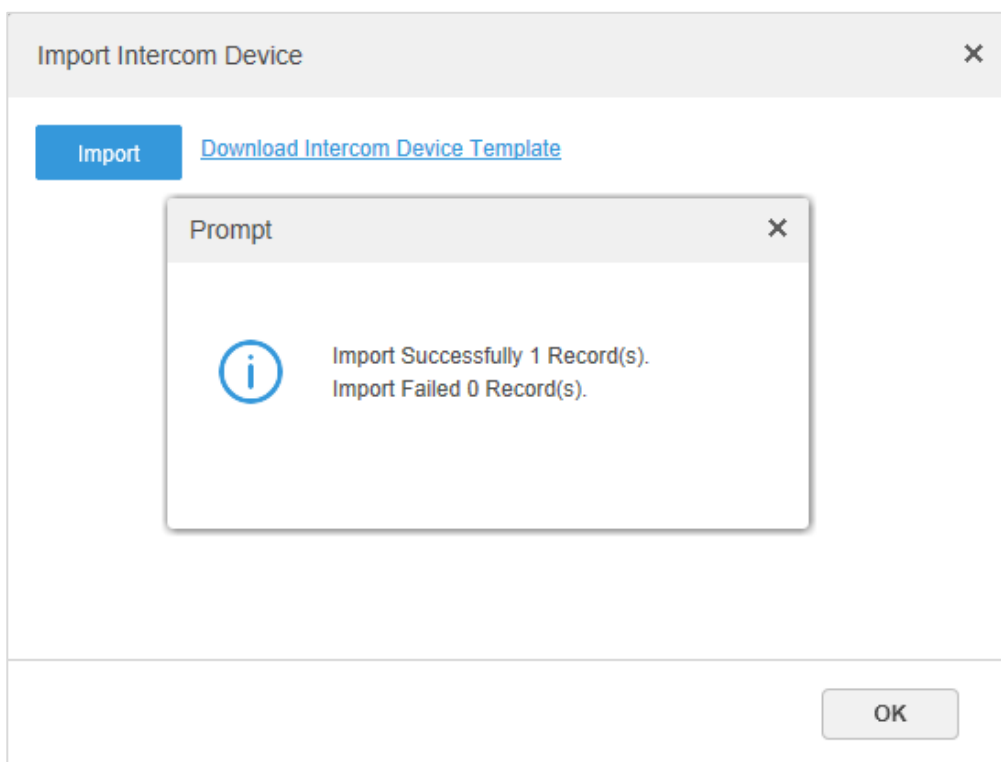
Step 4 Fill in the template according to the actual networking situation and then save the information.


Step 5 Click **Import** and select the completed template according to interface tips.



If the device is already added to DSS Pro in the template, then the system will prompt if it is to cover the existed device. You can select according to the actual situation.

Figure 3-25 Import video intercom devices (2)



Step 6 Click  and close the prompt box.

Step 7 Click **OK**.

3.4.5 Editing Devices

Modify device information and organization.

3.4.5.1 Modifying Device Information

Step 1 Click  and select **Device** on the New Tab interface.

Step 2 Click the corresponding  of device list.



Click **Get Info** and the system will synchronize device information.

Figure 3-26 Basic information

Step 3 Modify device basic information on the **Basic Info** interface.

Step 4 Click **Video Channel**, and then set the device channel name, channel features, camera type, No., keyboard code and face function.

Different types of devices have different features; the actual interface shall prevail. Device features include intelligent alarm, fisheye, face detection, face recognition and more. Select features according to the capability of the camera.

Figure 3-27 Set video channel features

Name	Camera Type	Features	SN	KeyBoard Code
Channel0	Fixed Camera	Intelligent Alarm, Elec...		

Step 5 Click the **Alarm Input Channel** tab, and then configure channel name and alarm type of alarm input.



Skip the step unless when the added devices support alarm input.

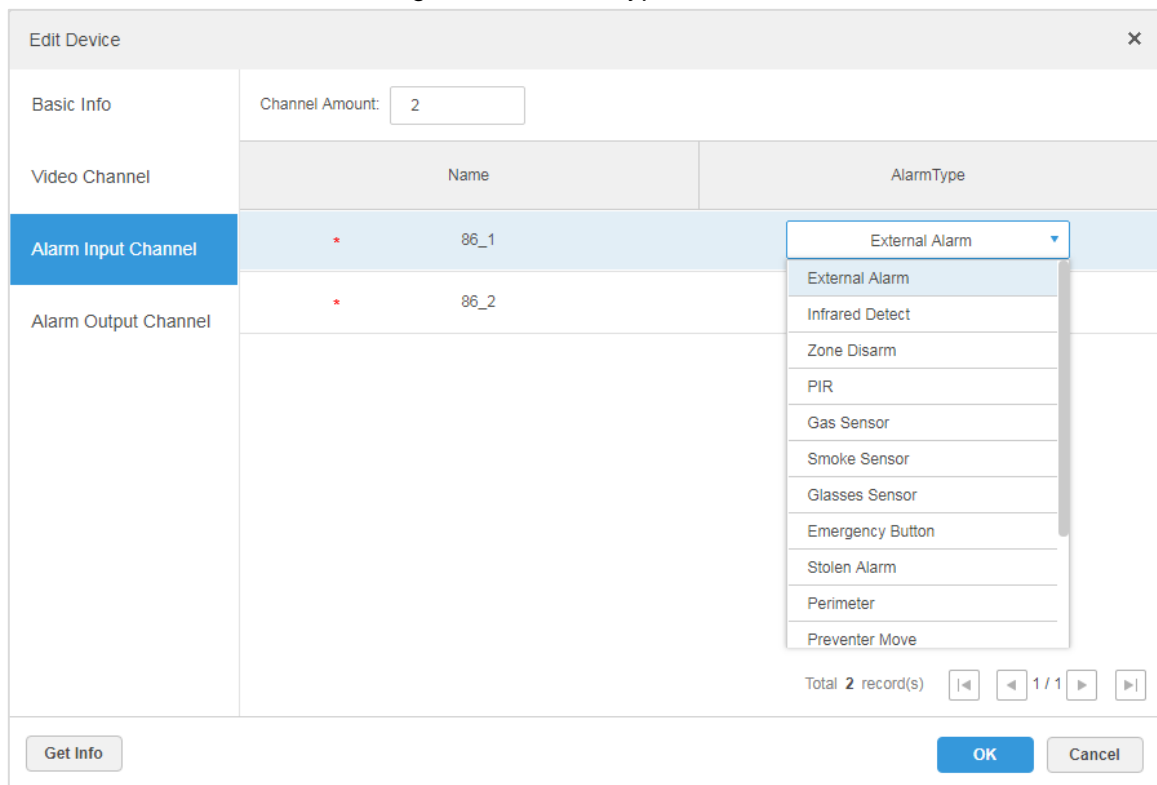
- Alarm type includes external alarm, IR detect, zone disarm, PIR, gas sensor, smoke sensor, glass sensor, emergency button, stolen alarm, perimeter and preventer move.
- Alarm type supports custom. Select **Customize Alarm Type** in the **Alarm Type** drop-down list. Click **Add** to add new alarm type. It supports max 30 custom newly-added alarm types.



Custom alarm supports modification and deletion.

- If custom alarm type is used by alarm plan, then it is not allowed to deleted but modified.
- When the name of the custom alarm type is modified, the history data remains the original name, while the new data adopts the modified name.
- The alarm input channel of alarm host is **Alarm Host Alarm** by default; the types of other alarm input channel are **External Alarm** by default.

Figure 3-28 Alarm type



Step 6 Click the **Alarm Output Channel** tab and then modify the name of alarm output channel.

Figure 3-29 Modify alarm output name

Video Channel	Name
Alarm Input Channel	* 86_1
Alarm Output Channel	* 86_2

Total 2 record(s) |< < 1 / 1 > >|

Get Info OK Cancel

Step 7 Click **OK** to finish modification.

3.4.5.2 Modifying Device Organization

You can move a device from an organization node to another one.

Step 1 Click **+**. On the **New Tab** interface, select **Organization**.

Step 2 Select a device to be moved, and then click **Move To**.

Figure 3-30 Move device


IP Address	Type	Home Server	Port	Status
	Access Control	Center Server	37777	Online
	IPC	Center Server	37777	Online
	NVR	Center Server	37777	Online
	NVR	Center Server	37777	Online
	VTS	Center Server	37777	Online
	Unit VTO	Center Server	37777	Online
	VMP	Center Server	37777	Online
	Access Control	Center Server	37777	Online

Step 3 Select the target organization node, and then click **OK**.

3.4.6 Binding Resources

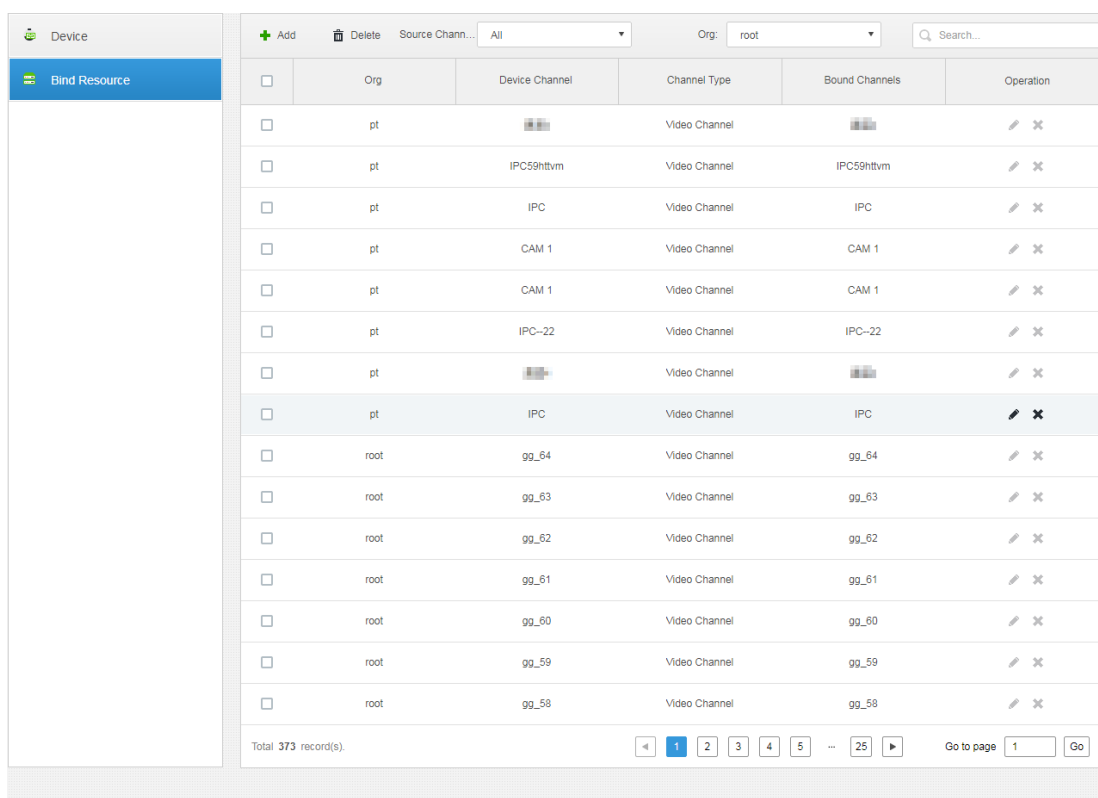
The platform supports binding resources for linked actions. You can bind a video channel with an alarm input channel, ANPR channel, POS channel, access control channel or another video channel, so that you can view the associated video for alarm, face and other businesses.



































Adding Resource Bind

Step 1 Log in to the Web Manager. Click , and then select **Device**.

Step 2 Click **Resource Bind**.

Figure 3-31 Bind resource

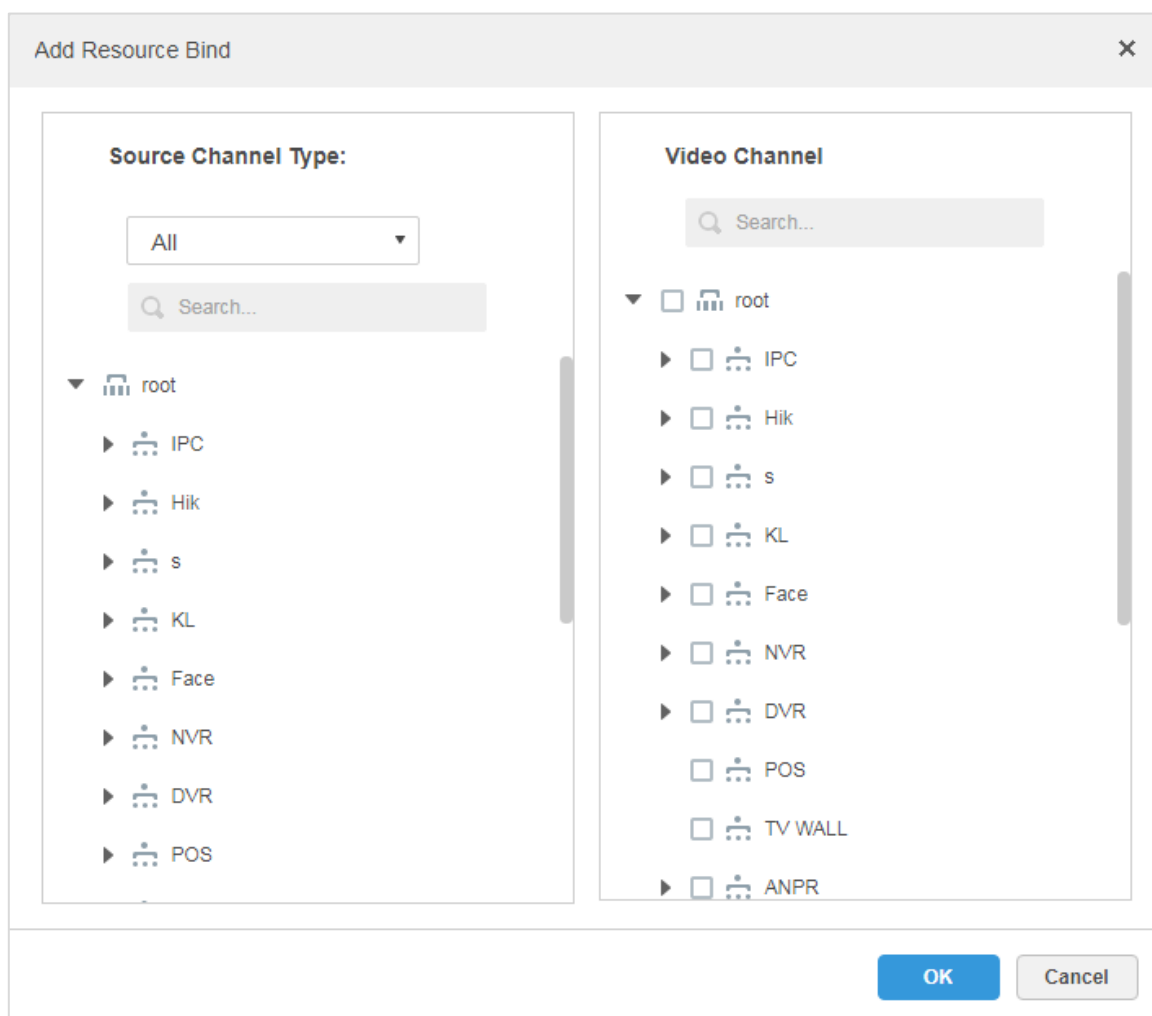


<input type="checkbox"/>	Org	Device Channel	Channel Type	Bound Channels	Operation
<input type="checkbox"/>	pt		Video Channel		 
<input type="checkbox"/>	pt	IPC59htvm	Video Channel	IPC59htvm	 
<input type="checkbox"/>	pt	IPC	Video Channel	IPC	 
<input type="checkbox"/>	pt	CAM 1	Video Channel	CAM 1	 
<input type="checkbox"/>	pt	CAM 1	Video Channel	CAM 1	 
<input type="checkbox"/>	pt	IPC-22	Video Channel	IPC-22	 
<input type="checkbox"/>	pt		Video Channel		 
<input type="checkbox"/>	pt	IPC	Video Channel	IPC	 
<input type="checkbox"/>	root	gg_64	Video Channel	gg_64	 
<input type="checkbox"/>	root	gg_63	Video Channel	gg_63	 
<input type="checkbox"/>	root	gg_62	Video Channel	gg_62	 
<input type="checkbox"/>	root	gg_61	Video Channel	gg_61	 
<input type="checkbox"/>	root	gg_60	Video Channel	gg_60	 
<input type="checkbox"/>	root	gg_59	Video Channel	gg_59	 
<input type="checkbox"/>	root	gg_58	Video Channel	gg_58	 

Total 373 record(s). 1 2 3 4 5 ... 25 Go to page Go

Step 3 Click **Add**.

Figure 3-32 Add resource to bind




Step 4 Select source channel and video channel respectively, and then click **OK**.

3.5 Adding Role and User

Users of different roles have different permissions of device access and operation. When creating a user, assign a role to it to give the corresponding permissions.

3.5.1 Adding User Role

A role is a set of permission. Classify users of the platform into different roles so that they can have different permissions for operating the devices, functions and other system resources.

Step 1 Log in to the Web Manager. Click , and then select **User**.

Step 2 Click the **Role** tab.

Step 3 Click **Add**, set role information, and then select device and control permissions and assign the rule to users.


- Select a role from the **Copy from** drop-down list to copy the settings to the selected rules.
- If no device and control permissions are selected for the user, this user will not have the corresponding permissions.

Figure 3-33 Add a role

Step 4 Click **OK**.

3.5.2 Adding User

Create a user account for logging in to the platform.

Step 1 Log in to the Web Manager. Click , and then select **User**.

Step 2 Click **User** tab.

Figure 3-34 Add a user (1)

Role + Add 🗑 Delete 📄 Import Domain User <input type="text" value="Search..."/>						
<input type="checkbox"/>	Username	Role	Status	User Type	Operation	
<input type="checkbox"/>	ym	Administrator	● Online	Normal User		
<input type="checkbox"/>	asd		● Offline	Normal User		
<input type="checkbox"/>	77888111	Administrator	● Offline	Normal User		
<input type="checkbox"/>	778888	Administrator	● Offline	Normal User		
<input type="checkbox"/>	1		● Offline	Normal User		
<input type="checkbox"/>	ll	Administrator,ll	● Offline	Normal User		
<input type="checkbox"/>	zhhq	Administrator	● Offline	Normal User		
<input type="checkbox"/>	testtk	Administrator,Operator,ll	● Offline	Normal User		
<input type="checkbox"/>	A	A-role	● Offline	Normal User		
<input type="checkbox"/>	chenjie	Administrator	● Offline	Normal User		
<input type="checkbox"/>	21396	Administrator	● Offline	Domain User		
<input type="checkbox"/>	lmx	ll	● Online	Normal User		
	system	Administrator:99,100,120,121	● Online	Normal User		

Total 13 record(s). Go to page 1 Go

Step 3 Click **Add**.

Figure 3-35 Add a user (2)

Basic Info

Username:
 Password Expiry:

Multiple Points of Presence: CN MAC Address:

Password:
PTZ Control Permission:

Confirm:
Email Address:

Remark:

Role

<input type="checkbox"/>	Role name
<input checked="" type="checkbox"/>	Administrator
<input type="checkbox"/>	Operator
<input type="checkbox"/>	role1

Device Permissions

- ▼ root
- ▼ 10.33.68.8
- Channel0

Control Permissions

- ▼ All Permissions
- ▼ Control Permissions
- Record
- Record Lock
- Record Tag
- PTZ
- Audio Talk




Step 4 Configure user information, select role below, and it will display device permission and operation permission of corresponding role on the right.



- The user has no **Device Permission** or **Operation Permission** if it fails to select **Role**.
- You can select several roles at the same time.

Step 5 Click **OK** to add the user.

Operations

- Click  to freeze user. The frozen user cannot log in to the Control Client, Web Manager and App.
- Click  to modify user information except username.
- Click  to delete user.

3.5.3 (Optional) Setting Domain User

This setting is optional. You can import domain users from the domain system of your current organization to create platform users.

Step 1 Configuring Domain Information


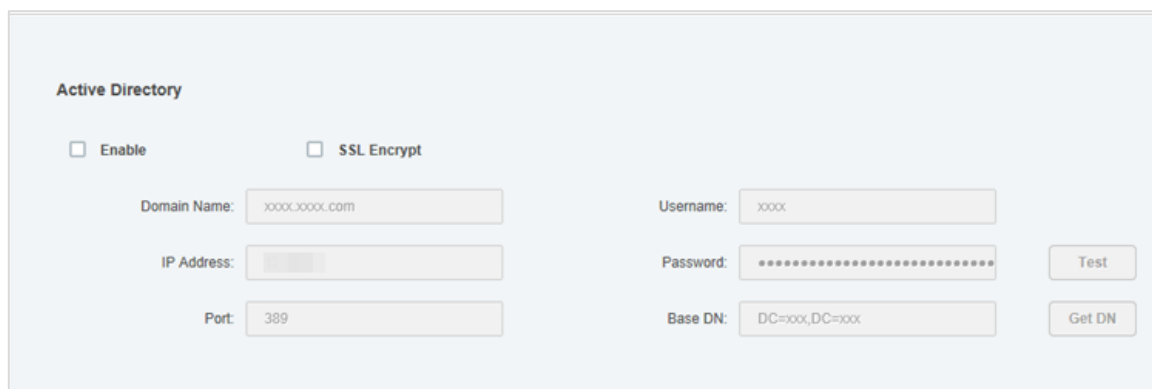
- 1) Log in to the Web Manager. Click , and then select **System** on the **New Tab** interface.
- 2) Click **Active Directory** and configure domain information.
- 3) Select the **Enable** check box, and then set domain information.
 - ◇ After setting domain information, click **Get DN** and it will acquire basic DN information automatically.
 - ◇ After getting DN information, click **Test** to test if domain information is available.


Figure 3-36 Set active directory



The screenshot shows the 'Active Directory' configuration page. At the top left, there are two checkboxes: 'Enable' (unchecked) and 'SSL Encrypt' (unchecked). Below these are several input fields: 'Domain Name' (containing 'xxxx.com'), 'IP Address' (empty), 'Port' (containing '389'), 'Username' (containing 'xxxx'), 'Password' (masked with dots), and 'Base DN' (containing 'DC=xxx,DC=xxx'). To the right of the 'Password' and 'Base DN' fields are two buttons: 'Test' and 'Get DN'.

- 4) Click **Save**.

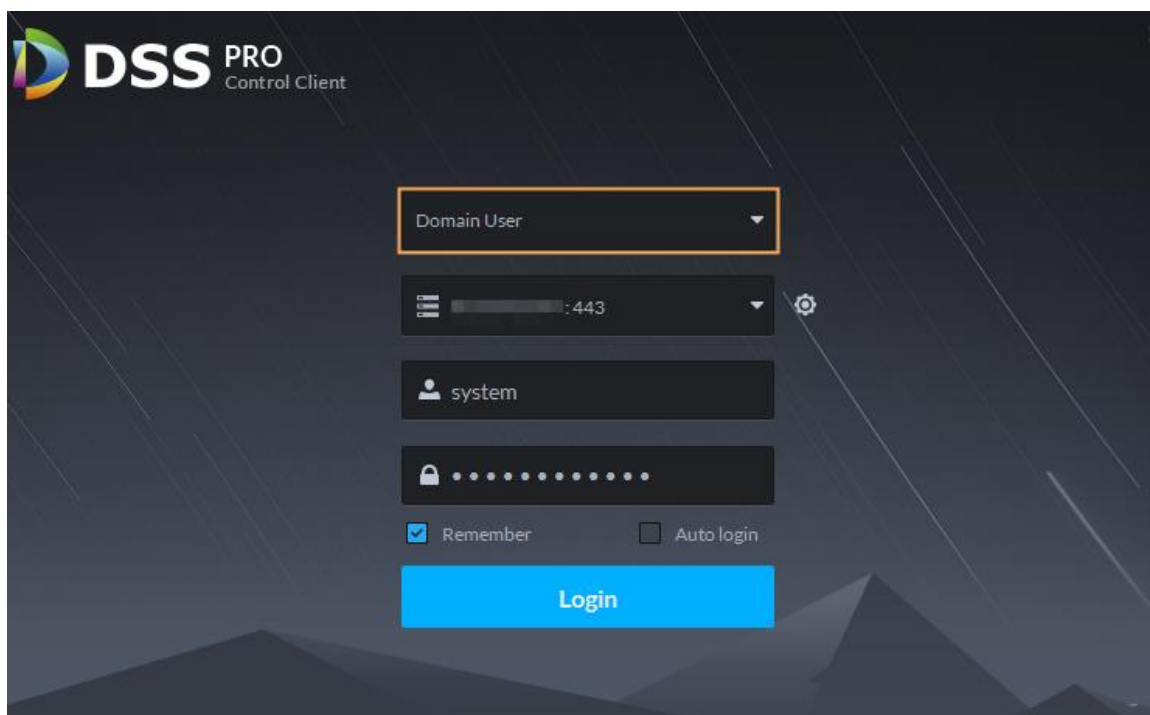
Step 2 Import domain users.

- 1) Log in to the Web Manager, click , and then select **User** on the **New Tab** interface.

- 2) Click the **User** tab, and then click **Import Domain User**.
- 3) Select the users to be imported, and then click **Next**.
You can also search for a user by entering keywords in the search box.
- 4) Select the roles, and then click **OK**.

To log in using a domain user account, start the Control Client, and then select **Domain User** for user type.

Figure 3-37 Domain user login



3.6 Configuring Record Plan

Configure record plans for video channels so that they can record videos accordingly.


3.6.1 Configuring Storage Disk

Add storage disks that can be used to store pictures and videos. You can add net disks and local disks.

3.6.1.1 Configuring Net Disk



- The storage server is required to be deployed.
- One user volume of the current net disk can only be used by one server at the same time.
- User volume is required to be formatted when adding net disk.

Step 1 Log in to Web Manager, click , and then select **Storage**.


Step 2 Select **Storage Config > Net Disk**.

Figure 3-38 Set net disk

Server Name	IP	Volume Name	Capacity(GB)	Free Capacity(GB)	Disk Type	Disk status	Operation
Center Server		20-pic	50.00	49.97	Picture	Normal	
Center Server		20-video	50.00	26.66	Video	Normal	
Center Server		26-1	100.00	38.44	Video	Normal	
Center Server		26-2	100.00	0.00	Video	Normal	
Center Server		26-3	100.00	0.00	Video	Normal	
Center Server		26-4	100.00	19.55	Video	Normal	
Center Server		26-5	100.00	95.95	Picture	Normal	
Center Server		4004-s2-1	300.00	250.67	Video	Normal	
Center Server		4004-s2-2	300.00	299.97	Video	Normal	
Center Server		e1	32.00	4.05	Video	Normal	
Center Server		e10	80.00	0.00	Video	Normal	
Center Server		e13	110.00	0.00	Video	Normal	
Center Server		e15	110.00	0.00	Video	Normal	
Center Server		e16	120.00	0.00	Picture	Normal	

Step 3 Click **Add**.

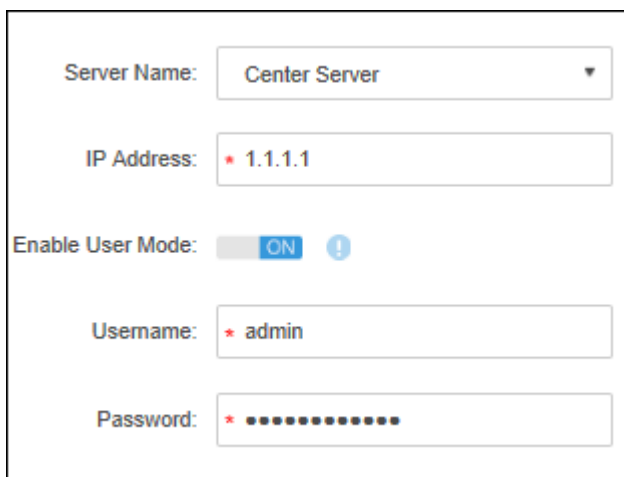
Step 4 Select server name, enter the IP address of net disk, and click **OK**.

- User mode: Enter the username and password of a disk user that have the permission of volumes on the net disk. Enable the user mode to add all the volumes of this user.
- User mode disabled: The platform shows the volumes not assigned to any user on the disk. The volumes in red are being used. To force to get it, click .



To force to get the disk, you need to format it. Data will be cleared after the disk is formatted. You are recommended to back up the data in advance.

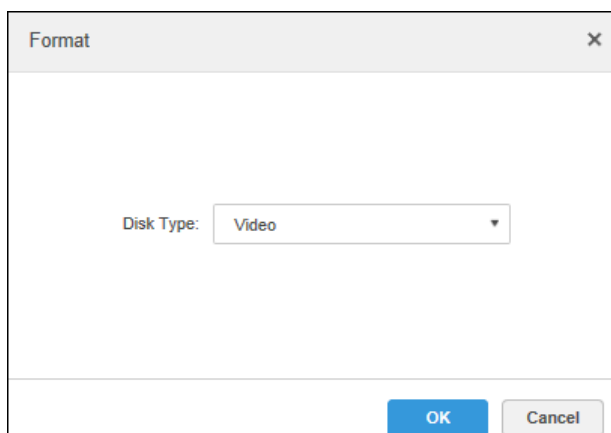
Figure 3-39 Add net disk



Step 5 Select disk, click **Format** or click the  next to the disk information to format the corresponding disk.

Step 6 Select format disk type, and then click **OK**.


Figure 3-40 Format disk



Step 7 Click **OK** in the prompt box to confirm formatting.

3.6.1.2 Configuring Local Disk

Configure local disk to store different types of files, including videos, ANPR snapshots, and face or alarm snapshots. In addition to the local disks, you can also connect an external disk to the platform server, but you have to format the external disk before using it.

Step 1 Click , and then select **Storage**.

Step 2 Select **Storage Config > Local Disk**.

Step 3 Configure local disk.


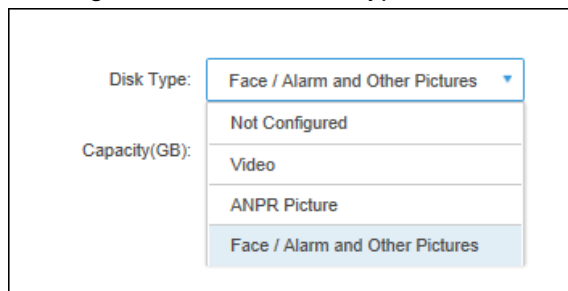
- Click  and configure disk type according to interface prompt.


Figure 3-41 Select disk type



Disk Type: Face / Alarm and Other Pictures ▼

Capacity(GB):

- Not Configured
- Video
- ANPR Picture
- Face / Alarm and Other Pictures

- Select disk and click **Format**, or click  next to disk information and format the disk according to interface prompt and configure disk type.

3.6.2 Configuring Disk Group Quota

Allocate disk groups for video storage.

Step 1 Click  and select **Storage** on the interface of **New** tab.

Step 2 Click the **Group Quota** tab.

Figure 3-42 Server status



Name	Status	Operation
172.22.151.19	● Online	
10.35.92.65	● Offline	
10.35.92.19	● Offline	
Center Server	● Online	


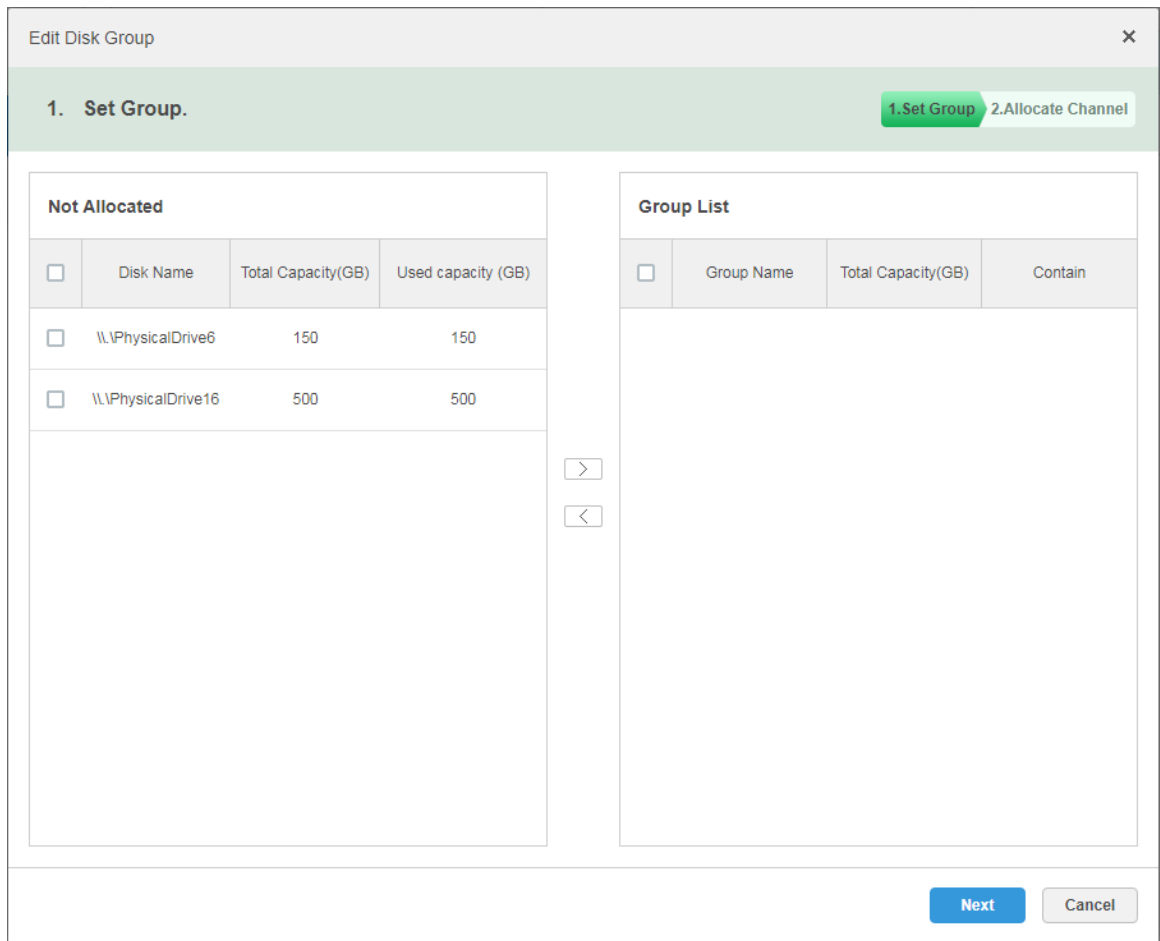

Step 3 Click  next to the online/offline of status server.

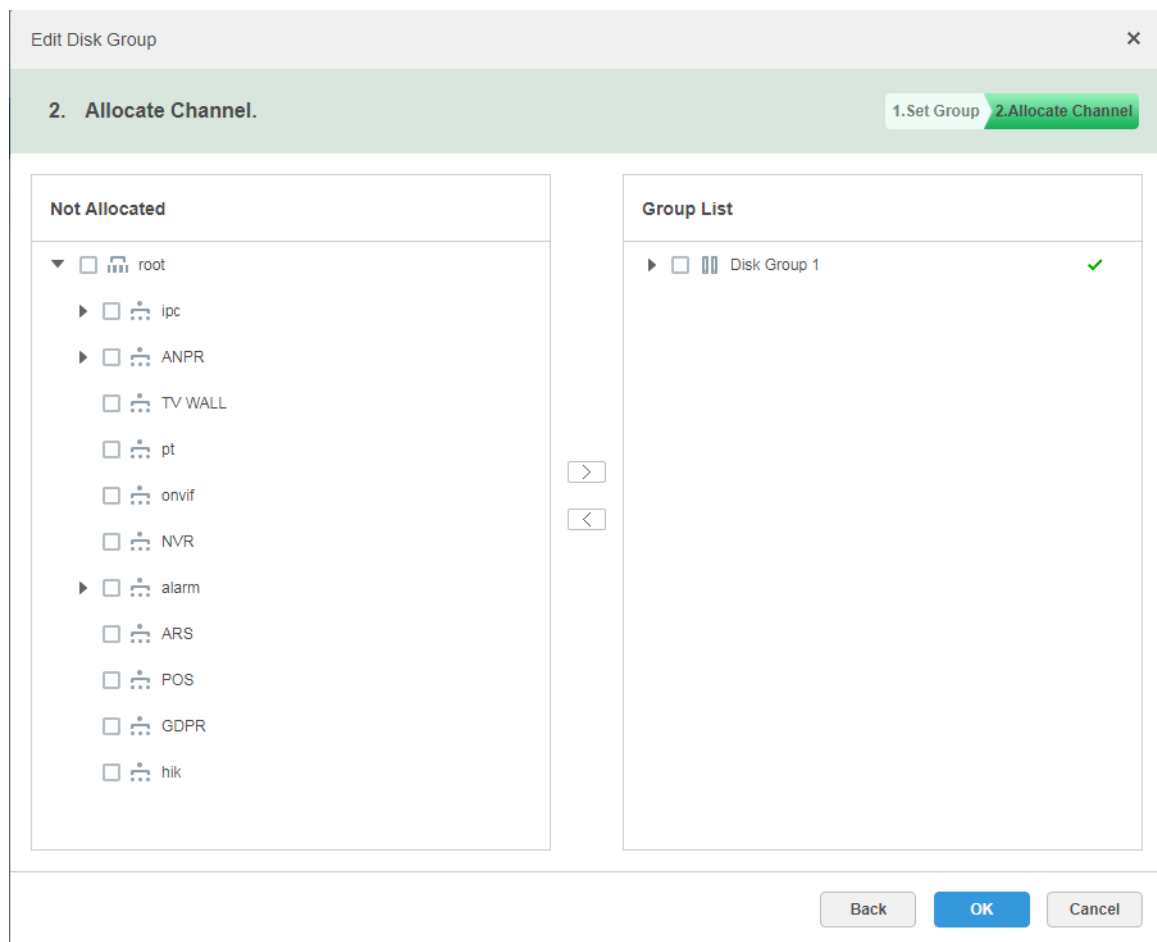
Figure 3-43 Edit disk group




Step 4 Select the undistributed disks on the left, click  and add it to the disk group list on the right.

Step 5 Click **Next** to distribute channels for disk group.

Figure 3-44 Allocate channels



Step 6 Select channels in the device list on the left, click  to add it to the disk group on the right.

Step 7 Click **OK**.

3.6.3 Adding Recording Plan

Step 1 Click  and select **Storage** on the interface of **New** tab.

Step 2 Click the **Record Plan** tab, and then click **Add**.

Figure 3-45 Add recording plan

Step 3 Select a video channel, and then set parameters.



- **Stream type:** Select main stream, sub stream 1, or sub stream 2. The stream type selected here must be enabled on the device.
- **Time template:** Select the system default template or new template. See "3.6.5 Adding Time Template."
- **Storage position:** Select **Store on the Server** to store on the platform server disks; select **Store on Recorder** to store on the device.

Step 4 Click **OK**.

Operations

- Enable/disable general plan

In the operation column, means that the plan has been enabled, click the icon and it becomes , and it means that the plan has been disabled.

- Edit General Plan

Click of corresponding plan to edit the general plan.

- Delete General Plan

◇ Select general plan, click **Delete** to delete plans in batches.

◇ Click of corresponding general plan to delete the individual general plan.

3.6.4 Configuring Storage Backup

Configure storage backup so that the videos on the device can be automatically uploaded to DSS Pro for redundant storage. The backup covers videos of the previous three days from now.

Step 1 Click **+** and select **Storage** on the interface of **New** tab.

Step 2 Click the **Backup Record Plan** tab.

Figure 3-46 Backup plan

Plan Name	Backup Record Length	Condition	Operation
PC_NVR	6	18:00 - 17:59 跨天	OFF
98	24	00:00 - 23:59	ON
NEW	1	02:00 - 00:01 跨天	OFF

Step 3 Click **Add** to add backup plan.

Step 4 Select corresponding devices on the left device tree, and enter plan name.

Step 5 Set backup conditions.

- Take time as condition.

Figure 3-47 Add backup plan

Add Backup Record Plan

Available Video Channels

- root
 - IPC
 - Hik
 - s
 - KL
 - Face
 - NVR
 - DVR
 - POS
 - TV WALL
 - ANPR

Backup record plan parameter.

Plan Name: *

Condition: Time

00:00 23:59

0 12 24 12 24

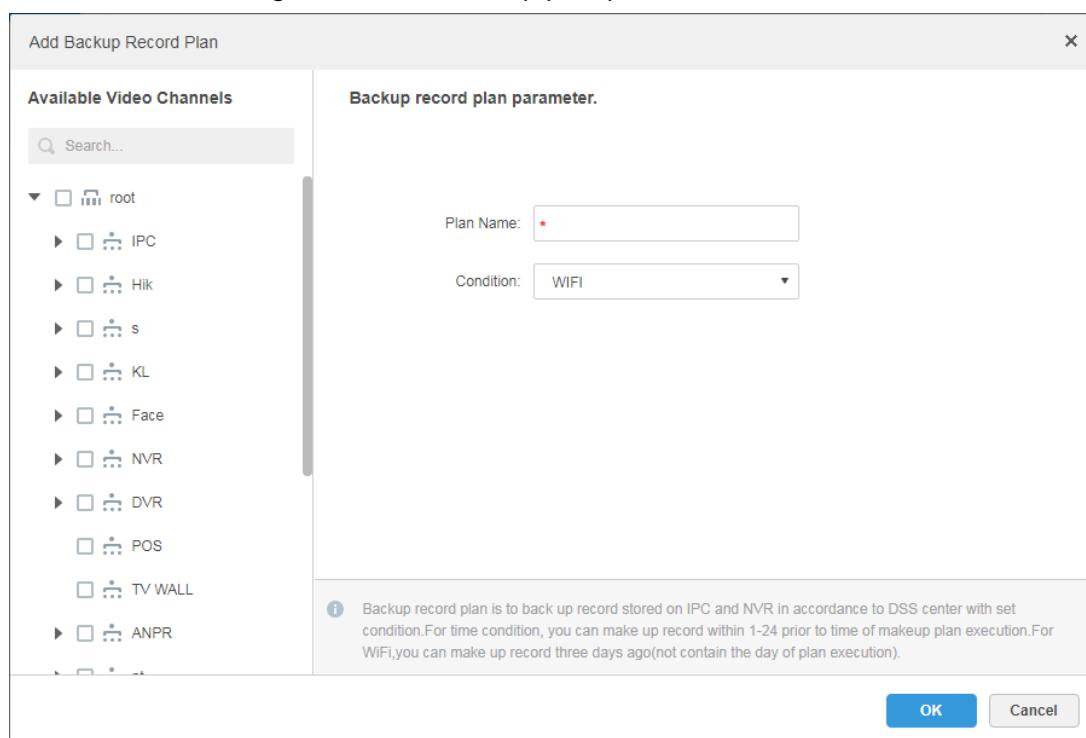
Backup Record Length: * Hour

OK **Cancel**

Backup record plan is to back up record stored on IPC and NVR in accordance to DSS center with set condition. For time condition, you can make up record within 1-24 prior to time of makeup plan execution. For WiFi, you can make up record three days ago (not contain the day of plan execution).

- Select **Time** in the backup condition.
 - Drag time line and set the time period of backup record plan.
 - Enter backup record length, click **OK**.
The time range is 1-24 hours.
- Take Wi-Fi as condition.

Figure 3-48 Set backup plan parameters



- 4) Select Wi-Fi in the backup record condition.
- 5) Click **OK**.

It will make backup record automatically when the network of backup device is switched to Wi-Fi.

Operations

- Enable/Disable backup record plan.

In operation column, means that the plan has been enabled; click the icon and it becomes , it means that the plan has been disabled.

- Edit record plan

Click the corresponding of the plan, and then you can edit the backup record plan.

- Delete record plan

◇ Select record plan, click **Delete** to delete plan in batches.

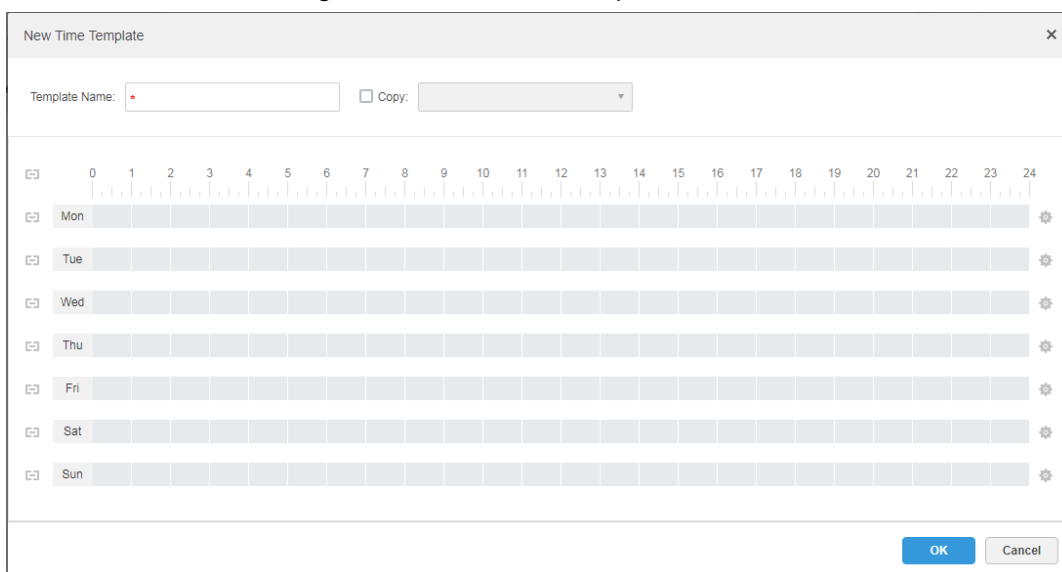
◇ Click the corresponding of record plan, then you can delete the plan individually.

3.6.5 Adding Time Template

Step 1 Click and select **Storage** on the interface of **New** tab.

Step 2 Select **New Time Template** in the **Time Template** drop-down box.

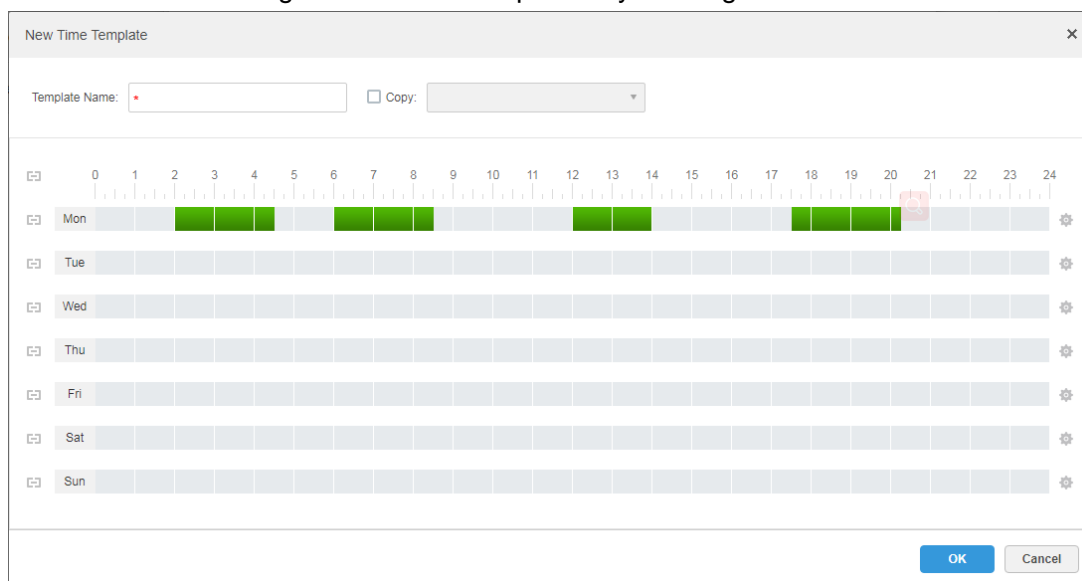
Figure 3-49 New time template



Step 3 Sets template name and time period.

- Press the left button and drag it to draw time period on the time line.

Figure 3-50 Set time period by drawing




- Click the  of the corresponding day, set time period on the **Period Setup** interface. See Figure 3-51.

Figure 3-51 Set time period by selecting

Period Setup [X]

Period1 02:00:00 — 04:30:00 + X

Period2 06:00:00 — 08:30:00 + X

Period3 12:00:00 — 14:00:00 + X

Period4 17:30:00 — 20:15:00 + X

All

Mon Tue Wed Thu Fri Sat Sun

OK Cancel



You can set up to 6 periods in one day.

Step 4 Click **OK** to save time template.



Select **Copy** and select the time template in the drop-down box, then you can directly copy the configuration of the time template.

3.7 Configuring Map

Select a map type between raster map and GIS map, and then drag the video channel, or alarm channel, and access control channel to the map before you can view them on the map during monitoring. The map displays alarm prompts, site video and resource position.

- A raster map is a floor plan or a picture of a place. The server enables raster map by default.
- GIS map includes Google map, Baidu map, and Gaode map. Take Google map for example.
 - ◇ Google online map: The online map is supported by the Google map server, and updates in real time. The PC for installing the Control Client is required to have access to Google's online map.
 - ◇ Google offline map: The offline map does not update. It is deployed on your local server. You need to get the offline map package for deploying it.

3.7.1 Adding Map

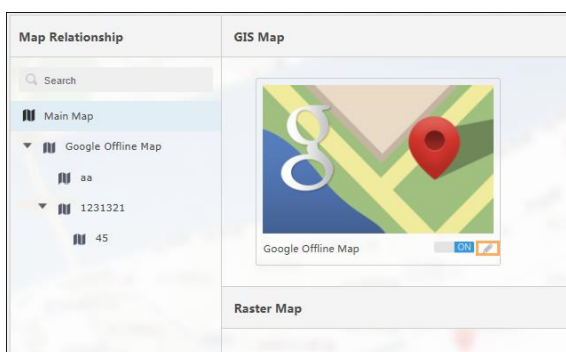
3.7.1.1 Adding GIS Map

Step 1 Log in to the Web Manager.

Step 2 Click  and select **Map** on the **New Tab** interface.

Step 3 Click  on the GIS map.

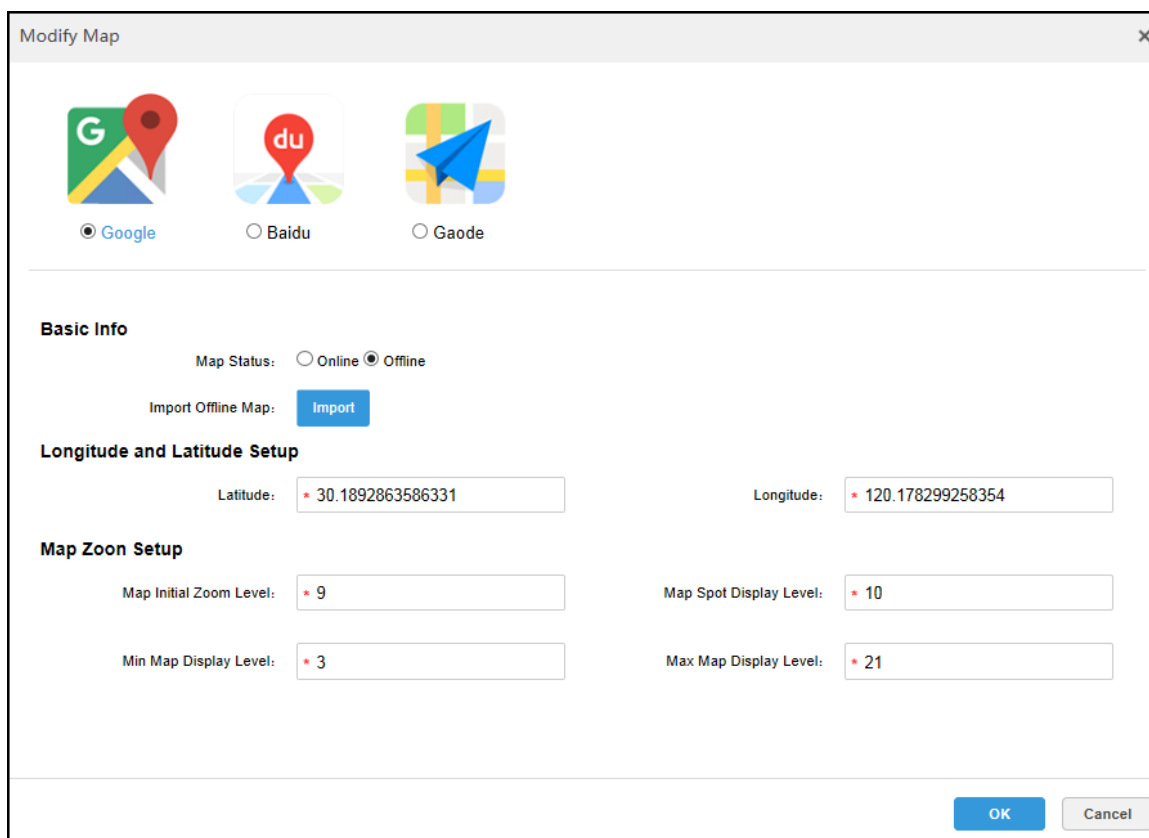
Figure 3-52 Map



Step 4 Select a map type, and then set parameters.

- Online map
 - 1) Select **Online**.
 - 2) Configure map information, and then click **OK**.
- Offline map
 - 1) Select **Offline**.
 - 2) Click **Import** and import offline map.
 - 3) Configure map information, and then click **OK**.

Figure 3-53 Map configuration



Modify Map

Google
 Baidu
 Gaode

Basic Info

Map Status: Online Offline

Import Offline Map:

Longitude and Latitude Setup

Latitude: Longitude:

Map Zoon Setup

Map Initial Zoom Level: Map Spot Display Level:

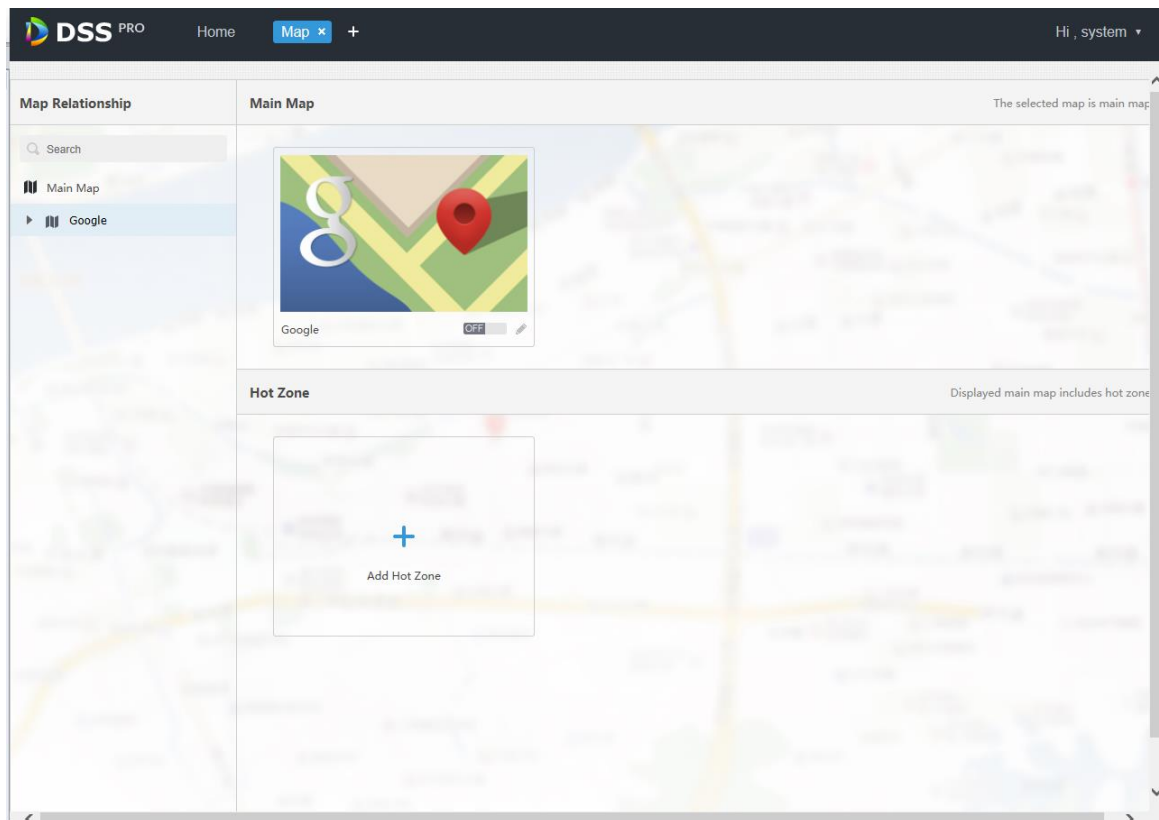
Min Map Display Level: Max Map Display Level:

Step 5 Add a hot zone.

Add the plane figure of a scenario, a parking lot for example, for area management.

- 1) On the map resource tree on the left, click the name of the map that you have just added, or open the GIS map and click **Add Hot Zone** at the upper-right corner.

Figure 3-54 GIS map



- 2) Click **Add Hot Zone**.

Figure 3-55 Add hot zone

Add Hot Zone
✕

Name:

Picture: Browse

Preview:

Import raster map, support PNG, JPG, JPEG

Remark:

Next
Cancel

- 3) Name the hot zone, upload the raster map of the zone, and then click **OK**.
- 4) Drag the map to adjust its position, and then click **OK**.
The hot zone is added.

3.7.1.2 Adding Raster Map

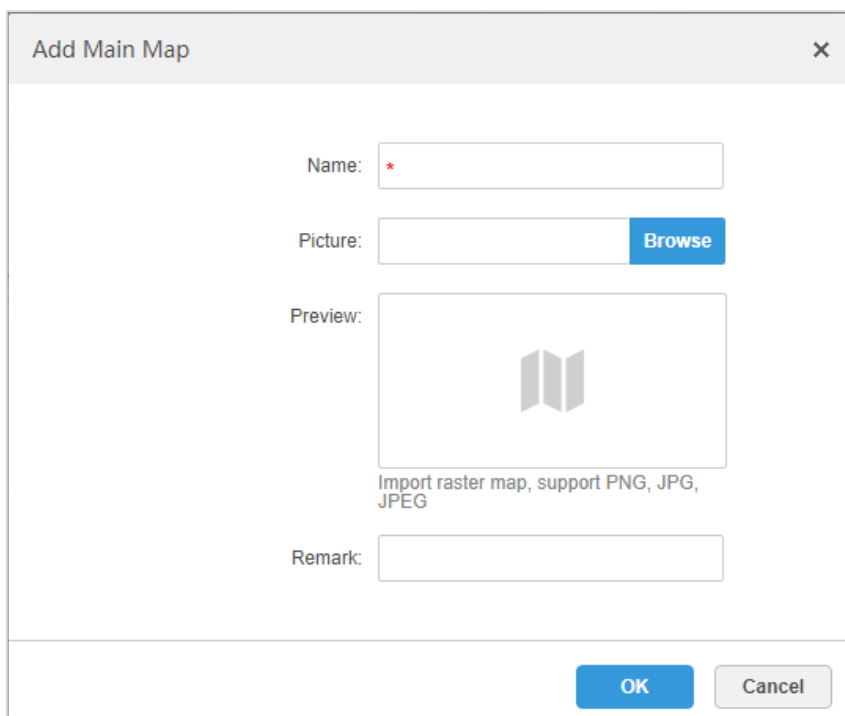
Import a raster map for adding a hot zone. You can add cameras, access control channels, and alarm channels onto the map to directly show them on the map.

Step 1 Log in to the Web Manager.

Step 2 Click  and select **Map** on the **New Tab** interface.

Step 3 Click **Add Raster Map**.

Figure 3-56 Adding main map



The screenshot shows a dialog box titled "Add Main Map" with a close button (X) in the top right corner. The dialog contains the following fields and elements:

- Name:** A text input field with a red asterisk (*) indicating it is required.
- Picture:** A text input field followed by a blue "Browse" button.
- Preview:** A large rectangular area containing a gray map icon.
- Text below Preview:** "Import raster map, support PNG, JPG, JPEG"
- Remark:** A text input field.
- Buttons:** "OK" (blue) and "Cancel" (gray) buttons at the bottom right.

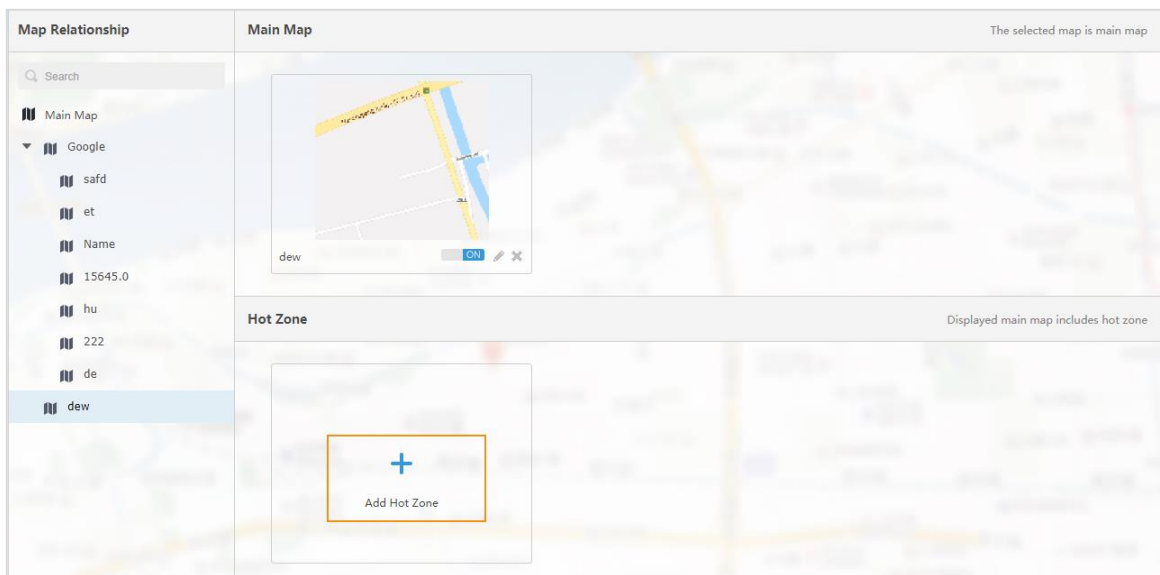
Step 4 Enter the map name, select the picture and then click **OK**.

Repeat from step 1 to step 2 to add more raster maps.

Step 5 Add a hot zone.

- 1) Click the added GIS map or raster map in the map list, or open the added map and click **Add Hot Zone** at the upper-right corner. The **Hot Zone** interface is displayed.

Figure 3-57 Adding hot zone



2) Click **Add Hot Zone**.

Figure 3-58 Adding hot zone

Add Hot Zone
✕

Name:

Picture: Browse

Preview:

Import raster map, support PNG, JPG, JPEG

Remark:

Next
Cancel

3) Enter the hot zone name, upload the picture, and then click **Next**.

4) Drag the picture to the desired position and click **OK**.

3.7.2 Marking Devices

Link a device to the map by dragging it to the corresponding location on the map according to its geographical location.

Step 1 Log in to the Web Manager, click , and then select **Map**.

Step 2 Click a main map from the main map section.

Figure 3-59 Map

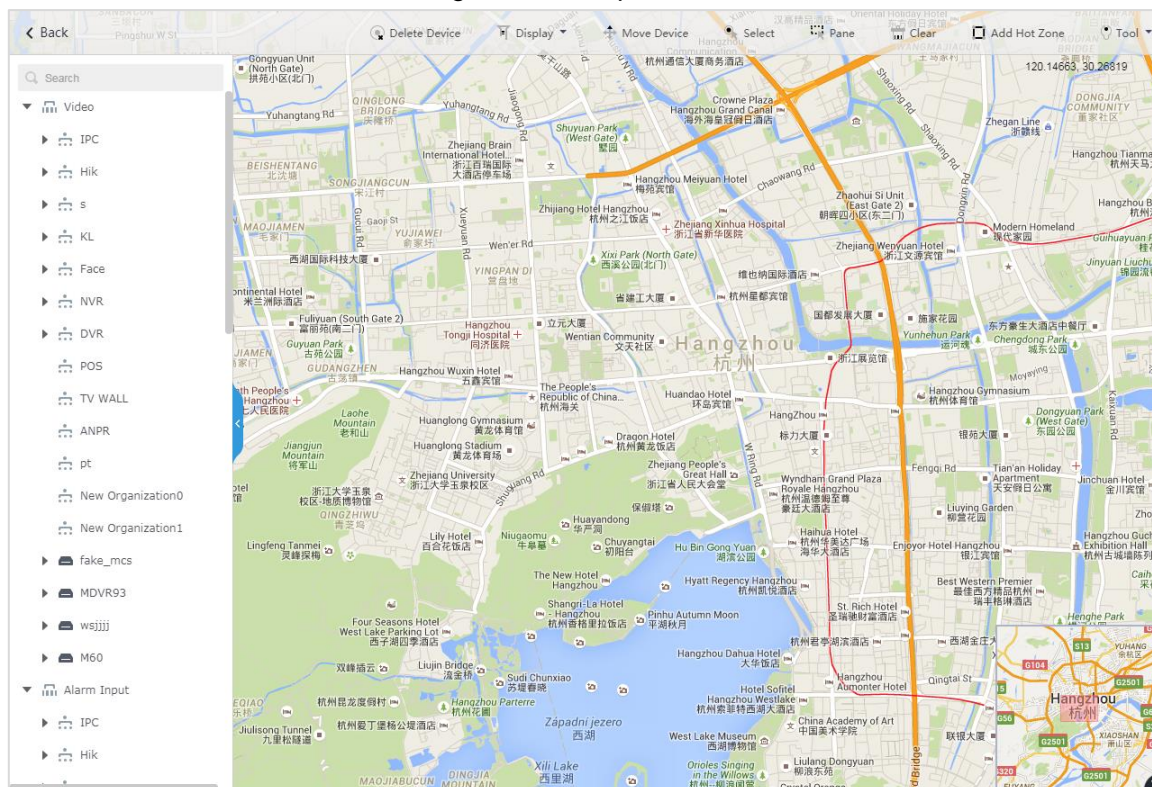


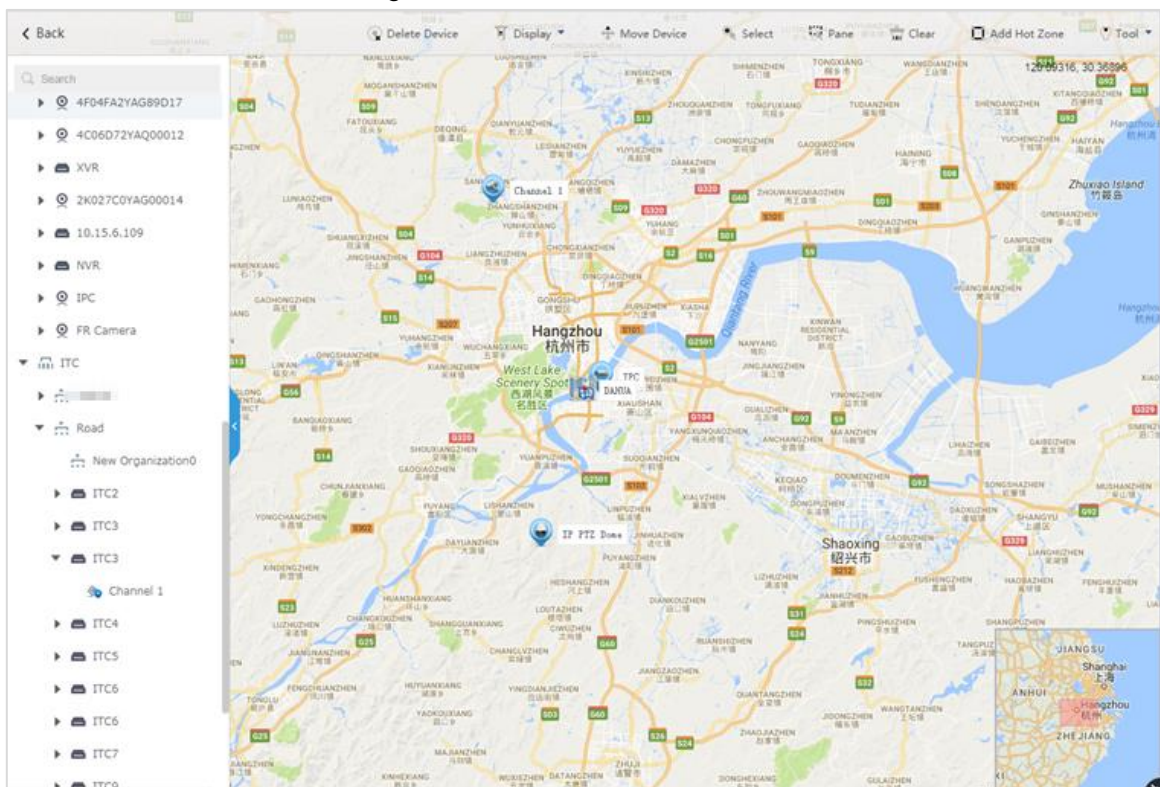
Table 3-1 Description

Parameters	Description
Display	<ul style="list-style-type: none"> Raster map displays: video; access control; alarm input; intelligence device. GIS map displays: video; alarm input; ITC; intelligence device.
Delete Device	Click to move the device location on the map.
Select	Select device via clicking on it.
Pane	Select device via box selection.
Clear	Clear the map.
Add Hot Zone	Click Add Hot Zone , select location on the map and add hot zone map. After entering hot zone, it can also continue to add lower-level hot zone map. Click hot zone on the client map, the system will automatically link the map to the hot zone map.

Tool	<p>Includes length, area, mark and reset.</p> <ul style="list-style-type: none"> ● Length: Measure the actual distance between two spots on the map. ● Area: Measure the actual area of the previous area on the map. ● Mark: Mark on the map. ● Reset: Restore the default location of the map.
Others	<ul style="list-style-type: none"> ● Click hot zone, and it can modify the information of hot zone map. ● Double-click hot zone, the system will automatically skip to hot zone map, and then it can drag it into the channel on the hot zone map.

Step 3 Drag the device channel from the left device tree to the corresponding location of the map.

Figure 3-60 Add a channel



4 Business Functions

This chapter introduces the configuration and operation of the video monitoring businesses, such as video wall, face recognition, ANPR, access control, and video intercom.

4.1 Preparations

Install the Control Client, and configure the basic settings before you can perform the business functions.

4.1.1 Installing Client

Daily video monitoring is achieved through the Control Client and mobile client.

4.1.1.1 Installing Control Client

4.1.1.1.1 Control Client Installation Requirements

To install Control Client, prepare a computer in accordance with the following requirements.

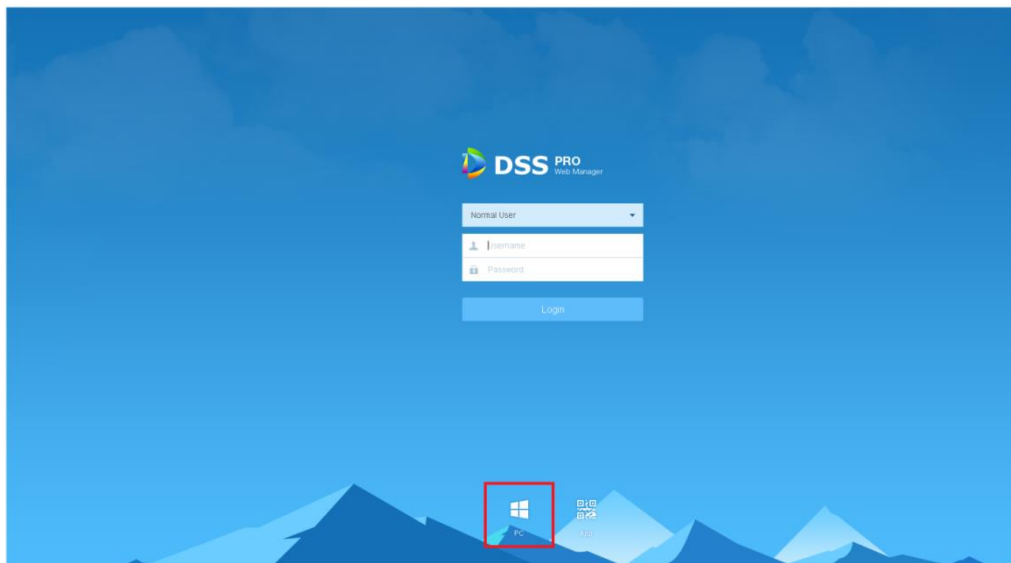
Table 4-1 Hardware requirements


Parameters	Description
Recommended Configuration	<ul style="list-style-type: none"> • CPU: i5-6500 • Main frequency: 3.20 GHz • Memory: 8 GB • Graphics: Inter HD Graphics 530 • Network Card: Gigabit Network Card • HDD Type: HDD 1T • DSS client installation space: 200 GB
Min. Configuration	<ul style="list-style-type: none"> • CPU: i3-2120 • Memory: 4 GB • Graphics: Inter(R) Sandbridge Desktop Gra • Network Card: Gigabit Network Card • HDD Type: HDD 300 GB • DSS client installation space: 100 GB

4.1.1.1.2 Downloading and Installing Control Client

Step 1 Enter IP address of DSS Pro into the browser and then press Enter.

Figure 4-1 Log in to the web manager



Step 2 Click  to download the client.

The **File Downloads** dialogue box is displayed.

Step 3 Click **Save** to save the client software package on the PC.

Step 4 Double-click the client setup.exe and begin installation.

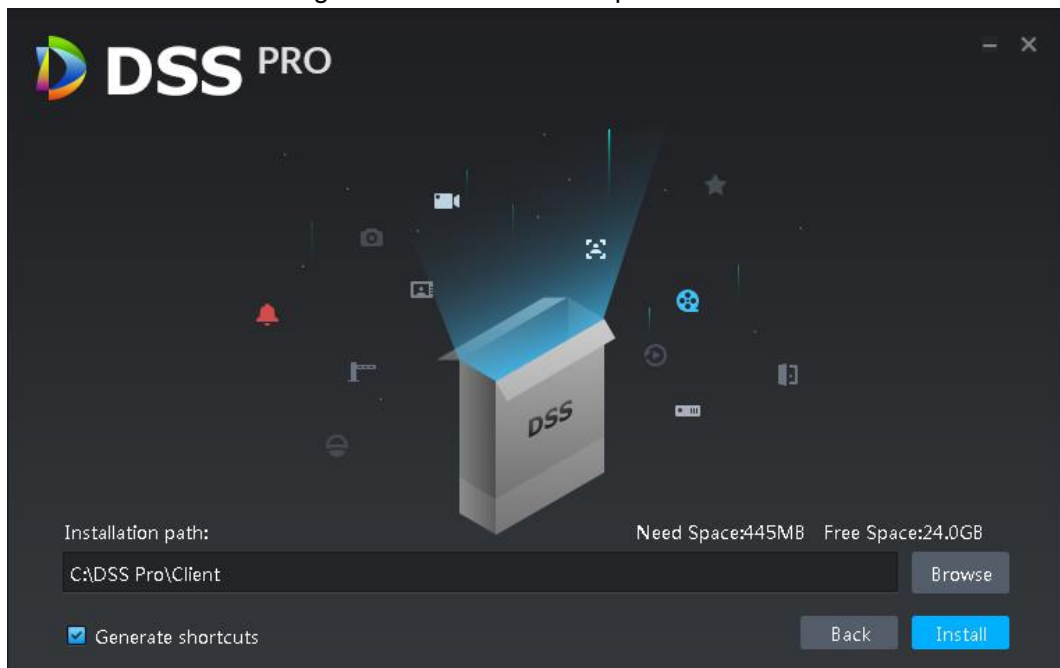
Figure 4-2 Accept agreement



Step 5 Select a language, select the box of **I have read and agree DSS agreement** and then click **Next** to continue.

Step 6 Select installation path.

Figure 4-3 Set installation path



Step 7 Click **Install** to install the client.

System displays installation process. It takes 3 to 5 minutes to complete. Please be patient.

Figure 4-4 Installation completed



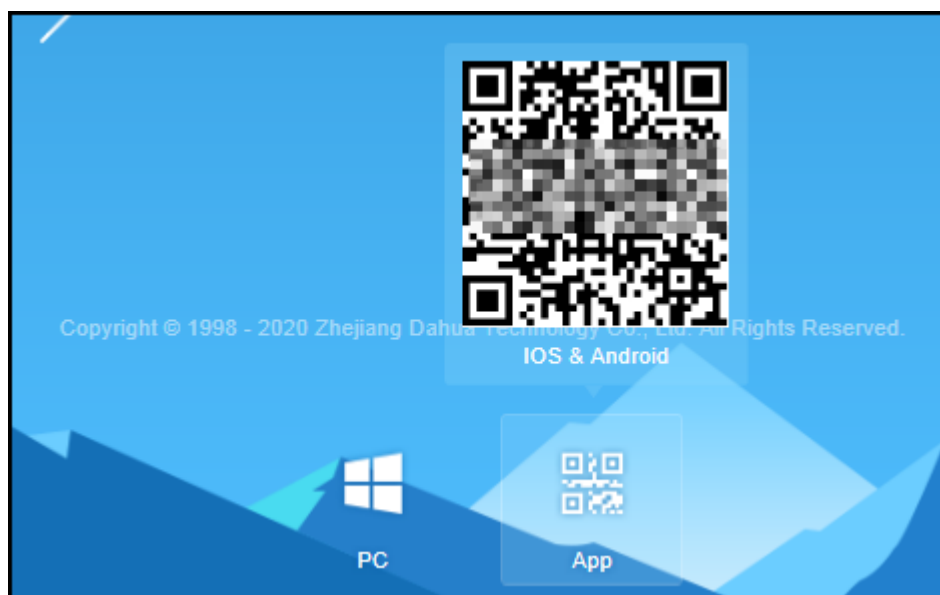
Step 8 Click **Run** to run the client.

4.1.1.2 Installing Mobile Client

Step 1 Enter IP address of DSS Pro into the browser and then press Enter.

Step 2 Click  to view QR code of mobile phone APP. Select iOS or Android.

Figure 4-5 Download App by scanning QR code



Step 3 Scan the QR code to start downloading and installing the mobile client.

4.1.2 Logging in to Client



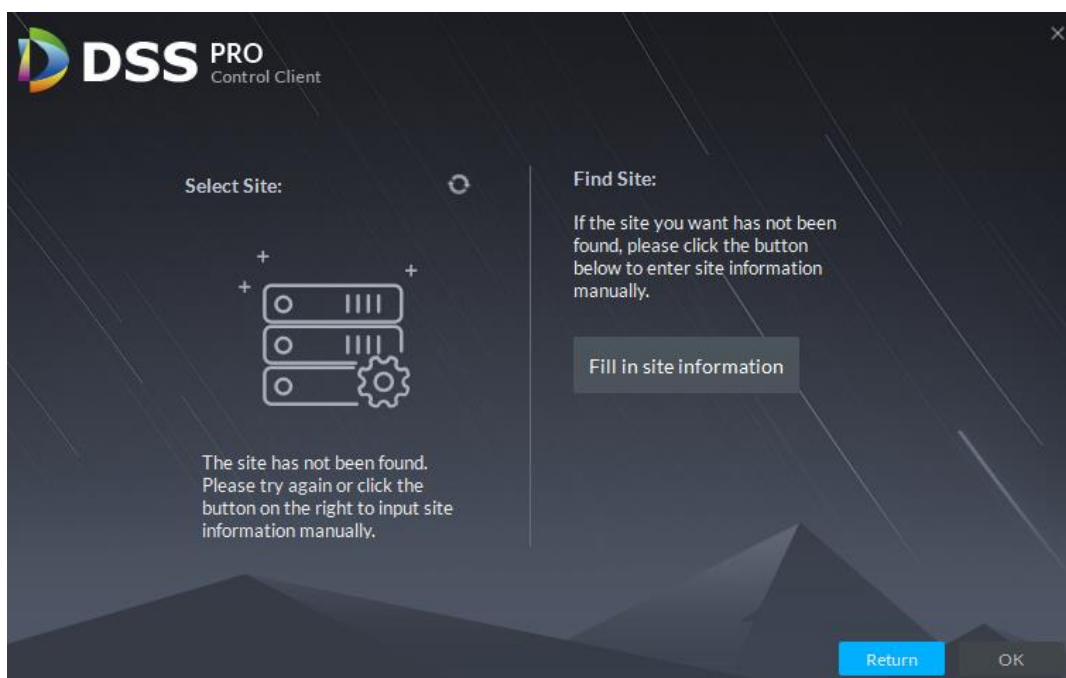
Step 1 Double-click  on the desktop.

- The first time you log in, the following interface is displayed, which proceeds to Step 2.



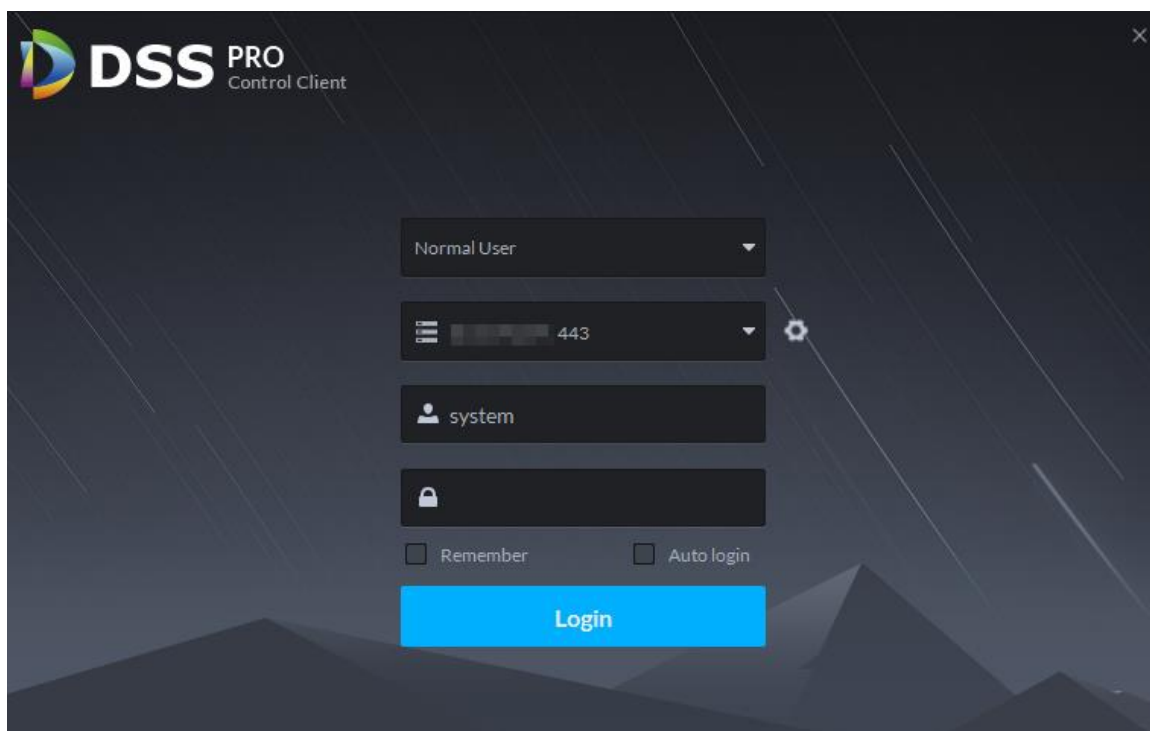
If you have not logged in to Web Manager to initialize the platform, you are required to select a DSS site, set system username and password, and set password protection questions. The questions are used for resetting password in the future when needed.

Figure 4-6 First-time login



- For second-time login or future login, the following interface is displayed, which proceeds to Step 3.

Figure 4-7 Log in to the control client



Step 2 Select the detected server on the left of the interface, or click **Fill in site** information, enter in IP address and port number, and then click **OK**.

Step 3 Enter **Username**, **Password**, **Server IP** and **Port**. Server IP means the IP address to install DSS Pro server or PC, Port is 443 by default.

Step 4 Click **Login**.

4.1.3 Homepage of Control Client

Figure 4-8 Homepage

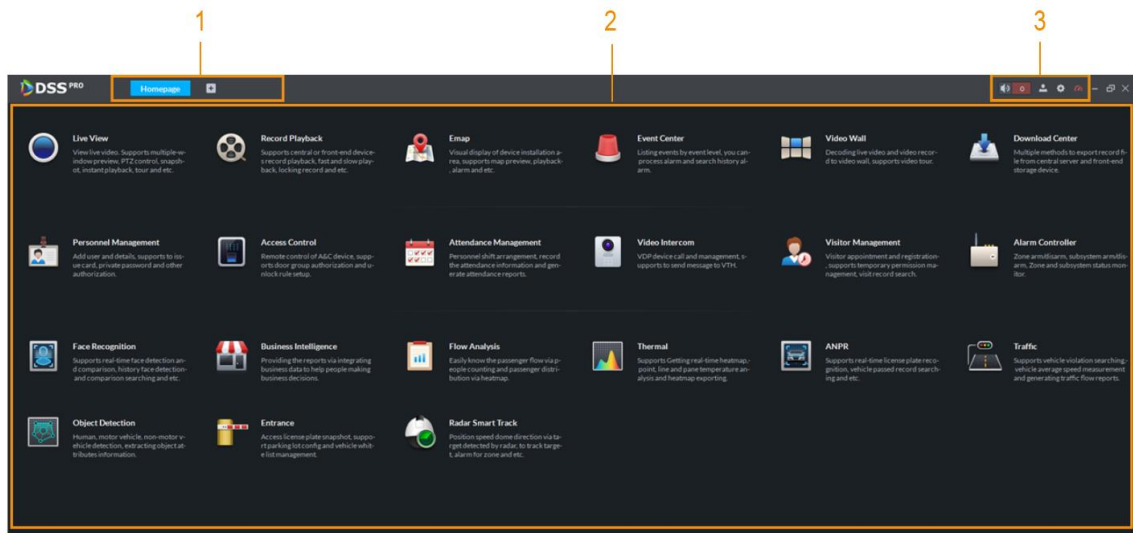








Table 4-2 Description

No.	Name	Function
1	Tab	Display all valid tabs. Click  and you can open the module you want.
2	Applications	Go to each application by clicking the icon.

No.	Name	Function
3	System settings	<ul style="list-style-type: none"> ● : Open/close alarm audio. ● : It displays alarm amount. Click the icon to go to Event Center. ● : User information: click the icon, and then you can log in to the Web Manager by clicking system IP address, modify password, lock client, view help file, and log out. <ul style="list-style-type: none"> ◇ Click platform IP address to go to the Web Manager. ◇ Click Change password to modify user password. ◇ Click Lock Client to lock client. To unlock client, click anywhere on the client and then enter password. ◇ Click About to view version information. ◇ Click Sign Out to exit client. ● : Local configuration. You can configure general settings, video settings, playback settings, snapshot settings, record settings, alarm settings, video wall, security settings and shortcut settings. See "4.1.4 Local Configuration" for details. ● : View system status, including network status, CPU status, and memory status.

4.1.4 Local Configuration

After logging in to the client for the first time, you need to configure the system parameters involving basic settings, video parameters, record playback, snapshot, recording, alarm, video wall, security settings and shortcut keys.

4.1.4.1 Configuring Basic Settings

Configure client language, client size, and time settings.


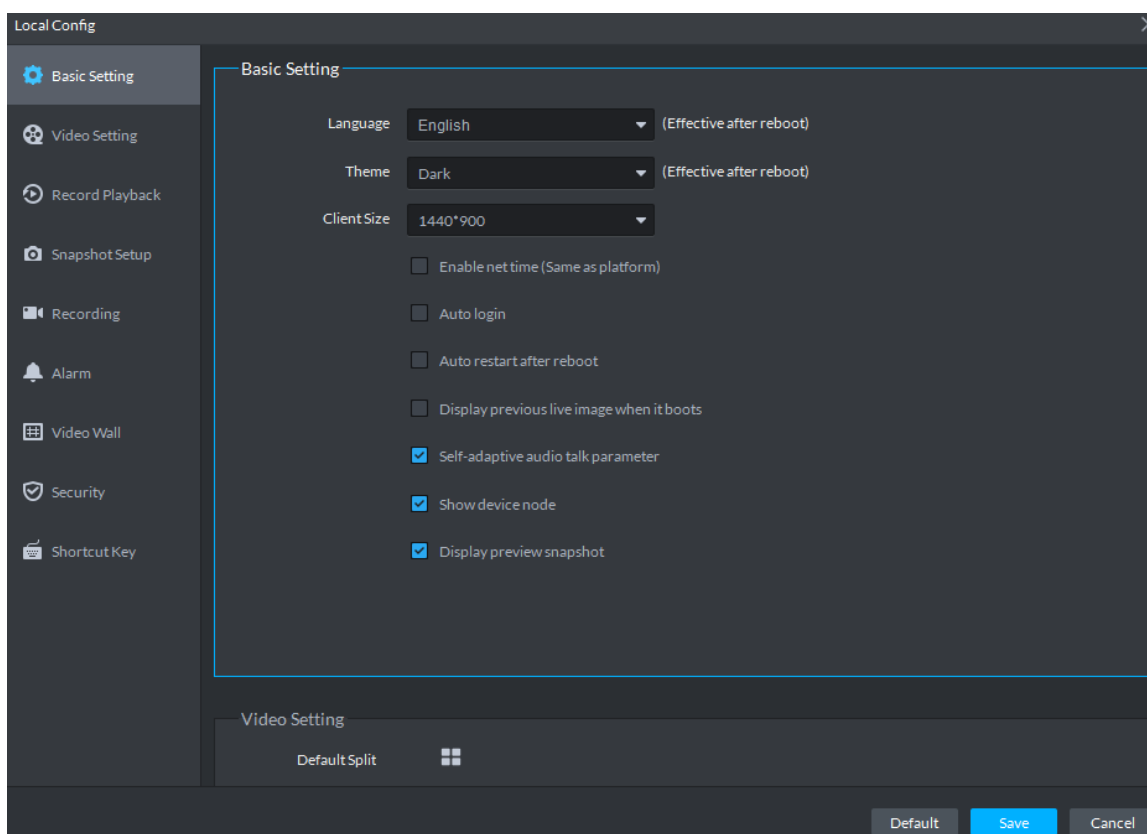
Step 1 Click  at the upper-right corner on the homepage.

Figure 4-9 Local configurations



Step 2 Click **Basic Setting** to set parameters.

Table 4-3 Video parameters

Parameters	Description
Language	Modify the language displayed on client; reboot the client to make it valid after setting.
Theme	Theme color includes dark and white. Reboot the client to make it valid after setting.
Client Size	Select client proper resolution according to PC display screen.
Enable net time	If checked, the client starts to synchronize network time with the server to complete time synchronization.
Auto login	<ul style="list-style-type: none"> If Remember Password and Auto Login are both selected on the Login interface, the system will skip the login interface and directly open the homepage when logging in next time. If Remember Password is not selected while Auto Login selected on the Login interface, when you log in again, Remember Password and Auto Login are selected by default, but you still need to enter the password to log in.

Parameters	Description
Auto restart after reboot	<ul style="list-style-type: none"> If Remember Password and Auto Login are both selected on the Login interface, the system will skip the login interface and directly open the homepage after restarting the PC next time. If Remember Password is not selected while Auto Login selected on the Login interface, after you restart the PC, the client login interface will appear.
Display previous live image after restarting	If enabled, system displays the last live view automatically after restarting the client.
Self-adaptive audio talk parameter	If enabled, the system automatically adapts to the device sampling frequency, sampling bit, and audio format for audio talk.
Show device node	Device tree displays device and the channels under the device. Otherwise it only displays channels.
Display preview snapshot	If enabled, when you hover over a channel on the device tree, the channel will display a thumbnail for you to get a glimpse of the image.

Step 3 Click **Save**.

4.1.4.2 Configuring Video Settings

Configure window split, stream type and play mode of live view, and instant playback length.

Step 1 Click  at the upper-right corner on the homepage.

Step 2 Click **Video Setting** to set parameters.

Figure 4-10 Configure video settings

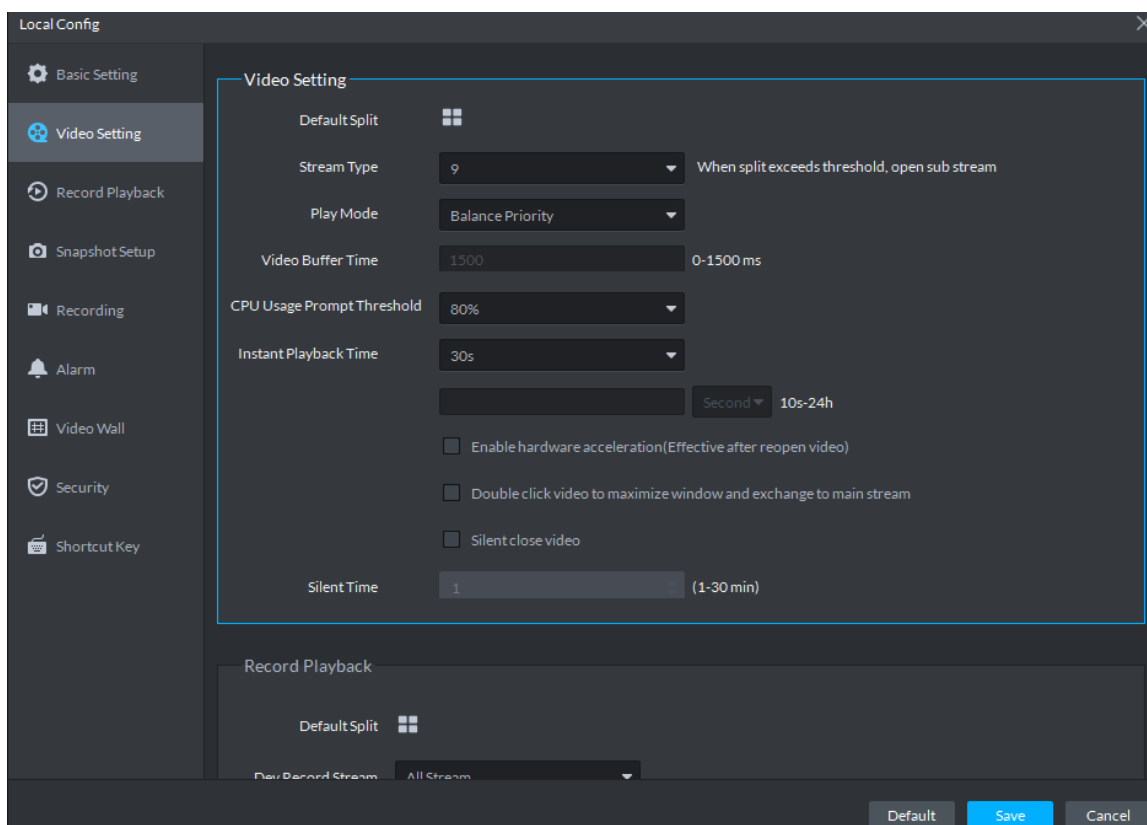



Table 4-4 Parameters

Parameters	Description
Default Split	Set split mode of the video window.
Stream Type	When the number of window splits is greater than the value selected here, the live video will switch from main stream type to sub stream type.

Parameters	Description
Play Mode	<p>Select play mode as required, including Real Time Priority, Fluency Priority, Balance Priority, as well as user-defined modes.</p> <ul style="list-style-type: none"> • Real-Time Priority The system might lower the image quality to avoid video lagging. • Fluency Priority The system might lower the image quality and allow for lagging to ensure video fluency. The higher the image quality, the lower the video fluency will be. • Balance Priority The system balances real-time priority and fluency priority according to the actual server and network performance. • Customize The system adjusts video buffering and lowers the impact on video quality caused by unstable network. The bigger the value, the more stable the video quality will be.
Video Buffer Time	Set video buffer time. It is only available when the play mode is the customized mode.
CPU Usage Prompt Threshold	The user will be asked to confirm whether to open one more video when the CPU usage exceeds the threshold.
Instant Playback Time	Click  on the Live View interface to play the video of the previous period. The period can be user-defined. For example, if you set 30 s, the system will play video of the previous 30 s.
Enable hardware acceleration (Effective after reopen the video)	<p>Enable the function to use the current computer GPU for decoding, so as to reduce CPU consumption and ensure video fluency.</p> <p>GPU requirements:</p> <ul style="list-style-type: none"> • ATI HD2000 and above • NVIDIA Geforce 8200 and above • Intel X4500 HD
Double-click video to maximize the window and switch to main stream	Select the check box to enable the function. If enabled, you can double-click a video window to maximize it and switch from sub stream to main stream.
Silent close video	The system closes live view automatically after inactivity for the pre-defined period.
Silent Time	

Step 3 Click **Save**.

4.1.4.3 Configuring Playback Settings

Configure stream type and window split of playback.

Step 1 Click  at the upper-right corner on the homepage.

Step 2 Click **Record Playback** to set parameters.

Figure 4-11 Configure playback settings

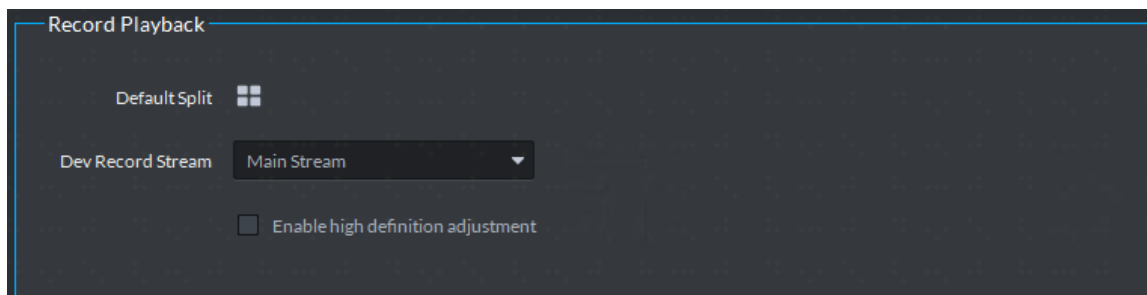



Table 4-5 Parameters

Parameters	Description
Default Split	Set default split mode of the playback window.
Dev Record Stream	Select a default stream type for video playback. Support selecting from Main Stream , Sub Stream or All Stream . If there is no video of the selected stream type, the system will not play video.
Enable high definition adjustment	If enabled, when the playback stream is big due to high definition, system reserves I frames to guarantee video fluency and reduce decoding, bandwidth and forwarding pressure.

Step 3 Click **Save**.

4.1.4.4 Configuring Snapshot Settings

Configure the format and storage directory of pictures captured during live view and playback.

Step 1 Click  at the upper-right corner on the homepage.

Step 2 Click **Snapshot Setup** to set parameters.

Figure 4-12 Configure snapshot settings

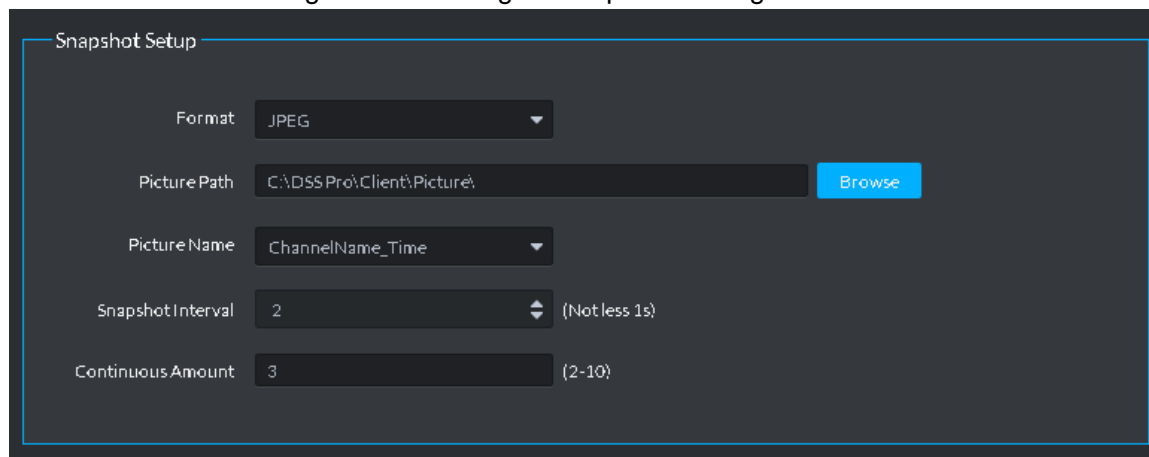



Table 4-6 parameters

Parameter	Description	
Format	Set snapshot image format. Support BMP and JPEG.	 <p>Snapshot here refers to the snapshot function during live view or playback.</p>
Picture Path	Set snapshot storage path.	
Picture Name	Select picture naming rule.	
Snapshot Interval	Set snapshot frequency and number. For example, if the Snapshot Interval is 10 and Continuous Amount is 4, when you right-click on the live/playback video and select Snapshot in the menu, 4 pictures will be captured at once, and the time interval between them is 10 seconds.	
Continuous Amount		

Step 3 Click **Save**.

4.1.4.5 Configuring Recording Settings

Configure the storage directory and name of the videos recorded manually during live view and playback.

Step 1 Click  at the upper-right corner on the homepage.

Step 2 Click **Recording** to set parameters.

Figure 4-13 Configure recording settings

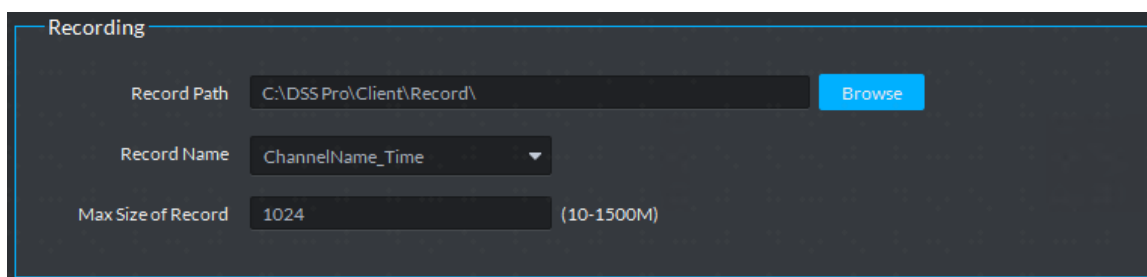


Table 4-7 Parameters

Parameters	Description
Record Path	Set storage path of the manual recording file during live view or playback.
Record Name	Set record file name rule.
Max. Size of Record	Set record file size.

Step 3 Click **Save**.

4.1.4.6 Configuring Alarm Settings

Configure alarm sound and alarm display method on the client.

Step 1 Click  at the upper-right corner on the homepage.

Step 2 Click **Alarm** to set parameters.

Figure 4-14 Configure alarm settings

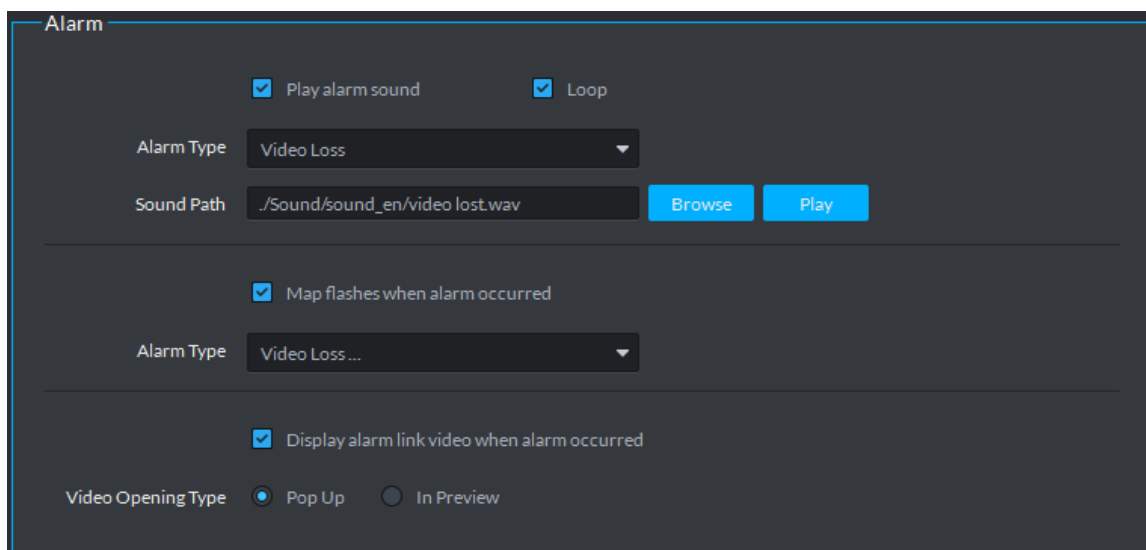


Table 4-8 Parameters

Parameters	Description
Play alarm sound	The alarm sound is triggered on the client computer when the Client receives an alarm. You can configure different sound types for different alarms, so that when an alarm is triggered, you will immediately know what happens. You can upload local sound files as the alarm sounds.
Loop	
Alarm Type	
Sound Path	<ul style="list-style-type: none"> Select the Play alarm sound check box to enable alarm sound. Select Loop to enable loop play of the sound for repeated warning. Select Alarm Type to set alarm sound for the selected alarm type. Click Browse to select the local sound file as alarm warning.
Map flashes when alarm occurred	Set alarm type for alarm notification on the map. When the corresponding alarm occurs, the device on the map will flash.
Display alarm link video when alarm occurred	If enabled, system will automatically open the linked video interface when an alarm occurs.
Video Opening Type	If Pop Up is selected, the alarm video will be played in an instant pop-up window; if In Preview selected, the alarm video will be played on the live view interface.

Step 3 Click **Save**.

4.1.4.7 Configuring Video Wall Settings

Configure the default binding mode and stream type of video wall.

Step 1 Click  at the upper-right corner on the homepage.

Step 2 Click **Video Wall** to set parameters.

Figure 4-15 Configure video wall settings

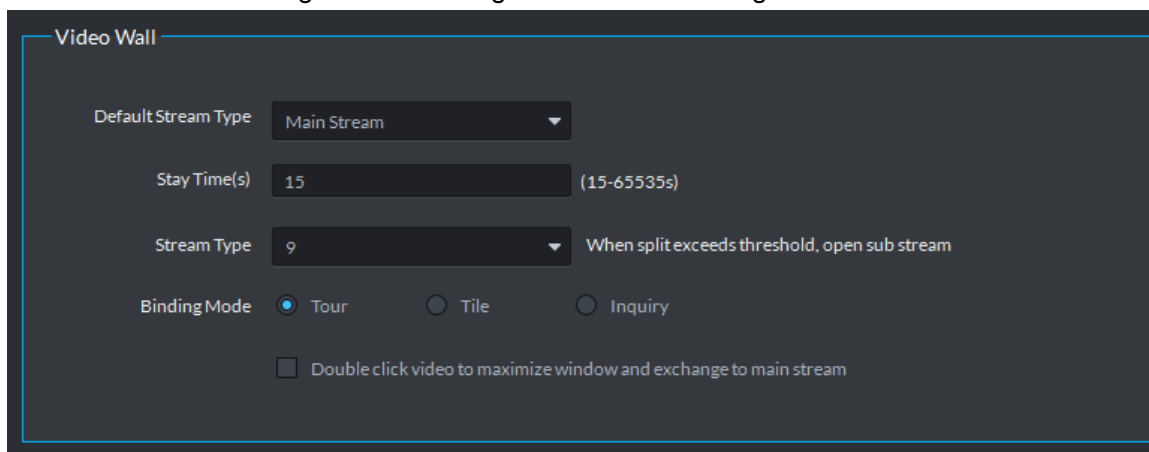



Table 4-9 Parameters

Parameter	Description
Default Stream Type	Select Main Stream , Sub Stream or Local Signal as the default stream type for video wall display.
Stay Time (s)	Set the default time interval between the channels for tour display. For example, if the Stay Time is five seconds, and three video channels are switching on one window (Tour), the video will switch among the three channels every five seconds.
Stream Type	Set the threshold of window split number. For example, if you select nine here, when the split number reaches or exceeds nine, all the nine channels will be decoded in sub stream; otherwise, the decoding type is main stream.
Binding Mode	<ul style="list-style-type: none"> ● Tour: Multiple video channels switch to decode in one window by default. ● Tile: Video channels are displayed in the windows by tile by default. ● Inquiry: When dragging a channel to the window, the system will ask you to select tour or tile mode.
Double-click video to maximize window and exchange to main stream	Double-click on the video to maximize the window, and meanwhile, the stream type will switch to main stream.

Step 3 Click **Save**.

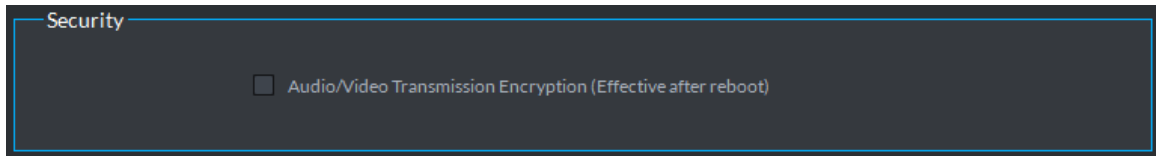
4.1.4.8 Configuring Security Settings

Enable audio/video decryption, so the client can play encrypted audio and video.

Step 1 Click  at the upper-right corner on the homepage.

Step 2 Click **Security**.

Figure 4-16 Audio/video decryption




Step 3 Click the check box next to **Audio/Video Transmission Encryption (Effective after reboot)**.

Step 4 Click **Save**.

This setting comes into effect after restarting the client.

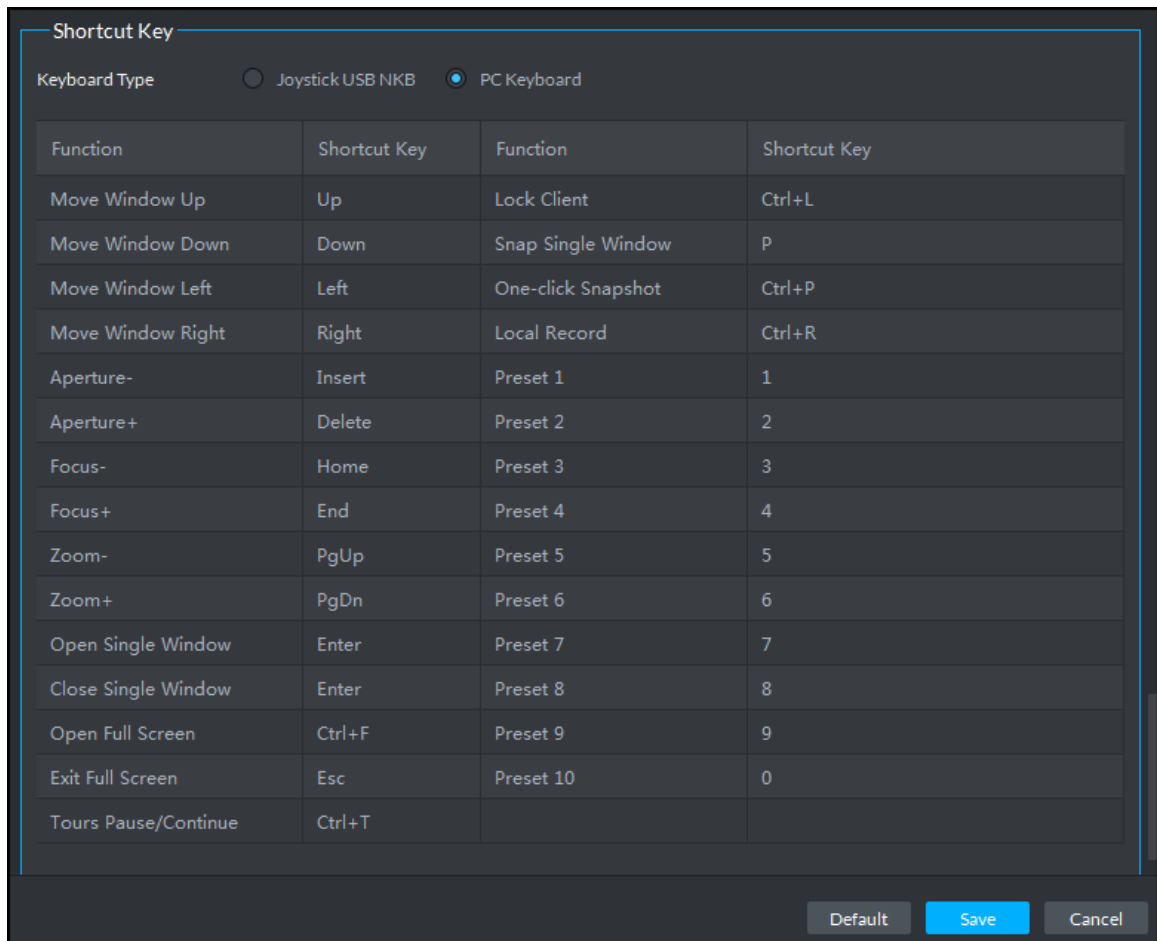
4.1.4.9 Viewing Shortcut Keys

Configure shortcut keys for quick client operation.

Step 1 Click  at the upper-right corner on the homepage.

Step 2 Click **Shortcut Key** to view shortcut keys of computer keyboard and USB joystick.

Figure 4-17 Configure shortcut keys



Step 3 Click **Save**.

4.2 Live View

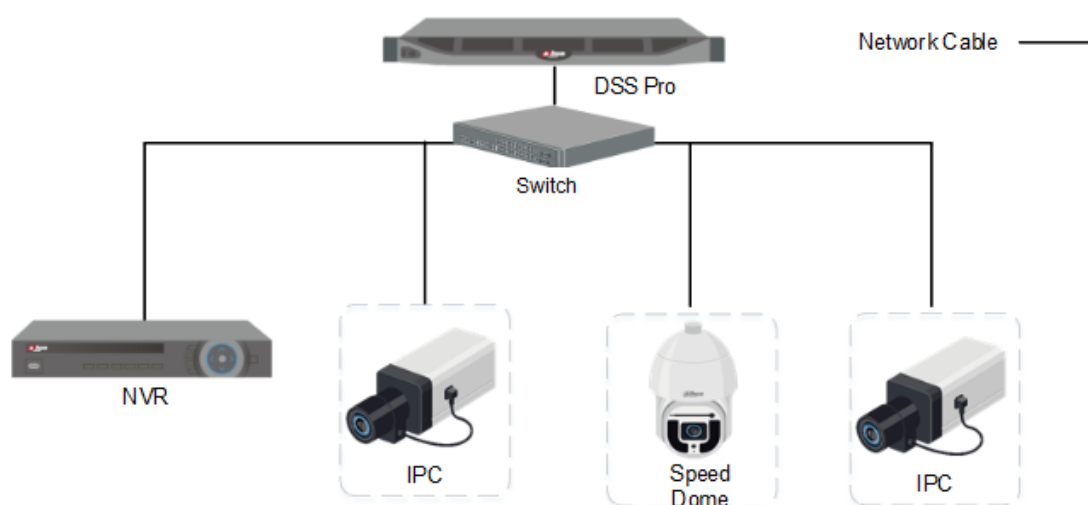
View live videos.



This section only introduces the live view operations of encoders. For POS and map live view, see the corresponding sections.

4.2.1 Typical Topology

Figure 4-18 Typical topology



- Cameras (IPC) are used to collect video streams. Some cameras support intelligent analysis, for example, face recognition. In addition to IP cameras, you can also connect analog cameras.



Analog cameras shall be connected to the platform through DVR.

- NVRs are used to manage cameras, record videos and pictures. Some NVRs support intelligent analysis. In addition to NVR, you can also connect DVR and IVSS to the platform.
- DSS Pro centrally manages all cameras, storage devices, and intelligent analysis devices, and provides live video monitoring and relevant operations.

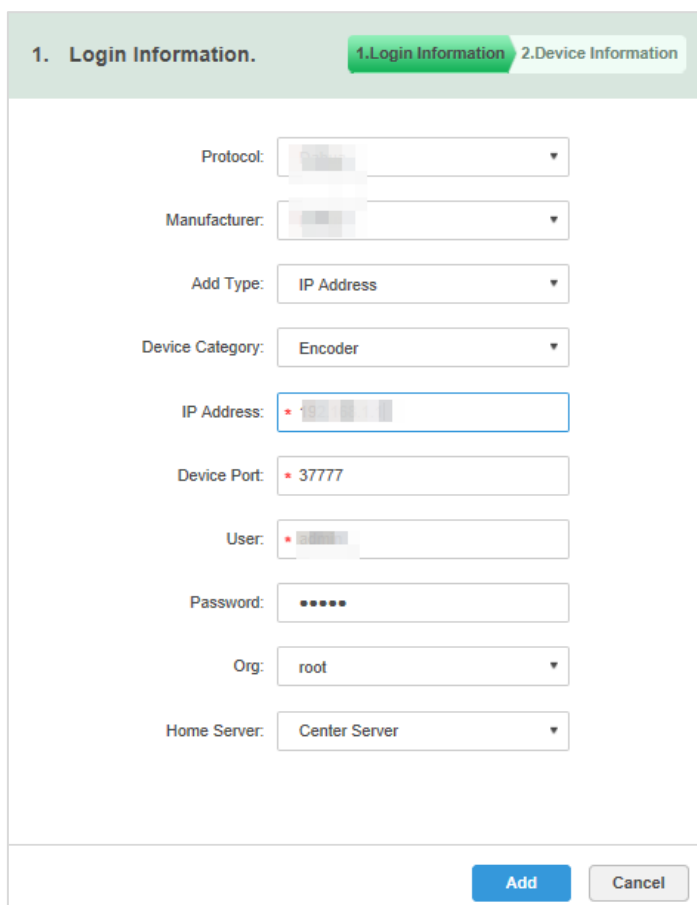
4.2.2 Preparations

Make sure that the following preparations have been made:

- Encoders (IPC, NVR, and more) are well deployed. To deploy, see the corresponding documents.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."

When adding an encoder, select **Encoder** for device category.

Figure 4-19 Add an encoder



4.2.3 Viewing Live Video

View real-time video of online channels in the system.

Step 1 Log in to the Control Client.

Step 2 Select **Live View**.

Step 3 View real-time video.

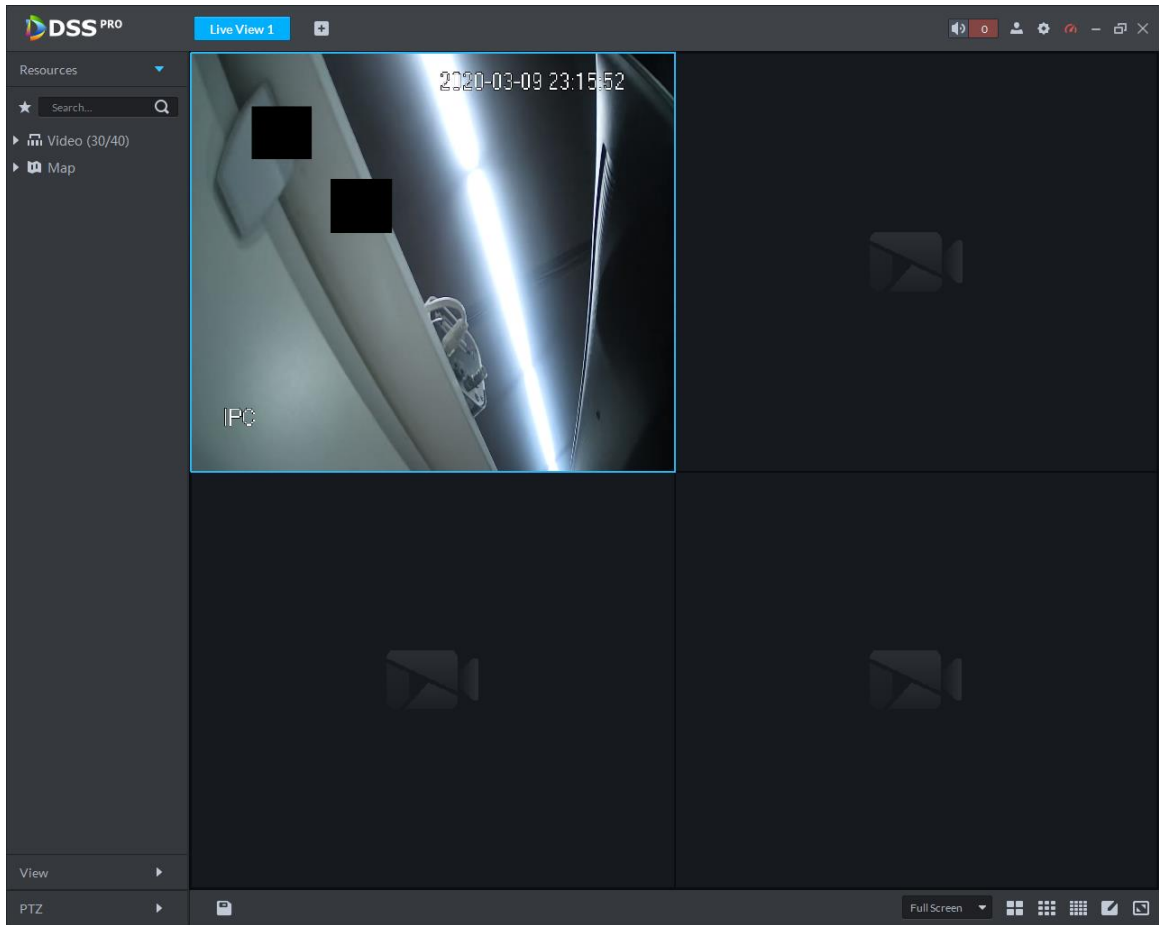
When you hover over a channel in the device tree, you can see the thumbnail of this channel. The thumbnail is a snapshot of the live image at the time. To enable the thumbnail, see "4.1.4.1 Configuring Basic Settings."

- Double-click a channel or drag the channel from the device list on the left to one window on the right.
- Double-click a device to view all channels under the device.
- Right-click a node, select **Tour**, and then set tour interval. The channels under this node will play in turn at the defined interval.



Close the on-going tour before starting live view.

Figure 4-20 Live view



Step 4 You can perform the following operations during live view.

- Move the mouse pointer to the video window, and then you can see the shortcut menu at the upper right.

Figure 4-21 Shortcut menu

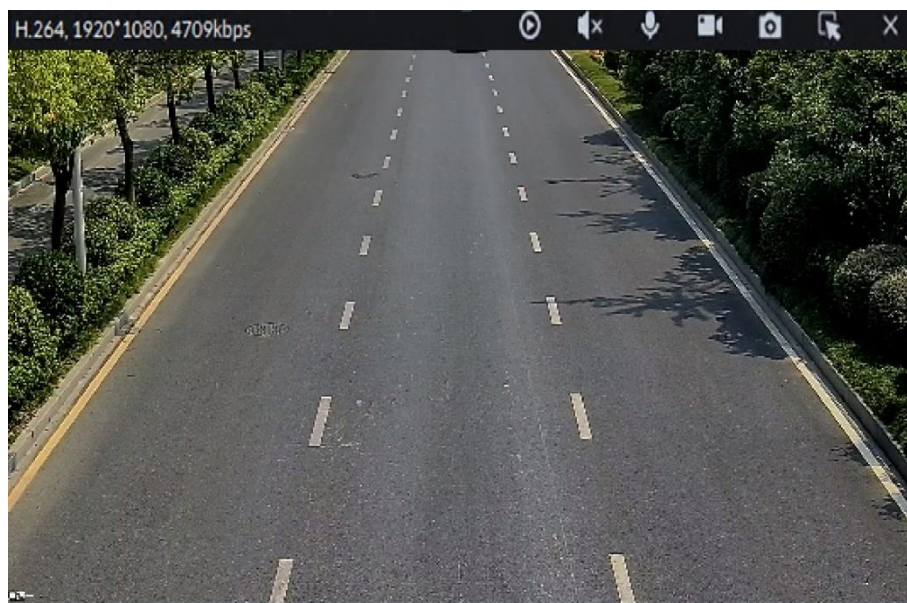









Table 4-10 Description

Icon	Name	Description
	Instant playback	Open/close instant playback. Go to Local config>General to set instant playback time. Make sure that there is a record on the platform or the device.
	Audio	Open/close audio.
	Audio talk	Open/close bidirectional talk.
	Local record	Click it, and then the system begins to record local file and you can view the record time at the upper left. Click again, and then system stops record and save the file on the PC.
	Snapshot	Click to snapshot once.
	Zoom	Zoom in, and it supports mouse wheel zooming after zooming in the image.
	Close	Click to close video.

- On the **Live View** video window, right-click on the live video, and then the shortcut menu is displayed.



The menu varies depending on device function capacity. The actual interface shall prevail.

Figure 4-22 Live video operation menu

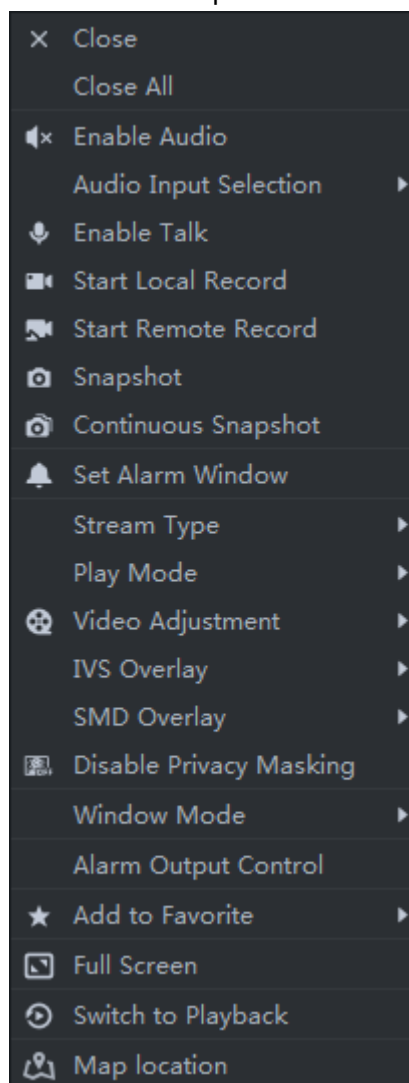







Table 4-11 Description

Parameters	Description
Close	Close the current video window.
Close All	Close all video windows.
Enable Audio	Same as  , to enable or disable camera audio.
Audio Input Selection	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Enable Talk	Same as  , to enable or disable audio talk of corresponding device. View self-adaptive Audio Talk parameters from Local Config > General ; when audio talk is on, it will automatically adapt to various parameters without showing a pop-up box.
Start Local Record	Same as  , to record audio and video of the current video window and save them in local PC.

Parameters	Description
Start Remote Record	Click to start remote recording. Click Stop Remote Record , and then the system stops recording. If the platform has configured video storage HDD, the record file is saved on the platform server.
Snapshot	Take a snapshot of the current image (one picture for each snapshot action). The default saving path is: C:\DSS Pro\Client\Picture\. To modify the path, see "4.1.4.4 Configuring Snapshot Settings."
Continuous Snapshot	Take a snapshot of the current image (three snapshots each time by default).
Set Alarm Window	Turn on/off alarm output.
Stream Type	Switch among Main stream , Sub stream 1 and Sub stream 2 . You can switch the video stream type when the video is not smooth enough due to big stream size or poor bandwidth. Bandwidth consumption degree: Main stream > sub stream 1 > sub stream 2.
Play Mode	Switch between the modes of Real-Time Priority , Fluency Priority , Balance Priority and Customize . <ul style="list-style-type: none"> ● Real-Time Priority The system might lower the image quality to avoid video lagging. ● Fluency Priority The system might lower the image quality and allow for lagging to ensure video fluency. The higher the image quality, the lower the video fluency will be. ● Balance Priority The system balances real-time priority and fluency priority according to the actual server and network performance. ● Customize The system adjusts video buffering and lowers the impact on video quality caused by unstable network. The bigger the value, the more stable the video quality will be. For details, see "4.1.4.4 Configuring Snapshot Settings."
Video Adjustment	Perform video adjustment and video enhancement.
IVS Overlay	The client does not show overlay lines over live video by default. When needed, you can click AI Overlay and enable Rule Overlay and Target Box Overlay , and then the live video shows overlay lines if the AI detection rules are enabled on the device. This configuration is effective with the current selected channel both in live view and playback.
SMD Overlay	Enable SMD Overlay to show target frame over live video. When SMD is enabled on the device, you can enable SMD Overlay for the device channel, and then the live video will display dynamic target frames. This configuration is effective with the current selected channel both in live view and playback.

Parameters	Description
Open Crowd Density Map	 <p>This function is only available for multisensor panoramic camera + PTZ camera.</p> <p>After selecting this function, the crowd density will be displayed on the image of the video. Double-click the image to hide it, and people in the video will be shown in blue dots.</p>
Disable Privacy Masking	For a camera that supports privacy masking of human face, you can disable the masking here to view the face image.
Fisheye View Mode	 <p>For fisheye camera only. When changing the video stream, the fisheye view mode keeps the configuration before the stream is changed.</p> <p>According to different installation methods, the fisheye view can be varied.</p> <ul style="list-style-type: none"> ● Ceiling mount: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8. ● Wall mount: 1P, 1P+3, 1P+4, 1P+8. ● Ground mount: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8.
Window Mode	Standard mode, 1+3 mode, 1+5 mode.
Alarm Output Control	Enable or disable channel alarm input/output.
Add To Favorites	You can add the active channel or all channels into Favorite.
Full Screen	Switch the video window to full screen mode. To exit full screen, double-click video window, or right-click to select exit full screen.
Switch to Playback	Switch from the current live view interface and the playback interface quickly, without going back to homepage first.
Map Location	Display location of the current device on the map.



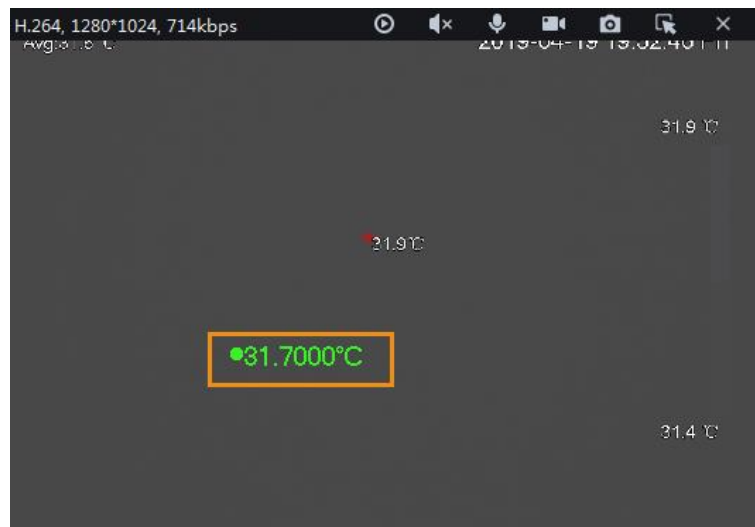
- During tour display, to exit tour, click ; to pause, click .
- To view real-time temperature of a point on the thermal camera view, hover over that point.

Figure 4-23 View temperature



See the following table for introduction to the live view interface.

Figure 4-24 Live view interface

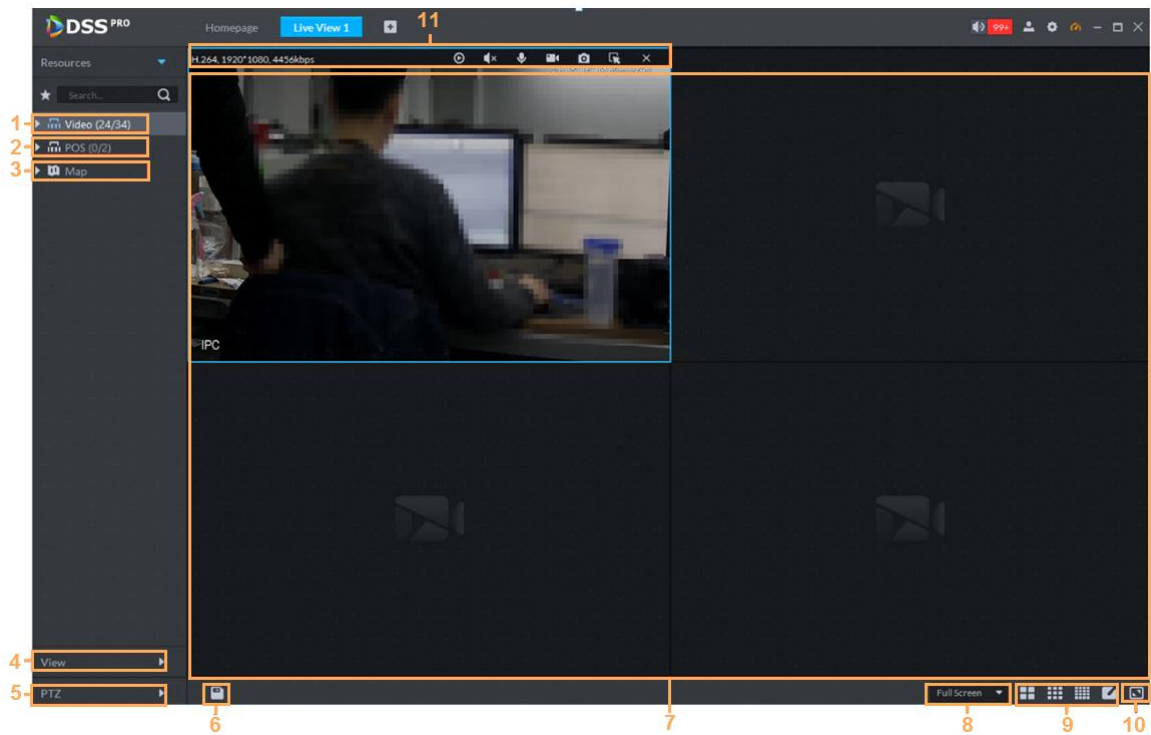









Table 4-12 Description

No.	Name	Function
1	Resources	<ul style="list-style-type: none"> You can search for a device or channel by name in . Fuzzy search is supported so that you can simply enter part of the name and then select the exact one from the given name list. : Add, delete or rename the favorites. Tour display of favorates channels is supported.  <ul style="list-style-type: none"> If you enable Show device node in Local Config > Basic Setting, then the device tree displays devices and their channels; otherwise the tree only display channels.
2	POS	Open POS and its corresponding video channel on the Live view interface.
3	Map Resource	Map can be opened in preview window, both GIS map and Raster map.
4	View	<ul style="list-style-type: none"> Save the current view of window split and video channels in the live view section, and name the view. You can directly select the view from the View tab to display it quickly next time. Channels under a view or view group can be displayed by tour (in turn). You can set the tour interval to be 10s, 30s, 1min, 2min, 5min or 10min. Maximum 100 views can be created.
5	PTZ	More information about PTZ of PTZ camera, see "4.2.9 PTZ."
6	Save view	Click  to save current video window as a view.
7	Video play	Real-time video play. Point to the video play window, and you can scroll forward to zoom in and backward to zoom out.
8	Display mode	Aspect ratio of the video window, selected from two modes for video play: Actual scale and fit-in window.
9	Window Split Mode	<p>Set window split mode. Support 1, 4, 6, 8, 9, 13, 16, 20, 25, 36 or 64 splits, or click  to set a customized split mode.</p>  <p>If the live-view channel number is more than the number of current windows, then you can turn page(s) by clicking  at the bottom of the interface.</p>
10	Full Screen	Switch the video window to Full Screen mode. To exit Full Screen , you can press Esc key or right-click on the video and select Exit Full Screen .

No.	Name	Function
11	Actions	Instant playback, audio, intercom, manual recording, take snapshot, zoom in, and more.

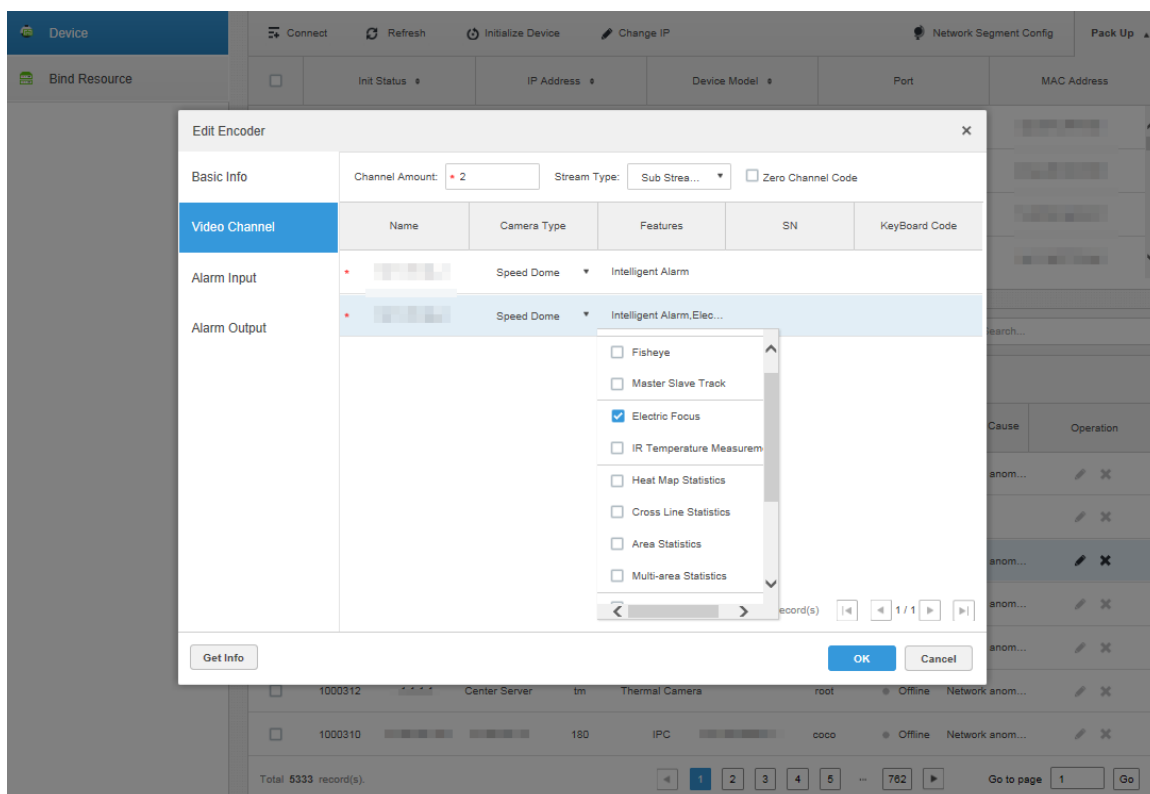
4.2.4 Electronic Focus

If a channel supports electronic focus, you can enable electronic focus for it on the platform to adjust video definition and size.



- If a channel does not support electronic focus, or if you did not modify the **Features** of the channel to **Electronic Focus**, this function will be unavailable for this channel on the platform.
- To modify channel **Features** to **Electronic Focus**, see Figure 4-25.

Figure 4-25 Set channel features



The **Electronic Focus** operation panel is displayed on the **Live View** interface if the selected channel supports this function.



The interface might vary according to the lens types of cameras. Lens types include embedded zoom lens and external CS electronic lens. The following figure is for reference only and the actual interface shall prevail.

Figure 4-26 Live View

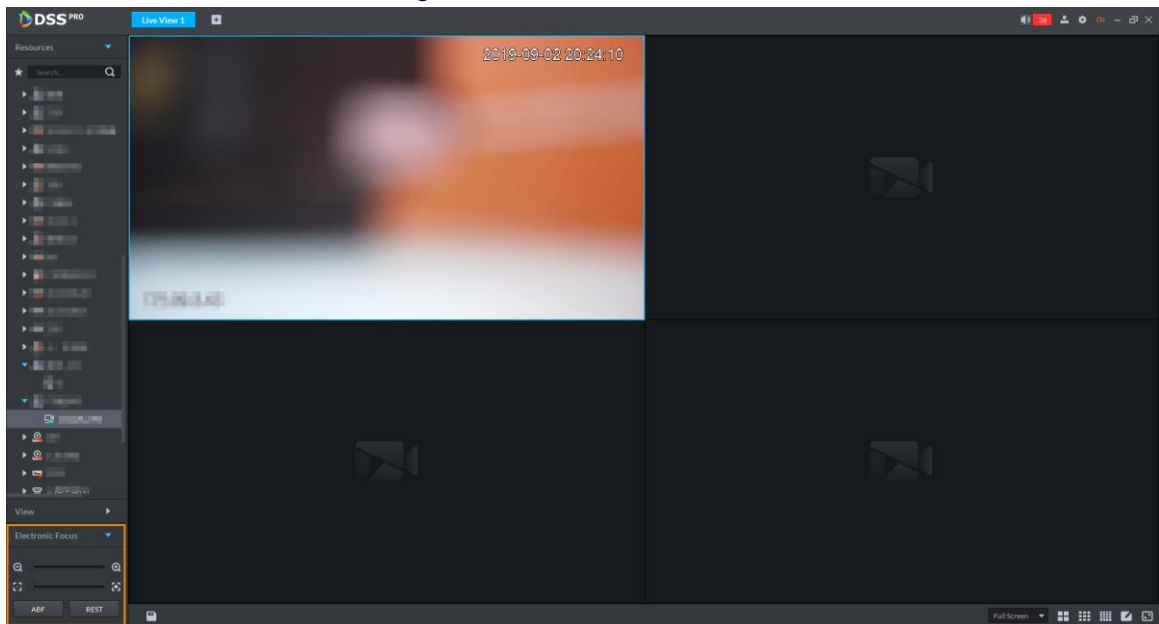


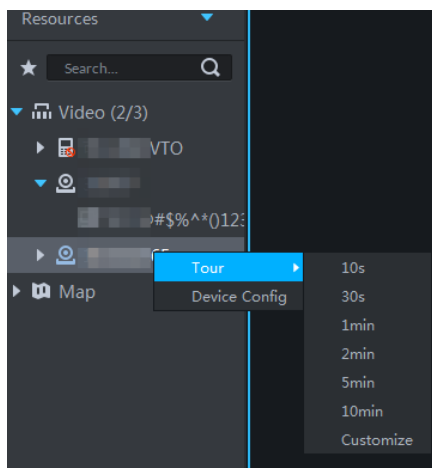
Table 4-13 Parameters description




Parameters	Description
Zoom +/- (for embedded zoom lens)	Zoom in/out. Click or click and hold or , or drag the slider to the left or right to zoom in/out.
Focus +/-	Adjust camera focus to achieve the best video definition. Click or click and hold or , or drag the slider to the left or right to adjust focus.
Auto Focusing (for embedded zoom lens)	Adjust image definition automatically.
ABF (auto back focusing, for external CS electronic lens)	 Other focusing operations are unavailable during auto focusing.
Reset	When image definition is imperfect, or after many times of zooming or focusing operations, you can click Reset to reset the lens, so as to eliminate lens deviation.

4.2.5 Tour

On the **Live View** interface, right-click a device or node, select **Tour**, and then select an interval. The channels under this device or node will be played in turn at the pre-defined interval. You can also customize the interval.

Figure 4-27 Start tour




- To stop the tour play, click  or right-click the window, and then select **Stop Tour**.
- To exit tour play, click ; to pause, click .

4.2.6 View

The current layout and resources can be saved as a view for quick play next time.

4.2.6.1 Creating View

Views are categorized into different groups, convenient for management and quick use. Group includes three levels, first-level root node, second-level grouping and third-level view.

Step 1 Log in to the Control Client, click  and then select **Live View**.

Step 2 Create a view group.

- 1) On the **Live View** interface, click the **View** tab.
- 2) Right-click **View**, select **New Folder**.
- 3) Enter folder name, click **OK**.

Step 3 Create view.

- 1) On **Live View** interface, click  according to your needs.
- 2) Enter **View Name**, select **View Group** and click **OK**.

4.2.6.2 Viewing View

- Live view

Select a view from the view list on **Live View** interface, double-click or drag it to video window, and then the system starts to play live video.
- Tour

On the **Live View** interface, right-click view group or root node, select **Tour** and tour period.

Figure 4-28 Entering video tour interface

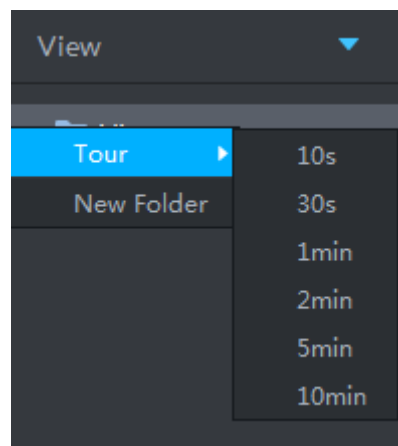


Figure 4-29 View tour



To exit tour play, click ; to pause, click .

4.2.7 Favorites

Add frequently used channels to favorites to realize quick search and call.

4.2.7.1 Creating Favorites

Step 1 Create favorites.


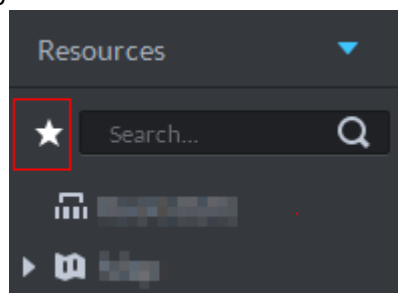
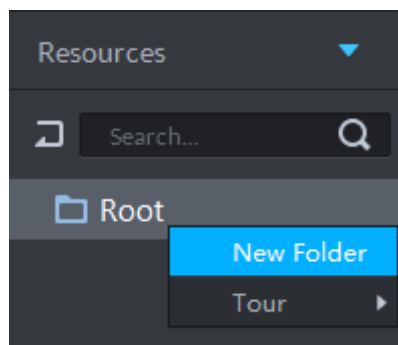
- 1) On **Live View** interface, click .

Figure 4-30 Enter favorites list



- 2) Right-click root node or created favorites, and then select **New Folder**.

Figure 4-31 Favorites list



- 3) Enter folder name, click **OK**.
Selected root node or favorites generates lower-level favorites.

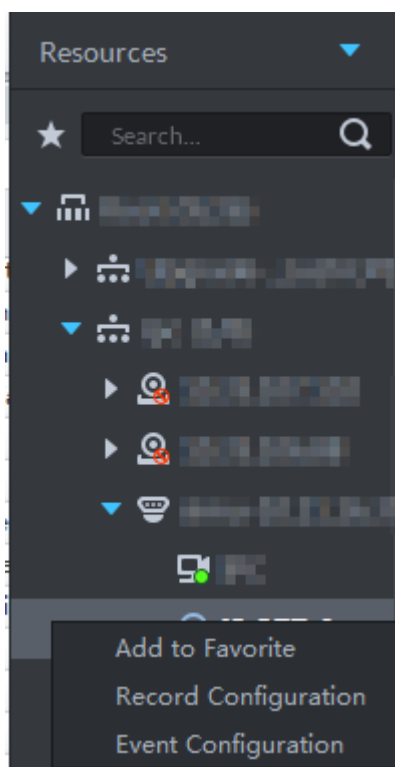
- 4) Click .

The system returns to device list.

Step 2 Favorite channel.

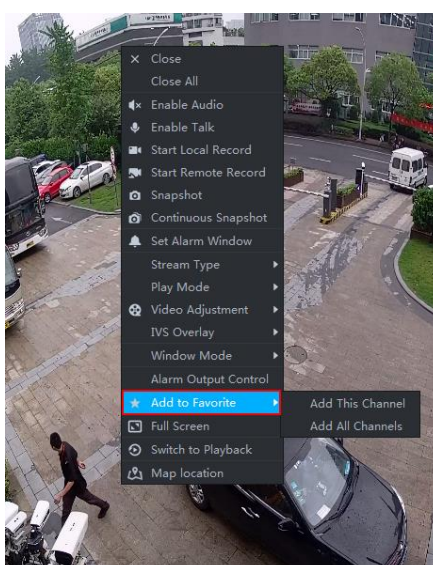
- In the device list on **Live View** interface, right-click channel, select **Add to Favorites**, and add the channel to favorite according to system prompt.

Figure 4-32 Favorite channel (1)




- On **Live View** interface, right-click the window with live view, and select **Add to favorite**, add it to favorite according to system prompt.

Figure 4-33 Favorite channel (2)






4.2.7.2 Viewing Favorites

- Live view

On **Live View** interface, click , open favorite list, select favorite or channel, Double-click or drag to video window and the system starts to play live video.

- Tour

On **Live View** interface, click , open favorite list, right-click root node or favorite, select **Tour** and tour period. The system plays root node or all channels under favorite in loop. To exit tour play, click ; to pause, click .

4.2.8 Region of Interest (RoI)

A window can be divided into 4 or 6 regions during live view. One area is used to play live video and other regions are used to zoom in regional image.

On **Live View** interface, right-click the window, select **Split Mode**, and then select a mode. For example, select 1+3 mode.

Figure 4-34 Split mode

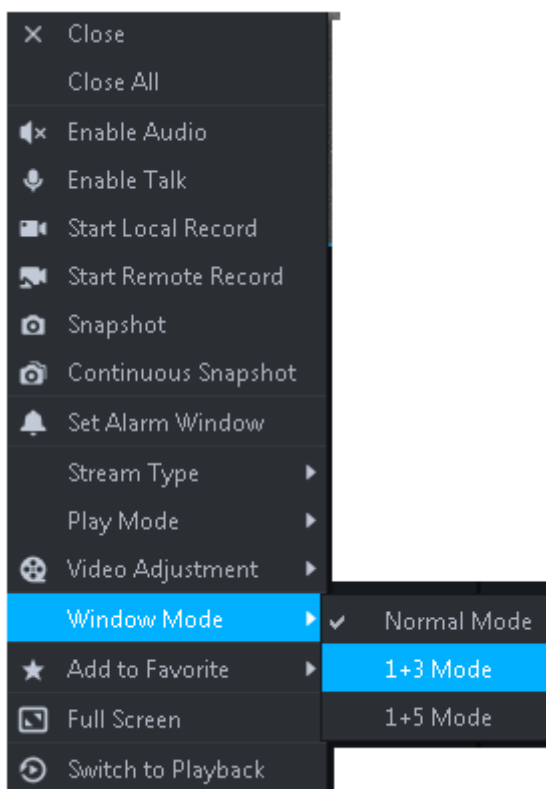
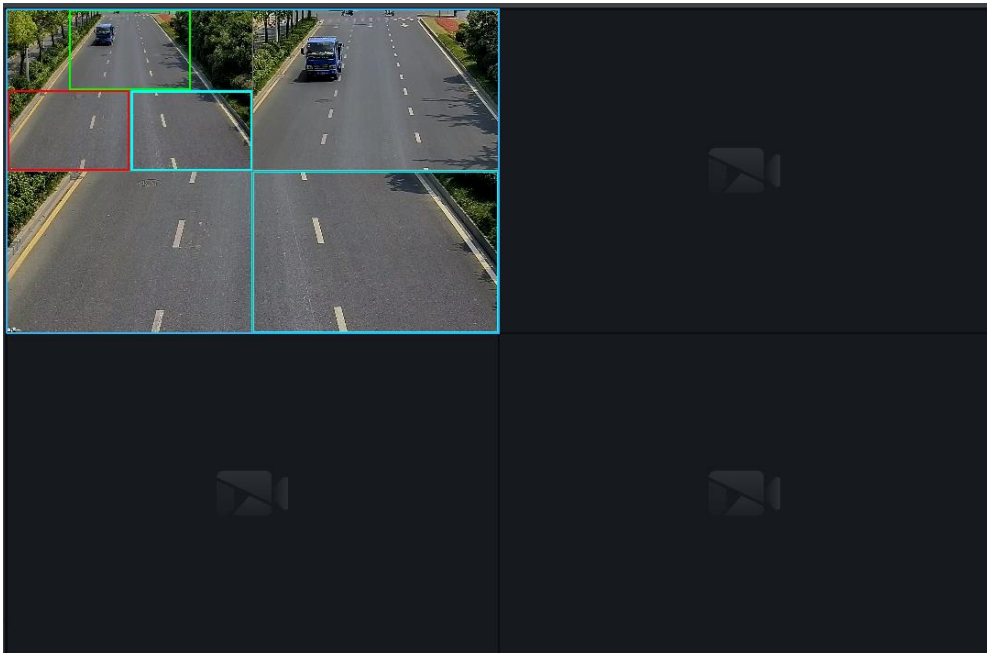


Figure 4-35 1+3 mode

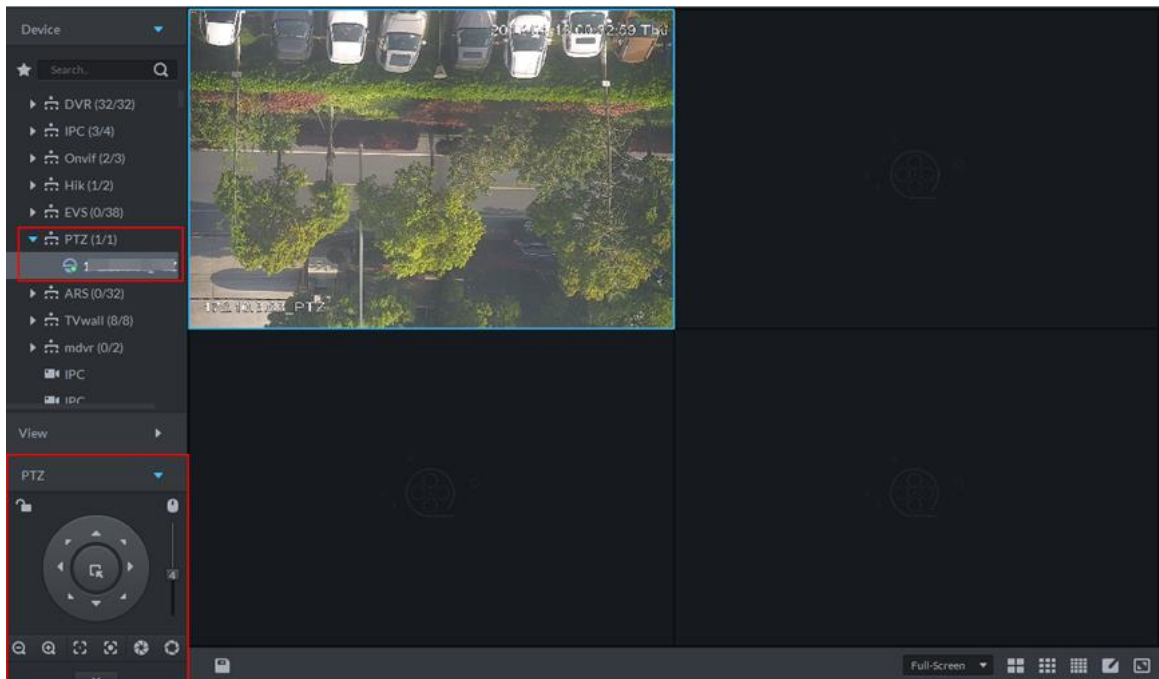


4.2.9 PTZ

Operate PTZ cameras during live view on the Control Client.

Step 1 On **Live View** interface, open video from the PTZ camera.

Figure 4-36 PTZ control panel




Step 2 Click  at the bottom of the interface. The PTZ menu is displayed.

Figure 4-37 PTZ menu

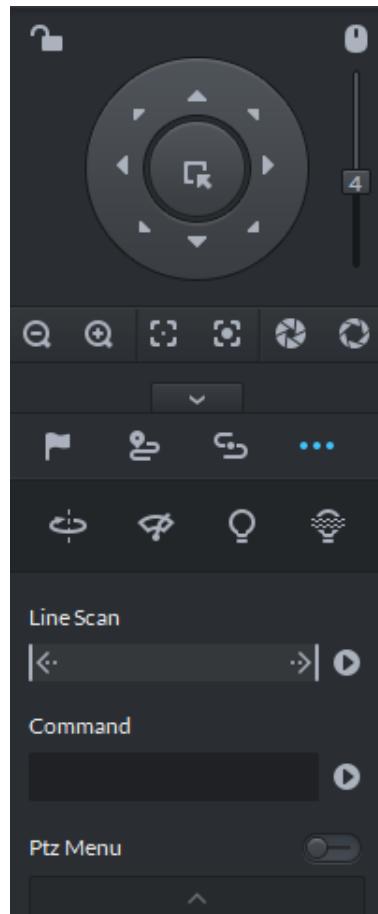

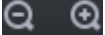





Table 4-14 Description


Parameters	Description
	<p>Click to lock the current PTZ. indicates that PTZ is locked.</p> <p>Different users have different PTZ operation priorities.</p> <ul style="list-style-type: none"> When a user of lower PTZ priority locks PTZ, user of higher PTZ priority can unlock and enable the PTZ by clicking . When a user of higher PTZ priority locks PTZ, user of low PTZ priority cannot unlock the PTZ, unless the PTZ camera automatically unlocks itself. Users of the same PTZ priority can unlock PTZ locked by each other. <p></p> <p>The default time for automatically unlocking PTZ is 30 seconds.</p>
	Control speed dome with mouse.
Direction Key	Set rotation direction of PTZ. Eight directions are available in total: up, down, left, right, upper left, upper right, lower left and lower right.
	<p>3D positioning and partial zooming.</p> <p></p> <p>This function can only be controlled with mouse.</p>


	Adjust rotation speed of PTZ from top to the bottom. Set the step size from 1 to 8.
	Zoom in/out.
	Adjust focus.
	Adjust brightness.
	Set preset, tour, pattern, scan, rotation, wiper, light, and IR light function.


4.2.9.2 Configuring Preset


A preset is a set of parameters involving PTZ direction and focus. By calling a preset, you can quickly rotate the camera to the pre-defined position.

Step 1 Click the direction key of the PTZ to rotate the camera to the needed direction.

Step 2 Click .

Step 3 Point to 1, and then click .

Step 4 Enter preset No., and then click .

Click  of a specific preset, and then camera will rotate to the related position.

4.2.9.3 Configuring Tour

Set Tour to enable camera to go back and forth among different presets.




To enable tour, at least 2 preset points are required.

Set tour to enable camera to automatically go back and forth between different presets.



To enable tour, Make sure that you have configured at least 2 preset points in advance.

Step 1 Click .


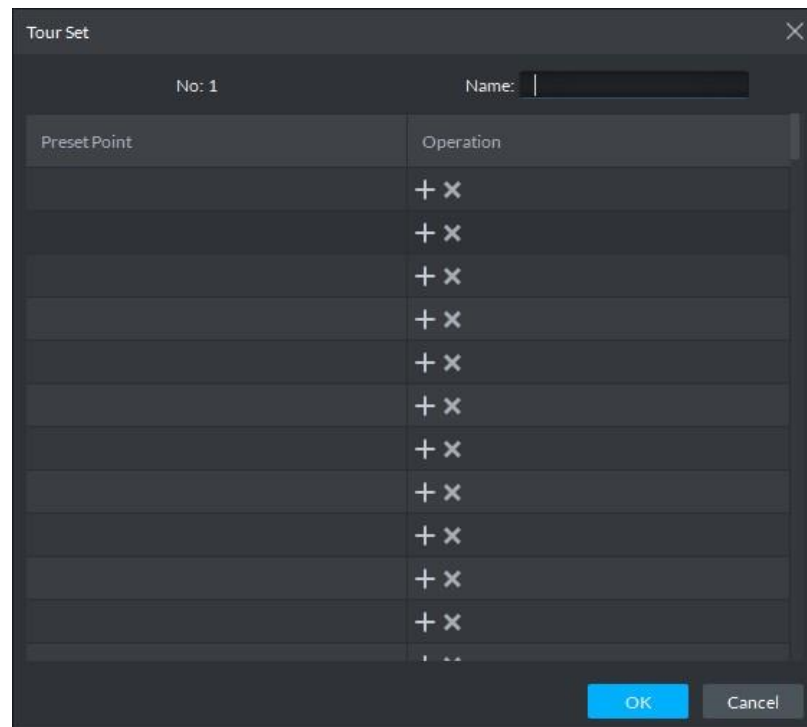
Step 2 Point to 1 and click .

Figure 4-38 Add preset



Step 3 Enter tour name, and click

Select a preset point from the dropdown list on the left.

Step 4 Click **OK**.

To start tour, point to 1 and click , then camera goes back and forth among the presets of Tour 1.

4.2.9.4 Configuring Pattern

A pattern is a record of a consecutive series of PTZ operations. You can select a pattern to repeat the corresponding operations quickly. See pattern configuration instructions as follows.

Step 1 Click

Step 2 Point to 1 and click , and then operate the 8 PTZ buttons of PTZ to set pattern.


Step 3 Click to complete pattern setup.


Step 4 Click , and then the camera will automatically repeat the pattern you have just set.


4.2.9.5 Configuring Scan

The camera automatically scans horizontally at a certain speed.


Step 1 Click

Step 2 Click PTZ button, and rotate PTZ to the left to a position, and then click  to set the left boundary.

Step 3 Continue to rotate PTZ to the right to a position, and then click  to set the right boundary.




Step 4 Click  to start scanning, then PTZ will rotate back and forth automatically within the two boundaries.

4.2.9.6 Enabling/Disabling Pan

Click , and then click . PTZ rotates 360° at a specified speed. Click  to stop camera rotation.


4.2.9.7 Enabling/Disabling wiper

Enable/disable the PTZ camera wiper. Make sure that the camera supports wiper function.



Click , and then click  to turn on wiper. Click  to turn off wiper.

4.2.9.8 Enabling/Disabling light

Turn camera light on/off. Make sure that the camera supports light.

Click , and then click  to turn on light. After enabling light, click  to turn off light.

4.2.9.9 Enabling/Disabling IR light

Click , and then click  to enable IR light. After enabling IR light, click  to disable.

4.2.9.10 PTZ Menu

Step 1 Click .

Figure 4-39 Menu

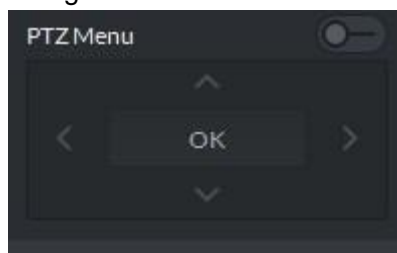


Table 4-15 PTZ menu parameter description

Parameters	Description
	Up/down button.
	Left/right. Move the mouse pointer to set parameters.
	Click to enable PTZ menu function. System displays main menu on the monitor window.
	Click to close PTZ menu function.
OK	It is the confirm button. It has the following functions. <ul style="list-style-type: none"> • If the main menu has the sub-menu, click OK to enter the sub-menu. • Move the mouse pointer to Back and then click OK to go to go back to the previous menu. • Move the mouse pointer to Exit and then click OK to exit the menu.

Step 2 Click **OK**.

Main menu

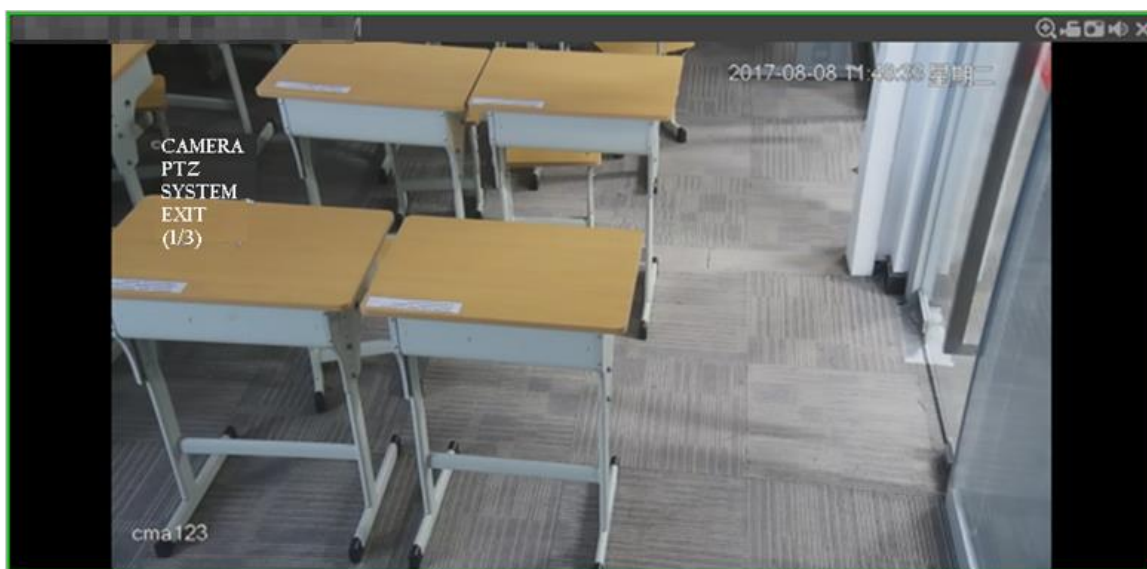


Table 4-16 Main menu parameter description

Parameters	Description
Camera	Move the mouse pointer to Camera and then click OK to enter camera settings sub-menu interface. Set camera parameters. It includes picture, exposure, backlight, day/night mode, focus and zoom, defog, and default.

Parameters	Description
PTZ	Move the mouse pointer to PTZ and then click OK to enter PTZ sub-menu interface. Set PTZ functions. It includes preset, tour, scan, pattern, rotation, PTZ restart, etc.
System	Move the mouse pointer to System and then click OK to enter system sub-menu interface. Set PTZ simulator, restore camera default settings, video camera software version and PTZ version.
Return	Move the mouse pointer to the Return and then click OK , and go back to the previous menu.
Exit	Move the mouse pointer to the Exit and then click OK , and exit PTZ menu.

4.3 Configuring Device Parameters

Configure the camera properties, video stream, snapshot, video overlay, and audio configuration for the device channel on the platform. Only support configuring the channels added via IP in Dahua protocols.



Device configuration differs by the capacities of the devices. The actual interfaces of other models shall prevail.

4.3.1 Configuring Camera Properties

Configure camera image parameters for the **Daytime**, **Night**, and **Regular** modes to ensure high image quality.

4.3.1.1 Configuring Property Files

Step 1 Log in to the Control Client.

Step 2 On the **Live View** interface, right-click the video device and select **Device Config**.



- For PTZ or speed dome, the PTZ control interface also displays.
- Click **More configuration** to open the web configuration interface of the device.

Figure 4-40 Select Device Config

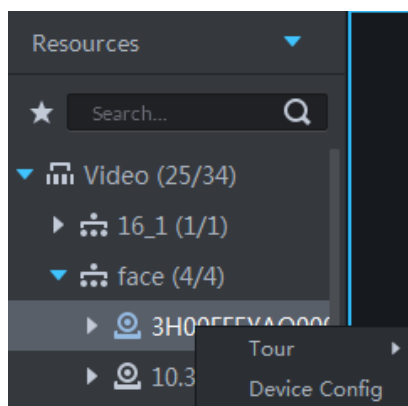
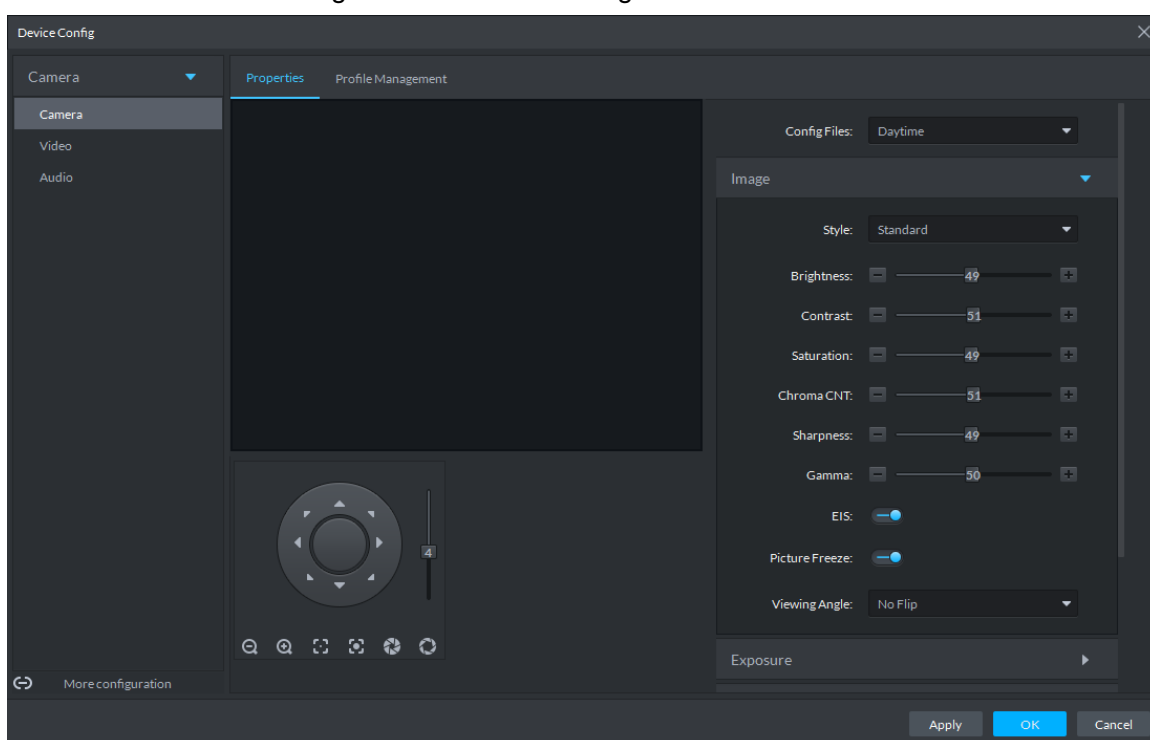


Figure 4-41 Device Config interface



Step 3 Select **Camera > Camera > Properties > Image**.

Step 4 Select **Profile Management**.

Step 5 Click **Image**.

Table 4-17 Image parameters

Parameter	Description
Style	You can set the image style to be Standard, Gentle, or Flamboyant.
Brightness	You can adjust the overall image brightness through linear tuning. The higher the value, the brighter the image and vice versa. If this value is set too high, images tend to look blurred.
Contrast	Adjusts the contrast of the images. The higher the value, the bigger the contrast between the bright and dark portions of an image and vice versa. If the contrast value is set too high, the dark portions of an image might become too dark, and the bright portions might be over-exposed. If the contrast value is set too low, images tend to look blurred.

Parameter	Description
Saturation	Adjusts color shade. The higher the value, the deeper the color and vice versa. The saturation value does not affect the overall brightness of the images.
Sharpness	Adjusts the edge sharpness of images. The higher the value, the sharper the image edges. Setting this value too high might easily result in noises in images.
Gamma	Changes image brightness by non-linear tuning to expand the dynamic display range of images. The higher the value, the brighter the image and vice versa.

Step 6 Click **Exposure** to set relevant parameters.



If the device that supports real wide dynamic (WDR) has enabled WDR, long exposure is not available.

Figure 4-42 Exposure

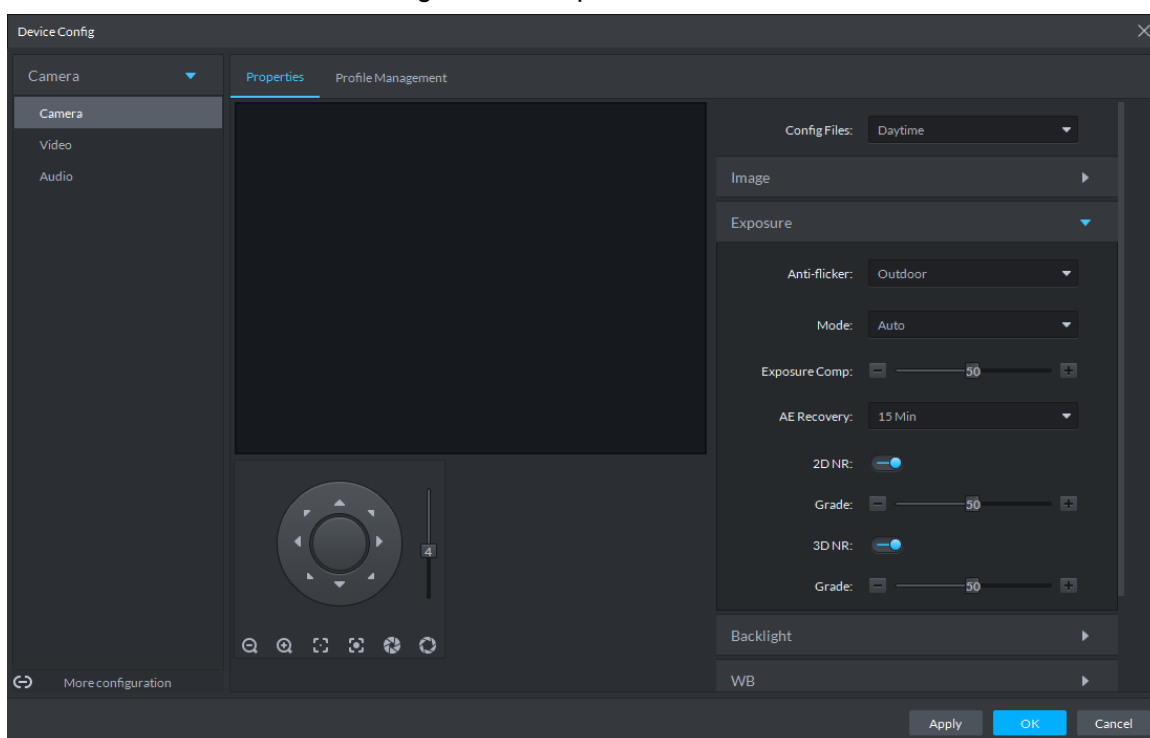



Table 4-18 Exposure parameters

Parameter	Description
Anti-flicker	<p>You can select from these three modes: 50Hz, 60Hz, or Outdoor.</p> <ul style="list-style-type: none"> 50Hz: With the 50Hz household power supply, the mode can automatically adjust exposure based on the brightness of the scene to ensure that the image does not yield horizontal stripes. 60Hz: With the 60Hz household power supply, the mode can automatically adjust exposure based on the brightness of the scene to ensure that the image does not yield horizontal stripes. Outdoor: In an outdoor scenario, you can switch the exposure modes to achieve your target effect.

Parameter	Description
Mode	<p>The following options are available for the different exposure modes of the camera:</p>  <ul style="list-style-type: none"> • If the Anti-flicker is set to Outdoor, you can set the Mode to Gain Priority or Shutter Priority. • Different devices have different exposure modes. The actual interfaces shall prevail. • Auto: Auto tuning of the image brightness based on the actual environment. • Gain Priority: Within the normal exposure range, the device adjusts itself automatically first in the preset range of gains as per the brightness of the scenes. If the image has not achieved the target brightness when the gains hit the upper limit or lower limit, the device adjusts the shutter automatically to achieve the best brightness. The Gain Priority mode also allows for adjusting the gains by setting up a gain range. • Shutter Priority: Within the normal exposure range, the device adjusts itself automatically first in the preset range of shutter values as per the brightness of the scenes. If the image has not achieved the target brightness when the shutter value hits the upper limit or lower limit, the device adjusts the gains automatically to achieve the best brightness. • Aperture Priority: The aperture is fixed at a preset value before the device adjusts the shutter value automatically. If the image has not achieved the target brightness when the shutter value hits the upper limit or lower limit, the device adjusts the gains automatically to achieve the best brightness. • Manual: You can set up the gains and shutter values manually to adjust image brightness.
3D NR	Reduces the noises of multiple-frame (at least two frames) images by using inter-frame information between two adjacent frames in a video.
Grade	<p>When 3D NR is On, you can set up this parameter.</p> <p>The higher the grade, the better the noise reduction effect.</p>

Step 7 Click **Backlight** to set up relevant parameters.

The Backlight mode offers Backlight Correction, Wide Dynamic, and Glare Inhibition features.

- Turning on **Backlight Correction** avoids silhouettes of relatively dark portions in pictures taken in a backlight environment.
- Turning on **Wide Dynamic** inhibits too bright portions and makes too dark portions brighter, presenting a clear picture overall.
- Turning on **Glare Inhibition** partially weakens strong light. This feature is useful in a toll gate, and the exit and entrance of a parking lot. Under extreme lighting conditions such as deep darkness, this feature can help capture the details of the faces and license plates.

Figure 4-43 Backlight

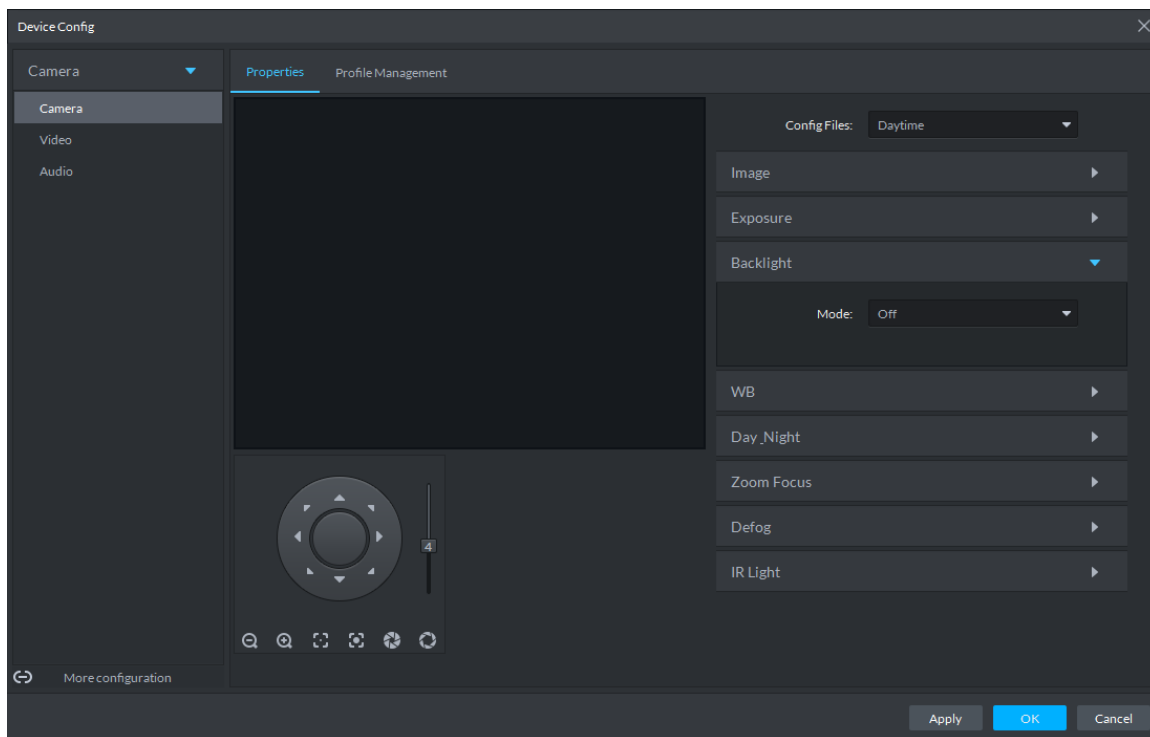



Table 4-19 Backlight parameters

Backlight mode	Description
SSA	The system adjusts image brightness automatically based on the environmental lighting conditions to show image details clearly.
Backlight Correction	You can select Default mode or Custom mode. <ul style="list-style-type: none"> When selecting the Default mode, the system adjusts exposure automatically to adapt to the environment and make the images taken in the darkest regions clear. When selecting the Custom mode and setting up a custom region, the system exposes the selected custom region to give the images taken in this region proper brightness.
Wide Dynamic	To adapt to the environmental lighting conditions, the system reduces the brightness in bright regions and increases the brightness in dark regions. This ensures clear display of objects in both bright and dark regions.  The camera might lose seconds of video recordings when switching from a non-wide dynamic mode to Wide Dynamic.
Glare Inhibition	The system inhibits the brightness in bright regions and reduces the size of the halo, to make the entire image less bright.

Step 8 Click **WB** to set relevant parameters.

The WB feature makes the colors of the images more accurate. In WB mode, white objects in the images appear white in various lighting conditions.

Figure 4-44 WB

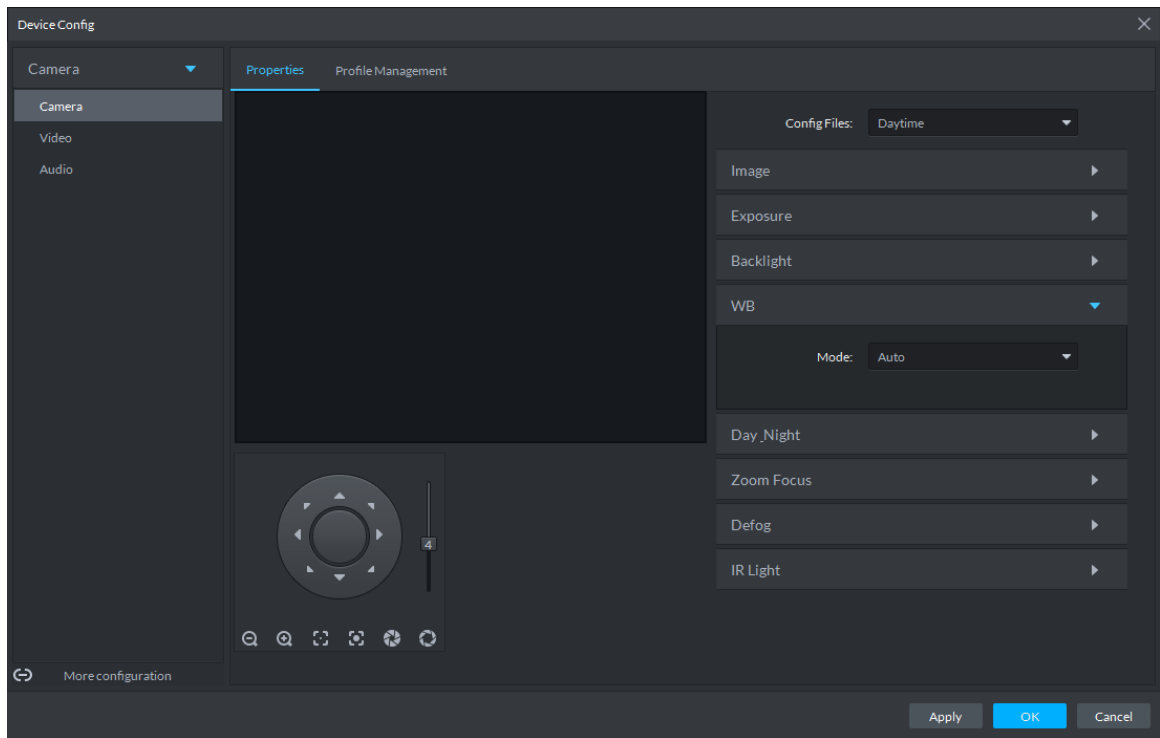


Table 4-20 WB parameters

WB mode	Description
Auto	The system automatically WB corrects different color temperatures to ensure normal display of image colors.
Natural Light	The system automatically WB corrects the scenes without manmade lighting to ensure normal display of image colors.
Street Lamp	The system automatically WB corrects the outdoor scenes at night to ensure normal display of image colors.
Outdoor	The system automatically WB corrects most outdoor scenes with natural lighting and manmade lighting to ensure normal display of image colors.
Manual	You can set up the red gains and blue gains manually for the system to correct different color temperatures in the environment accordingly.
Regional Custom	You can set up custom regions and the system WB corrects different color temperatures to ensure normal display of image colors.

Step 9 Click **Day & Night** to set up relevant parameters.

You can set up the display mode of images. The system can switch between the Colored mode and the Black&White mode to adapt to the environment.

Figure 4-45 Day & night

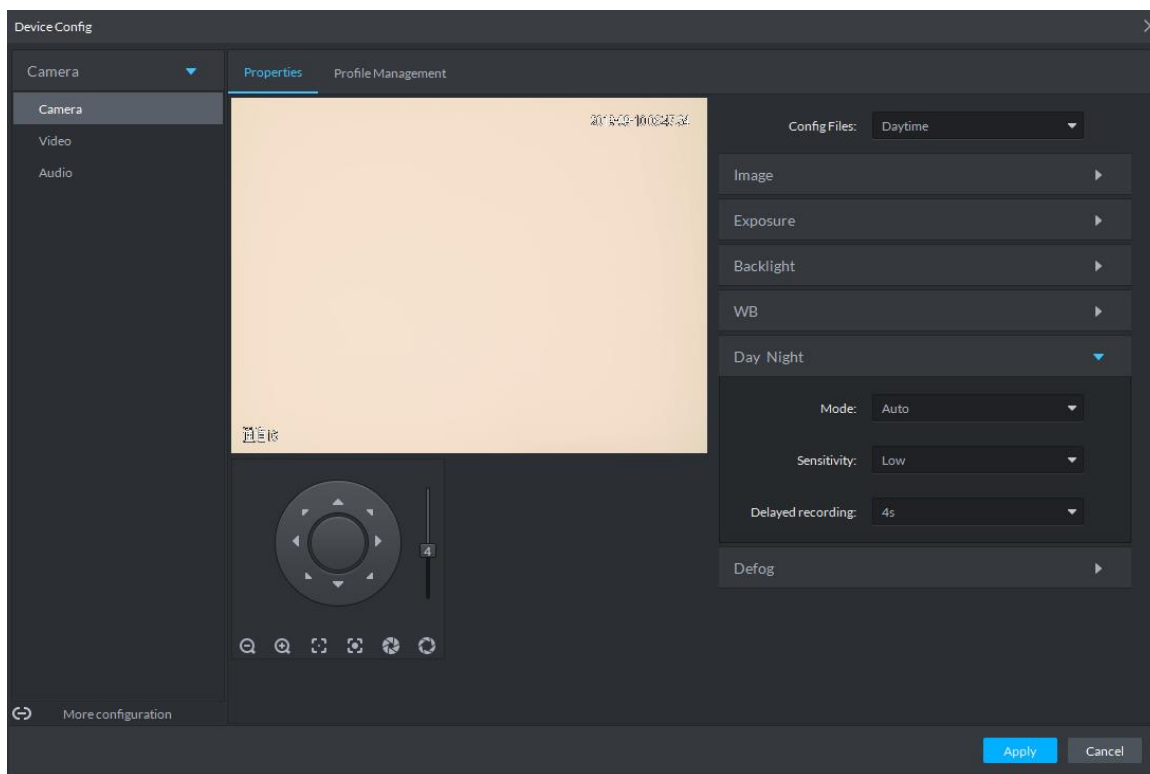



Table 4-21 Day & night parameters

Parameter	Description
Mode	<p>You can set up the image display of the camera to the Colored mode or the Black&White mode, including the following options:</p> <p> The Day & Night settings are independent of the Config Files settings.</p> <ul style="list-style-type: none"> ● Colored: The camera displays colored images. ● Auto: The camera automatically selects to display colored or black&white images based on the environmental brightness. ● Black&White: The camera displays black&white images.
Sensitivity	<p>You can set up this parameter when the Day & Night mode is set to Auto. Defines the sensitivity of the camera in switching between the Colored mode and the Black&White mode.</p>
Delayed recording	<p>You can set up this parameter when the Day & Night mode is set to Auto. Defines the delay of the camera in switching between the Colored mode and the Black&White mode. The lower the delay, the faster the switch between the Colored mode and the Black&White mode.</p>

Step 10 Click **Defog** to set up relevant parameters. See Figure 4-46. For details of the parameters, see Table 4-22.

Image quality drops when the camera is placed in the foggy or hazy environment. You can turn on **Defog** to make the images clearer.

Figure 4-46 Defog

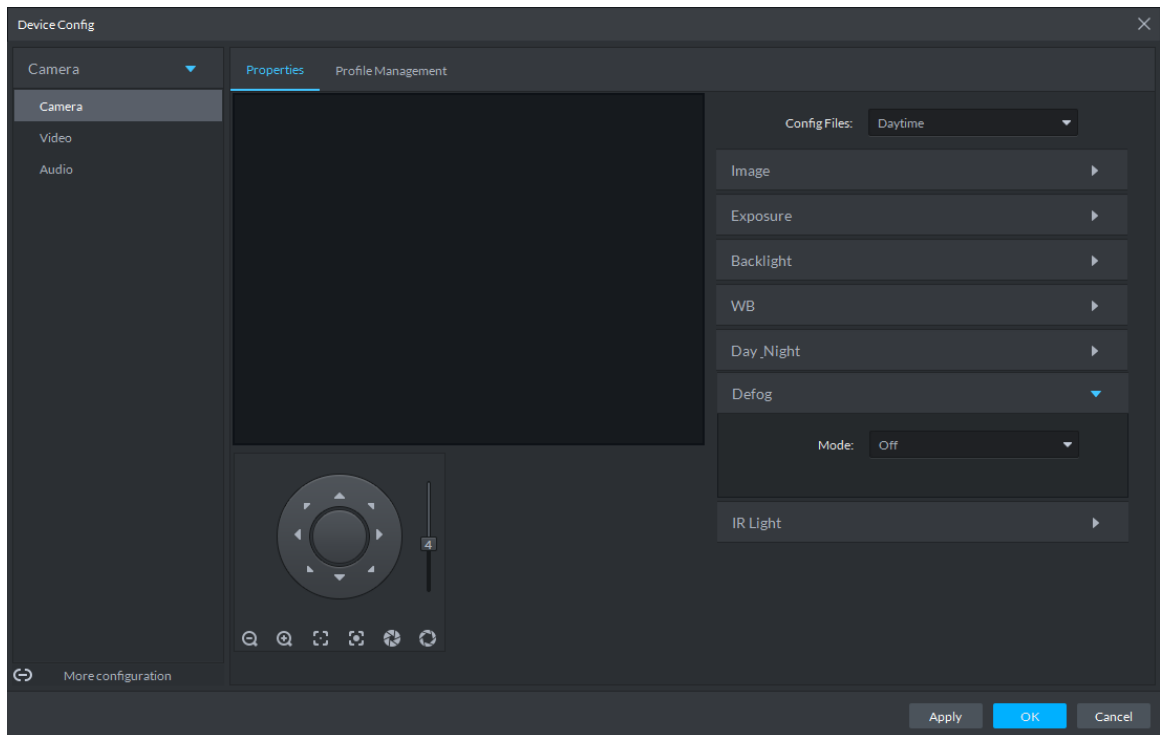


Table 4-22 Defog parameters

Defog mode	Description
Manual	You can set up the defog intensity and the atmospheric light intensity manually. The system adjusts the image quality as per such settings. The atmospheric light intensity mode can be set to Auto or Manual for light intensity adjustment.
Auto	The system adjusts the image quality automatically to adapt to the surrounding conditions.
Off	Defog disabled.

Step 11 Click **IR Light** to set relevant parameters.

Figure 4-47 IR light

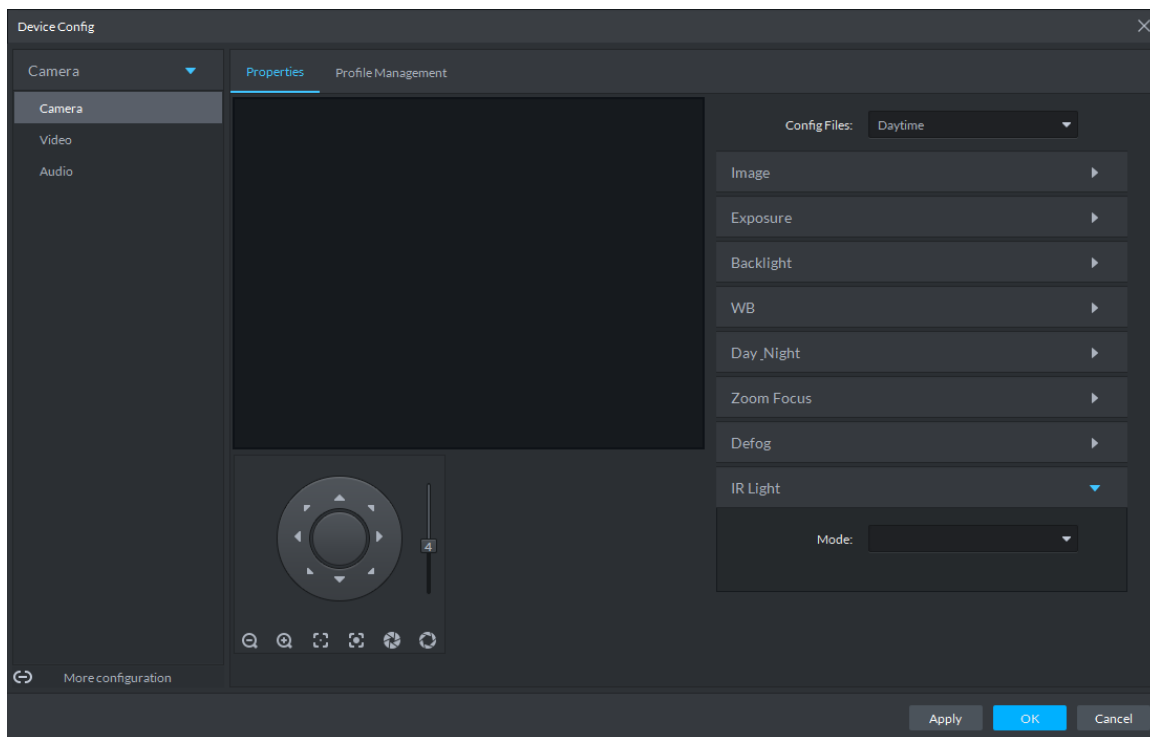


Table 4-23 IR light parameters

IR Light mode	Description
Manual	You can set up the IR Light brightness manually. The system fills light for images as per the preset IR Light brightness.
SmartIR	The system adjusts the brightness of the light to adapt to the surrounding conditions.
ZoomPrio	The system adjusts the IR Light automatically to adapt to the brightness changes in the environment. <ul style="list-style-type: none"> When the scene darkens, the system opens the near light first. If the required brightness still cannot be achieved when the near light runs at full power, the system turns on the far light. When the scene becomes brighter, the system reduces the brightness of the far light all the way until it is turned off, before adjusting the brightness of the near light. When the lens focus is adjusted to a certain wide end, the system keeps the far light off to avoid over-exposure at the near end. You can also set up lighting correction manually to fine tune the brightness of the IR Light.
Off	IR Light disabled.

Step 12 Click **OK**.

If you want to set the configuration files in a different mode, repeat the steps to complete the configurations.

4.3.1.2 Applying Configuration Files

Apply the image parameters as configured in the pre-defined periods.

Step 1 Log in to the Control Client.

Step 2 On the **Live View** interface, right-click the video device and select **Device Config**.

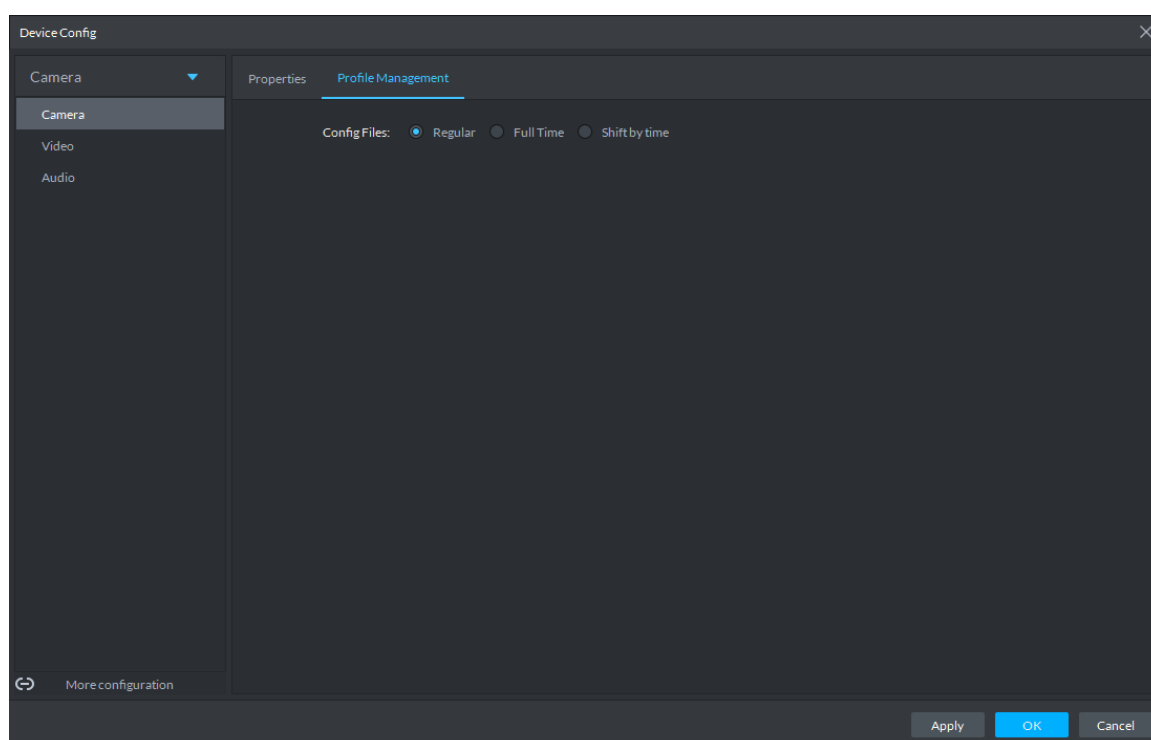
Step 3 Select **Camera > Camera > Properties > Profile Management**.

The **Profile Management** interface is displayed.

Step 4 Setting up configuration files.

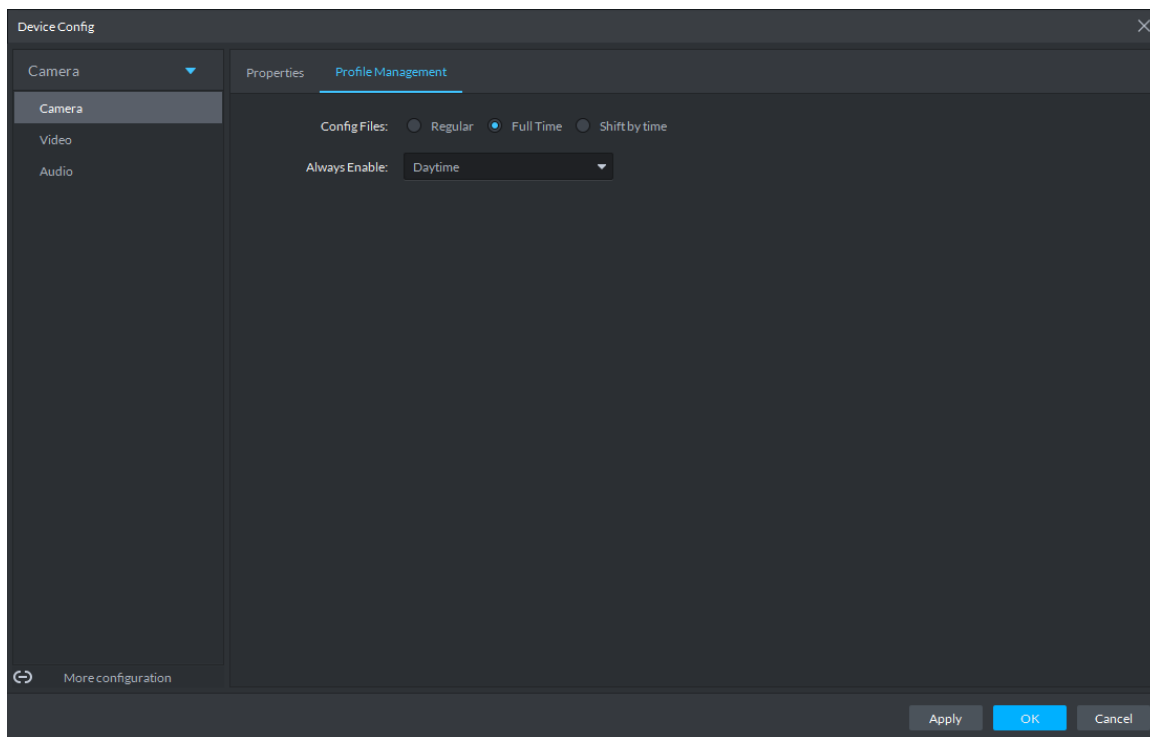
- When **Config Files** is set to **Regular**, the system monitors the objects as per regular configurations.

Figure 4-48 Set configuration files as regular



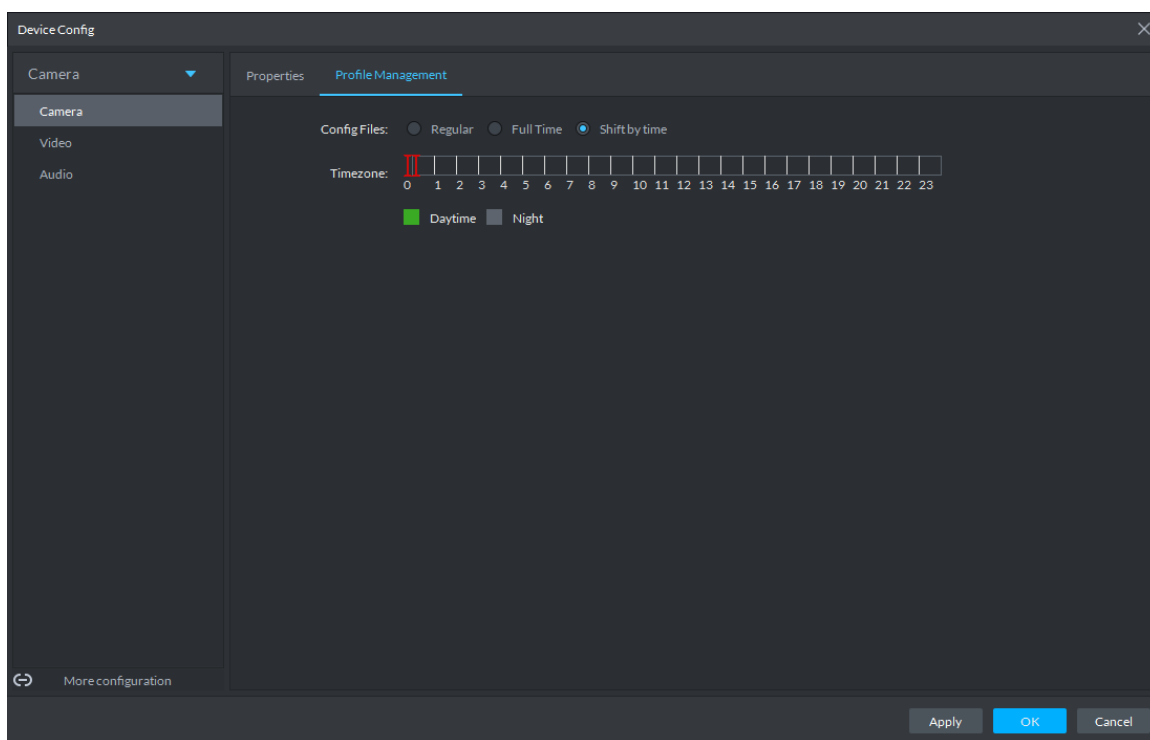
- When **Config Files** is set to **Full Time**, you can set **Always Enable** to **Daytime** or **Night**. The system monitors the objects as per the **Always Enable** configurations.

Figure 4-49 Set configuration files as full time



- When **Config Files** is set to **Shift by time**, you can drag the slider to set a period of time as daytime or night. For example, you can set 8:00–18:00 as daytime, 0:00–8:00 and 18:00–24:00 as night. The system monitors the objects in different time periods as per corresponding configurations.

Figure 4-50 Set configuration files as shift by time



Step 5 Click **OK** to save the configurations.

4.3.2 Video

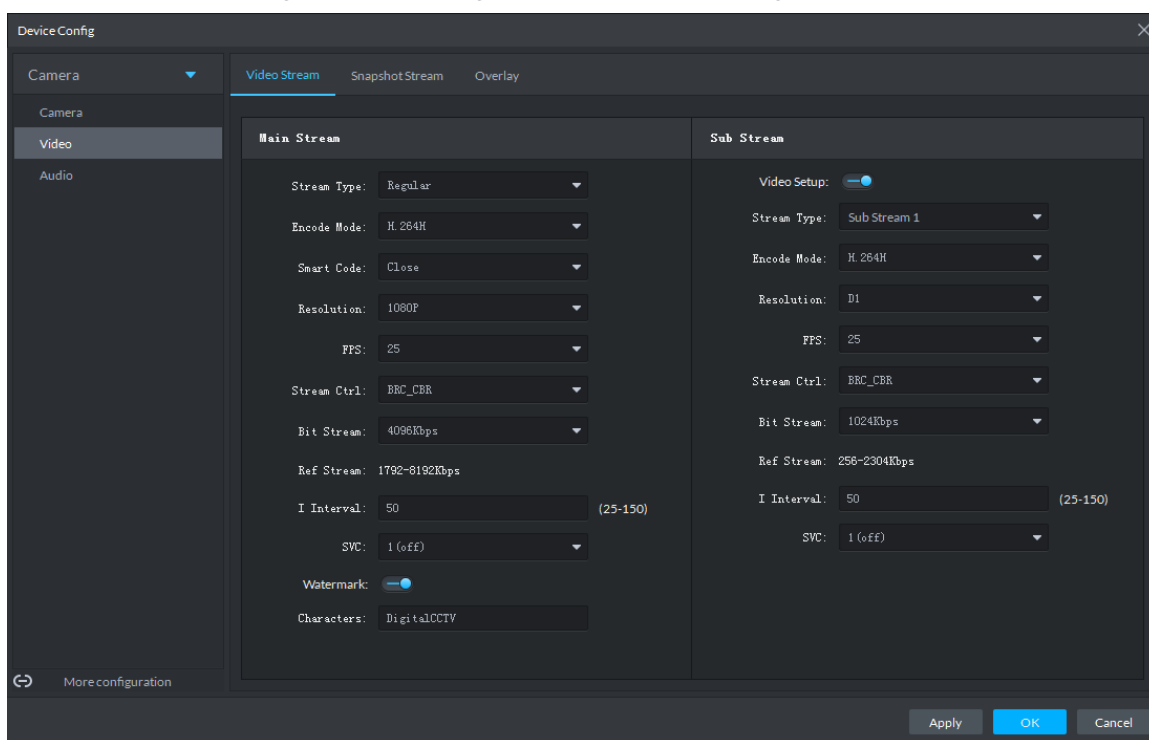
Set video parameters such as video stream, snapshot stream, overlay, ROI, saving path, and video encryption.

4.3.2.1 Video Stream

Set the video stream parameters such as stream type, encoding mode, resolution, frame rate, stream control, stream, I frame interval, SVC, and watermark.

Step 1 On the **Device Config** interface, select **Camera > Video > Video Stream**.

Figure 4-51 Configure video stream settings





Step 2 Set Video Stream.



The default values of streams might vary in different devices. The actual interfaces shall prevail.

Table 4-24 Video stream parameters

Parameter	Description
Video Setup	Indicates whether to set up the Sub Stream parameters.

Parameter	Description
Encode Mode	Encoding modes available: <ul style="list-style-type: none"> • H.264: H.264B (Baseline Profile), H.264 (Main Profile), H.264H (High Profile). Bandwidth consumption level at the same image quality: H.264B > H.264 > H.264H. • H.265: Main Profile encoding, consuming less bandwidth than H.264 at the same image quality. • MJPEG: Frame-by-frame compression, requiring large bandwidth and high video stream to ensure clear image. To achieve better video image, it is recommended that you select the largest stream value from the given options.
Smart Code	Turning on Smart Code helps compress the images more and reduce the storage space.  <p>When Smart Code is on, the device does not support sub stream 2, ROI, IVS event detection. The actual screens shall prevail.</p>
Resolution	The resolution of the videos. Different devices might have different max resolutions. The actual interfaces shall prevail.
FPS	The number of frames per second in a video. The higher the FPS, the more distinct and smooth the images.
Stream Ctrl	The following video stream control modes are available: <ul style="list-style-type: none"> • BRC_CBR: The bit stream changes slightly around the preset value. • BRC_VBR: The bit stream changes according to the monitored scenes.  <p>When the Encode Mode is set to MJPEG, BRC_CBR remains the only option for stream control.</p>
Image Quality	This parameter can be set only when Stream Ctrl is set to BRC_VBR. Video image quality is divided into six grades: Best, Better, Good, Bad, Worse and Worst.
Bit Stream	This parameter can be set only when Stream Ctrl is set to BRC_CBR . You can select the proper stream value from the drop-down box based on actual scenarios.
Ref Stream	The system will recommend an optimal range of stream values to users based on the resolution and FPS set up by them.
I Interval	Refers to the number of P frames between two I frames. The range of I Interval changes with FPS. It is recommended to set the I Interval to be two times as the FPS value.
SVC	FPS is subject to layered encoding. SVC is a scalable video encoding method on time domain.
Watermark	Turn on Watermark to enable this feature. You can verify the watermark characters to check whether the video has been tempered or not.
Characters	Characters for watermark verification. The default value is DigitalCCTV.

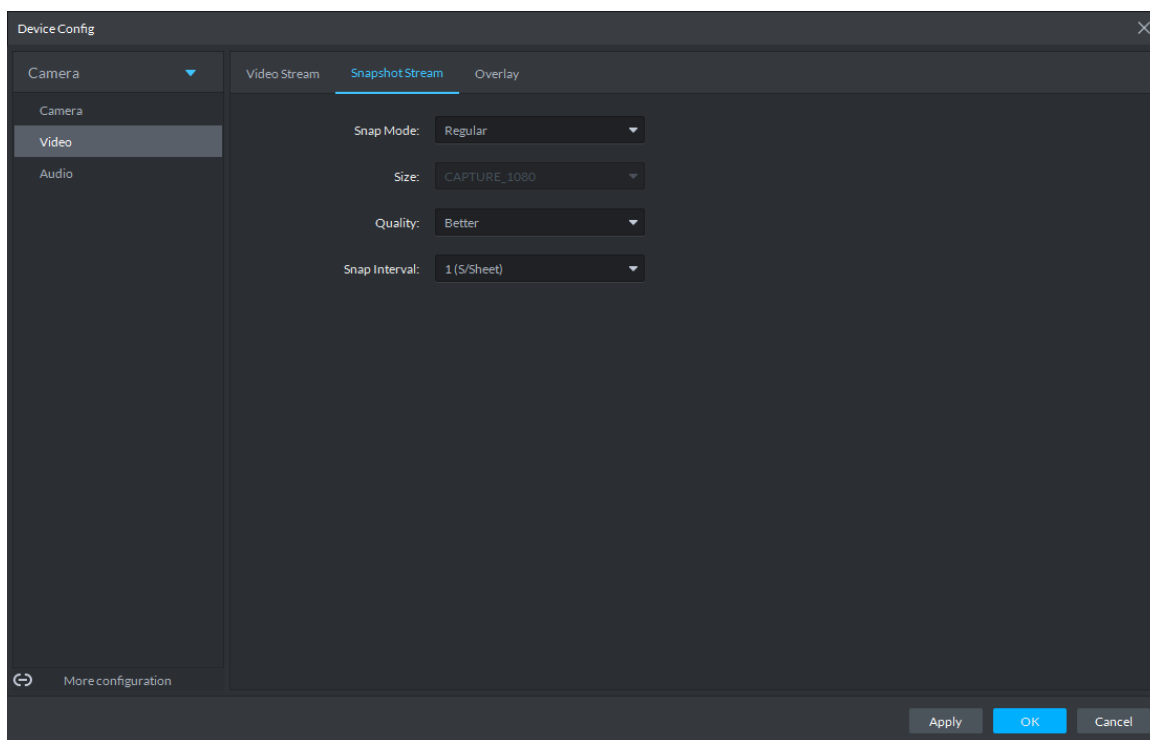
Step 3 Click **OK**.

4.3.2.2 Snapshot Stream

Set snapshot parameters, including snapshot type, picture size, picture quality, and snapshot speed.

Step 1 On the **Device Config** interface, select **Camera > Video > Snapshot Stream**.

Figure 4-52 Configure snapshot stream settings



Step 2 Set **Snapshot Stream**.

Table 4-25 Snapshot stream parameters

Parameter	Description
Snap Mode	It includes Regular and Trigger . <ul style="list-style-type: none"> Regular refers to capturing pictures within the time range set up in a time table. Trigger refers to capturing pictures when video detection, audio detection, IVS events, or alarms are triggered, provided that video detection, audio detection, and corresponding snapshot functions are turned on.
Size	Same as the resolution in Main Stream.
Quality	Sets up image quality. It is divided into six grades: Best, Better, Good, Bad, Worse and Worst.
Snap Interval	Sets up the frequency of snapshots. Select Custom to manually set up the frequency of snapshots.

Step 3 Click **OK** .

4.3.2.3 Overlay

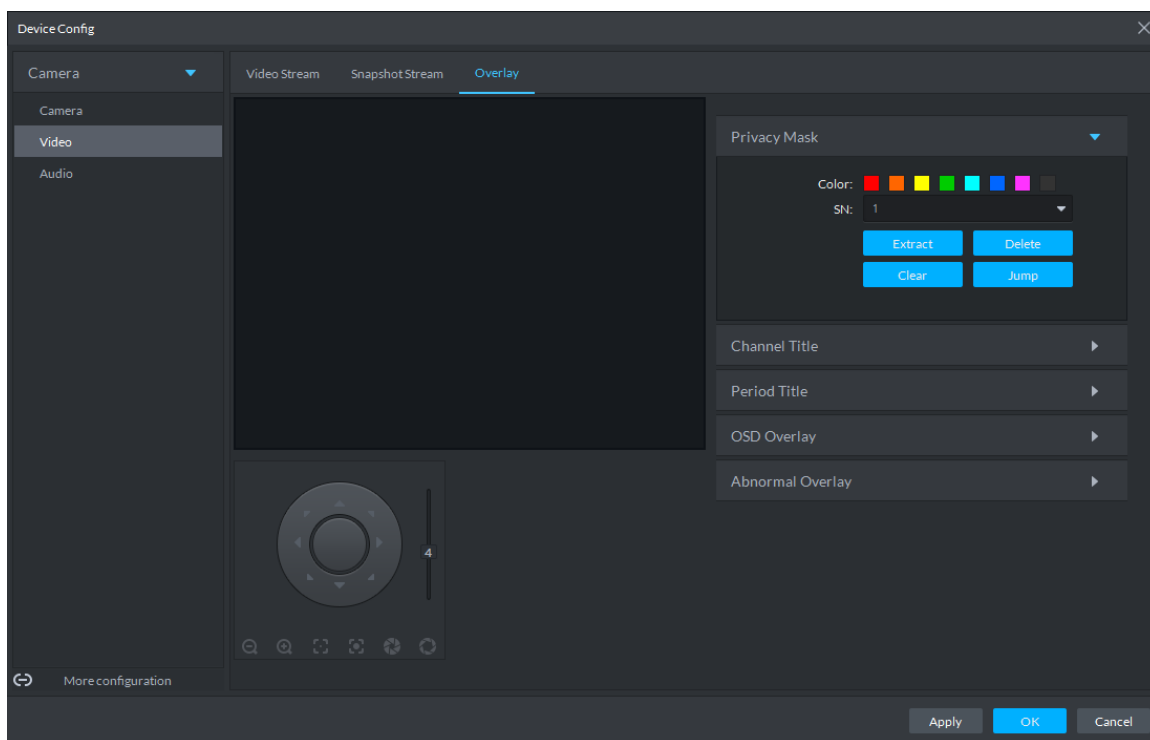
Set video overlay parameters, including tampering, privacy mask, channel title, period title, geographic position, OSD, font, and picture overlay.

Step 1 On the **Device Config** interface, select **Camera > Video > Overlay**.

Step 2 (Optional) Set privacy mask.

- 1) Click the **Privacy Mask** tab.

Figure 4-53 Configure overlay settings



- 2) Select **Enable** and drag a box to the target area for privacy protection.

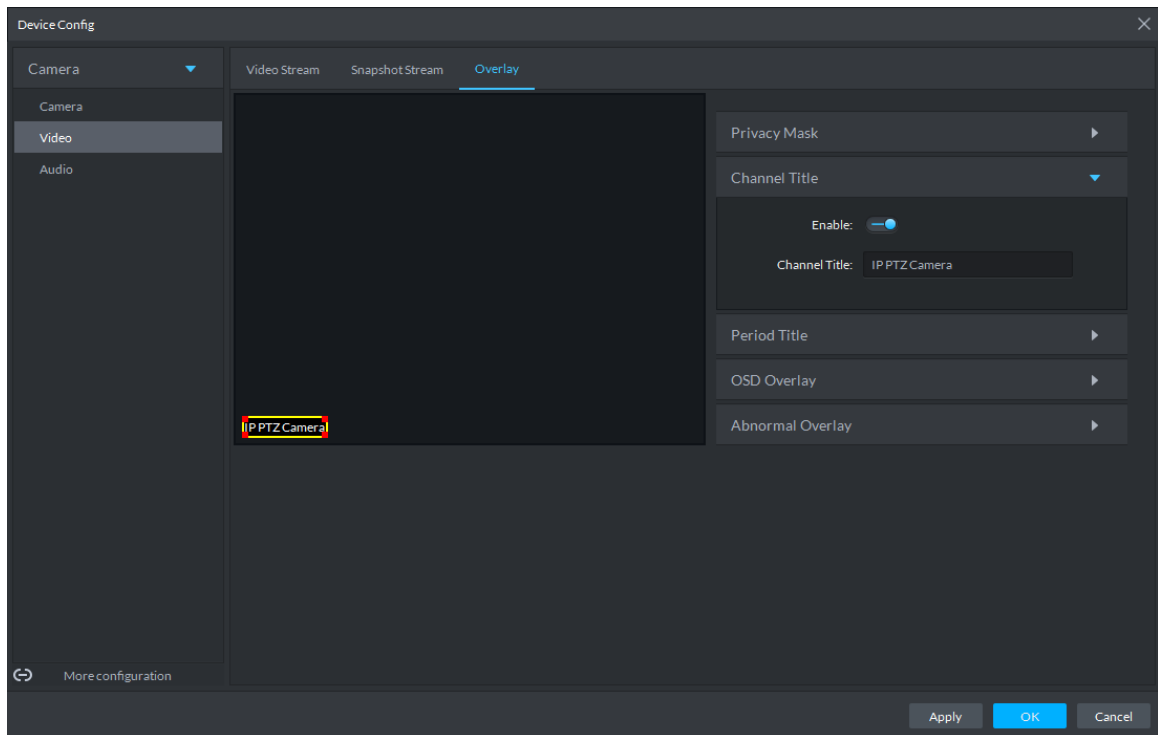


- You can draw up to four boxes.
- Click **Clear** to delete all boxes; to delete a box, select it and click **Delete**, or right-click and delete the box you want.

Step 3 (Optional) Set channel title.

- 1) Click the **Channel Title** tab.

Figure 4-54 Set channel title



- 2) Select **Enable** and set up the Channel Title, which is then displayed in the video images.

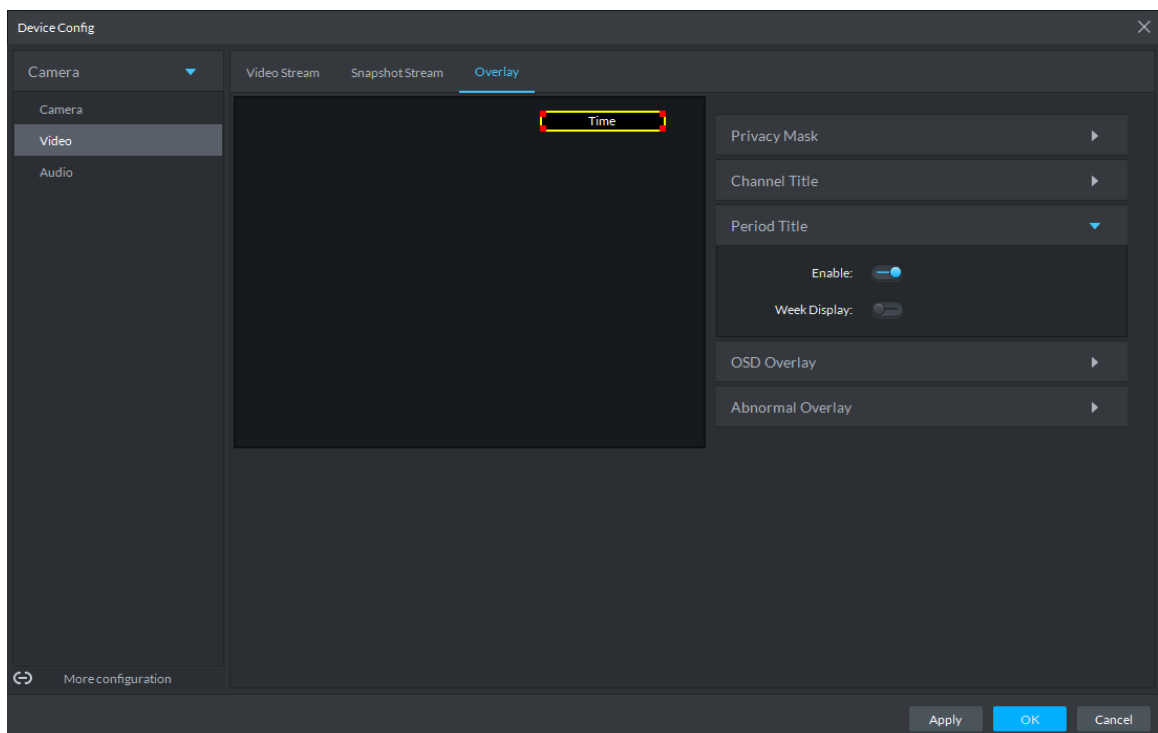


In the video image, the channel title box can be moved to a proper position.

Step 4 (Optional) Set period title.

- 1) Click the **Period Title** tab.

Figure 4-55 Set period title



- 2) Select **Enable** and the time information is displayed in the video images.
- 3) Select **Week Display** and the week information displays in video images.



In the video image, the period title box can be moved to a proper position.

Step 5 Click **OK**.

4.3.3 Audio

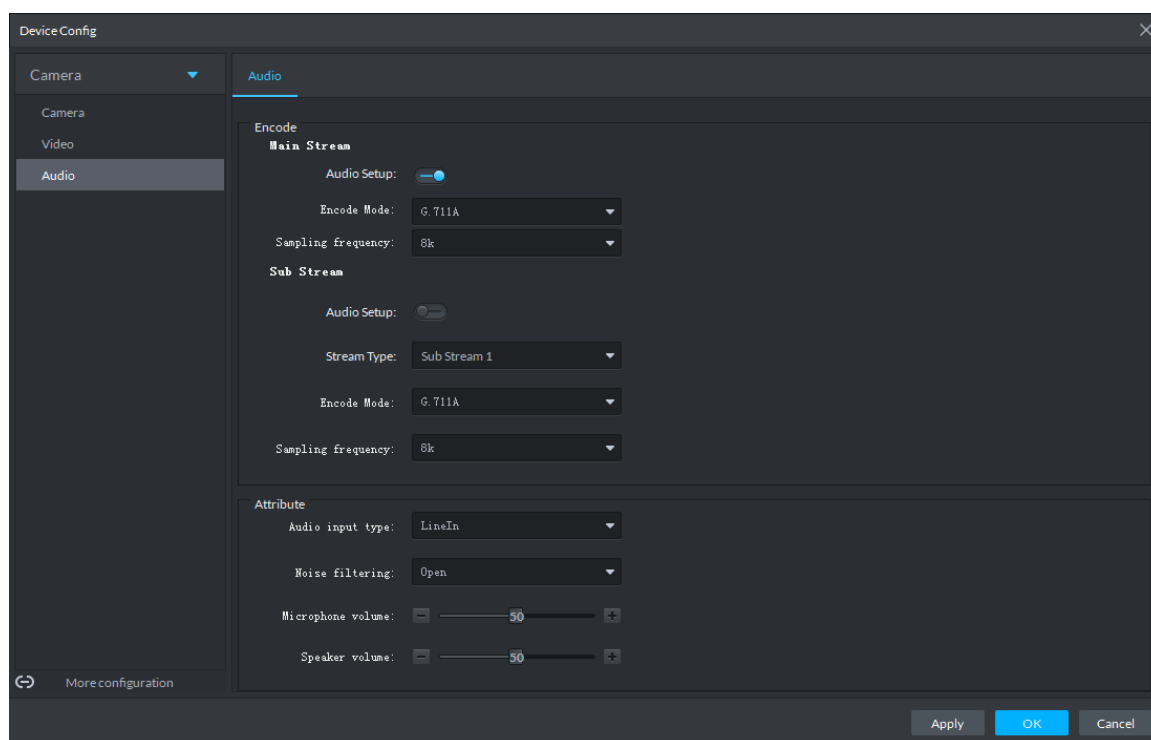
Set audio parameters such as encoding mode, sampling frequency, audio input type, and noise filtering.



Some devices do not support audio functions.

Step 1 On the **Device Config** interface, select **Camera > Audio**.



Figure 4-56 Configure audio settings



Step 2 Set parameters.

Table 4-26 Audio parameters

Parameter	Description
Enable	Audio cannot be enabled unless video has been enabled. After choosing Enable in Main Stream or Sub Stream sections, the network transmits a mixed flow of videos and audios. Otherwise, the transmitted flow only contains video images.
Encode Mode	The encoding modes of audios include G.711A, G.711Mu, AAC, and G.726. The preset audio encode mode applies both to audio talks and voice talks.

Parameter	Description
Sampling frequency	Available audio sampling frequencies include 8K, 16K, 32K, 48K, and 64K.
Audio input type	The following types of audios connected to devices are available: <ul style="list-style-type: none"> • LineIn: The device must connect to external audio devices. • Mic: The device does not need external audio devices.
Noise filtering	After enabling noise filtering, the system automatically filters out the noises in the environment.
Microphone volume	Adjusts the microphone volume.  Only some devices support adjusting microphone volume.
Speaker volume	Adjusts the speaker volume.  Only some devices support adjusting speaker volume.

Step 3 Click **OK**.

4.4 Event and Alarm

The platform receives device alarms and displays them according to your alarm configurations on the platform. After enabling and configuring alarm plans on the Web Manager, the Control Client can display the corresponding alarms for you to handle. The system supports the following alarm linkage actions:

- Link camera
When the alarm happens, the client will play the linked camera video, or the linked camera will be triggered to start recording or take snapshot.
- Link PTZ
When the alarm happens, the linked PTZ camera will be triggered to turn to a specific preset point.
- Link alarm output
When the alarm happens, the linked alarm output channel will output alarm signal. If the channel is connected with a siren, the siren will make a sound.
- Link video wall display
When the alarm happens, the linked video will be displayed on the video wall.
- Link email
When the alarm happens, the system will automatically send an email as configured.
- Link user
When the alarm happens, the system will notify a specific user as configured.
- Link door
When the alarm happens, the linked door will open or close as configured.



- You need to configure each alarm type on the Web Manager.
- One alarm can have multiple linkage actions.

4.4.1 Configuring Events

4.4.1.1 Preparations


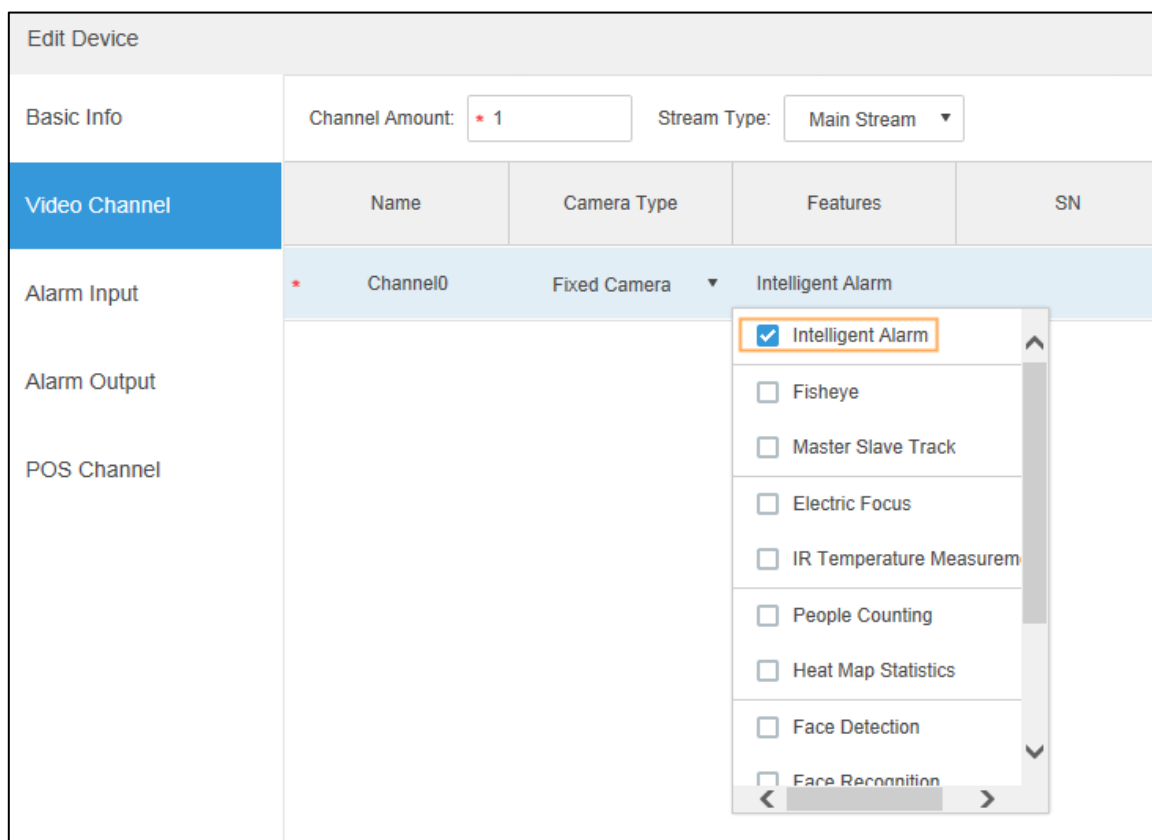
- Devices are well deployed. For details, see the corresponding documents.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
- ◇ Take configuring IVS alarm for example. On the **Device** interface, click  of the device, and then select **Intelligent Alarm** for **Features**.

Figure 4-57 Edit features (1)



The screenshot shows the 'Edit Device' interface. On the left, there is a sidebar with sections: 'Basic Info', 'Video Channel' (highlighted in blue), 'Alarm Input', 'Alarm Output', and 'POS Channel'. The main area displays configuration for 'Channel0' with 'Fixed Camera' selected. A dropdown menu for 'Features' is open, showing a list of features with checkboxes:

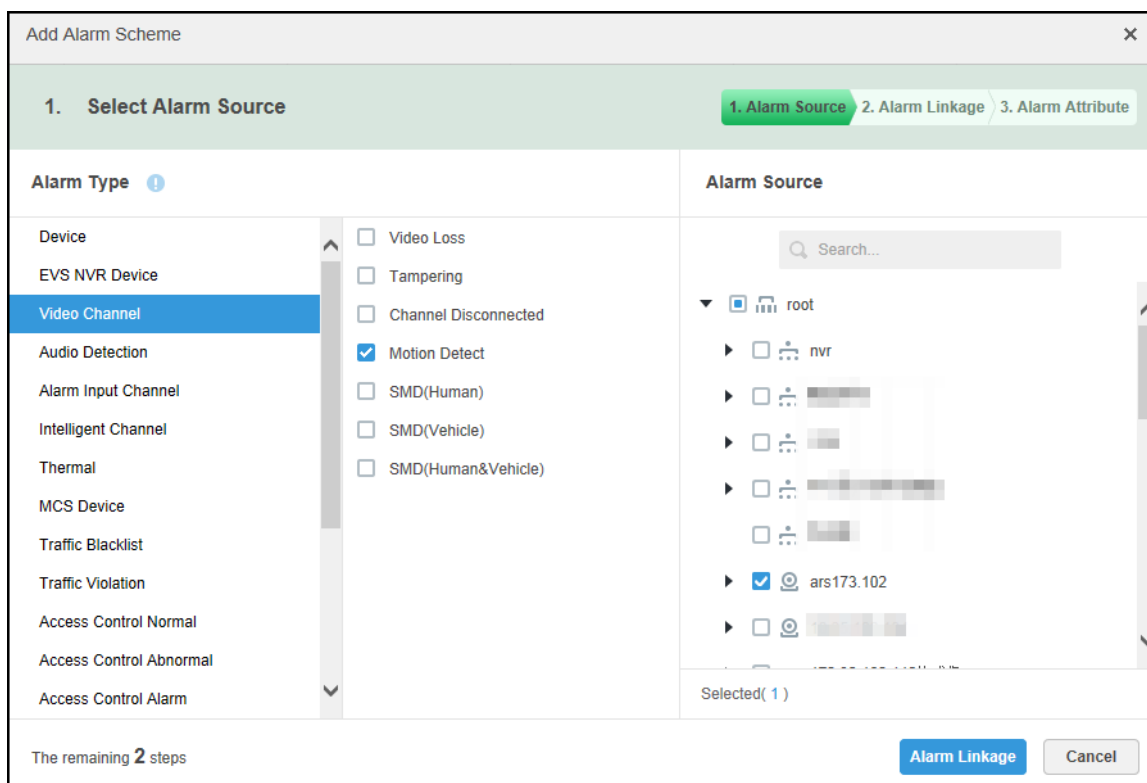
Name	Camera Type	Features	SN
Channel0	Fixed Camera	Intelligent Alarm	

The 'Intelligent Alarm' feature is checked (indicated by a blue checkmark and an orange border). Other features listed include Fisheye, Master Slave Track, Electric Focus, IR Temperature Measurement, People Counting, Heat Map Statistics, Face Detection, and Face Recognition.

4.4.1.2 Configuring Events

Step 1 Click **Add**.

Figure 4-58 Edit alarm scheme

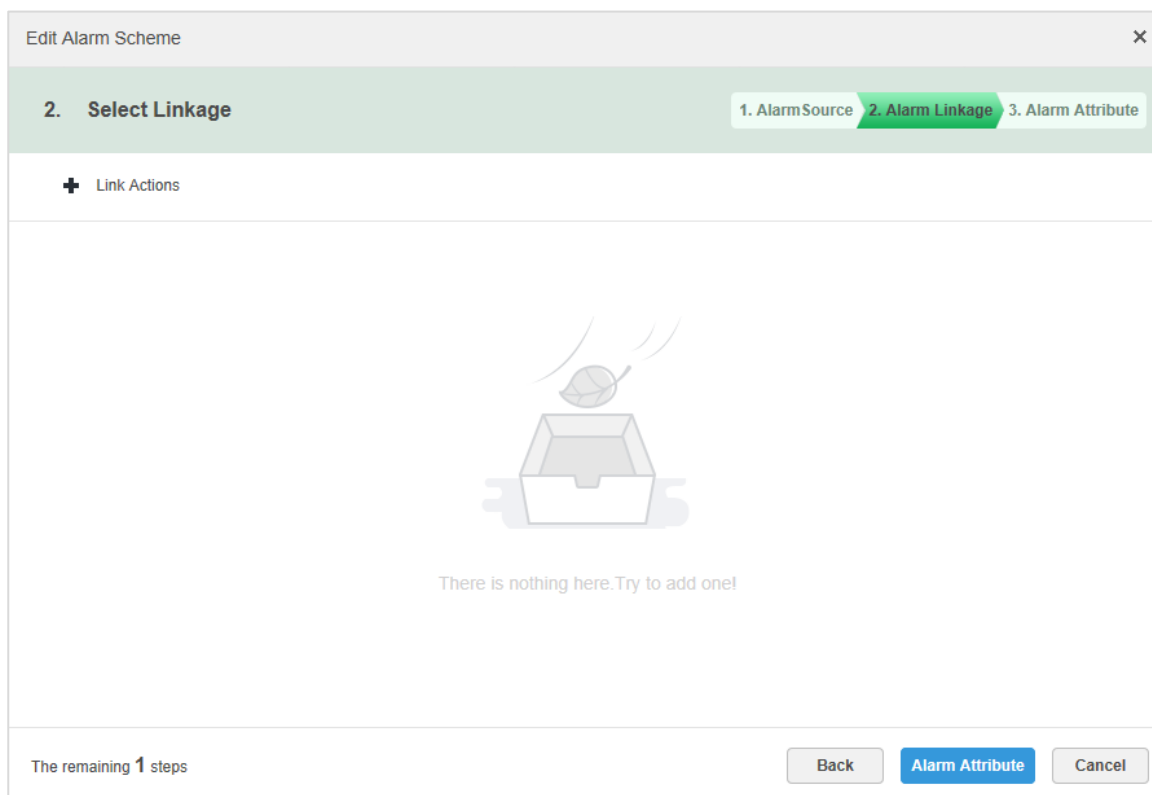



Step 2 Configure alarm source.


Alarm type can be classified into general types and custom types. General types of alarms are received from the devices and there is no need for configuration here. Custom types of alarms are defined by the user here.


- General alarm types (all types except for the **Custom Alarm** on the list)
Select an alarm type and the relevant alarm source, and then click **Alarm Linkage**.

Figure 4-59 Add alarm scheme



- Custom alarm types
 Take Stay No. Alarm for example.
 If you want to be notified if the number of people goes beyond a threshold inside a place, your store for example, where the entrances and exits are equipped with people-counting cameras, you can configure a Stay No. Alarm. The alarm can combine the cameras, two or more, to calculate and monitor the total number of people that have not left.
- 1) On the **Alarm Type** list, scroll down until you find the **Custom Alarm**. Click it, and then select **Stay No. Alarm**.


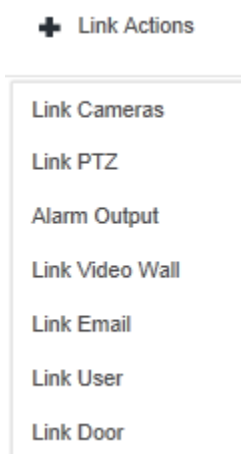
The data statistics for Stay No. alarm is refreshed every 5 minutes.
- 2) In the **Alarm Source** section, enter the rule name, and the people number threshold that triggers an alarm if reached.


The people number threshold for the Stay No. Alarm is limited up to 1 million.
- 3) Click **Add**, select a camera in the **Channel Name** column, and then select a people-counting tripwire. For example, an entry people-counting tripwire.

 - The people-counting tripwires are configured on the camera. For details, see the camera *User's Manual*.
 - On the camera, do not modify the settings of the tripwires that have been associated here; otherwise the Stay No. Alarm configuration will become invalid.

- For the relevant cameras used for the Stay No. Alarm, do not disable the people-counting feature on the platform; otherwise the Stay No. Alarm configuration will become invalid.
- 4) Click **Add** again, and repeat the previous step to select another camera and tripwire. For example, an exit people-counting tripwire.
- Step 3 Configure alarm linkage actions.

- 1) Click **+** .

Figure 4-60 Link actions



- 2) Select linkage actions.
- ◇ Click **Link Cameras**, and then set parameters.



To achieve video pop-up on the client when the associated alarm is triggered, after configuring the camera linkage settings here, remember to select **Open camera video on client when alarm is triggered**, and then select **Display alarm link video when alarm occurred** in **Local Config > Alarm** on the Control Client.

Figure 4-61 Link camera

Edit Alarm Scheme
✕

2. Select Linkage

1. Alarm Source
2. Alarm Linkage
3. Alarm Attribute

Link Cameras
+

Link Bind Camera

Select Camera

Link bind camera prompt
All video channels bind themselves, you can configure the source binding on the device config page.

Position:

Stream Type:

Record Time: s

Prerecord Time: s

Capture a picture of camera when alarm is triggered.

Open camera video on client when alarm is triggered.

The remaining 1 steps

Back
Alarm Attribute
Cancel

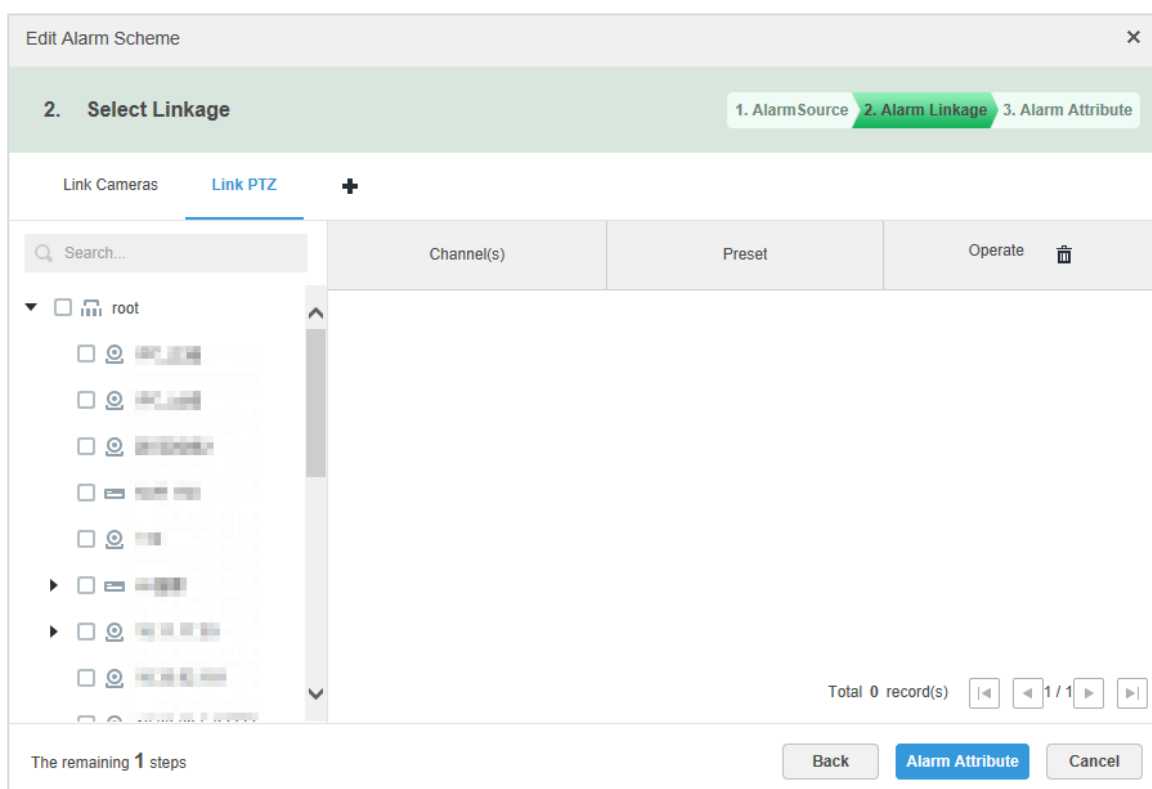
Table 4-27 Parameters

Parameter	Description
<div style="display: flex; flex-direction: column; gap: 10px;"> <div style="display: flex; align-items: center;"> <input checked="" type="radio"/> Link Bind Camera </div> <div style="display: flex; align-items: center;"> <input type="radio"/> Select Camera ! </div> </div>	<ul style="list-style-type: none"> Bind camera: Select this option to let the alarm trigger the video of the camera that has been bound to the current camera (the camera you are configuring alarm for). If the camera for which you are configuring alarm has not been bound to any other camera (see "3.4.6 Binding Resources"), the platform thinks that it is bound to itself. Select a camera for linkage: Manually select a camera to link with the alarm. <p> Custom alarms cannot link camera.</p>
Position	Set whether to record and store the video on server or device.
Stream Type	Set the stream type of recording video. Main stream has higher quality than sub stream, but consumes more storage and bandwidth than sub stream.
Record Time	Set the duration of video recording.
Prerecord Time	The recording time before setting link camera, the selected device is required to support record and it already exists in the device recording.
Capture a picture of camera when alarm is triggered.	Confirm if it captures camera picture.

Parameter	Description
Open camera video on client when alarm is triggered.	Confirm if it opens camera video window on the client during alarm.

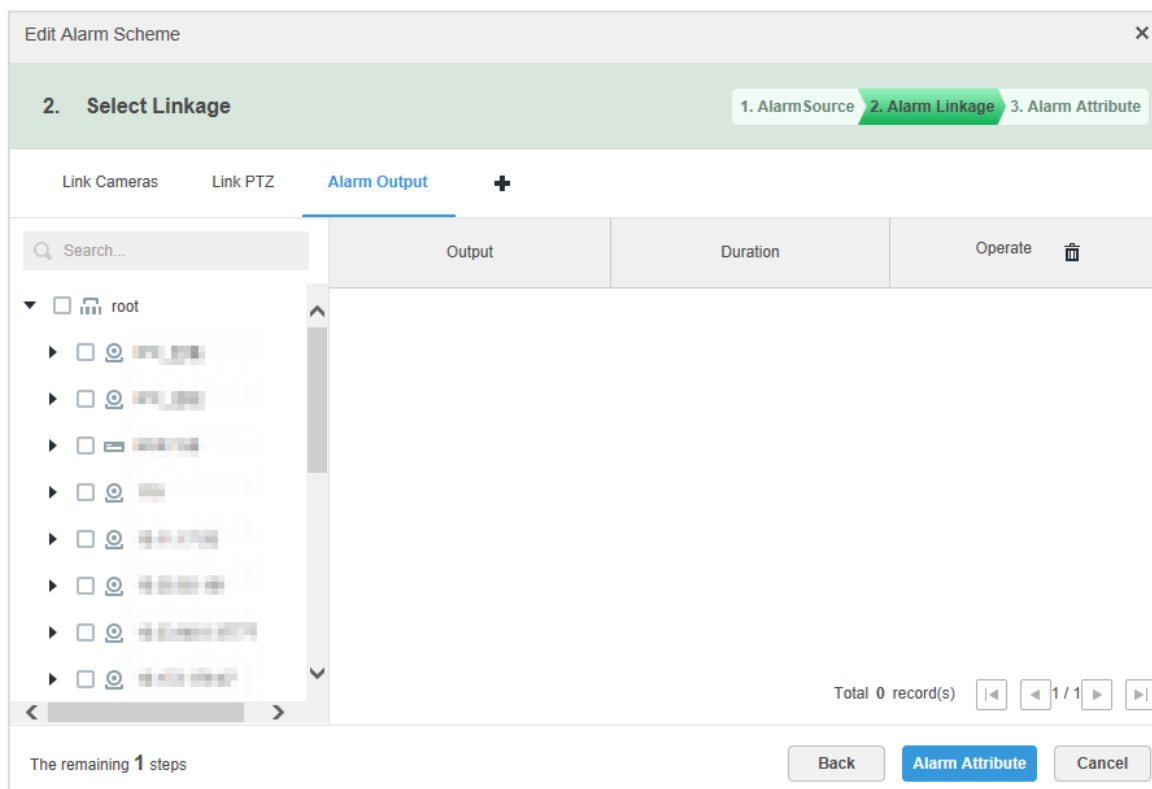
- ◇ Click **Link PTZ**, select the channels which need PTZ to link device, and then set prerecord actions.

Figure 4-62 Link PTZ



- ◇ Click **Alarm Output**, select alarm output channel, and then set duration.

Figure 4-63 Link alarm output

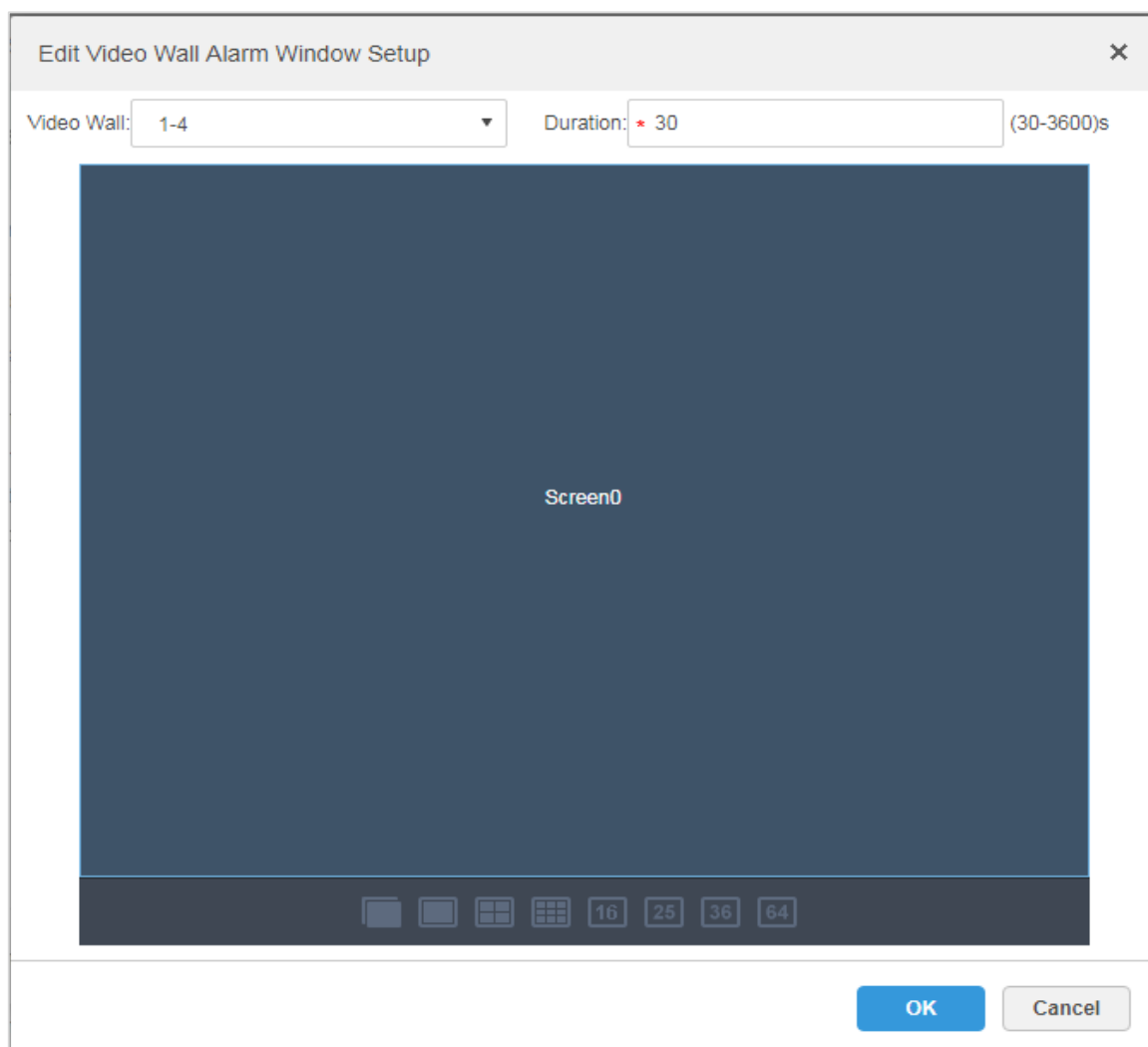


- ◇ Click **Link Video Wall**, select link camera on the left of the interface, select video wall on the right of the interface. When selecting **Link Bind Camera** and **Link Camera**, the interfaces will display differently, please base on the actual display. Click **Video Wall Alarm Window Setup** to set duration and select the video channel which needs to be displayed on wall.

Figure 4-64 Link video wall (1)

The screenshot shows a web-based configuration window titled "Edit Alarm Scheme". At the top, there are three progress steps: "1. AlarmSource", "2. Alarm Linkage" (highlighted in green), and "3. Alarm Attribute". Below this, there are four tabs: "Link Cameras", "Link PTZ", "Alarm Output", and "Link Video Wall" (which is selected and underlined). A plus sign icon is next to the "Link Video Wall" tab. On the left side, there are two radio button options: "Link Bind Camera" (selected) and "Select Camera". Below these options is a text prompt: "Link bind camera prompt. All video channels bind themselves, you can configure the source binding on the device config page." To the right of the radio buttons, there is a "Video Wall:" label followed by a dropdown menu showing "rf". Further right is a button labeled "Video Wall Alarm Window Setup". The bottom of the window features a status bar with the text "The remaining 1 steps" on the left and three buttons: "Back", "Alarm Attribute" (highlighted in blue), and "Cancel" on the right.

Figure 4-65 Link video wall (2)



- ◇ Click **Link Email**, select email template and recipient.
 The mail template can be configured, click the ▼ next to **Mail Template** and select **New Mail Template**, set new mail template.
 Point to **Subject**, and then click and select **Event Time**, **Event Source** and other options.

Figure 4-66 Link email

Edit Alarm Scheme

2. **Select Linkage** 1. Alarm Source 2. Alarm Linkage 3. Alarm Attribute

Link Cameras Link PTZ Alarm Output Link Video Wall **Link Email** +

Email Template:

Address:

Subject:

Send event image

Please pay attention, there is alarm. The following is the details

Time:

Location:

Event Source:

The remaining 1 steps

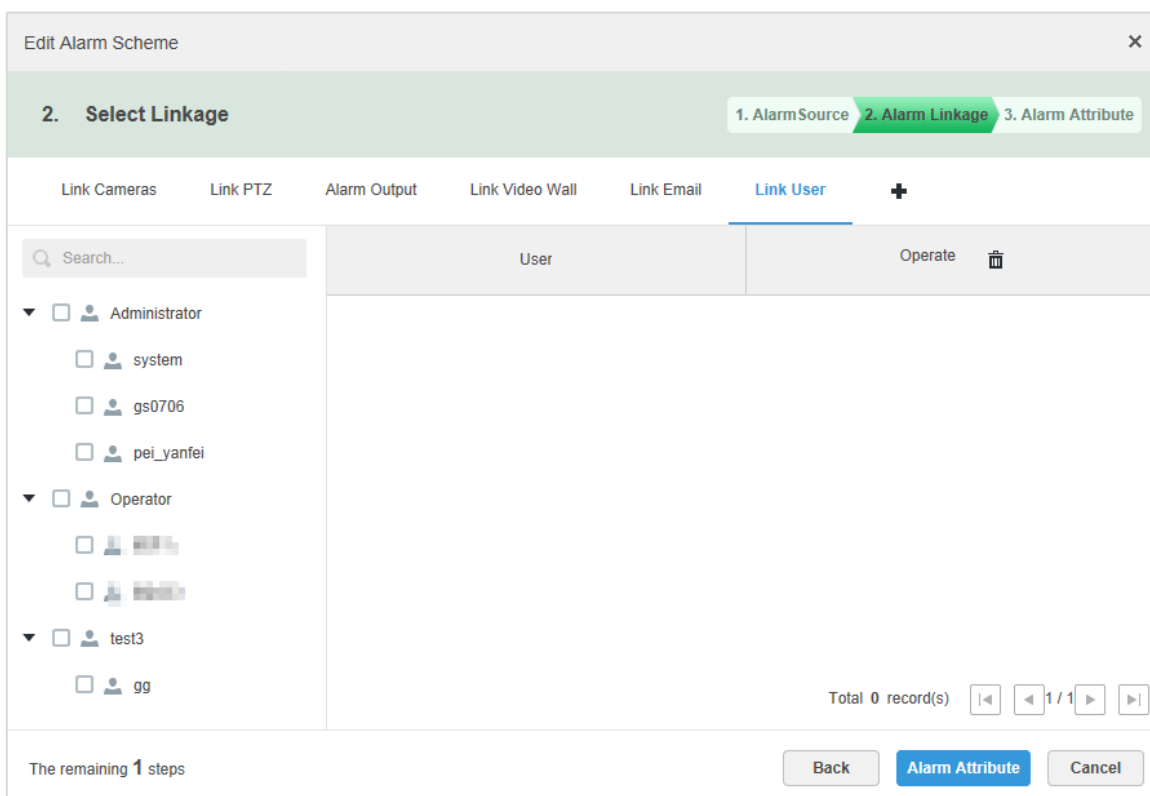
Figure 4-67 Set email template

Add Alarm Scheme

Template Name	Mail Content:
Default	Template Name: <input type="text"/>
test <input type="button" value="edit"/> <input type="button" value="delete"/>	<input type="text" value="Event time Org name Event source Event type"/>
12 <input type="button" value="edit"/> <input type="button" value="delete"/>	Subject: <input type="text"/>
<input type="button" value="+"/> New Template	Mail Content: <input type="text"/>

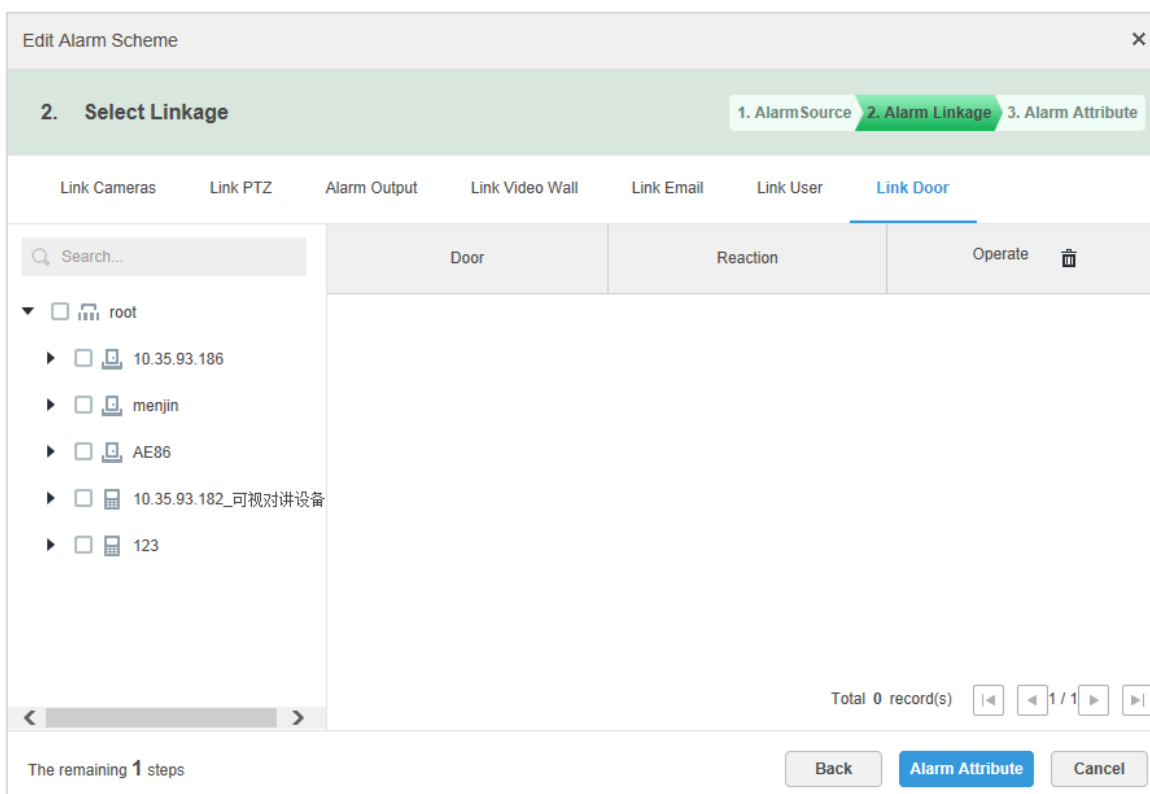
◇ Click **Link User**, and then select the users to be informed.

Figure 4-68 Link user



- ◇ Click **Link Door**, select the access control device, and then set the linkage action.

Figure 4-69 Link door



Step 4 Click **Alarm Attribute**.

Figure 4-70 Configure alarm attribute

The screenshot shows a window titled "Edit Alarm Scheme" with a close button (X) in the top right corner. Below the title bar is a progress indicator with three steps: "1. AlarmSource", "2. Alarm Linkage", and "3. Alarm Attribute" (which is highlighted in green). The main content area contains the following fields:

- Name: (with a red asterisk indicating a required field)
- Time Template: (with a dropdown arrow)
- Priority: (with a dropdown arrow and a red square icon)
- Remark:

At the bottom left, it says "The remaining 0 steps". At the bottom right, there are three buttons: "Back", "OK", and "Cancel".

Step 5 Configure alarm attribute.

- 1) Set alarm name.
- 2) Select alarm time template and priority.
- 3) Click **OK**.

The system displays the added alarm scheme.

Step 6 In the **Operation** column, click OFF to enable scheme. When the icon changes into ON, means that the scheme has been enabled.

Operations

- Edit

Click the of corresponding scheme, and then you can edit the alarm scheme.

- Delete

◇ Select alarm scheme, click Delete to delete scheme in batches.

◇ Click the corresponding of alarm scheme, then you can delete the alarm scheme individually.

- Disable

In the **Operation** column, click ON to disable an event. OFF indicates that the event is disabled.

4.4.2 Viewing Alarms

4.4.2.1 Configuring Alarm Settings

Configure alarm notification methods, such as audible warning and flashing on map.




Step 1 Log in to the Control Client, click  at the upper-right corner, and then select **Local Config > Alarm**.

Figure 4-71 Set alarm parameters

Step 2 Set parameters, and then click **Save**.

Table 4-28 Alarm parameter description

Parameters	Description
Play alarm sound	Select the check box to enable alarm sound. There is sound warning when an alarm occurs.
Loop	Select the check box to enable loop. Alarm sound repeats when an alarm occurs.  The loop function can be enabled only when Play alarm sound is enabled.
Alarm Type	Select the alarm types that need sound warning or map warning.  The loop function can be enabled only when Play alarm sound is enabled.
Sound Path	Select the sound file.

Parameters	Description
Map flashes when alarm occurred	Select the check box to enable map warning, and then select the alarm types that need map warning. The device icon on the map flashes when there is an alarm from it.
Display alarm link video when alarm occurred	Select the check box to enable alarm video display, and then select a video display method between Pop up and In Preview .
Video Opening Type	The way how alarm video is displayed when an alarm occurs.

4.4.2.2 Searching for and Handling Alarms



You can modify and delete custom alarms.

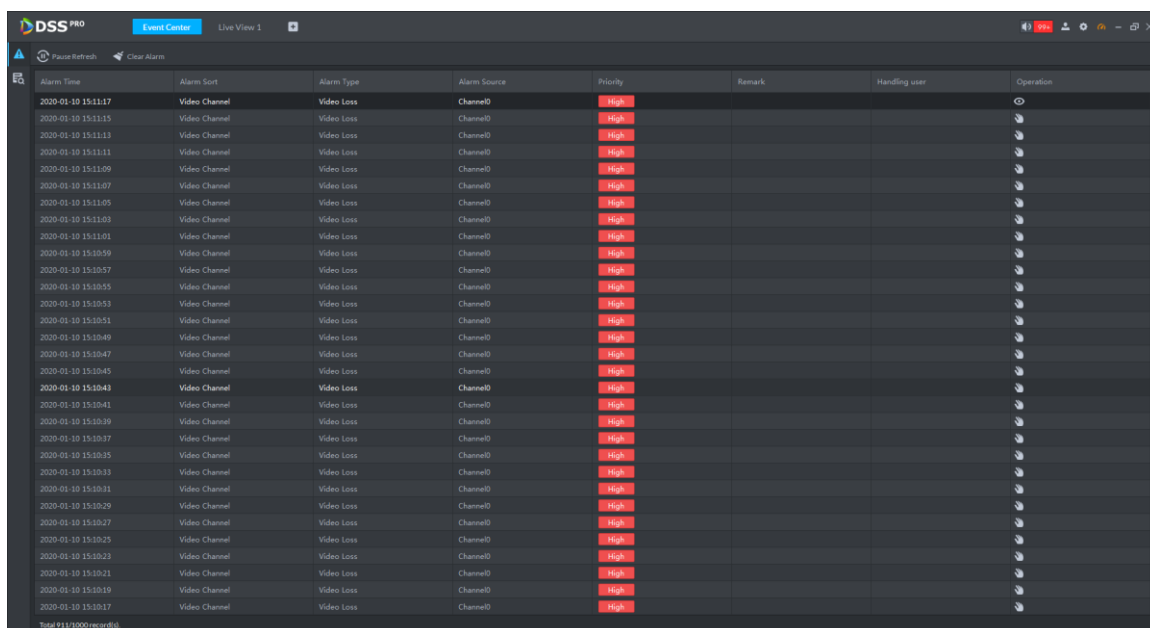
- If a custom alarm is used by an alarm scheme, it cannot be deleted.
- If a custom alarm is not used by an alarm scheme, it can be deleted. The alarm type of the channel restores default after the custom alarm is deleted.
- If the custom alarm name is modified, the old configurations still have the old name, while the new configurations will have the new name.

4.4.2.2.1 Handling Real-time Alarms

Step 1 Log in to the Control Client, click , and then select **Event Center**.

Step 2 Click  to open the **Real-time Alarm** interface.

Figure 4-72 Real-time alarms



Alarm Time	Alarm Sort	Alarm Type	Alarm Source	Priority	Remark	Handling user	Operation
2020-01-10 15:11:17	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:11:15	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:11:13	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:11:11	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:11:09	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:11:07	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:11:05	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:11:03	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:11:01	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:59	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:57	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:55	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:53	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:51	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:49	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:47	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:45	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:43	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:41	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:39	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:37	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:35	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:33	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:31	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:29	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:27	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:25	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:23	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:21	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:19	Video Channel	Video Loss	Channel0	High			
2020-01-10 15:10:17	Video Channel	Video Loss	Channel0	High			

Total 911/1000 records.



The alarm list is refreshed in real time. To stop refreshing, click ; to resume

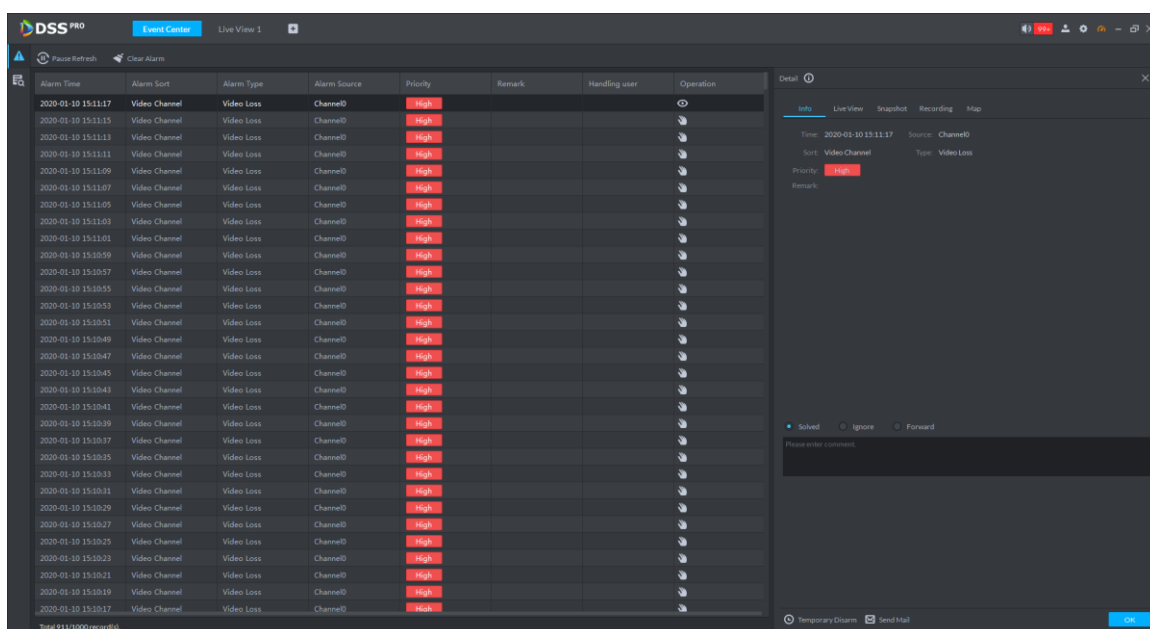
refreshing, click .

Step 3 Click to claim an alarm.

Step 4 View alarm details and handle the alarm.

- 1) Click to view alarm details.
You can only handle the pending and unclaimed alarms.
- 2) Browse through the **Info**, **Live View**, **Snapshot**, **Recording** and **Map** tabs to view details.

Figure 4-73 Handle Alarms



- 3) Select the handling result, such as **Solved**, **Ignore** or **Forward**, and then comment.
- 4) Click **Save**.
 - ◇ Disarm Temporarily: Click **Disarm Temporarily**, set disarm time, and then click **OK**.
 - ◇ Send Email: Click **Send Email**, set email details, and then click **OK**.

4.4.2.2 Alarm Search

Step 1 Log in to the Control Client, click , and then select **Event Center**.

Step 2 Click to open the **Query Alarm** interface.

Step 3 Specify the search conditions, and then click **Search**.

Figure 4-74 Alarms

Alarm Time	Alarm Sort	Alarm Type	Alarm Source	Priority	Remark	Handling user	Status	Operation
2018-08-31 11...	Video Channel	Video Loss	Channel0	Low	111		Pending	
2018-08-31 11...	Video Channel	Video Loss	Channel0	Low	111		Pending	
2018-08-31 11...	Video Channel	Video Loss	Channel0	Low	111		Pending	
2018-08-30 13...	Video Channel	Video Loss	Channel0	Low	111	system	Pending	
2018-08-30 13...	Video Channel	Video Loss	Channel0	Low	111	chenjie	Processed	
2018-08-30 13...	Video Channel	Video Loss	Channel0	Low	111	chenjie	Processed	
2018-08-30 13...	Video Channel	Video Loss	Channel0	Low	111		Pending	
2018-08-30 13...	Video Channel	Video Loss	Channel0	Low	111		Pending	
2018-08-30 13...	Video Channel	Video Loss	Channel0	Low	111		Pending	
2018-08-30 13...	Video Channel	Video Loss	Channel0	Low	111	chenjie	Processed	

Operations

- Select a number from the **Per page** drop-down list to determine the maximum number of alarms displayed on one page.
- Click **Export** to export alarms.
- Click to claim alarm and click to handle alarm.

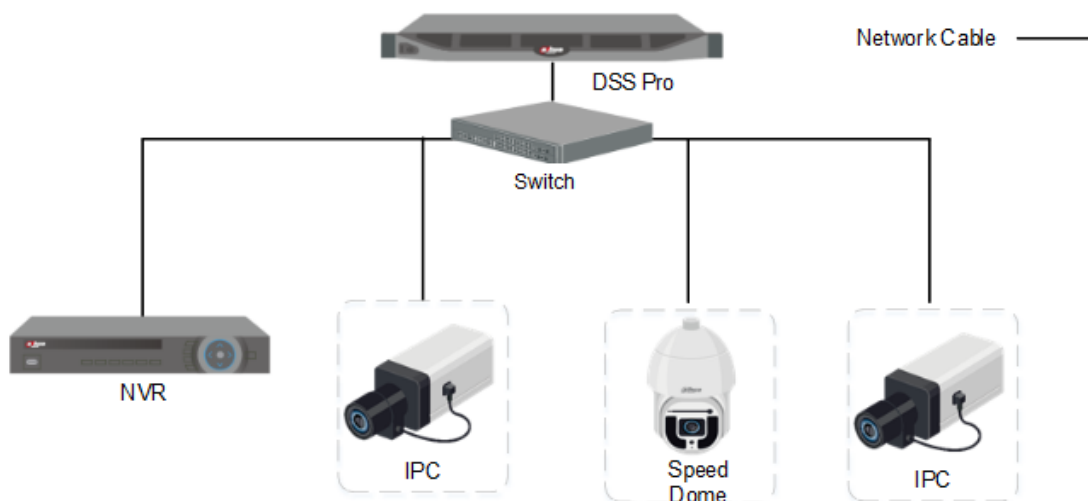
4.5 Intelligent Analysis

IVS includes tripwire analysis, intrusion detection, abandoned object, loitering detection, fast-moving, crowd gathering, missing object and parking detection. The actual camera capability shall prevail. With IVS configured, when a target is detected, the system will trigger an event as you have set and display it on the platform.

4.5.1 Typical Topology

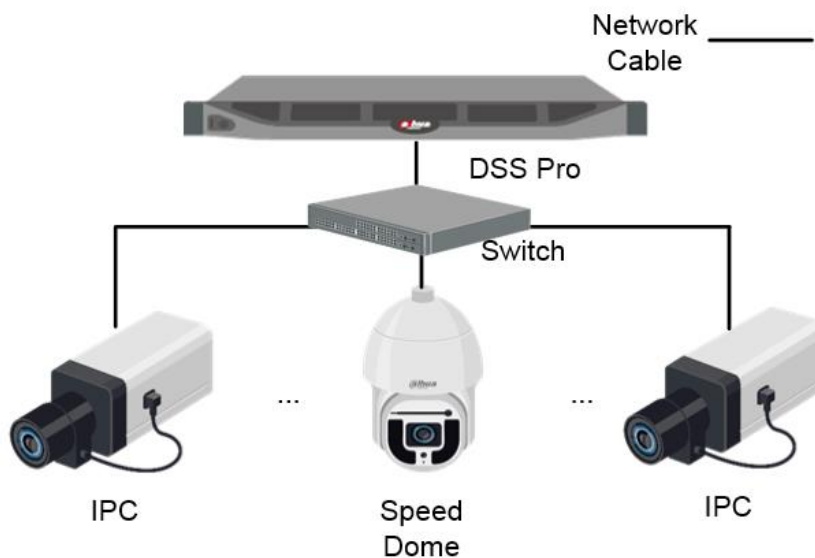
- Intelligent analysis performed by NVR, IVSS and IVS. Take NVR for example.

Figure 4-75 Intelligent analysis topology



- ◇ Cameras collect video stream.
- ◇ NVR, IVSS and IVS device perform intelligent analysis
- ◇ DSS Pro is used to manage all cameras and IVS devices, and receive IVS alarms.
- Intelligent analysis performed by camera

Figure 4-76 Intelligent analysis topology (1)



- ◇ Cameras collect video stream.
- ◇ DSS Pro is used to manage all cameras and IVS devices, and receive IVS alarms.

4.5.2 Configuring Intelligent Analysis



You can only configure IVS settings for cameras directly added to the platform.

See requirements as follows when deploying devices:

- The total target ratio does not exceed 10% of the screen.

- The size of the target in the picture is not less than 10 pixels × 10 pixels, the target size of the abandoned object is not less than 15 pixels × 15 pixels (CIF image); the target height and width is not more than 1/3 of the picture height and the recommended target height is 10% of the picture height.
- The difference between the brightness value of the target and the background is not less than 10 gray levels.
- At least ensure that the target appears continuously for more than 2 seconds in the field of view, the moving distance exceeds the target's own width, and is not less than 15 pixels (CIF image).
- Minimize the complexity of the monitoring and analysis scenario when conditions permit. It is not recommended to use the smart analysis function in scenarios with dense targets and frequent light changes.
- Avoid glass, ground reflection and water surface; avoid branches, shadows and mosquito interference; avoid backlit scenes and direct light.

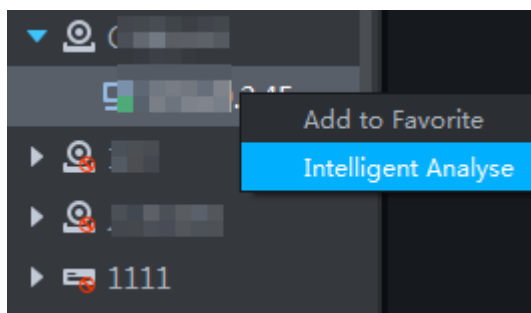
4.5.2.1 Enabling IVS Smart Plan

Enable IVS functions.

Step 1 Go to the IVS configuration interface.

- 1) Log in to the Control Client, select **Live View**.
- 2) Right-click an IPC channel on the **Live View** interface, and then select **Intelligent Analyze**.

Figure 4-77 Go to intelligent analysis interface



Step 2 Enable IVS smart plan.



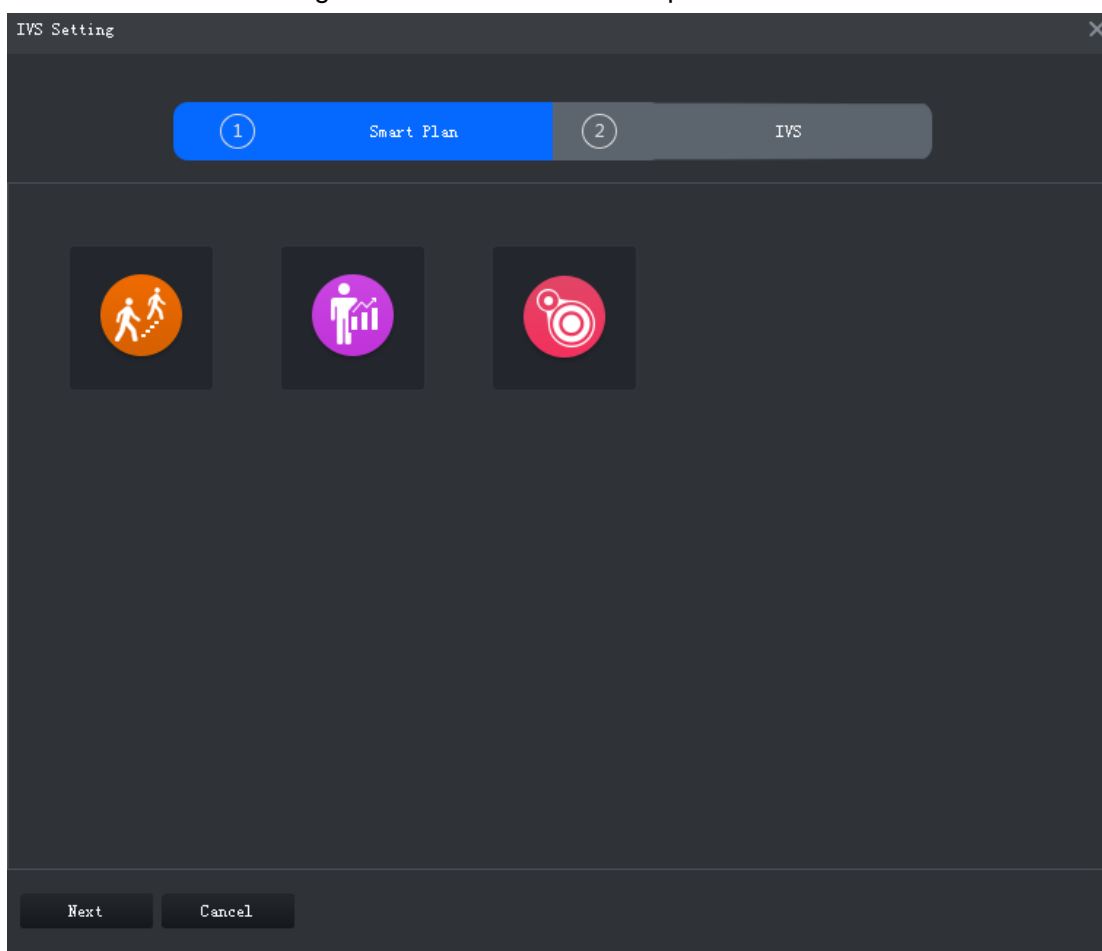
- 1) Click  on the smart plan interface to enable IVS smart plan.
When the icon is displayed in the white frame, it means the smart plan is selected.
If another smart plan has been selected, click that smart plan icon to deselect it and then click  to select IVS.

Figure 4-78 Enable IVS smart plan



Step 3 Click **Next** to go to the **IVS Setting** interface.

4.5.2.2 Calibrating Depth of Field


After setting one horizontal gauge and three vertical gauge and the actual geographical distances of each gauge, the system can estimate the internal parameters (internal geometrical features and optical properties) and external parameters (the network camera position and direction on the actual environment) of network camera, so as to work out the relation between the two-dimensional image and three dimensional objects in the current surveillance environment.



Calibrate depth of field for fast-moving detection. Skip this section if you do not need this function.

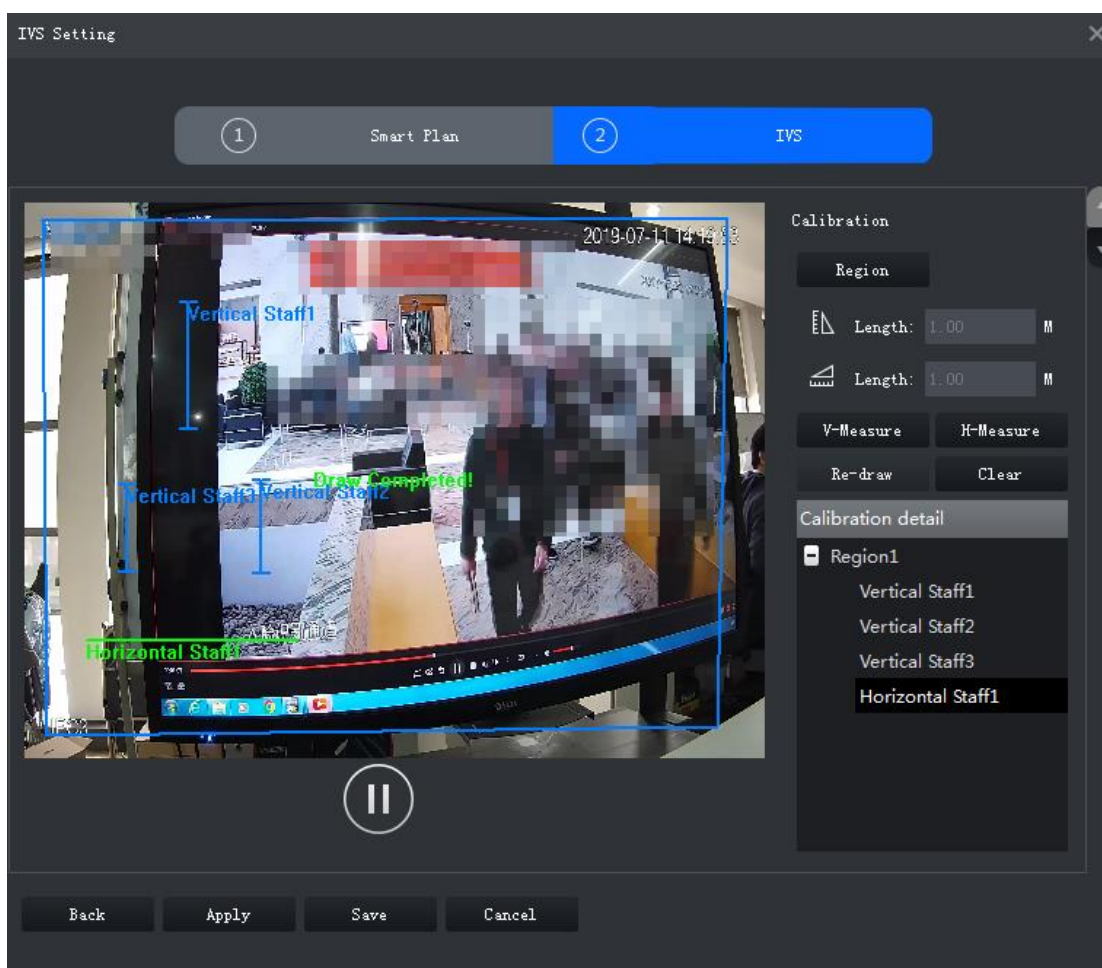
Step 1 After selecting the smart plan in the **Smart Plan** interface, click **Next**.

Step 2 Click **Region** and draw calibration zone on the video. Right-click to finish.

Step 3 Set length value of the vertical gauge. Click  and then draw a vertical gauge in the calibration area. Click to finish.

Draw another three vertical gauges in the calibration area.

Figure 4-79 Calibrating depth of field



Step 4 Set length value of horizontal gauge. Click and then draw a horizontal gauge in the calibration area. Click to finish.



- To modify the gauge, you can select it and click **Re-draw**. You can also select the calibration and click **Re-draw** to draw new calibration areas and gauges.
- To delete a gauge, select it and click **Delete**. To delete a calibration area and the gauges in it, select the area and click **Delete**.

Step 5 Click **Apply** to save.

Step 6 (Optional) Vertical/horizontal measuring

Do the following steps to measure distance.

- Click **V-Measure** and draw vertical line in the calibration area. The measuring result will be displayed.
- Click **H-Measure** and draw horizontal line in the calibration area. The measuring result will be displayed.

4.5.2.3 Configuring Detection Region

Configure the detection zone of IVS.


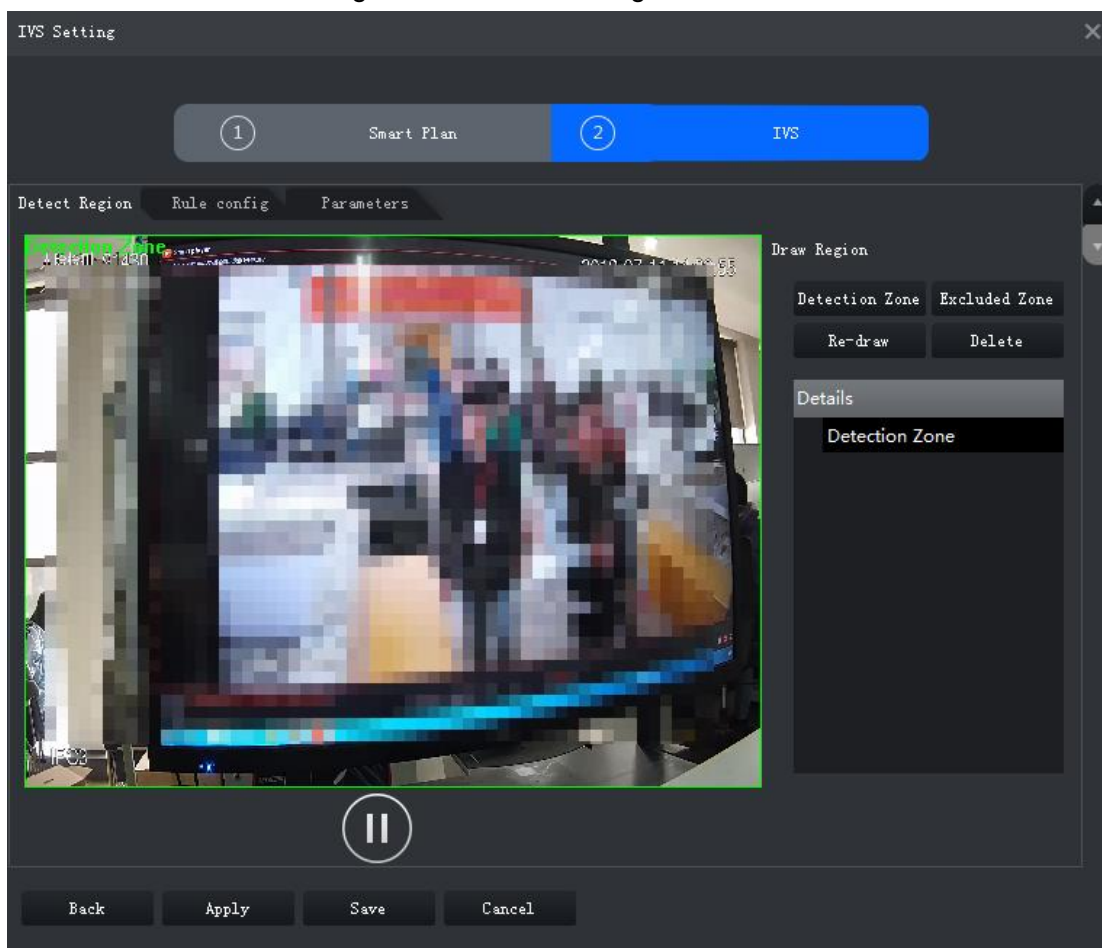
- Step 1** Click .
- Step 2** Click **Detection Zone**, and then draw the frame of the detection zone on the video and right-click to finish.
- Step 3** Click **Excluded Zone**, and then draw the frame of the zone on the video and right-click to finish.

Figure 4-80 Detection region



4.5.2.4 Configuring IVS Rule

Configure IVS detections such as fence-crossing, tripwire, intrusion, abandoned object, loitering detection, fast-moving, crowd gathering, missing object and parking detection.

Functions	Description	Applicable Scenarios
Fence-crossing	Alarm is triggered when a target is crossing the pre-defined fence.	Roads, airports and other areas with restricted zones.
Tripwire	Alarm is triggered when a target is crossing the pre-defined tripwire.	Restricted zone borders

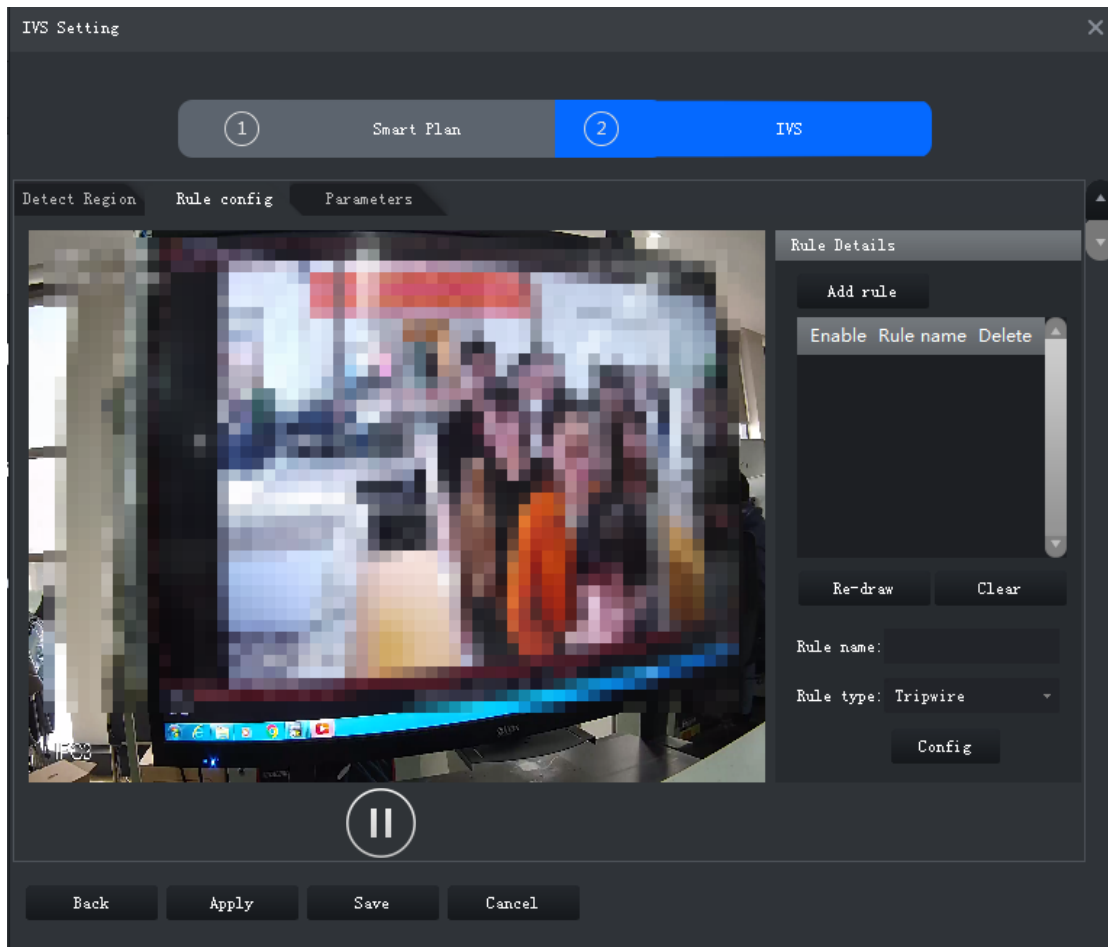
Functions	Description	Applicable Scenarios
Intrusion	Alarm is triggered when a target is entering, leaving, or appears in the detection area.	Restricted zone borders
Abandoned Object	Alarm is triggered when an object is left in the detection area and the existence time is longer than the threshold.	Places where the target is sparse and has no obvious and frequent light changes. The detection area is required to be as simple as possible.
Missing Object	Alarm is triggered when an object is removed from the detection area and not put back after the pre-defined time period.	
Fast-moving	Alarm is triggered when the moving speed of a target exceeds the threshold.	Places with low target density and no obvious blocking. The camera should be installed right above the monitoring area, and the light direction is as vertical as possible with the direction of motion.
Parking Detection	Alarm is triggered when a target remains still within a time period longer than the pre-defined time duration.	Road monitoring and traffic management.
People Gathering	Alarm is triggered when people gathering is detected or people density is larger than the threshold.	Long or medium distance monitoring. For example, outdoor squares, government gates, and station entrances and exits.
Loitering	Alarm is triggered when a target keeps loitering in a time period longer than the threshold. Alarm will be triggered again if the target stays in the detection area after the first alarm.	Enterprise zones, halls and more.

4.5.2.4.1 Tripwire

When a target is detected crossing a line, an alarm will be triggered immediately.


Step 1 On the **IVS Setting** interface, click **Rule config**.

Figure 4-81 Rule configuration interface



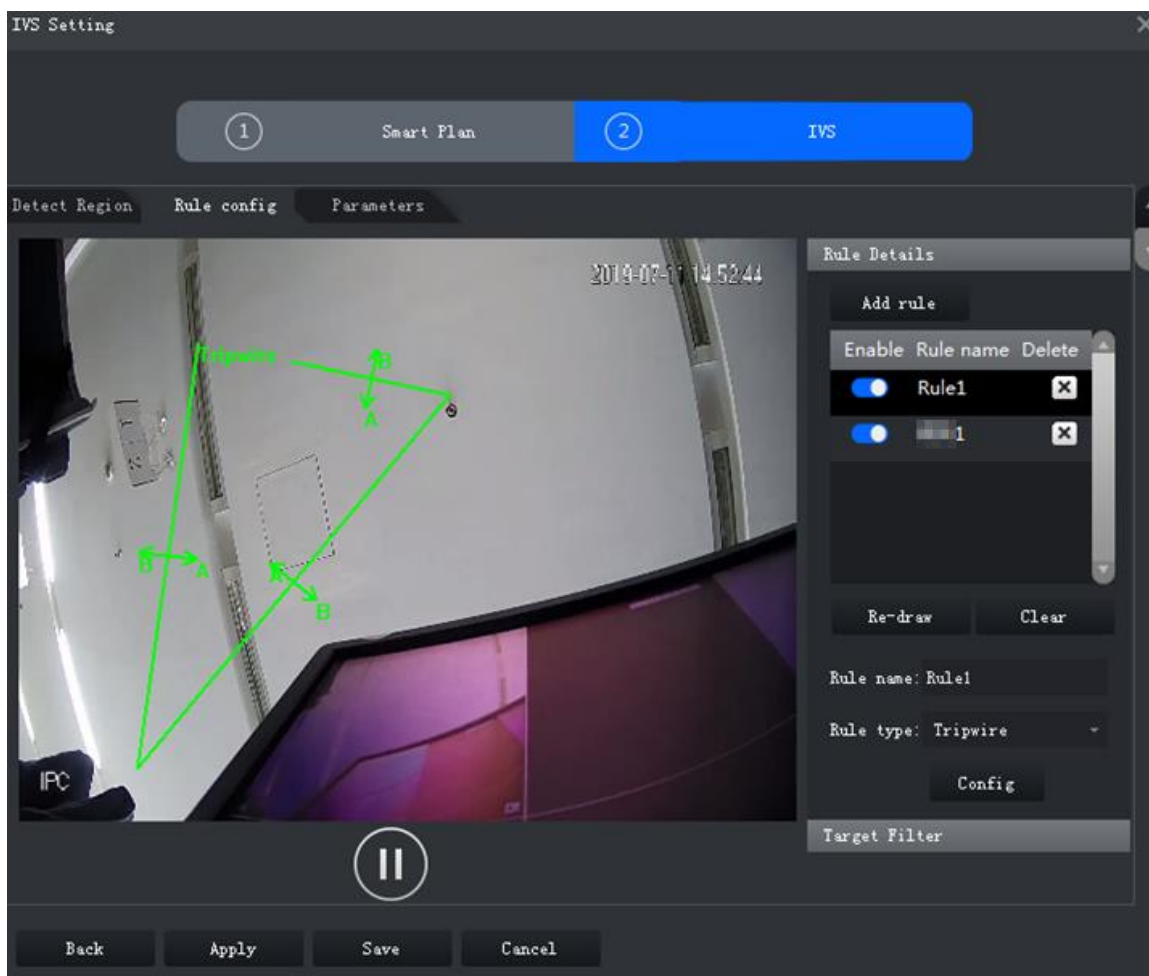
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

- 1) Enable rule.  indicates rule is enabled.
- 2) Modify rule name.
- 3) Select **Tripwire** in the drop-down list of **Rule type**.

Step 4 Draw a line on the video and right-click to finish.

Figure 4-82 Tripwire



Step 5 Set parameters, arming schedule and alarm linkage.

- 1) Click **Config** and set parameters.

Figure 4-83 Set parameters

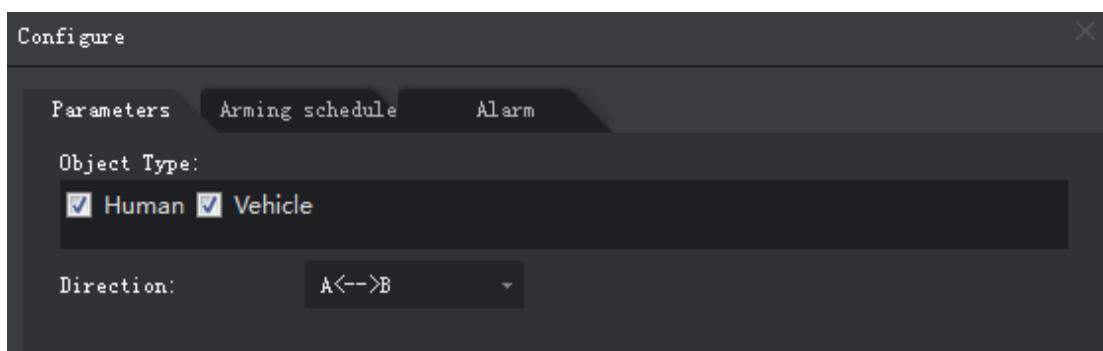


Table 4-29 Parameters

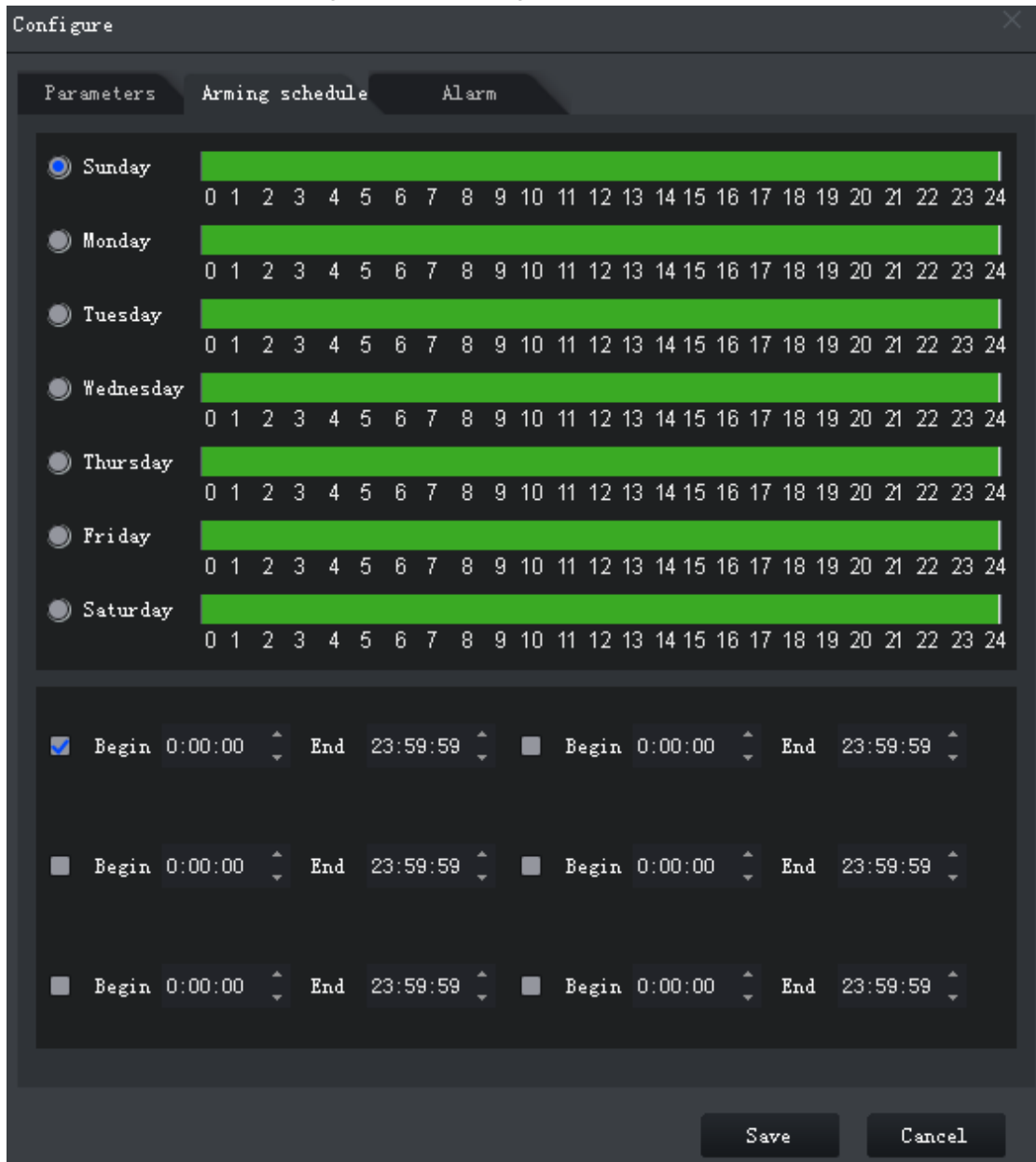
Parameter	Description
Object Type	Only human or vehicle can trigger alarm.
Direction	When the target is moving in the rule direction, it is an intrusion. Directions include A→B, B→A and A↔B.

- 2) Click **Arming schedule**, select day and hours and then set the start time and end time.



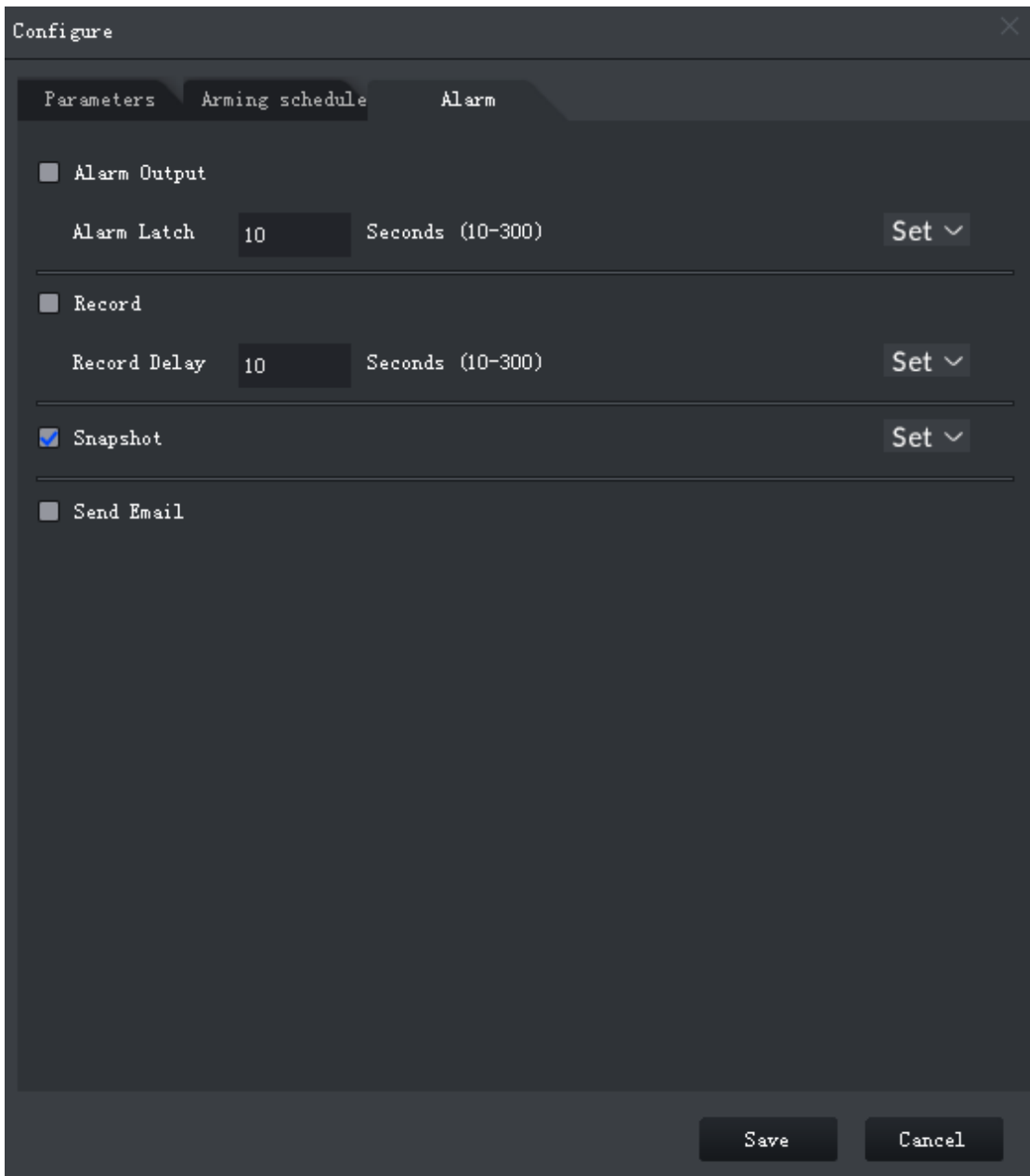
The default arming schedule is 24 hours per day.

Figure 4-84 Arming schedule



3) Click **Alarm**, and then set linkage actions.

Figure 4-85 Alarm linkage



Configure

Parameters Arming schedule Alarm

Alarm Output

Alarm Latch 10 Seconds (10-300) Set ▾

Record

Record Delay 10 Seconds (10-300) Set ▾

Snapshot Set ▾




Send Email

Save Cancel

Table 4-30 Parameters

Parameter	Description
Alarm Output	Connect alarm output devices to the alarm output interfaces. When an alarm is triggered, the system will send the alarm to the alarm output device.
Alarm Latch	The alarm output action will delay stopping after the alarm event ends.

Click **Set** next to **Alarm Latch** and select an alarm output channel.

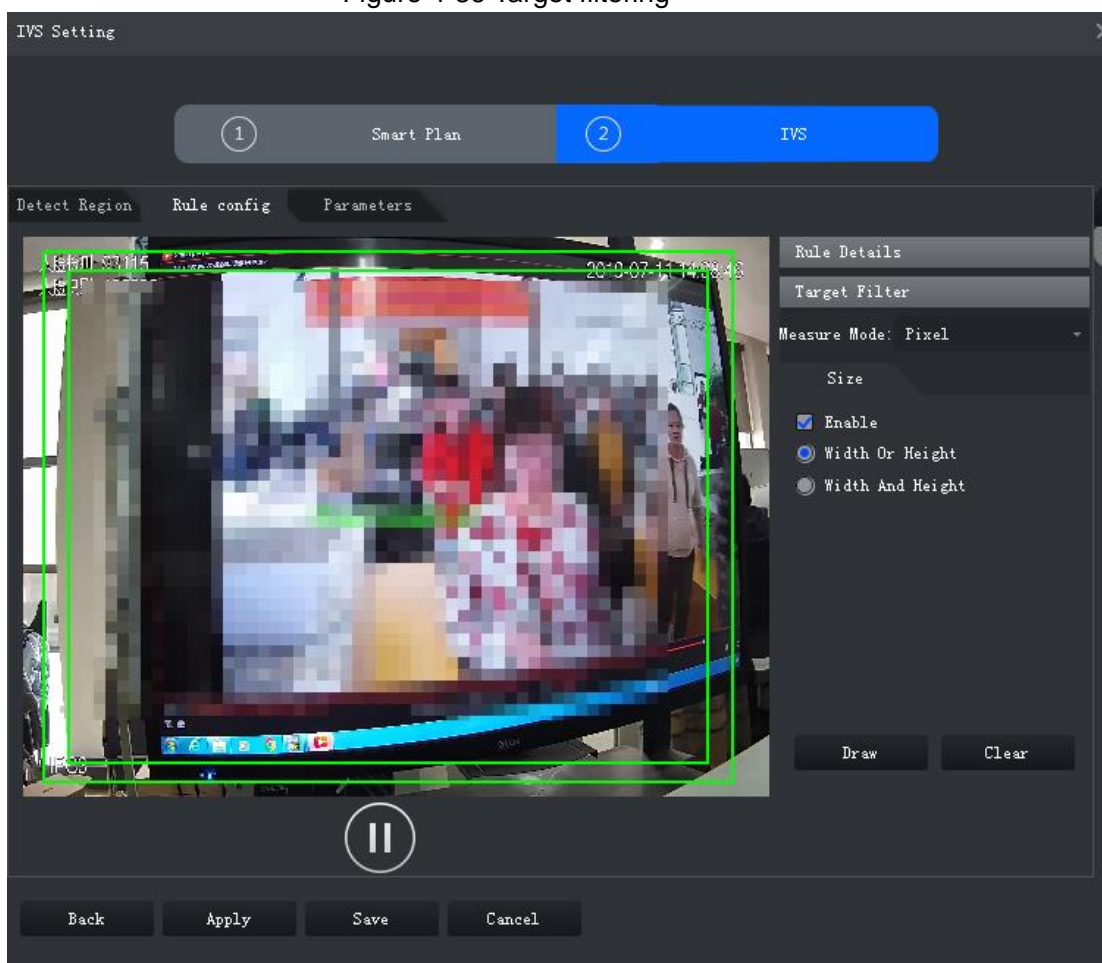
Parameter	Description	
Record	When an alarm happens, it will trigger video recording immediately.  It requires the device to have recording schedules already. See device manual for detailed instruction.	Click Set next to Record and select an alarm output channel.
Record Delay	Video recording delays stopping for a while after the alarm event ends.	
snapshot	The system will take snapshots automatically when an alarm happens.  It requires the device to have snapshot schedules already. See device manual for detailed instruction.	Click Set next to Snapshot to select the snapshot channel.
Send Email	The system will send an email to the related mail address when an alarm happens.  It requires the device to have email configured already. See device manual for detailed instruction.	–

4) Click **Save**.

Step 6 Draw target-filtering frame.

The filtering frame is used to filter targets that are too big or too small. When the target size is within the preset value, it can trigger alarm.

Figure 4-86 Target filtering



- 1) Click **Target Filter**.
- 2) Select **Enable**.
- 3) Select a filtering method, **Width or Height** or **Width and Height**. Select filtering frame and drag the frame corners to adjust the size.



Select filtering frame, and click **Clear** to delete it.

Step 7 Click **Apply**.


4.5.2.4.2 Intrusion

When a target is detected entering or leaving an area, an alarm will be triggered.

Step 1 On the **IVS Setting** interface, click **Rule config**.

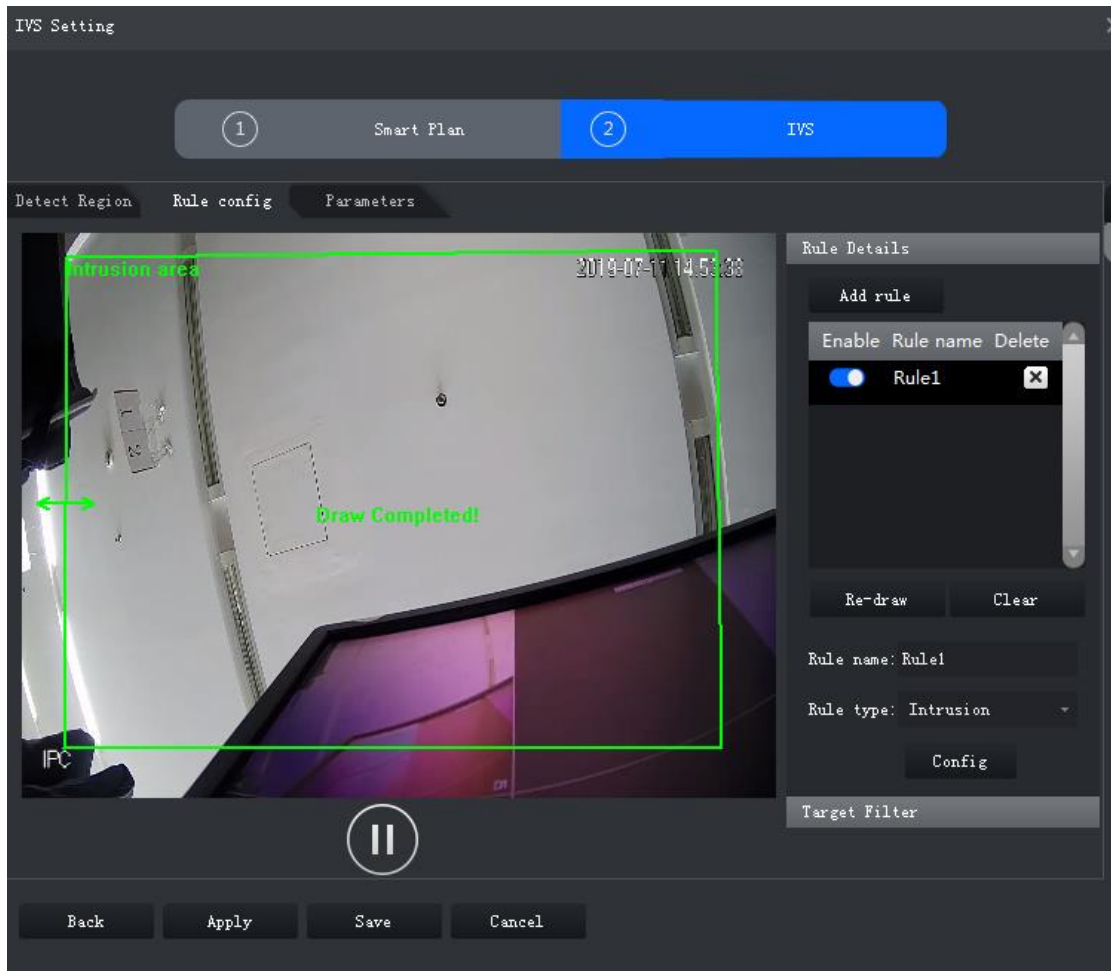
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

- 1) Enable rule.  indicates rule is enabled.
- 2) Modify rule name.
- 3) Select **Intrusion** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish.

Figure 4-87 Intrusion



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.5.2.4.1 Tripwire."

Figure 4-88 Set parameters



Table 4-31 Parameters

Parameter	Description
Object Type	Only human or vehicle can trigger alarm.
Action List	Appear and cross

Parameter	Description
Direction	When a crossing-zone action is selected, Direction setting will be effective. Direction includes entering zone, leaving zone and two-way.

Step 6 Click **Apply**.


4.5.2.4.3 Abandoned Object

When an object appears and stays in the detection area for a time period, system will trigger an alarm.

Step 1 On the **IVS Setting** interface, click **Rule config**.

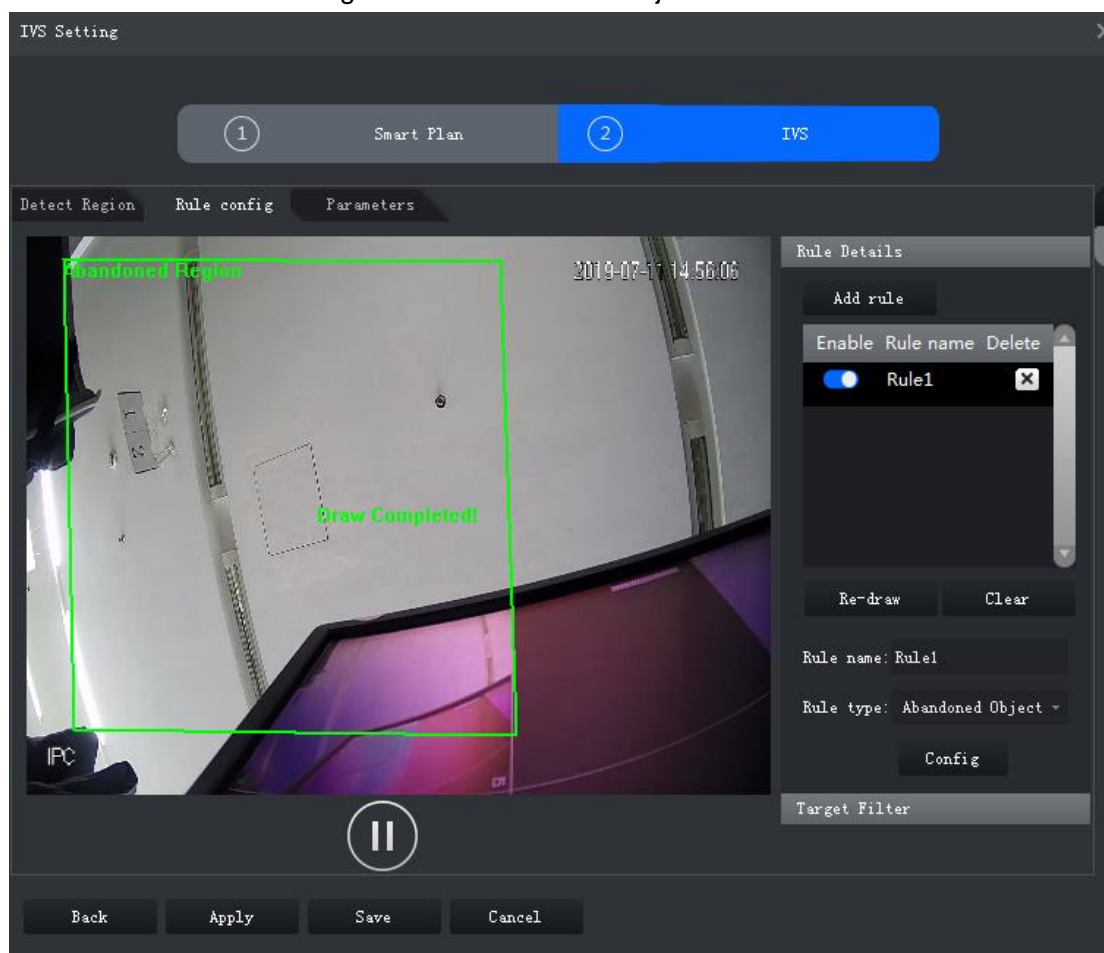
Step 2 Click Add rule.

Step 3 Enable rule and modify the name and type.

- 1) Enable rule.  indicates rule is enabled.
- 2) Modify Rule name.
- 3) Select **Abandoned Object** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish.

Figure 4-89 Abandoned Object



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.5.2.4.1 Tripwire."

Figure 4-90 Set parameters

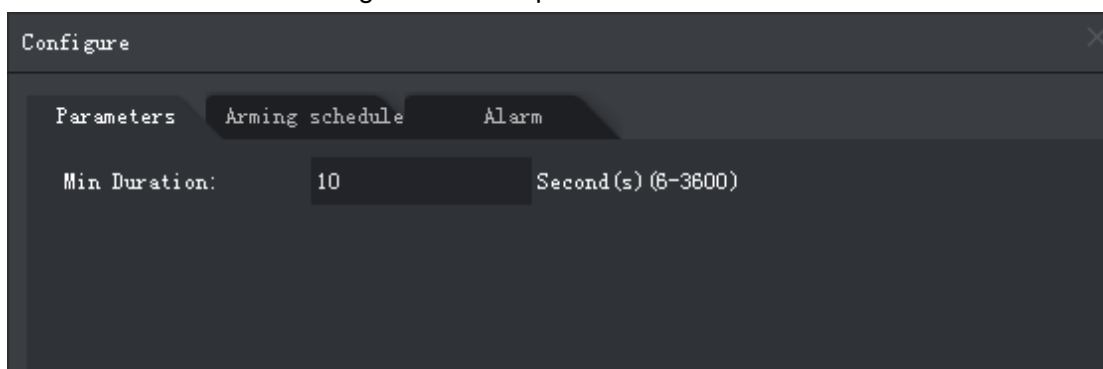


Table 4-32 Parameters

Parameter	Description
Min Duration	The minimum time period between appearing and alarm triggering.

Step 6 Click **Apply**.

4.5.2.4.4 Fast-Moving

When a target appears and its moving speed is or exceeds the preset value for the preset time period, system will trigger an alarm.




To ensure the accuracy of fast-moving detection, Make sure that you have completed the calibration configuration. See "4.5.2.2 Calibrating Depth of Field for details."

Step 1 On the **IVS Setting** interface, click **Rule config**.

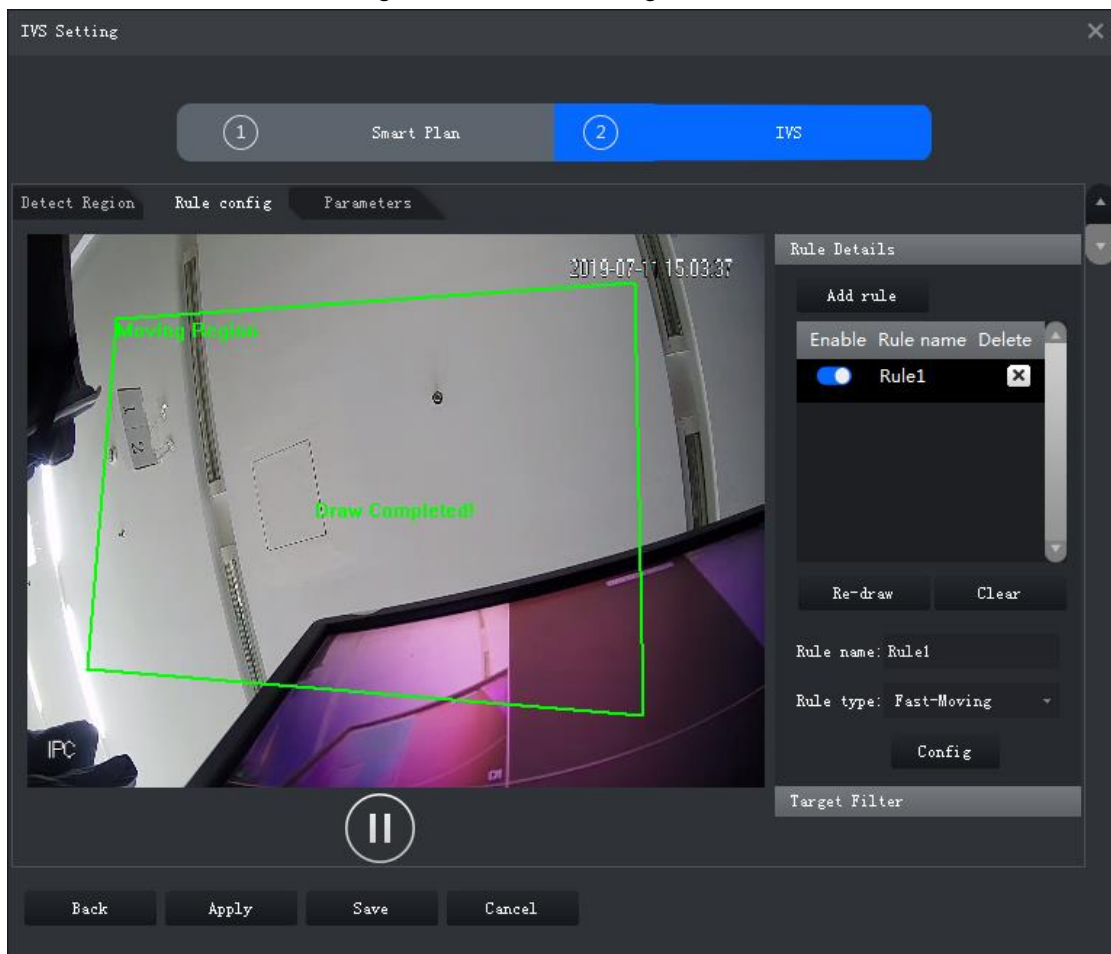
Step 2 Click Add rule.

Step 3 Enable rule and modify the name and type.

- 1) Enable rule.  indicates rule is enabled.
- 2) Modify rule name.
- 3) Select **Fast-Moving** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish.

Figure 4-91 Fast-moving



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.5.2.4.1 Tripwire."

Figure 4-92 Set parameters

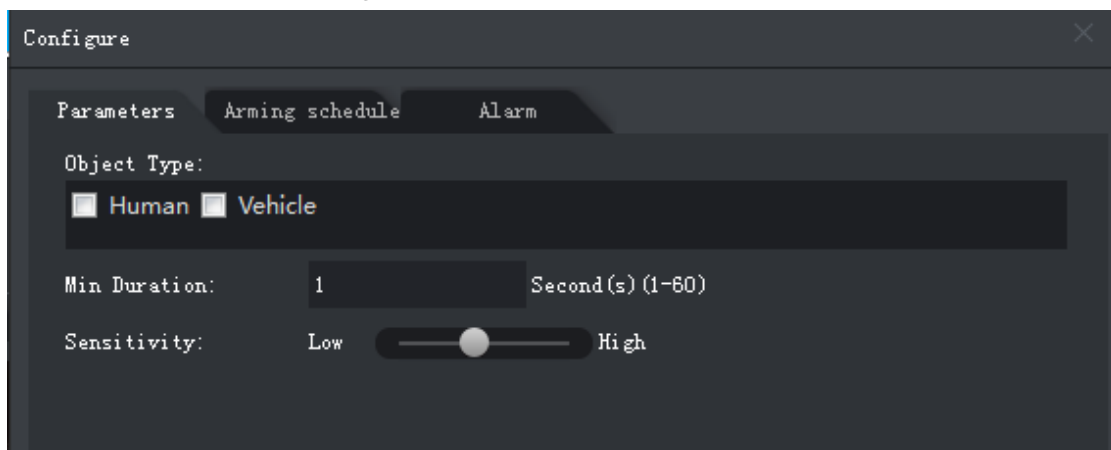


Table 4-33 Parameters

Parameter	Description
Object Type	Only human or vehicle can trigger alarm.
Min Duration	The minimum duration of fast-moving in the detection zone.
Sensitivity	It is recommended to keep the default value.

Step 6 Click **Apply**.


4.5.2.4.5 Parking Detection

When a vehicle is detected parking in an area, an alarm will be triggered.

Step 1 On the **IVS Setting** interface, click **Rule config**.

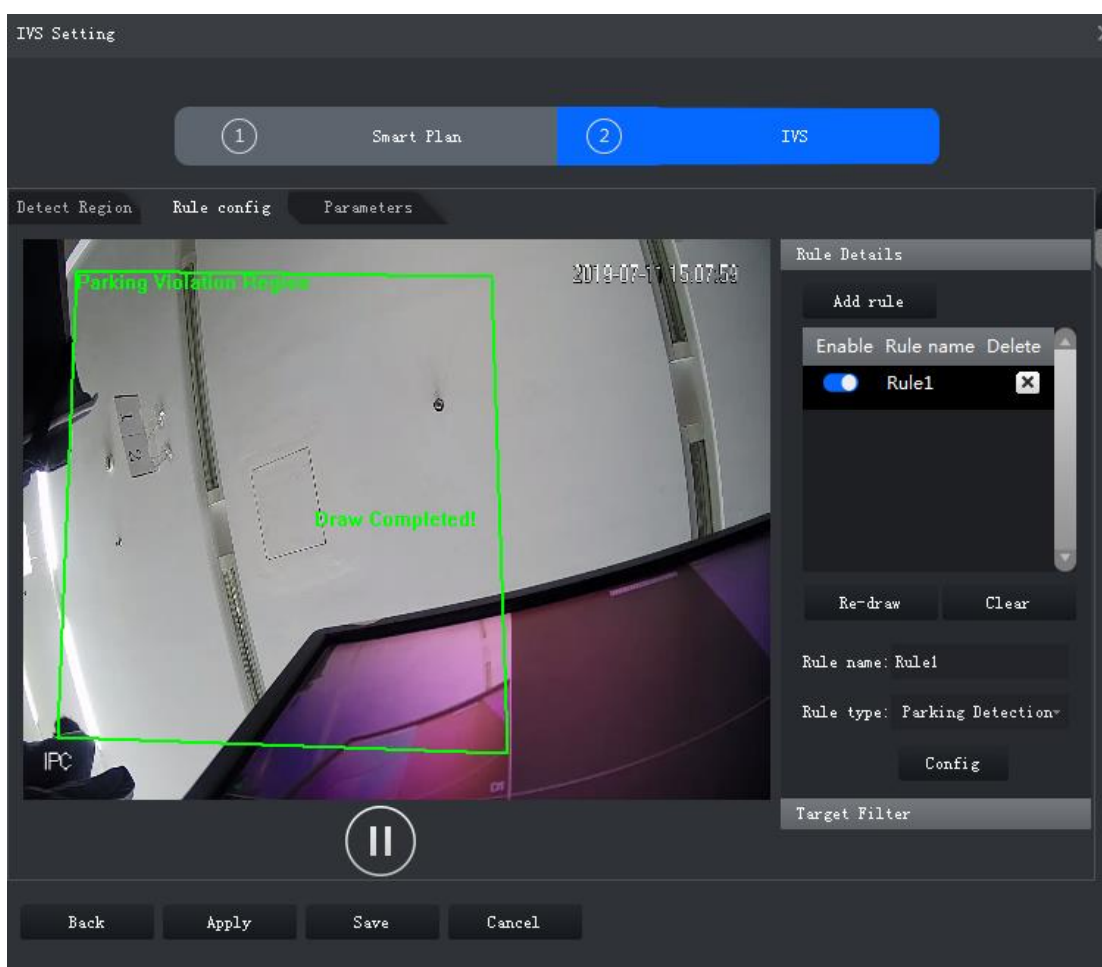
Step 2 Click Add rule.

Step 3 Enable rule and modify the name and type.

- 1) Enable rule.  indicates rule is enabled.
- 2) Modify rule name.
- 3) Select **Parking Detection** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish.

Figure 4-93 Parking detection



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.5.2.4.1 Tripwire."

Figure 4-94 Set parameters

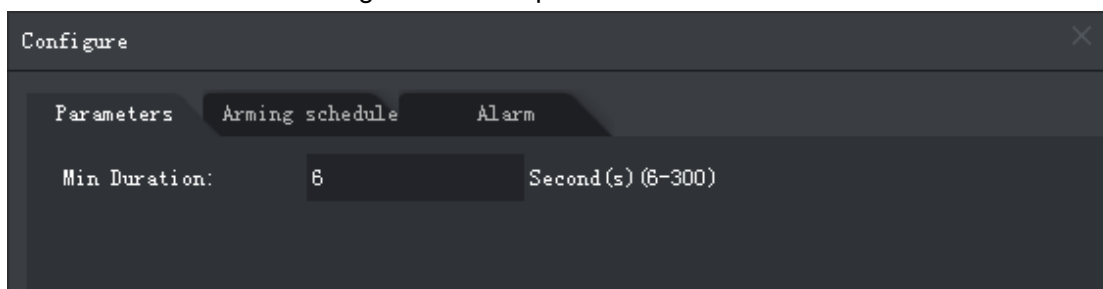


Table 4-34 Parameters

Parameter	Description
Min Duration	The minimum time duration from parking to alarm triggering.

Step 6 Click **Apply**.

4.5.2.4.6 Crowd Gathering

When the people crowd size in the detection zone exceeds the preset value, system will trigger an alarm.

Step 1 On the **IVS Setting** interface, click **Rule config**.

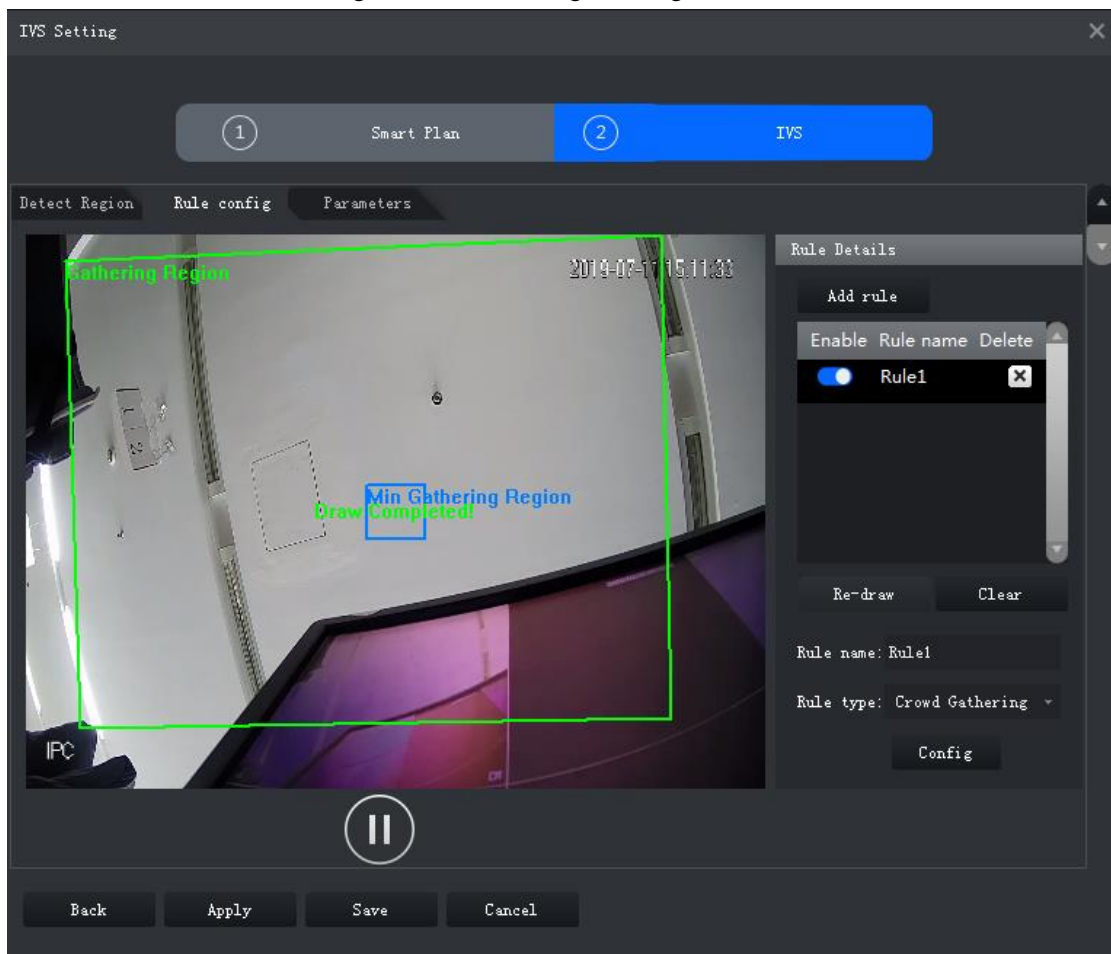
Step 2 Click Add rule.

Step 3 Enable rule and modify the name and type.

- 1) Enable rule. indicates rule is enabled.
- 2) Modify rule name.
- 3) Select **Crowd Gathering** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish. Click the **Min Gathering Region** and drag the zone corners to adjust the size.

Figure 4-95 Crowd gathering



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.5.2.4.1 Tripwire."

Figure 4-96 Set parameters

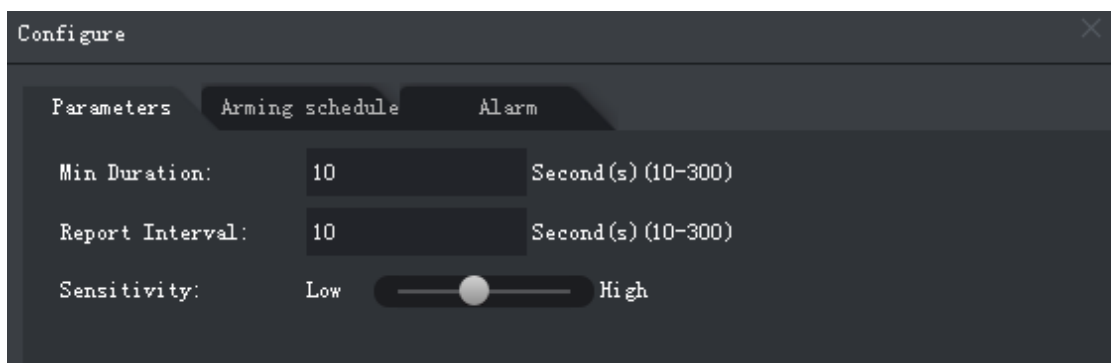


Table 4-35 Parameters

Parameter	Description
Min Duration	The minimum duration from the time crowd gathering being detected to alarm triggering
Report Interval	If the event still exists after the first alarm, system will trigger more alarms by the preset alarm interval.
Sensitivity	It is recommended to keep the default value.

Step 6 Click **Apply**.


4.5.2.4.7 Missing Object

If an object has been moved out of the detection zone and not put back anymore for a certain time period, system will trigger an alarm.

Step 1 On the **IVS Setting** interface, click **Rule config**.

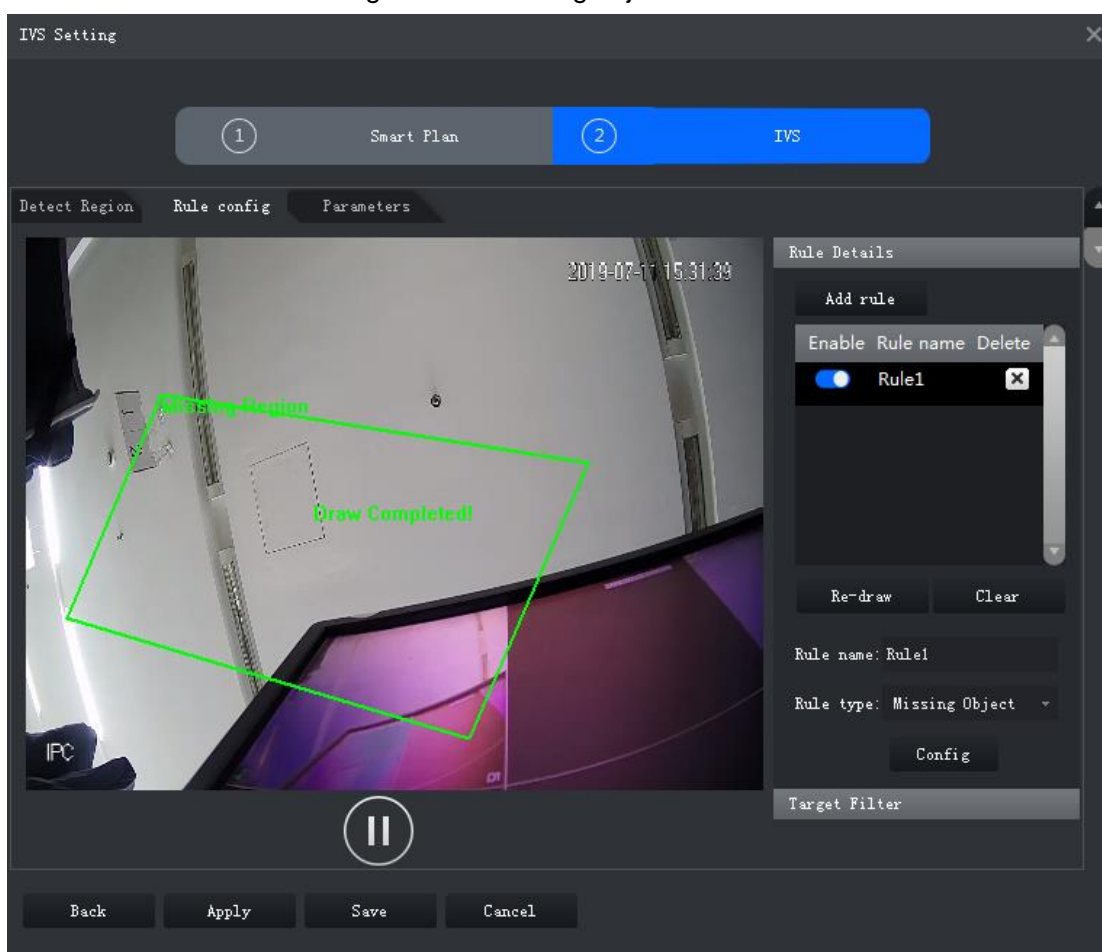
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

- 1) Enable rule.  indicates rule is enabled.
- 2) Modify rule name.
- 3) Select **Missing Object** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish.

Figure 4-97 Missing object



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.5.2.4.1 Tripwire."

Figure 4-98 Set parameters

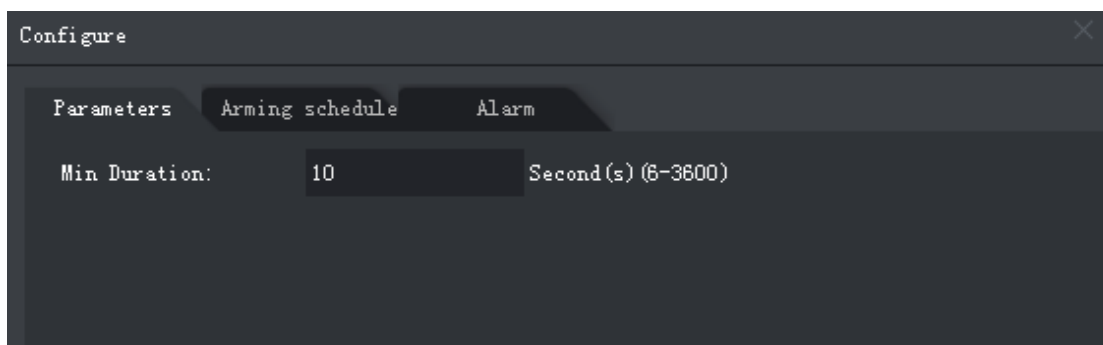


Table 4-36 Parameters

Parameter	Description
Min Duration	The minimum time duration from object disappearing to alarm triggering.

Step 6 Click **Apply**.


4.5.2.4.8 Loitering Detection

When a target stays in the detection zone after appearing for a certain time period, an alarm will be triggered.

Step 1 On the **IVS Setting** interface, click **Rule config**.

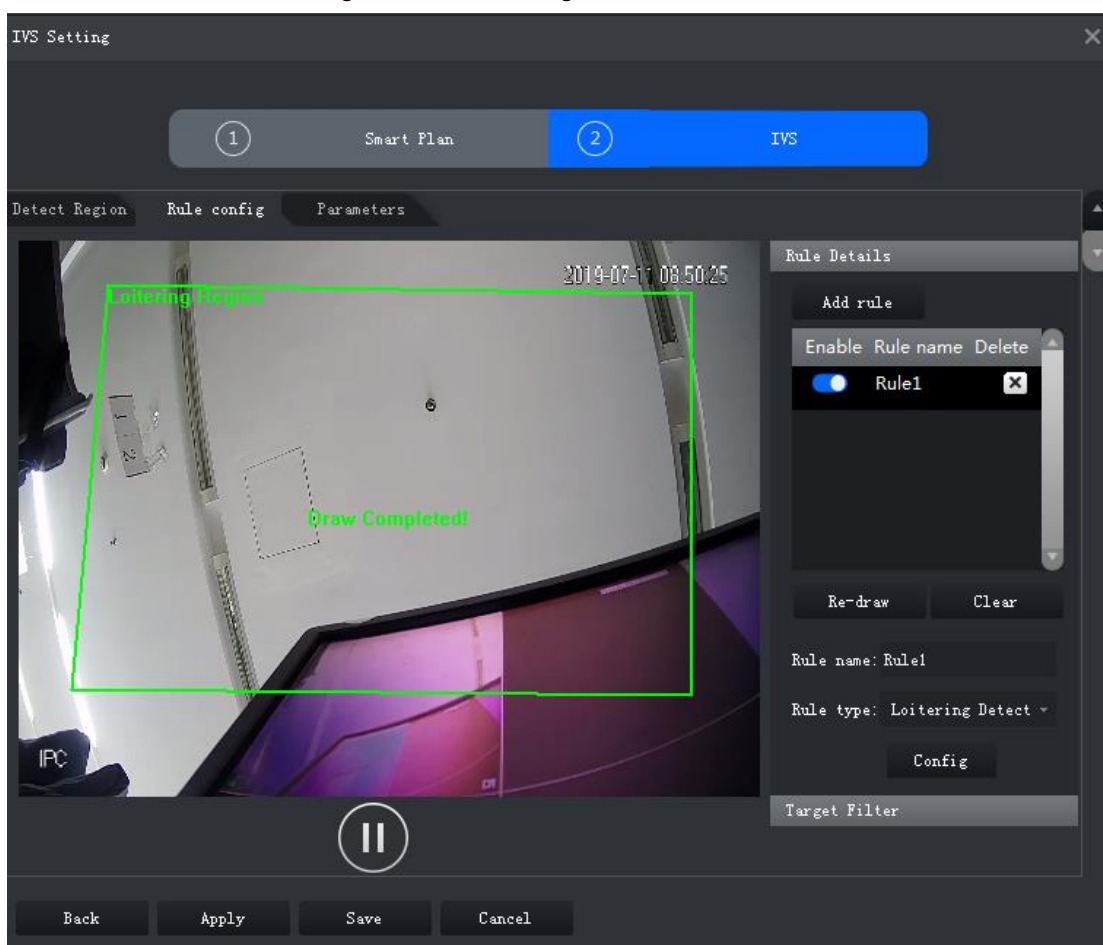
Step 2 Click Add rule.

Step 3 Enable rule and modify the name and type.

- 1) Enable rule.  indicates rule is enabled.
- 2) Modify rule name.
- 3) Select **Loitering Detect** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish.

Figure 4-99 Loitering detection



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.5.2.4.1 Tripwire."

Figure 4-100 Set parameters

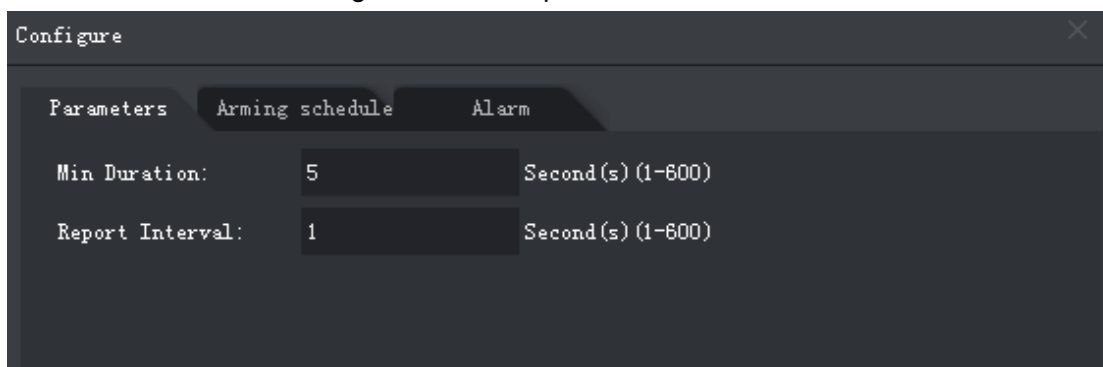


Table 4-37 Parameters

Parameter	Description
Min Duration	The minimum time duration from target appearing to alarm triggering.
Report Interval	If the event still exists after the first alarm, system will trigger more alarms by the preset alarm interval.

Step 6 Click **Apply**.

4.5.2.5 Setting Parameters

Set common parameters for the IVS, including disturbance filter and sensitivity.

Step 1 Click **Parameters** after configuring rules in the **Rule config** interface.

Step 2 Set parameters.

Figure 4-101 Parameters

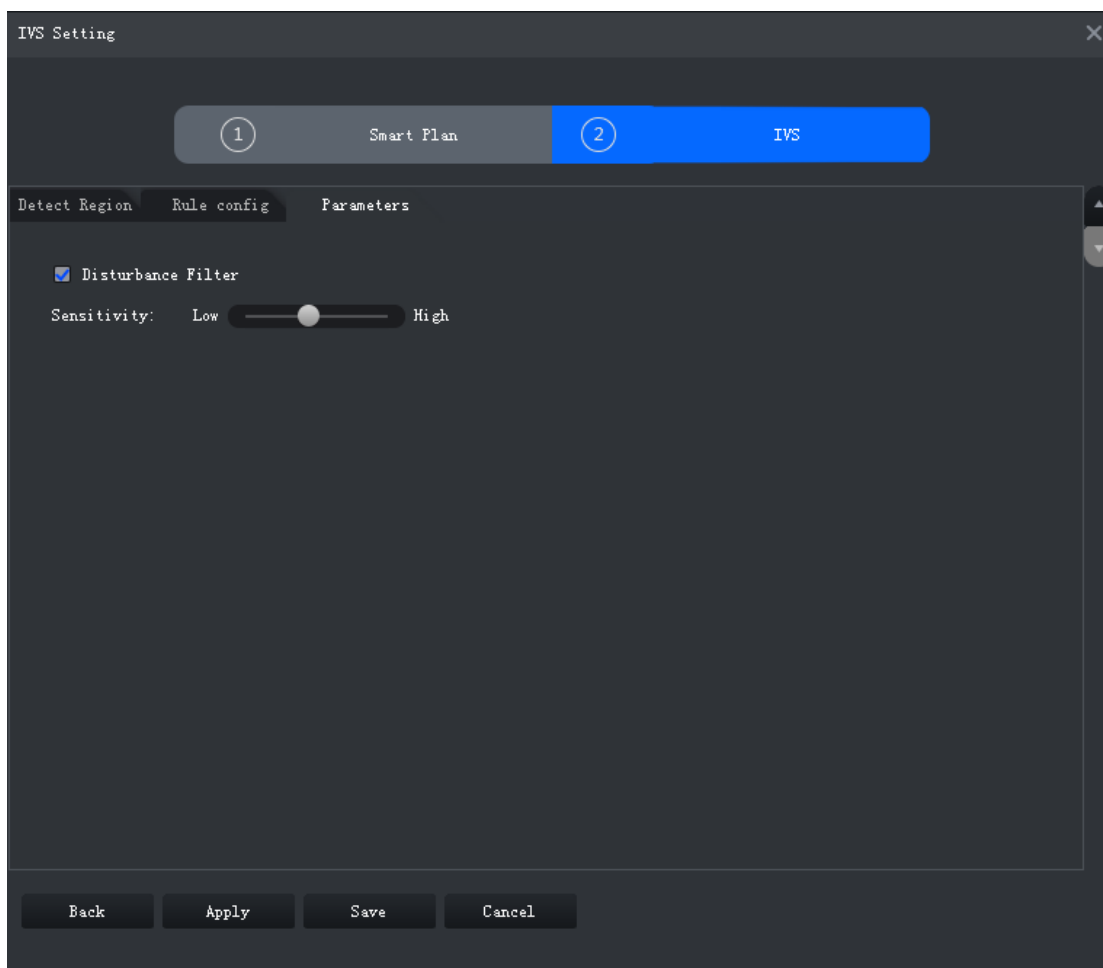


Table 4-38 Parameters

Parameter	Description
Disturbance Filter	Filter false targets including waving plants and water waves. This function may cause target omissions as some parts of a true target may be judged as false factors.
Sensitivity	Control detection sensitivity. The smaller the value is, the lower the false detection rate will be and the higher omission rate will happen. The bigger the value is, the higher false detection rate will be and the lower the omission rate will happen.

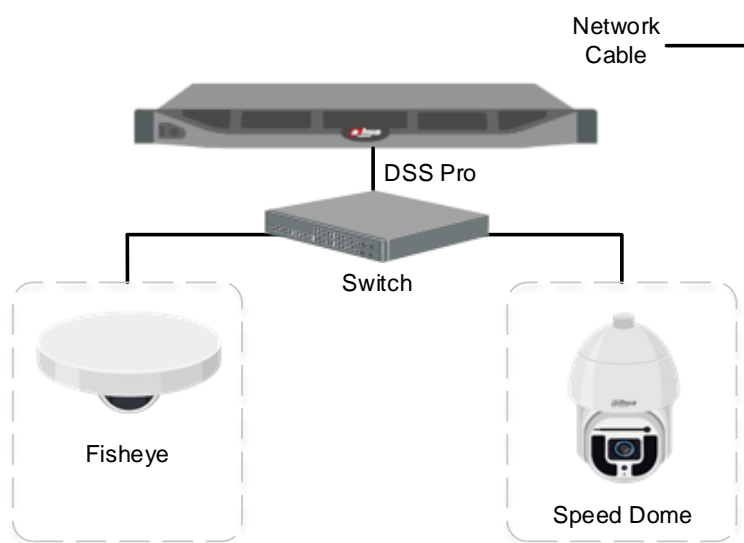
Step 3 Click **Save**.

4.6 Fisheye-PTZ Smart Track

Link a PTZ camera to a fisheye camera so that when the fisheye camera detects a target, the PTZ camera automatically rotates to it and track.

4.6.1 Typical Topology

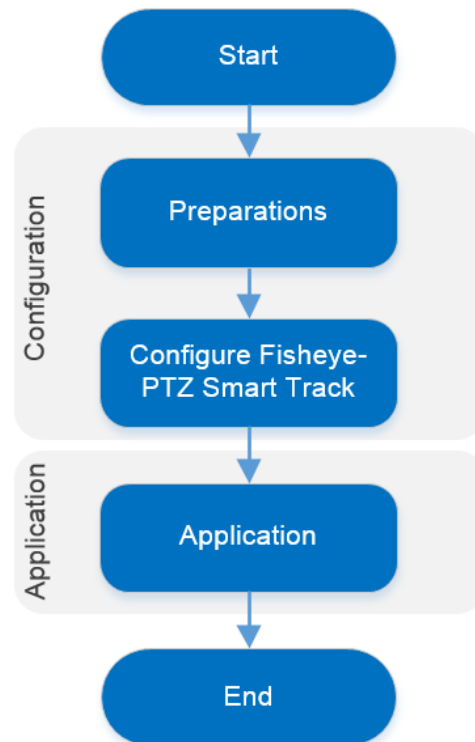
Figure 4-102 Fisheye and PTZ smart track topology



- Fisheye camera is used to monitor the whole view. PTZ camera is used to track the target and capture details.
- DSS Pro is used to manage all cameras, configure smart track, and view live video. It supports PTZ operations, snapshot and video recording.

4.6.2 Business Flow

Figure 4-103 Fisheye-PTZ smart track



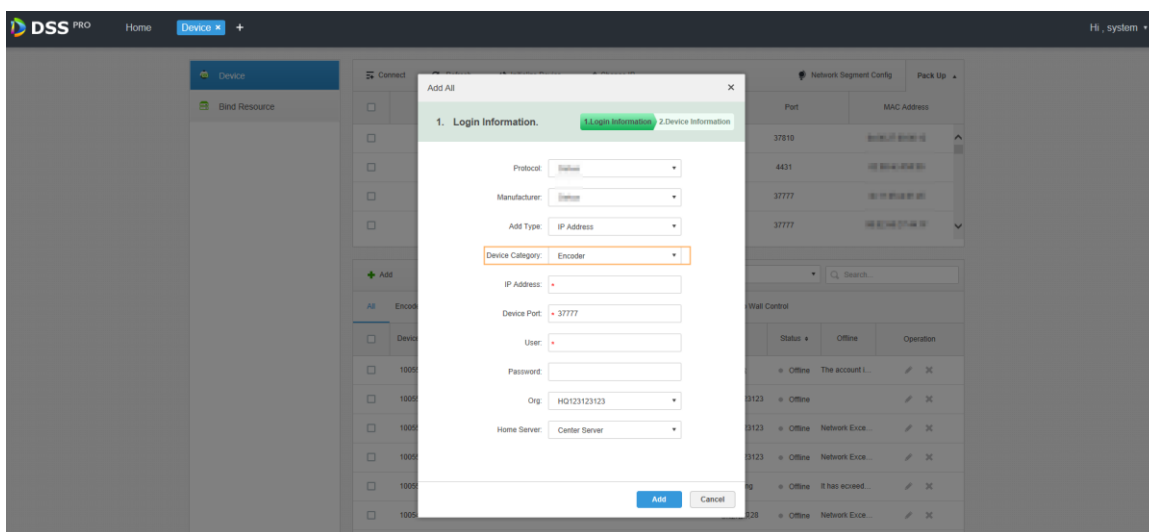
4.6.3 Configuring Fisheye-PTZ Smart Track

4.6.3.1 Preparations

Make sure that the following preparations have been made:

- Fisheye camera and PTZ camera are well deployed. To deploy, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding cameras, select **Encoder** for **Device Category**. See Figure 4-104.

Figure 4-104 Set device category




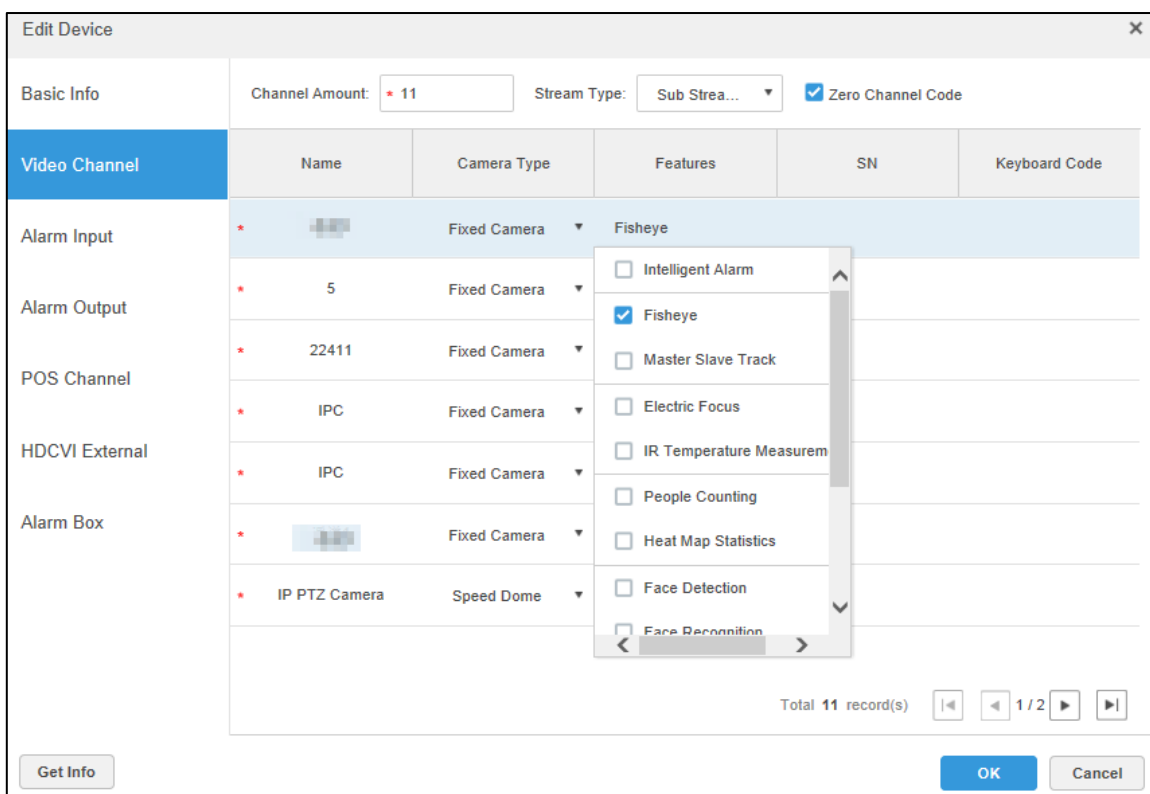
- ◇ On the **Device** interface of Web Manager, after the fisheye camera is added, click  of it, and select **Fisheye** in the **Features** drop-down list.

Figure 4-105 Set fisheye camera features



4.6.3.2 Configuring Fisheye-PTZ Smart Track

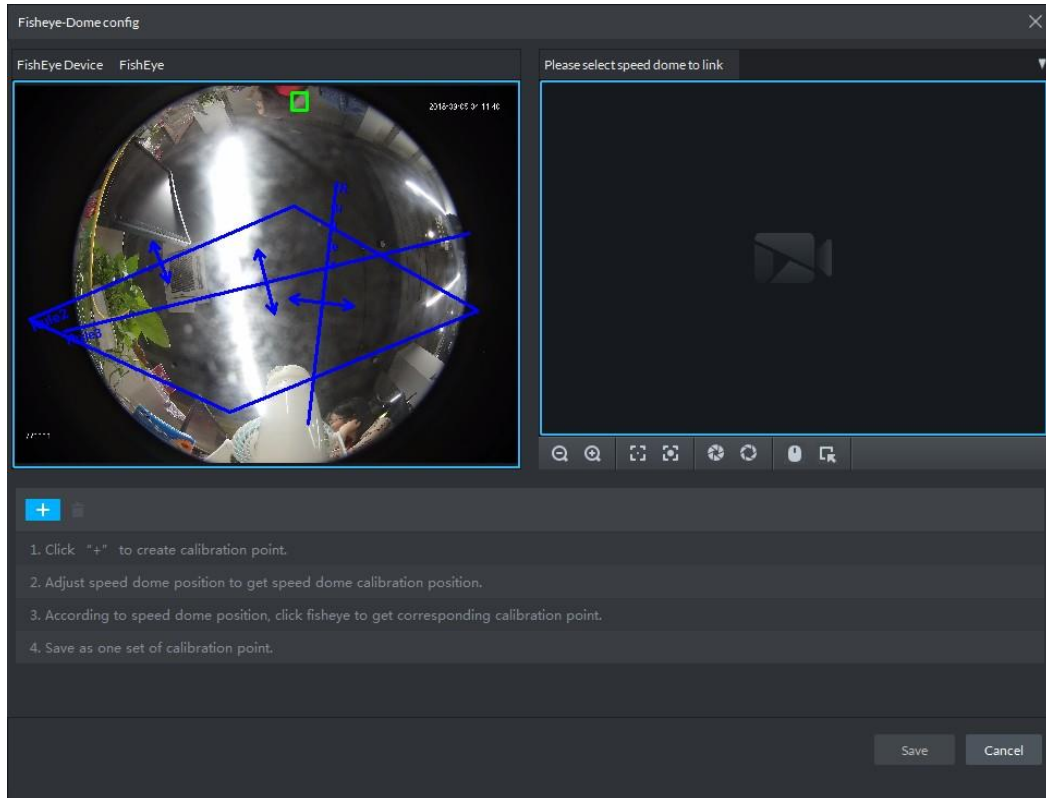
Step 1 On the homepage of Control Client, select **Live View**.

Step 2 From the device tree on the left, right-click on a fisheye camera, and then select **Smart Track**.



If it is not the first time to use the smart track function, select the fisheye camera, right-click, and then select **Smart Track Modify**.

Figure 4-106 Set smart track rules (1)



Step 3 Click  after the Select linkage PTZ camera and then select a PTZ camera.

Step 4 Click  and then move the  of the fisheye on the right to select a position.


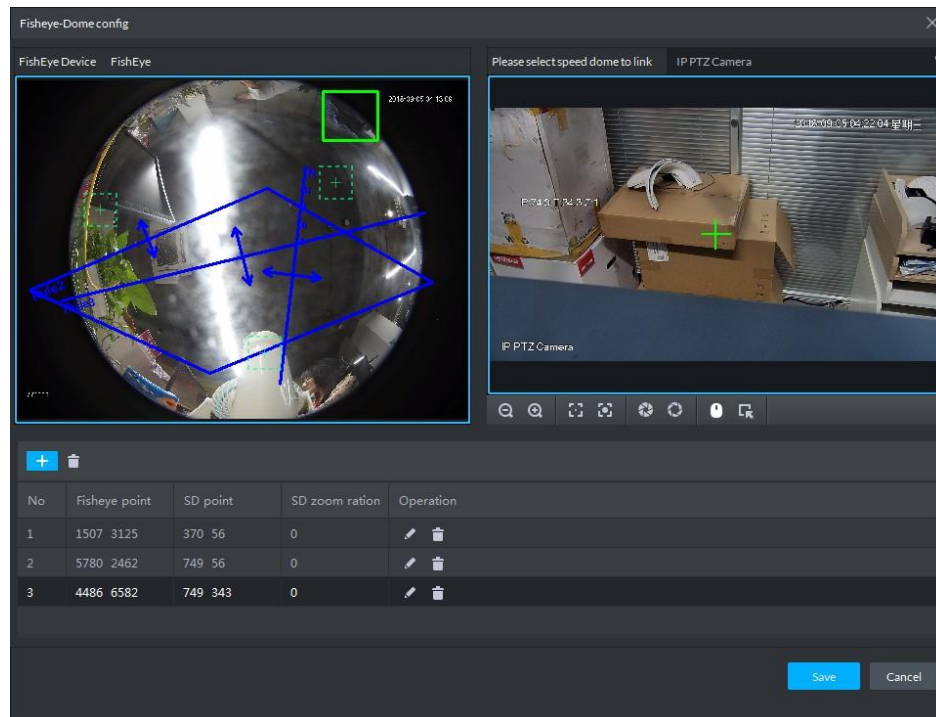
Click  on the general PTZ camera to find the position. Adjust the PTZ camera to find the position and move the PTZ to the center position (The green cross on the image).

Figure 4-107 Set smart track rules (2)



- Select 3-8 mark points on fisheye camera.
- When you find mark point on the left side of general PTZ camera, click to zoom out PTZ.
- Click to 3D position, and when you click a certain point on the left side of PTZ camera, it will automatically move to the center.

Step 5 Click to save the calibration point.

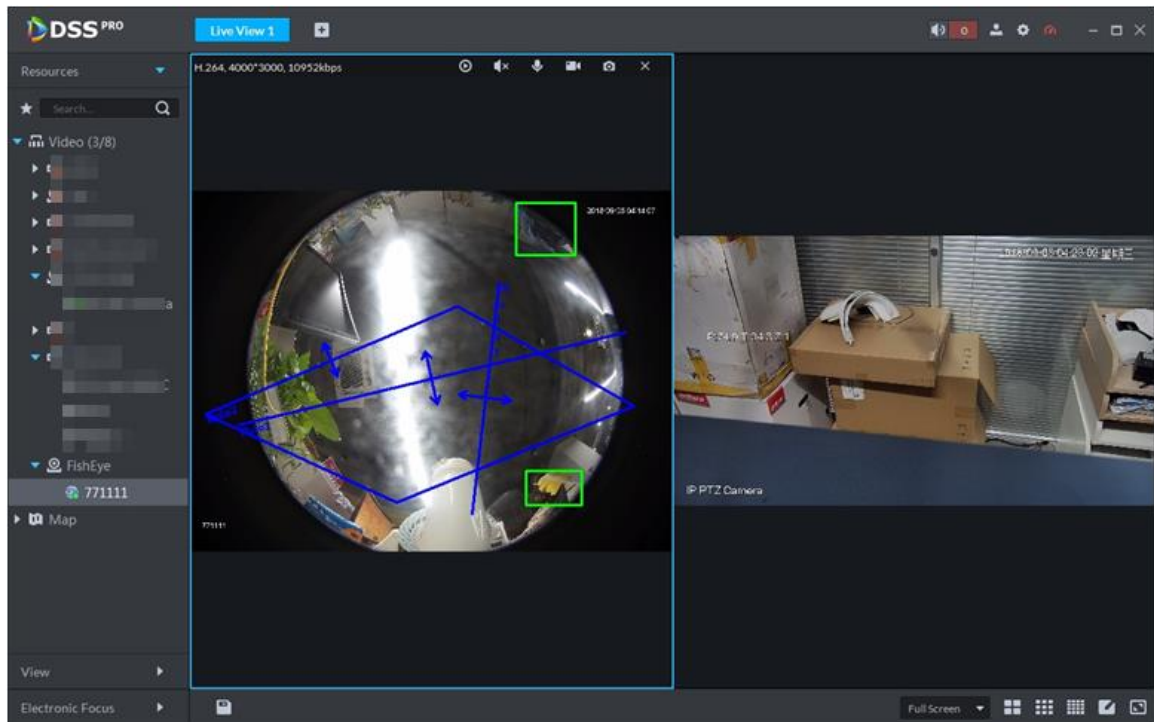
See above steps to add at least three calibration points. These three points shall not be on the same straight line.

Step 6 Click **Save**.

4.6.4 Applying Fisheye-PTZ Smart Track

Step 1 On the homepage of Control Client, select the fisheye device on the device tree and then right-click to select **Smart Track**.

Figure 4-108 Select a smart track channel



Step 2 Click any point on the left of fisheye, general PTZ camera on the right will auto link to corresponding position


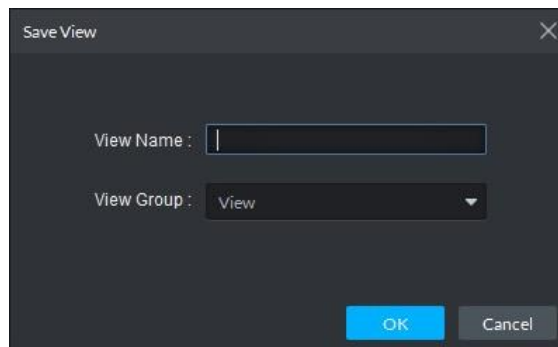
Step 3 Click , system pops up **Save View** box.

Figure 4-109 Save view



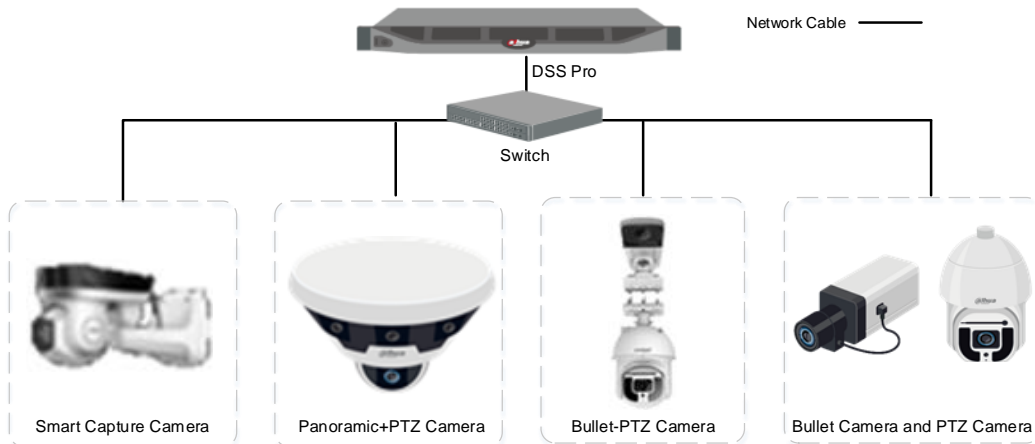
Step 4 Enter view name, select group, and click **OK**.

4.7 Bullet-PTZ Smart Track

When a target is detected in the bullet camera view, the PTZ camera can automatically go to track the target.

4.7.1 Typical Topology

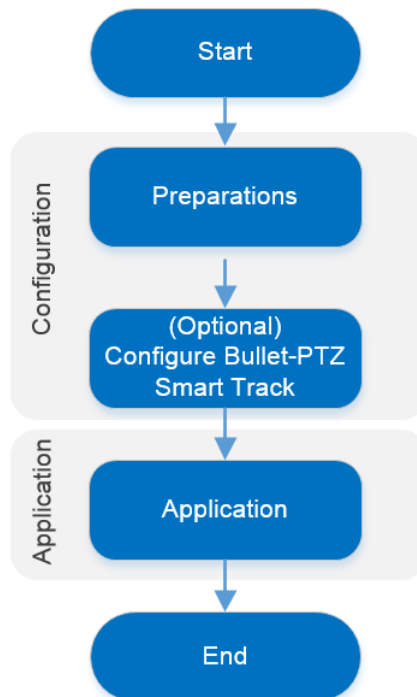
Figure 4-110 Bullet-PTZ smart track topology



- You can use the panoramic + PTZ camera, starlight smart capture camera, bullet-PTZ camera or separate bullet camera and PTZ camera for bullet -PTZ smart track.
- Bullet camera is used to monitor the whole view. PTZ camera is used to track the target and capture details. DSS Pro is used to manage all cameras, configure smart track, and view live video. It supports PTZ operations, snapshot and video recording.

4.7.2 Business Flow

Figure 4-111 Bullet-PTZ smart track



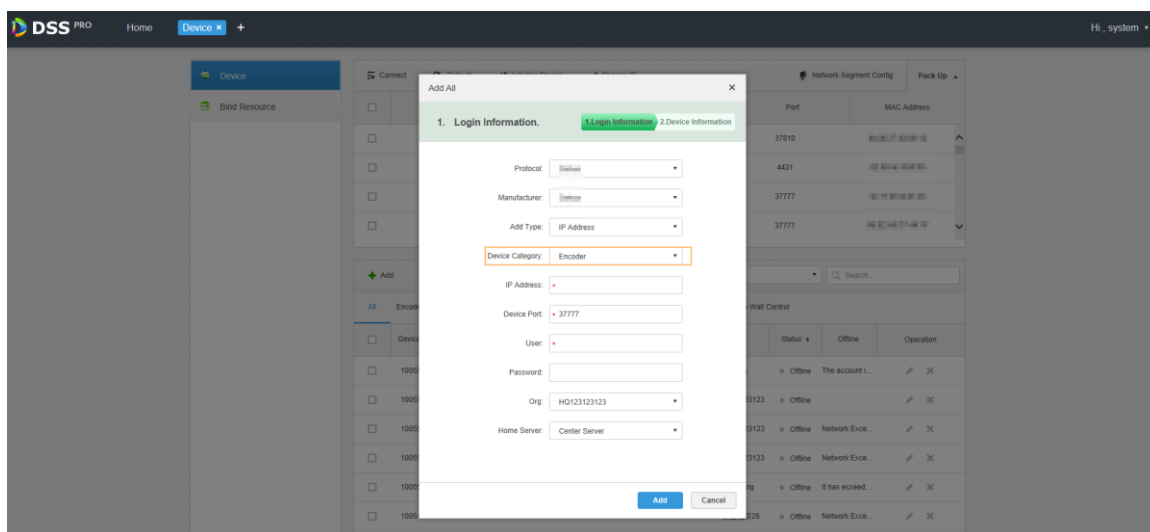
4.7.3 Configuring Bullet-PTZ Smart Track

4.7.3.1 Preparations

Make sure that the following preparations have been made:

- Cameras are well deployed. To deploy, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations." During configuration, note that:
 - ◇ When adding cameras, select **Encoder** for **Device Category**.

Figure 4-112 Set device category




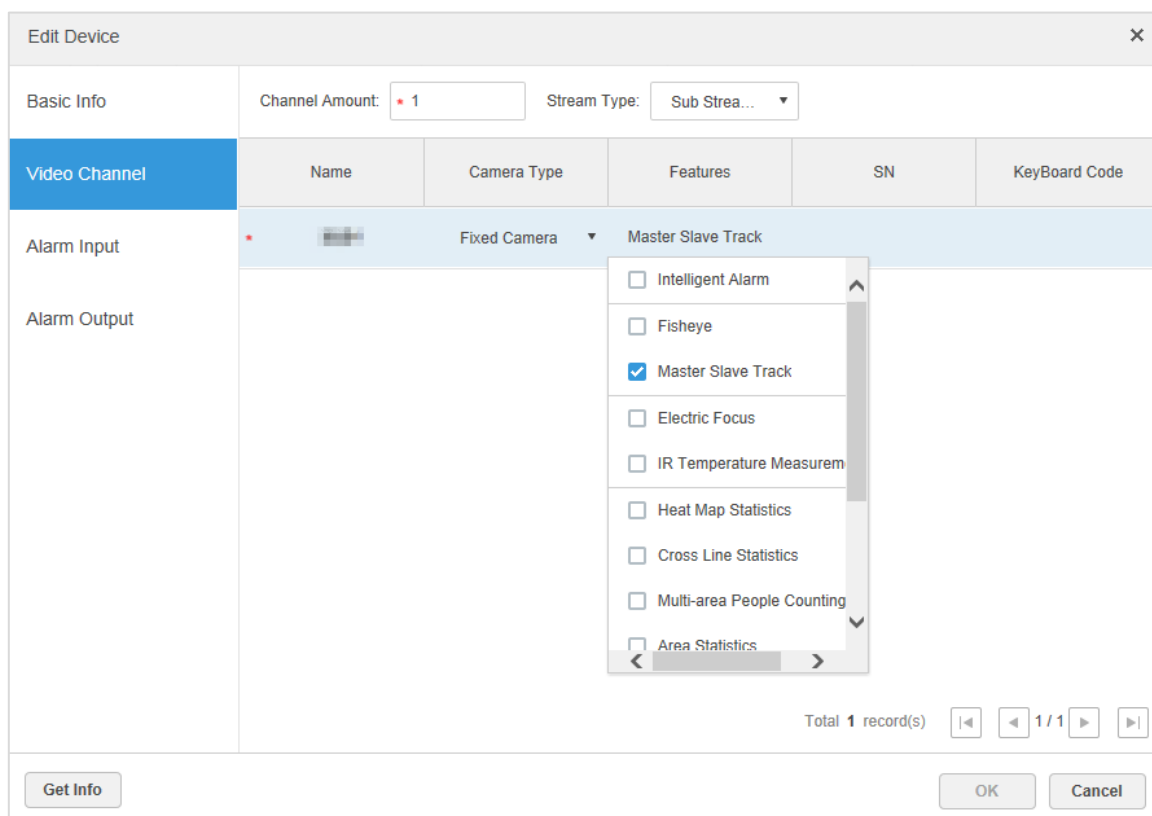
- ◇ On the **Device** interface of Web Manager, click  of the bullet camera, starlight smart capture camera, or panoramic + PTZ camera, and then select **Master Slave Track** for **Features**.


Figure 4-113 Set camera features



4.7.3.2 Configuring Bullet-PTZ Smart Track Settings

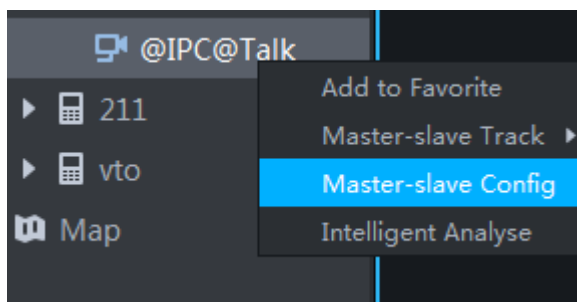
Relate bullet camera view to PTZ camera view. Skip this section if you use panoramic + PTZ camera.

- Single-sensor bullet camera
Select two views to calibrate coordinates, 4 coordinates for each view.
- Multi-sensor bullet camera
Calibrate one view for each sensor of the camera, 4 coordinates for each view.

Step 1 Log in to the Control Client, click , and then select **Live View**.

Step 2 In the device tree, right-click the bullet camera, and then select **Master-slave Config** to open the device login interface.

Figure 4-114 Master slave config



Step 3 On the device login interface, set bullet camera and PTZ camera parameters.

- Separate mode: The bullet camera and PTZ camera are separate. Their login information is different. The bullet camera information is already displayed. Specify PTZ camera information as needed.
- Bullet-PTZ camera: The bullet camera and PTZ camera are integrated in one camera. Their login information is the same.

Step 4 Click **Login and Link** to open the smart track calibration interface.

Step 5 Use the PTZ control panel to rotate the PTZ camera view on the left side to the position where the bullet camera is overlooking.

Step 6 Click **Start**.



During the calibration, PTZ control is unavailable to ensure accuracy of calibration. To operate PTZ during the calibration, click **Pause**. To resume calibrating, click **Start**.

Step 7 Calibrate coordinates.

- 1) Click **Add** next to **Coordinate 1**, and then two frames appear in the bullet view. Move the two frames to the same positions, and then the coordinate values appear in the boxes of the **Coordinate 1**.
- 2) Repeat the previous step to finish the remaining 3 coordinate groups.
- 3) Click **Save**.
- 4) Click **OK** on the confirmation dialogue box.
 - ◇ If the bullet camera is multi-sensor, the next calibration view is displayed.
 - ◇ If the bullet camera is single-sensor, the next coordinate-group calibration interface is displayed.
- 5) Complete the calibration of all coordinates.
The **Apply** button is highlighted on the finishing interface.
- 6) Click **Apply**.

4.7.4 Applying Bullet-PTZ Smart Track

Smart track application includes manual positioning, 3D positioning, manual tracking, auto tracking and preset return.

4.7.4.1 Manual Positioning

Click any position on the bullet image, and the PTZ will position the image to the area designated by bullet due to smart track. Click the red spot on the bullet image, and the PTZ central point will move to the corresponding location automatically.

Figure 4-115 Manual positioning



4.7.4.2 3D Positioning

Select an area on the bullet image, and the PTZ camera will position the image to the corresponding area, meanwhile zoom in or out.

- Draw rectangular box from upper left to lower right, zoom in after being positioned by PTZ camera.
- Draw rectangular box from lower right to upper left; zoom out after being positioned by PTZ camera.

Figure 4-116 3D positioning (1)



Before Positioning



After Positioning

Figure 4-117 3D positioning (2)



4.7.4.3 Manual Track



- Bullet PTZ all-in-one camera, panoramic + PTZ camera and individual bullet have been configured with smart rules. For detailed operation, see device user manual.
- IVS Overlay is required to be selected on the bullet image, enable target box overlay. Target box will be displayed only when there is moving target appears in the image.
- Manual track priority is higher than auto track.

Click moving target box (valid inside the box as well) in the bullet monitoring image, and the color of target box changes, PTZ camera will track the selected target.

Figure 4-118 Manual track



Before Tracking



After Tracking

4.7.4.4 Auto Track

After auto track is enabled, when there is target triggering IVS rule in the bullet image, then PTZ camera will automatically track the target that triggers IVS rule. If there are more than two tracking targets in the image, then it will select tracking target according to trigger time.



- Bullet PTZ all-in-one camera, panoramic + PTZ camera and individual bullet have been configured with smart rules. For detailed operation, see device user manual.

- IVS Overlay is required to be selected on the bullet image, enable target box overlay. Target box will be displayed only when there is moving target appears in the image.
- Manual track priority is higher than auto track.

In the device list on **Live** interface, select individual bullet, bullet PTZ all-in-one camera or panoramic + PTZ camera, right-click and select **Auto Track > On** and enable auto track. When there is moving target in the image, then PTZ camera will track the target automatically.

Figure 4-119 Select automatic track

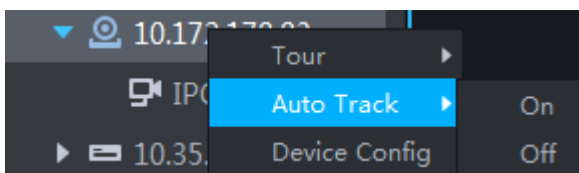


Figure 4-120 Automatic track



4.7.4.5 Preset Return

Enable preset return when idle during calibration, in any status, when there is no target triggering track within the specific period on the bullet image, then PTZ image will return to the designated preset.

4.8 Radar-PTZ Smart Track

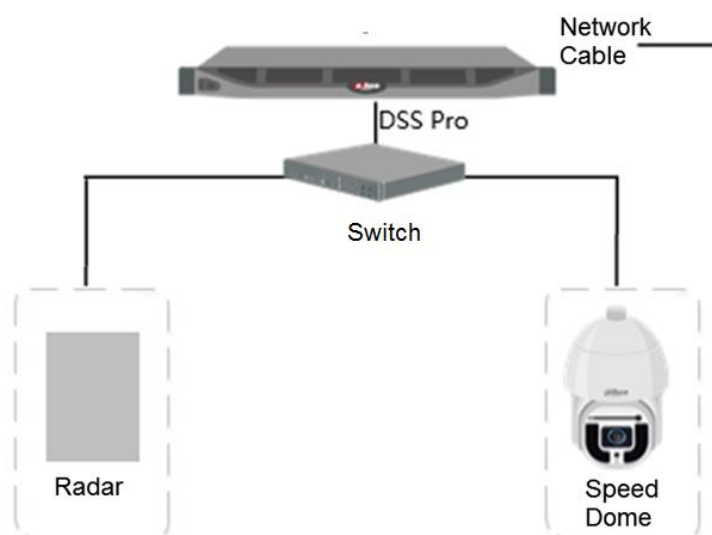
When the radar detection zone is intruded, the associated PTZ camera will track this target automatically.



The interface pictures in this section might vary depending on the radar device type, and the actual interface shall prevail.

4.8.1 Typical Topology

Figure 4-121 Radar-PTZ smart track topology



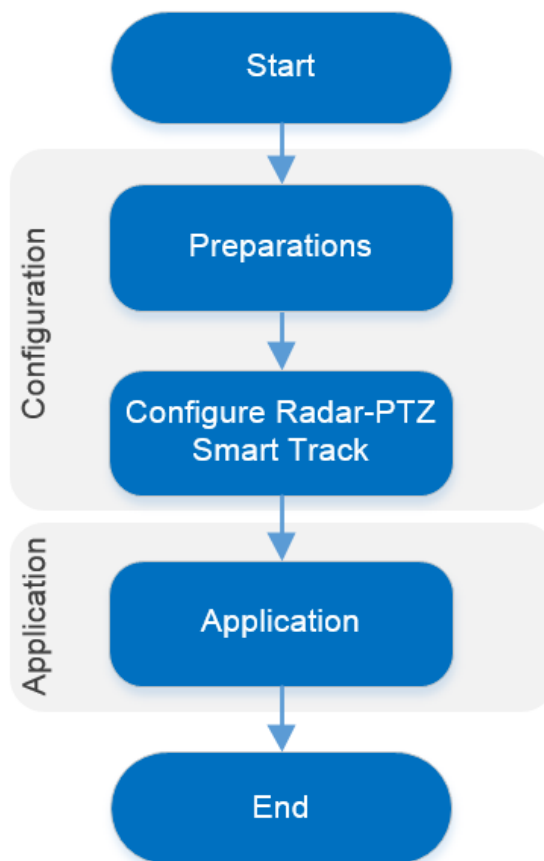
- Radars detect and tracks targets.
- The speed domes collect videos and follows the targets.
- DSS Pro is used to manage radars and cameras, configure smart track, and view live video. It supports PTZ operations, snapshot and video recording.



In addition to radar and speed dome, you can also use the radar + PTZ camera for the smart track.

4.8.2 Business Flow

Figure 4-122 Radar-PTZ smart track business flow



4.8.3 Configuring Radar-PTZ Smart Track

4.8.3.1 Preparations

Make sure that the following preparations have been made:

- Radars and cameras are well deployed. To deploy, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations." During configuration, note that:
 - ◇ When adding a radar, select **Radar** as its device category.
 - ◇ When adding a radar + PTZ camera, select **Encoder** as its device category, and then select **Smart Track (Radar + PTZ)** in the **Features** drop-down list for its video channel.

Figure 4-123 Modify device features

Edit Encoder
✕

Basic Info

Channel Amount:
Stream Type:

	Name	Camera Type	Features	SN	KeyBoard Code
Video Channel					
Alarm Input	* IP PTZ Camera	Speed Dome ▾	Smart Track (Radar...		
Alarm Output					

Total 1 record(s)
 ⏪ ⏩ 1 / 1

Get Info
OK
Cancel



4.8.3.2 Configuring Radar-PTZ Smart Track

Configure map. The map displays device and target locations. You can also view the associated live videos on the map.

Step 1 On the **Homepage** of the Control Client, select **Radar Smart Track**.

Step 2 Add a map picture.

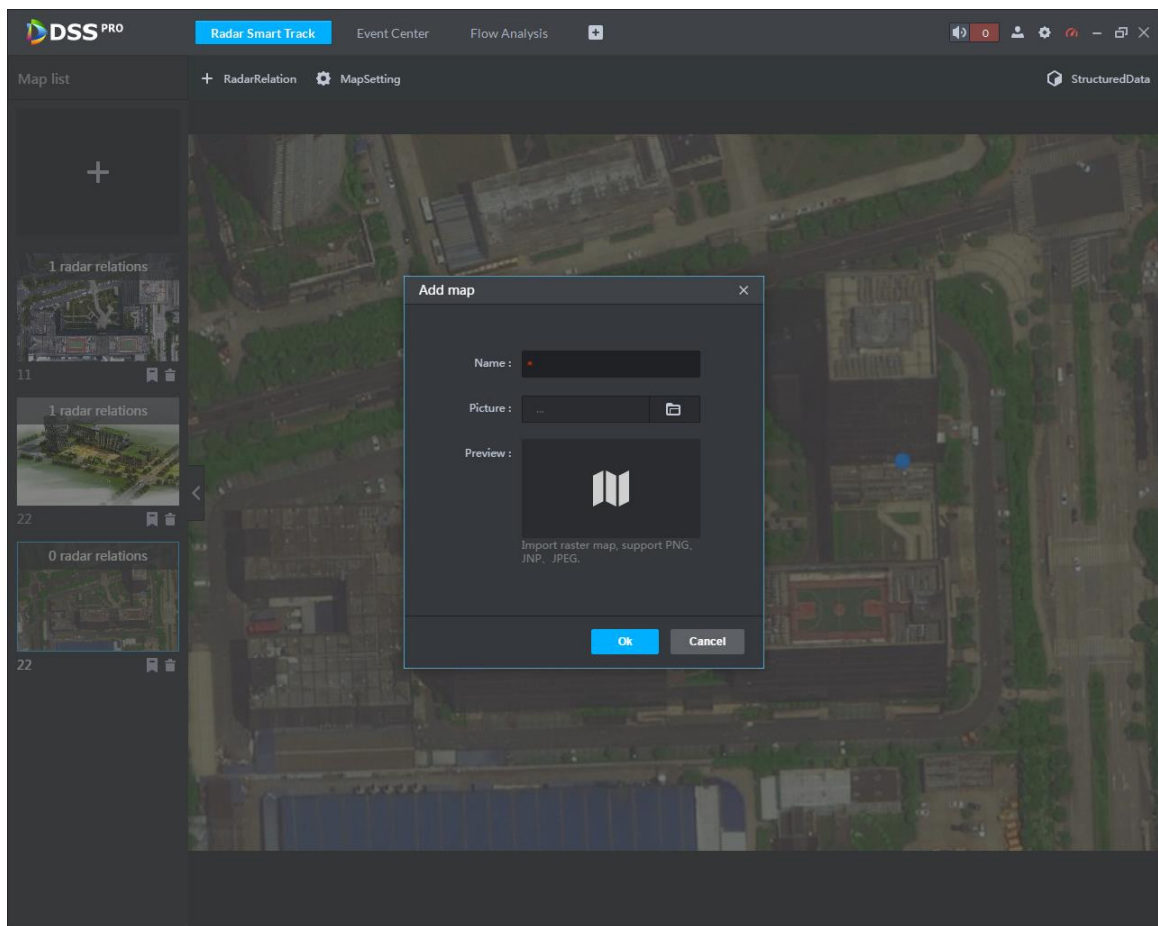
You can add up to 10 maps.

- 1) Click .
- 2) Enter map name, and then click  to select a picture.



Support the .png, .jpg and .jpeg picture formats.

Figure 4-124 Add a map



- 3) Click **OK**.

Step 3 Calibrate.

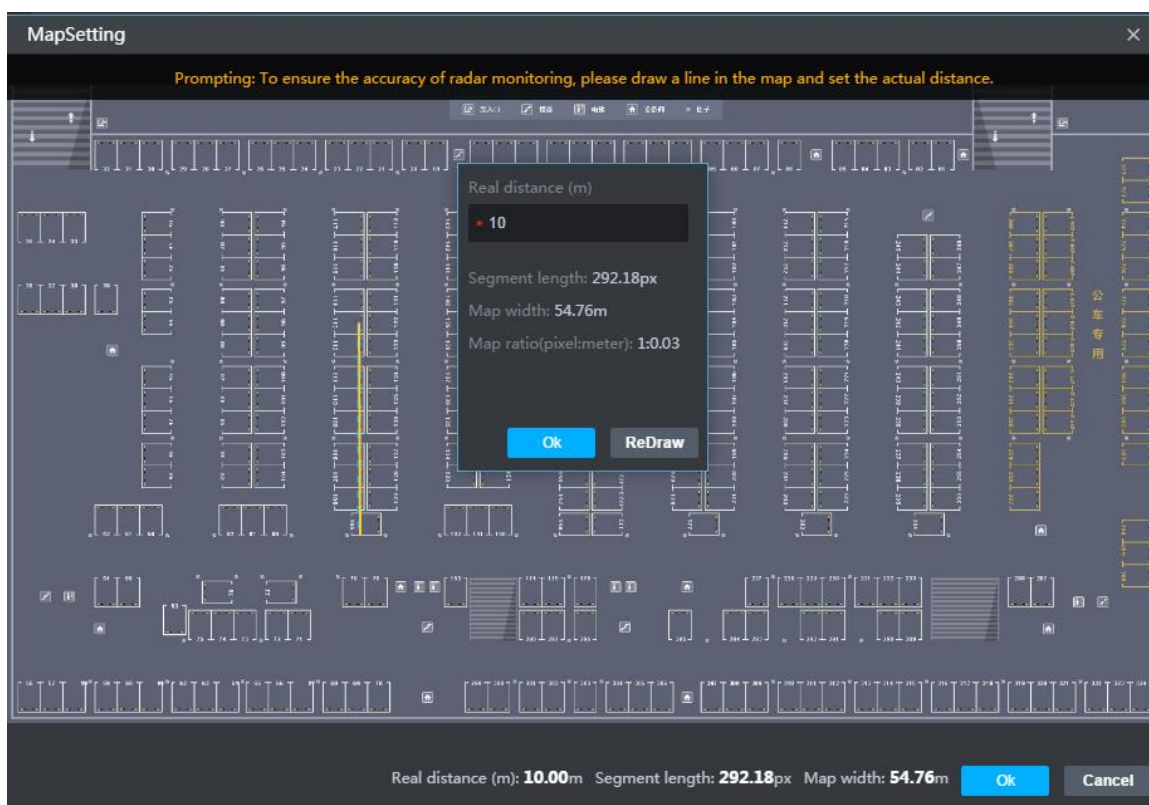
Calibrate map distance with the actual geographical distance to ensure the accuracy of radar measuring. Make sure to select a definite distance to calibrate.

- 1) Draw a distance on the map.



The **Map Setting** interface is displayed by default after a map picture is imported. You can also click **Map Setting** to get into this interface.

Figure 4-125 Calibrate





- 2) Enter the real geographical distance of the drawn line, and then click **OK**.
The line turns into yellow.
- 3) Click **OK**.
- 4) (Optional) click the  icon on the left of the **Radar Smart Track** interface to set the corresponding map as the main map.
If there are multiple maps, the main map is displayed on the **Radar Smart Track** interface by default.  indicates that the map is a main map.

Figure 4-126 Set the main map



Step 4 Add devices.

- 1) Click Radar Relation.
- 2) Select a device in the **Radar** drop-down list, and then drag it to the actual location on the map.
- 3) Set the X and Y coordinates values for the radar location.

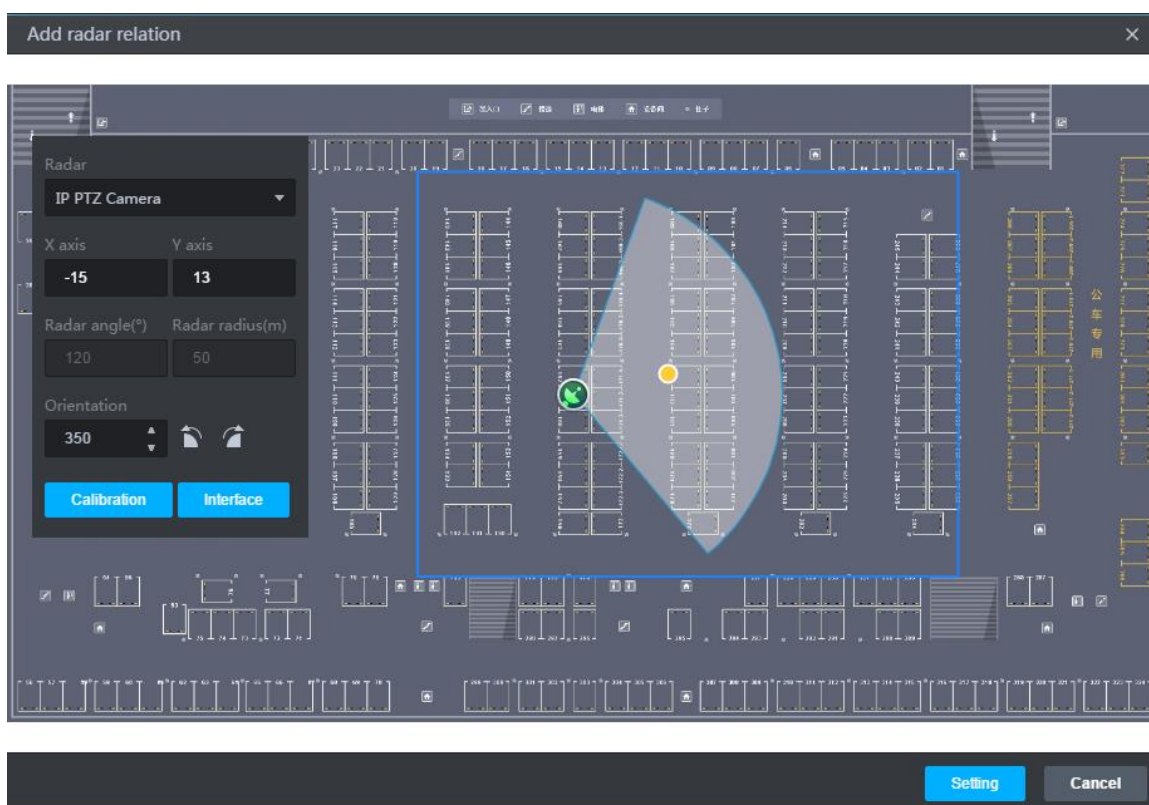
- 4) Set radar **Orientation** value or click and to adjust the orientation. 10 degrees for each click.

The horizontal direction is 0 degree by default.



- The radar angle and radar radius values are automatically obtained from the device.
- The **Calibration** button is not available now.
- Click **Interface** to view PTZ camera video. The radar view is displayed at the upper-left corner of the PTZ video.

Figure 4-127 Add a radar relation



Step 5 (Optional) Bind PTZ camera.

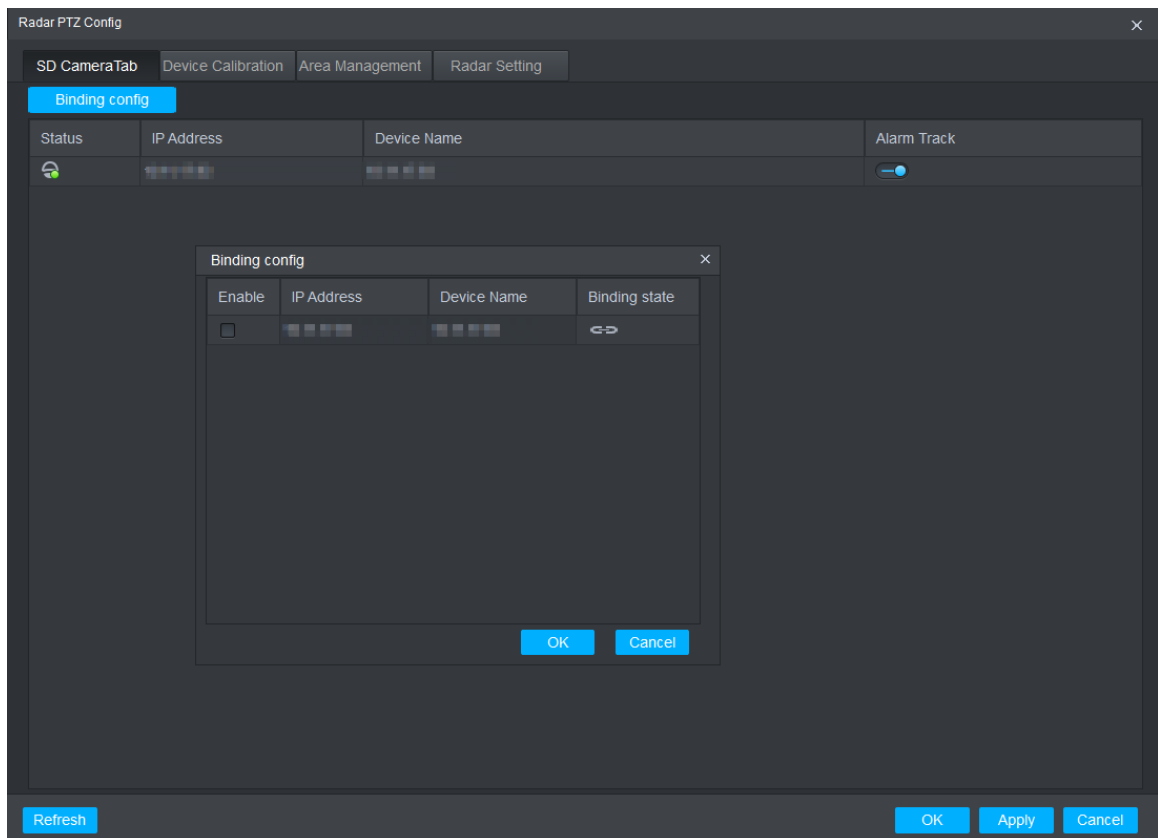
If you are using general radar, you need to bind a PTZ camera for it.

- 1) Click **Radar Relation**.
- 2) On the **Add radar relation** interface, click **Setting**, and then click **Binding config**.
- 3) Select a PTZ camera, and then click **OK**.



- You can select multiple PTZ cameras to bind to the radar.
- The **Alarm Track** function is enabled by default after the binding configuration.

Figure 4-128 Bind PTZ camera



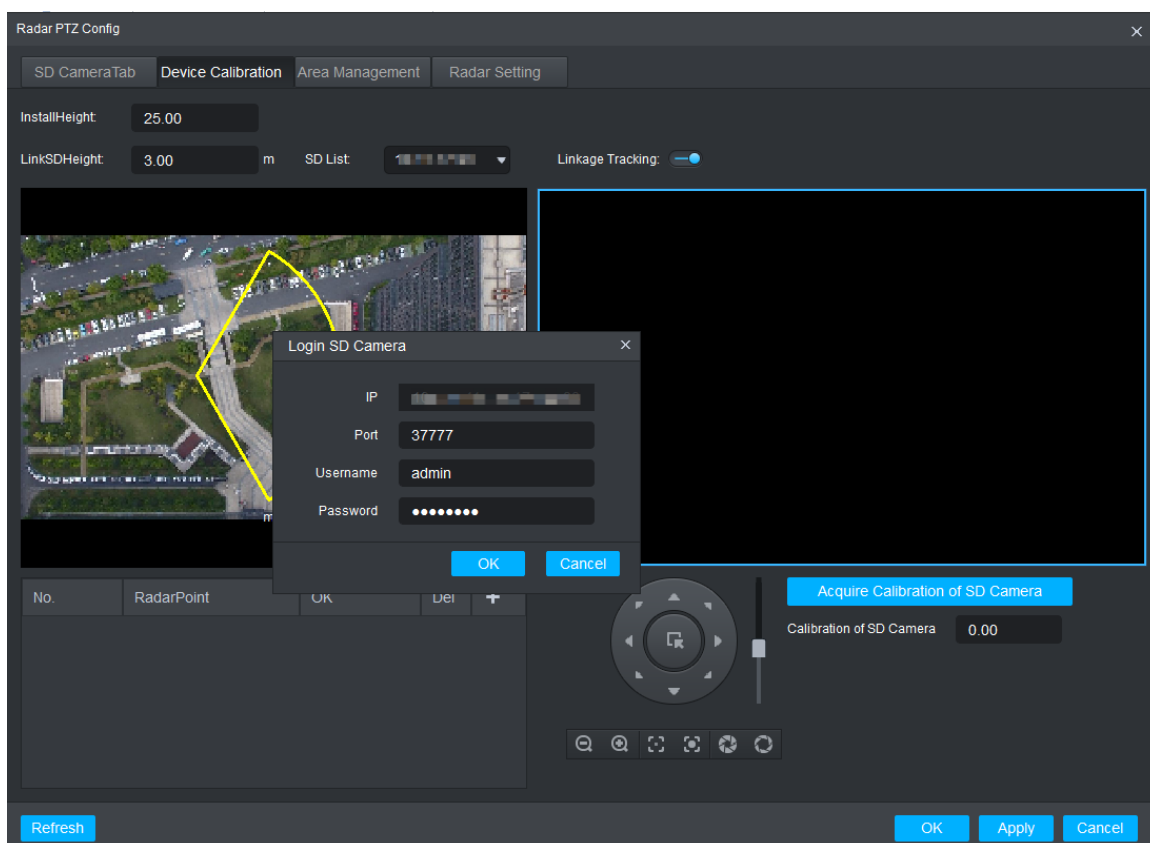
- 4) Enable or disable **Alarm Track** as needed.


When **Alarm Track** is enabled and radar and PTZ have been calibrated, the automatic tracking is triggered once the radar detection zone is intruded.

Step 6 Calibrate radar and PTZ camera to make sure that they are consistent in geographic information.



- 1) On the **Radar PTZ Config** interface, click the **Device Calibration** tab.
- 2) Confirm PTZ camera information, and then click **OK** to log in to PTZ.
PTZ video is displayed on the right.

Figure 4-129 Device calibration



- 3) Set the values of **InstallHeight** and **LinkSDHeight**. They are the real values of the height where the radar and speed dome camera (PTZ camera) are mounted.
- 4) Click , and then on the radar view on the left, click the target position. On the PTZ camera video, operate the PTZ control panel to rotate the PTZ view to that target position.





Click  next to **Linkage Tracking** to disable the function before the calibration; otherwise the view might be unstable.  indicates that the function is disabled.

- 5) Click **Apply**.

Step 7 Manage areas.

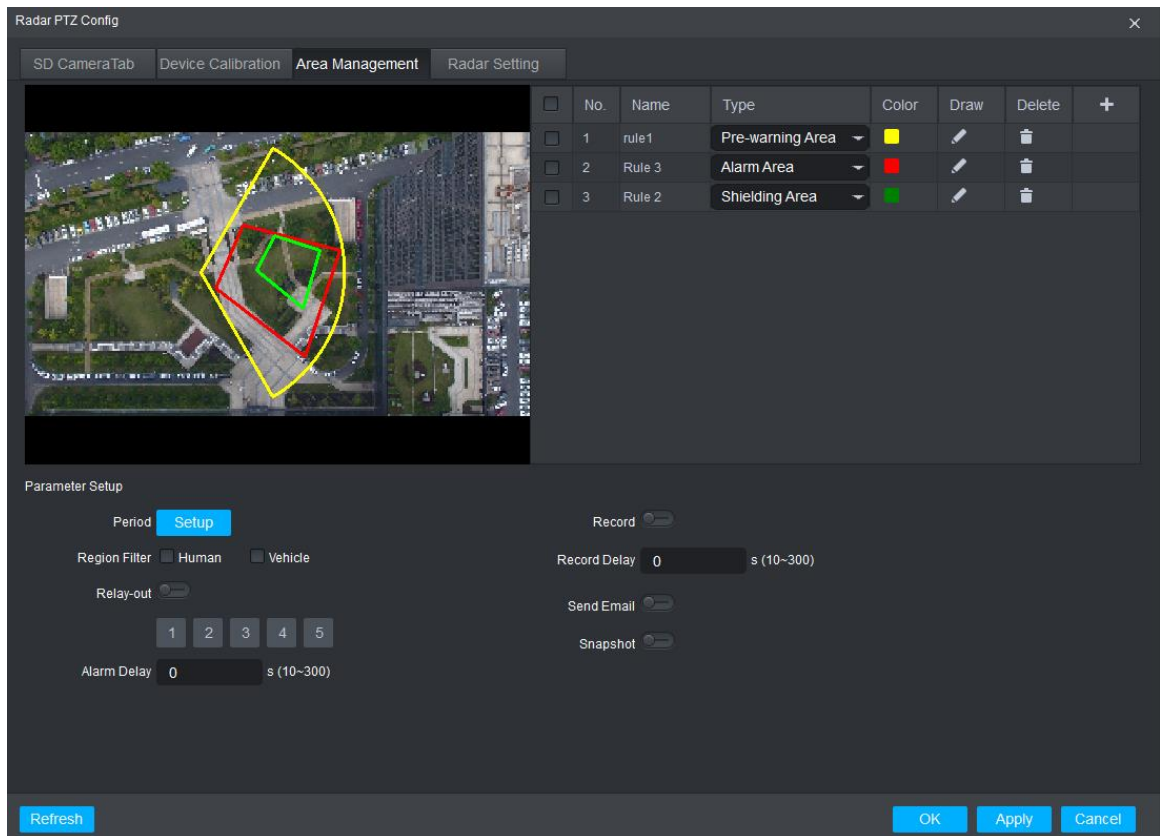
Set alarm area, shielding area, and pre-warning area.

- 1) On the **Radar PTZ Config** interface, click the **Area Management** tab.
- 2) Click  to add an area. Click  and then draw the area on the map.



On the map, click to start drawing, and then right-click to finish.


Figure 4-130 Area management



3) Set parameters.

Table 4-39 Area rule description

Parameter	Description
Name	Name of rule. Double-click to modify the default rule name.

Parameter	Description
Type	<p>Area type includes:</p> <ul style="list-style-type: none"> • Alarm area: In an alarm area, when a target is detected, the target moving track is displayed, and the PTZ camera is linked to track the target, and there will be an alarm for warning. Targets outside of the alarm area will have only the moving tracks, but the PTZ cameras will not follow and there is no alarm. • Shielding area: A target in a shielding area is not displayed with a moving track or followed by the PTZ camera. A target outside of the shielding area will have a moving track and be followed by the PTZ camera, in addition to which, there will also be an alarm for warning. • Pre-warning area: It has the same function with the alarm area, but with lower priority. <p>An alarm area is generally inside a pre-warning area. In this way, the detected target triggers a warning first in the pre-warning area, and then when it enters the alarm area, an alarm will be triggered.</p>  <ul style="list-style-type: none"> • In the radar view, if there is no alarm area, targets are displayed with moving tracks and followed by PTZ cameras, but there will be no alarm. • In the radar view, if there are targets both in and outside the alarm area, the PTZ camera only tracks the one inside the alarm area. • In the radar view, in the overlapped section of the alarm area, shielding area and pre-warning area, targets are displayed with moving tracks and followed by PTZ camera, and trigger alarms.

4) Click **Apply**.

Step 8 Configure radar settings.

- 1) On the **Radar PTZ Config** interface, click the **Radar Setting** tab.
- 2) Set tracking parameters.

Figure 4-131 Radar setting

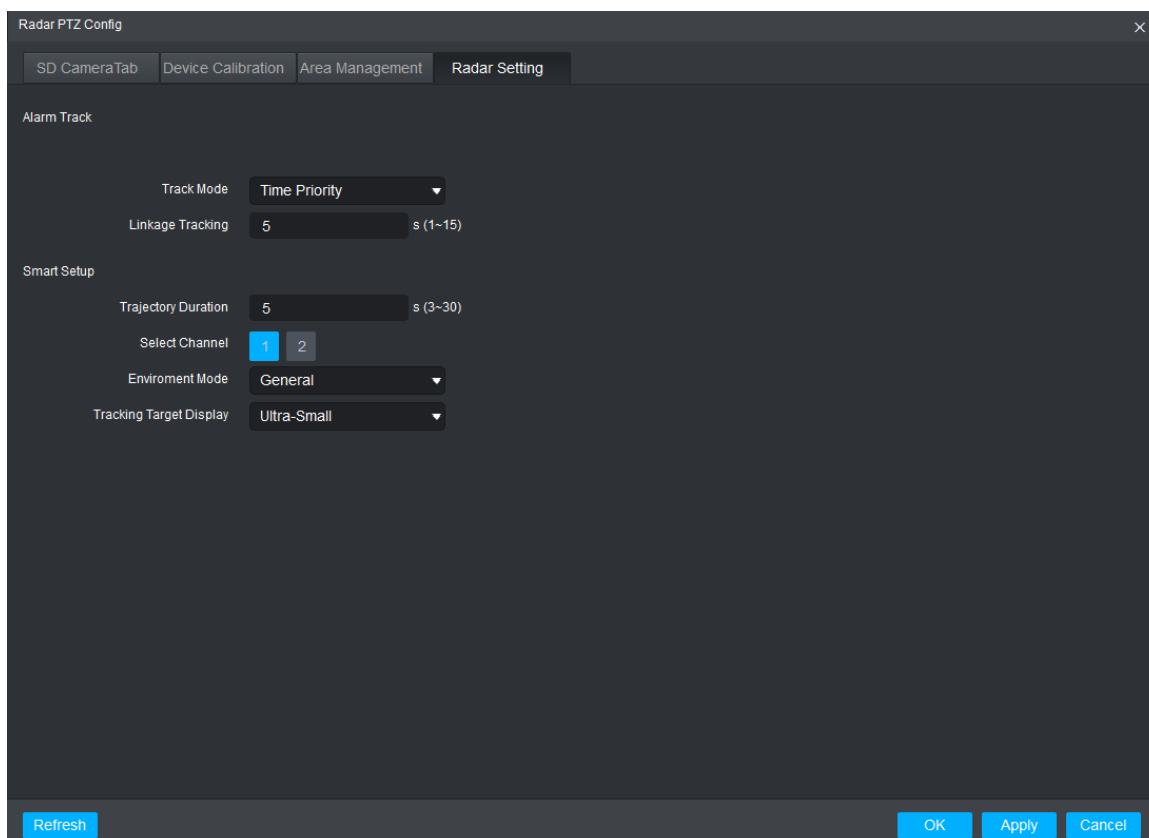


Table 4-40 Parameters description

Parameter	Description
Track Mode	Set track mode and time duration as needed.
Linkage Tracking	<ul style="list-style-type: none"> Tour: According to the linkage tracking duration setting, switch to another target after a few seconds. Time Priority: Follow the target which appears earliest into the radar view. Location Priority: Follow the target closest to the radar.
Trajectory Duration	Set the time length of the displayed moving track.
Select Channel	Select a radar frequency band to avoid interference.
Environment Mode	Select a suitable environment mode. Different environments adopts different algorithms for the best effect.
Tracking Target Display	Set the size of target displayed on the PTZ view during tracking.

3) Click **OK**.

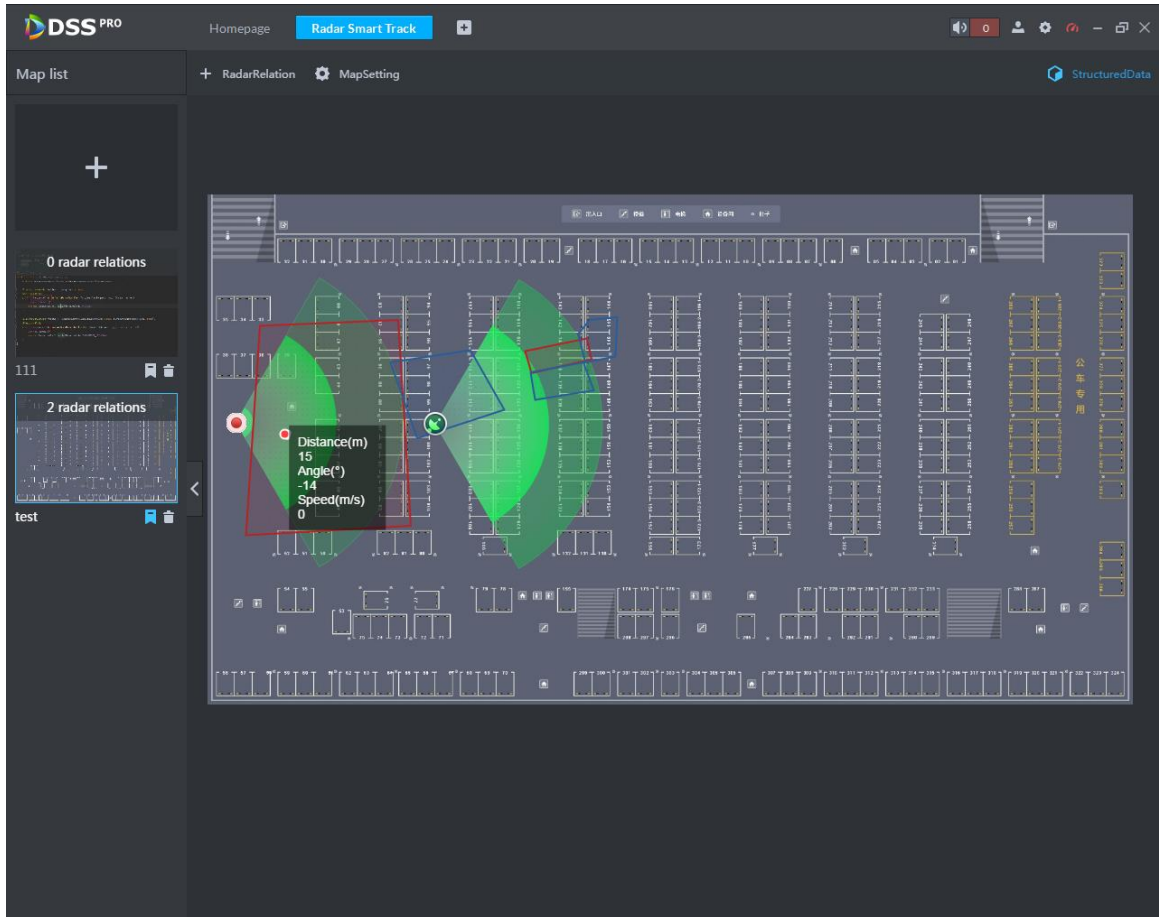
4.8.4 Radar-PTZ Smart Track Monitoring

Step 1 On the **Homepage** interface of the Control Client, select **Radar Smart Track**.



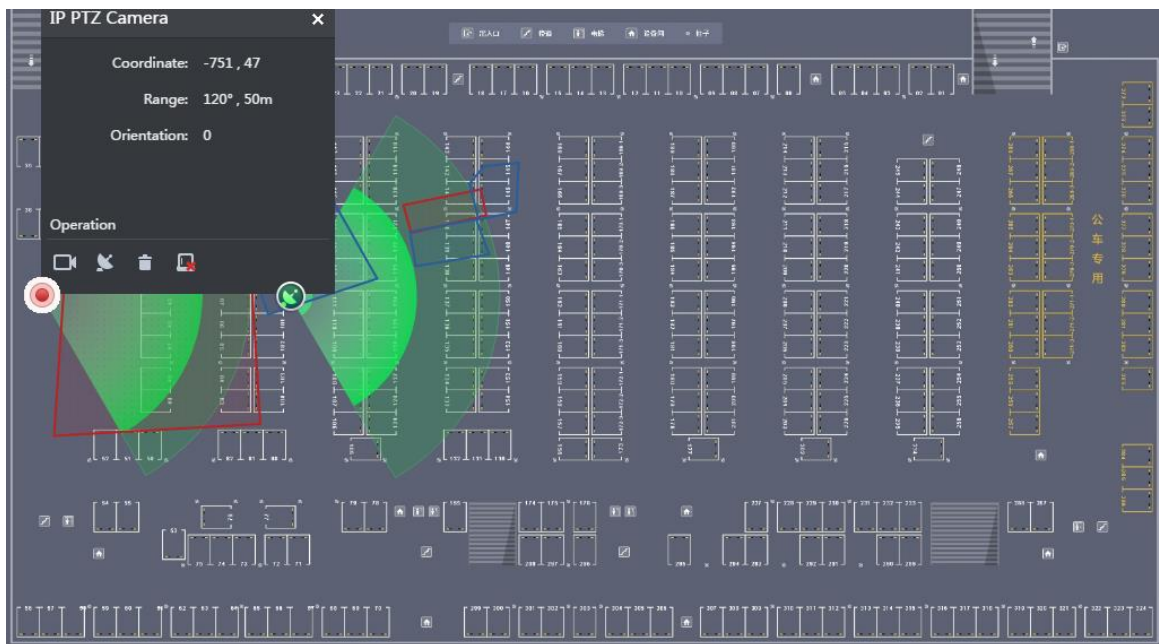
- On the map, if the radar device has an alarm, the radar point flashes red.
- Click **Structured Data** at the upper-right corner of the **Radar Smart Track** interface to enable structured data display, and then the targets inside the alarm area are displayed with features information on the map.

Figure 4-132 Radar-PTZ smart track (1)



Step 2 Click the radar icon on the map.

Figure 4-133 Radar-PTZ smart track (2)



Support the following operations:


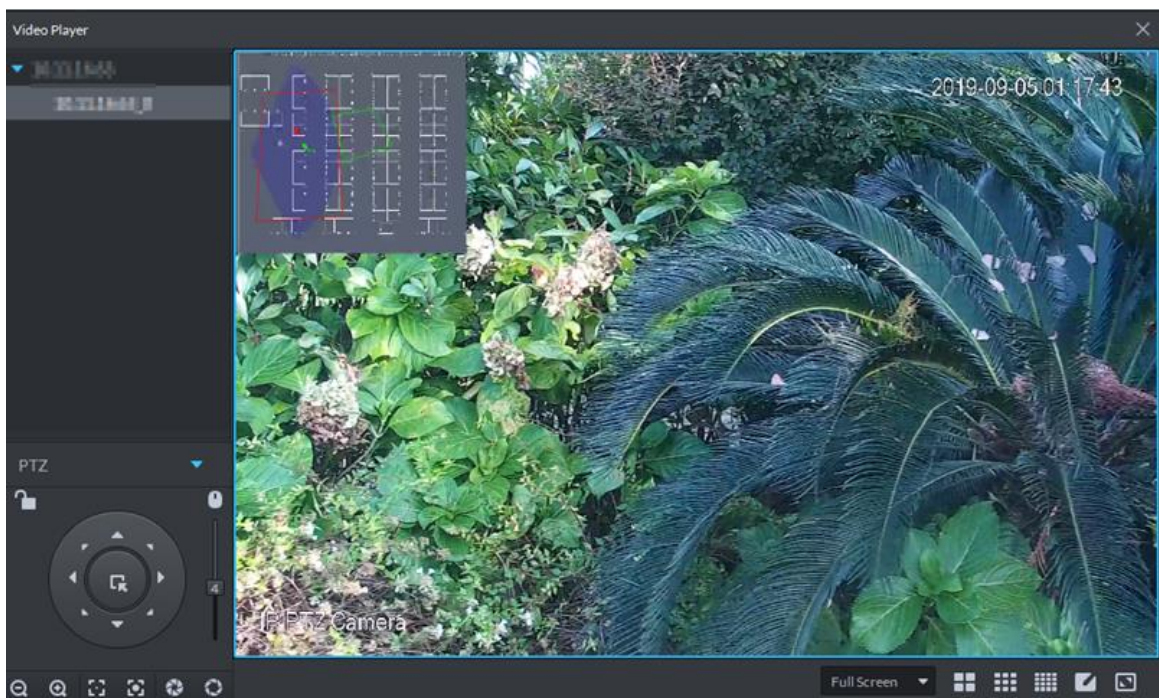



- Click , and then the live video is displayed.

Figure 4-134 Live video



- Click , and then the Add radar relation interface is displayed. You can add more devices onto the map. For details, see "3.7.1 Adding Map."
- Click  to delete radar.
- Click  to cancel alarms.

4.9 Record

You can search and play back records stored in the device or the platform.

4.9.1 Preparations

- Encoders such as cameras and NVRs or DVRs are well deployed.
- DSS Pro is well deployed. For details, see "3 Basic Configurations."
- The device or DSS Pro has recorded videos.

4.9.2 Playback

Play back recorded videos.

4.9.2.1 Playing Back Recorded Videos

Step 1 Log in to Control Client, and then select **Record Playback**.

Figure 4-135 Playback interface

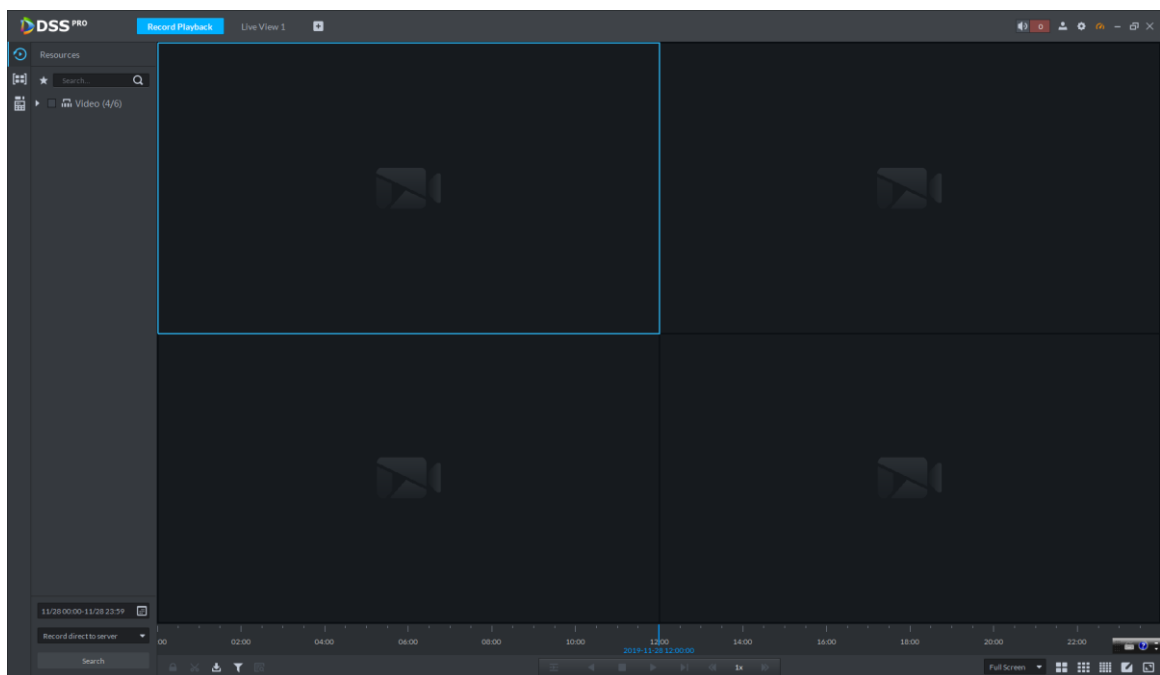








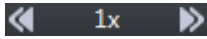
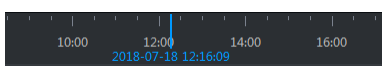


Table 4-41 Description


Icon	Description
	Lock the video stored on server within some period of designated channel. Locked video will not be overwritten when disk is full.

Icon	Description
	Cut video
	Download video
	Filter video according to record type.
	Make dynamic detection analysis over some area of the record image, it only replays the video with dynamic image in the detection area.
	Playback record files of the same period from different channels on selected windows.
	Stop/pause playback
	Frame by frame playback/frame by frame backward.
	Fast/slow playback. Max. supports 64X or 1/64X.
	During playback, you can drag time progress bar to play back record at the specific time.

Step 2 Select a channel on the device tree.

Step 3 Select date and record storage position. Click **Search**.

Blue dots on the calendar indicate existence of video files.

Step 4 Select a window that has video and then click  to play.

Step 5 Hover over the video, and then the icons appear. You can perform the following actions.

Figure 4-136 Video playback

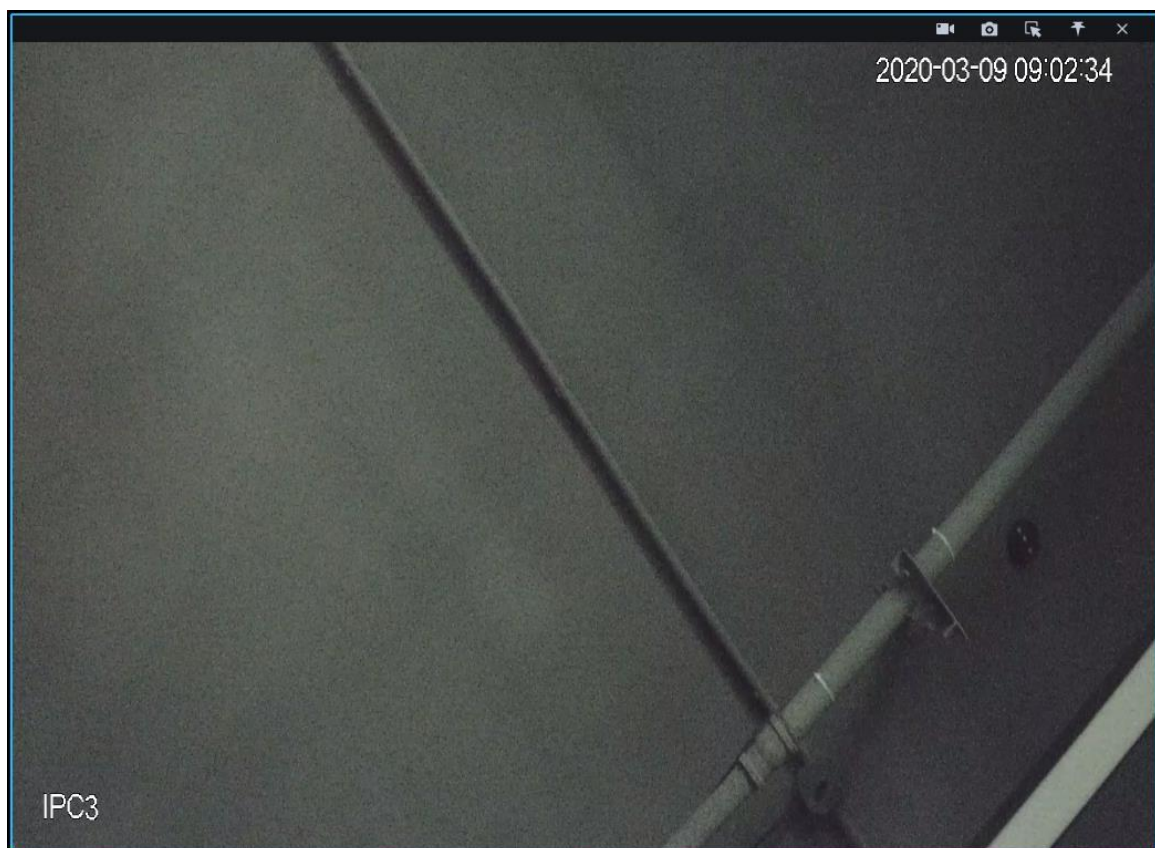


Table 4-42 Description

Icon	Name	Description
	Tag	Tag the videos of interest for easy search in the future. For details, see "4.9.2.5 Tagging Videos."
	Local Recording	Click this icon to start recording. The recorded video is stored locally. The saving path is "C:\DSS Pro\Client\Record\" by default. To modify the path, see "4.1.4 Local Configuration."
	Snapshot	Take a snapshot of the current image and save it locally. The saving path is "C:\DSS Pro\Client\Picture\" by default. To modify the path, see "4.1.4 Local Configuration."
	Zoom	Select a section to zoom it in for viewing details.
	Close	Close the window

- Right-click the video, and then you can perform the following actions.



The shortcut menu varies depending on the camera functionality. The actual shall prevail.

Figure 4-137 Shortcut menu

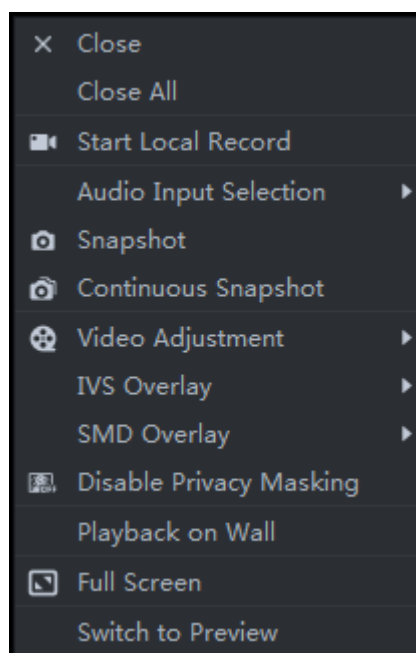


Table 4-43 Description

Name	Description
Close	Close the current video window.
Close All	Close all video windows.
Start Local Record	Record audio and video of the current video window and save them locally.

Name	Description
Audio Input Selection	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Snapshot	Take a snapshot of the current image (one picture for each snapshot action). The default saving path is: C:\DSS Pro\Client\Picture\. To modify the path, see "4.1.4.4 Configuring Snapshot Settings."
Continuous Snapshot	Take a snapshot of the current image (three snapshots each time by default).
Video Adjustment	Perform video adjustment and video enhancement.
IVS Overlay	The client does not show overlay lines over live video by default. When needed, you can click AI Overlay and enable Rule Overlay and Target Box Overlay , and then the live video shows overlay lines if the AI detection rules are enabled on the device. This configuration is effective with the current selected channel both in live view and playback.
SMD Overlay	Enable SMD Overlay to show target frame over live video. When SMD is enabled on the device, you can enable SMD Overlay for the device channel, and then the live video will display dynamic target frames. This configuration is effective with the current selected channel both in live view and playback.
Disable Privacy Masking	For a camera that supports privacy masking of human face, you can disable the masking here to view the face image.
Playback on Wall	Play the current channel on video wall. For configuration of video wall, see "4.10 Video Wall."
Full Screen	Switch the video window to full screen mode. To exit full screen, double-click video window, or right-click to select exit full screen.
Switch to Preview	Go to live view.

4.9.2.2 Record Type Filter

Filter video according to record type, record type includes schedule record; alarm record and motion detect record.

Step 1 Log in to Control Client, and then select **Record Playback**.


Step 2 On **Record Playback** interface, set search conditions to search for videos. Select a window that has videos, and then click .

Figure 4-138 Record playback interface

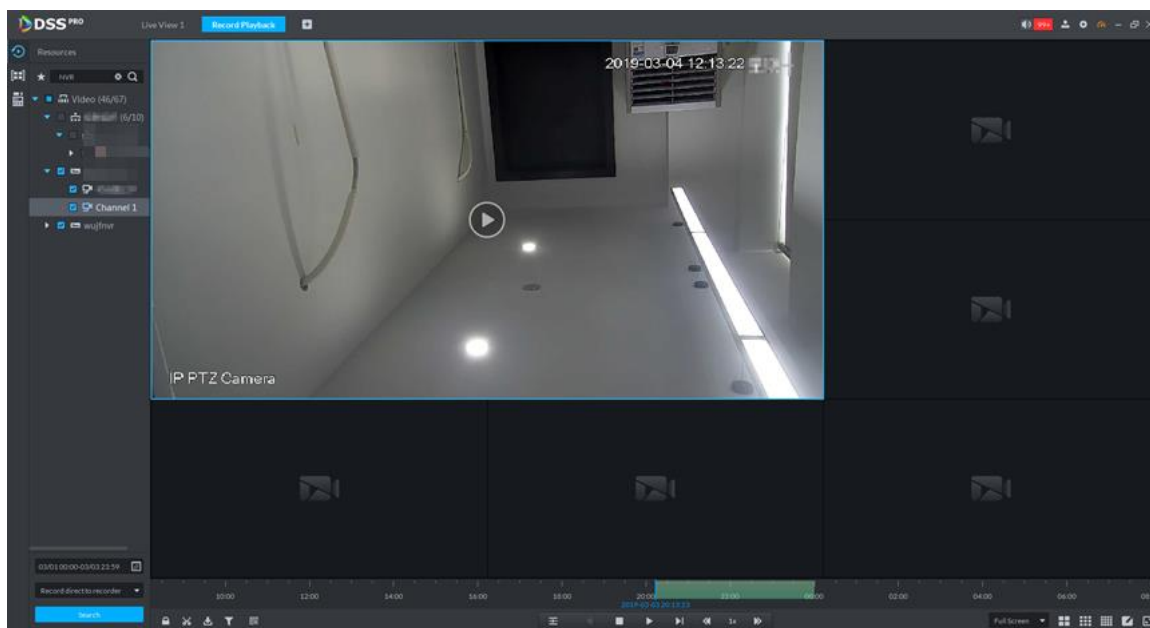
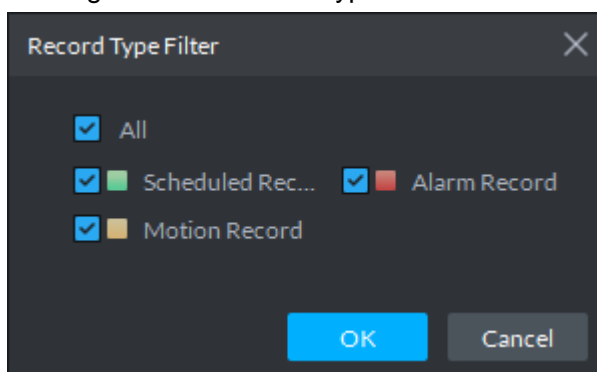


Figure 4-139 Record type filter



- Step 3** Select a record type (or types) and then click **OK**.
The system only displays the video of selected type.

4.9.2.3 Smart Search

With the Smart Search function, you can select a zone of interest on the video image to view motion records within this section. The relevant camera is required to support Smart Search; otherwise the search result will be null.

Step 1 Log in to Control Client, and then select **Record Playback**.


Step 2 On **Record Playback** interface, set search conditions to search for videos. Select a window that has videos. Click , and then select a type.
The smart search interface is displayed. 22x18 squares are displayed in the window.

Figure 4-140 Enable smart search

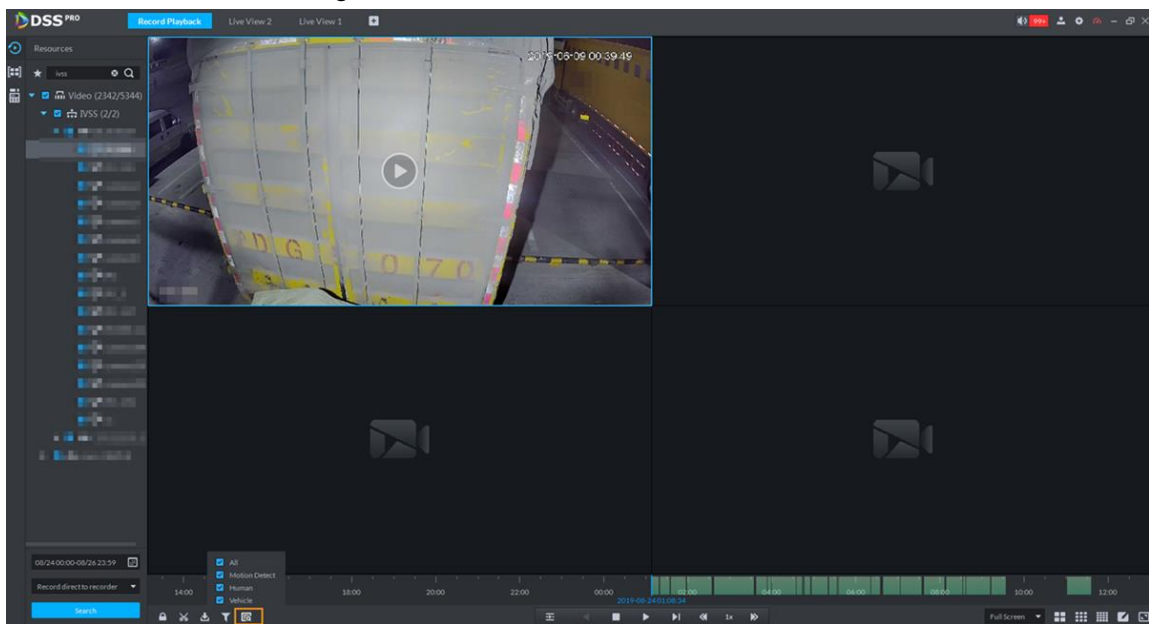
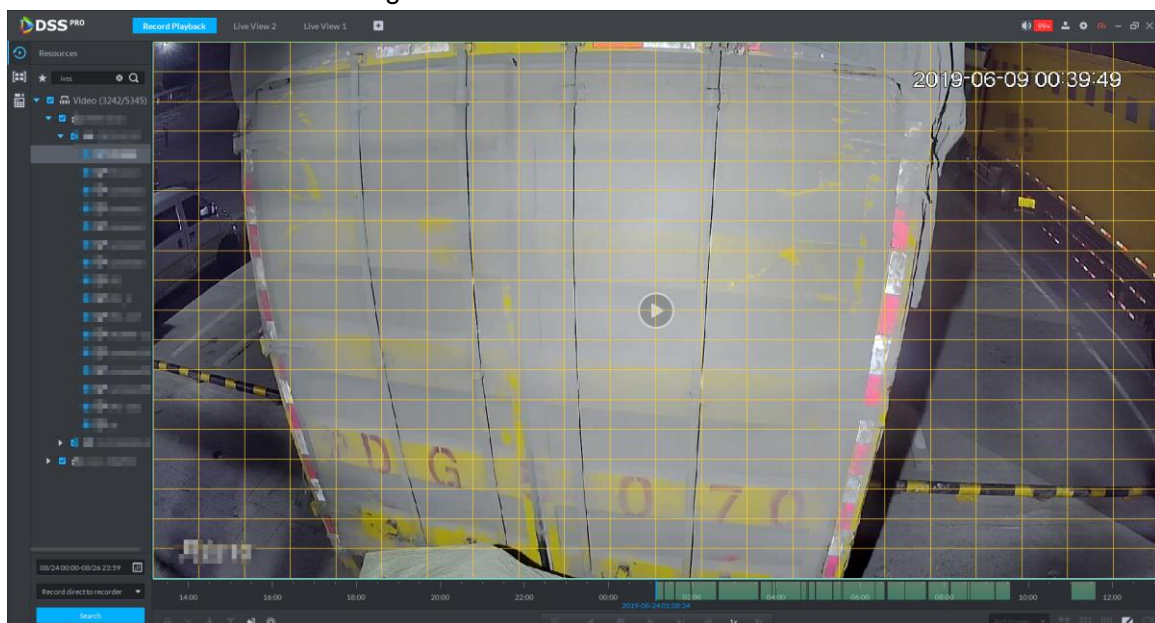


Figure 4-141 Smart search



Step 3 Click the squares and select detection areas.




- Select detection area; Move the mouse pointer to image, press mouse left button and drag the mouse to select square.
- For selected area, click again or select square to cancel it.

Step 4 Click  and start smart search analysis.

- If there is search result, the time progress bar will become purple and display dynamic frame.
- If there is no search result, or selected playback device fails to support smart search, then it will prompt that smart search result is null.



Click  and you can reselect detection area.

Step 5 Click the play button on the image or control bar.
The system plays search results. The search results are marked purple on the on the timeline.

Step 6 Click  to exit Smart Search.

4.9.2.4 Locking Videos

Lock the video stored on the server within some period of specific channel. The locked video will not be overwritten when disk is full.



You can only lock the central video stored on the server.

Step 1 Log in to Control Client, and then select **Record Playback**.


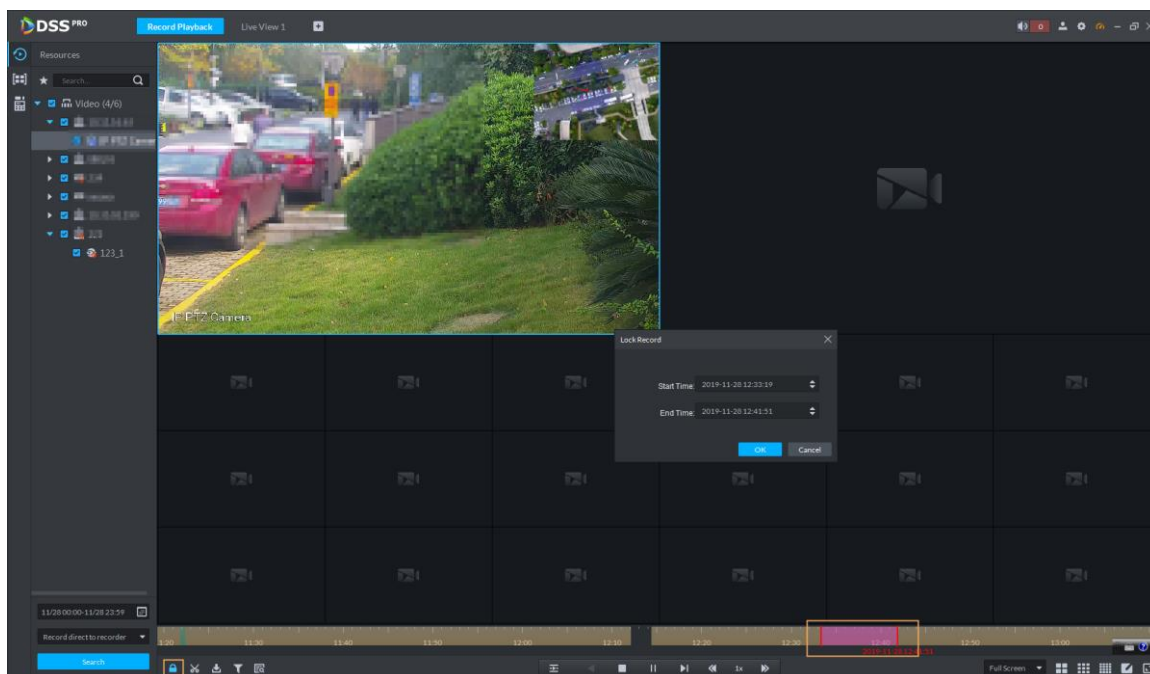
Step 2 Set search conditions and then click search. Select a window that has recorded video, and then click  at the bottom of the **Record Playback** interface, and then click on the timeline to mark the start point and end point of the video clip you need.

Figure 4-142 Lock record



Step 3 Confirm the start and end time, and then click **OK**.

4.9.2.5 Tagging Videos

You can tag records of interest for quick search.

Step 1 Log in to Control Client, and then select **Record Playback**.


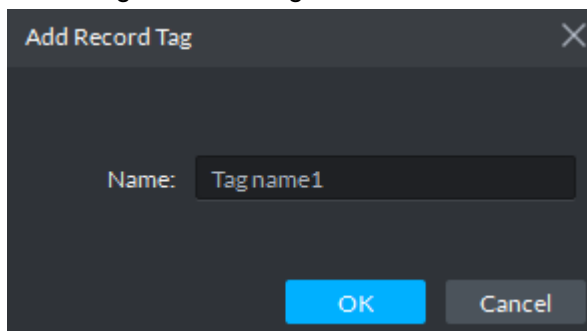
Step 2 On **Record Playback** interface, move the mouse pointer to the window that is playing record. Click  at the upper-left corner.

Figure 4-143 Tag a video



Step 3 Name the tag, and then click **OK**.

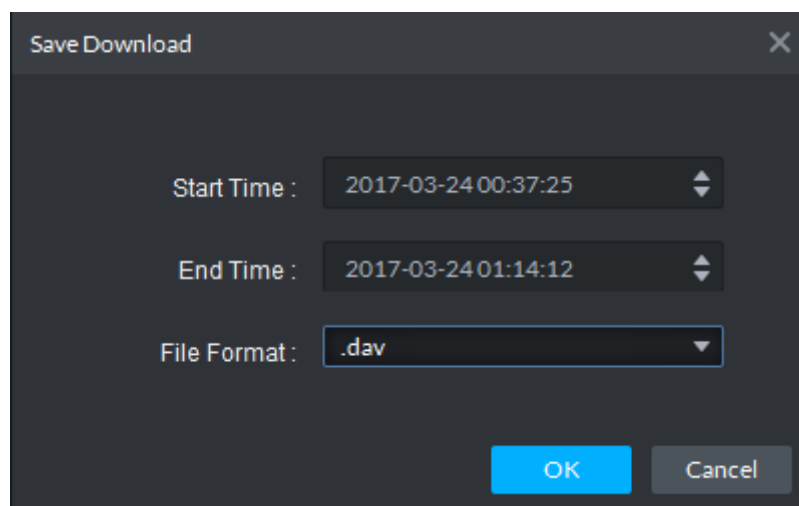
4.9.2.6 Clipping Videos

Step 1 Log in to Control Client, and then select **Record Playback**.

Step 2 Click  at the bottom of the **Record Playback** interface (Make sure that there is record in the window).

Step 3 On the timeline, click to select the start and end time.

Figure 4-144 Save download



Step 4 Set file format and then click **OK**.

4.9.2.7 Downloading Videos

You can download the videos of interest stored in the server or the device. The downloaded videos are in .avi, mp4, or .asf format.

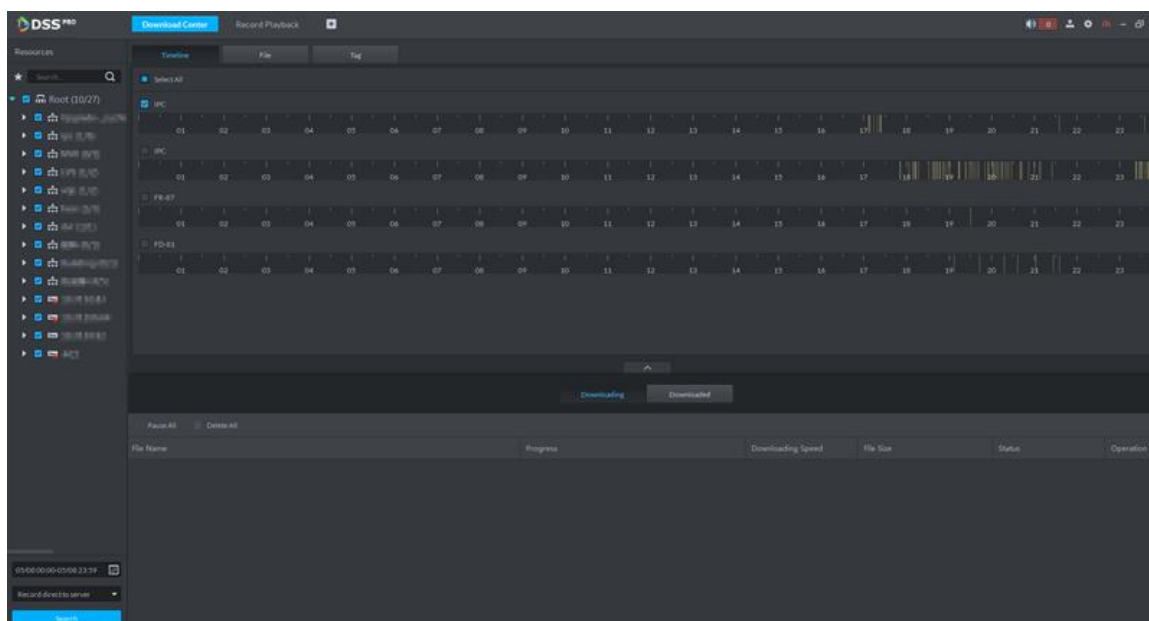
Three ways to download videos:

- Download clipped videos from the timeline.
- Download video files from the file list.
- Download videos by searching video tags.



Step 1 Click  on the **Record Playback** interface, or click  and then select **Download Center**.

Step 2 Set search conditions, and then click **Search**.


Figure 4-145 Download center



Step 3 Select videos to download.

- To download videos by clipping the timeline, click the **Timeline** tab, and then select the start and end time of the video clip by clicking on the timeline.
- To download videos by selecting the searched video files, click the **File** tab, and then click .
- To download tagged videos, click the **Tag** tab, and then click .

Step 4 In the password verification dialogue box that appears, enter the password, and then click **OK**.

Step 5 In the **Record Download** dialogue box, confirm the time span, and then, if necessary, click  to select a video format. Click **OK**.

The download progress is displayed. During the download process, you can pause, stop and cancel the download task by clicking the corresponding icons.

4.9.3 POS Search

Search for POS receipts, and view related videos. Support displaying videos starting from half an hour before the receipt printing moment. The maximum length is 24 hours. The video is played from 30 seconds prior to the receipt printing moment. For details, see "4.14 POS."

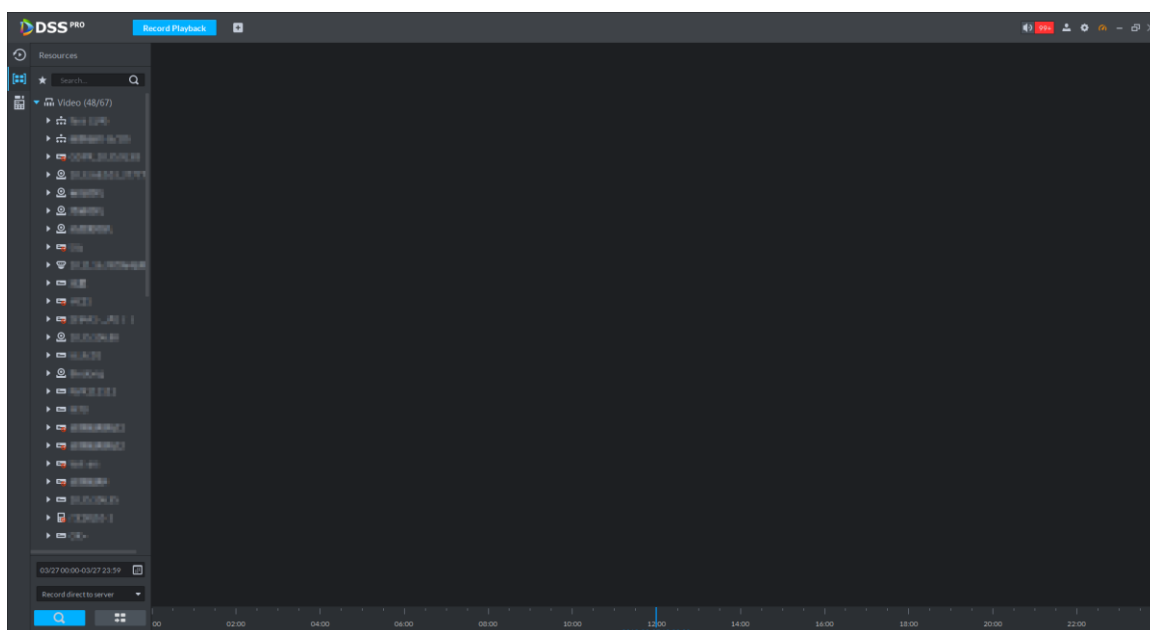
4.9.4 Searching by Thumbnail


Divide the searched video into levels and display in the form of thumbnail, which is the select ROI. You can view the searched video and image change of ROI at different time, and realize fast search.

Step 1 Log in to Control Client, and then select **Record Playback**.

Step 2 On **Record Playback** interface, click .

Figure 4-146 Thumbnail



Step 3 In the organization tree, select a video channel and then set search period and record position. Click .



There is a blue dot at the top-left corner of the date if the channel has record files. See Figure 4-147.

Figure 4-147 Select time

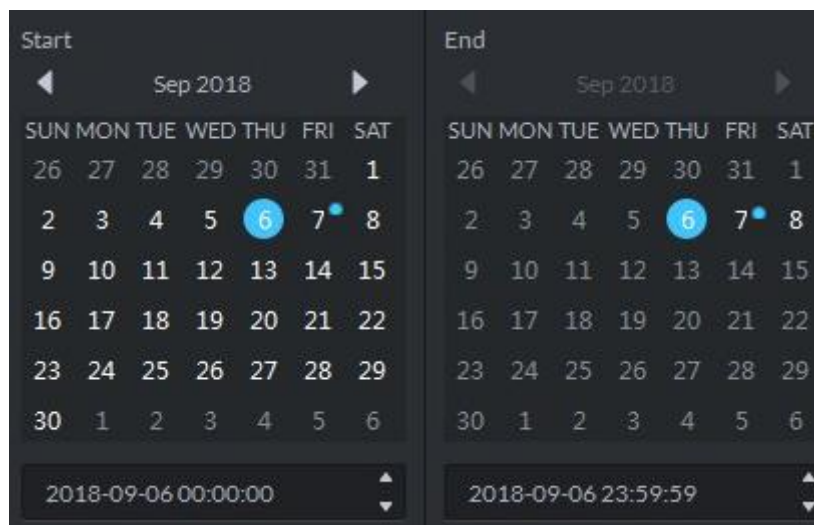
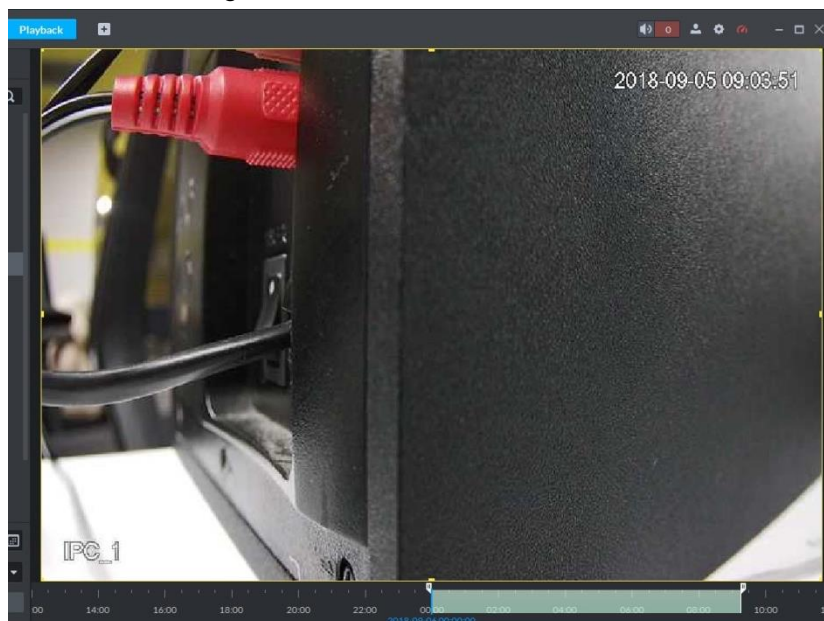


Figure 4-148 Search result




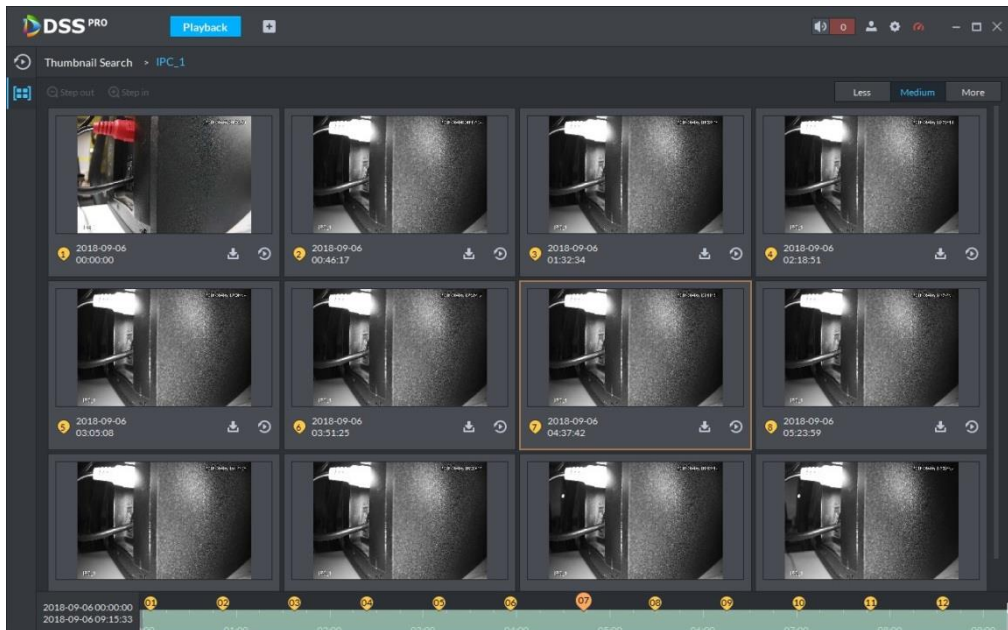
Step 4 Drag the yellow frame on the right to set thumbnail range. Click .

Figure 4-149 Thumbnail search



- System displays search results in suitable mode by default. Click Less, suitable, more to see proper mode.
- Double-click the thumbnail, system search again for the record between current image and the next image.


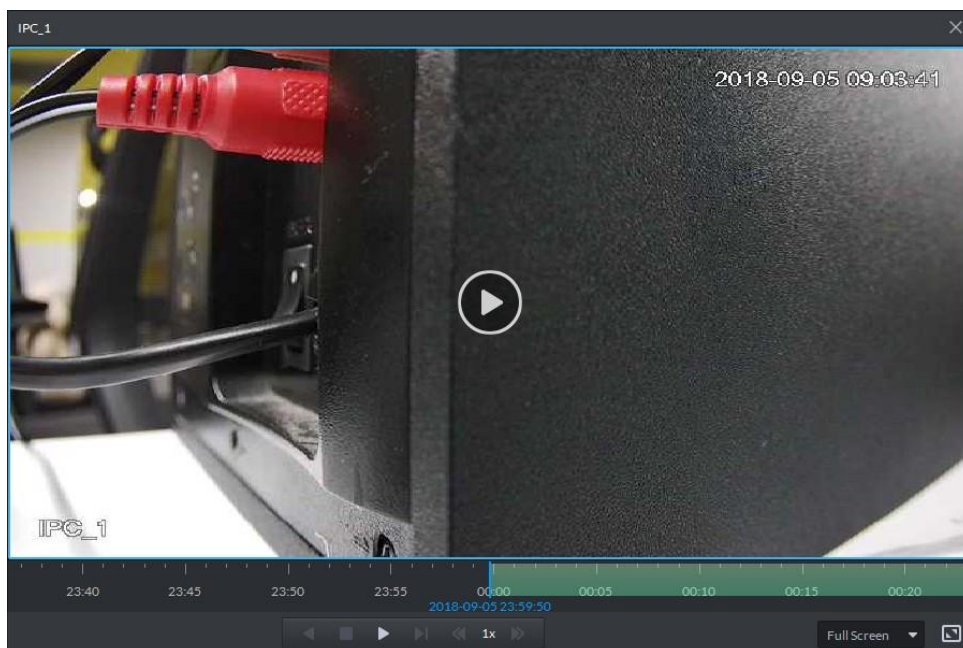
Step 5 Click the  at the bottom right corner of the thumbnail, you can view the corresponding video related to the thumbnail.

Figure 4-150 Video playback



Step 6 Download Record



If videos of different stream type exist in the download period, then it can only be saved as .dav.


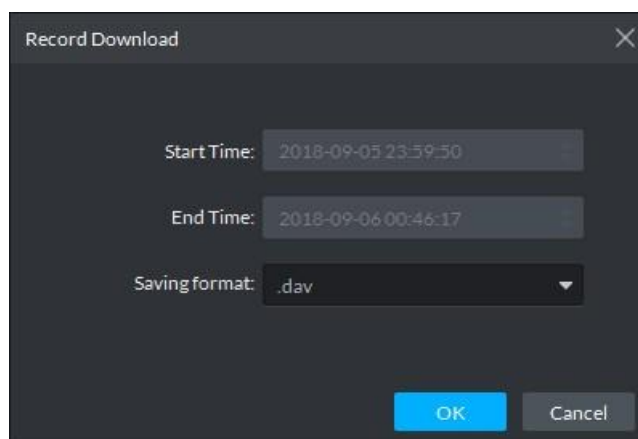
- 1) Click  at the right corner of the thumbnail, and then system downloads the record between current image and the next image.

Figure 4-151 Download video



- 2) Select a file format and then click **OK**.
Go to the **Download Center** to view download detailed information. For details, see "4.9.2.7 Downloading Videos."

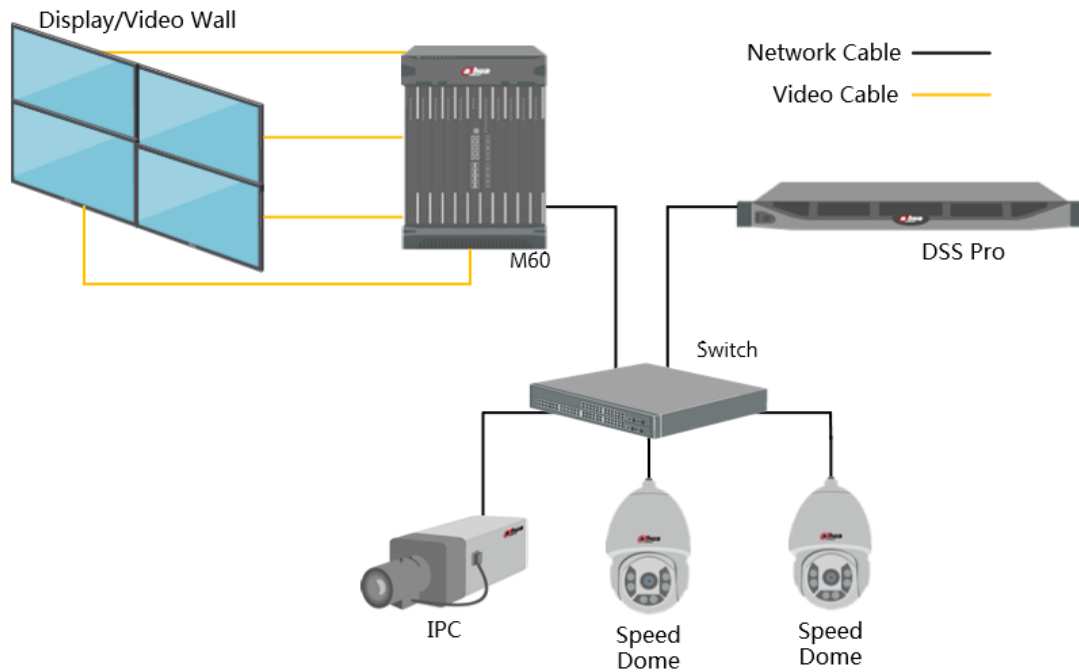
4.10 Video Wall

A video wall, which is consisted of multiple video screens, is used Control Center for displaying videos on the wall, instead of small PC displays.

Complete video wall settings before you can view videos on the wall.

4.10.1 Typical Topology

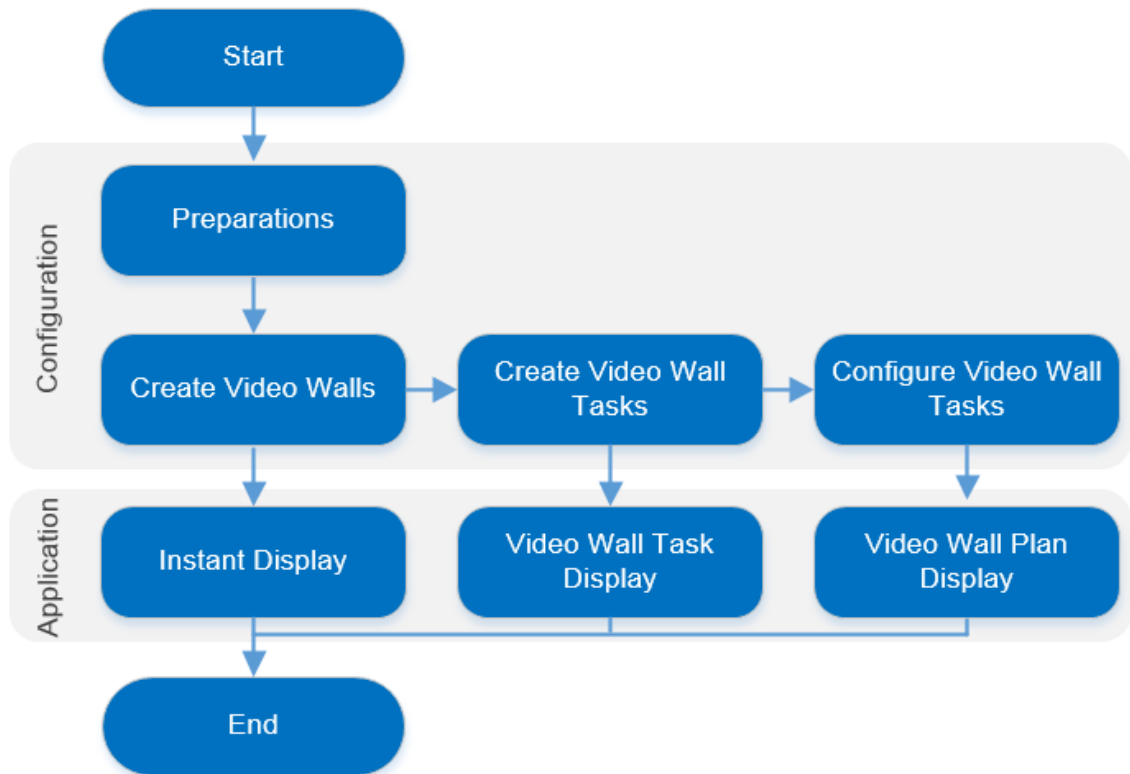
Figure 4-152 Typical topology



- Cameras (IPC) are used to collect video streams. Some cameras support intelligent analysis, for example, face recognition.
- M60 is a decoder. It converts the digital video signal into analog signal for video display. In addition to M60 as shown in the topology, you can also use M70 and other decoder models.
- DSS Pro centrally manages all cameras, decoders and controllers. It supports video wall configuration.

4.10.2 Business Flow

Figure 4-153 Video wall business flow



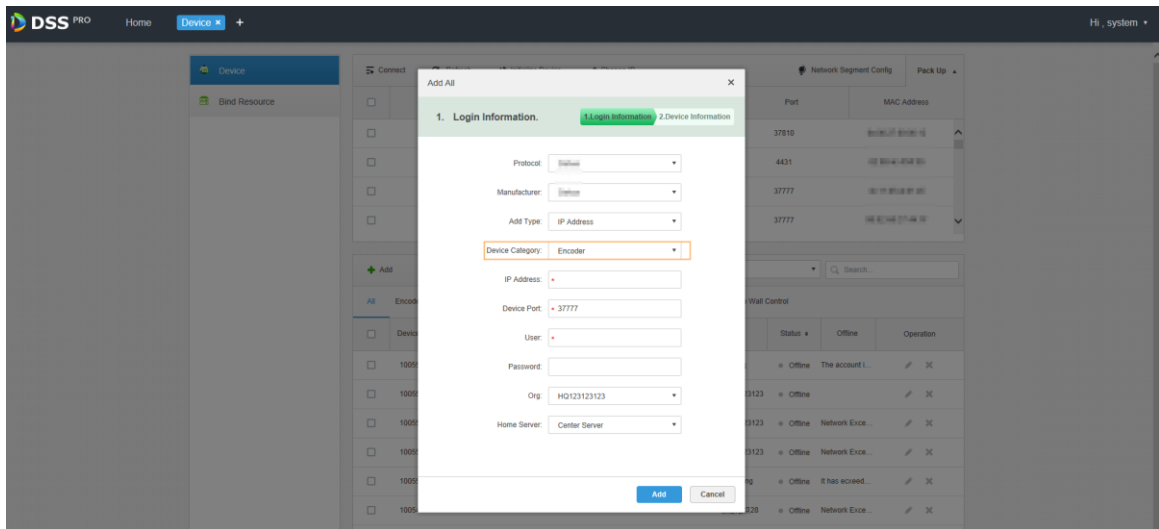
4.10.3 Configuring Video Wall

4.10.3.1 Preparations

To achieve video display on the wall, you need to make sure that:

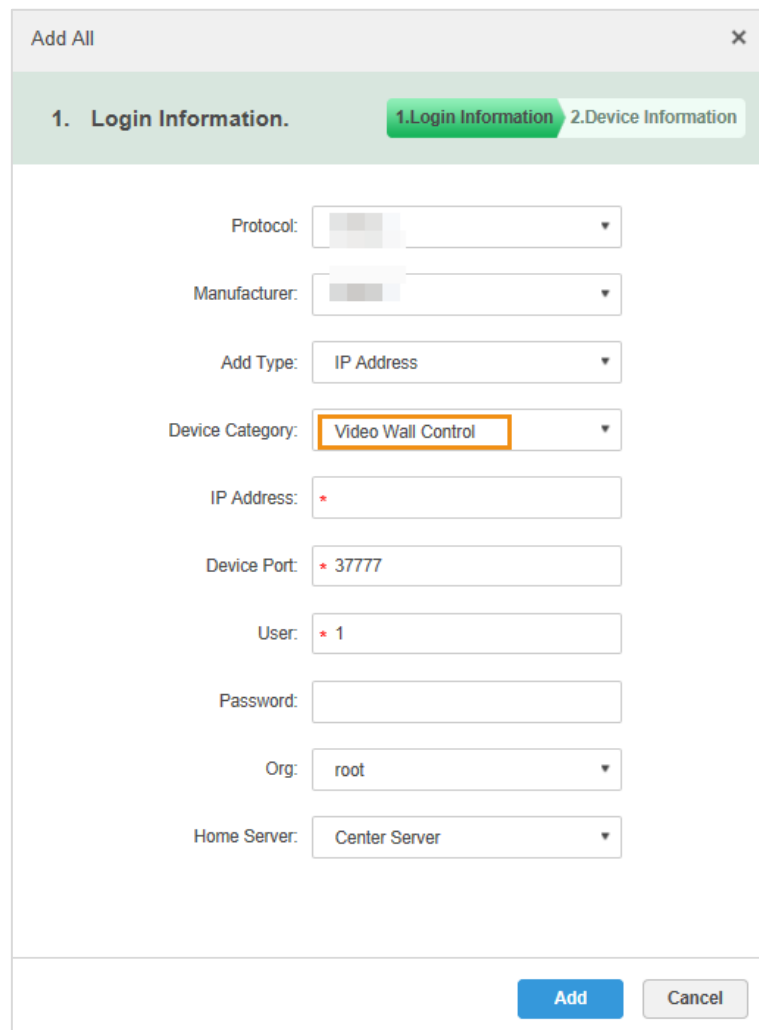
- Cameras, decoders and video wall are well deployed. To deploy, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations." During configuration, note that:
 - ◇ When adding a camera, select **Encoder** for **Device Category**.

Figure 4-154 Set device category



- ◇ When adding a decoder, select **Video Wall Control** for **Device Category**.

Figure 4-155 Add a decoder



- A glimpse of the video wall configuration interface

Figure 4-156 Video wall interface

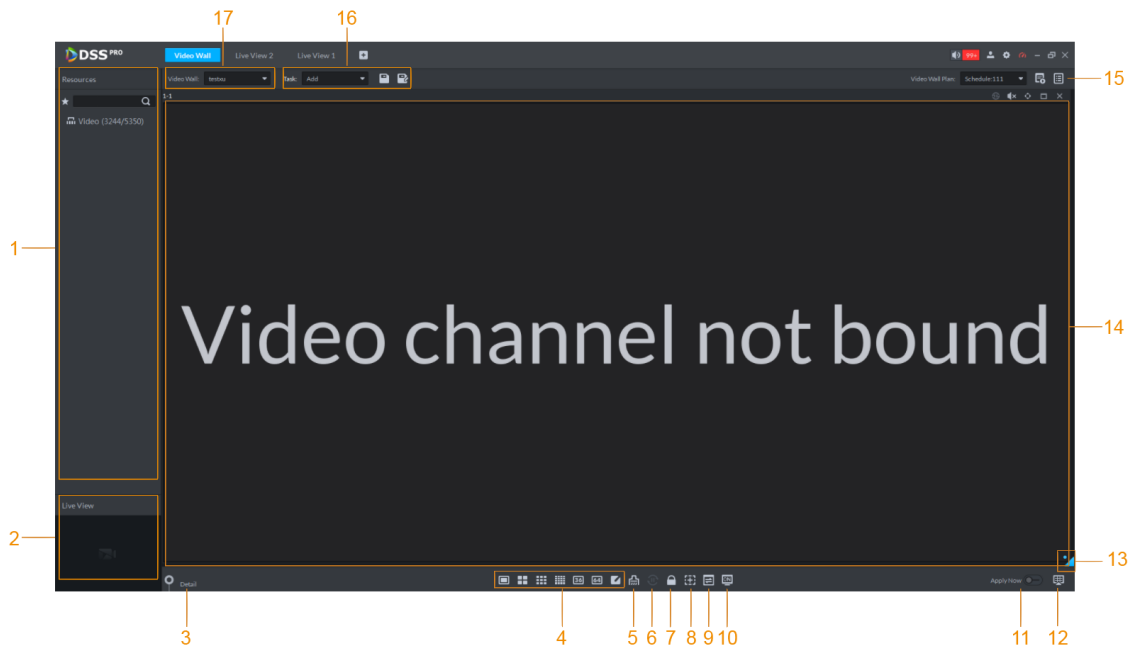



Table 4-44 Description

No.	Name	Function
1	Device Tree	<p>If you enable Show device node in Local config > Basic, the device tree will display devices and all channels. If you clear the Show device node check box, the device tree will only display channels.</p> <p>Click to view the channels in the Favorites folder.</p> <p>Support searching for devices or channels by entering device name or channel name in <input type="text" value="Search.."/></p>
2	Live View	View channel video.
3	Detailed Information	<p>View the screen, window, and channel bound information.</p> <ul style="list-style-type: none"> Click to view live video of the current channel at the bottom left. Click to adjust sequence. Click to delete the video channel on the current window. Click the Stay Time (s) column or click to modify the video play duration of the current channel during tour. Click the Stream column or to modify stream type.
4	Window Split	Set window split mode.
5	Clear	Clear all screens.

No.	Name	Function
6	Start/stop All Tours	Start or stop all tours.
7	Lock Window	Click to lock the window. Operation is not allowed on a locked window.
8	Add Box	Marked the selected window with a red frame.
9	Back Display	View video image of the selected channel window.
10	Screen On/off	Turn a screen on or off.
11	Apply Now	If you enable the function, system automatically outputs the video to the wall after you set the task.
12	Decode to Wall	Click it to manually output the video to the wall.
13	Eagle Eye	View current video wall layout.
14	Video Wall	Video wall area.
15	Video Wall Task	Configure scheduled tasks and tour tasks. See "4.10.3.4 Video Wall Plan" for details.
16	Task Management	Add, save or delete a task.
17	Video Wall Selection	Select a video wall.

4.10.3.2 Adding Video Wall

Add a video wall layout on the platform.

Step 1 Click  on the Web Manager, and select **Video Wall** on the **New Tab** interface.

Step 2 Click **Add Video Wall** or .

Step 3 Enter **Video Wall Name**, and then select a window splicing mode.







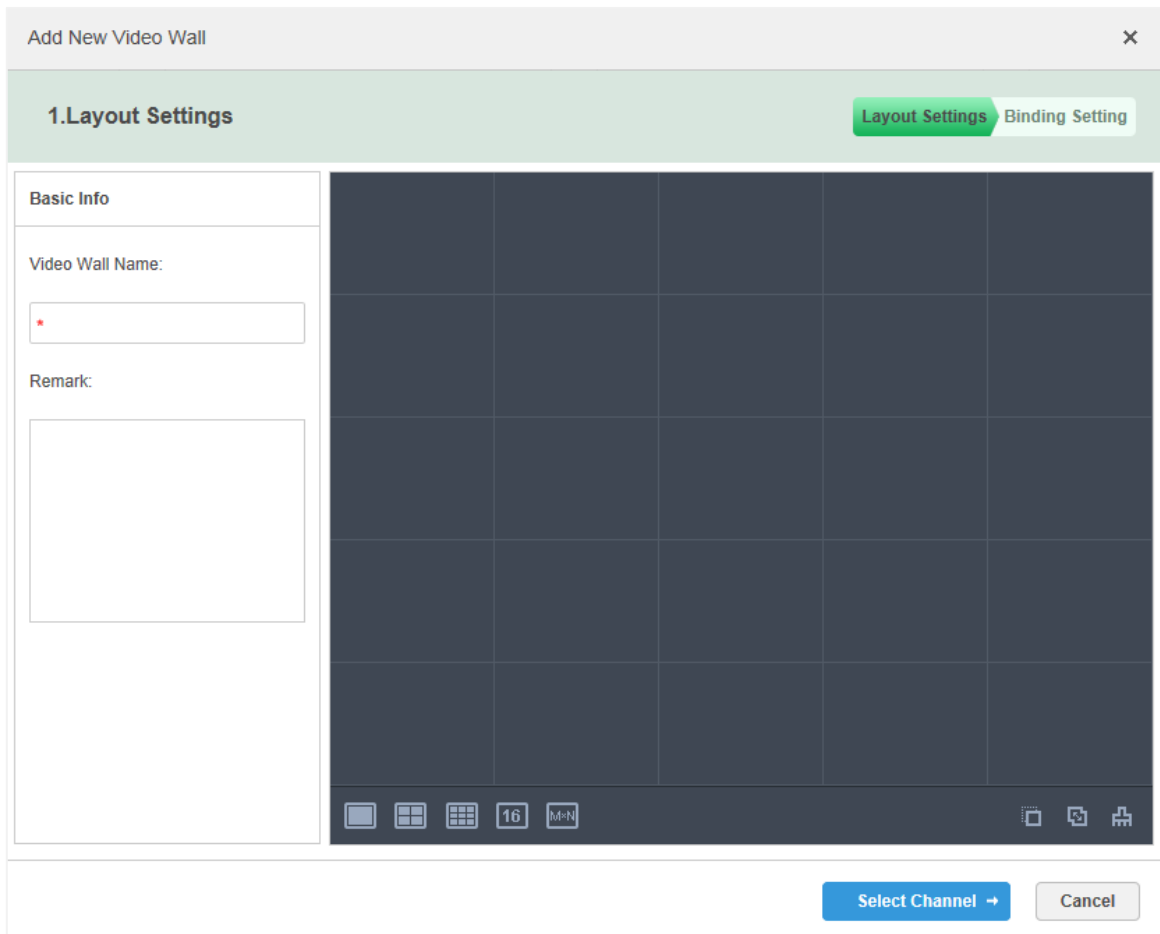
- Select a splicing mode from among 1×1, 2×2, 3×3, 4×4 or set a custom mode by clicking .
- A multi-screen splicing mode is a combined screen by default. You can perform video roaming on it. For example, with a 2×2 combined screen, if you close 3 of them, the other one will be spread out on the combined screen. To cancel combination, click the combined screen, and then click .
- To create a combined screen, press and hold Ctrl, select multiple screens, and then click .
- To clear the created screen, click .

Figure 4-157 Add a video wall



Add New Video Wall

1. Layout Settings

Layout Settings Binding Setting

Basic Info

Video Wall Name:

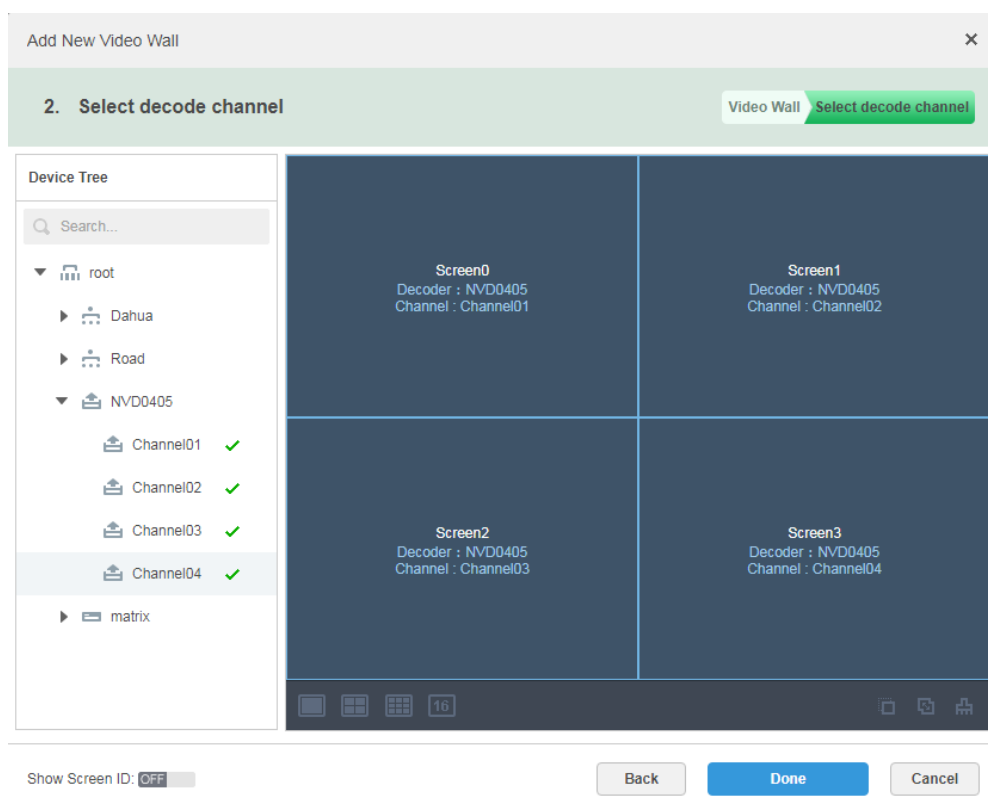
Remark:

Select Channel → Cancel

Step 4 Click **Select Channel**.

Step 5 Select the encoder which needs to be bound in the device tree, and drag it to the corresponding screen.

Figure 4-158 Select a decoding channel




- You can set if it displays ID in the screen, **Show Screen ID: OFF** means that the screen ID has been disabled; click the icon and it becomes **Show Screen ID: ON**, and then it means that screen ID has been enabled.
- Each screen in a combined screen must be bound with a decoding channel.

Step 6 Click **Done**.

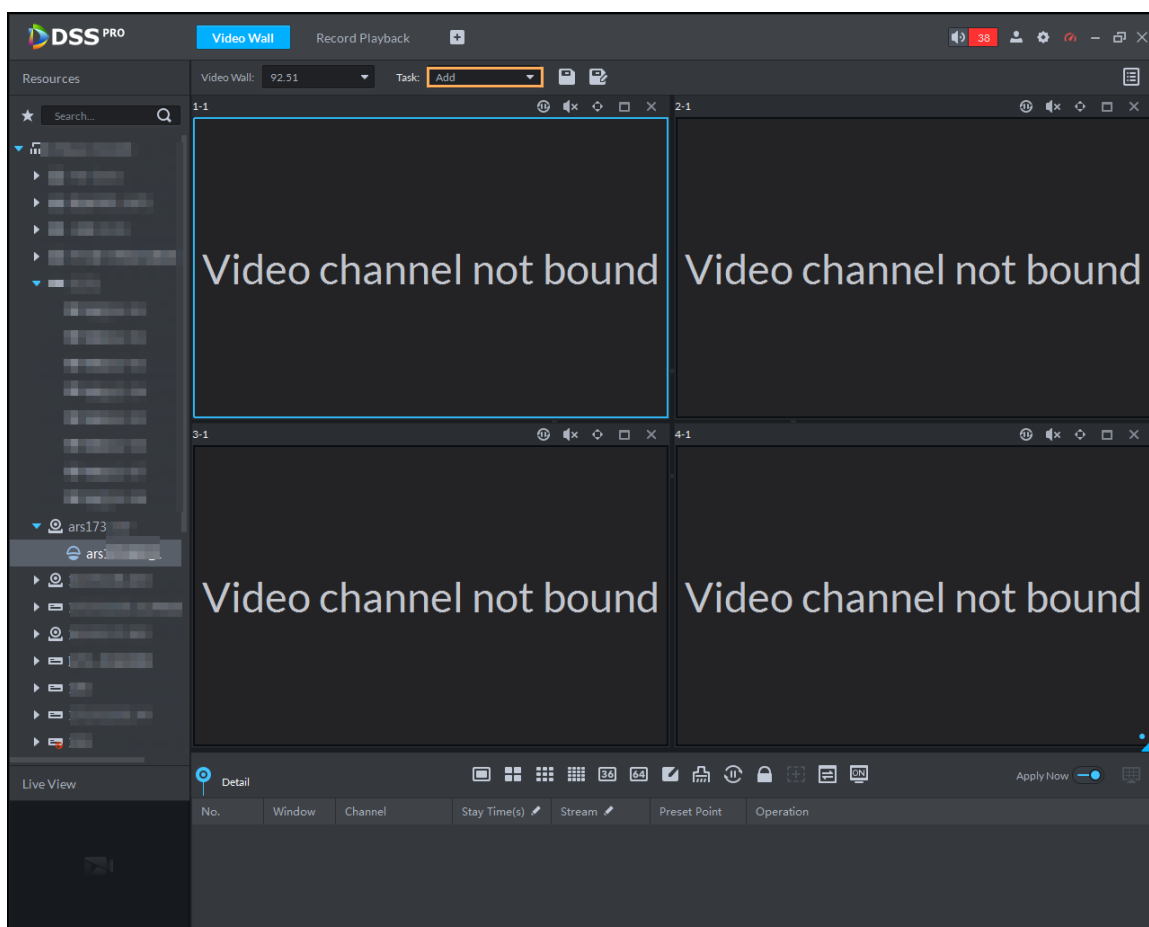
4.10.3.3 Configuring Video Wall Display Tasks


Display videos on the wall manually or in accordance with the pre-defined configuration.

Step 1 Click  on the Control Client, and then select **Video wall**.

Step 2 In the **Task** drop-down list, select **Add**.

Figure 4-159 Add a video wall task



Step 3 Click  to stop video wall display.

Step 4 From the device tree, select a camera, and then drag it to a screen, or select a window, drag the camera to the **Detail** section.



If you do not close video wall display in advance, this action will delete the bound camera and play the selected camera on the wall.

Step 5 Click .



If you have selected an existing task in the **Task** drop-down list, this action will refresh the configuration of the selected task. The task will be played on the wall immediately.

Step 6 Name the task, and then click **OK**.

- During video wall display of a task, if you have rebound the video channel, click




to start video wall display manual.

- During video wall display, click  or  to stop or start tour display.

4.10.3.4 Configuring Video Wall Plans

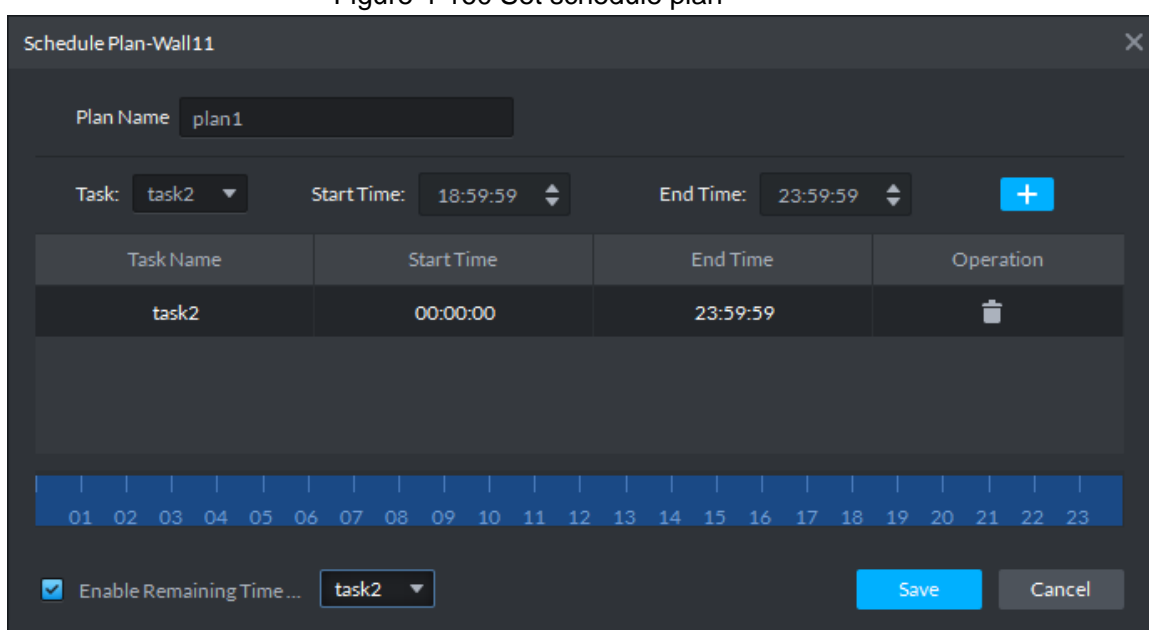
4.10.3.4.1 Configuring Timed Plans

Configure a time schedule of tasks, and then you can play the plan on the wall. If the schedule is not completely filled up with the tasks, you can define other tasks for the empty section.

Step 1 On the **Video Wall** interface, click  at the upper-right corner.

Step 2 Hover over , and then select .


Figure 4-160 Set schedule plan



Schedule Plan-Wall11

Plan Name: plan1


Task: task2 Start Time: 18:59:59 End Time: 23:59:59

Task Name	Start Time	End Time	Operation
task2	00:00:00	23:59:59	

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Enable Remaining Time... task2 Save Cancel

Step 3 Enter the plan name.

Step 4 Select a video task, set start time and end time, and then click .

Repeat this step to add more tasks. The start and end time cannot be repeated.



Select the **Enable remaining time schedule** check box, and then set the task. The video wall displays the selected task during the remaining period.

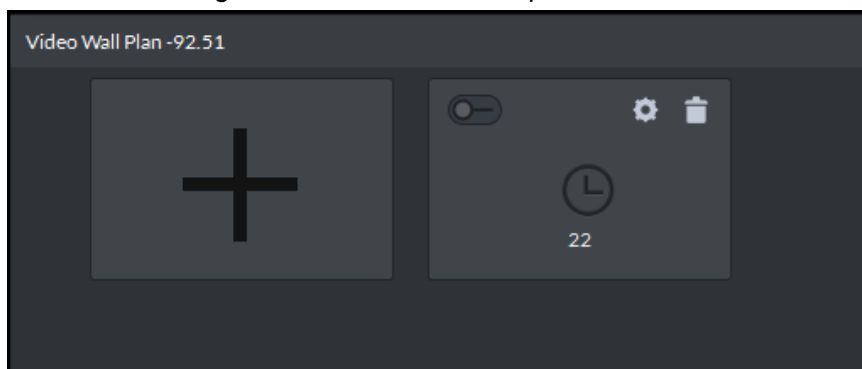
Figure 4-161 Task time

Task Name	Start Time	End Time	Operation
1	05:00:00	10:59:59	
1	10:59:59	19:59:59	

Step 5 Click **Save**.

Step 6 Click to start the plan.

Figure 4-162 Enable timed plan



Operations

- Modify plan: Click of the corresponding plan, it is to modify plan..
- Delete plan: Click of the corresponding plan, it is to delete the plan.

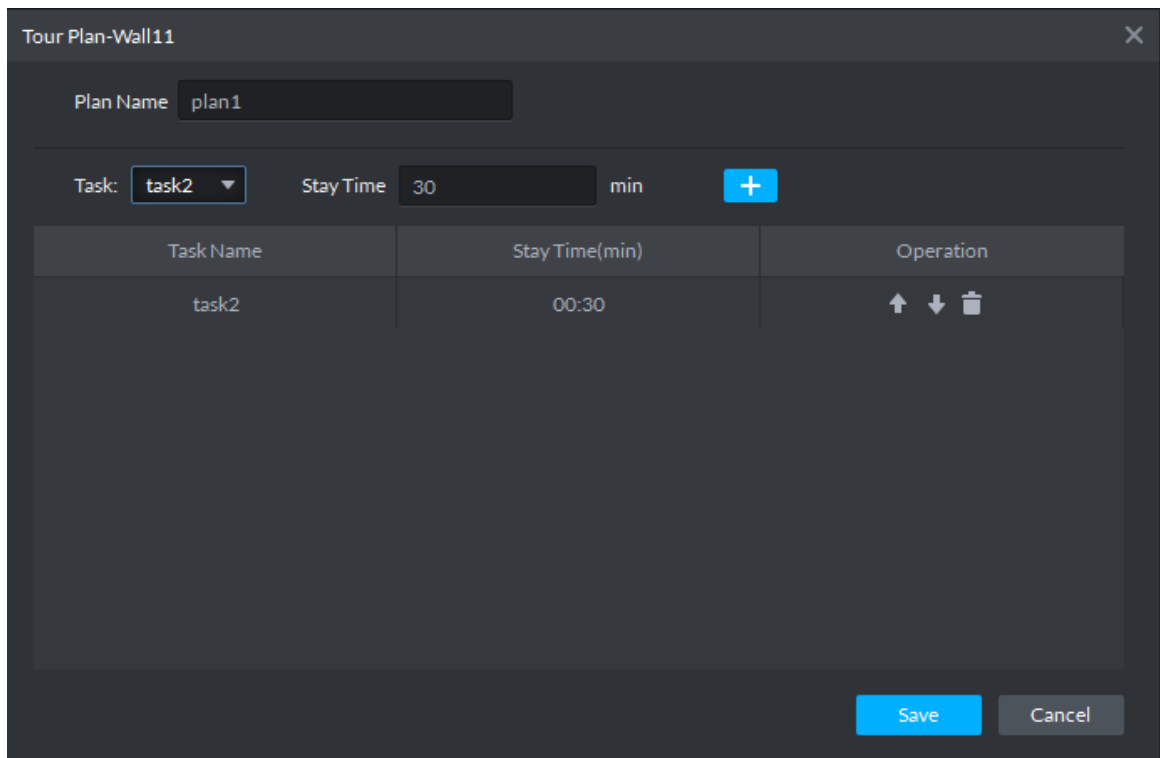
4.10.3.4.2 Configuring Tour Plans


After setting video wall tasks, you can configure the sequence and interval of tasks so that they can automatically play in turn on the wall.

Step 1 On the **Video Wall** interface, click at the upper-right corner.

Step 2 Hover over , and then select .

Figure 4-163 Tour plan



Step 3 Enter task name, select a video task and then set stay time. Click .

Repeat this step to add more tasks.





Click  to adjust task sequence; click  to delete task.

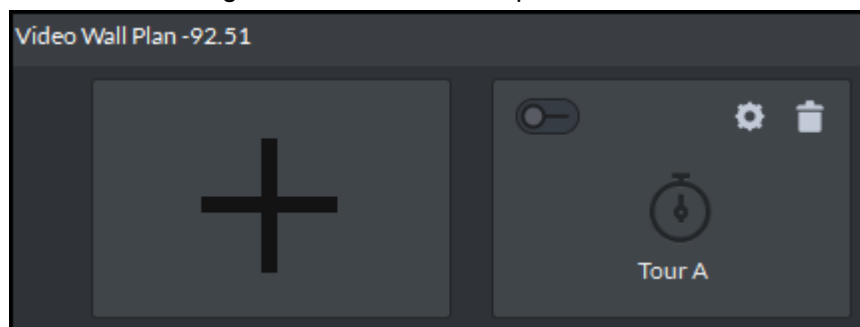
Figure 4-164 Tour information

Task Name	Stay Time(min)	Operation
1	00:30	↑ ↓ 🗑️
1	00:30	↑ ↓ 🗑️



Step 4 Click **Save**.

Step 5 Click  to start the tour plan.

Figure 4-165 Enable tour plan



Operations

- Modify plan: Click  of the corresponding plan, it is to modify plan.
- Delete plan: Click  of the corresponding plan, it is to delete the plan.


4.10.4 Video Wall Applications



Make sure that decoder video ports are connected to the video wall screens.

4.10.4.1 Instant Display

Drag a camera to the video wall screen for instant display on the wall.

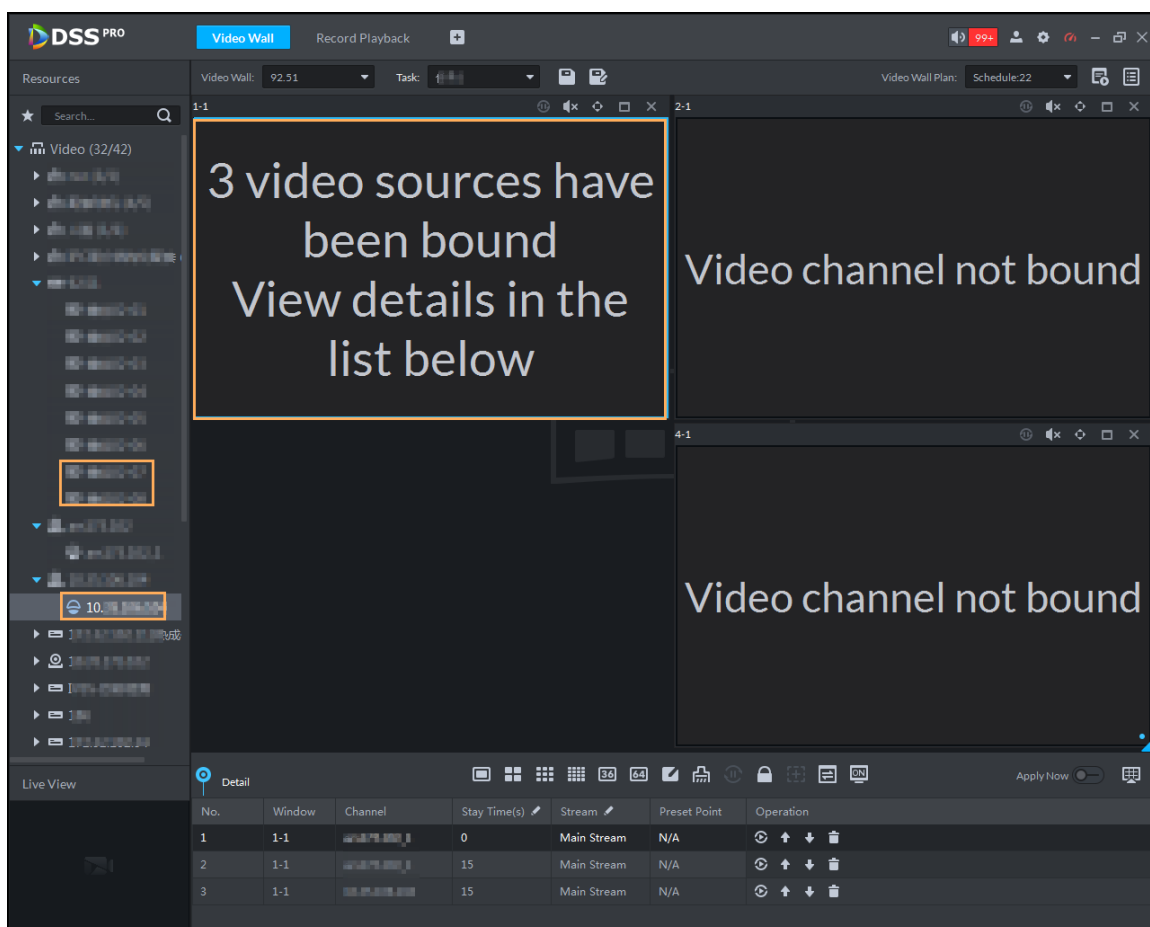
Step 1 Log in to the Control Client, click , and then select **Video wall**.

Step 2 In the **Video Wall** drop-down list, select a video wall.

Step 3 Click  to start video wall display.

Step 4 Drag a camera from the device tree to a screen, or select a window and drag the camera to the **Detail** section.

Figure 4-166 Bind video channel

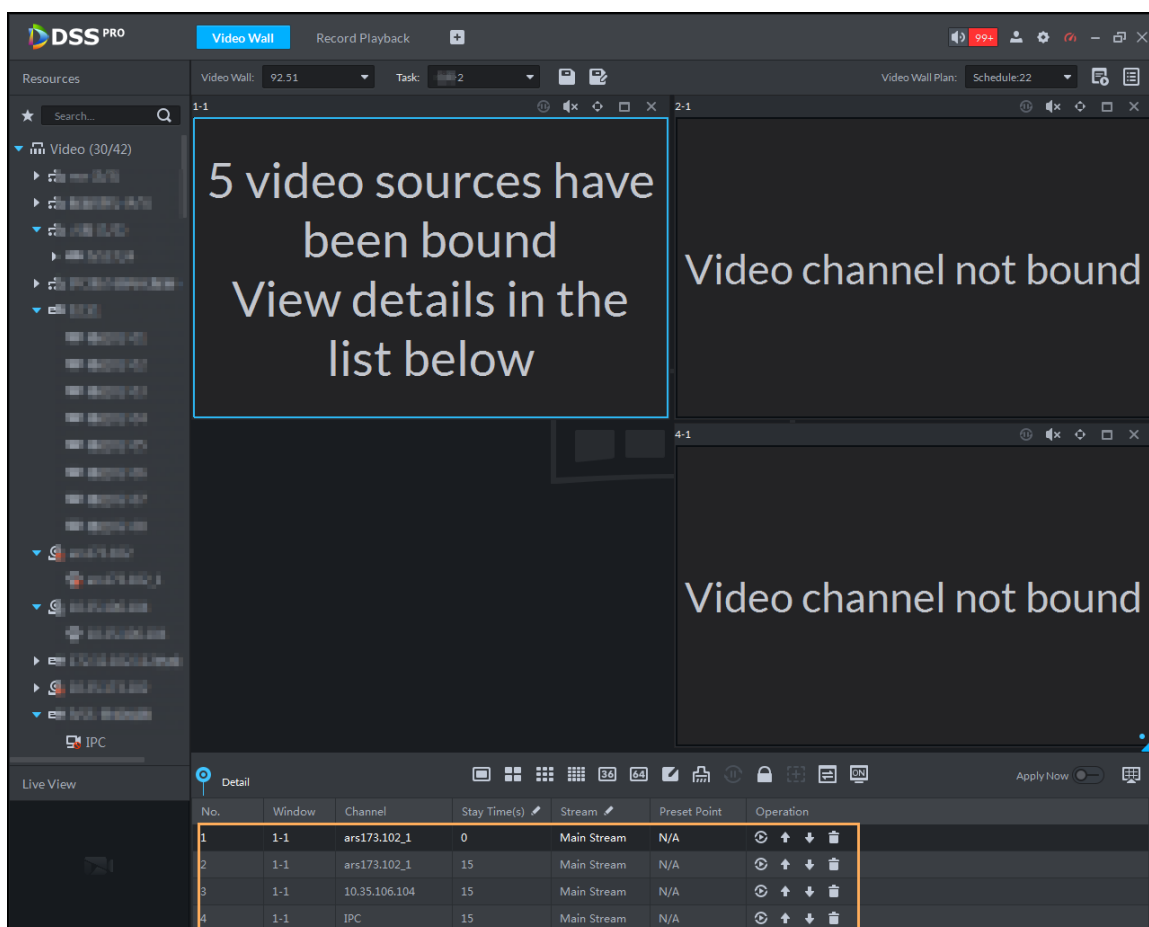


For a fisheye camera, right-click it to select the installation mode for fisheye dewarp.

Step 5 Select a screen, and then click **Detail** to view detailed information about the screen and channel, including stream type, preset and display sequence.

- Click to view live video of the current channel at the bottom left.
- Click to adjust sequence.
- Click to delete the video channel on the current window.

Figure 4-167 Set video channel parameters




4.10.4.2 Video Wall Task Display

Display a pre-defined task on video wall.








Make sure that there are pre-defined tasks.

Step 1 Log in to the Control Client, click , and then select **Video wall**.

Step 2 In the **Task** drop-down list, select a task.

Step 3 Operations available.

- After changing the video channel that is being displayed, click  at the lower-right corner before you can see the effect on video wall.
- Click   to pause or stop.
- Select a screen, and then click **Detail** to view detailed information about the screen and channel, including stream type, preset and display sequence.
 - ◇ Click  to view live video of the current channel at the bottom left.
 - ◇ Click  to adjust sequence.

- ◇ Click  to delete the video channel on the current window.

4.10.4.3 Video Wall Plan Display


Display a pre-defined plan on video wall.



Make sure that there are pre-defined plans. For details, see "4.10.3.4 Configuring Video Wall Plans."

The video wall automatically works as the plans have been configured. To stop the current plan,

click  at the upper-right corner of the **Video Wall** interface, and then it changes to .

Click  to start again.

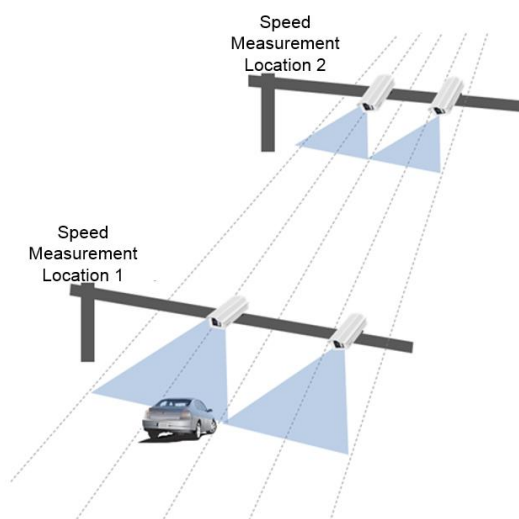
4.11 Traffic

Use this feature for vehicle speed measurement, and traffic violation and vehicle flow search.

- Interval speed measurement

Vehicles are detected when they get through the speed measurement locations. According to distance and time, DSS Pro calculates the average speed of vehicles, and then determines whether a vehicle is speeding or driving too slow.

Figure 4-168 Interval speed measurement



- Violation

If a violation is detected at the measurement location, the system will upload the vehicle information and snapshots to DSS Pro. DSS Pro supports violation records search.

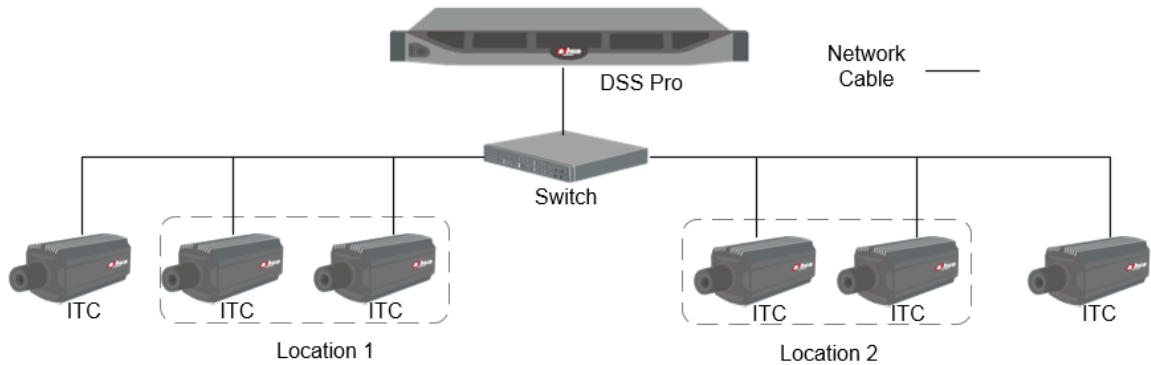
- Traffic flow

The cameras at the traffic monitoring locations analyzes traffic situation in the relevant lanes and uploads the results to DSS Pro. The results are uploaded once per second by

default. And you can modify that frequency on the device (1 to 250 times per second). The results include the total vehicle volume, average speed, lane occupancy ratio and numbers of different vehicle types. Vehicle types include car, passenger vehicle, small truck, and large truck. Vehicle traffic data retention period is at least 2 years.

4.11.1 Typical Topology

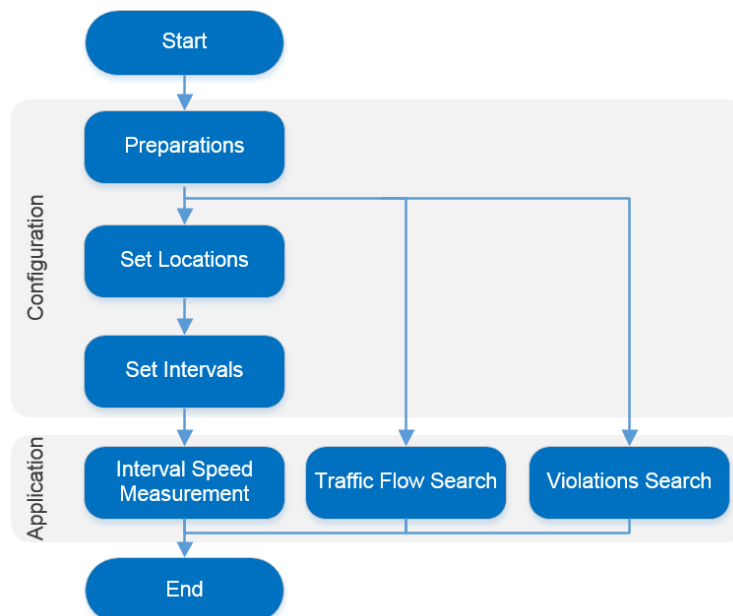
Figure 4-169 Typical topology



- The ITC cameras capture vehicle information.
- DSS Pro centrally manages all devices, calculates average speed, triggers speeding or low-speed alarms, and provides traffic and violation record search.

4.11.2 Business Flow

Figure 4-170 Traffic monitoring business flow



4.11.3 Configuring Traffic Monitoring

4.11.3.1 Preparations

Make sure that the following preparations have been made:

- ITC cameras are well deployed, and the traffic flow analysis function and violation events are well configured. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding an ITC camera, select **ANPR** for device category, and then select **ANPR Device** for device **Type**.

Figure 4-171 Add ITC camera (1)

1. Login Information. 1.Login Information 2.Device Information

Protocol: [dropdown]

Manufacturer: [dropdown]

Add Type: IP Address [dropdown]

Device Category: ANPR [dropdown]

IP Address: * [text input]

Device Port: * 37777 [text input]

User: * [text input]

Password: [password field]

Org: root [dropdown]

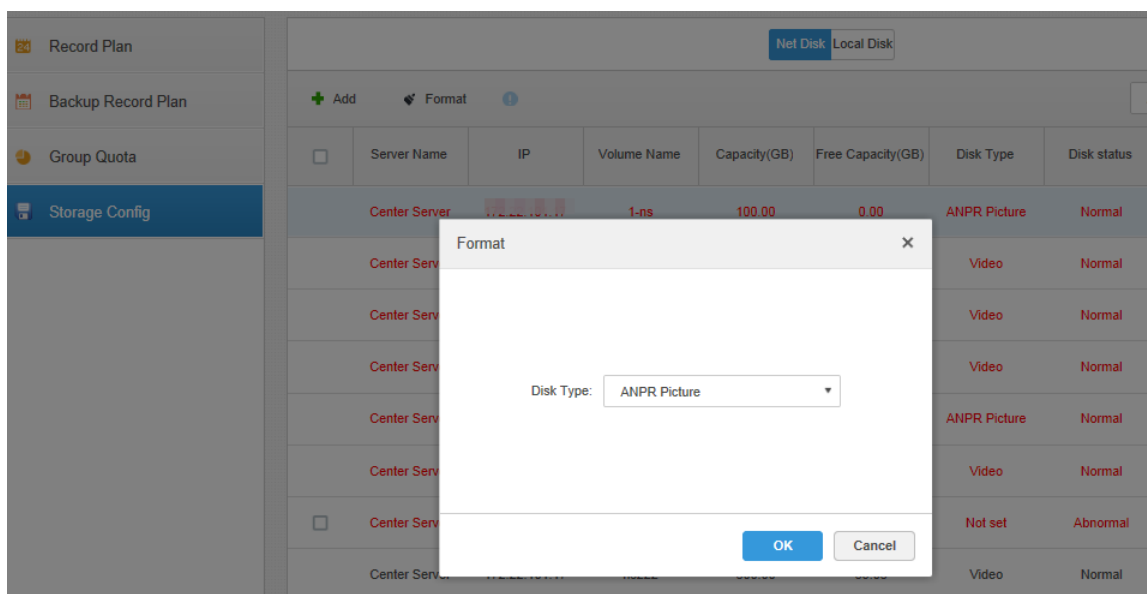
Home Server: Center Server [dropdown]

Add Cancel

Figure 4-172 Add ITC camera (2)

- ◇ The vehicle snapshots are only stored in the **ANPR Picture** disks. On the **Storage** interface, configure at least one **ANPR Picture** disk. Otherwise vehicle pictures cannot be viewed.

Figure 4-173 Disk type



4.11.3.2 Configuring Location

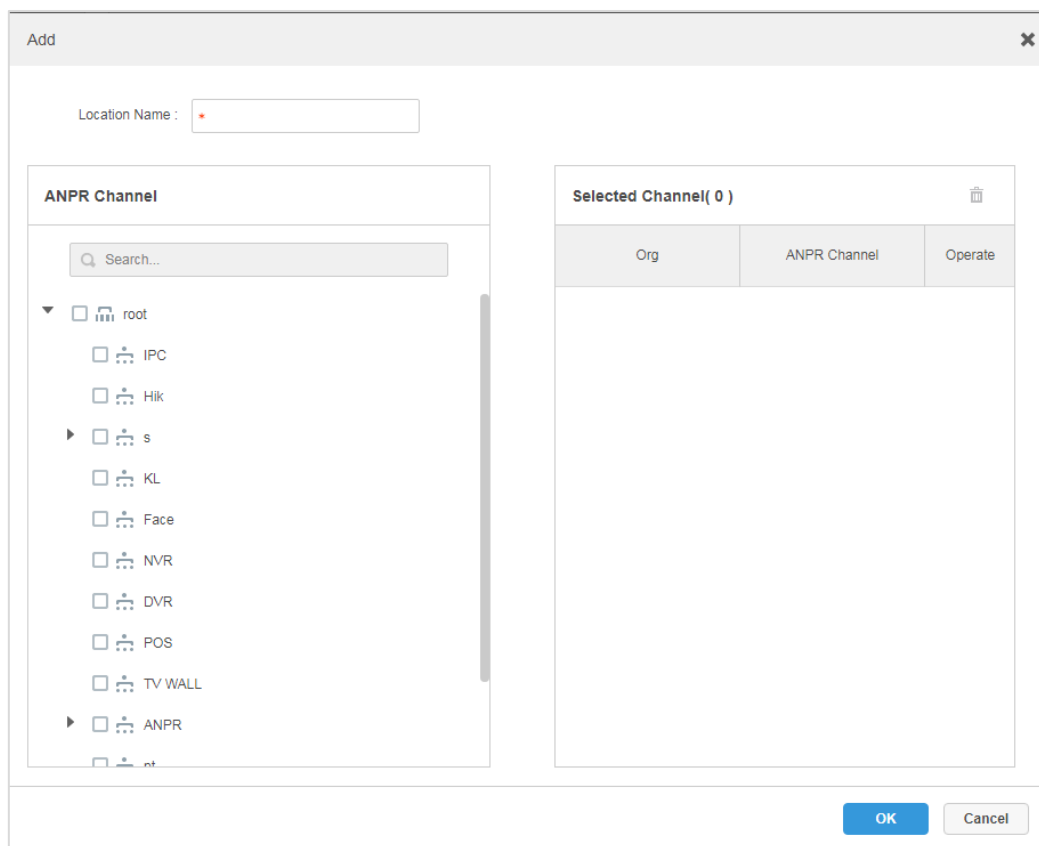
Configure locations for speed measurement. One location is equipped with one or more ANPR cameras.

Step 1 Click **+** on the Web Manager, and then select **Average Speed** on the **New Tab** interface.

Step 2 Click the **Location Config** tab.

Step 3 Click **Add** to open the **Add** interface.

Figure 4-174 Add a location



Step 4 Enter **Location Name**, select one or several ANPR channels (multiple ANPR cameras for monitoring lanes of the same direction) as location.



One ANPR channel can only exist in one location. The ANPR camera which has been configured with location cannot be selected again.

Step 5 Click **OK**.

4.11.3.3 Configuring Location Interval

Configure location interval parameters including distance, and speed range, so that the platform can calculate vehicle speed and determine violations accordingly.

Step 1 Click **+** on the Web Manager, and then select **Region Setup** on the **New Tab** interface.

Step 2 Click the **Region Setup** tab.

Step 3 Click **Add** to open the **Add** interface.

Figure 4-175 Add a region


The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Region Name :** A text input field with a red asterisk (*) indicating it is required.
- Start Location :** A dropdown menu with "hou-23" selected.
- End Location :** A dropdown menu with "hou-23" selected.
- Length(m) :** A text input field with a red asterisk (*) indicating it is required.
- Big Vehicle Speed Li... :** A slider control ranging from 0 to 220.
- Small Vehicle Speed ... :** A slider control ranging from 0 to 220.
- Turn On/Off :** A toggle switch currently set to "OFF".

At the bottom right of the dialog, there are two buttons: "OK" (highlighted in blue) and "Cancel".

Step 4 Set the parameters of region setup.

Table 4-45 Parameters

Parameter	Description
Region Name	Name the region
Start Location	Select locations.
End Location	 <p>If a vehicle is not detected passing the end location after the maximum travel time (region section length divided by minimum speed limit), the vehicle record will be removed, and there will be no speed information for it.</p>
Length (m)	Set the length of section.
Big Vehicle Speed Limit (km/h)	Set the speed limit for large and small vehicles. Set minimum speed and maximum speed respectively.

Parameter	Description
Small Vehicle Speed Limit (km/h)	
Turn on/off	Enable or disable the region configuration.

Step 5 Click **OK**.

4.11.4 Traffic Management Applications

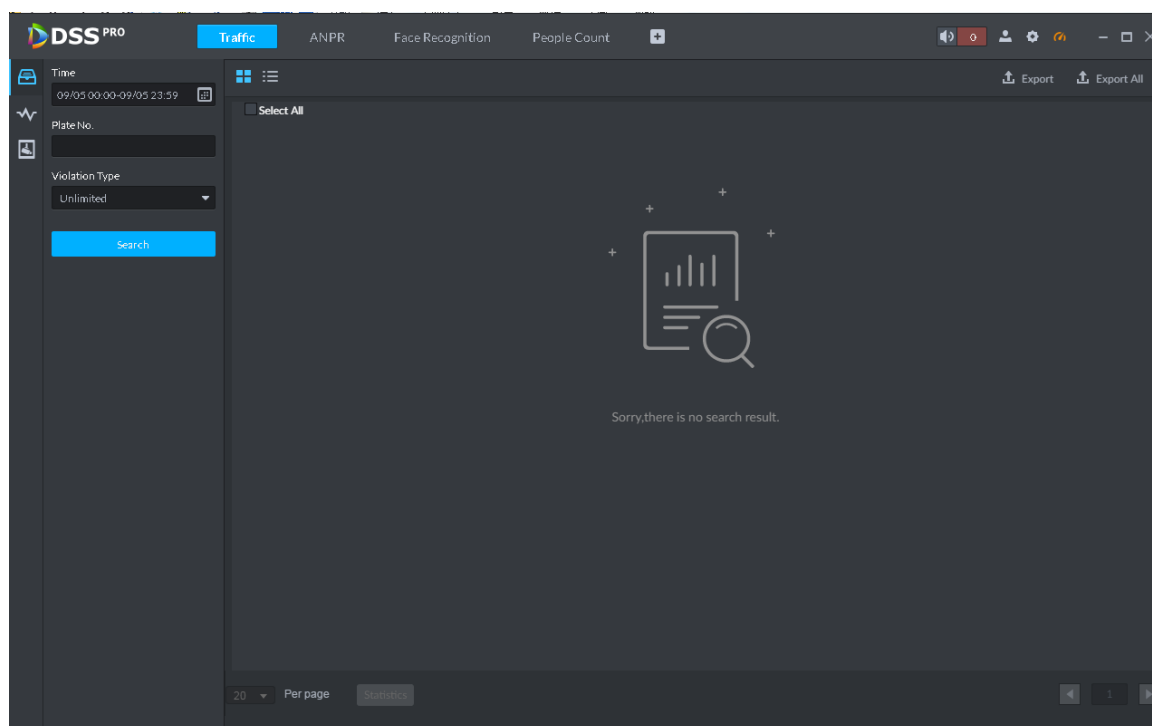
4.11.4.1 Searching for Violation Records

Search for vehicle violation information.

Step 1 Click  on the Control Client, and then select **Traffic**.

Step 2 Click .

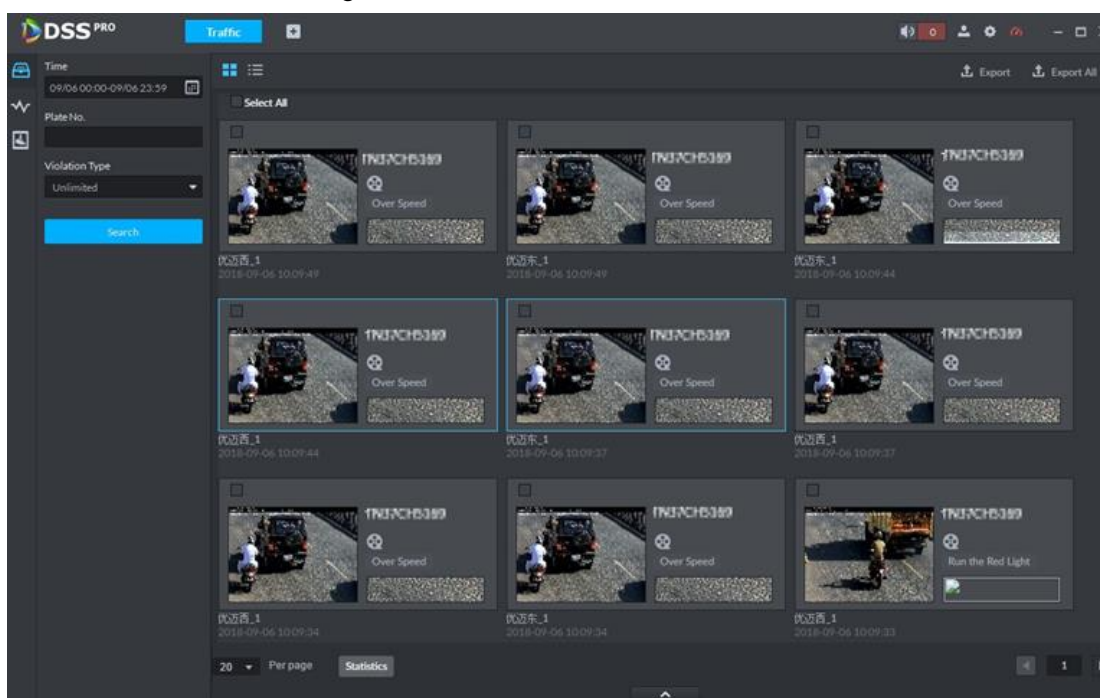
Figure 4-176 Violation record search



Step 3 Set search criteria. It includes time, plate number, and violation type.

Step 4 Click **Search**.

Figure 4-177 Violation records



Step 5 View and export violation records.



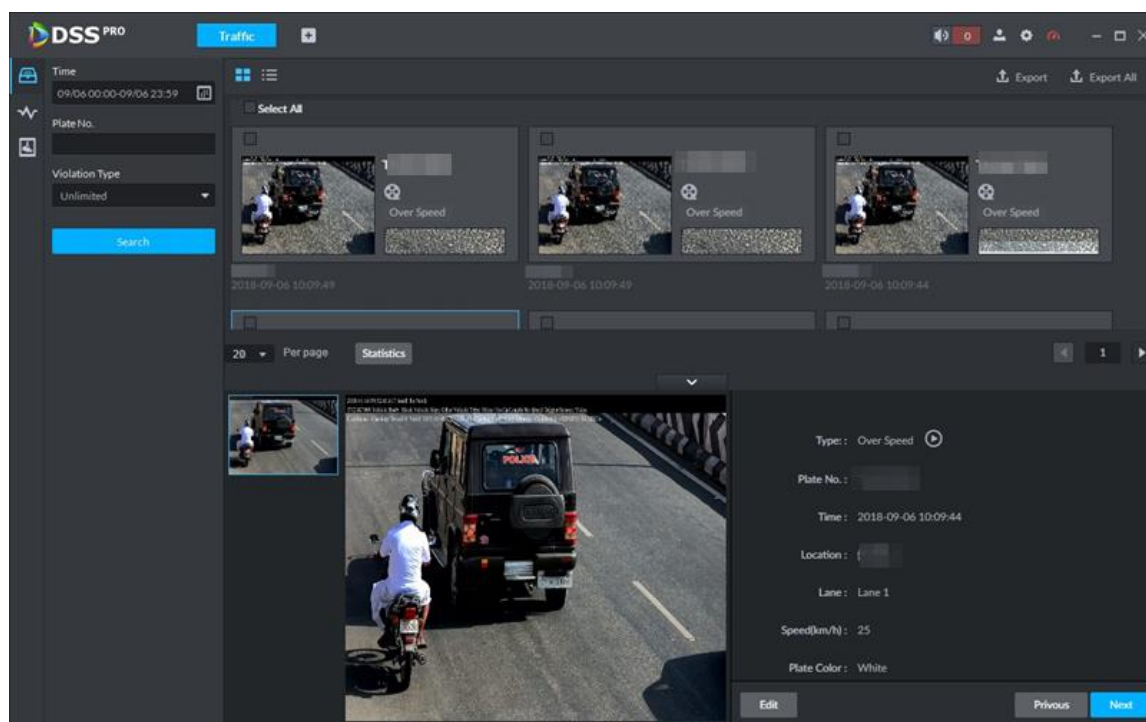
- Select the view mode () or list mode ().
- Double-click a violation record to view detailed vehicle information.


Figure 4-178 Vehicle record



- Select a violation record, and then click **Export** to export selected violation information. To export all searches, click **Export All**.

4.11.4.2 Vehicle Flow Search

View the history traffic flow of a lane.

Step 1 Click  on the Control Client, and then select **Traffic**.


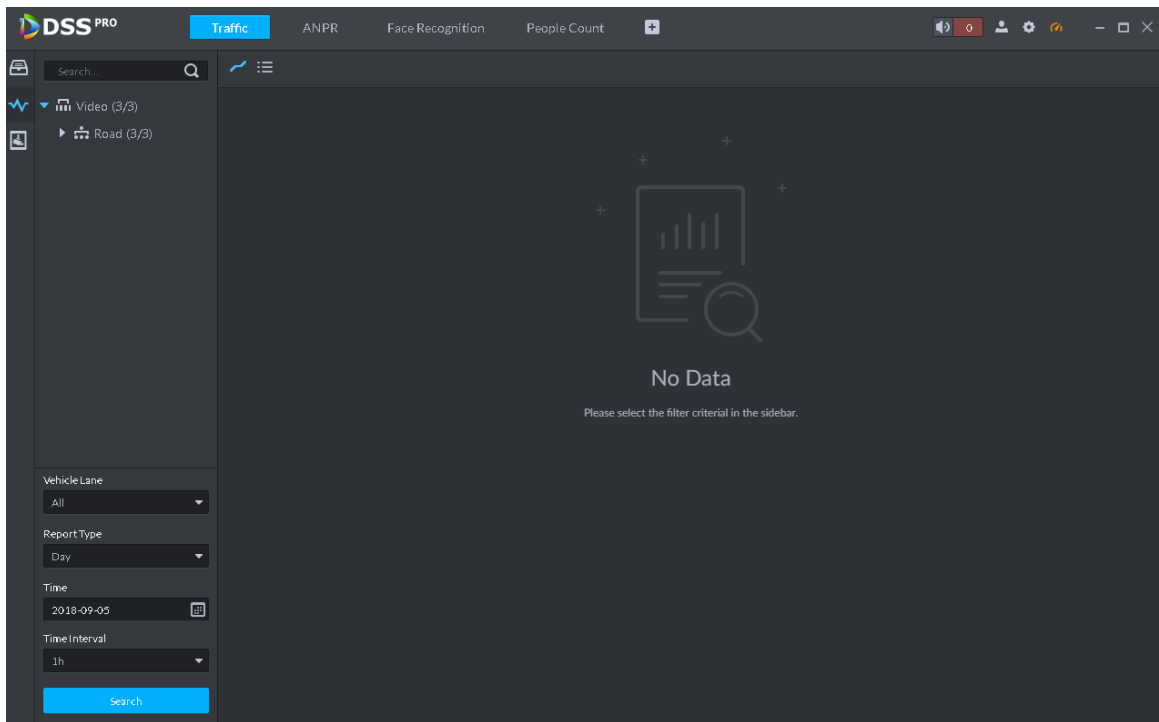
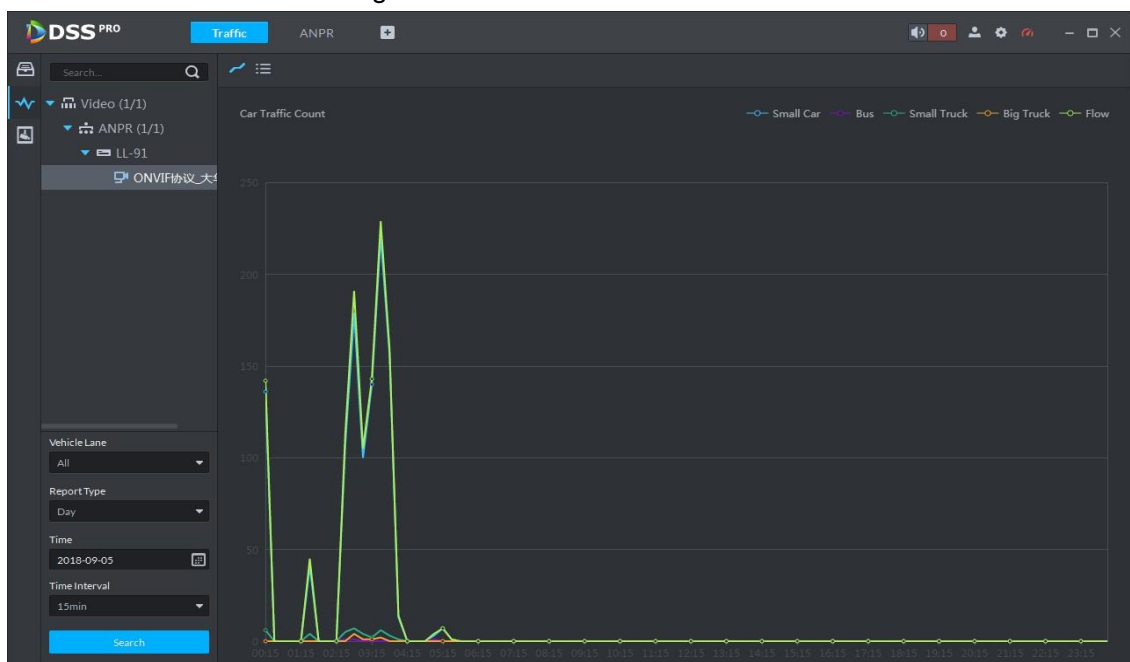
Step 2 Click .

Figure 4-179 Vehicle flow search





Step 3 Select device channel, plate number, report type, interval, and then click **Search**.

Figure 4-180 Search result



View and export the searches.

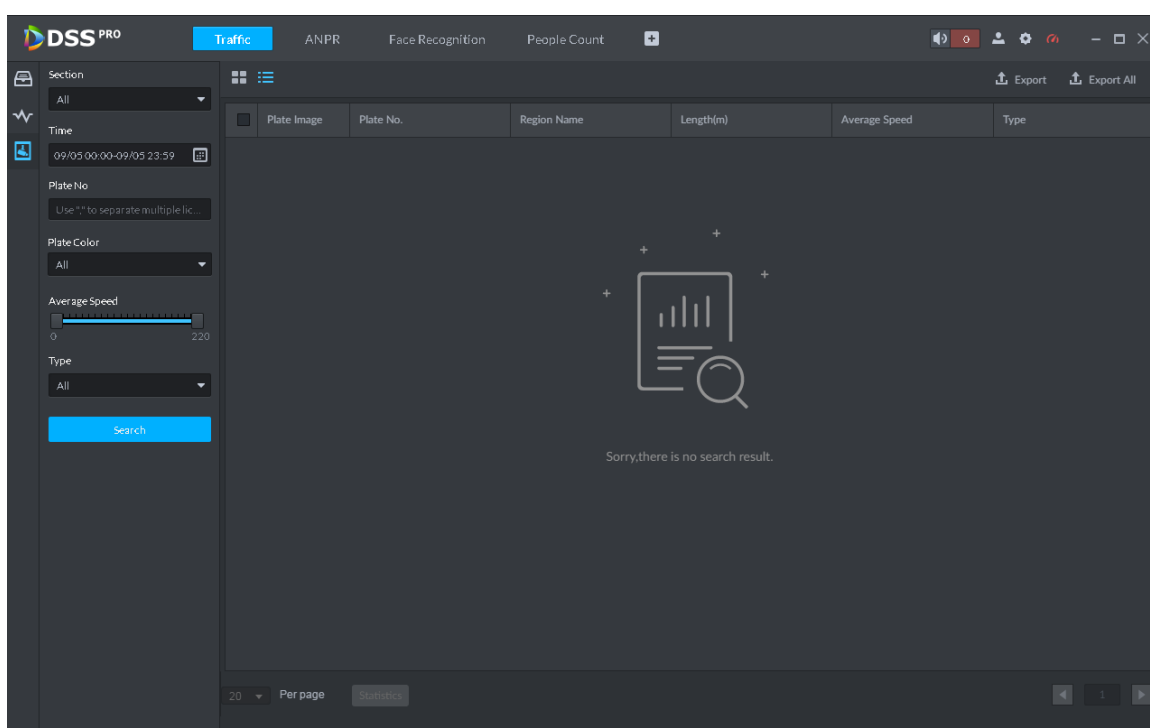
- Click the line chart mode () or list mode ()
- To export all searches, click **Export All**.

4.11.4.3 Vehicle Speed Search

Step 1 Click  on the Control Client, and then select **Traffic**.

Step 2 Click .

Figure 4-181 Vehicle speed search

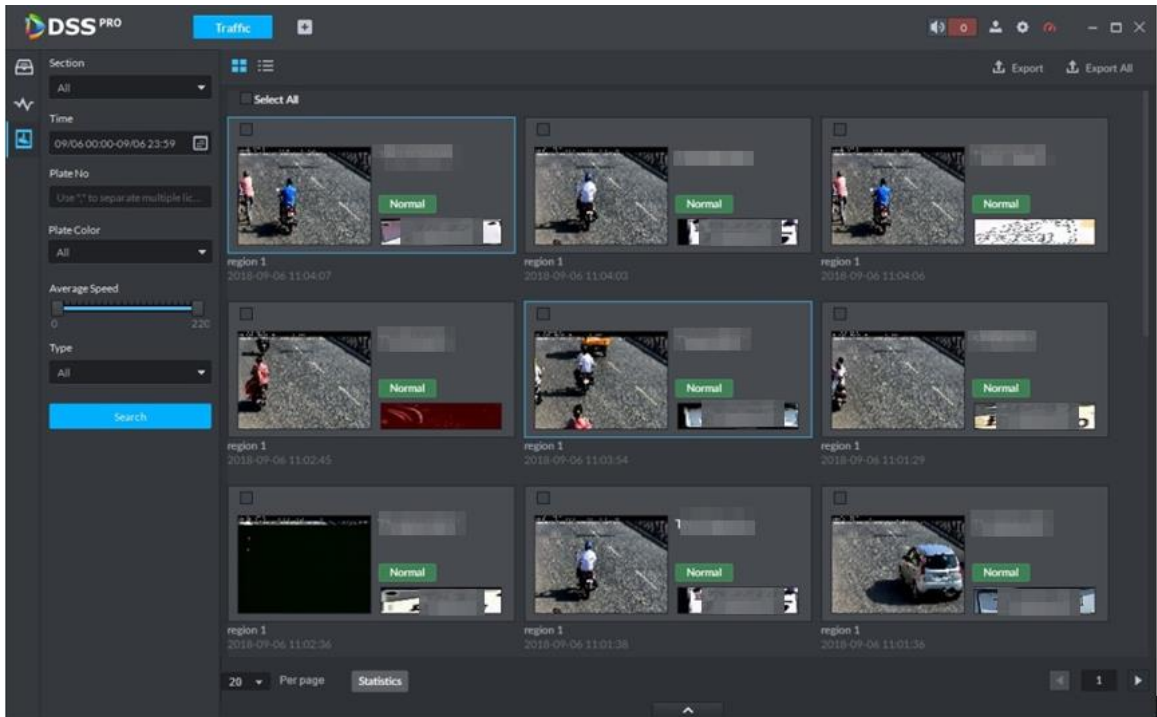


Step 3 Select search range, time, lane number, plate color, average speed, type, and then click **Search**.



In thumbnail mode, system displays the earliest image of the current range as the main image by default.

Figure 4-182 Search results



View and export the searches.

- Click the view mode () or list mode ().
- Double-click a record to view detailed information.

Figure 4-183 Vehicle details

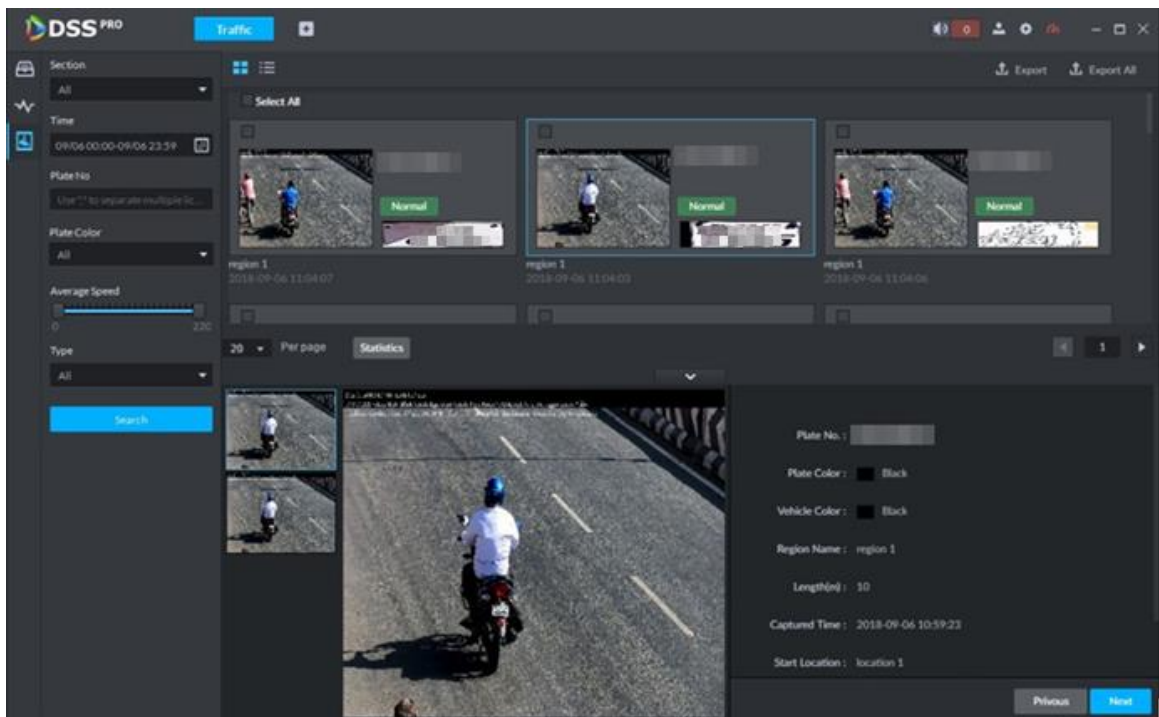
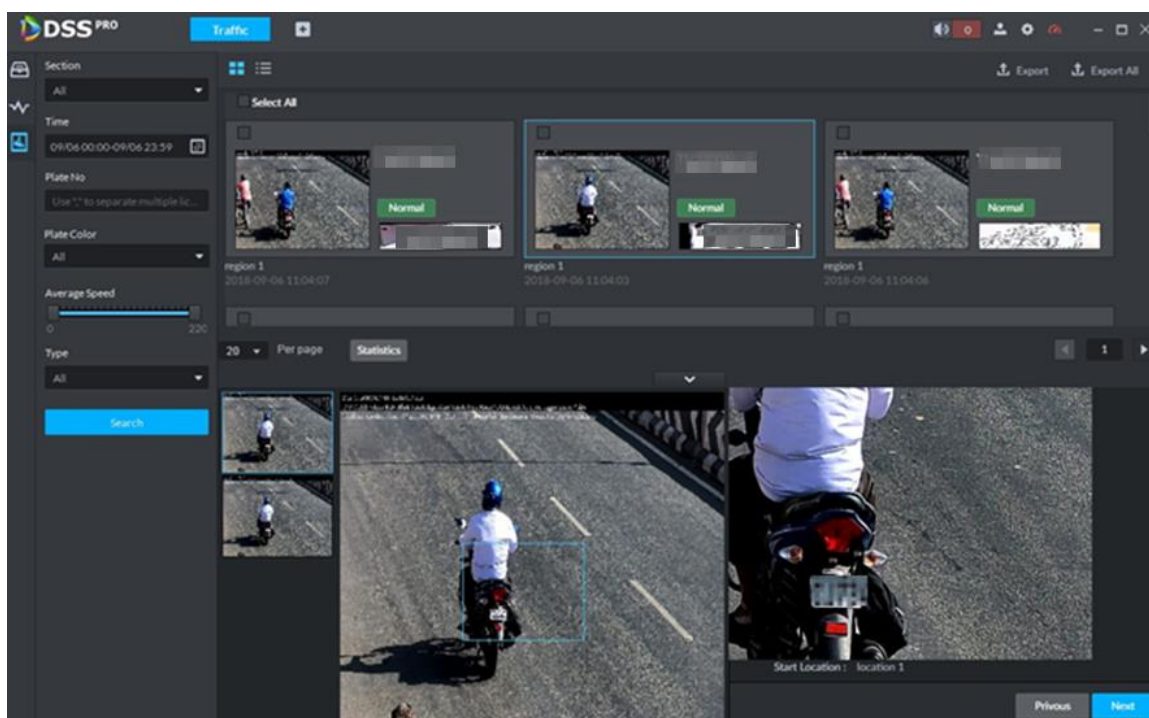


Figure 4-184 large image for details



- Select a record, and then click **Export** to export selected vehicle information. To export all searches, click **Export All**.

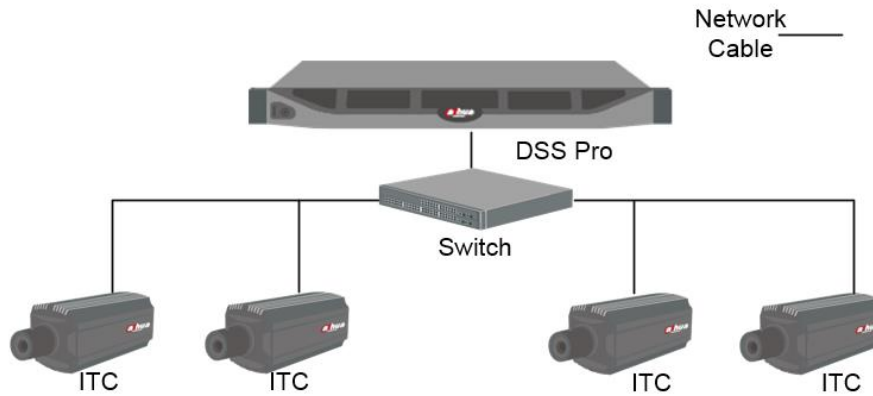
4.12 ANPR

View automatic number plate recognition in real time or search for records. You can view the moving track of a vehicle. This is useful for road monitoring.

- Automatic number plate recognition
DSS Pro displays vehicle snapshots and ANPR results in real time.
- Vehicle records
Search for vehicle records according to the filtering conditions you have set.
- Vehicle track
According to the ANPR camera locations that a vehicle has passed through, DSS Pro displays the driving track of the vehicle on the map.
- Arm record
Search for records of vehicles on the restricted list.

4.12.1 Typical Topology

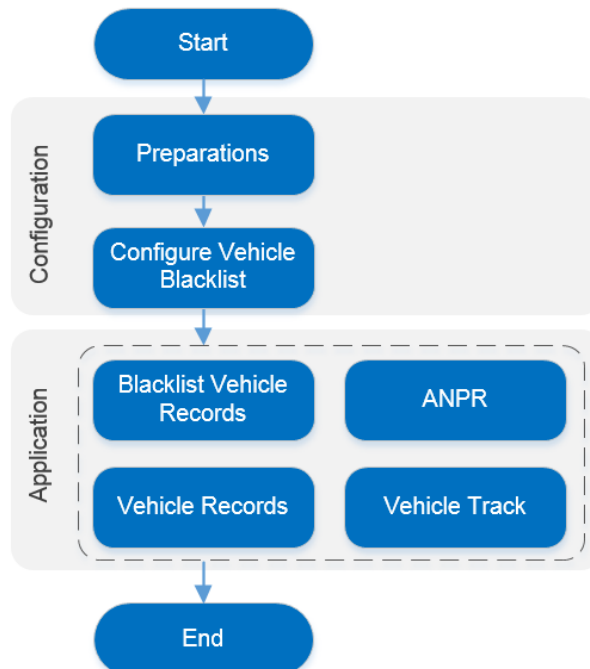
Figure 4-185 Typical topology



- ANPR cameras (ITC camera) capture and recognize vehicles.
- DSS Pro centrally manages ANPR cameras, receives and displays vehicle snapshots and information uploaded by the cameras.

4.12.2 Business Flow

Figure 4-186 Automatic number plate recognition



4.12.3 Configuring ANPR

4.12.3.1 Preparations

Make sure that the following preparations have been made:

- ANPR cameras are well deployed, and the ANPR function is well configured. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding an ITC camera, select **ANPR** for device category, and then select **ANPR Device** for device **Type**.

Figure 4-187 Add ITC camera (1)

The screenshot shows a web-based configuration form titled "1. Login Information." with a progress indicator showing "1.Login Information" and "2.Device Information". The form contains the following fields:

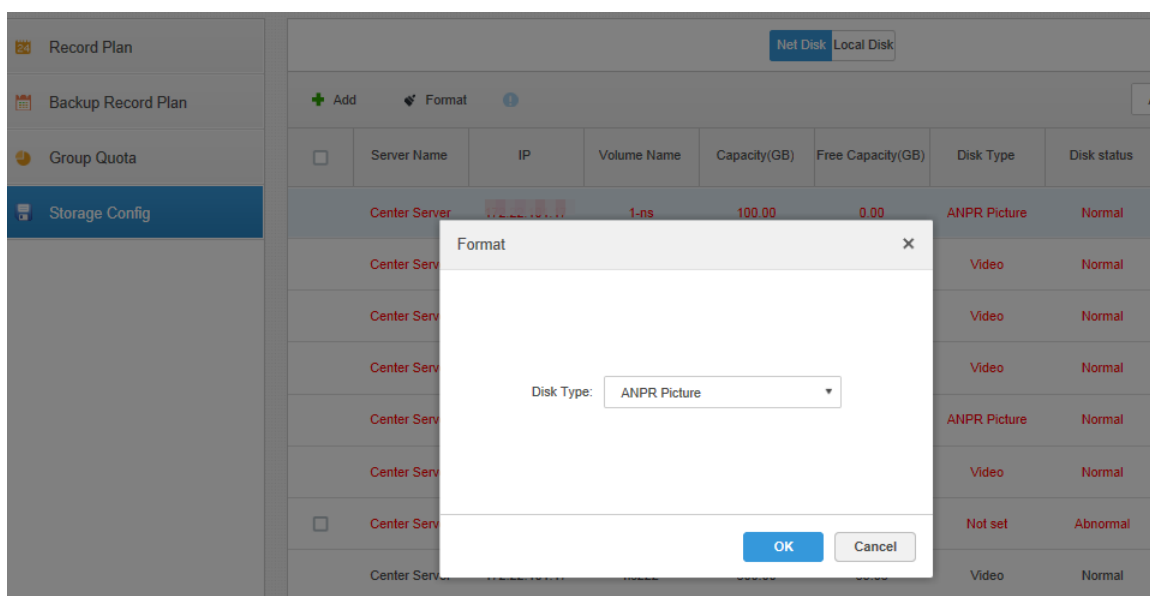
- Protocol: [Dropdown menu]
- Manufacturer: [Dropdown menu]
- Add Type: IP Address [Dropdown menu]
- Device Category: ANPR [Dropdown menu]
- IP Address: [Text input field]
- Device Port: 37777 [Text input field]
- User: [Text input field]
- Password: [Text input field with masked characters]
- Org: root [Dropdown menu]
- Home Server: Center Server [Dropdown menu]

At the bottom right of the form, there are two buttons: "Add" (highlighted in blue) and "Cancel".

Figure 4-188 Add ITC camera (2)

- ◇ The ANPR snapshots are only stored in the **ANPR Picture** disks. On the **Storage** interface, configure at least one **ANPR Picture** disk. Otherwise vehicle pictures cannot be viewed.

Figure 4-189 Disk type



4.12.3.2 Configuring and Arming Vehicle Restricted List

Configure a list of specific target vehicles so that an alarm is triggered once a vehicle in this list is recognized.

- Step 1** Click on the Web Manager, and then select **Vehicle Restricted List** on the **New Tab** interface.

Figure 4-190 Vehicle restricted list

<input type="checkbox"/>	Plate No.	Arm Type	Start Time	End Time	Arm Status	Armed Person	Operate
<input type="checkbox"/>	1211111111	Over Speed Vehicle	2018-09-15 11:27:35	2018-10-06 00:00:00	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4999x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4998x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4997x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4996x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4995x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4994x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4993x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4992x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4991x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4990x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4989x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4988x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4987x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON
<input type="checkbox"/>	4986x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	<input type="checkbox"/> ON

Total 5006 record(s). 1 2 3 4 5 ... 334 Go to page 1 Go

Step 2 Click **Add**.

Figure 4-191 Add a vehicle

Add
✕

Plate No. :

Start Time :

End Time :

Vehicle Type :

Plate Color :

Vehicle Logo :

Vehicle Color :

Arm Type :

Step 3 Set vehicle information, including plate number, start time, vehicle type, plate color, vehicle logo, vehicle color and arming type.

Step 4 Click **OK**.

Operations

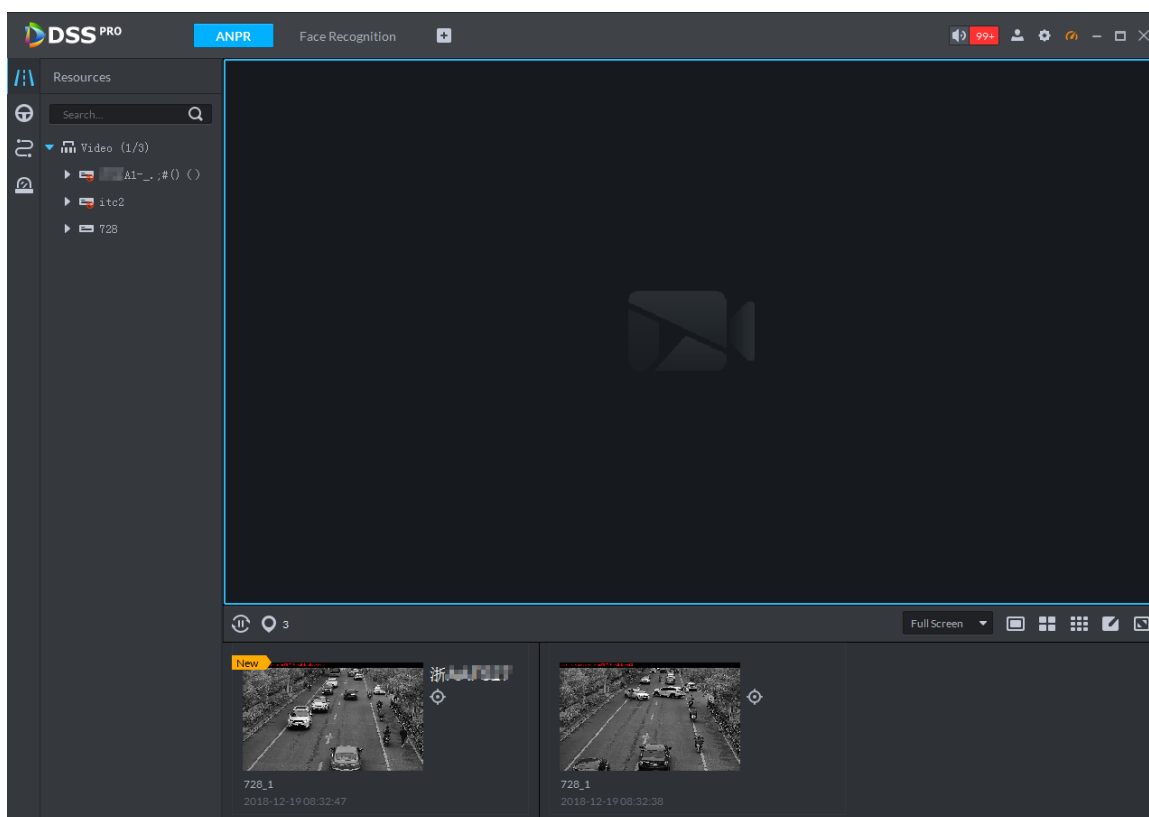
- Arm/Disarm
Click **Arm** to arm the vehicle; click **Disarm** to disarm the vehicle.
- Import
Click **Import** to import vehicle information in batches.
- Export
 - Select the vehicles of interest, and then click **Export Selected** to export the selected vehicle information; to export all searches, click **Export All**.

4.12.4 ANPR Applications

4.12.4.1 Live ANPR

Step 1 Click  on the Control Client, select **ANPR**, and then click  to open the **ANPR** interface.

Figure 4-192 ANPR interface




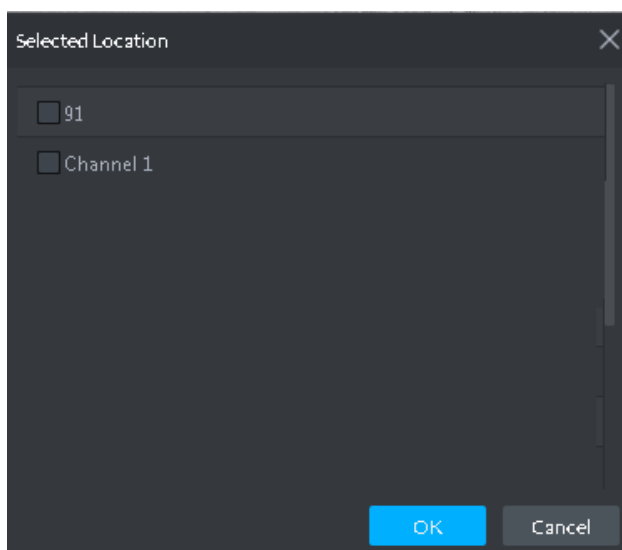
Step 2 Click .

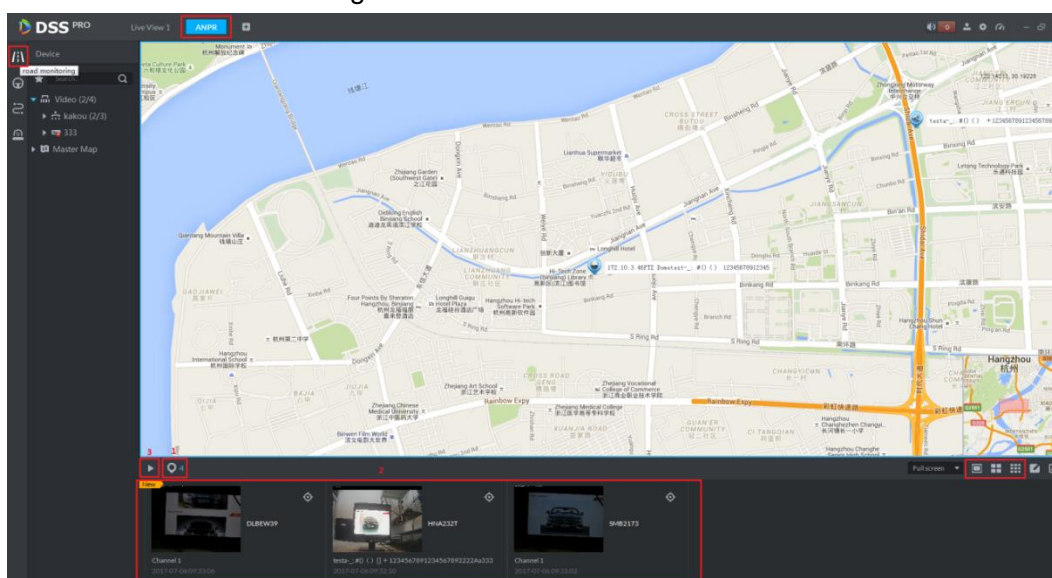
Figure 4-193 Select an ANPR channel



Step 3 Select an ANPR channel, and then click **OK**.

The selected channel quantity and the latest passing vehicle image are displayed on the rolling pane.

Figure 4-194 ANPR view



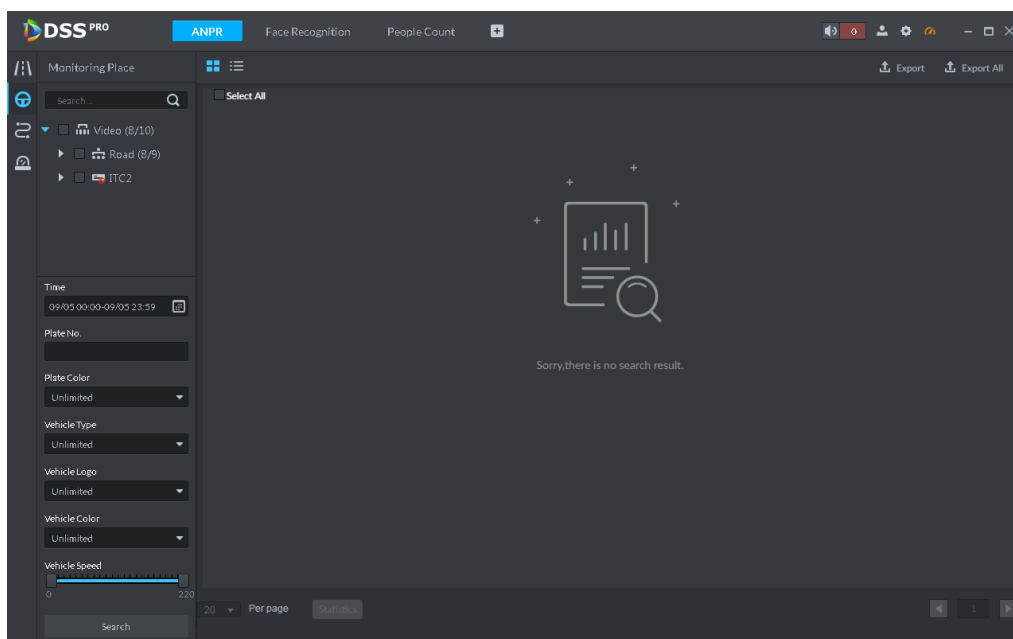
Step 4 Double-click the image to view image details including plate number, snapshot time, ANPR channel name, vehicle logo, and vehicle color.

4.12.4.2 Searching for Vehicle Records

Step 1 Click  on the Control Client, and then select **ANPR**.

Step 2 Click .

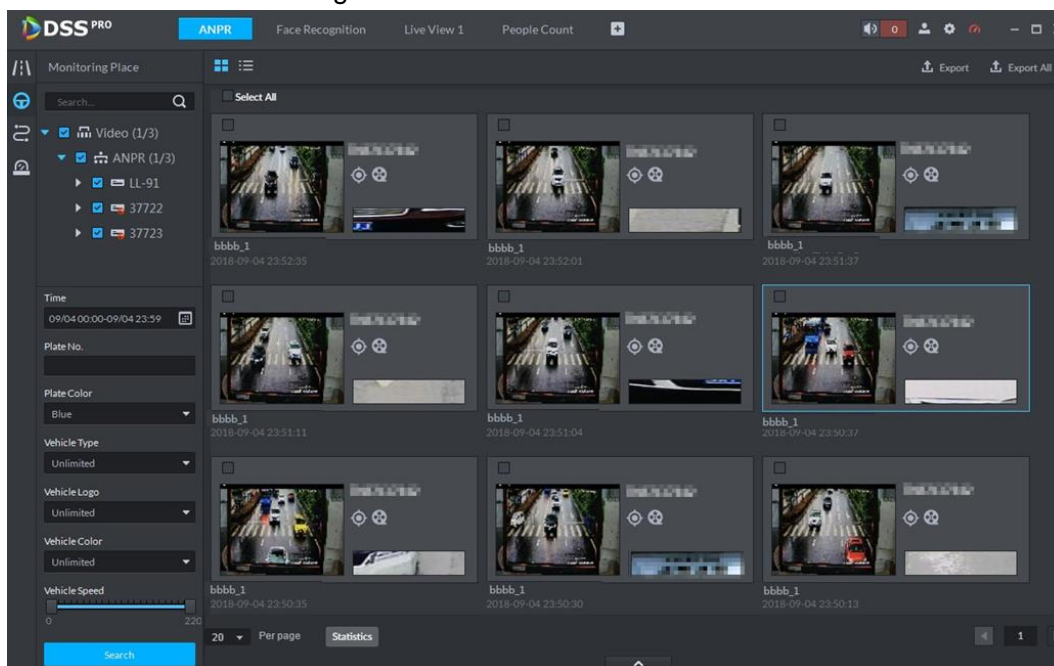
Figure 4-195 Vehicle record search



Step 3 Select video channel and search criteria. It includes time, plate number, plate color, plate type, vehicle logo, vehicle body color and lane.

Step 4 Click **Search**.

Figure 4-196 Search results



Step 5 Manage the records.




- Click the view mode () or list mode ()
- Select a snapshot image and then click  or double-click the image to view detailed information. Hover over the image to view the close image.

Figure 4-197 Vehicle record

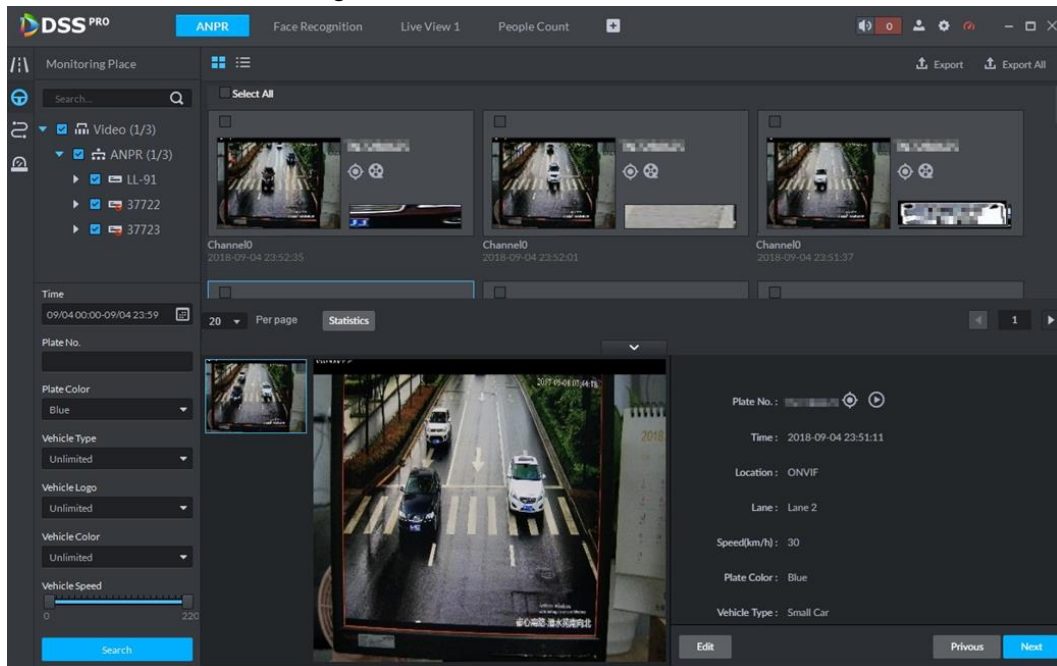
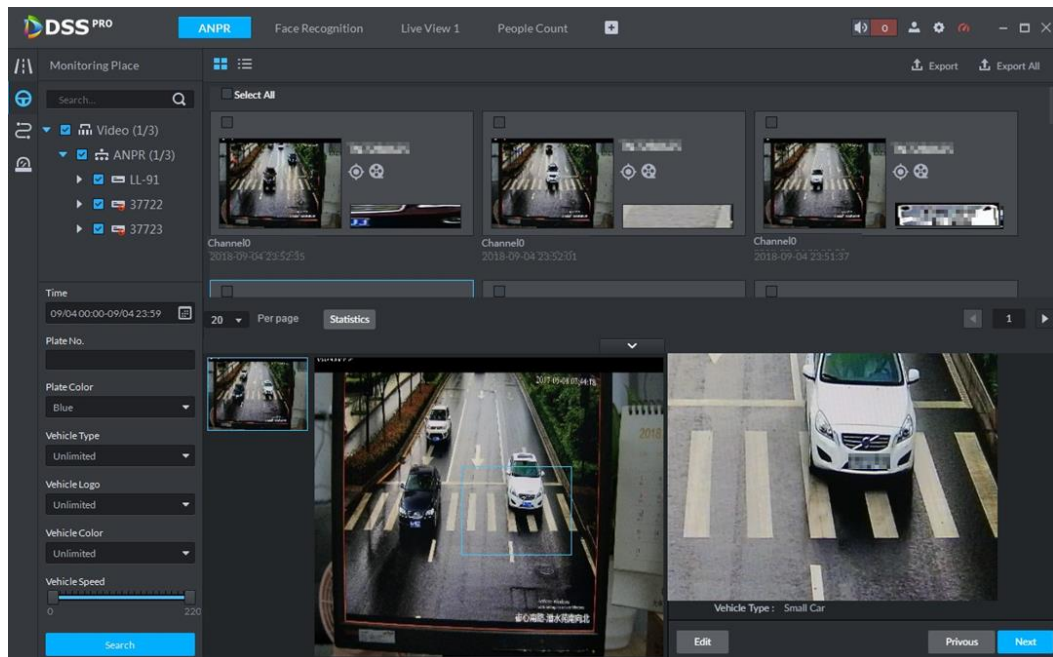


Figure 4-198 Close image




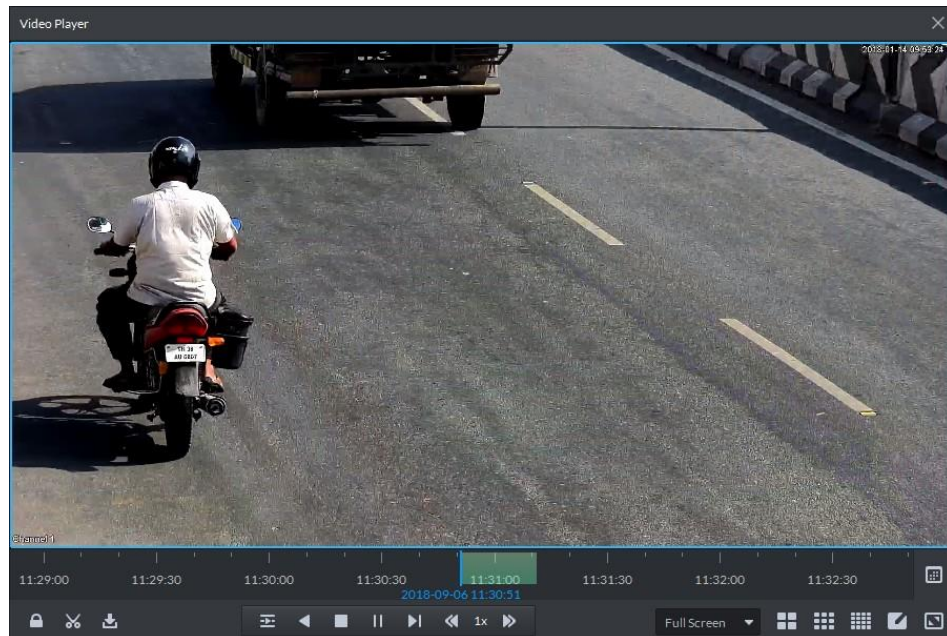

- Click  to play back the video 10 second before and after the ANPR moment.

Figure 4-199 Vehicle video playback




- Click  to view the vehicle running track. See "4.12.4.3 Vehicle Track for details."
- Export: Select the vehicle information and then click **Export** to export the selected vehicle record. To export all searches, click **Export All**.

4.12.4.3 Viewing Vehicle Track

View the moving track of a vehicle along the ANPR locations on the map.



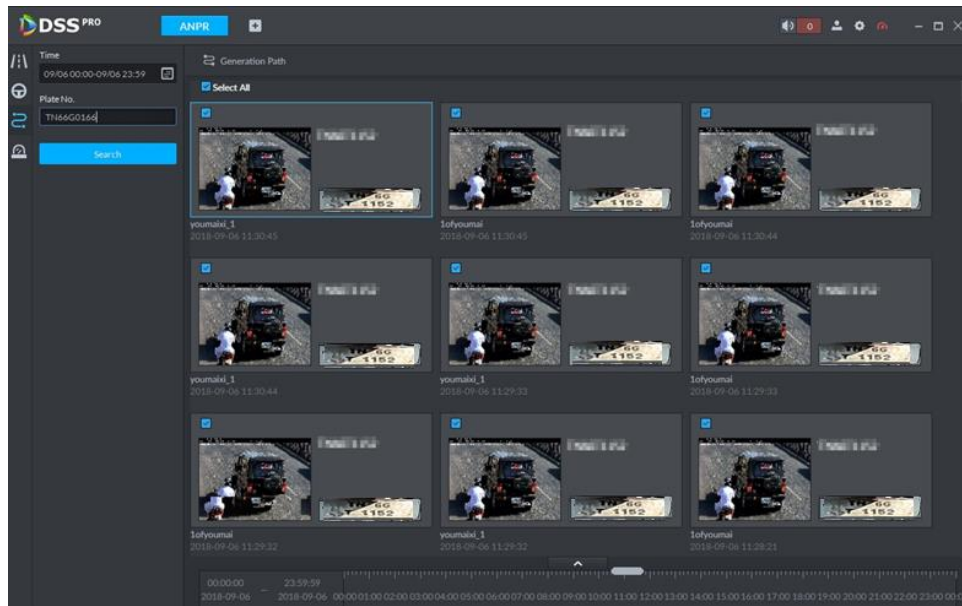
Make sure that you have well configured the ANPR cameras on the map. To configure, see "3.7 Configuring Map."

Step 1 Click  on the Control Client, and then select **ANPR**.

Step 2 Click .

Step 3 Specify time and then enter a plate number. Click **Search**.

Figure 4-200 Vehicle track records




Step 4 Select a record, and then click **Generate Path** to view the vehicle track on the map.

4.12.4.4 Restricted Vehicles Records

View records of restricted vehicles.

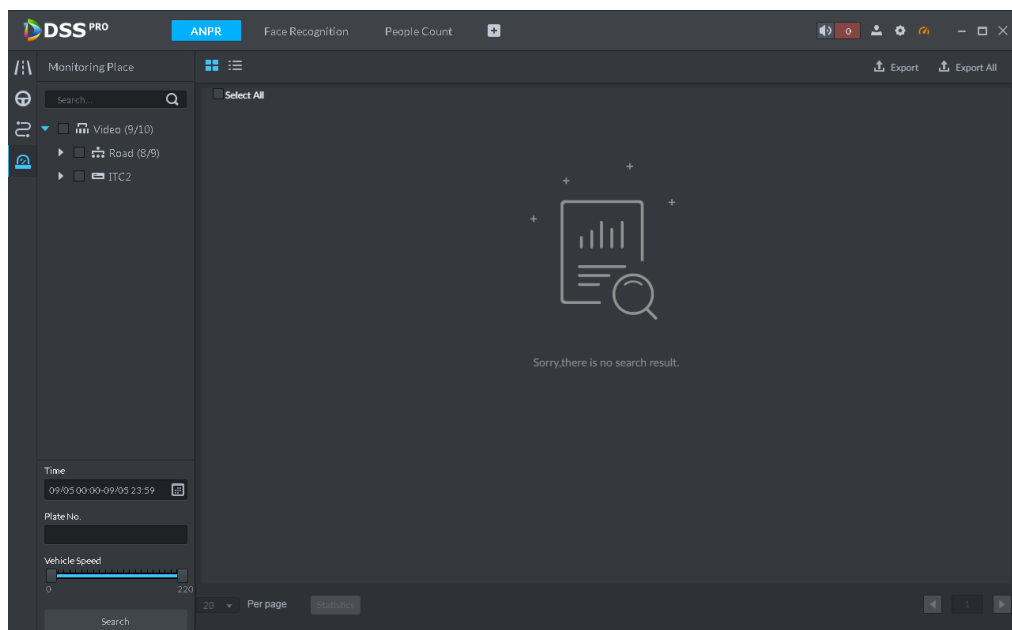


Make sure that you have configured and armed vehicle restricted list.

Step 1 Click  on the Control Client, and then select **ANPR**.

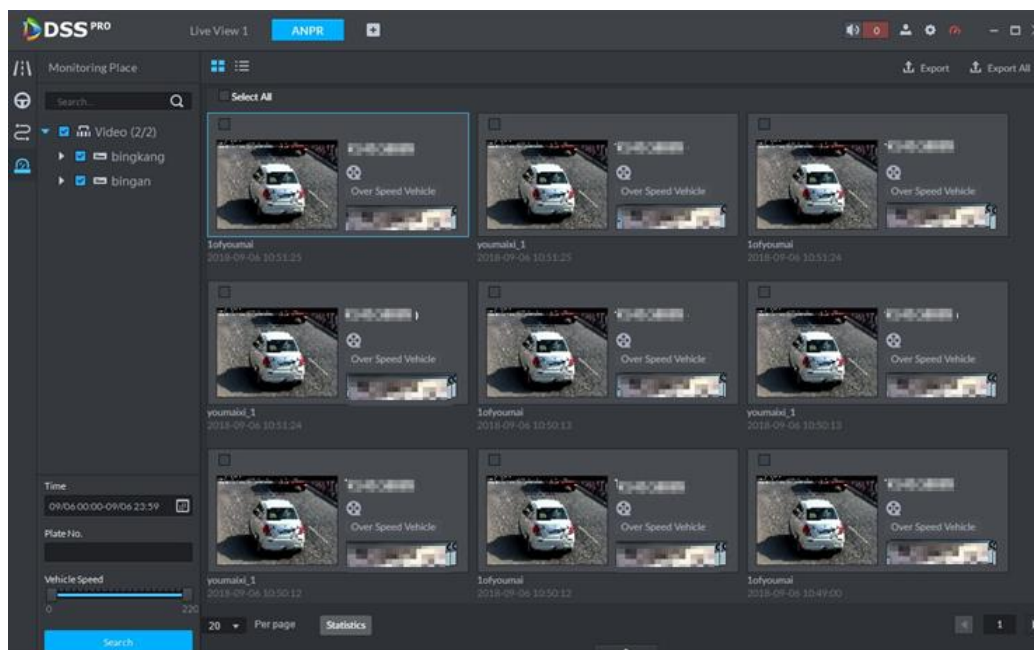
Step 2 Click .

Figure 4-201 View restricted vehicle records



Step 3 Select a channel, and then set time, plate number, and speed. Click **Search**.

Figure 4-202 Search results



Step 4 Manage the records.




- Click the view mode () or list mode ().
- Select the snapshot image, and then click  or double-click the image, to view detailed information. Hover over the image to view the close image.

Figure 4-203 Vehicle details

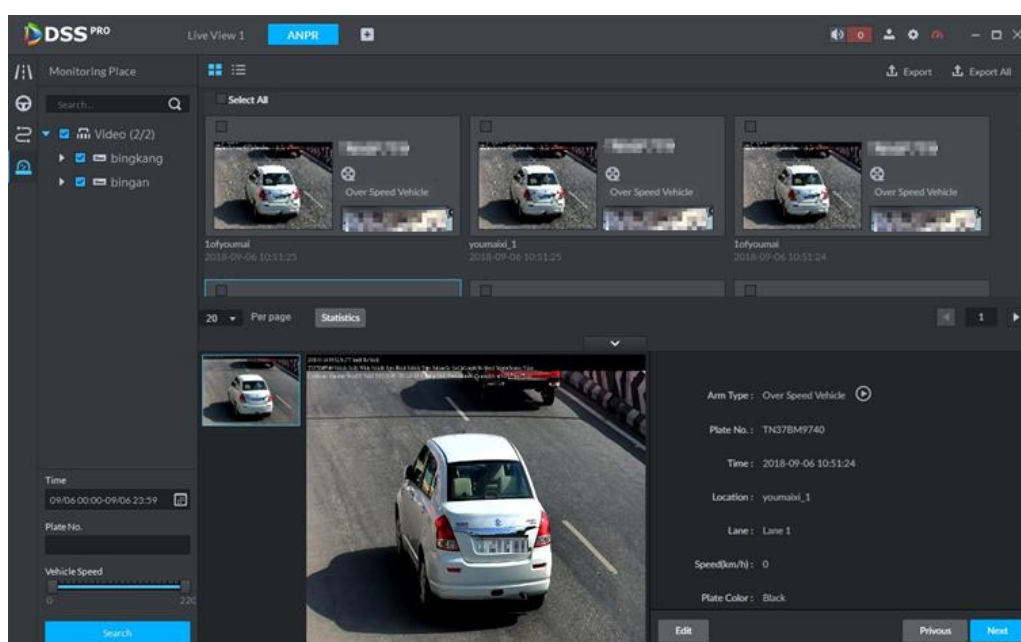
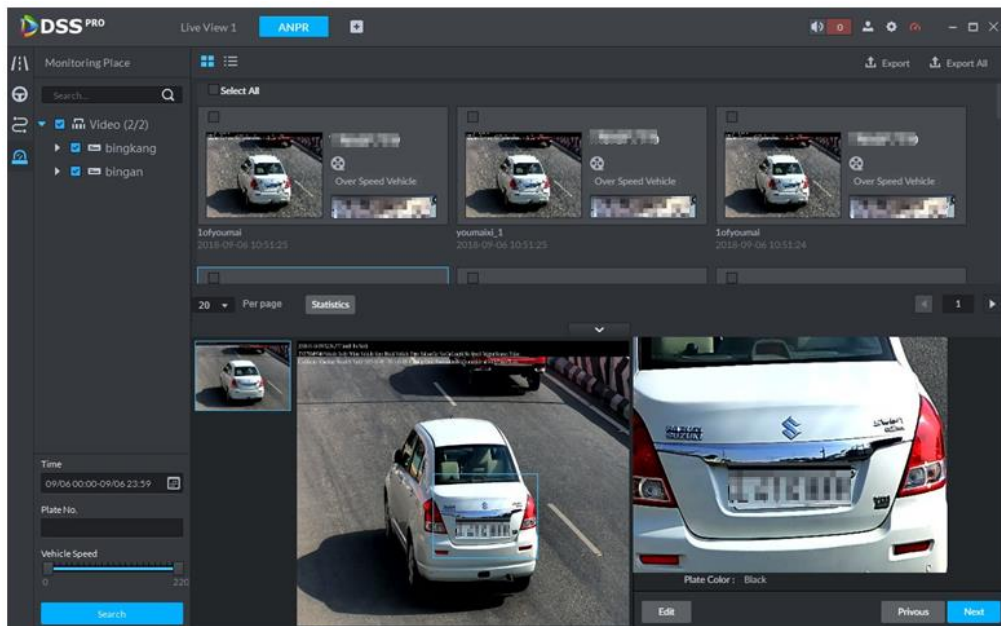


Figure 4-204 Close image




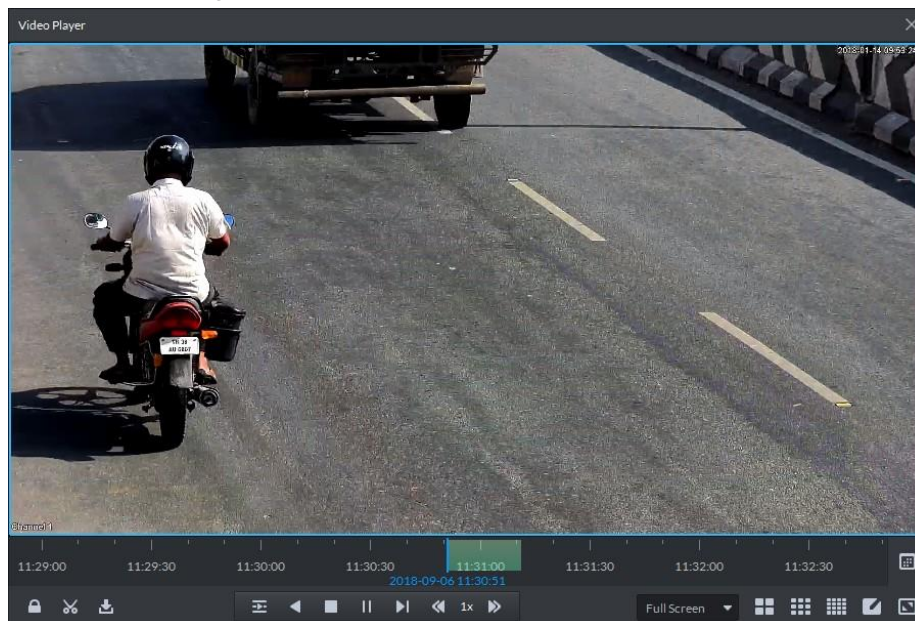

- Click  to play back the video 10 second before and after the ANPR moment.

Figure 4-205 Vehicle video playback



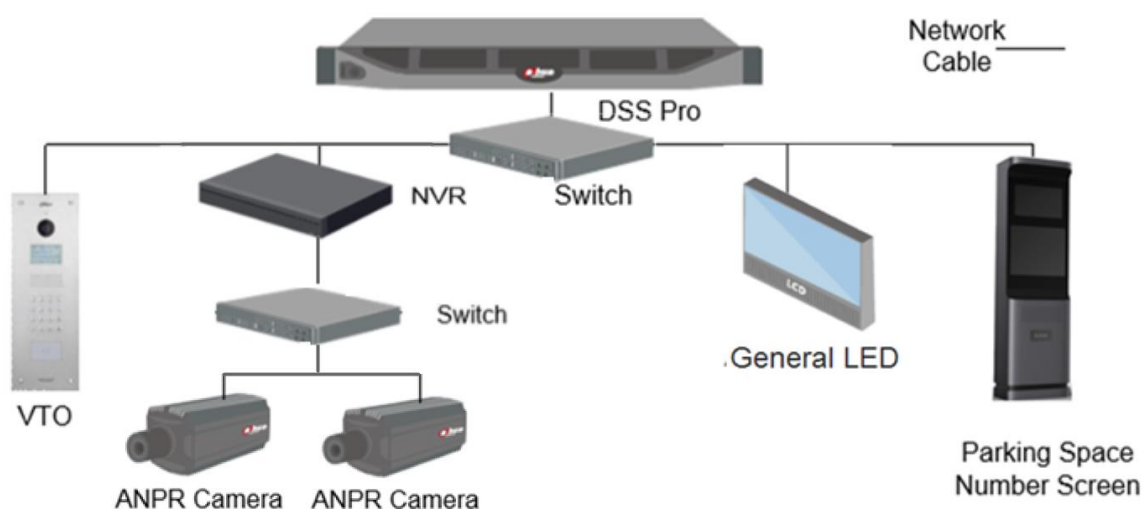
- Click  to view the vehicle running track. See "4.12.4.3 Vehicle Track" for details.
- Export: Select the vehicle record and then click **Export** to export the selected vehicle record. To export all searches, click **Export All**.

4.13 Entrance

Achieve vehicle entrance and exit control with the functions such as ANPR, parking space number display, alarm, and search. In case the vehicle is not recognized by the ANPR camera, the visitor can use VTO (outdoor station) to open the barrier by entering password, swiping card, fingerprint authentication or face recognition, or call the administrator for letting go.

4.13.1 Typical Topology

Figure 4-206 Typical topology



The entrance module supports single camera mode and dual camera mode. In the single camera mode, there is one ANPR camera for one entrance or exit; in the dual camera mode, there are two ANPR cameras for one entrance or exit. The dual camera mode improves vehicle recognition ratio.

- ANPR camera detects and recognizes vehicles coming and going.



In the dual camera mode, the barrier only connects to the main camera. For details, see "4.13.3.3 Configuring Parking Lot."

- In case the vehicle is not recognized by the camera, the driver can use the VTO (Door station) to open the barrier or call the administrator for letting go.
- NVR is used to store ANPR videos and pictures and upload relevant data to DSS Pro.
- DSS Pro centrally manages all devices. It supports configuring parking lot settings and display live and history ANPR videos and pictures.
- The screen displays parking space numbers.

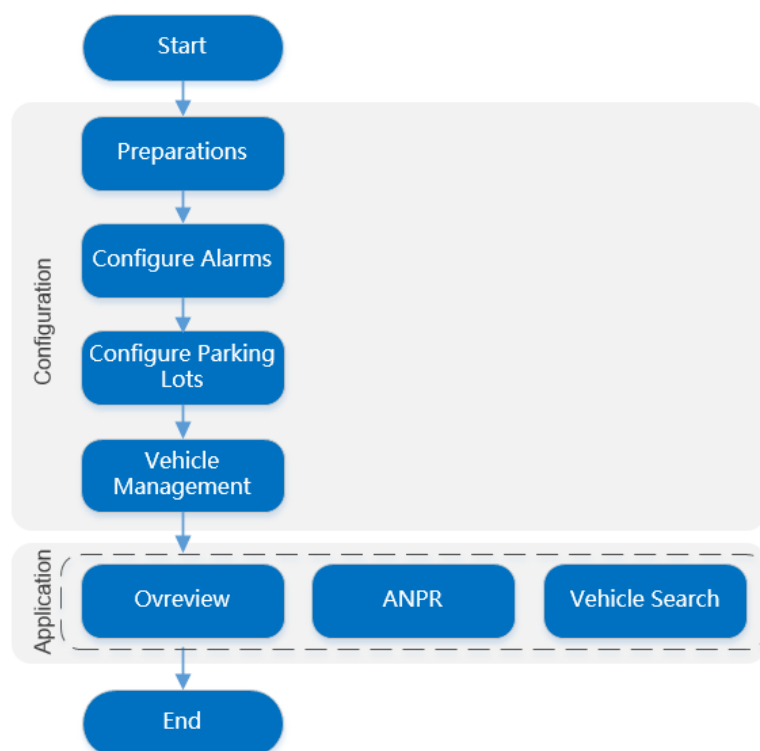
Platform Performance

- ANPR camera management

- ◇ In the single camera mode, one entrance or exit is equipped with one camera, and the platform can manage up to 12 ANPR cameras for respectively 6 entrances and 6 exits.
- ◇ In the dual camera mode, one entrance or exit is equipped with two cameras, and the platform can manage up to 24 ANPR cameras for respectively 6 entrances and 6 exits.
- ANPR performance
 - ◇ The maximum ANPR concurrency is 24 per 3 second.
 - ◇ Speed of opening barrier < 0.5 s.
 - ◇ Number plate upload < 0.3 s.
- ANPR records storage capacity
 - ◇ Up to 5 million entry records.
 - ◇ Up to 5 million on-site vehicle records.
 - ◇ Up to 5 million vehicle snapshot records.

4.13.2 Business Flow

Figure 4-207 Vehicle entrance monitoring business



4.13.3 Configuring Entrance Settings

4.13.3.1 Preparations

Make sure that the following preparations have been made:

- ANPR cameras, VTO (optional), parking space number screen, general LED screen, barrier gate and NVR are well deployed. ANPR cameras are correctly added to NVR. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding an ANPR camera, select **ANPR** for device category, and then select **Access Snapshot Device** for device **Type**.

Figure 4-208 Add ANPR camera (1)

1. Login Information. 1.Login Information 2.Device Information

Protocol: [dropdown]

Manufacturer: [dropdown]

Add Type: IP Address [dropdown]

Device Category: ANPR [dropdown]

IP Address: * [text input]

Device Port: * 37777 [text input]

User: * [text input]

Password: [password field]

Org: root [dropdown]

Home Server: Center Server [dropdown]

Add Cancel

Figure 4-209 Add ANPR camera (2)

2. Device Information. 1.Login Information 2.Device Information

Device Name: Entrance A

Type: Access Snapshot Device

Device Series: Dahua ITC

Device Model:

Device SN:

Role: Administrator, Operator

Video Channel: 1

POS Channel:

- ◇ When adding an NVR on the **Device** interface of Web Manager, select **Encoder** for device category.

Figure 4-210 Add NVR

1. Login Information. 1.Login Information 2.Device Information

Protocol:

Manufacturer:

Add Type: IP Address

Device Category: Encoder

IP Address:

Device Port: 3777

User: admin

Password:

Org: root

Home Server: Center Server

On the **Device** interface, click of the NVR, and then select **Access Snapshot** for **Features** for the corresponding channels.

Figure 4-211 Edit video channel features

Video Channel	Name	Camera Type	Features	SN	KeyBoard Code
Alarm Input	* IP Camera	Speed Dome	Access Snapshot		
Alarm Output	* Thermal	Speed Dome	Intelligent Alarm		
POS Channel	* IPC	Fixed Camera	Intelligent Alarm, Elec...		
HDCVI External	* IPC	Fixed Camera	Intelligent Alarm		
Alarm Box	* Thermal	Fixed Camera	Intelligent Alarm		
	* IPC	Fixed Camera	Intelligent Alarm		

- ◇ When adding VTO, select **Video Intercom** for device category.



The enable status of unit and building on the VTO must be consistent with that on the platform. Or else you might fail to add VTO. For details, see the corresponding User's Manual, or see "4.21.3.2 Configuring Building/Unit."

Figure 4-212 Add VTO

- ◇ Add a screen.
Add a general LED screen or parking space number screen. The parking space number screen supports Dahua screen and Jiuzhou screen.
- 1) When adding a screen on the **Device** interface of Web Manager, select **LED Device** for device category.

Figure 4-213 Add a screen


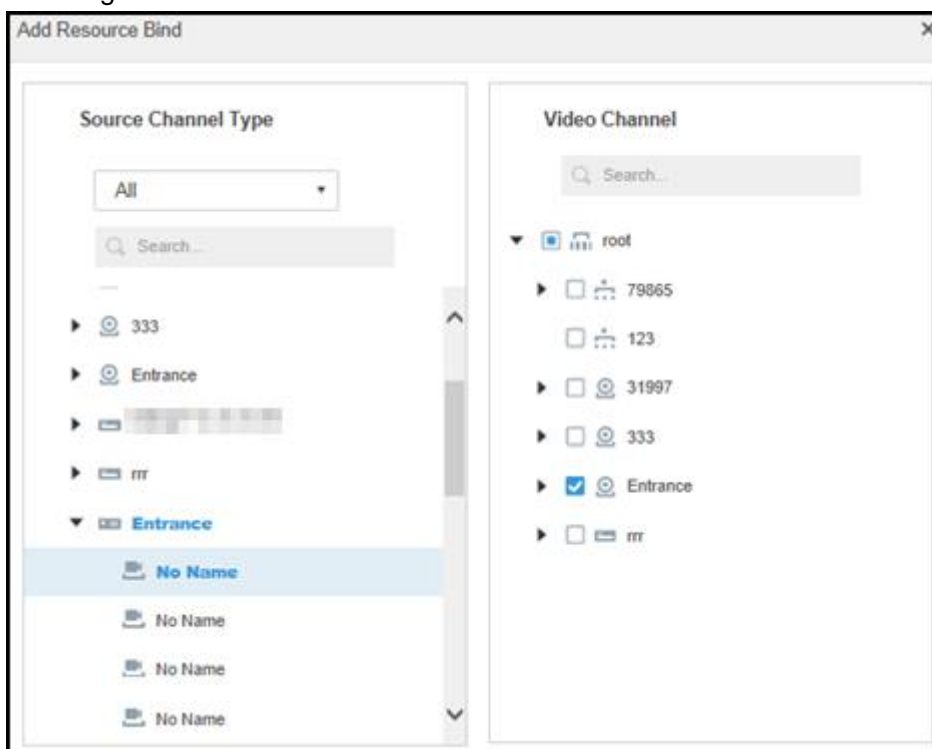
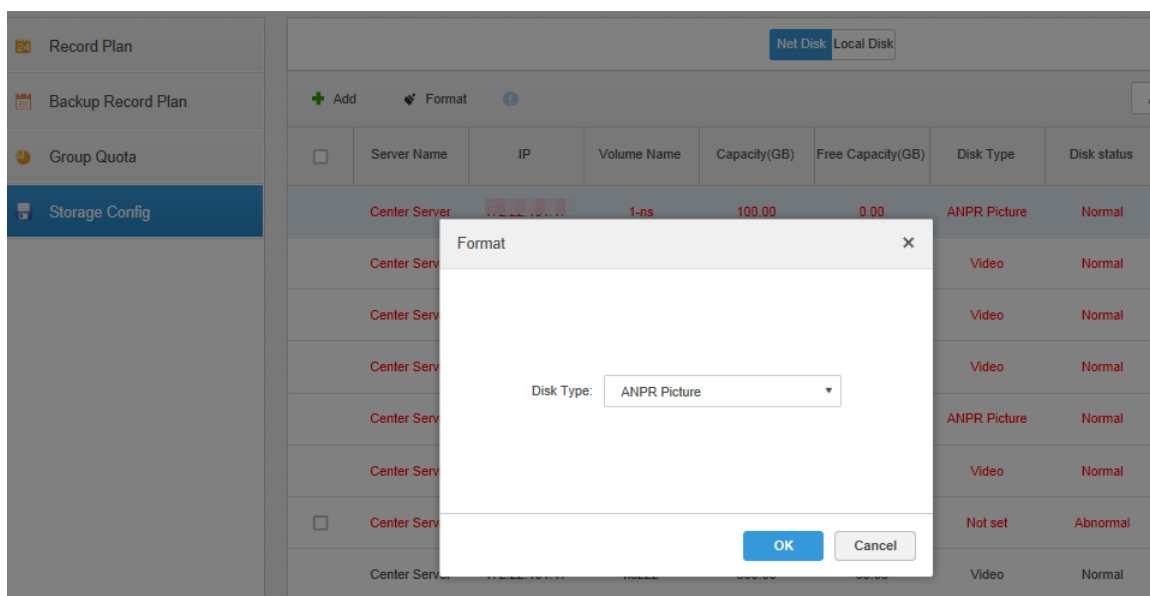
- 2) On the **Device** interface, click the  of the screen, and then select character color and the contents to be displayed.
The contents you select here will be displayed on the screen when there is no parking space left in the parking lot.
- ◇ (Optional) On the **Bind Resource** interface, bind video channels for the ANPR channel.
This is useful when you have installed other cameras at the entrance to view and record the video of the entire background, not just the vehicle part. You can view video from the bound camera when checking the alarm details.

Figure 4-214 Bind a video channel to the ANPR camera



- ◇ The ANPR snapshots are stored in the **ANPR Picture** disks. On the **Storage** interface, configure at least one **ANPR Picture** disk. Otherwise vehicle pictures cannot be viewed.

Figure 4-215 Disk type



- If you need the VTO feature, you need to configure personnel information and assign permissions.

4.13.3.2 Configuring Alarms

- License plate snapshot

The ANPR camera captures vehicle number plates and uploads the results to the platform. Alarm is triggered when a vehicle number plate is captured. You can view the 10 s videos before and after the alarm.

- **Blacklist alarm**

Group the unwelcome vehicles to the blacklist (restricted list). An alarm is triggered when a vehicle in the blacklist (restricted list) is detected.



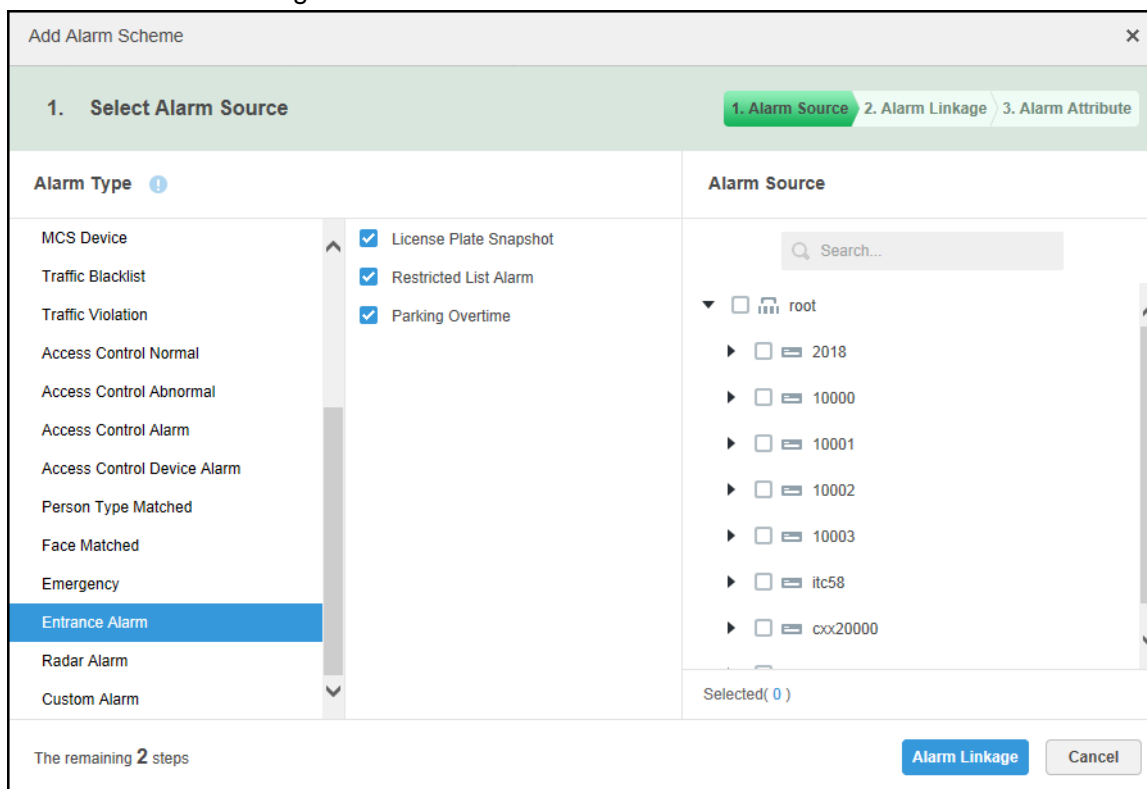
To group a vehicle into the vehicle list, see "4.13.3.4 Vehicle Management."

- **Parking overtime**

Alarm is triggered when the parking time of a vehicle reaches the threshold.


Configure alarms on the **Event** interface of Web Manager. See "4.4 Event" for more details.

Figure 4-216 Add entrance alarm scheme



4.13.3.3 Configuring Parking Lot

Generally, one parking lot is considered as an area. Parking lot configuration includes setting parking space quantity, barrier control rules and other information. Bind an ANPR camera for recognizing vehicles, and bind a VTO (outdoor station) for authorizing human.

Step 1 Click  on the Control Client, and then select **Entrance**.

Step 2 Click .

Step 3 Click **New Parking Lot**, and then configure parking lot information.

Figure 4-217 Add a parking lot

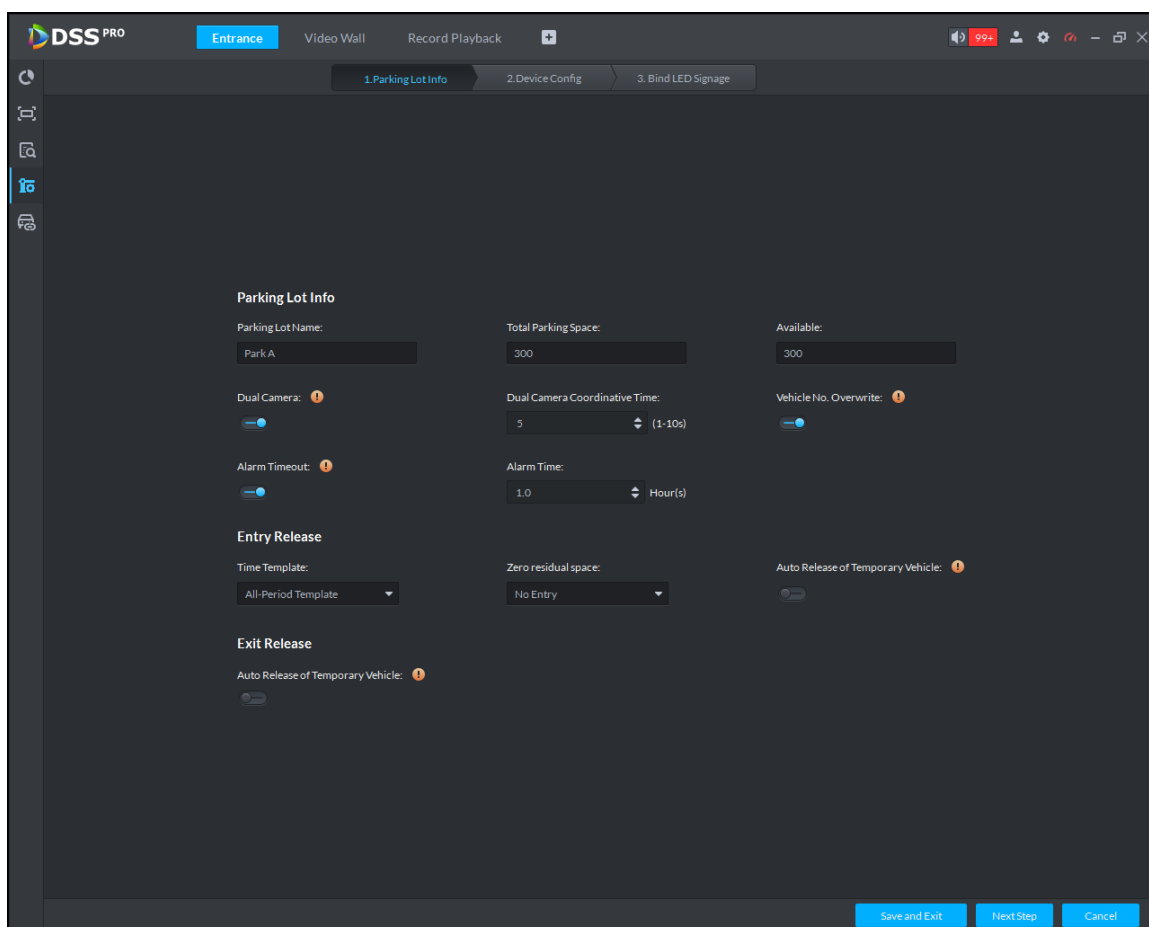



Table 4-46 Parameters

Parameter	Description	
Parking lot information	Name	Parking lot name, used to recognize different areas.
	Total parking space	Total available parking space of the area.
	Available	Available parking lot quantity when configuring area.
	Dual Camera	If one ANPR camera cannot meet your requirement of recognition ratio, you can add a sub camera.
	Dual Camera Coordination Time	The vehicles captured by the two cameras within the defined period are considered as one vehicle. Set the time according to your on-site distances and camera positions.
	Vehicle No. Overwrite	If an on-site vehicle has another entry record (exception case), the calculation of parking space will go wrong. To avoid that, you can enable this function, so that the system only keeps the last entry record.
	Alarm Timeout	An alarm will occur when a vehicle has not left the parking lot after the timeout threshold. You can configure parking overtime alarm on the Web Manager.
	Alarm Time	

Parameter		Description
Entry Release	Time Template	Select the time template which conforms to entry release. If default template fails to meet the requirement, you can select Manage Time Template to set custom time template. Default templates include: <ul style="list-style-type: none"> ● All-period template: 00:00 to 24:00 daily. ● Weekday template: 00:00 to 24:00 Mon to Fri. ● Weekend template: 00:00 to 24:00 Sat and Sun.
	Zero residual space	Release options when remaining space is zero. <ol style="list-style-type: none"> 1. No entry. Any vehicle is not allowed to enter. 2. All Any vehicle is allowed to enter. 3. Trusted list Trusted vehicles include several vehicle types, such as no group, general and VIP. Only the three types of vehicles above are allowed to enter when remaining space is zero. 4. VIP Only VIP vehicle is allowed to enter when remaining space is zero.  Vehicle type should be set during vehicle management.
	Auto Release of Temporary Vehicle	The vehicles not registered on DSS Pro are considered as visitor vehicles. Confirm whether to unlock barrier automatically when a visitor vehicle enters.
Exit Release	Auto Release of Temporary Vehicle	The vehicles not registered on DSS Pro are considered as visitor vehicles. Confirm whether to unlock barrier automatically when a visitor vehicle exits.

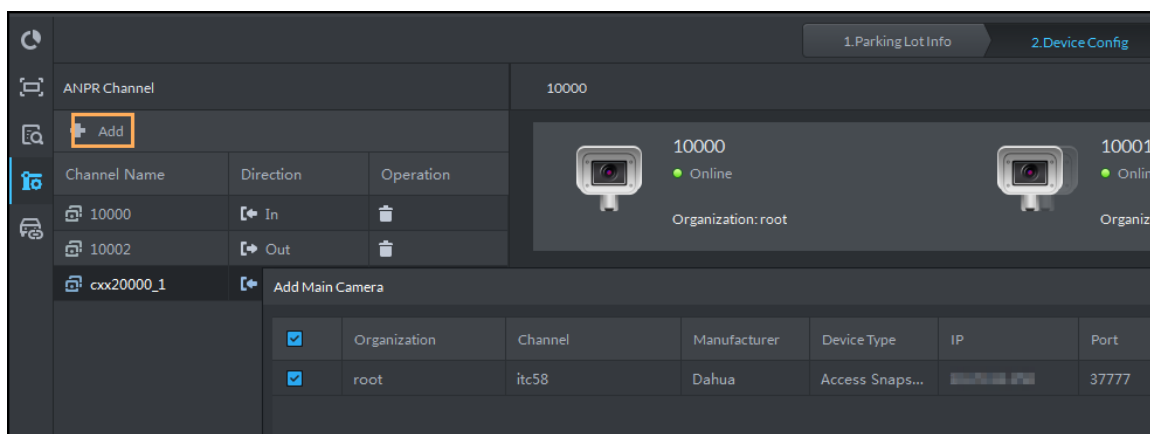
Step 4 Click **Next Step**.

Step 5 Add the main ANPR camera.

Click **Add**, select a camera, and then click **OK**.

If there are multiple entrances and exits, add all the main cameras.

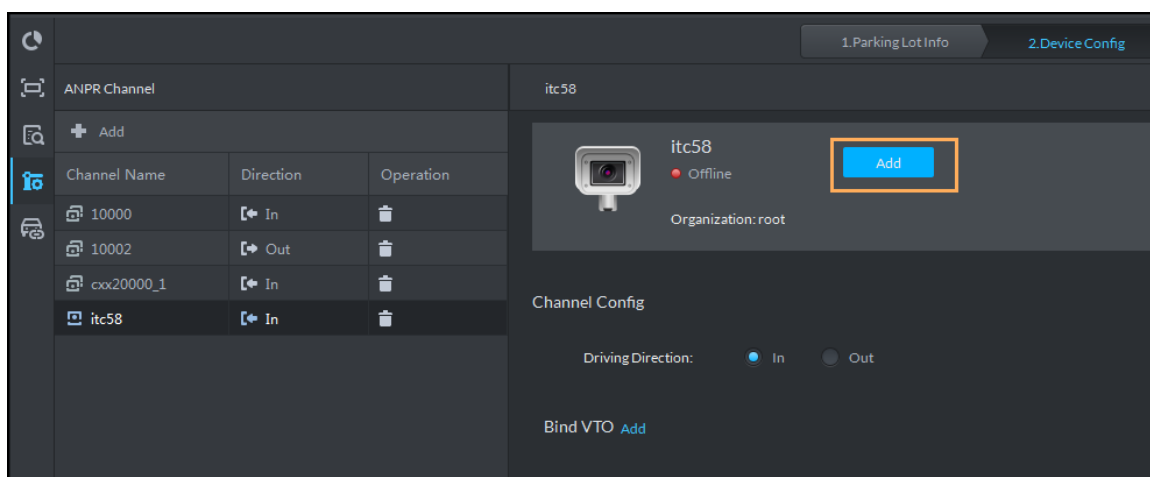
Figure 4-218 Add a main camera



Step 6 Add a sub camera for the main camera, set the lane direction, bind VTO and the LED screen.

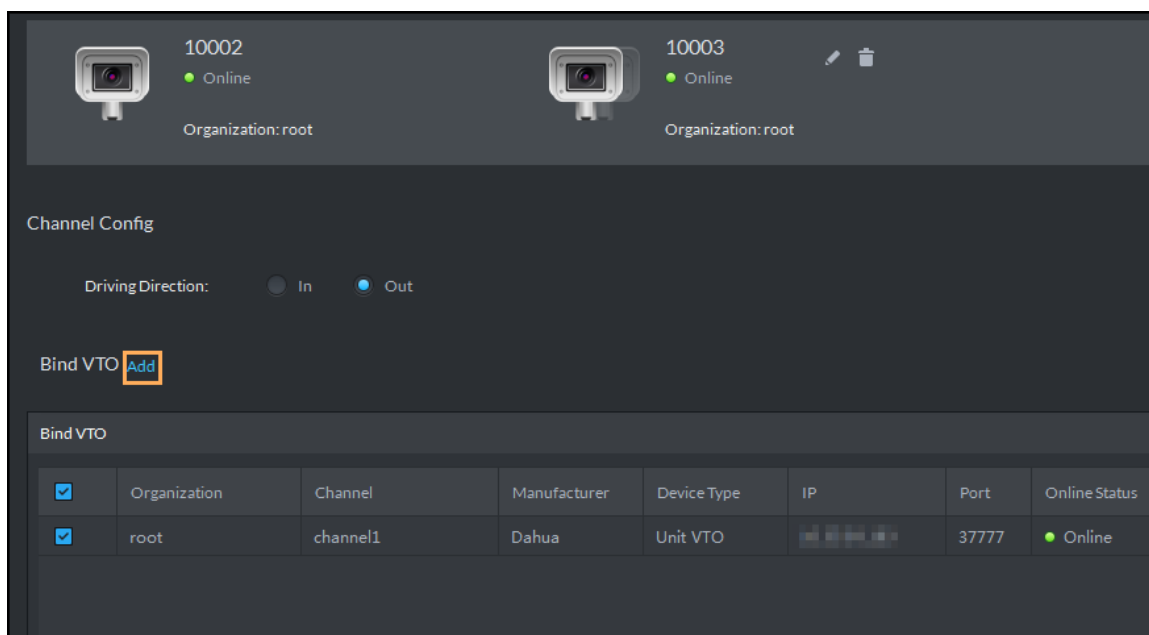
- 1) Select the main camera from the device tree.
- 2) (Optional) Click **Add**, select a sub camera, and then click **OK**.
Sub camera is needed only when you configure the dual camera mode.

Figure 4-219 Add a sub camera



- 3) Select the driving direction.
- 4) (Optional) Click **Add**, select the target VTO, and then click **OK**.
VTO is used for access control and opening barrier. Skip this step if you do not need VTO.

Figure 4-220 VTO information



- 5) (Optional) To add a general LED screen, click **Add** next to **Bind General LED Display**, select the screen, and then click **OK**.


Step 7 Click **Next Step**.

Step 8 To add a parking space LED screen, click **Add LED**, select the screen, and then click **OK**.

Step 9 Click **Save and Exit**.

4.13.3.4 Vehicle Management

Manage vehicle information including vehicle type, department, related personnel and barrier control rule, which are used to confirm if the vehicle can enter.

Step 1 Click  on the Control Client, and then select **Entrance**.

Step 2 Click .

Step 3 Click **Add** to add vehicle information.

Figure 4-221 Add vehicle information

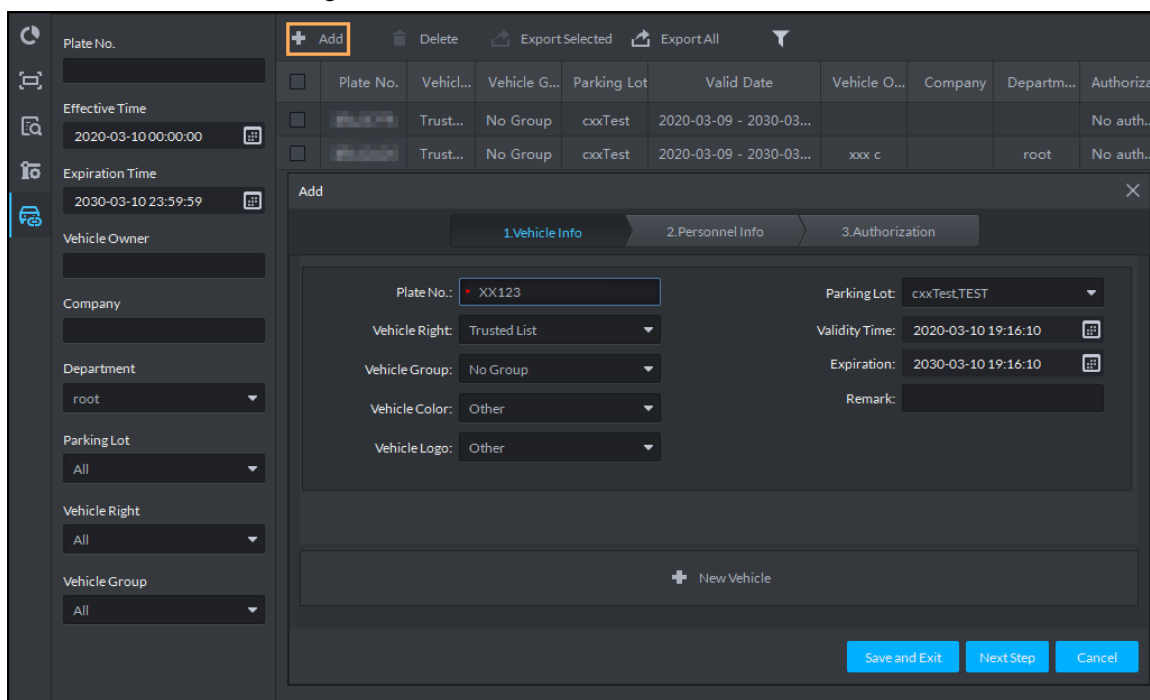


Table 4-47 Parameters

Parameter	Description
Plate No.	The plate number of added vehicle.
Vehicle Right	Select a group for the vehicle to give corresponding access permission. <ul style="list-style-type: none"> Vehicles in the trusted list can get in and out of the parking lot. To configure access permission for trusted vehicles when the parking space reduces to zero, go to the Parking Lot Config interface. Alarm is triggered when a restricted vehicle is detected. Restricted vehicles are guarded away.
Vehicle Group	Group the vehicles. You can select No Group , Visitor Group , VIP Group or General Vehicle . To configure access permission for VIP vehicles when the parking space reduces to zero, go to the Parking Lot Config interface.
Vehicle Color	Color of added vehicle. Set Not Recognized if vehicle color cannot be recognized. Select Other for those beyond the selected range.
Vehicle Logo	Main vehicle logos on the market.
Parking Lot	The parking lot where the vehicle belongs (required).
Validity Time	Validity period of added vehicle.
Expiration	
New Vehicle	If there are several vehicles, click the button to add more. One person can add up to 5 vehicles.

Step 4 Click **Next**.

Figure 4-222 Personnel info

Step 5 Specify personnel information. Click **Next Step**.

Step 6 Select ANPR devices, and then click **Save and Exit**.

- Trusted vehicle information will be sent to the ANPR camera. In case of disconnection between the camera and the platform, the camera can still control barrier according to the list.
- The restricted vehicle information will not be sent to the camera.

Figure 4-223 Authorization

4.13.4 Entrance Applications

4.13.4.1 Overview

View the free parking ratio of current parking area; make statistics over real-time quantity and on-site vehicle quantity, view quantity of entrance and exit vehicle within some period.

Log in to the Control Client, and then select **Entrance**. Click  on the **Entrance** interface to view parking lot information.

Figure 4-224 Overview



Table 4-48 Parameters

No.	Description
1	Interface displays the information of selected area; see other items for included content.
2	Display total parking spaces, occupied parking and free parking ratio of the selected parking lot.
3	Select occupied parking space quantity of selected area, the result can be displayed by line chart or bar chart. Hover over the image to display corresponding time and occupied parking lot quantity.
4	Select vehicle access quantity of some period, supports day, week, month and year. Select time after period is selected; the system displays vehicle access quantity of selected period within the area. Blue means entered vehicle while orange means exited vehicle. The result can be displayed by line chart or bar chart. Hover over the image to display corresponding time and occupied parking space quantity.

No.	Description
5	Display following data. <ul style="list-style-type: none"> ● Accumulated vehicle flow (hourly) Vehicle flow within current hour (for example, it is 8:42, and then it will make statistics about vehicle flow between 8:00 and 8:42). <ul style="list-style-type: none"> ● Accumulated vehicle flow (Daily) Vehicle flow of the day (Start statistics from 00:00) <ul style="list-style-type: none"> ● Parking turnover The bigger the parking turnover is, the shorter the vehicle stays in the parking lot, and then parking space reuse ratio is higher. If it is a paid parking lot, then it will make more money. <ul style="list-style-type: none"> ● Parking Use Ratio The bigger the parking use ratio is, the average time of vehicle parking is longer.
6	Automatically refresh overview information every 5 minutes. Click Refresh to sync real-time data.

4.13.4.2 Number Plate Recognition

Log in to the Control Client, and then select **Entrance**. Click  on the **Entrance** interface to view live video and ANPR results.

Figure 4-225 License plate recognition

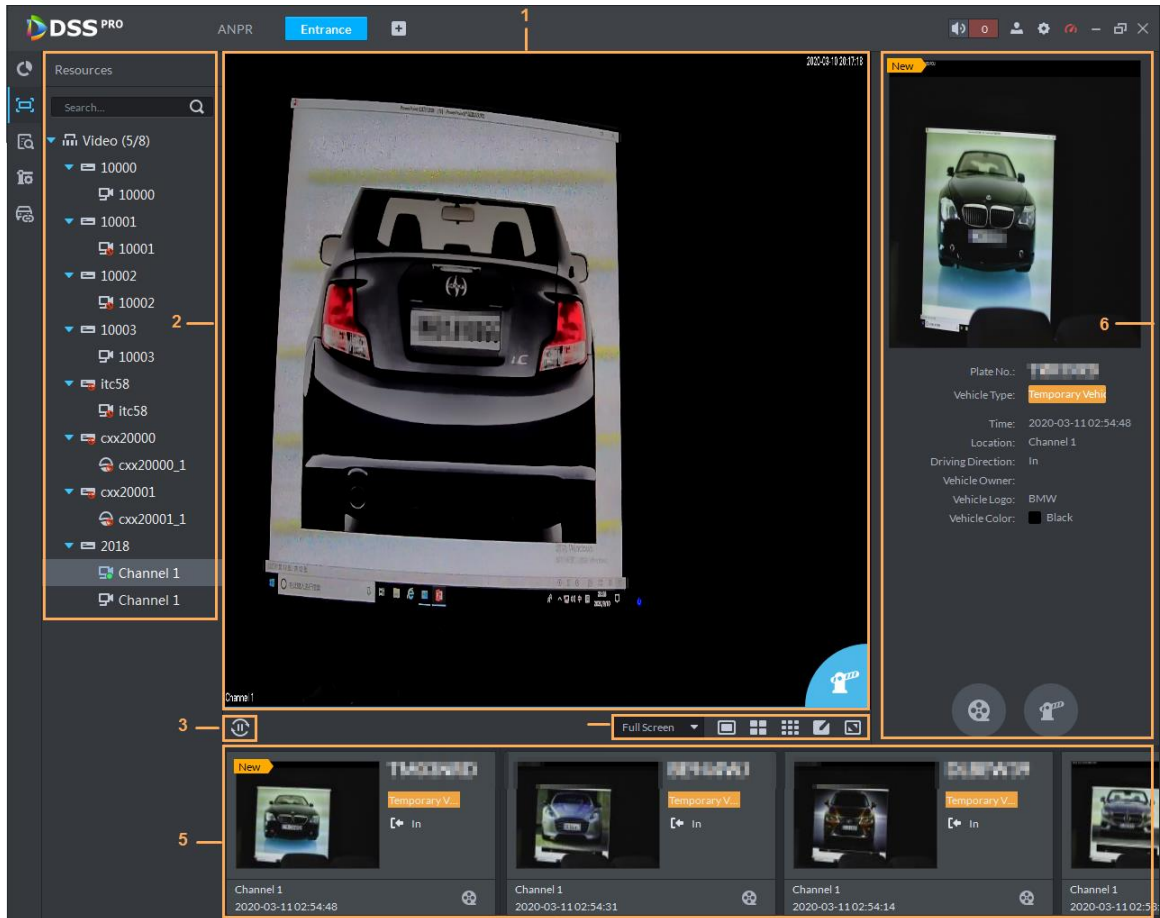






Table 4-49 Description

No.	Description
1	Real-time image display area. Select window, and Double-click video channel bound by ANPR in the device list, or drag the video channel bound by ANPR to window, and the interface displays real-time image. Move the mouse on the image, interface displays unlock button  , click it to unlock barrier.
2	Device list. Display ANPR device and bound video channel.
3	Click the icon and it becomes  , and the interface will no longer ANPR recognition information. Click  and the icon becomes  , the interface will update real-time ANPR recognition information.

No.	Description
4	<ul style="list-style-type: none"> , set height and width ratio of video window, it plays video by two modes which are original scale and full screen. , used to set image split mode, which includes 1 split, 4 splits and 9 splits, or click and customize split mode. , switch video window to Full Screen mode. If you want to exit Full Screen, you can also press ESC button or right-click to select Exit Full Screen.
5	Display latest 4 snapshots of LPR. More details as follows. <ul style="list-style-type: none"> Double-click and display snapshot details, vehicle information, snapshot panoramic picture and vehicle matting. Click and view video of linked channel.
6	Display license plate snapshot and vehicle which need to be released manually. More operation as follows. <ul style="list-style-type: none"> Click and unlock barrier to release vehicle. Click and view video of linked channel.

4.13.4.3 Vehicle Search

Search for entry and exit records, on-site vehicles and snapshot records.

4.13.4.3.1 Searching for Entry and Exit Records

Step 1 Click on the Control Client, and then select **Entrance**.

Step 2 Click on the **Entrance** interface.

Step 3 Click the **Vehicle Access** tab.

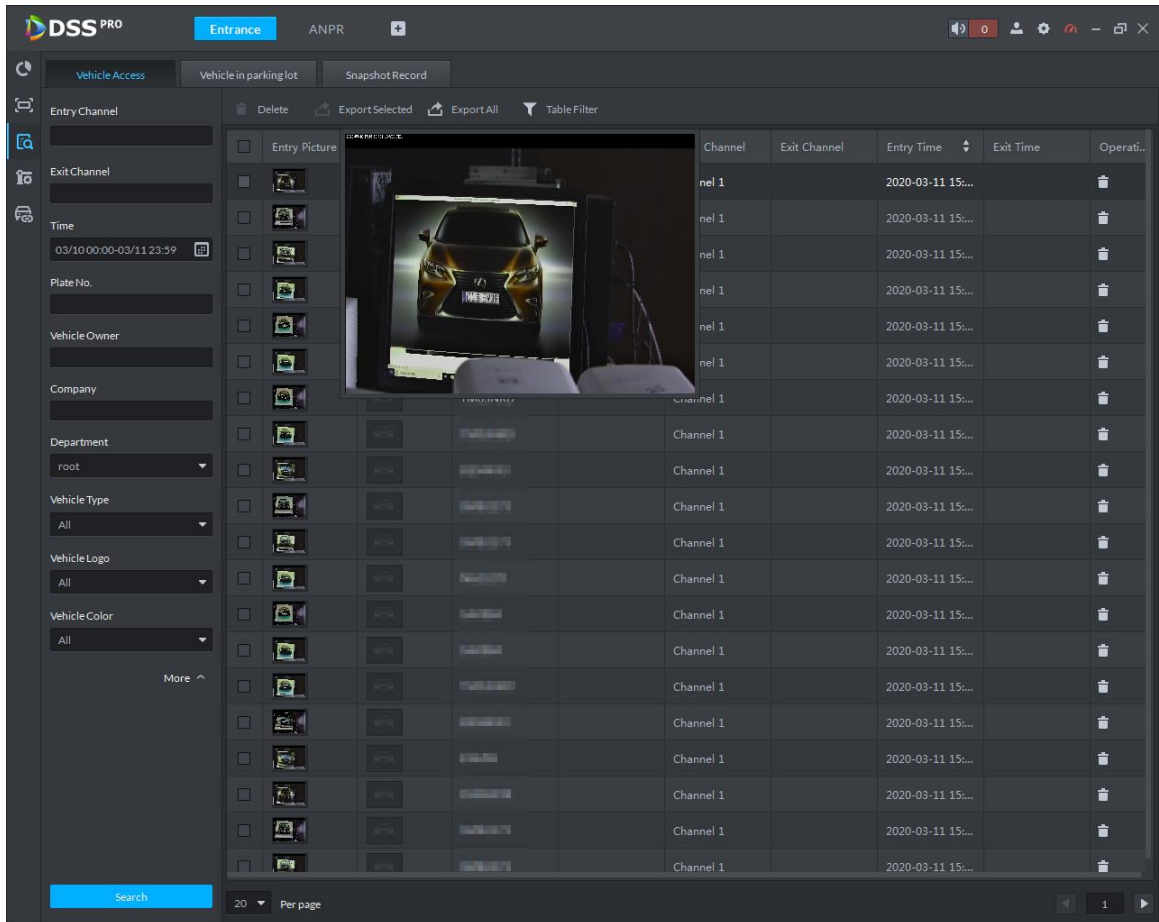
Step 4 Set search conditions, and then click **Search**.



Click **More** and you can search by vehicle owner, department and vehicle type etc.

- Move the mouse pointer to the entry or exit picture, and then the system will display a bigger picture.

Figure 4-226 View bigger picture



- Double-click the record, and detailed information is displayed on the right. For the dual camera mode, the snapshots from both the cameras are displayed; for the single camera mode, there is only one snapshot. Double-click the snapshot in **Info** to view bigger picture, drag the green box to the number plate to confirm the number. Click **Edit** to modify vehicle information, click **OK** to save configuration. Click **Video** to view linked video.

Figure 4-227 Details (1)

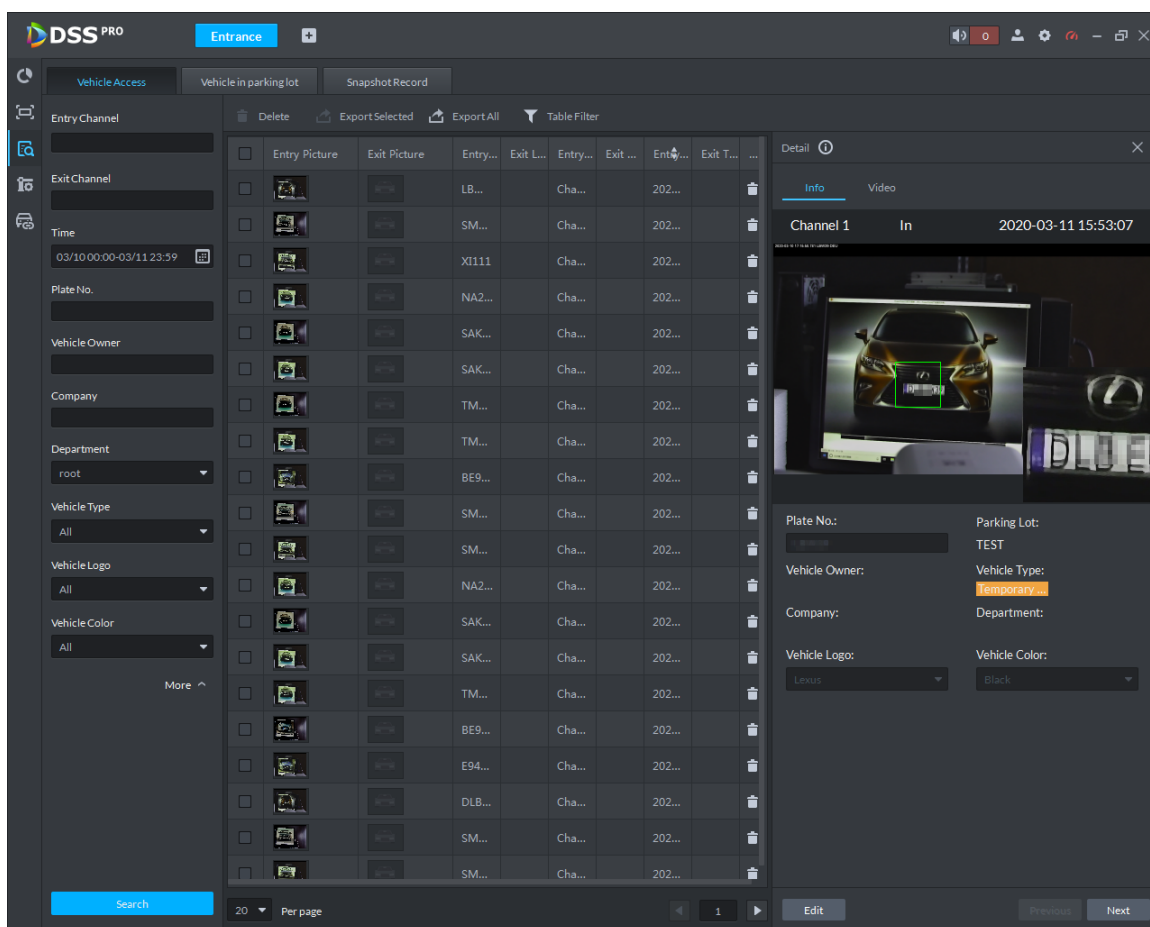
The screenshot displays the DSS PRO software interface. At the top, there are tabs for 'Vehicle Access', 'Vehicle in parking lot', and 'Snapshot Record'. The 'Vehicle Access' tab is active, showing a table of records. The table has columns for 'Entry Picture', 'Exit Picture', 'Entry...', 'Exit L...', 'Entry...', 'Exit ...', 'Entry...', 'Exit T...', and a trash icon. The records include various vehicle types and license plate numbers. On the right side, a 'Detail' panel is open, showing 'Info' and 'Video' tabs. The 'Info' tab displays details for a specific record, including 'Plate No.', 'Parking Lot', 'Vehicle Owner', 'Vehicle Type', 'Company', 'Vehicle Logo', and 'Vehicle Color'. The 'Video' tab shows a video feed of the vehicle's entry and exit.


Entry Picture	Exit Picture	Entry...	Exit L...	Entry...	Exit ...	Entry...	Exit T...	
		LB...	Cha...	202...				
		SM...	Cha...	202...				
		XI111	Cha...	202...				
		NA2...	Cha...	202...				
		SAK...	Cha...	202...				
		SAK...	Cha...	202...				
		TM...	Cha...	202...				
		TM...	Cha...	202...				
		BE9...	Cha...	202...				
		SM...	Cha...	202...				
		SM...	Cha...	202...				
		NA2...	Cha...	202...				
		SAK...	Cha...	202...				
		SAK...	Cha...	202...				
		TM...	Cha...	202...				
		BE9...	Cha...	202...				
		E94...	Cha...	202...				
		DLB...	Cha...	202...				
		SM...	Cha...	202...				
		SM...	Cha...	202...				

Detail Panel:


- Info:** Channel 1, 2020-09-11 15:53:07
- Video:** In, Out
- Plate No.:** [Redacted]
- Parking Lot:** TEST
- Vehicle Owner:** [Redacted]
- Vehicle Type:** Temporary
- Company:** [Redacted]
- Department:** [Redacted]
- Vehicle Logo:** Lexus
- Vehicle Color:** Black


Figure 4-228 Details (2)



- To export all searches, click **Export All**.
- To set information display item, click  and select items to be displayed.
- Click **Next** to display the next record. Click **Previous** to go to the previous record.

4.13.4.3.2 Searching for On-site Vehicles

Step 1 Click  on the Control Client, and then select **Entrance**.

Step 2 Click  on the **Entrance** interface.

Step 3 Click **Vehicle in parking lot**.

Step 4 Set search condition, and then click **Search**.



Click **More** to search by vehicle owner, department and vehicle type.

- If the vehicle is confirmed not in the parking lot, select the vehicle information, click

Force to Exit or .

- To export all the information of on-site vehicles that can be searched, click **Export All**.

- Click to set items to be displayed.
- Click view mode () or list mode () to select different display mode.

4.13.4.3.3 Searching for Snapshot Records

Step 1 Click on the Control Client, and then select **Entrance**.

Step 2 Click on the **Entrance** interface.

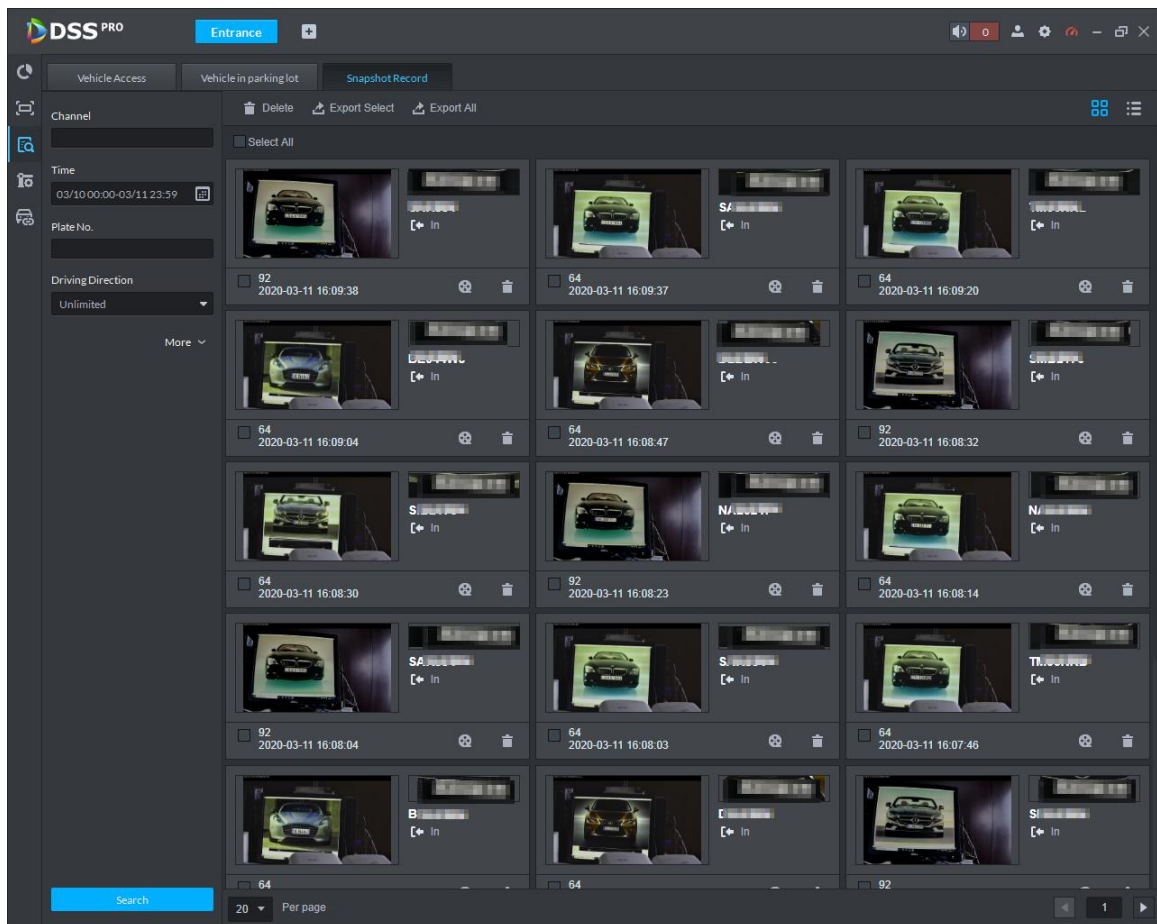
Step 3 Click **Snapshot Record**.

Step 4 Set search condition, and then click **Search**.



Click **More** to search by vehicle owner, department and vehicle type.

Figure 4-229 Search results



- To export all the information of on-site vehicles that can be searched, click **Export All**.
- Click view mode () or list mode () and select different display modes.
- Click to view video.

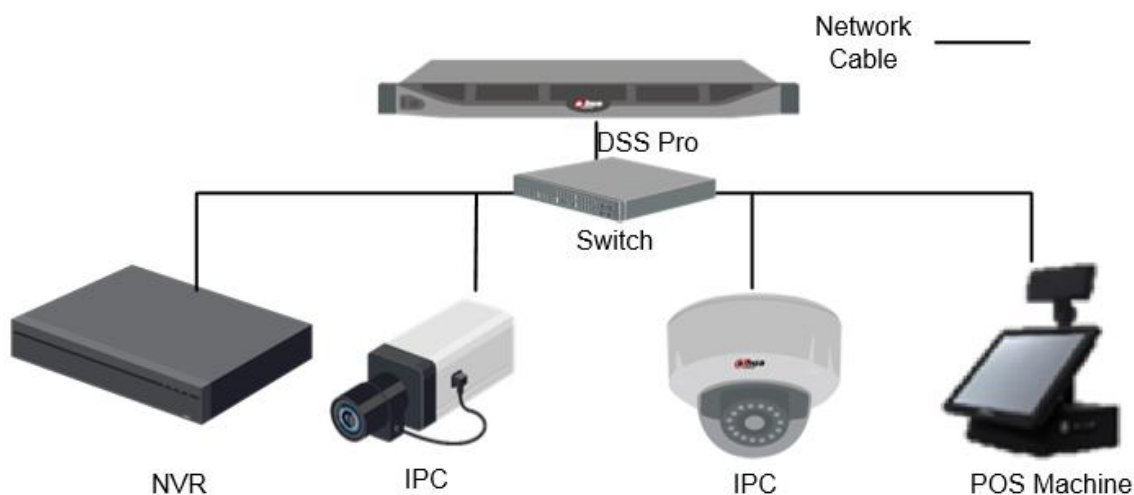
4.14 POS

View POS live video and records.

- Live view
View live POS video and the transaction details overlapped on the video.
- Playback
Search for POS transaction records and play the recorded video. The POS video clip can start 30 seconds earlier than the POS receipt printing.

4.14.1 Typical Topology

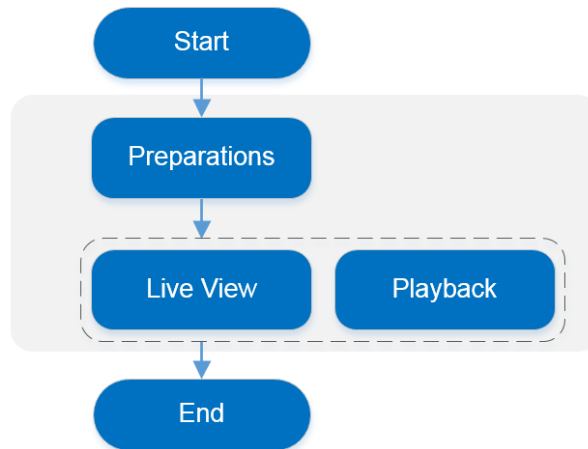
Figure 4-230 Typical topology



- Cameras record videos of each POS transaction.
- NVRs are connected with cameras and POS machines, and store videos.
- POS machines record transaction details and generate receipts.
- The platform centrally manages NVRs and cameras, and provides live videos and POS transaction video records.

4.14.2 Business Flow

Figure 4-231 POS business flow



4.14.3 Configuring POS Monitoring

4.14.3.1 Preparations

Make sure that the following preparations have been made:

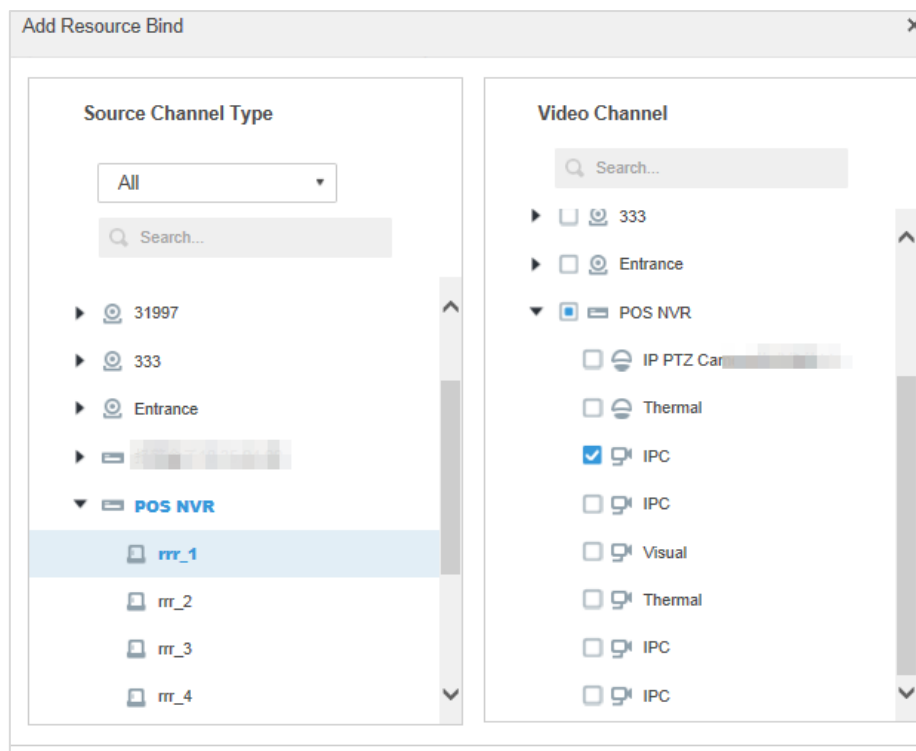
- Cameras, NVRs and POS machines are correctly deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding an NVR on the **Device** interface of Web Manager, select **Encoder** for device category.



At least one POS channel is connected to NVR.

Figure 4-232 Add NVR

- ◇ On the **Bind Resource** interface, bind video channels to the POS channels.
Figure 4-233 Bind video channels to POS channels



4.14.3.2 Setting POS End Sign

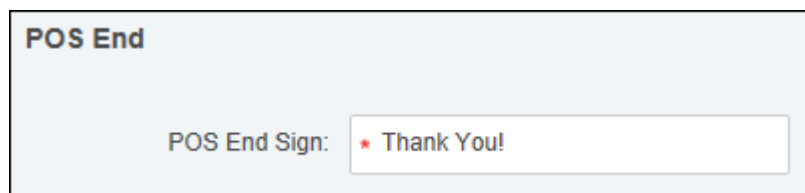
Set the end string of POS transaction receipt.

Step 1 Log in to the Web Manager, click , and then select **System** on the **New Tab** interface.

Step 2 Click the **POS End** tab.

Step 3 Set the end line of POS receipt.

Figure 4-234 Set POS end sign



POS End

POS End Sign: * Thank You!

Step 4 Click **Save**.

4.14.4 POS Applications

View live and recorded videos of POS transactions.

4.14.4.1 POS Live View

View real-time POS transaction video and details.



This section introduces how to enable settings of live view and POS format. For more details about live view, see "4.2 Live View."


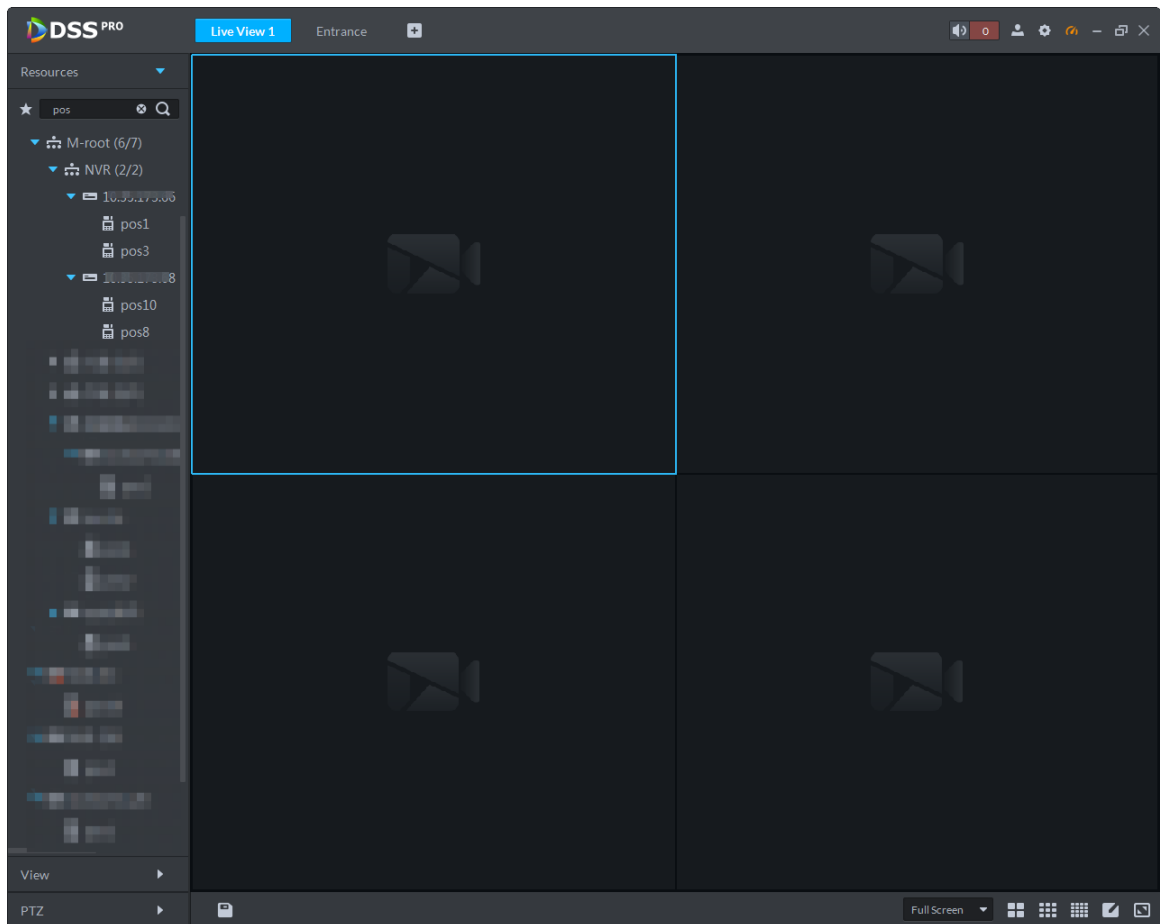
Step 1 Click  on the Control Client, and then select **Live View**.

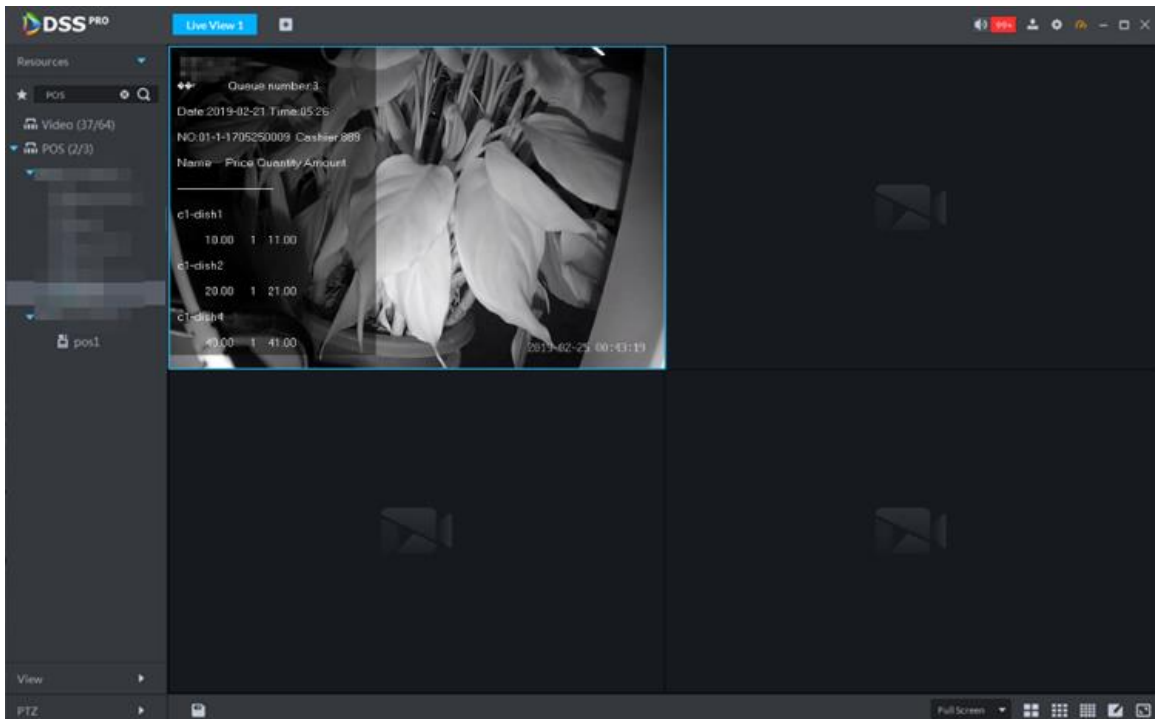
Figure 4-235 Live view



Step 2 View POS video.

- Select a POS-linked camera, double-click or drag it to window.
- Double-click a POS device to display all the POS-linked cameras under it.

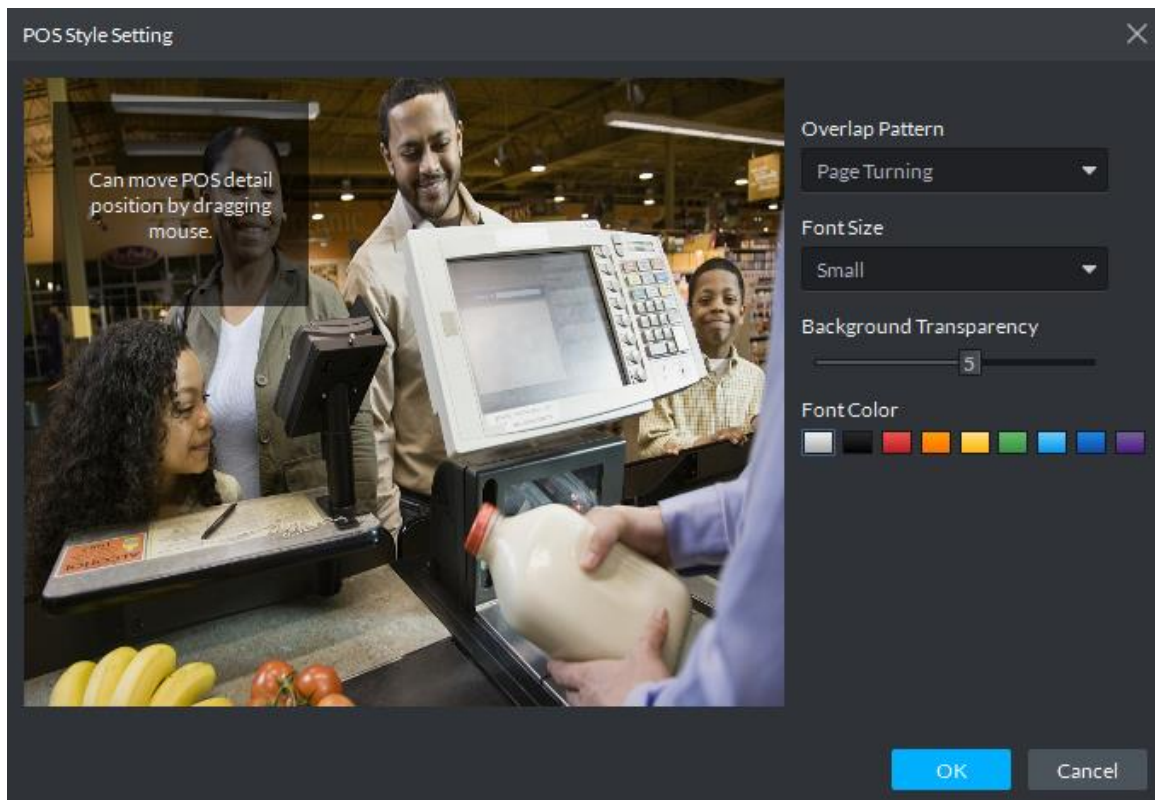
Figure 4-236 POS video



Step 3 (Optional) Set POS information style.

- 1) Right-click and select **Set POS Style** on the live interface.

Figure 4-237 POS style setting



- 2) Set **Overlap Pattern**, **Font Size**, **Background Transparency** and **Font Color**.


- 3) Move the mouse pointer to POS information overlay area, press mouse left button and move it to adjust POS information overlay position.
- 4) Click **OK** and save configuration.

4.14.4.2 POS Playback

Search POS receipt, view related video of receipt. You can search the video half an hour before and half an hour after the time when POS receipt is printed, and you can start to play video 30s before the time when POS receipt is printed.



This section mainly introduces how to replay related video of POS receipt.

Step 1 Click  on the Control Client, and then select **Record Playback**.


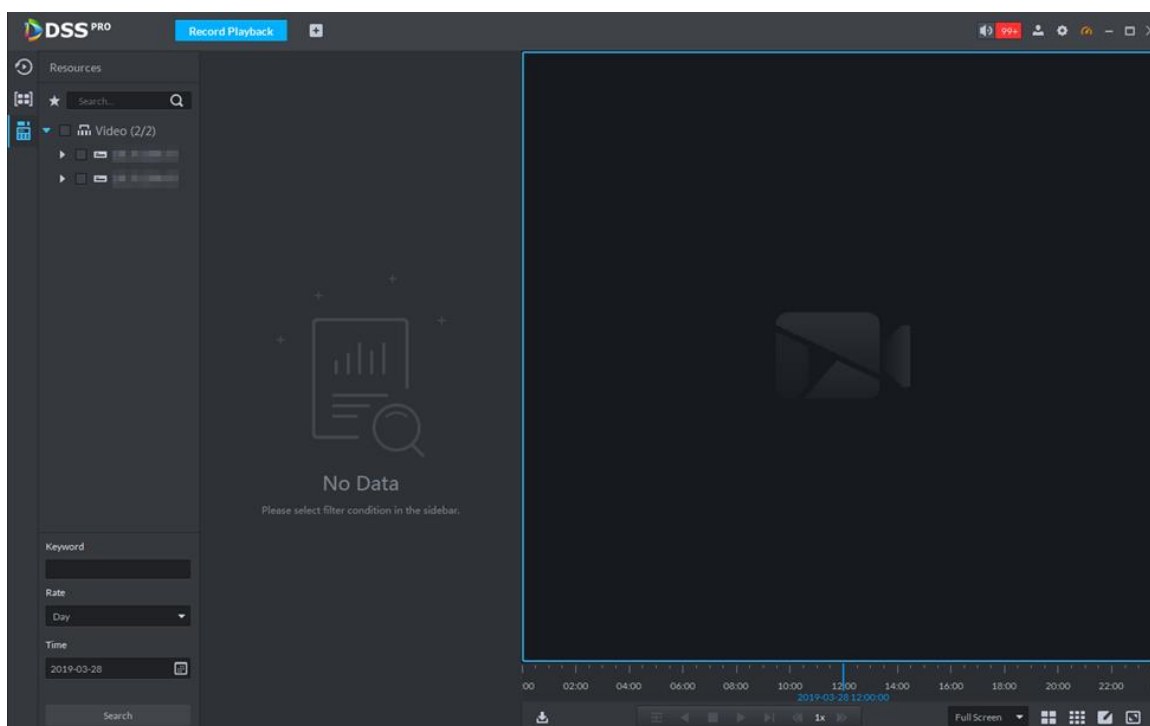
Step 2 Click .

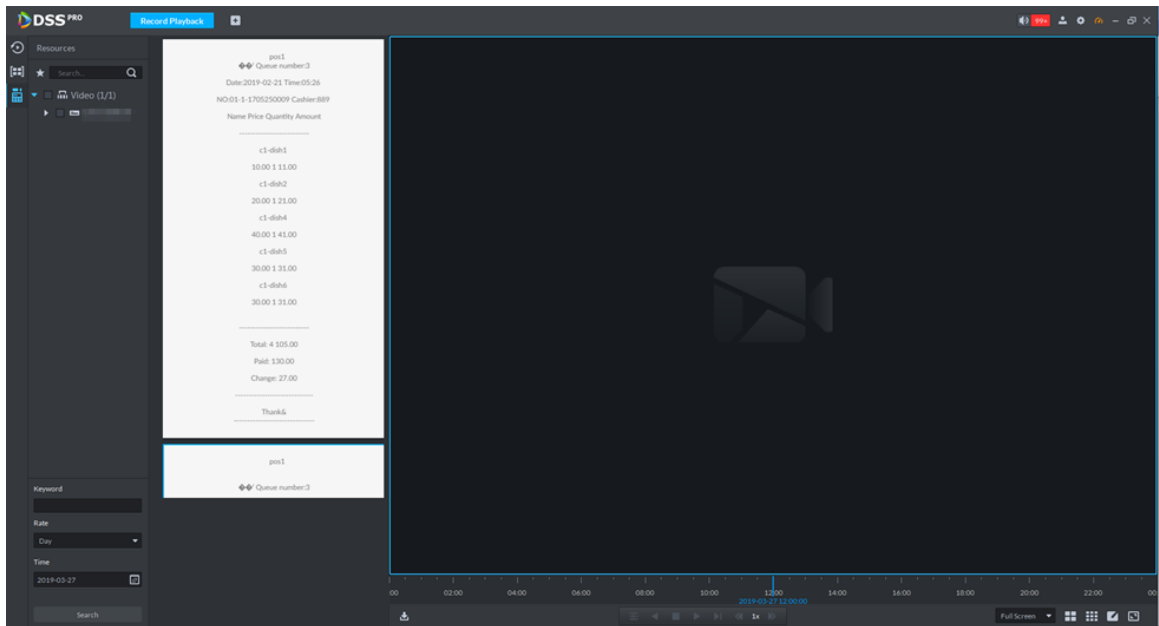
Figure 4-238 POS search



Step 3 Select channel from the device tree.

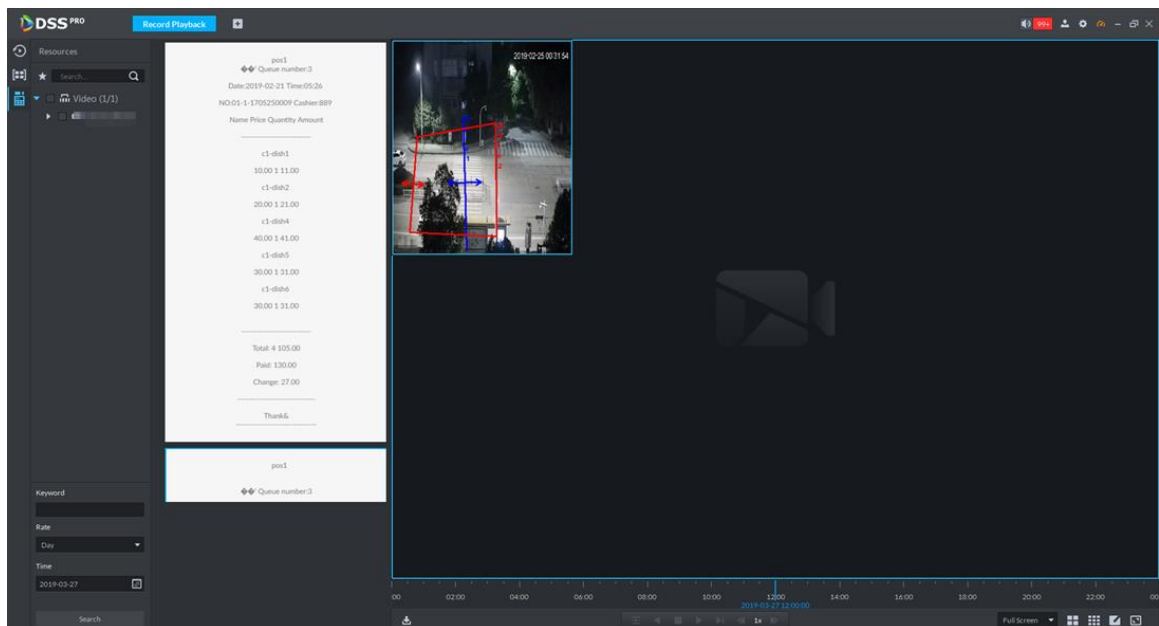
Step 4 Enter **Keyword**, select **Date** and **Time**, click **Search**.

Figure 4-239 Search result



Step 5 Double-click the POS information of related video that needs to be replayed.

Figure 4-240 POS video



4.15 Flow Analysis

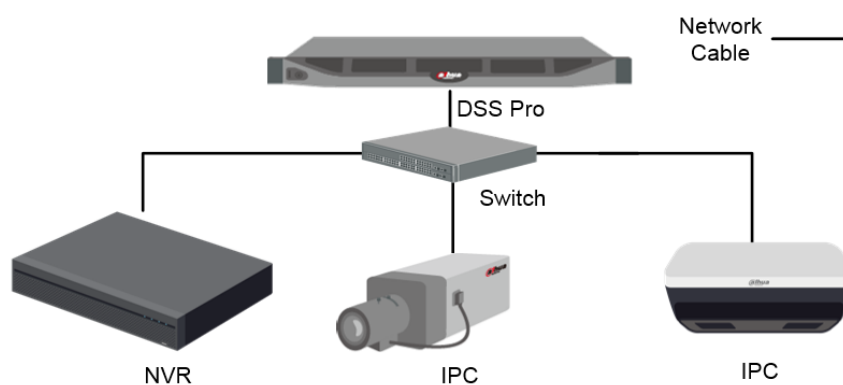
The system provides people counting report, stay people report and heatmap report.

- Flow analysis report
Cameras report the analysis results to the platform, and then the platform can process and show the corresponding reports.

- People stay report
The platform calculates and shows the numbers of people stay according to the analysis data reported by cameras.
- Heatmap
A heatmap shows people distribution in an area during a specific period in different colors, so that you can see which section is more popular and which is less.

4.15.1 Typical Topology

Figure 4-241 Typical topology



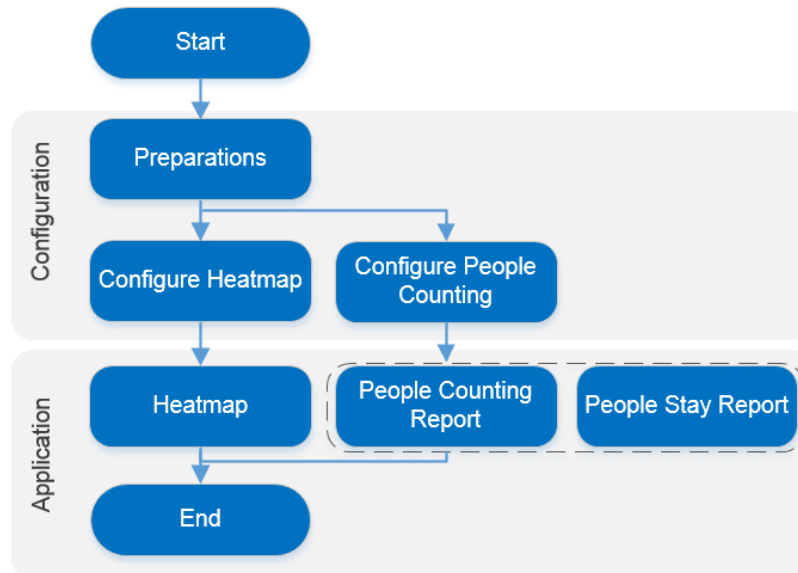
- Cameras record videos and analyze people flow.
- NVRs are connected with cameras. They analyze people flow and store videos.
- The platform centrally manages all NVRs and cameras, receive analysis results from cameras and shows the reports.



Flow analysis can be done by people counting camera or intelligent NVR.

4.15.2 Business Flow

Figure 4-242 Flow analysis business flow



4.15.3 Configuring Flow Analysis

4.15.3.1 Preparations

Make sure that the following preparations have been made:

- Cameras and NVRs with people counting or heatmap function are correctly deployed, and heatmap or people-counting rules have been configured and enabled on the devices. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding a camera or NVR on the **Device** interface of Web Manager, select **Encoder** for device category.

Figure 4-243 Add device

- ◇ On the **Device** interface, click of the camera channel, and then select **Heat Map Statistics** or **People Counting** for **Features**.

Figure 4-244 Edit video channel features

Video Channel	Name	Camera Type	Features	SN	KeyBoard Code
*	IP PTZ Camera	Dome Camera	People Counting		

4.15.3.2 Configuring Heatmap

Heatmap displays the distribution of moving objects in colors of different shades. It reflects the temperature of regions by different colors. For example, red means the temperature is relatively high, and blue means the temperature is relatively low. The configuration interface might vary depending on the camera type. This section takes configuring Stereo Vision people counting camera for example.



You can configure heatmap on the platform only when the camera is directly connected to the platform. Otherwise, configure it on the camera or NVR.

Step 1 Go to the **Intelligent Analyze** interface.


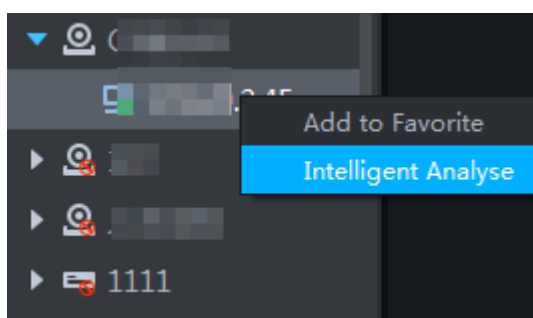
- 1) Log in to the Control Client, click , and then select **Live View**.
- 2) Right-click a camera, and then select **Intelligent Analyze**.

Figure 4-245 Go to intelligent analysis interface



Step 2 Click  to select heatmap.


When the icon is displayed in the white frame, it means it is selected. If another smart plan, which is conflicting with Heatmap, is selected already, click that smart plan icon to deselect it and then click  to select heatmap.

Figure 4-246 Smart plan

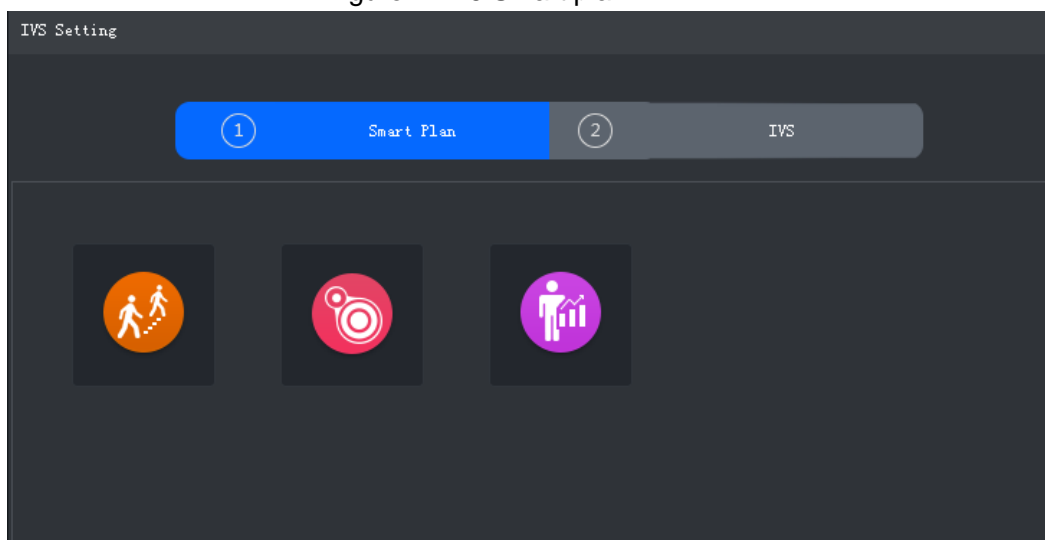
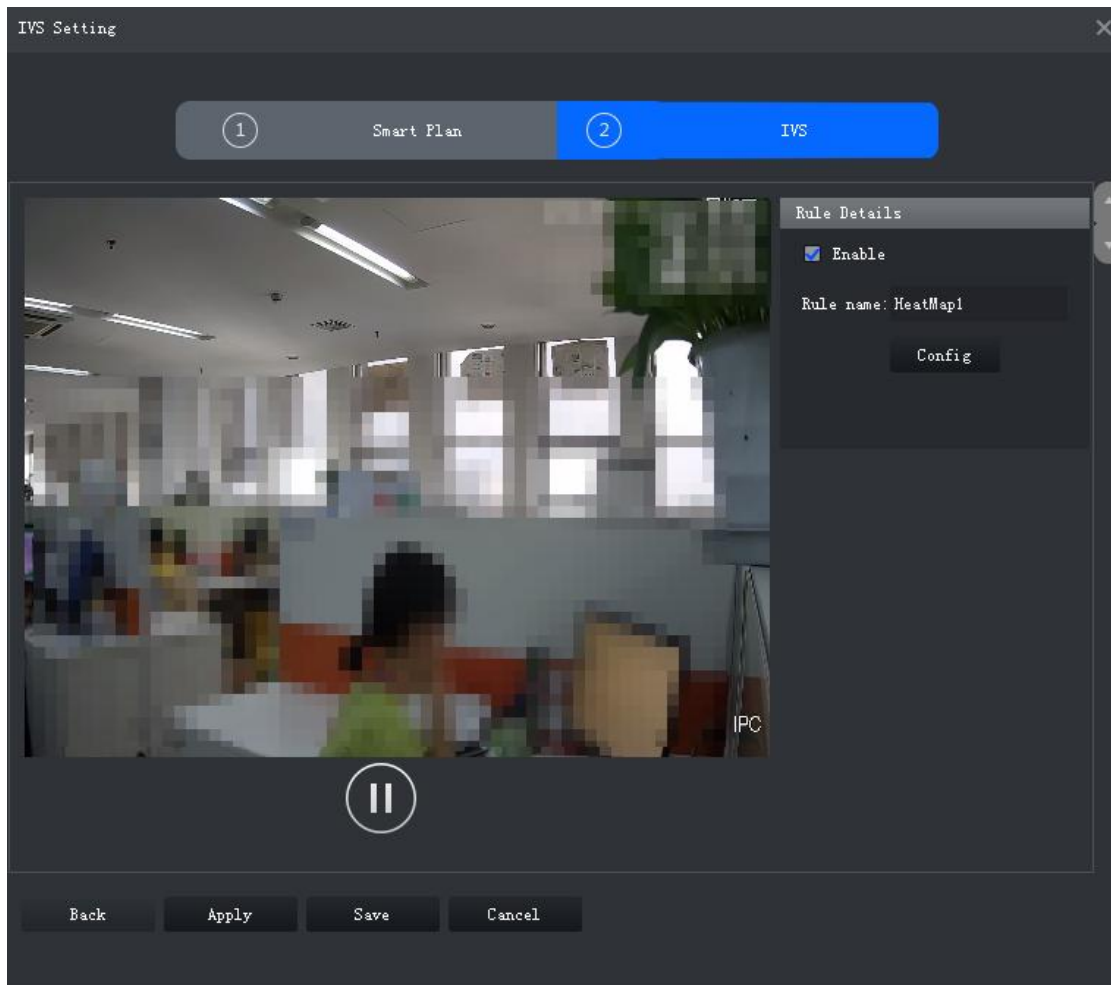


Figure 4-247 Heatmap



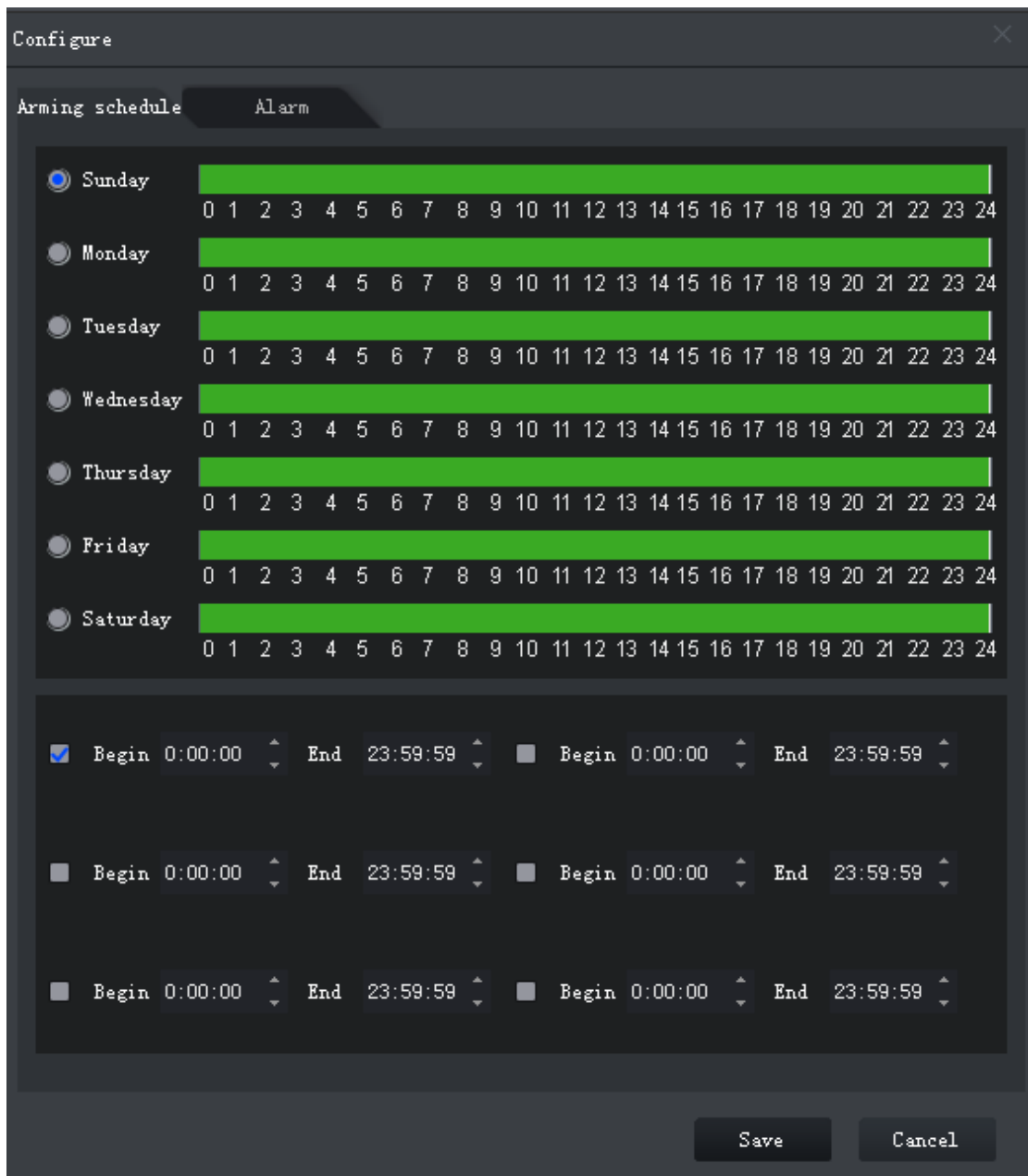
Step 3 Select the **Enable** check box to enable heatmap.

Step 4 Modify rule name.

Step 5 Configuring arming schedule and alarm linkage.

1) Click **Config**.

Figure 4-248 Configure



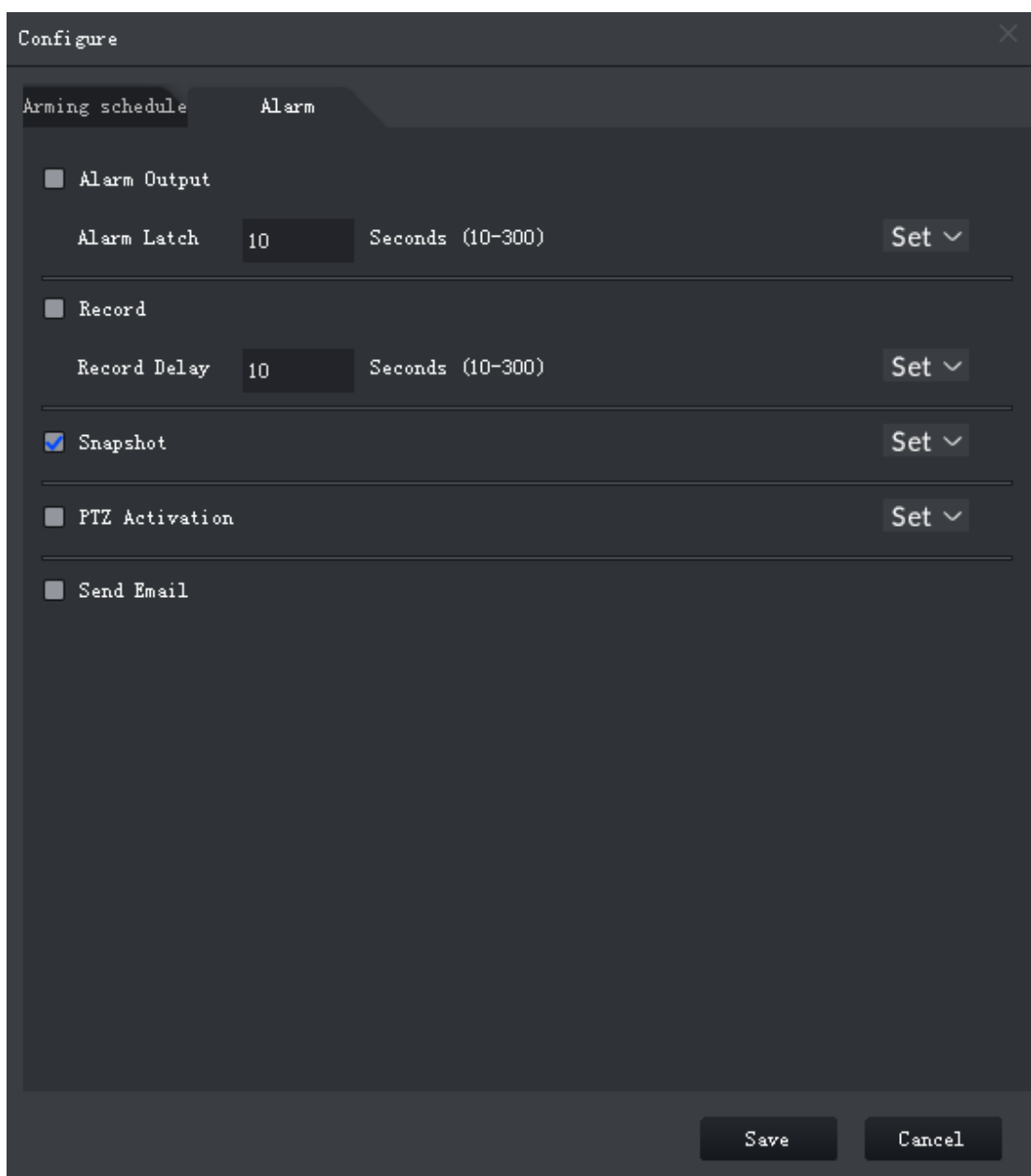
- 2) Click **Arming schedule**, select day and hours, and then set the start time and end time.



The default arming schedule is 24 hours per day.

- 3) Click **Alarm** to set linkage actions.

Figure 4-249 Alarm



Configure

Arming schedule Alarm

Alarm Output

Alarm Latch 10 Seconds (10-300) Set ▾

Record

Record Delay 10 Seconds (10-300) Set ▾

Snapshot Set ▾

PTZ Activation Set ▾




Send Email

Save Cancel

Table 4-50 Parameters

Parameter	Description
Alarm output	Connect alarm output devices to the alarm output interfaces. When an alarm is triggered, the system will send the alarm to the alarm output device.
Alarm latch	The alarm output action will delay stopping after the the alarm event ends.

Click Set next to **Alarm Latch** and select an alarm output channel.

Parameter	Description	
Record	When an alarm happens, it will trigger auto video recording immediately.  It requires the device to have recording schedules already. See device manual for detailed instruction.	Click Set next to Record to select the recording channel.
Record delay	Video recording delays stopping for a while after the alarm event ends.	
Snapshot	The system will take snapshots automatically when an alarm happens.  It requires the device to have snapshot schedules already. See device manual for detailed instruction.	Click Set next to Snapshot to select the snapshot channel.
Send email	The system will send an email to the related mail address when an alarm happens.  It requires the device to have email configured already. See device manual for detailed instruction.	None

4) Click **Save**.

Step 6 Click **Save**.


4.15.3.3 Configuring People Counting

Configure people counting settings to analyze the number of people entry and exit.



You can configure people counting on the platform only when the camera is directly connected to the platform. Otherwise, configure it on the camera or NVR.

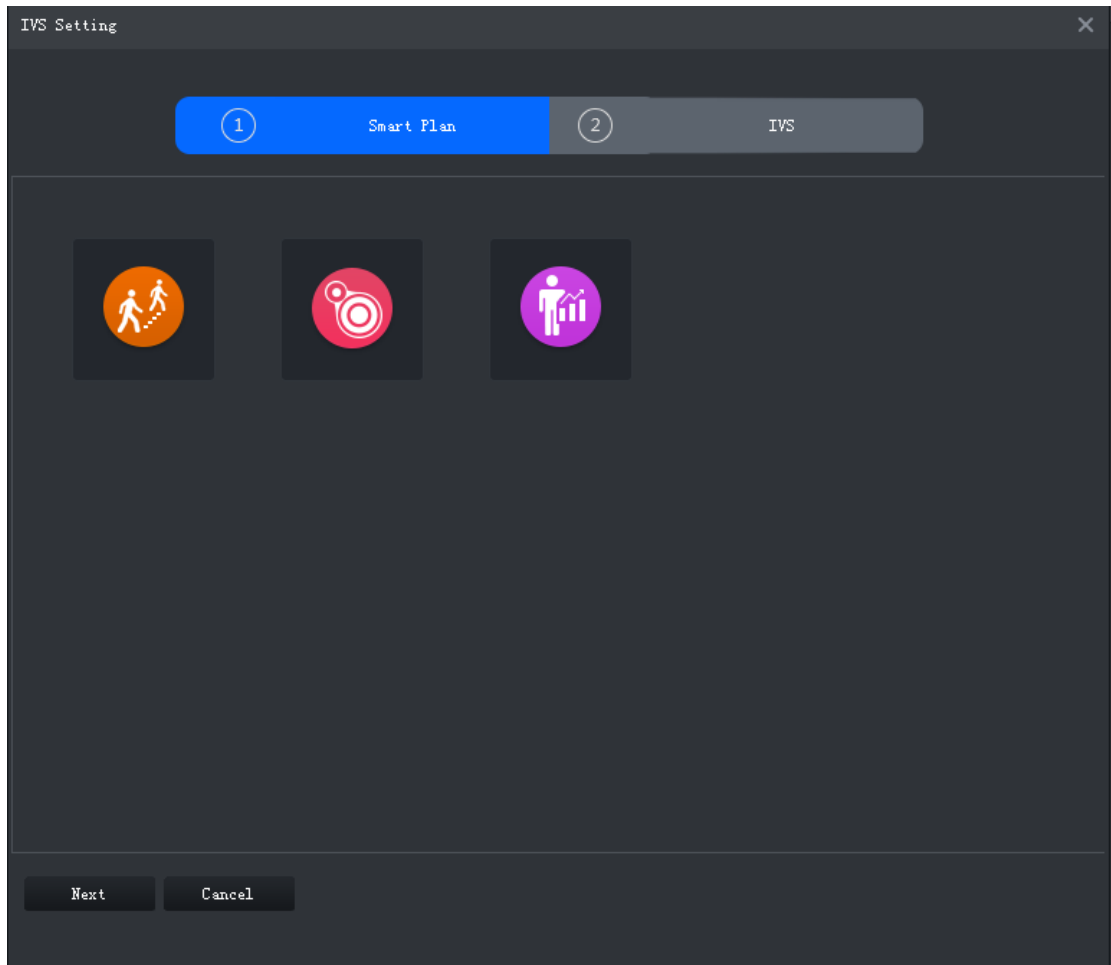
Step 1 Go into the **Intelligent Analyze** interface.

Step 2 Click  to select people counting.

When the icon is displayed in the white frame, the smart plan is selected. If another smart plan, which is conflicting with people counting, is selected, click that smart plan

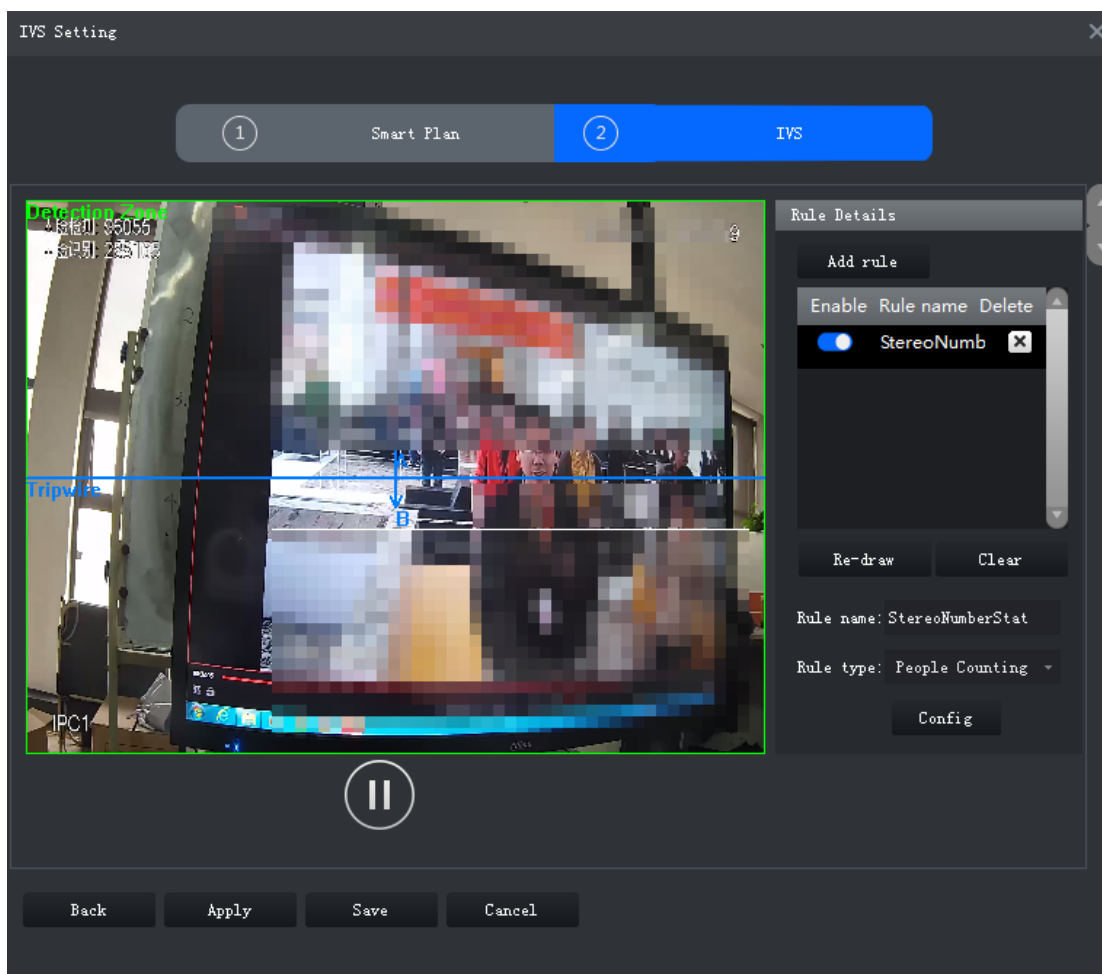
icon to deselect it and then click  to select people counting.

Figure 4-250 Smart plan



Step 3 Click **Next**.
The **IVS Setting** interface is displayed.

Figure 4-251 People counting



Step 4 Click **Add rule**.

Step 5 Enable rule and modify the name and type.

- 1) Enable rule. indicates rule is enabled.
- 2) Modify rule name.
- 3) Select rule type in the drop-down list of **Rule type**.
 - ◇ **People Counting**: System detects the number of people entry and exit in the detection zone. When the number of entry/exit/stay exceeds the preset value, system will trigger an alarm.
 - ◇ **ManNumDetection**: System detects people number and the duration of stay inside the detection zone. When the people number or duration of stay exceeds the preset value, system will trigger an alarm.

Step 6 Select the default zone or line on the video and click **Clear** to delete it or **Re-draw** to draw a new one.

People counting requires to draw a detection zone and a line while **ManNumDetection** requires only a detection zone.

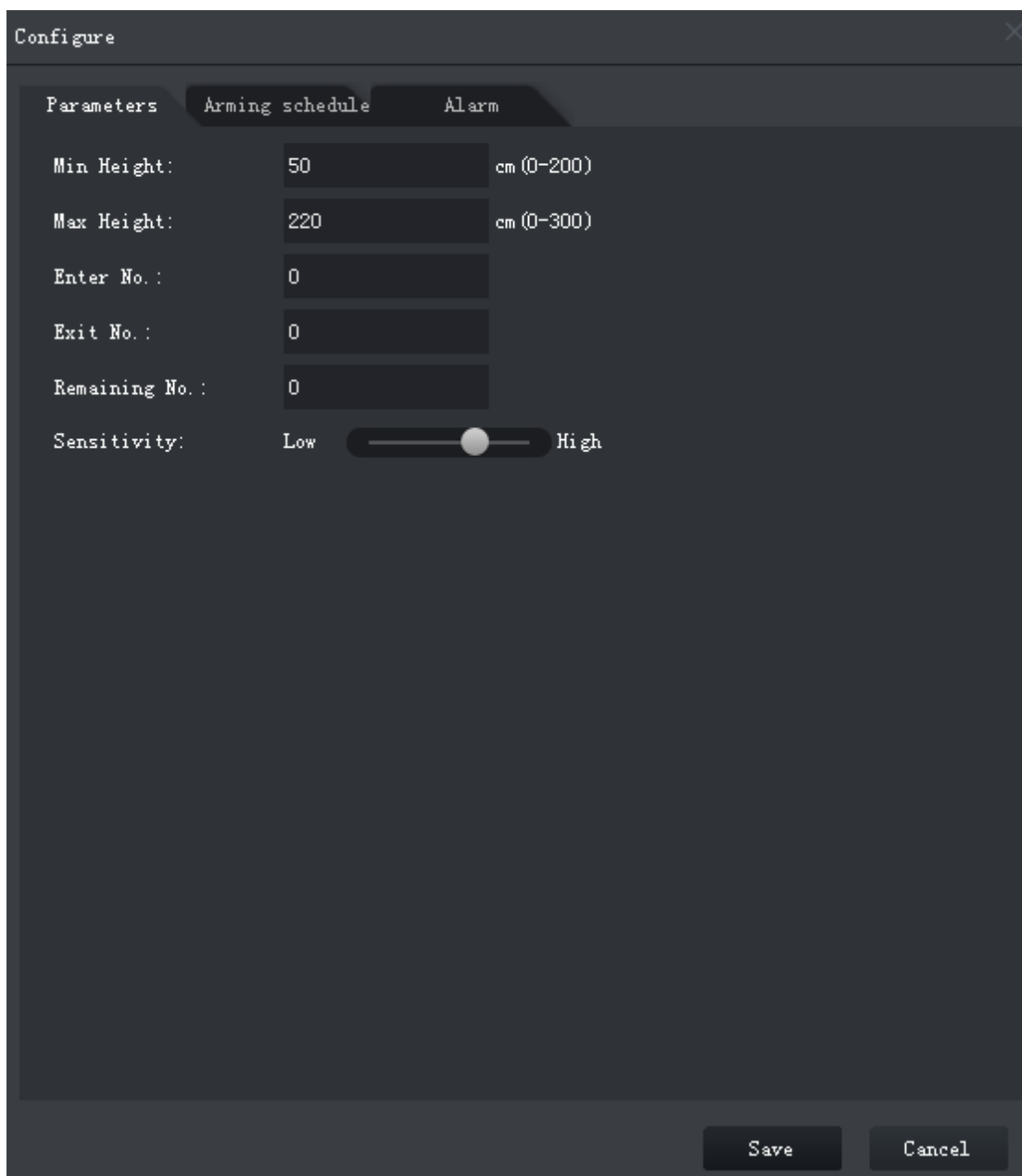


When drawing the line from left to right, the direction is A to B, and then people flow from A to B is entry number and B to A is exit number. When drawing the line from right to left, the direction is B to A, and then people flow from B to A is entry number and A to B is exit number.

Step 7 Set parameters, arming schedule and alarm linkage.

- 1) Click **Config** and set parameters.

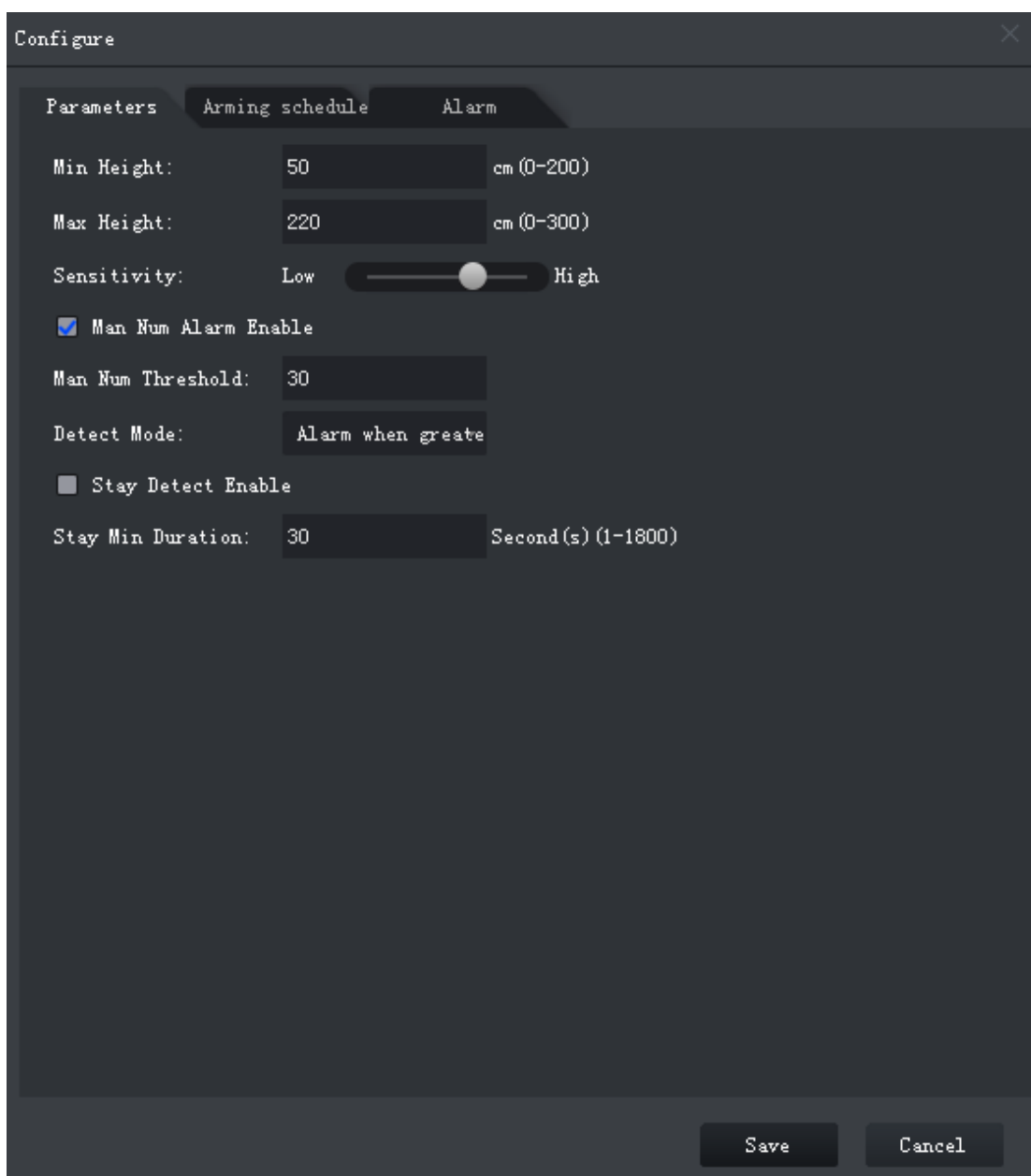
Figure 4-252 Set parameters (People counting)



Parameter	Value	Range
Min Height:	50	cm (0-200)
Max Height:	220	cm (0-300)
Enter No.:	0	
Exit No.:	0	
Remaining No.:	0	
Sensitivity:	Low	Low to High

Buttons: Save, Cancel

Figure 4-253 Set parameters (ManNumDetection)



Configure

Parameters Arming schedule Alarm

Min Height: 50 cm (0-200)

Max Height: 220 cm (0-300)

Sensitivity: Low High

Man Num Alarm Enable

Man Num Threshold: 30

Detect Mode: Alarm when create

Stay Detect Enable

Stay Min Duration: 30 Second(s) (1-1800)

Save Cancel

Table 4-51 Parameters

Parameter	Description
Min Height	When the target height is between the minimum height and maximum height, system will trigger the statistics rule.
Max Height	
Man Num Alarm Enable	When the people number in the zone reaches, exceeds or is smaller than the preset value, system will trigger an alarm.
Man Num Threshold	
Detect Mode	
Stay Detect Enable	When the people stay time in the zone is exceeds the preset value, system will trigger an alarm.

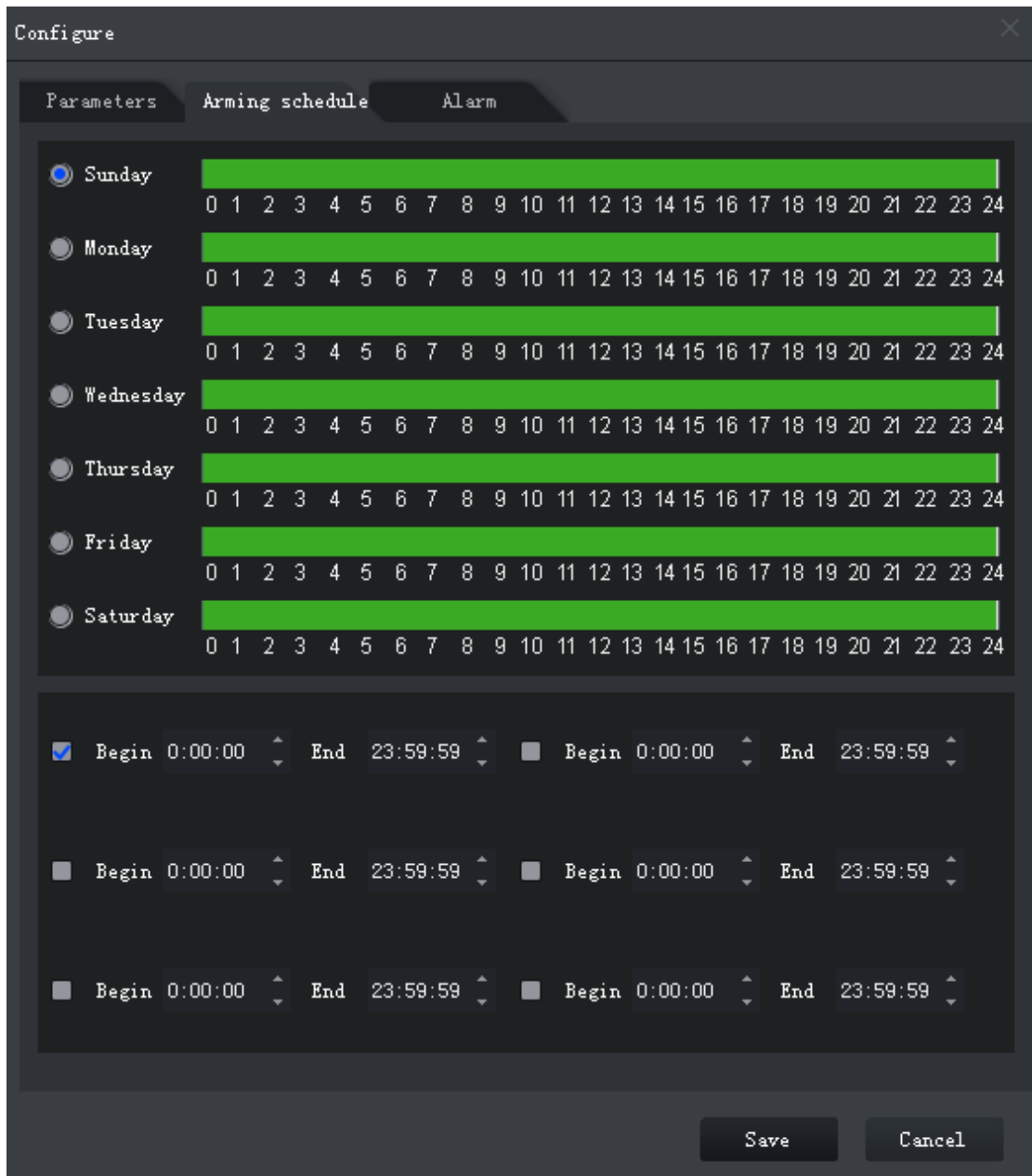
Parameter	Description
Stay Min Duration	
Enter No.	When the entry number exceeds the preset value, system will trigger an alarm.
Exit No.	When the exit number exceeds the preset value, system will trigger an alarm.
Remaining No.	When the remaining people number exceeds the preset value, system will trigger an alarm.
Sensitivity	It is recommended to keep the default value.

- 2) Click **Arming schedule**, select day and hours and then set the start time and end time.



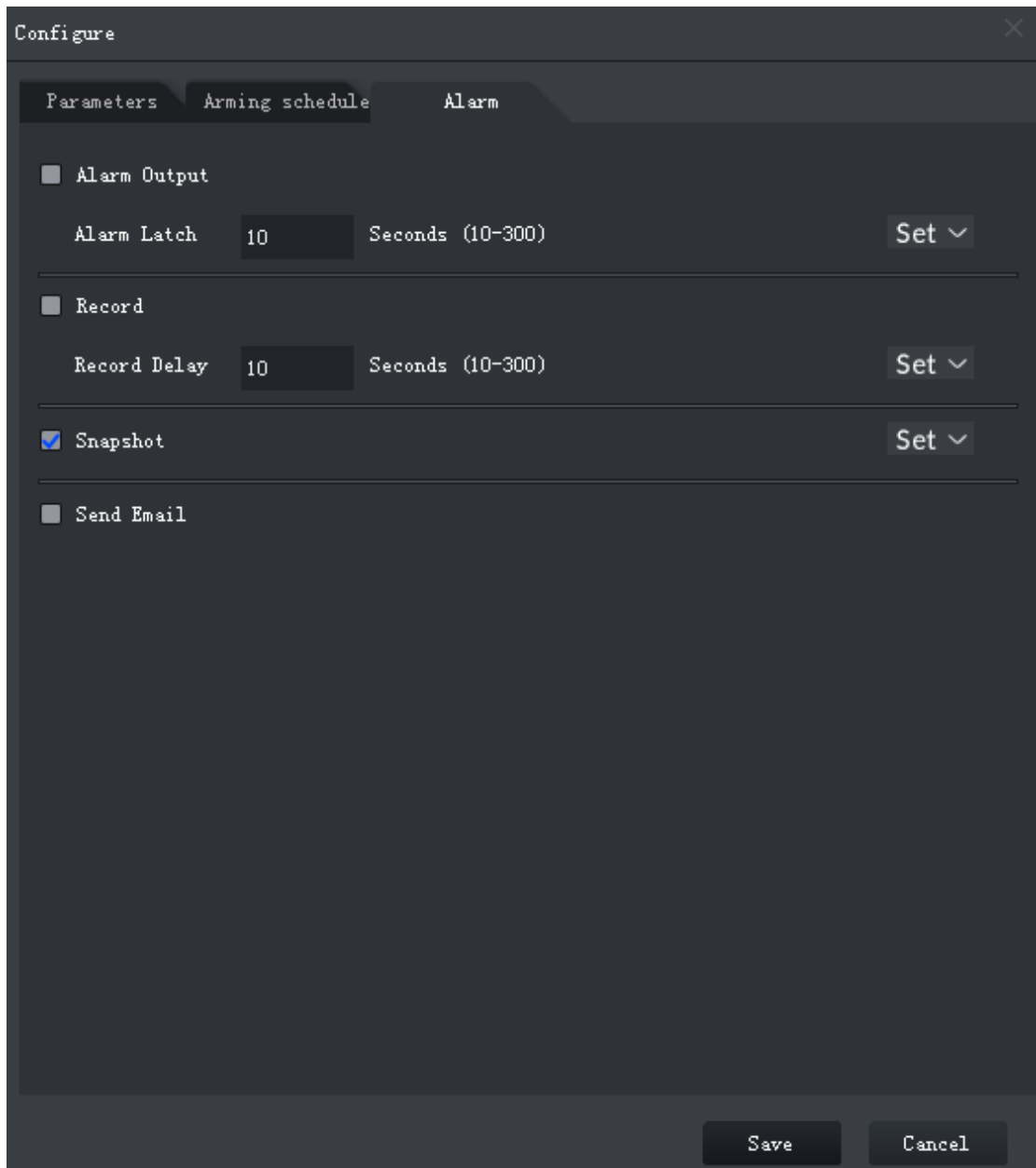
The default arming schedule is 24 hours per day.

Figure 4-254 Arming schedule



3) Click **Alarm** to set linkage actions.

Figure 4-255 Alarm



The screenshot shows a 'Configure' window with three tabs: 'Parameters', 'Arming schedule', and 'Alarm'. The 'Alarm' tab is active. It contains the following settings:




- Alarm Output
- Alarm Latch: 10 Seconds (10-300) [Set ▼]
- Record
- Record Delay: 10 Seconds (10-300) [Set ▼]
- Snapshot [Set ▼]
- Send Email

At the bottom of the window are 'Save' and 'Cancel' buttons.

Table 4-52 Parameters

Parameter	Description
Alarm output	Connect alarm output devices to the alarm output interfaces. When an alarm is triggered, the system will send the alarm to the alarm output device.
Alarm latch	The alarm output action will delay stopping after the alarm event ends.

Click **Set** next to **Alarm Latch** and select an alarm output channel.

Parameter	Description	
Record	When an alarm happens, it will trigger auto video recording immediately.  It requires the device to have recording schedules already. See device manual for detailed instruction.	Click Set next to Record to select the recording channel.
Record delay	Video recording delays stopping for a while after the alarm event ends.	
Snapshot	The system will take snapshots automatically when an alarm happens.  It requires the device to have snapshot schedules already. See device manual for detailed instruction.	Click Set next to Snapshot to select the snapshot channel.
Send email	The system will send an email to the related mail address when an alarm happens.  It requires the device to have email configured already. See device manual for detailed instruction.	

4) Click **Save**.

Step 8 Click **Save**.

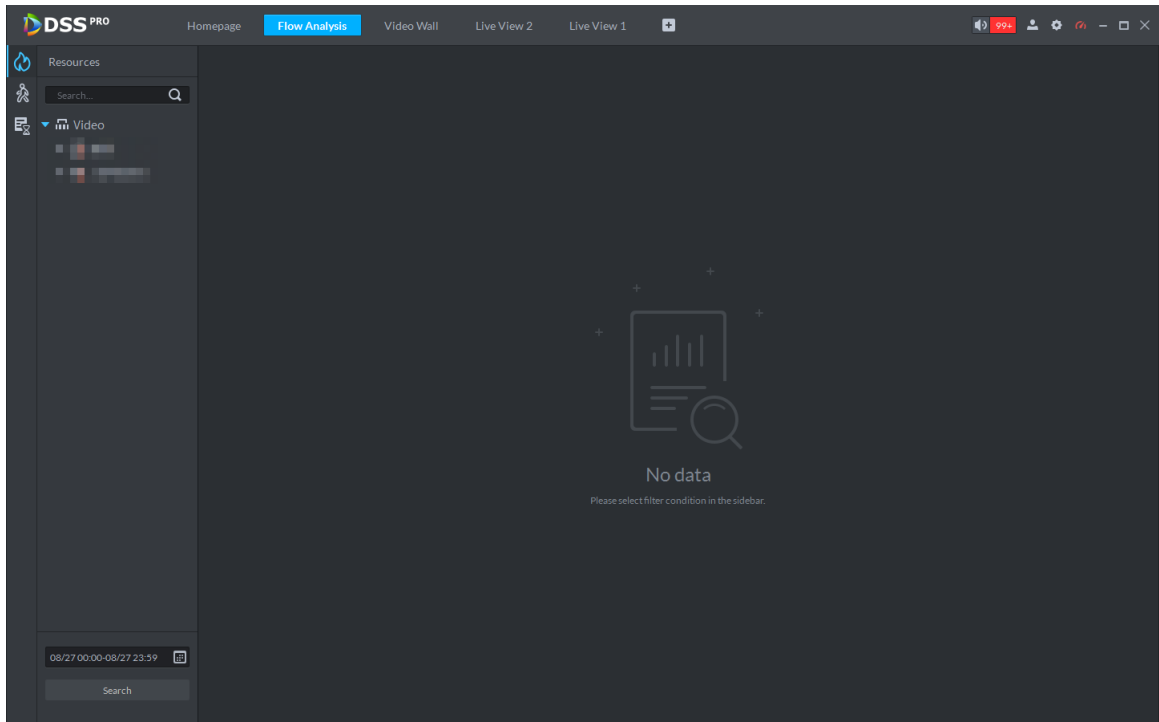
4.15.4 Flow Analysis Applications


4.15.4.1 Heatmap

Heatmap displays the distribution of moving objects in colors of different shades. It reflects the temperature of regions by different colors. For example, red means the temperature is relatively high, and blue means the temperature is relatively low.

Step 1 Click  on the homepage, and then click **Flow Analysis**.

Figure 4-256 Heatmap



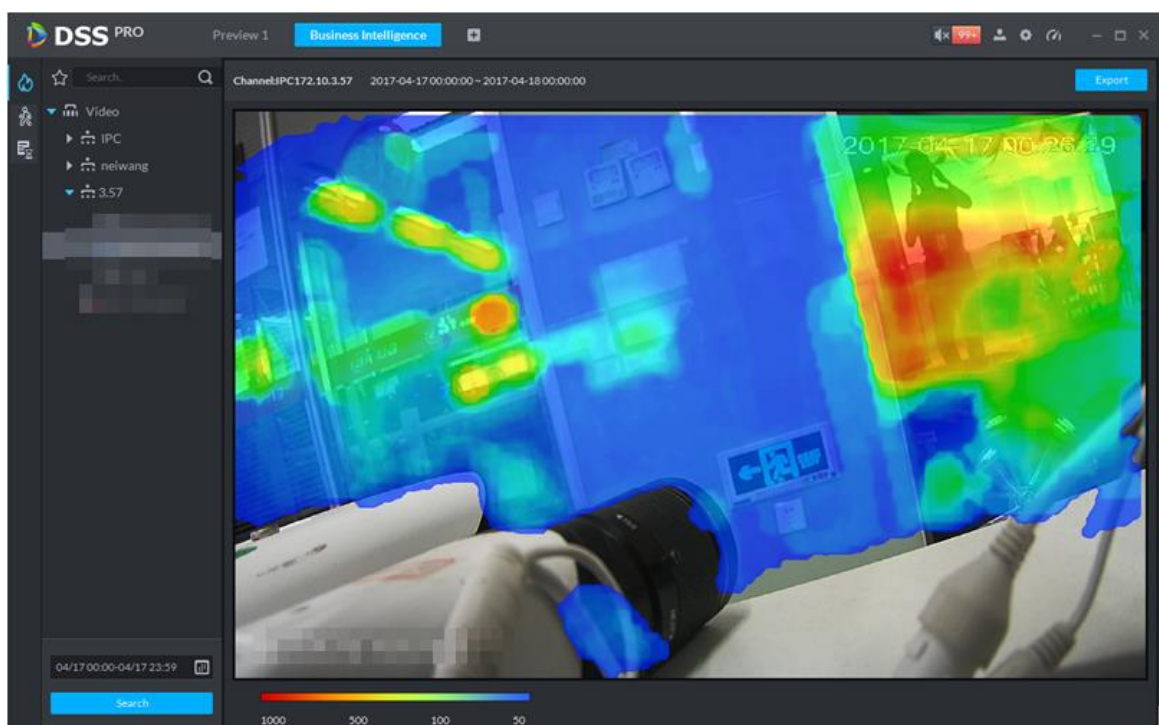
Step 2 Click the  tab on the flow analysis interface.

Step 3 Select a channel, set time, and then click **Search**.



The device sends heatmap data to platform in real time. Heatmap data of a channel can be searched once the channel is added to the platform. You can only search within a week at one time.

Figure 4-257 Heatmap interface



Step 4 Click **Export** at the upper-right corner to export heat map in .bmp format.

4.15.4.2 People Counting Report

View reports of the numbers of people entry and exit in a specific time period. A day report also includes the number of people who has not yet left the target area in the defined period.

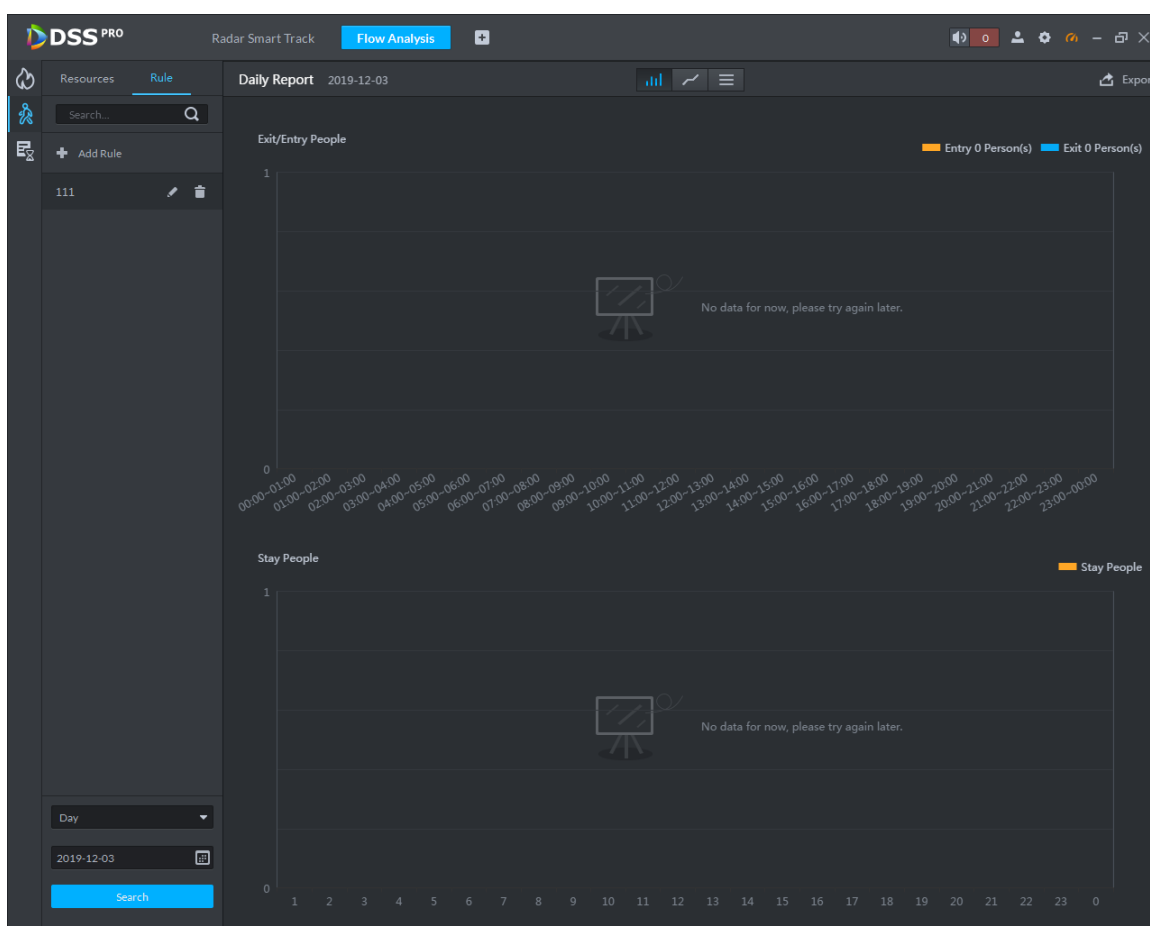
The statistics can be generated by camera or by people-counting rule.

4.15.4.2.1 Generating Report by Camera

Select the camera of interest to view the people-counting statistics. For example, if your store has one door, to view the total number of people entry and exit from your store, select the people-counting camera for generating the report.


Step 1 On the **Flow Analysis** interface, click 

Figure 4-258 People counting interface



Step 2 Click the **Resources** tab.

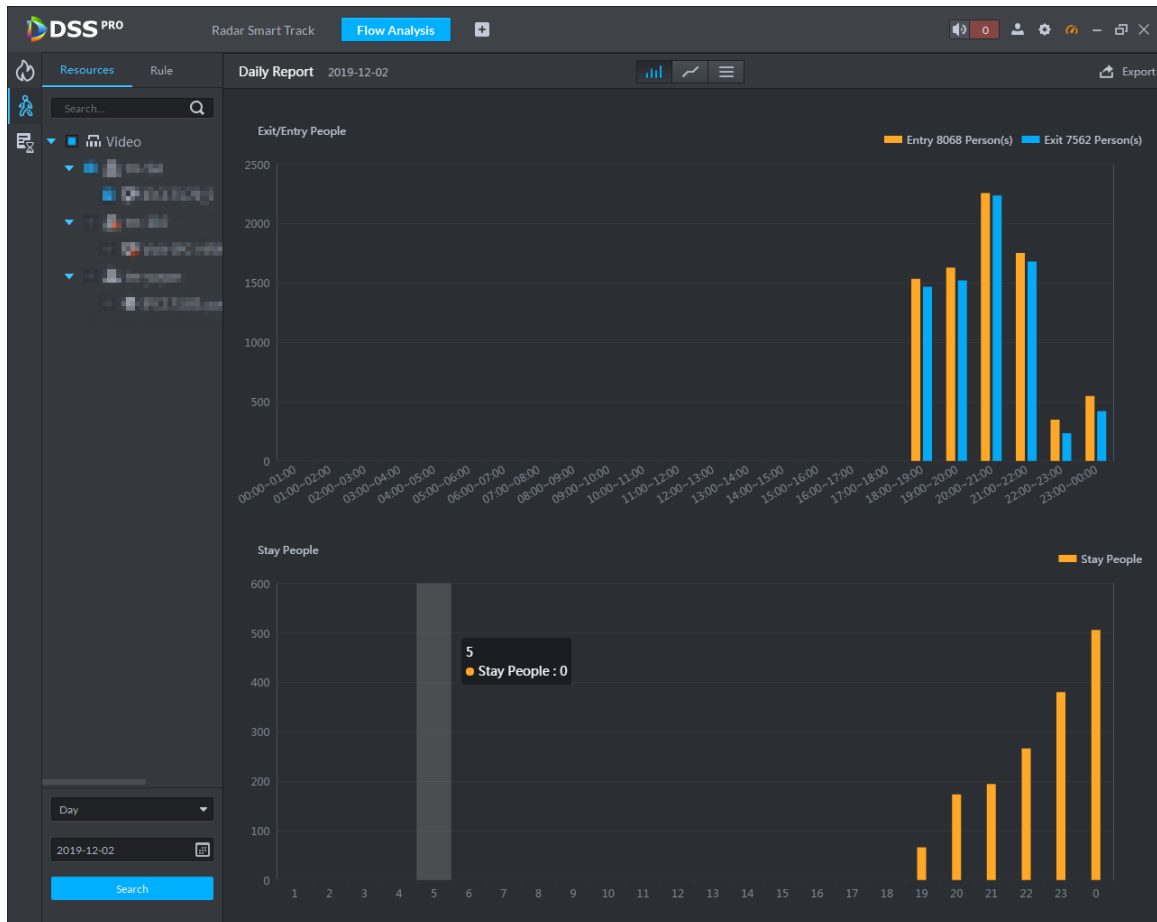
Step 3 Select a people-counting channel, set report type and search time, and then click **Search**. The report is displayed.

To switch to line chart or list, click the corresponding tabs on .



Stay People report (number of people still in a place) is only available for the daily report.

Figure 4-259 People-counting report by camera



Step 4 To save the report, you can click **Export** at the upper-right corner. The report is exported in the .pdf format.

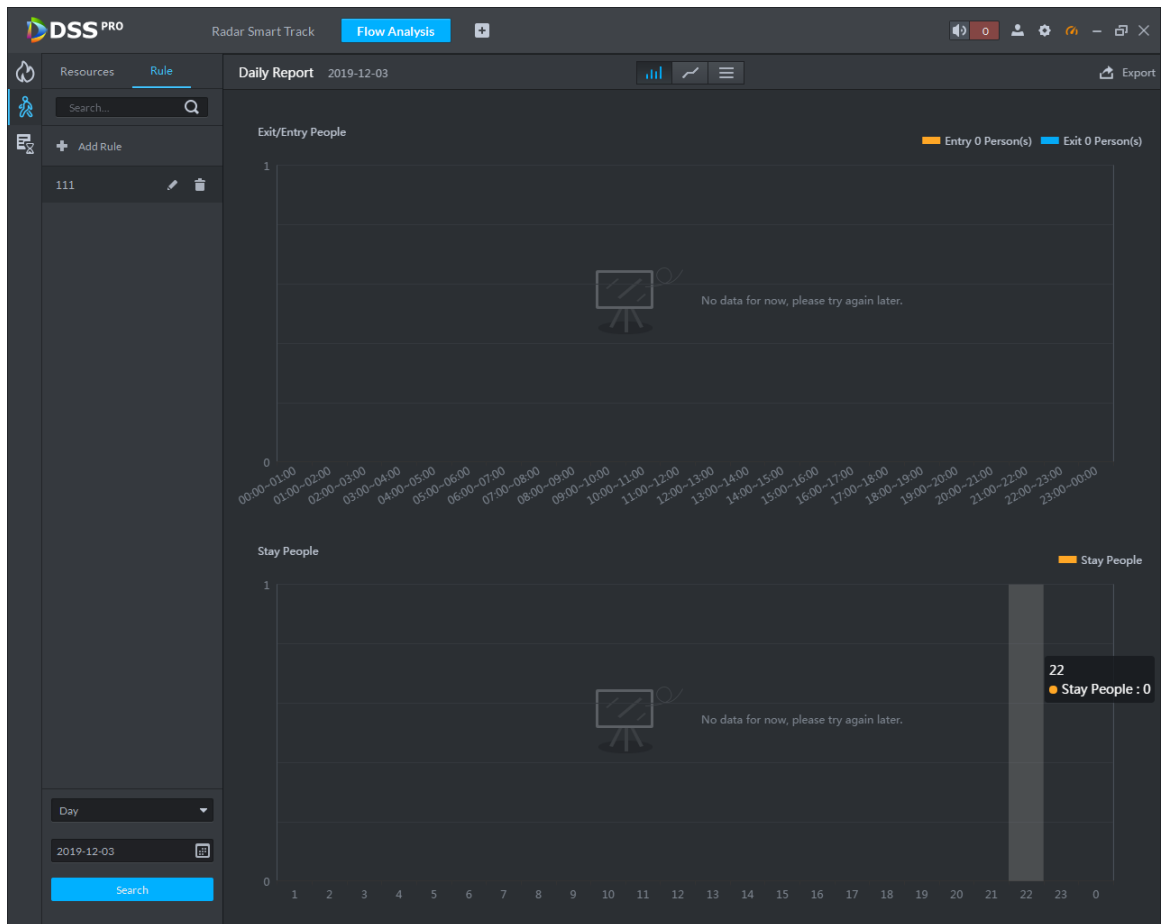
4.15.4.2.2 Generating Report by People-Counting Tripwire

To view the people-counting report of an area, if the total statistics result must be generated from multiple people-counting tripwires, you can select all the relevant tripwires for generating the report.

Step 1 On the **Flow Analysis** interface, click 

Step 2 Click the **Rule** tab.

Figure 4-260 Rule interface



Step 3 Add rules.

- 1) Click **Add Rule**.

Figure 4-261 Add rule

- 2) Enter rule name.
- 3) Click **Add**, select a channel and one or more rules as needed.
If your store has two doors each equipped with a people-counting camera, you need to add both the two cameras, and select the corresponding rules from them.
- 4) Click **OK**.

Step 4 Click the rule name to select a rule, set the search period (day, week, month, or year), set the date from the calendar, and then click **Search**.
The report is generated. See Figure 4-262.

To switch to line chart or list, click the corresponding tabs on



Stay People report (number of people still in a place) is only available for the daily report.

Figure 4-262 People-counting report by rule



Step 5 To save the report, you can click **Export** at the upper-right corner. The report is exported in the .pdf format.

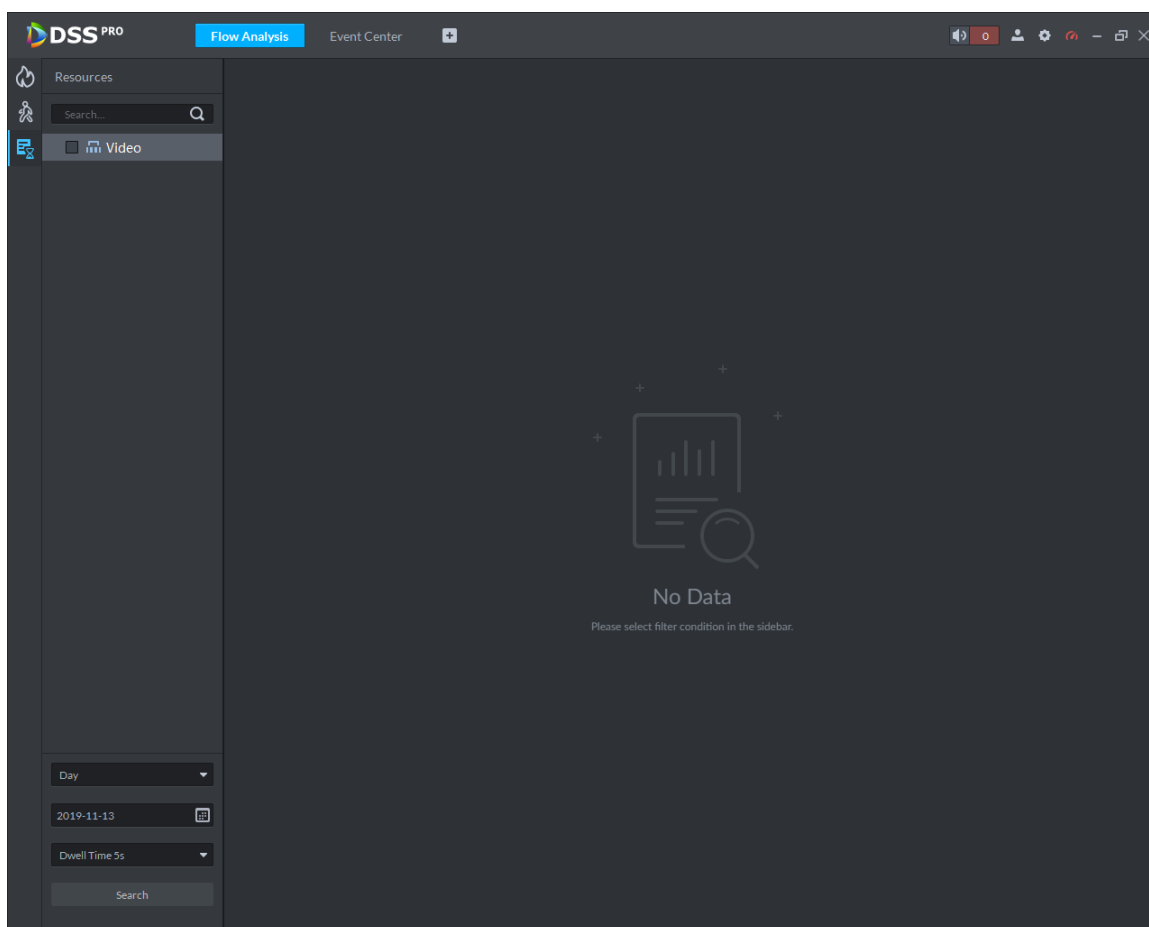
4.15.4.3 Dwell Time Report

With the people-counting cameras deployed at entrances and exits, the system can calculate the number of people that have stayed in an area for a specific period. You can view the daily, weekly and monthly report on the Control Client.

For example, to view the daily report of the number of people that stayed in an area for 5 seconds, see the following procedure.

Step 1 On the **Flow Analysis** interface, click

Figure 4-263 Dwell time report



Step 2 Select cameras, select **Day** in the **Day** drop-down list, set a date on the calendar, and then select **Dwell Time 5s** in the corresponding drop-down list. Click **Search**.
The report is displayed.

Step 3 (Optional) To export the report, click **Export**.

4.16 Human Face Recognition

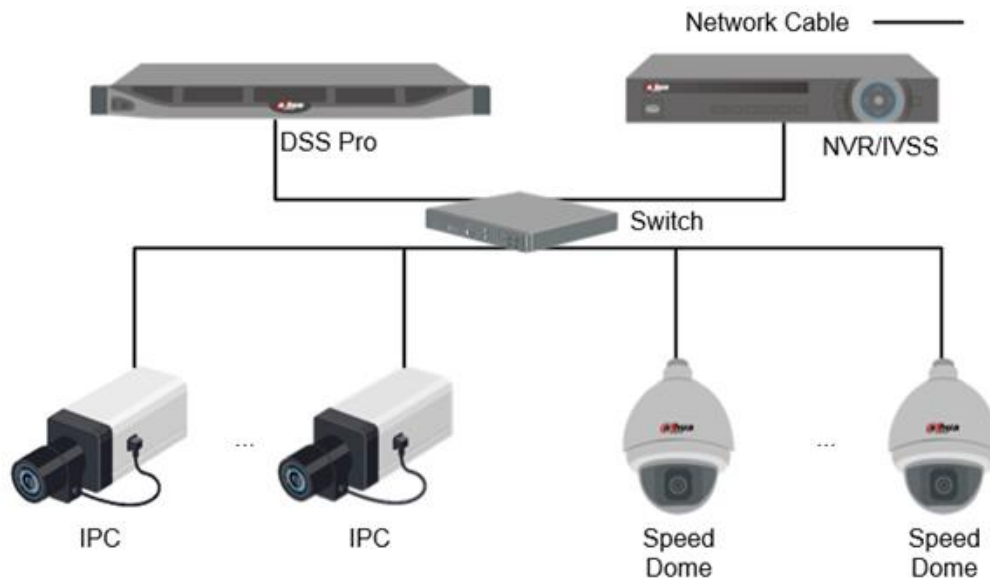
Configure face recognition settings on the device and the platform before you can view face recognition results on the platform.

4.16.1 Typical Topology

The face recognition feature is available on select models of NVR, IVSS and FR camera.

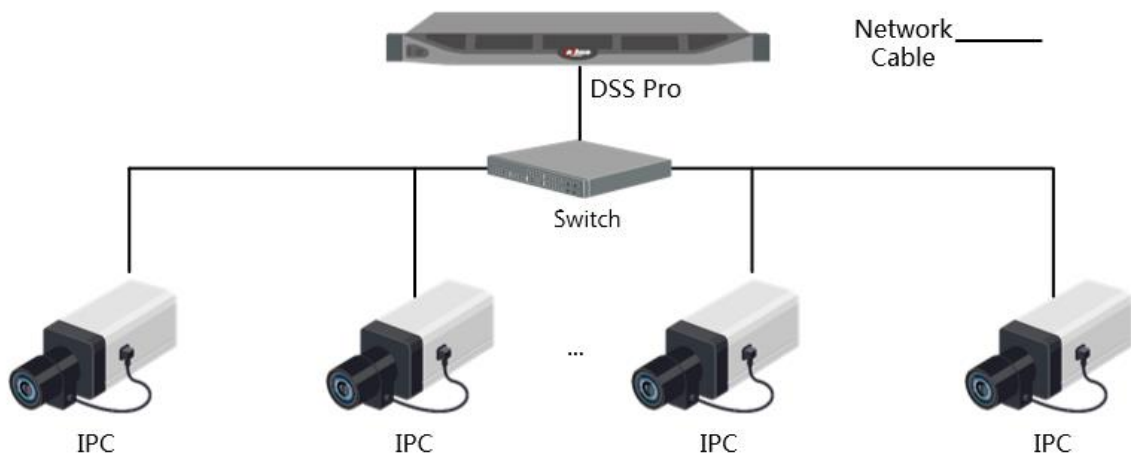
- Face recognition by NVR/IVSS

Figure 4-264 Typical topology (NVR/IVSS)



- ◇ Cameras record videos.
- ◇ NVR/IVSS is used for face recognition and storage.
- ◇ DSS Pro centrally manages cameras, NVRs, and face database, and provides live view and face search.
- Face recognition by camera

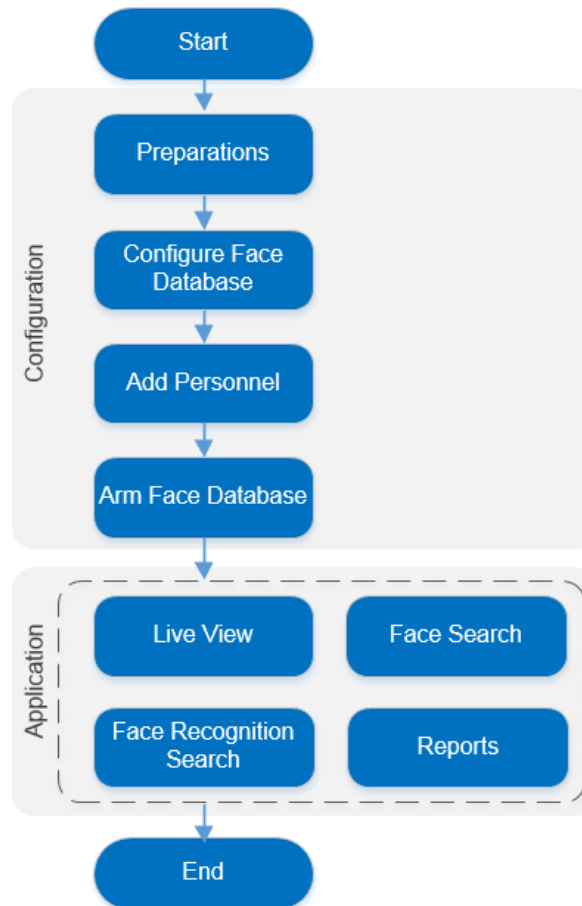
Figure 4-265 Typical topology (camera)



- ◇ Cameras collect face videos, detect and recognize faces.
- ◇ DSS Pro centrally manages cameras, NVRs, and face database, and provides live view and face search.

4.16.2 Business Flow

Figure 4-266 face recognition business flow



4.16.3 Configuring Face Recognition

4.16.3.1 Preparations

Make sure that the following preparations have been made:

- Face recognition devices are correctly deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding face recognition devices on the **Device** interface of Web Manager, select **Encoder** for device category.

Figure 4-267 Add device

- ◇ After adding a face recognition NVR or IVSS, set face recognition features for the corresponding channels.

On the **Device** interface, click of the NVR or IVSS, and then select **Face Recognition for Features**.

Figure 4-268 Edit features (1)

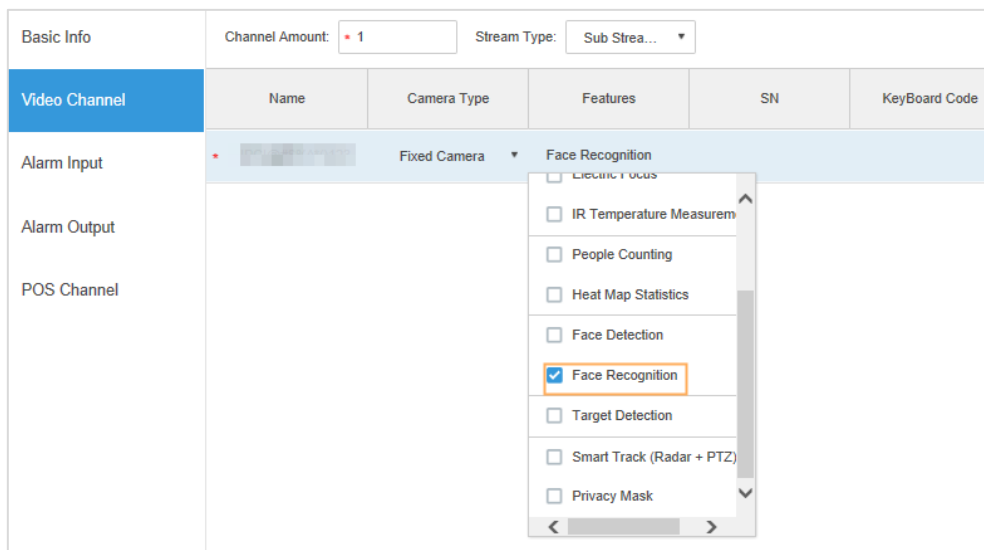
Video Channel	Name	Camera Type	Features	SN	KeyBoard Code
Alarm Input	* IP PTZ Camera	Speed Dome	Face Recognition		
Alarm Output	* Thermal	Speed Dome	<input type="checkbox"/> People Counting <input type="checkbox"/> Heat Map Statistics <input type="checkbox"/> Face Detection <input checked="" type="checkbox"/> Face Recognition <input type="checkbox"/> Target Detection <input type="checkbox"/> Access Snapshot <input type="checkbox"/> Smart Track (Radar + PTZ) <input type="checkbox"/> Privacy Mask		
POS Channel	* IPC	Fixed Camera			
HDCVI External	* IPC	Fixed Camera			
Alarm Box	* Visual	Fixed Camera			
	* Thermal	Fixed Camera			
	* IPC	Fixed Camera			

- ◇ On the **Device** interface, click of the face recognition camera or face detection camera, and then select **Face Recognition** or **Face Detection** for **Features**.



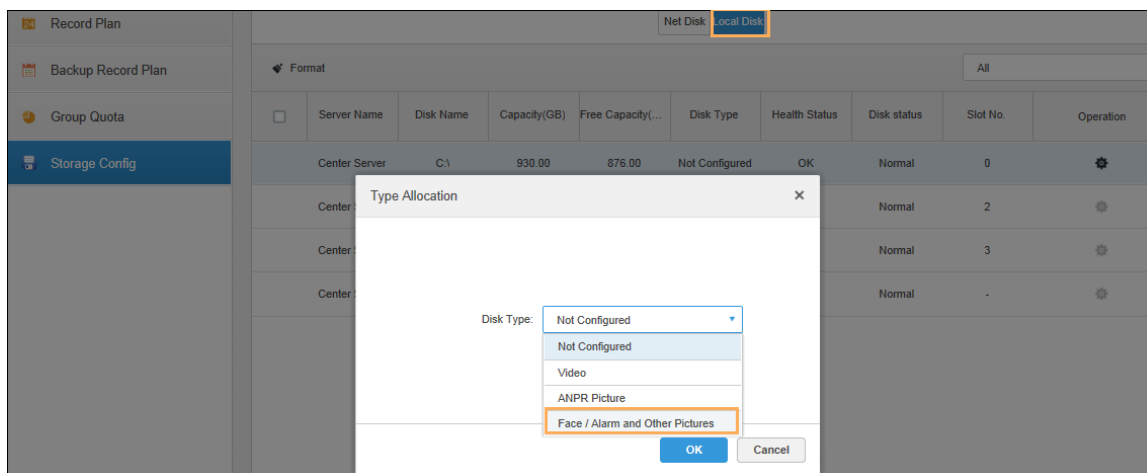
The platform can automatically obtain the features of the face recognition camera.

Figure 4-269 Edit features (2)



- ◇ Face snapshots are stored in the **Face/Alarm and Other Pictures** disk. On the **Storage Config** interface, configure at least one local disk for picture storage. Otherwise, the platform cannot display snapshots.

Figure 4-270 Set face snapshot storage disk



4.16.3.2 Configuring Face Database

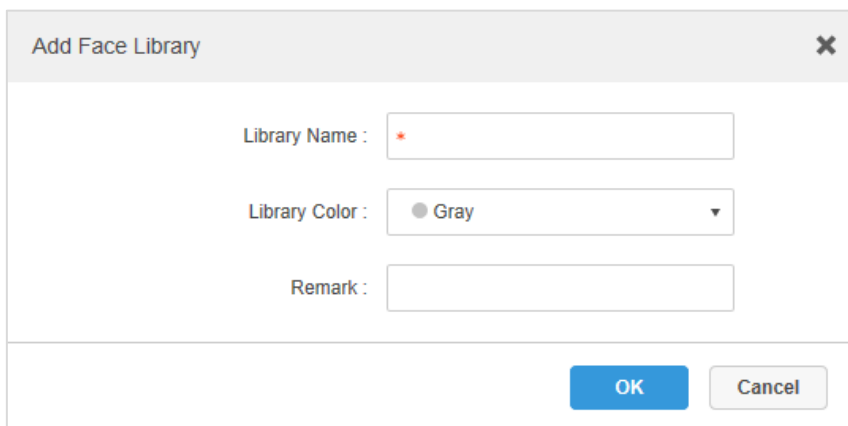
Configure face database which contains people face information, so the system can compare the detected face with those in the database to determine who it is and whether to let go. The platform supports up to 50 face databases.

4.16.3.2.1 Creating Face Database

Step 1 Click  on the Web Manager, and then select **Face Database**.




Step 2 Click **Add**.

Figure 4-271 Add a face database



Step 3 Enter database name, select color, and then click **OK**.

Other Operations

- Search database
Filter the database by face database type or keyword.
- Add face database
Click  to add face information.
- Modify database
Click  to modify database name and database description.
- Delete database
Click  .


4.16.3.2.2 Configuring Person Type

Up to 16 types are allowed. Face alarms can be configured and triggered by people type.

Step 1 Click the face database which needs to be added with person.

Step 2 Click **Person Type Config**.

Figure 4-272 Set person types

Person Type Config ✕		
+ Add ✕ Delete		
	Person Type	Operation
<input type="checkbox"/>	* 4	✕
<input type="checkbox"/>	* 3	✕
<input type="checkbox"/>	* 2	✕
<input type="checkbox"/>	* 1	✕
<input type="checkbox"/>	* TEST	✕
<input type="checkbox"/>		✕
<input type="checkbox"/>	* 11	✕
Total 7 record(s).		<input type="button" value="⏪"/> <input type="button" value="⏩"/> 1 / 1 <input type="button" value="⏪"/> <input type="button" value="⏩"/>
<input type="button" value="Close"/>		

Step 3 Click **Add** and enter type name in the column of **Person Type**. Support adding up to 16 person types.

Step 4 Click ✕ to disable the window.

4.16.3.2.3 Adding Face database Information

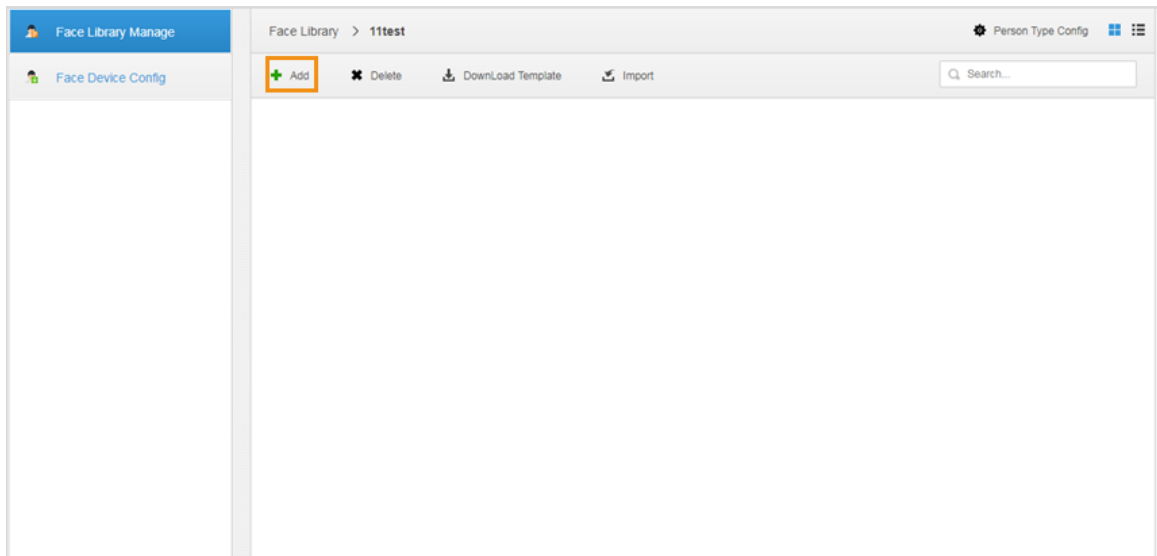
Add people information one by one or in batches. Face recognition is based on the matching between detected face and faces in the database. The platform supports up to 300 thousand faces.

Adding Faces One by One

Step 1 Enter people information interface in two ways:

- Click the database which needs to be added with people on the **Face database Manage** interface.

Figure 4-273 Add a face database




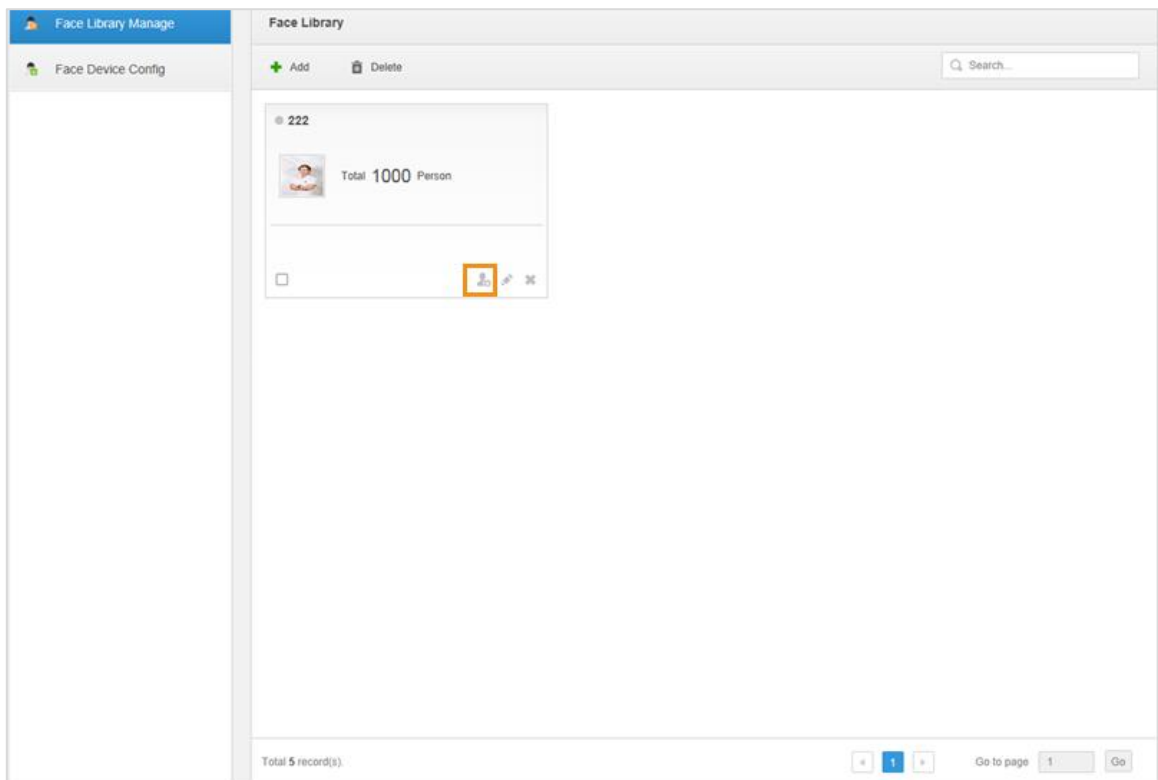
- Click  on the person card.

Figure 4-274 Set person details



Step 2 Enter person information.

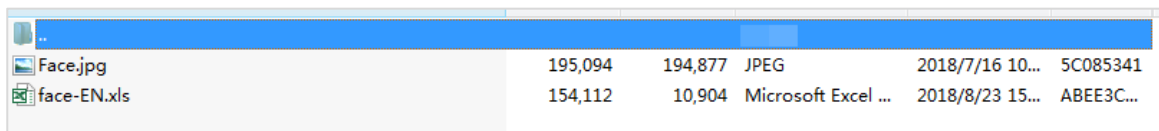
Step 3 Click profile photo and upload a face picture.

Step 4 Click **OK**.

Adding Faces in Batches

Prepare face pictures in advance if you want to import in batches, and compress it into zip, rar or 7z files. The ID cannot be repeated. Currently batch import supports max 10,000 pictures at one time.

Figure 4-275 Zip file

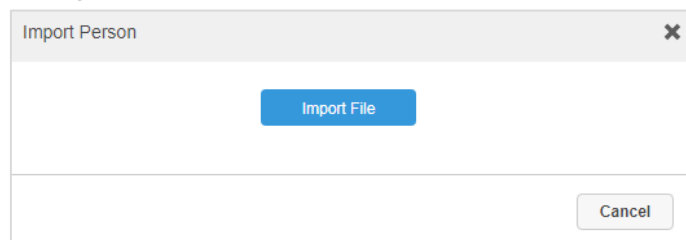


Face.jpg	195,094	194,877	JPEG	2018/7/16 10...	5C085341
face-EN.xls	154,112	10,904	Microsoft Excel ...	2018/8/23 15...	ABEE3C...

Step 1 Click the database to add people on the interface of **Face database Manage**.

Step 2 Click **Import**.


Figure 4-276 Import faces in batches (1)




Step 3 Click **Import File** and upload compressed package according to prompt.

Operations

- Query person

Enter key words into the query text box, and then press Enter or click .

- Delete person

- ◇ Click  on person interface and then you can delete person individually.
- ◇ Select person, and then click **Delete** to delete person in batches.

4.16.3.3 Arming Face Recognition Channels

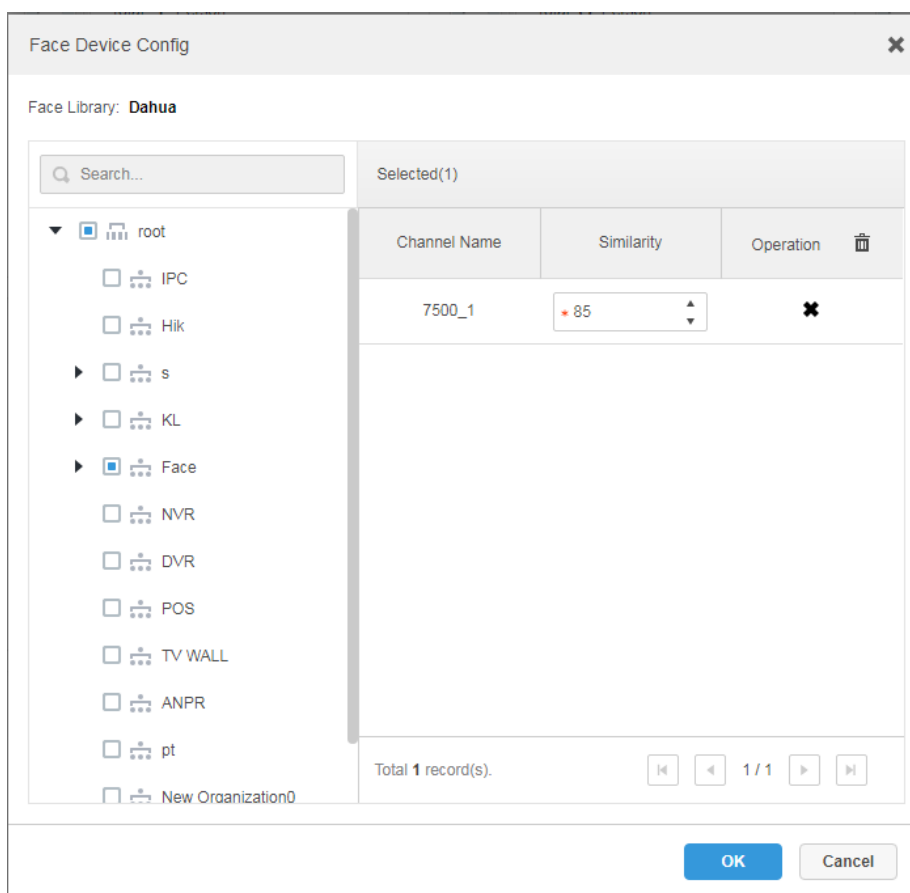
Enable real-time face recognition. To arm specific people, you can arm the face database of the people. The armed face database is sent to the devices.

Step 1 Click  and select **Face Database** on the **New Tab** interface.

Step 2 Click **Face Device Config** on the left of navigation bar.

Step 3 Click  to start arming.

Figure 4-277 Select a channel

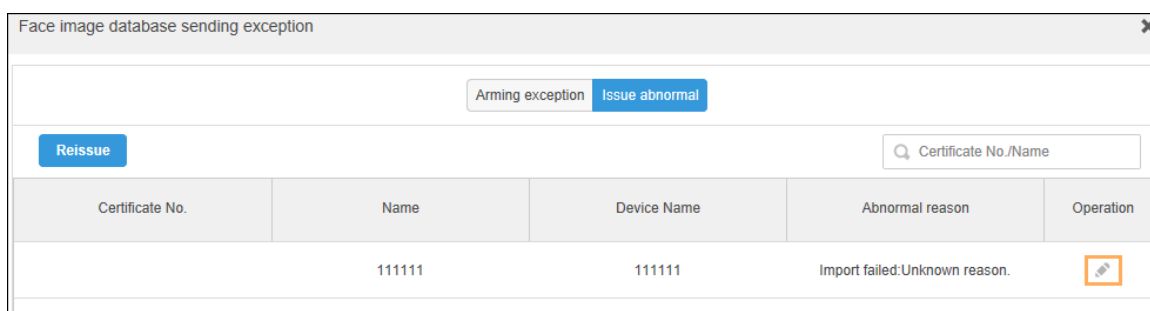


Step 4 Select the target channels, and then set similarity.

Step 5 Click **OK**.

- If the arming is prompted failed, appears on the database card. Click it to check detailed reason.
- To re-arm, click , modify people information, and then click **Reissue**.

Figure 4-278 Modify people information



Operations

- **Modify arm**
Arm has been implemented; click and it can modify related device and similarity value on the arm interface.
- **Disarm**

Click on the interface of Arm Manage to disarm.

4.16.4 Face Recognition Applications

View live or recorded face recognition videos and search for face records. You can search for records by face attributes, or by simply uploading a face image.

4.16.4.1 Real-Time Face Recognition

View face recognition in real time.

Step 1 Click on the Control Client, and then select **Face Recognition**.

Step 2 Click .

Figure 4-279 Live video

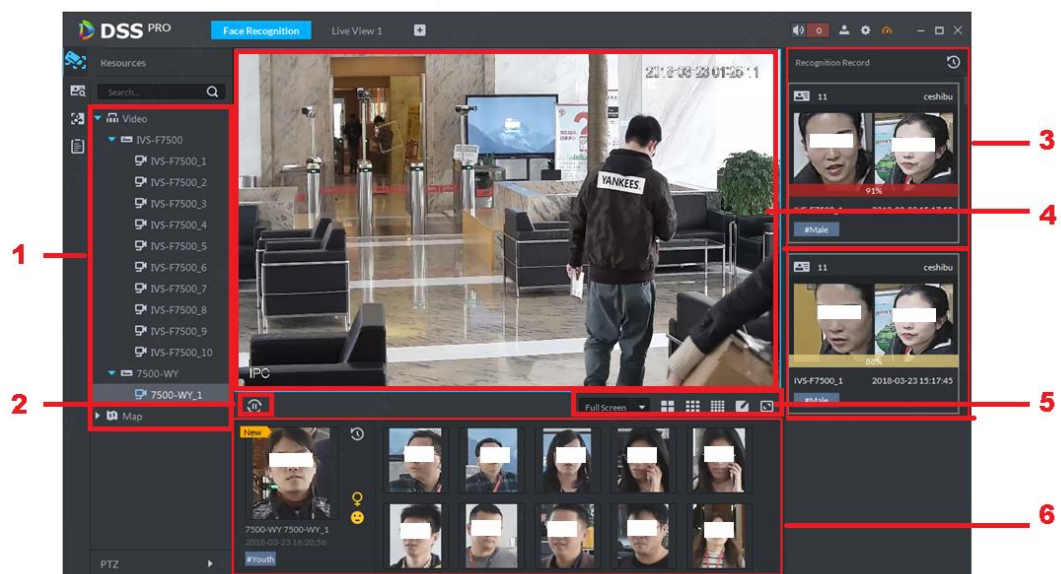


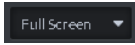




Table 4-53 Description

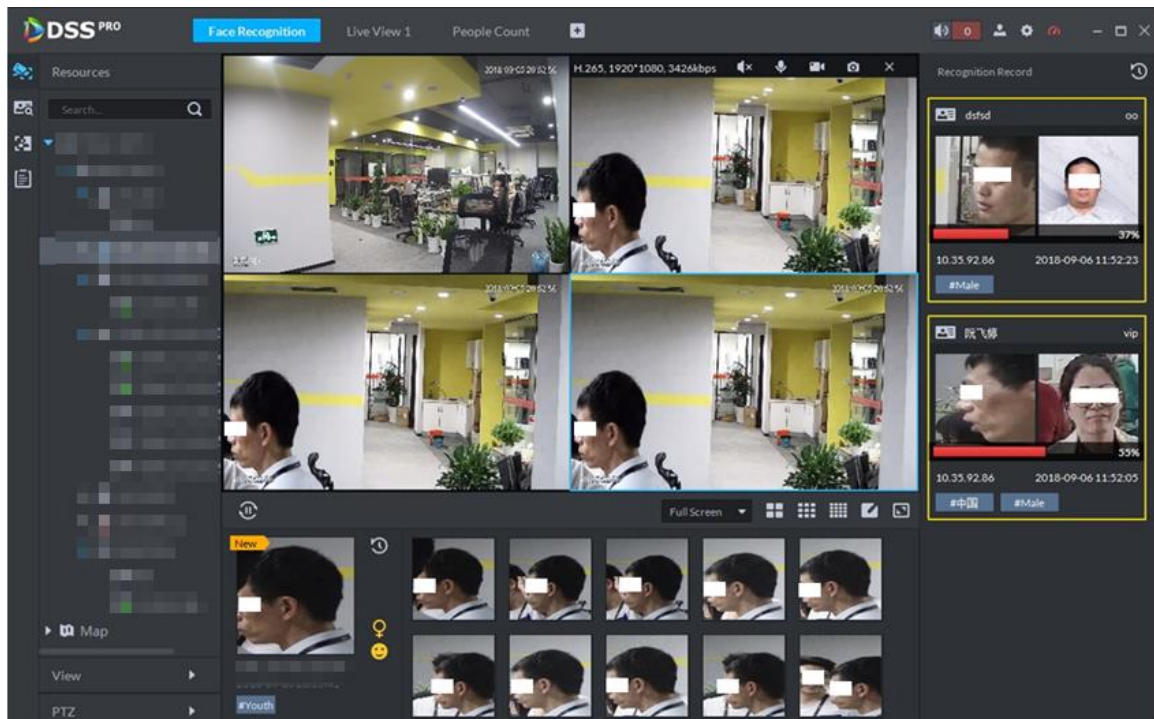
No.	Name	Description
1	Device Tree	Display face detection and face recognition device information.

No.	Name	Description
2	Pause Refresh/Start Refresh	<ul style="list-style-type: none"> : When this icon is on the interface, the snapshot display pane does not refresh human face snapshot image. Click the icon, system displays real-time face image. : When this icon is on the interface, the snapshot display pane refreshes human face snapshot image. Click the icon, system refreshes human face snapshot image.
3	Face Record	Display the face snapshots of the opened video channels.
4	Monitor Window	Display channel preview video. In multiple-window display mode, double-click the window to switch to 1-window display mode. Double-click the window again to restore original mode.
5	 Full Screen	Image Display Rate There are two modes: full screen, and original scale. The full screen refers to one window at the full screen.
		Window Split Switch Display switched window amount. System supports customized settings.
		Full Screen Display The system displays window at full screen.
6	Face Recognition Records	Display recognition records of the opened video channels.

Step 3 Enable live view.

- Select a monitor window, and then double-click a channel or record file.
- Drag the channel or the video file to the monitor window.

Figure 4-280 Enable live view



Step 4 Face monitoring.


- Double-click a snapshot image to view details
- Right-click the snapshot, and then you can register faces, search for faces, query tracks, and export snapshots.
- Right-click the recognition record, and then you can query recognition records and face tracks and export snapshots.

4.16.4.2 Face Search

With the human face recognition function, you can search the face databases or snapshot records for face pictures of interest by setting person features such as age and gender or uploading a face picture. The face database contains all registered faces; the snapshot records are all the faces captured by the cameras.



Searching by image is only available with IVSS and NVR.

Step 1 Click  on the Control Client, and then select **Face Recognition**.

Step 2 Click .

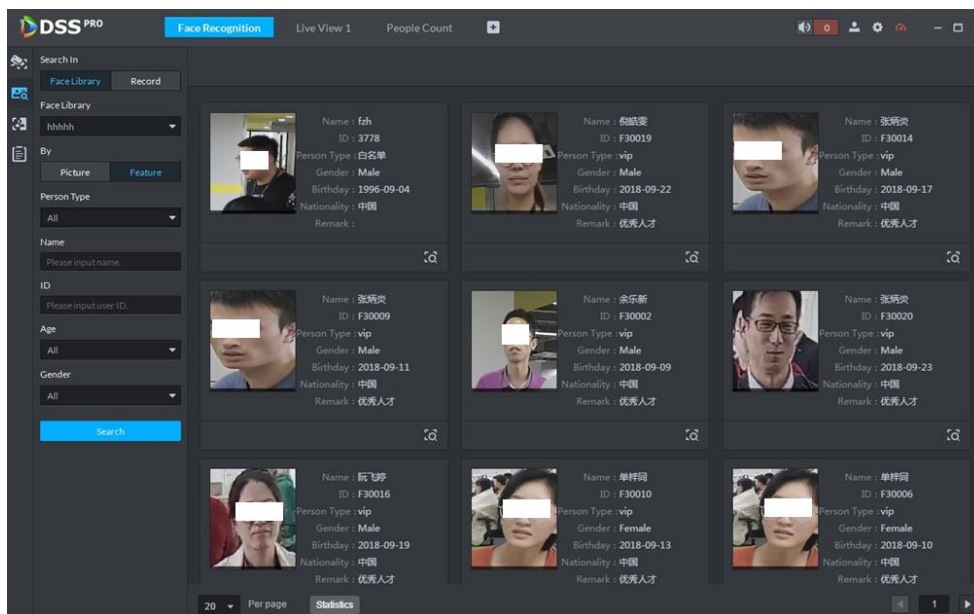
Step 3 Set search conditions.

- You can search the face database (by selecting the **Face database** option under **Search in**) or snapshot records (by selecting the **Record** option under **Search in**).
- You can upload a face picture to match or set target features to narrow down the conditions.

- When you search by Record or Picture, you can select **Start from Earliest Time** or **Start from Current Time** from the **Sequence** drop-down list to set time sequence for the results. Up to 1000 results can be displayed.

Step 4 Click **Search**.

Figure 4-281 Search result



When searching a face database, the results are displayed in list; when searching the snapshot records, you can choose to display the results in list or view face tracks on the map. To introduce search results, now we take searching snapshot records as an example.




- When searching the snapshot records by uploading a face picture, the search progress is displayed at the top-right corner. To end searching, click .
- It is not available to search for face tracks on map when you are searching the face database.
- The face track function is only available when you have linked the relevant cameras onto the map.
- Click **List**, and then the search results are displayed in list.

Figure 4-282 Search results in list

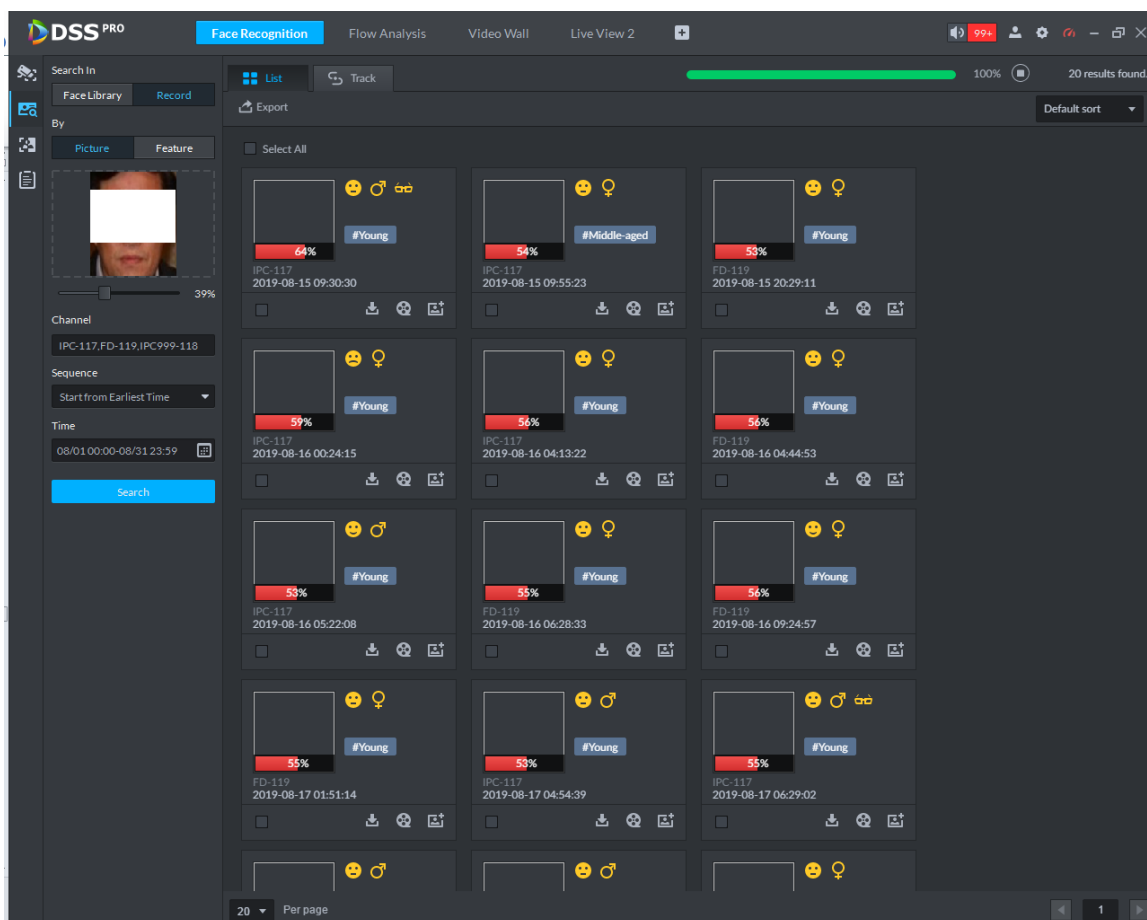




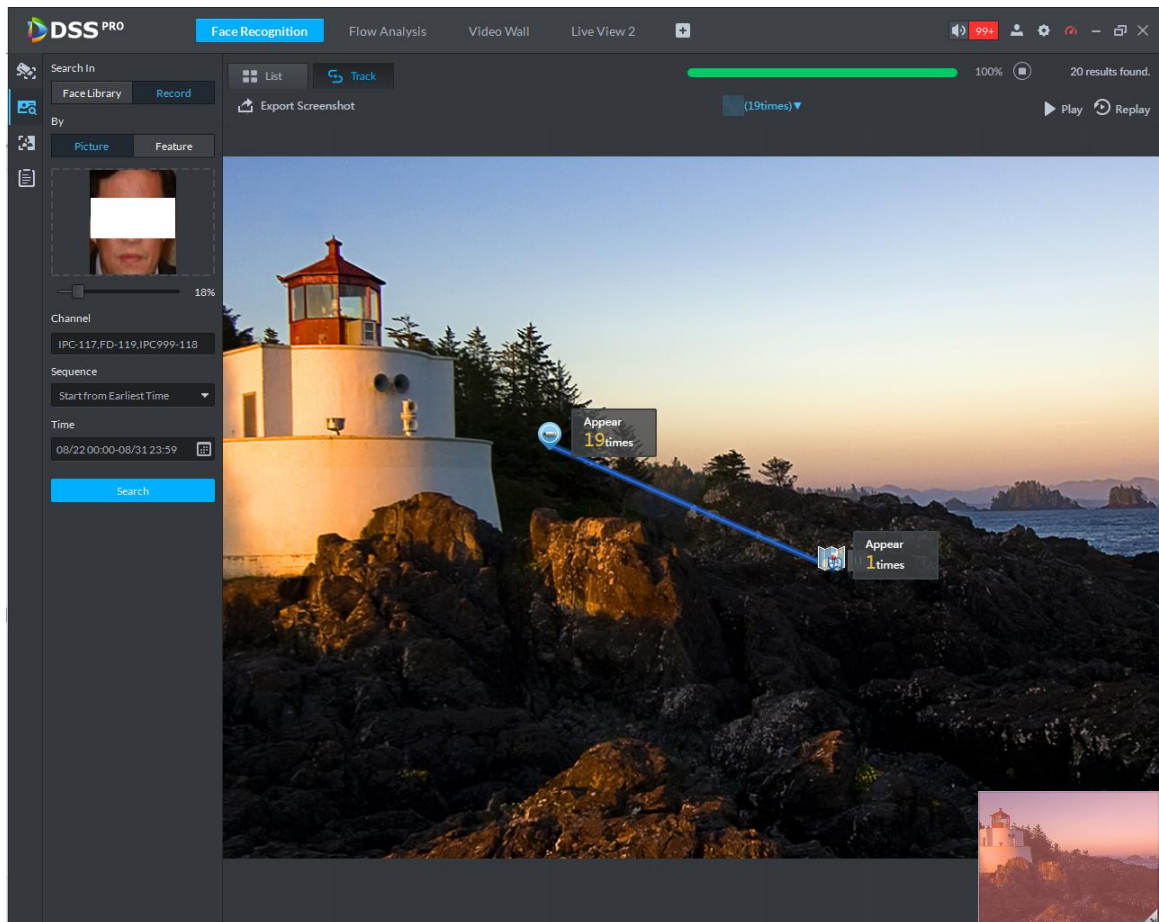


Table 4-54 Functions description

Operation	Description
Download Record	Click  to save rar file to the specified path. The .rar file contains the human face snapshot images and snapshot panorama images.
Playback record	Click  to playback the 15-seconds video record before and after the snapshot.
Add person	Add the snapshot person to the database. 1. Click  . 2. Set person information and then click OK .
Search record	You can upload a face image to search for the target face record. 1. Click  , and then system goes to human face search interface with the snapshot image. 2. Click Search . The search results are displayed.

- Click **Track**, the face track is displayed on the map.

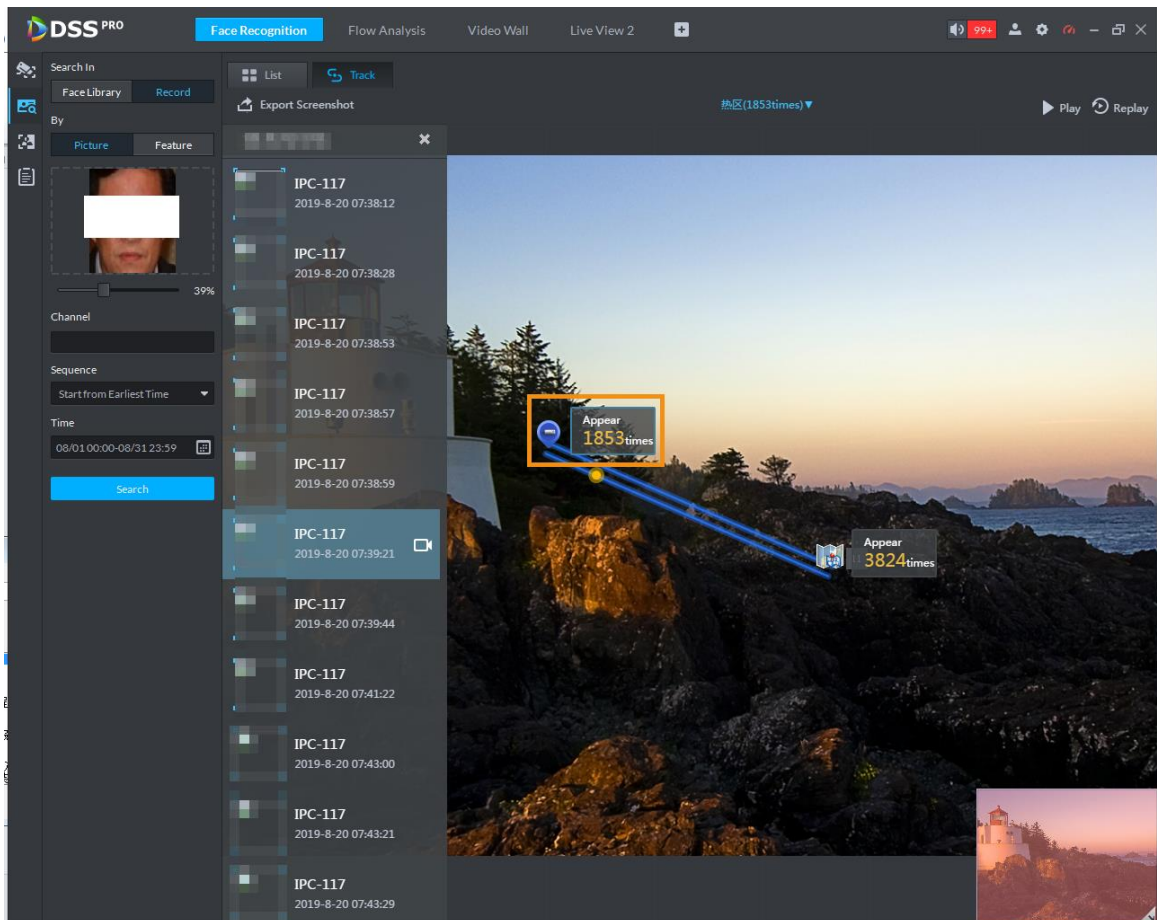
Figure 4-283 Face track on map



You can perform the following operations on the map.

- Double-click the device on the map, and the detailed snapshot records are listed on the left.

Figure 4-284 View detailed snapshot records



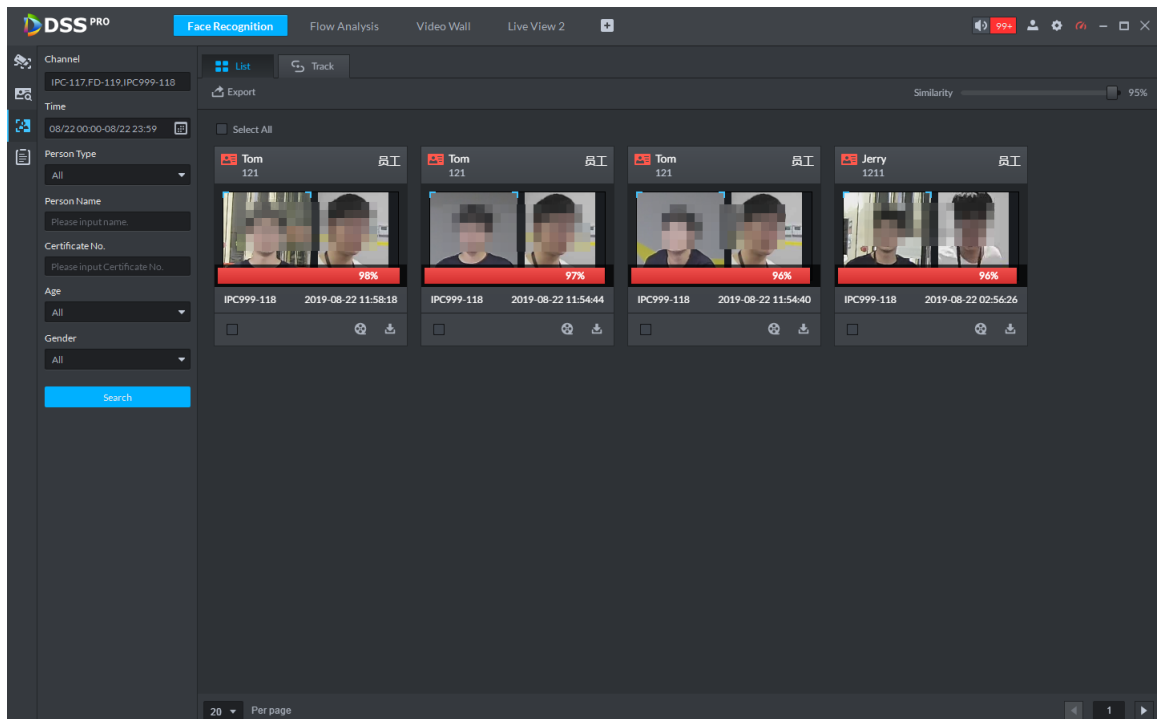
- Click to play the moving track. Click to stop. Click to play again.
- Click to play back video.
The video is uploaded by device. Playback will fail if the video is not stored on the device.
- Double-click a piece of record on the left to view the details.
- To export the track picture, click **Export Screenshot**, and then follow the onscreen instruction to save the picture locally.

4.16.4.3 Face Recognition Record Search

Search for recognized faces by time, device, person type, name, gender, age and certificate number. You can view search results in list or check face tracks on the map.

Step 1 On the **Face Recognition** interface, click

Figure 4-285 Recognition record search



Step 2 Set search criteria.

You can search by time, device, person type, name, gender, age and certificate number.

Step 3 Click **Search**.

Support viewing records in list or checking face tracks on the map.



To achieve the face track function, make sure that you have linked face cameras onto the map.

- Click **List**, and then the records are displayed in list. Double-click a search result, and the detailed information is displayed. There is no image on the left if you do not upload image when setting search criteria.

Figure 4-286 Records in list

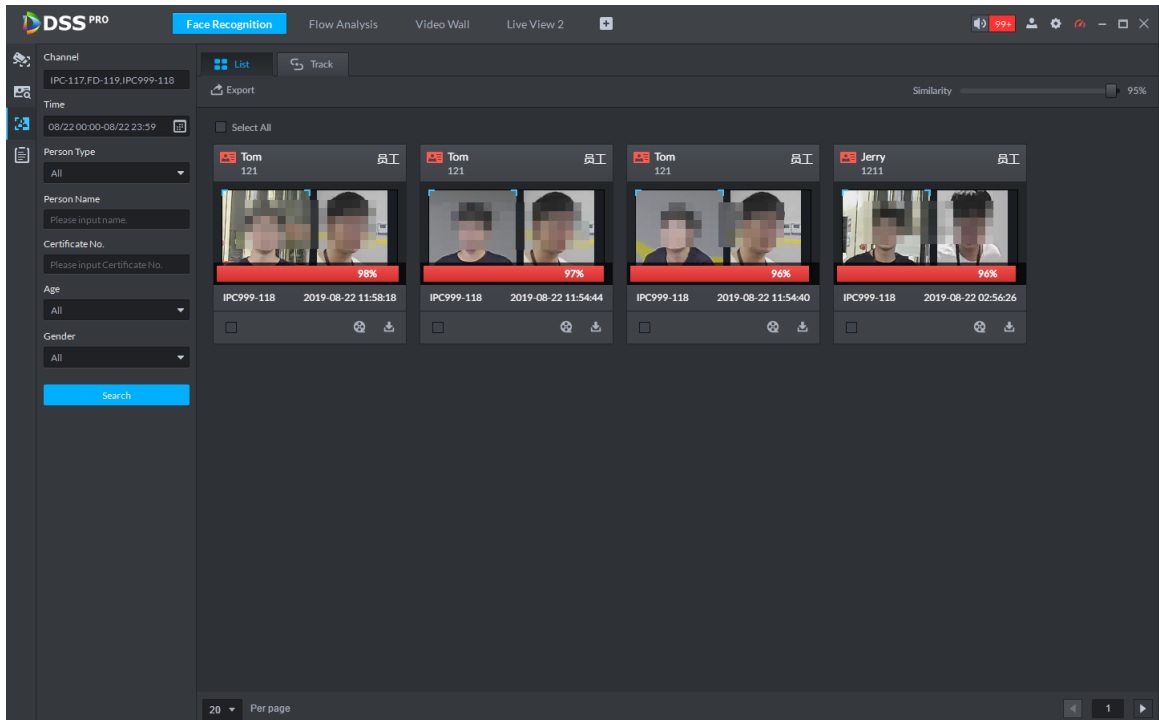


Figure 4-287 Record details

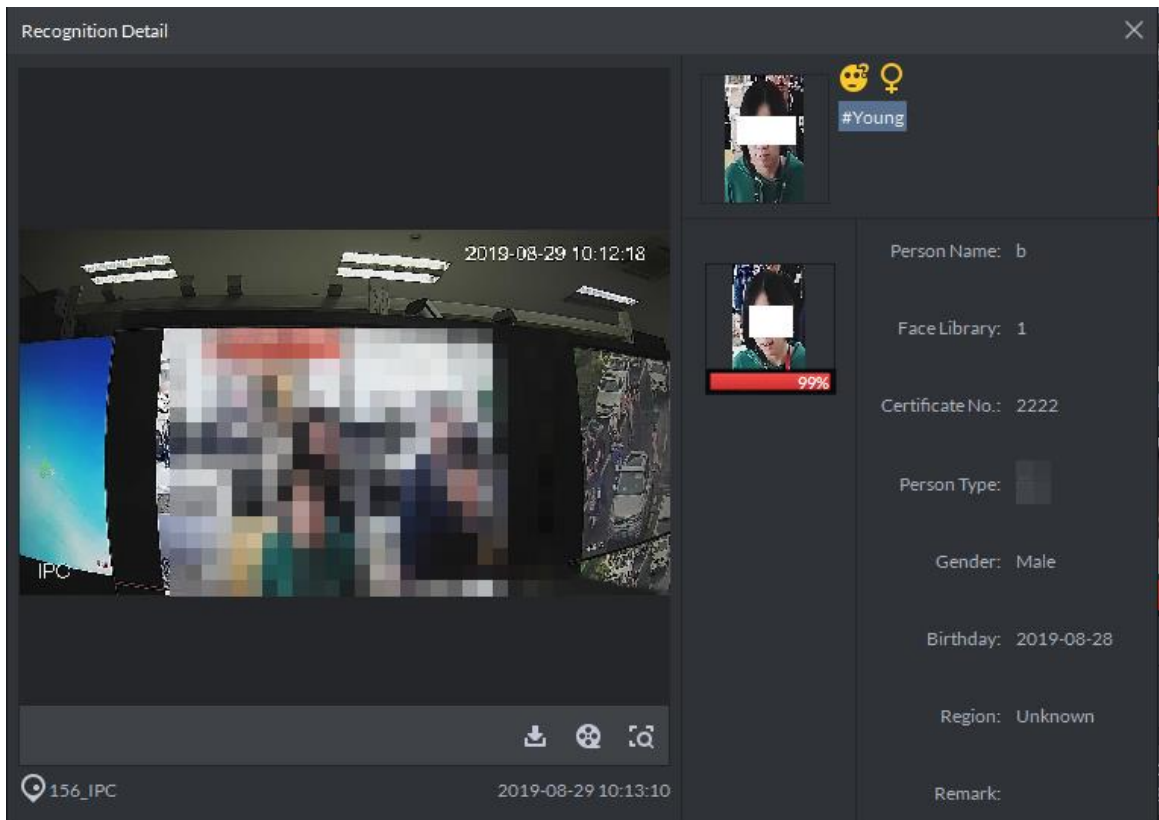





Table 4-55 Functions description


Operation	Description
Download Record	Click  to download video.

Operation	Description
Playback record	Click  to play back the 10-seconds video records before and after the snapshot.
Search record	Click  to search for records.

- Click **Track**. The face track is displayed on the map. For more instruction about face track operation, see "4.16.4.2 Face Search."

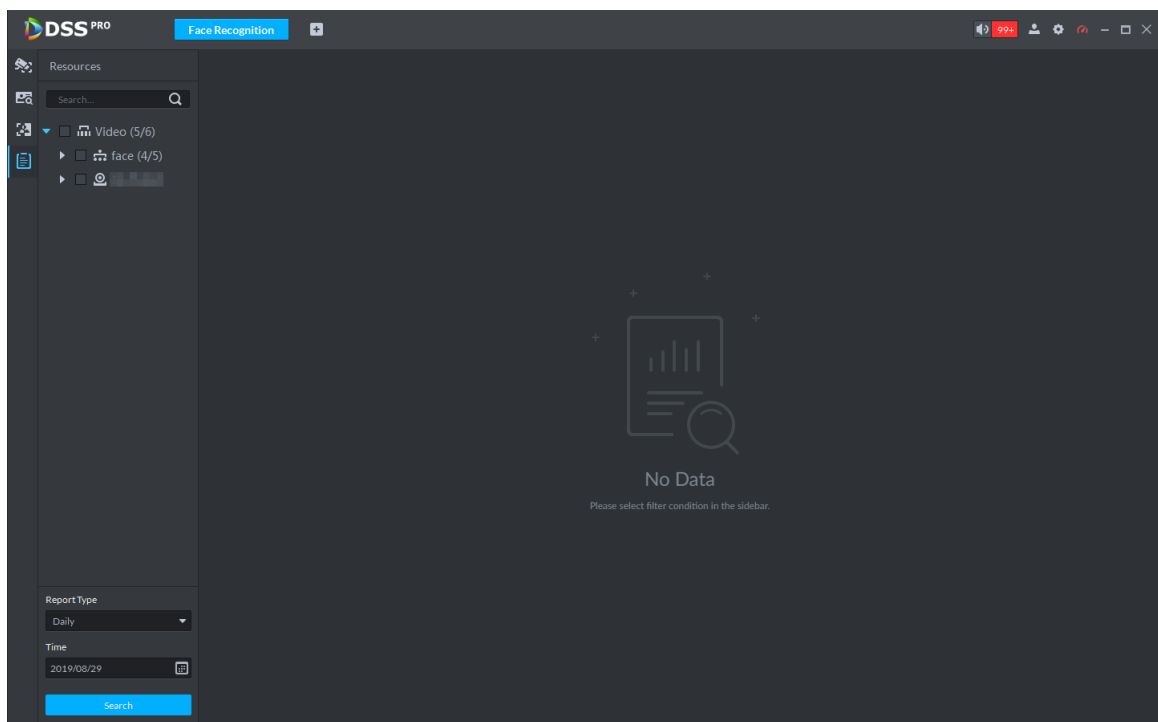
4.16.4.4 Face Reports

View face reports that show face statics involving age, gender, and other properties.

Step 1 Click  on the Control Client, and then select **Face Recognition**.

Step 2 On the **Face Recognition** interface, click .

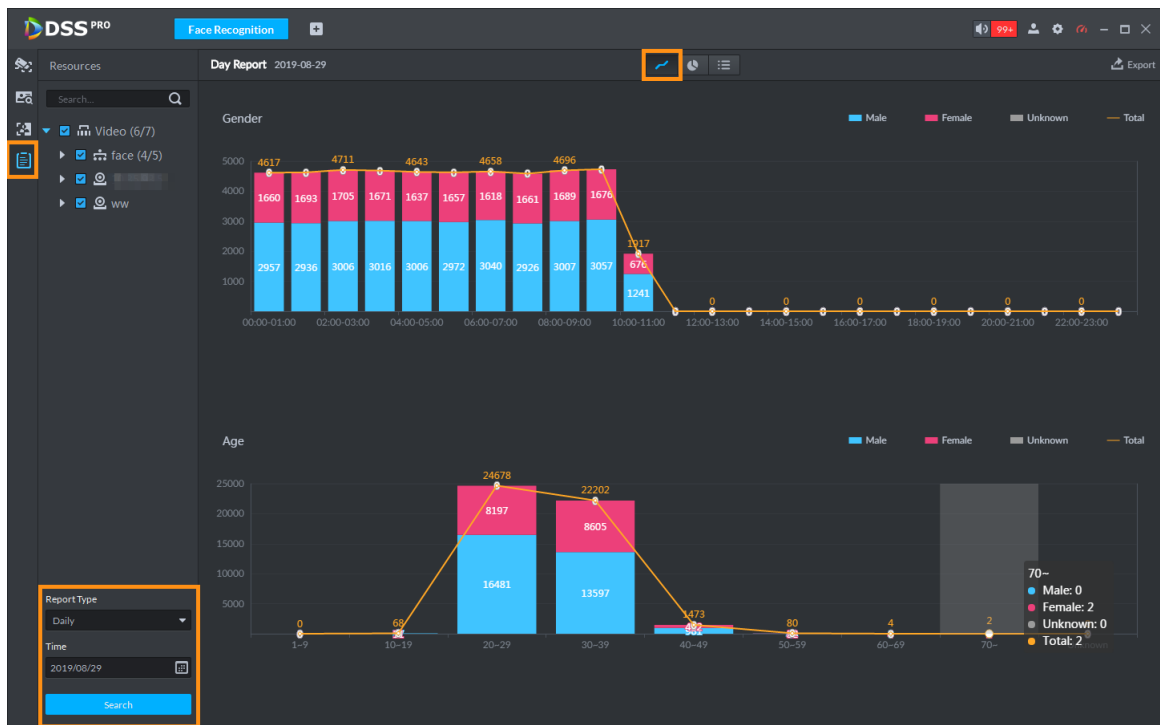
Figure 4-288 Statistics report search





Step 3 Set search criteria.
Set video channel, report type and time.

Step 4 Click **Search**.

Figure 4-289 Reports



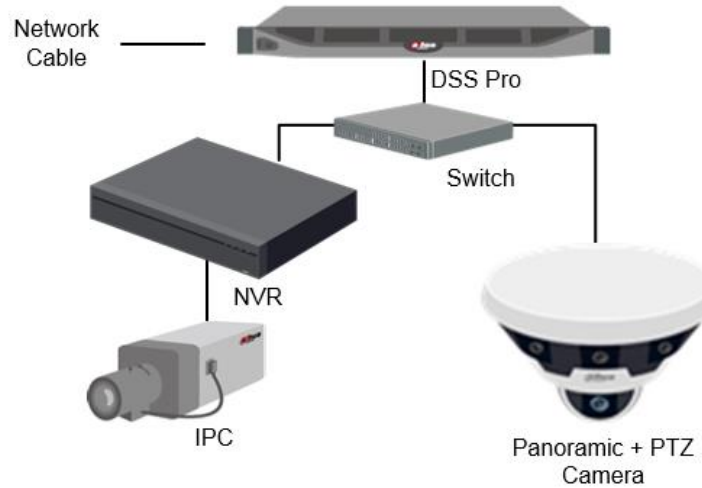
- Results are displayed by line chart by default.
- Click  to display by pie chart.
- Click  to display by list.
- Click **Export** to export statistics result in .xlsx format.

4.17 Target Detection

View and search for metadata of people, vehicle and non-motor vehicle.

4.17.1 Typical Topology

Figure 4-290 Typical topology



- General cameras record videos.
- Video metadata cameras such as panoramic + PTZ camera record videos and analyze people, vehicles and non-motor vehicles.
- NVRs manage cameras and analyze people, vehicles and non-motor vehicles.
- The platform centrally manages NVRs and cameras, receive analysis results from cameras and shows the reports.



Target detection can be done by video metadata cameras or intelligent NVRs.

4.17.2 Business Flow

Figure 4-291 Target detection business flow



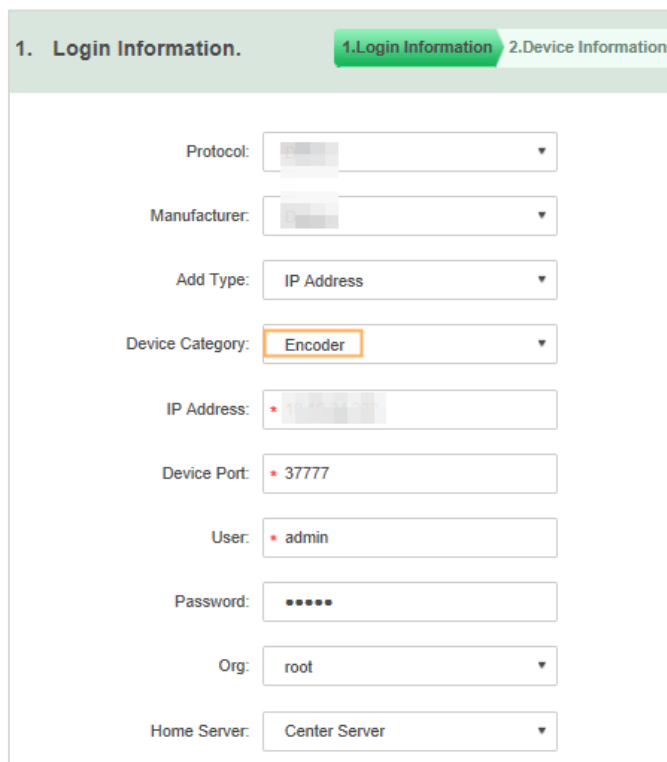
4.17.3 Target Detection Applications

4.17.3.1 Preparations

Make sure that the following preparations have been made:

- Cameras and NVRs are correctly deployed, and video metadata is enabled on them. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding a camera or NVR on the **Device** interface of Web Manager, select **Encoder** for device category.

Figure 4-292 Add device




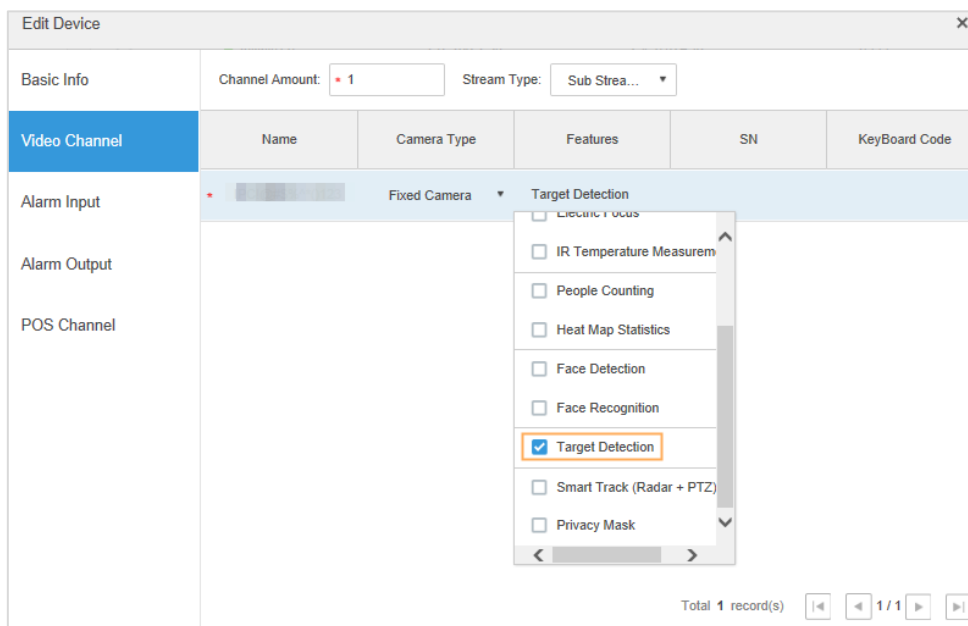
- ◇ On the **Device** interface, click  or of the camera or NVR, and then select **Target Detection** for **Features**.

Figure 4-293 Edit video channel features



4.17.3.2 Viewing Real-time Detection

To view the real-time snapshots captured by the cameras, including information about human, vehicles, and non-motor vehicles:

Step 1 Log in to the Control Client, click , and then select **Object Detection**.

Step 2 Click .

The real-time detection interface is displayed.

Figure 4-294 Real-time detection interface

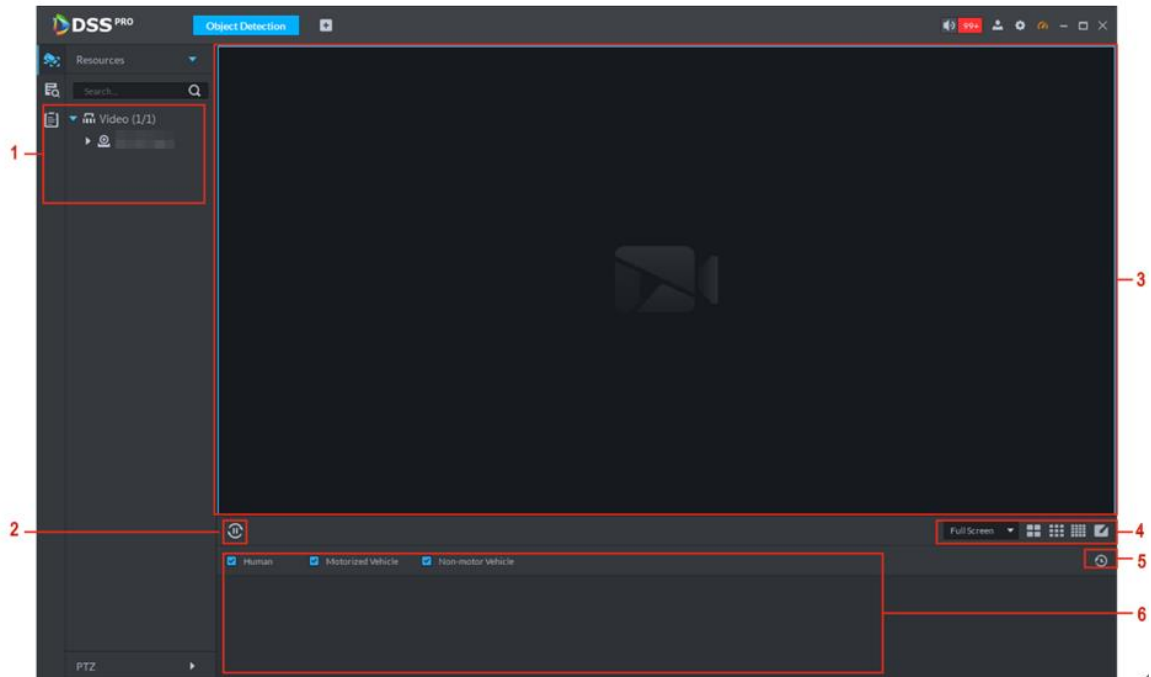


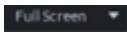



Table 4-56 Description

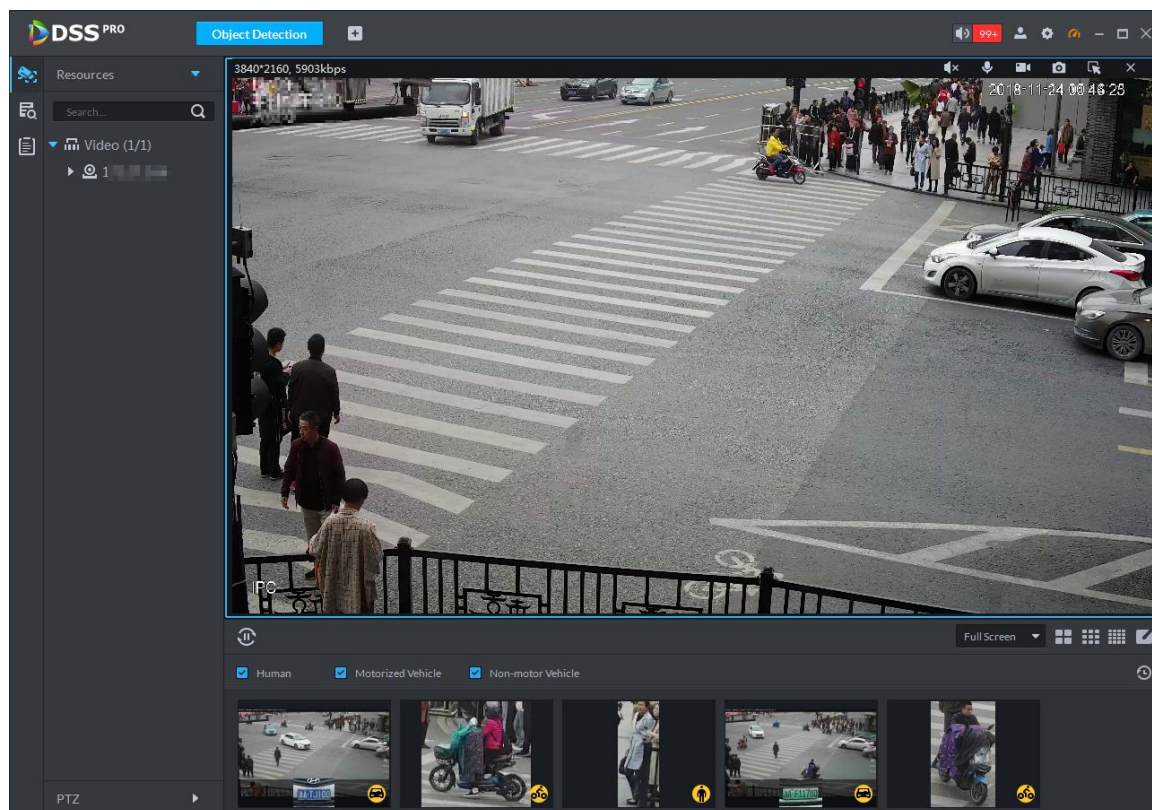
No.	Name	Description
1	Device Tree	Displays device information.
2	Pause Refresh/Start Refresh	<ul style="list-style-type: none"> If the interface displays , the snapshot display area does not refresh snapshots. Click this icon to refresh face snapshots in real time. If the interface displays , the snapshot display area refreshes face snapshots. Click this icon to stop refreshing snapshots.
3	Monitoring window	Displays the channel live video. In the multi-window display mode, double-click a window to switch to single window display. Another double-clicking returns to the original multi-window display mode.
4	 Full Screen	Picture display ratio
		Number of windows
5	The button that allows for jumping to the Report Statistics interface.	Click this icon to jump to the Report Statistics interface.
6	Snapshot display area	Displays the captured face snapshots.

Step 3 Turn on live view.



- Select the monitoring window (a white frame means the window has been selected), and double-click any channel or video recording to enable real-time monitoring.
- Drag the channel or video recording to the monitoring window.

Step 4 Turn on the live view display. The client displays snapshots in real time.

Figure 4-295 Live view display



Step 5 Double-click the snapshot to view details.

- Human snapshots display body cutout, types of tops, colors of tops, types of bottoms, colors of bottoms, carrying bags or not, wearing caps or not, and the gender. If faces are recorded, the system displays face snapshots, age, facial expression, wearing glasses or face masks. You can zoom in any part of the human body image, go to the search interface, and view the recordings. You can quickly go to search by image interface or register the faces to the database.
- Vehicle snapshots display the panoramic view of vehicles, vehicle type, vehicle color, license plate color, and logo. You can view license plate snapshots, play linked videos and zoom in specified parts of the vehicle image.
 - ◇ Click  and save .rar files in the specified path.
 - ◇ Click  to play back the video recordings timed before and after the snapshot.
- Non-motor vehicle snapshots display the panoramic view, vehicle type, vehicle color, and the number of people involved.

4.17.3.3 Searching for Target Detection Records

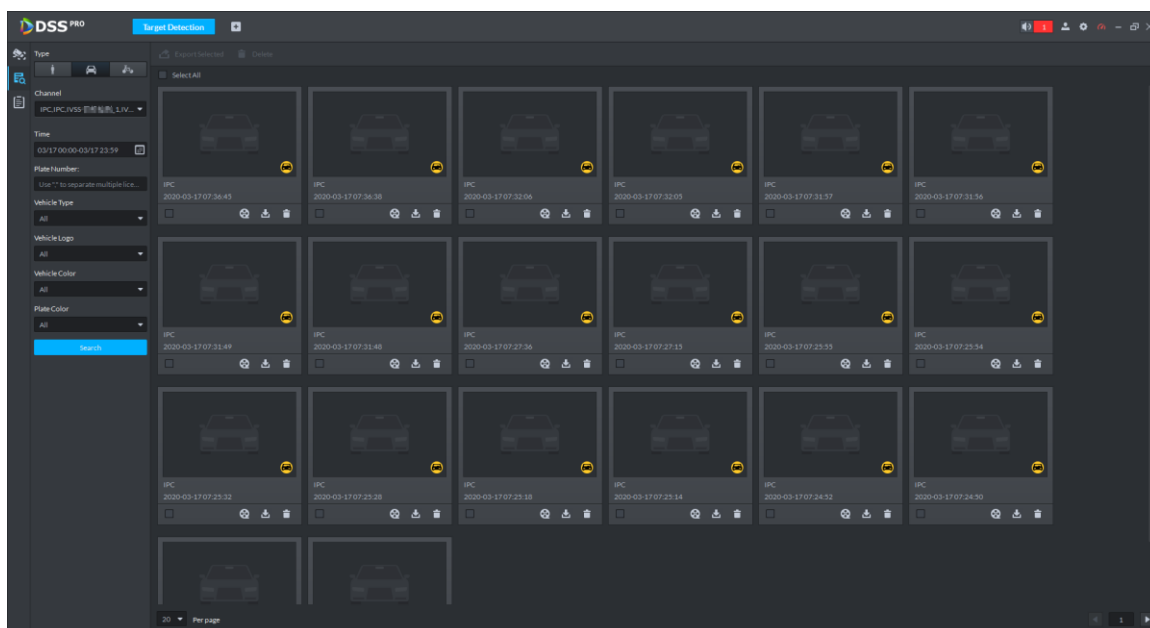
Step 1 Log in to the Control Client, click , and then select **Object Detection**.

Step 2 Click .

Step 3 Set search conditions and click **Search**.

You can search by human, vehicle and non-motor vehicle. If you use IVSS or smart MVR for target detection, you can upload a picture to search for similar targets.

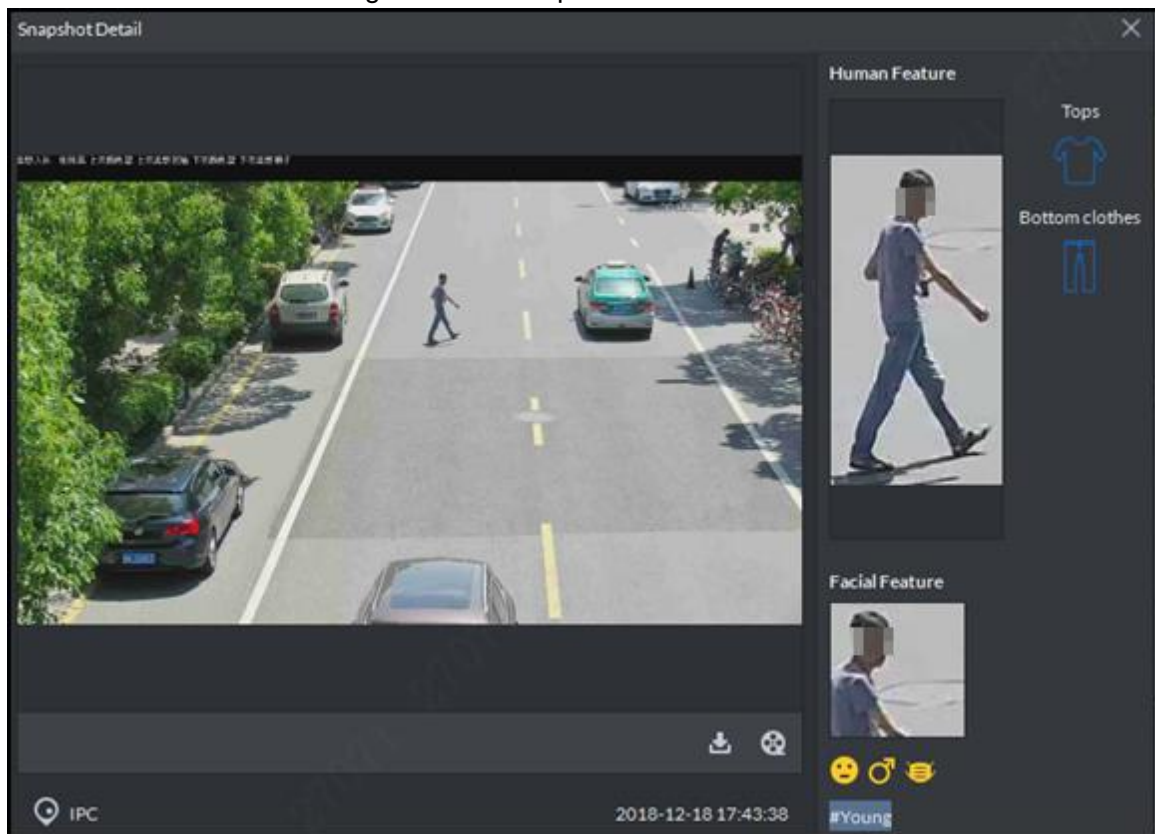
Figure 4-296 Search results





Step 4 Actions available.


- Double-click the snapshot to view details.

Figure 4-297 Snapshot details



- To download video, click .
- To play video, click .
- To export searches, select the records, and then click **Export Selected**.

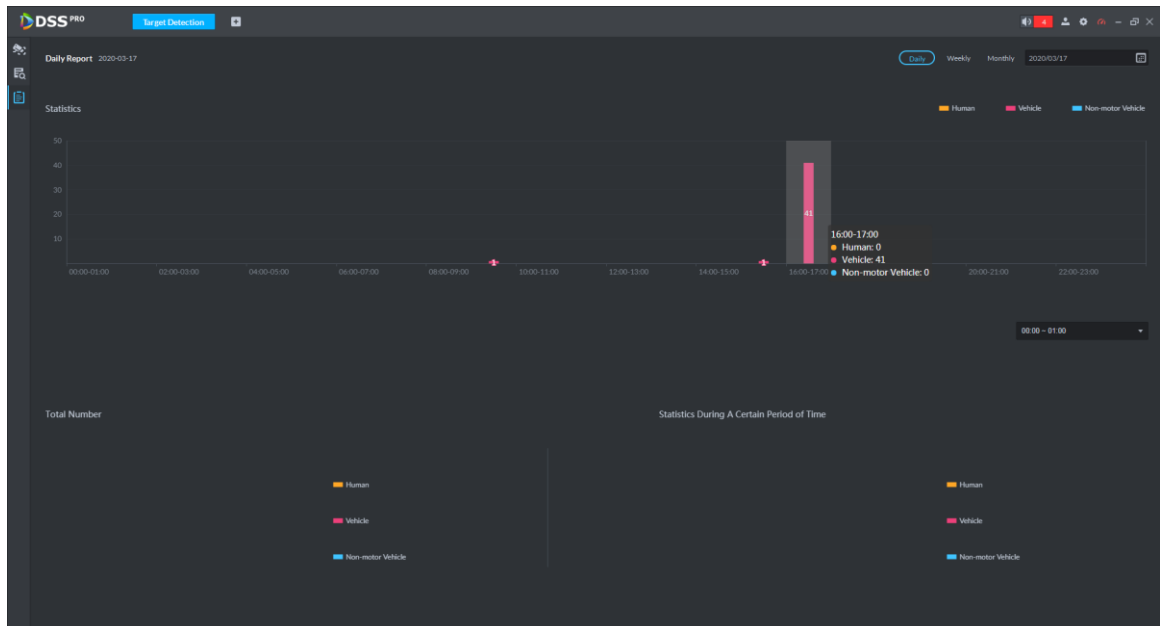
4.17.3.4 Reports

Step 1 Click  on the Control Client, and then select **Object Recognition**.

Step 2 Click .

Step 3 On the upper-right corner, select the period type and date. The report shows the people, motor-vehicle and non-motor vehicle data during the defined period.

Figure 4-298 Report interface



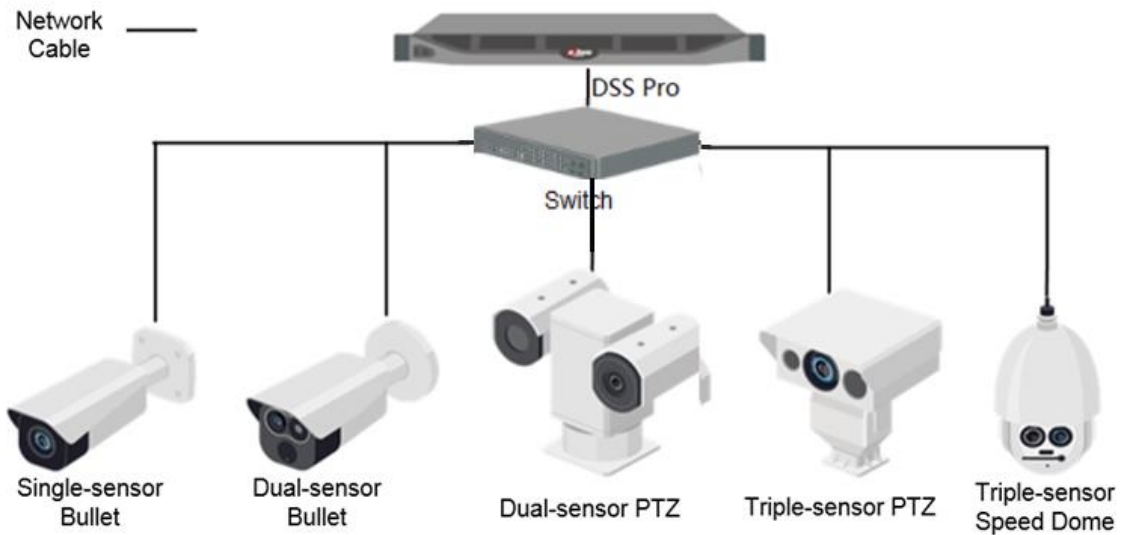
4.18 Thermal

View live or recorded videos of thermal cameras for temperature monitoring. The thermal cameras can be connected to the platform directly or through NVR, IVSS or EVS.

- Real-time temperature measurement
 After adding devices on the Web Manager, log in to the Control Client. On the **Thermal** interface, drag a thermal camera from the device tree to the live view window, and then click anywhere on the video to view the temperature of the point.
- Thermal analysis
 After adding thermal devices on the Web Manager, you can view the thermal view on the Control Client. You can use the thermal analysis tools to generate temperature information and temperature ratio on the thermal view. You can also select one or more sections on the thermal view, and use the tools to calculate maximum temperature, minimum temperature, average temperature and temperature difference.

4.18.1 Typical Topology

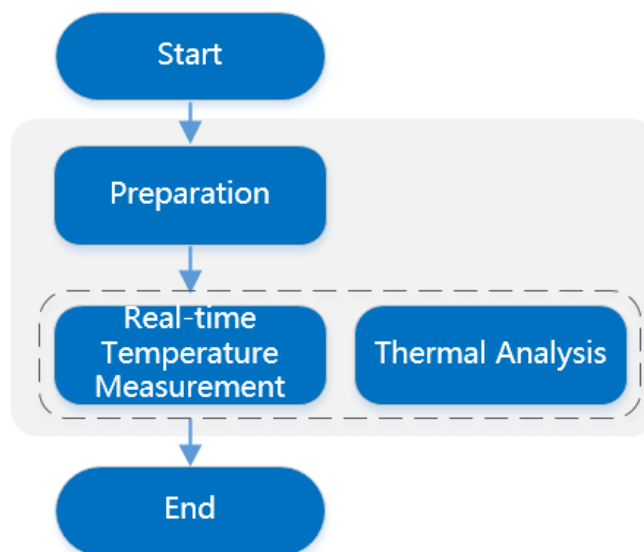
Figure 4-299 Typical topology



- Thermal devices record videos, analyze temperature, and upload thermal information to the platform.
- The platform centrally manages all devices, receive and analyze thermal data, and provides reports.

4.18.2 Business Flow

Figure 4-300 Thermal business flow



4.18.3 Thermal Applications

4.18.3.1 Preparations

Make sure that the following preparations have been made:

- Thermal devices are correctly deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding thermal devices on the **Device** interface of Web Manager, select **Encoder** for device category.

Figure 4-301 Add device

1. Login Information. 1.Login Information 2.Device Information

Protocol: [dropdown]

Manufacturer: [dropdown]

Add Type: IP Address [dropdown]

Device Category: Encoder [dropdown]

IP Address: * [text input]

Device Port: * 37777 [text input]

User: * admin [text input]

Password: [password field]

Org: root [dropdown]

Home Server: Center Server [dropdown]


- ◇ After the device is added, click , and select **IR Temperature Measurement** from the **Features** drop-down box.

Figure 4-302 Set device features

Edit Device
✕

Basic Info
Channel Amount:
Stream Type:
 Zero Channel Code

	Name	Camera Type	Features	SN	KeyBoard Code
Video Channel					
Alarm Input	* 1_1	Fixed Camera	Intelligent Alarm,IR T...		
Alarm Output					
POS Channel					
HDCVI External					

- Intelligent Alarm
- Fisheye
- Master Slave Track
- Electric Focus
- IR Temperature Measur...
- Heat Map Statistics
- Cross Line Statistics
- Area Statistics
- Multi-area Statistics

↑
↓

Total 1 record(s)
|< < 1 / 1 > >|

Get Info
OK
Cancel

4.18.3.2 Real-time Temperature Measurement

Step 1 Click on the Control Client, and then select **Thermal**.

Figure 4-303 Thermal interface

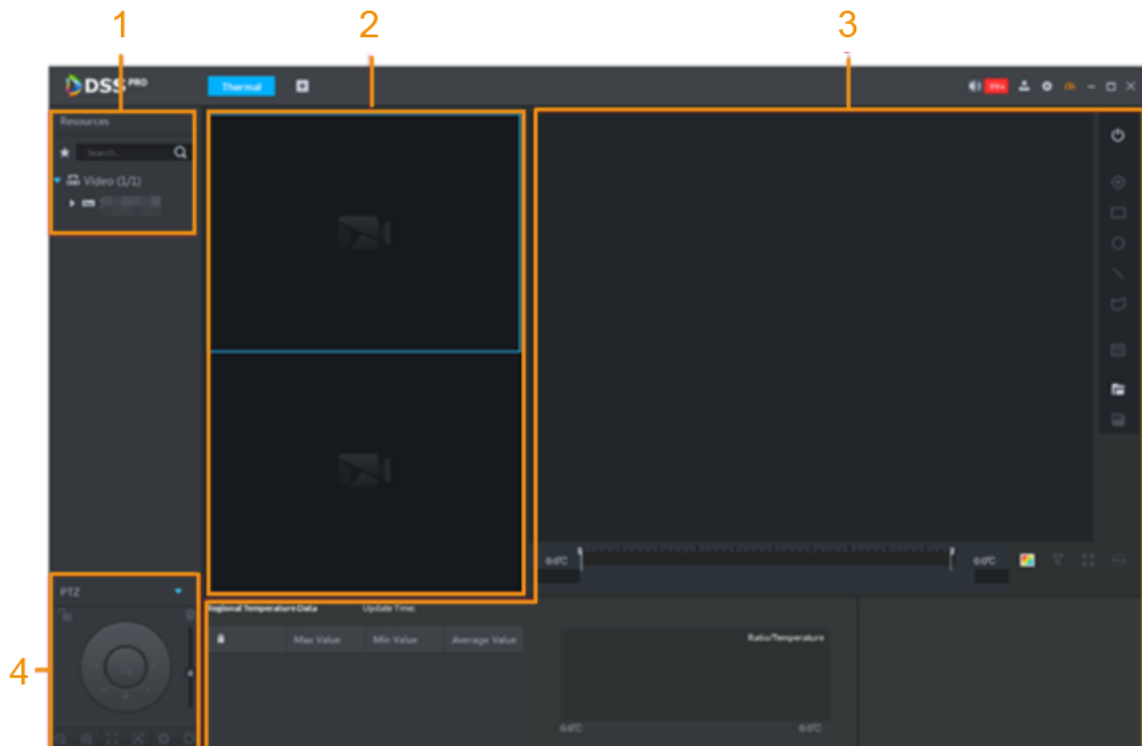


Table 4-57 Description

No.	Module name	Description
1	Device Tree	<ul style="list-style-type: none"> If in Local Config > Basic Setting, you select Show device node, the Device Tree shows the device and the channels under it. If the selection is undone, channels of all devices are displayed. Supports searching and querying in <input type="text" value="Search..."/> by organization name, device name, or channel name.
2	Preview	You can preview channel videos. Drag the channel to the window or select the window and double-click a channel to open videos of corresponding channels.
3	Heatmap	The heatmap is formed by capturing the temperature value of each pixel point on the thermal image and can be analyzed on the client. See "4.18.3.3 Heatmap Analysis" for specific steps.
4	PTZ Control	To control the PTZ or speed dome, rotate the device to zoom in/out, change focus and adjust aperture.

Step 2 Drag a thermal camera from the device tree to a window to play the live video, and then click anywhere on the video to view the temperature of this point.

Figure 4-304 Real-time temperature measurement



Hover over the video to display the shortcut menu.

Figure 4-305 Menu



Table 4-58 Description

No.	Icon name	Description
1	Real-time Tagging	<ul style="list-style-type: none"> If in Local Config > Basic Setting, you select Silent Real-time Tagging, the Tagging dialog box does not display at the time of real-time tagging. If Silent Real-time Tagging is not selected, you can edit the tag name.
2	Audio	Turn on or off audio.
3	Intercom	Turn on or off audio talks.

No.	Icon name	Description
4	Local Record	Click this icon and the system begins recording a local video. Clicking this icon again stops recording and the recorded video file is stored locally.
5	Snapshot	Click this icon and the system takes snapshots automatically.
6	Off	Click this icon to turn off this video channel.

4.18.3.3 Heatmap Analysis

Heatmap of devices can be obtained on the client. The heatmap analysis tools available on the client can generate temperature values and the ratio of each temperature value on the heatmap. You can also select one or more monitored regions on the heatmap. The tools can calculate the max temperature, min temperature, and average temperature within a region, and also temperature differences.

Figure 4-306 Heatmap and analysis tool interface

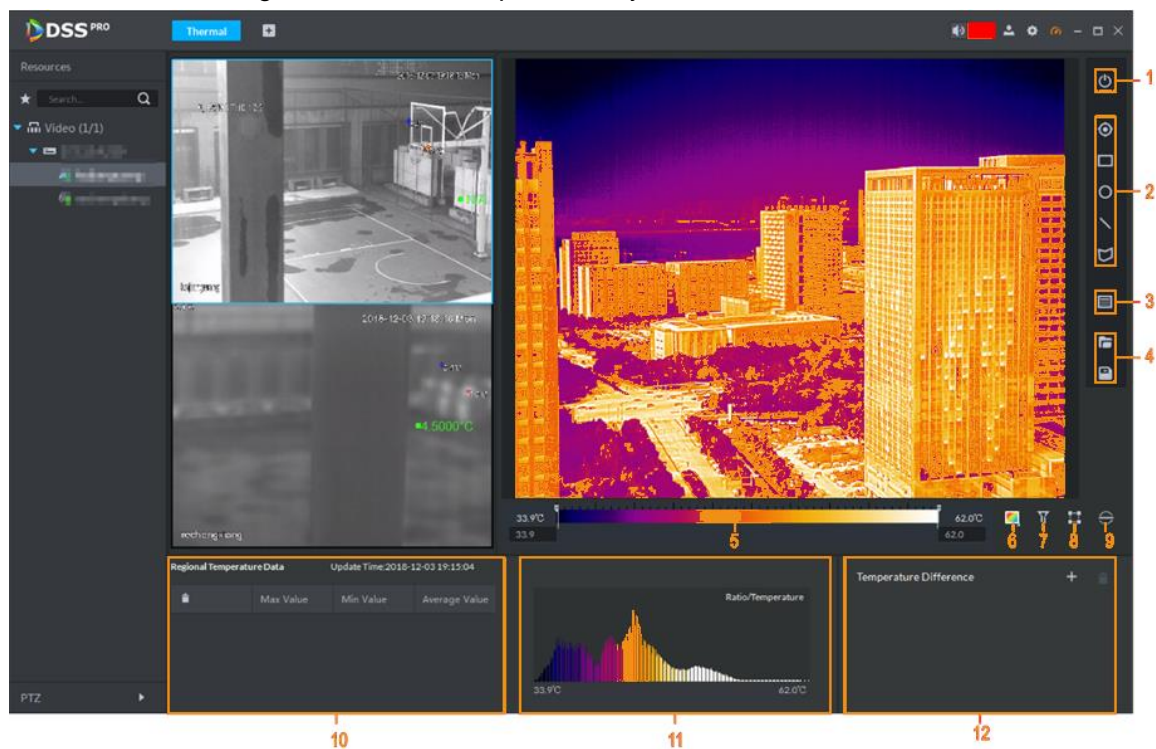


Table 4-59 Parameters

No.	Module name	Description
1	Query heatmap	You can obtain heatmap manually.
2	Draw a region	You can draw a region on the heatmap to measure the temperature. The region can be a point, a rectangle, a circle, a line segment, or a polygon. See 4.18.3.3.2Regional Temperature for specific steps.
3	Mode	Not supported for now.

No.	Module name	Description
4	File processing	You can import heatmap processing files (.dtp) to the client for analysis, or generate heatmap analysis reports.
5	Temperature display	<p>Generates a bar reflecting the color changes corresponding to different temperature values, based on the rendering plan selected in the heatmap. The data at the two ends defines the temperature range in the heatmap.</p> <ul style="list-style-type: none">• Temperature-color correlation: When the mouse is placed at a color spot, the temperature of the color spot is displayed.• Enhanced temperature comparison display: After inputting temperature values in the boxes at the two ends of the bar, the heatmap only displays the colors of the regions within this temperature range. Regions with temperatures below the preset min value are displayed in the leftmost color on the bar; regions with temperatures above the preset max value are displayed in the rightmost color on the bar.

No.	Module name	Description
6	Rendering Plan	<p>Click to color the infrared image. 14 color plans are available.</p> <ul style="list-style-type: none"> ● White-heat: In gray-scale images, the parts with higher temperature are brighter. ● Black: In gray-scale images, the parts with lower temperature are brighter. ● Purple-yellow: Colors mostly fall within the purple-red-yellow range. The parts with lower temperatures are purpler, and higher temperatures more yellow. ● Rainbow: Colors mostly fall within the blue-green-red-yellow range. The parts with lower temperatures are bluer, and higher temperatures more yellow. ● Red-yellow: Colors mostly fall within the red-yellow range. The parts with lower temperatures are redder, and higher temperatures more yellow. ● Blue-yellow: Colors mostly fall within the blue-purple-red-yellow range. The parts with lower temperatures are bluer, and higher temperatures more yellow. ● Iron red: Similar colorway to the Blue-yellow plan but less bright. ● Amber: Mainly dark brown. The parts with higher temperatures are brighter. ● Jade: Colors mostly fall within the purple-red-yellow-green-blue range. The parts with lower temperatures are purpler, and higher temperatures bluer. ● Sunset: Colors mostly fall within the blue-red-yellow range. The parts with lower temperatures are bluer, and higher temperatures more yellow. ● Red and Blue: In colored images, objects with higher temperatures are displayed in red, and those with lower temperatures are displayed in blue. Usually used to give warnings. ● Oil painting: Colors mostly fall within the purple-blue-green-yellow-red range. The parts with lower temperatures are purpler, and higher temperatures redder. ● Pomegranate: Mainly burgundy. The parts with higher temperatures are brighter. ● Emerald: Mainly azure green. The parts with higher temperatures are brighter. <p>The default setting is White-heat.</p>

No.	Module name	Description
7	Temperature Filter	Filters the temperatures on the heatmap. You can set up a temperature range. The heatmap within this temperature range is displayed in other colors. See "4.18.3.3.3 Temperature Filter" for specific steps.
8	Select isothermal region	The isothermal lines are mainly used to highlight some parts of the image. The temperature range is around a median temperature, between an upper limit and a lower limit. Those above the lower limit appear in bright colors, and those below the lower limit appear in black & white. See "4.18.3.3.3 Temperature Filter" for specific steps.
9	Reset isothermal region	Click to delete the isothermal regions already drawn.
10	Regional Temperature Data	On the heatmap, select a region (except for points). The table displays the max temperature, min temperature, and average temperature of the selected region. See "4.18.3.3.2 Regional Temperature" for specific steps.
11	Temperature ratio	It displays the ratios of various temperature values on the heatmap intuitively.
12	Temperature Difference	The differences of max temperature, min temperature, and average temperature within the same region or across different regions can be calculated. See "4.18.3.3.2 Regional Temperature" for specific steps.

4.18.3.3.2 Regional Temperature



Draw a detection region on the heatmap and you can see the max temperature, min temperature, and average temperature in this region on the client. After adding multiple regions on the heatmap, you can compare the temperature differences across multiple regions.

Drawing a Region and Measuring the Temperature

Step 1 In the region drawing section, select a shape and draw on the heatmap.

The **Regional Temperature Data** section is automatically updated with the max temperature, min temperature, and average temperature of the region.



- Place the mouse near the edge of the region. When the mouse changes into , moving the mouse changes the size of the regular region.
- Place the mouse within the region. When the mouse changes into , moving the mouse changes the position of the regular region.
- Delete a single regular region: Select a region in **Regional Temperature Data** section, or a regular region on the heatmap. Right-click and select **Delete** to delete the corresponding regular region.


- Delete all regular regions: In **Regional Temperature Data** section, click , or select any regular region, right-click and select **Delete All** to delete all regular regions.

Figure 4-307 Draw a region

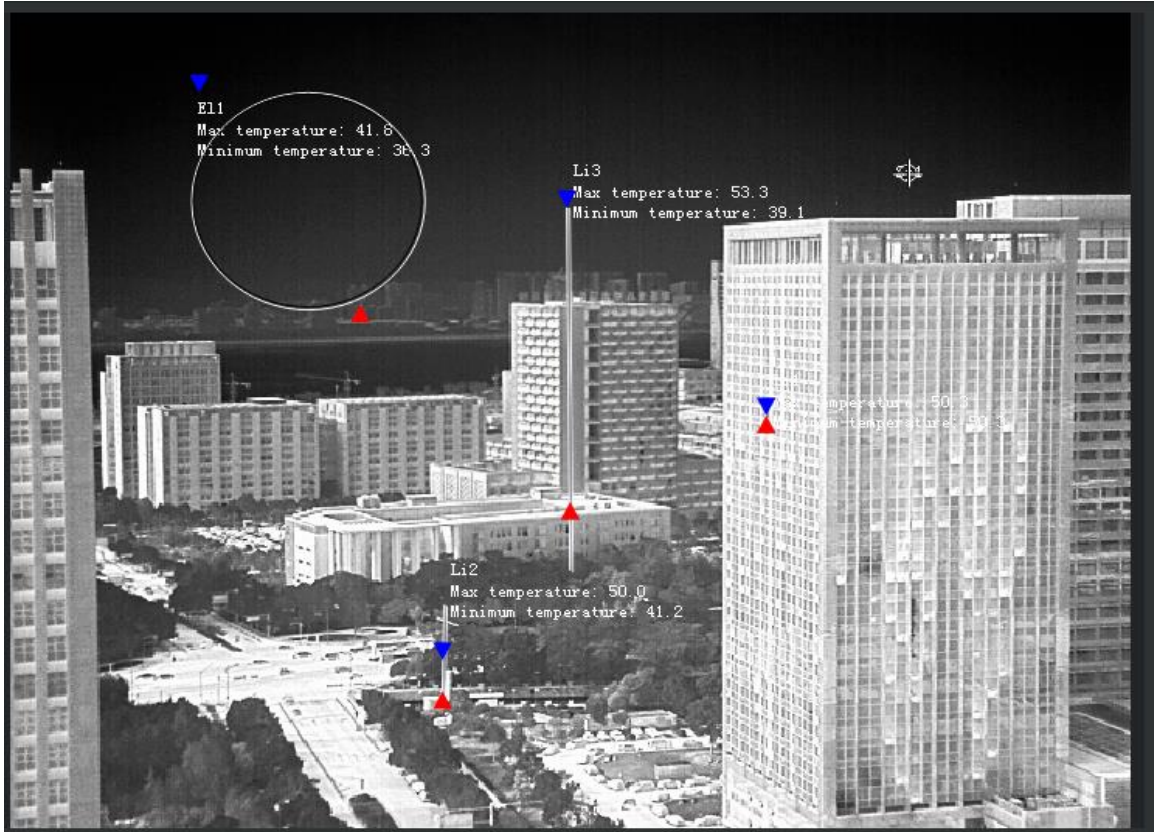



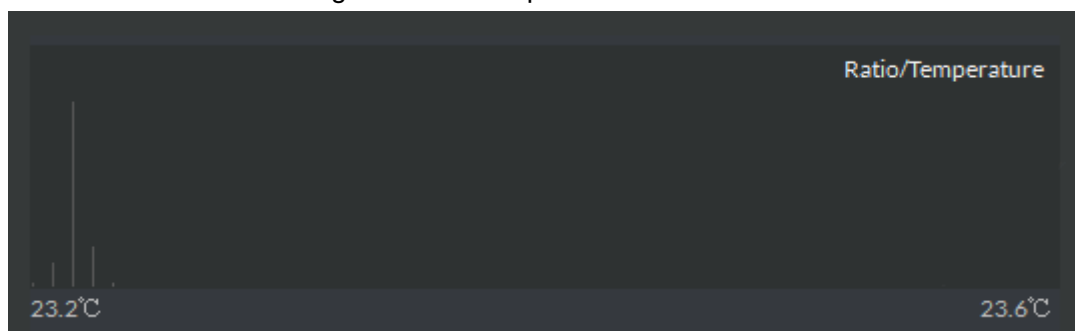
Figure 4-308 Regional temperature data

Regional Temperature Data		Update Time:2018-12-18 17:55:15	
	Max Value	Min Value	Average Value
E11	23.6	23.3	23.4
Rect1	23.6	23.3	23.4
Li1	23.5	23.3	23.4

Step 2 Click any temperature data.

Temperature ratios of the region can be displayed in the gradient graph on the side. Place the mouse on the graph and the temperature range and its ratio on the heatmap can be displayed.

Figure 4-309 Temperature ratio



Temperature Difference

Support up to 100 temperature difference calculation rules.

Step 1 Click  in the **Temperature Difference** section to add rules for calculating the temperature difference.






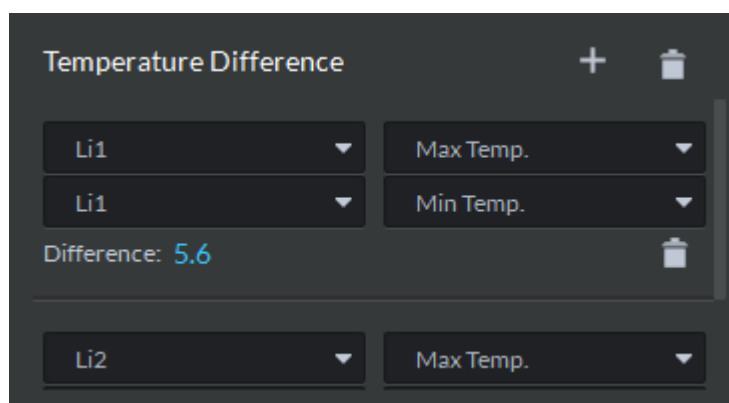
- Click  on the right side of  to delete all temperature difference calculation rules.
- Click  on the right side of each difference to delete the corresponding temperature difference calculation rule.

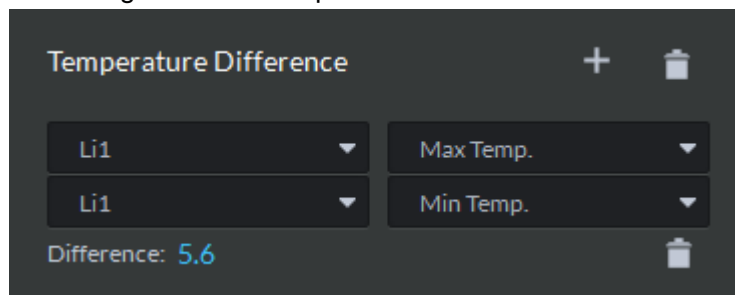
Figure 4-310 Temperature difference interface



Step 2 Click the drop-down box on the left side and select regions that have been set up, such as Li1, E11.

Step 3 Click the drop-down box on the right side and select the temperature to be compared with, such as the Max Temp., Min Temp., or Average Temp.
The system automatically calculates the temperature difference.

Figure 4-311 Temperature difference



4.18.3.3.3 Temperature Filter

Temperature Filter

To set up temperature limits, and select and highlight regions that fall within the limits on the heatmap.


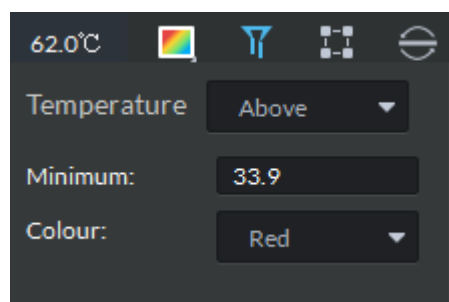
Step 1 Click  to enable temperature filter.

Figure 4-312 Temperature filter



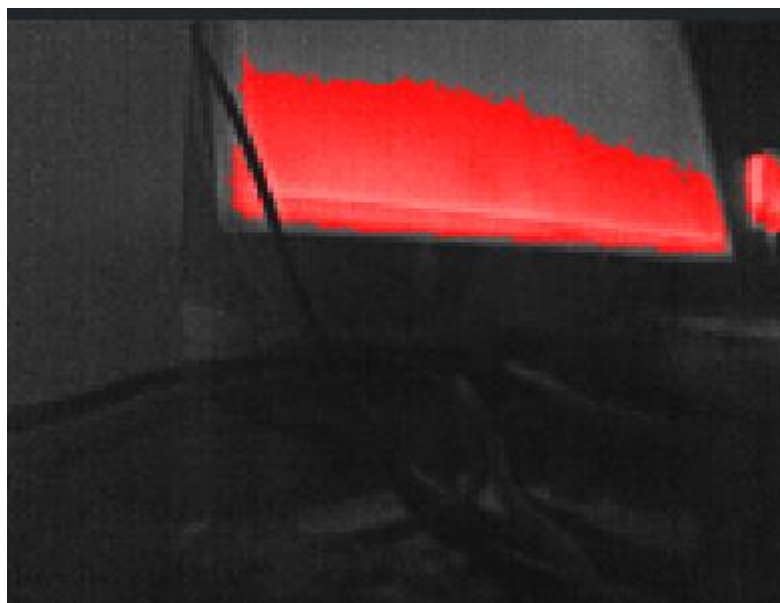
Step 2 Select the temperature filtering criteria. Available options include **Above**, **Below**, or **Between**.

Step 3 Input the temperature limits and set up colors.
The client displays the temperature filtering results.




- When Above or Below is selected as the filtering criteria, just fill in one value as the limit.
- When Between is selected, fill in both the upper limit and the lower limit.

Figure 4-313 Temperature filtering results



Select isothermal region

The isothermal region is mainly used to highlight some objects in the image. With the drawn isothermal region as the benchmark, regions with higher temperatures display in bright colors, and those with lower temperatures display in dark colors.

Step 1 Click .

Step 2 Draw regions on the heatmap.

The color bar below the heatmap only displays the temperatures within the region.





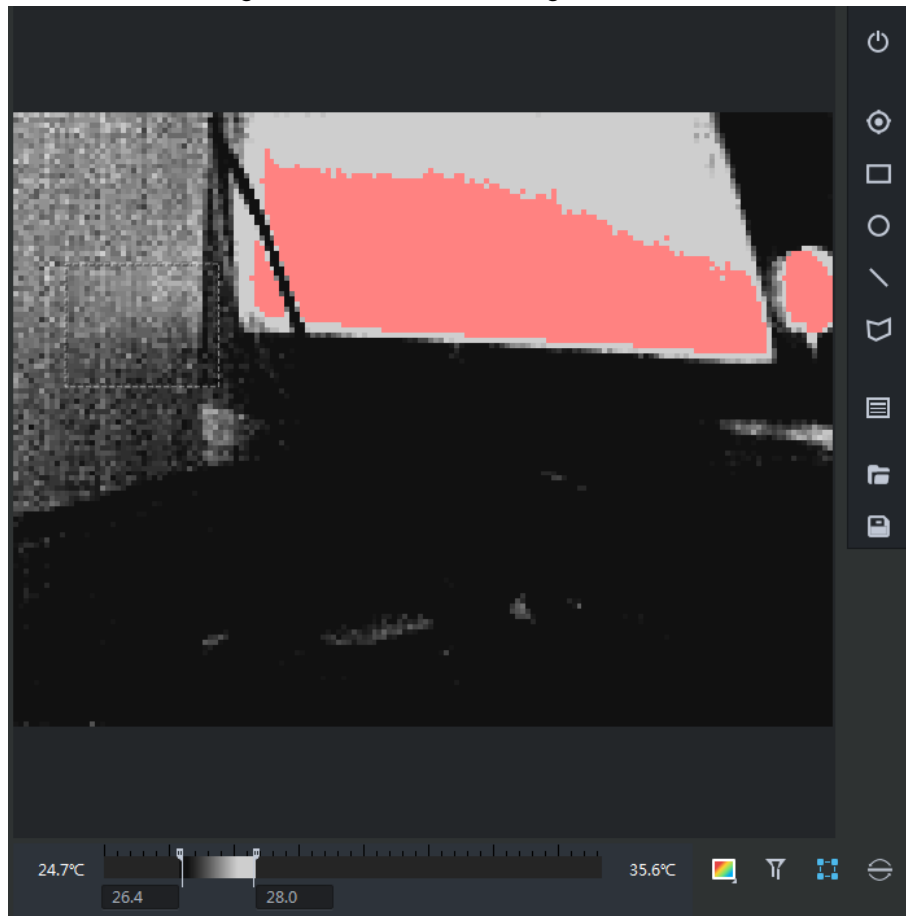

- Place the mouse near the edge of the region. When the mouse changes into , dragging the mouse changes the region size.
- Only one isothermal region is allowed on the heatmap.
- Click  to delete the isothermal regions already drawn.

Figure 4-314 Isothermal region



4.18.3.3.4 File processing

Import Local Heatmap

Step 1 Click .

The heatmap import interface is displayed.



The system supports .dtp heatmap file only.

Step 2 Select a heatmap file and follow the instructions on the interface to import it into the system.

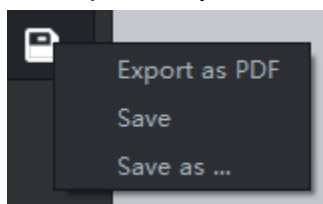
Import heatmap files to the client and analyze them.

Generate Heatmap Analysis Result

You can generate heatmap analysis reports in .pdf.

Step 1 Click .

Figure 4-315 Export analysis results

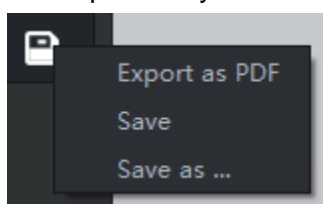


Step 2 Click **Export as PDF** and follow the instructions on the interface to save the exported file.

Save Heatmap

Step 1 Click .

Figure 4-316 Export analysis results



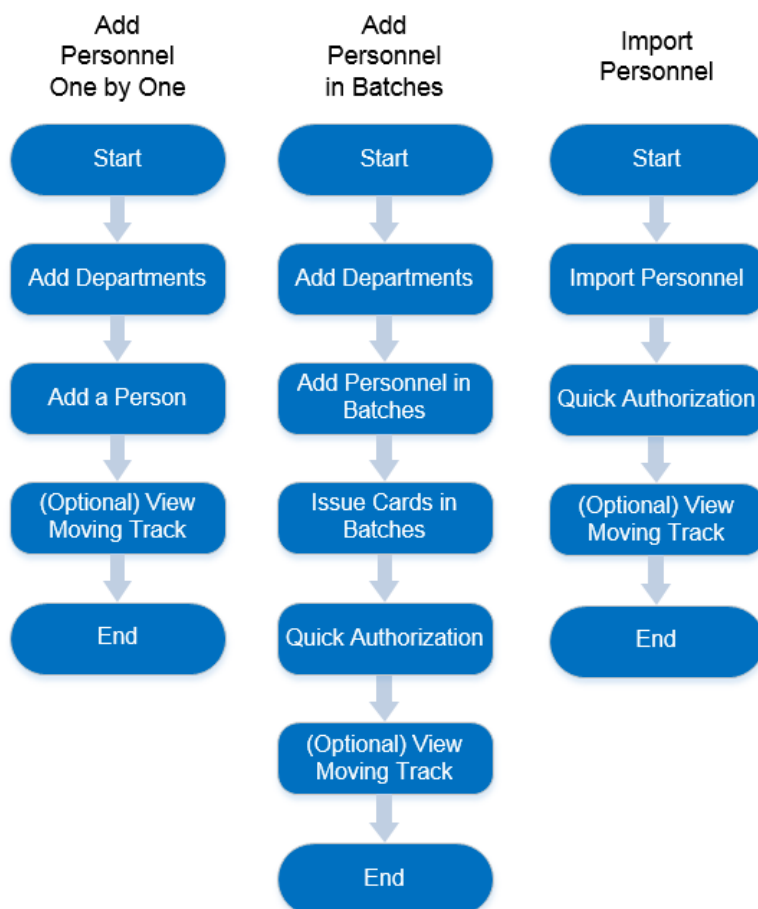
Step 2 Save heatmap.

- Click **Save** to save the rules already set up on the heatmap.
- Click **Save as...**, select the save path in the popup interface, and click **Save** to save the heatmap to a local disk.

4.19 Personnel Management

Configure personnel information for the applications of access control, vehicle control, video intercom and attendance management. Personnel information contains card number, password, face picture, and more.


Figure 4-317 Personnel Management



4.19.1 Configuring Personnel Information

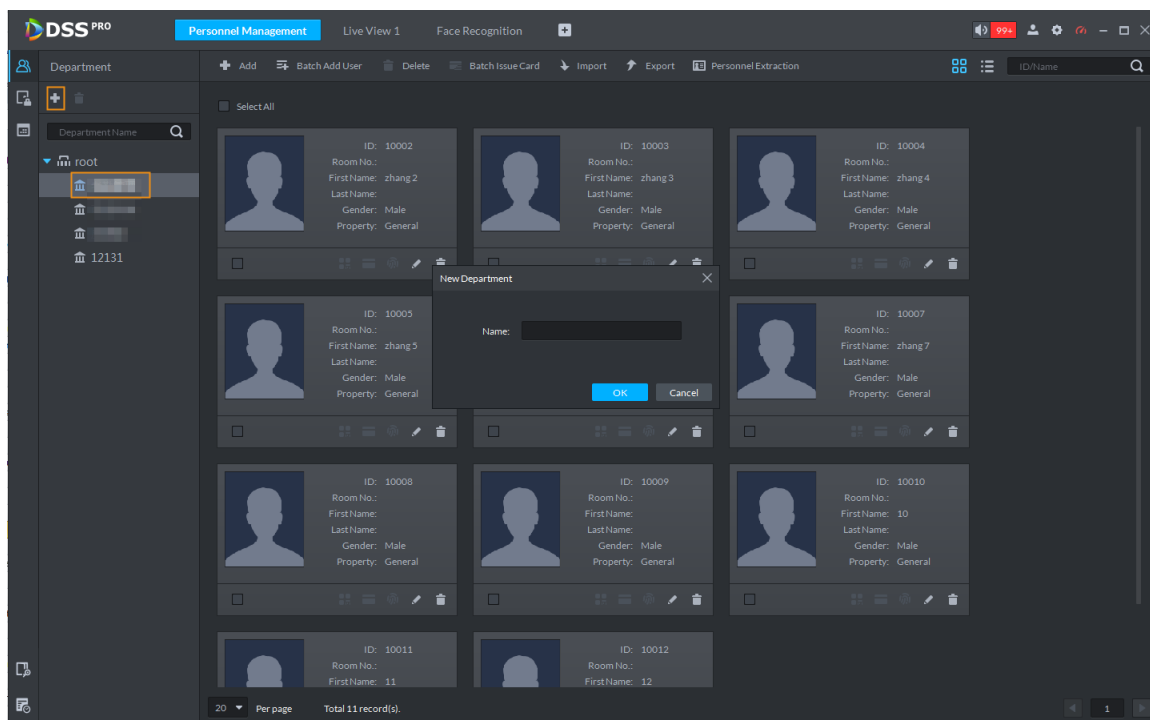
4.19.1.1 Adding Departments

Adding department is to manage personnel in the added departments.

Step 1 Click  on the Control Client, and then select **Personnel Management**.

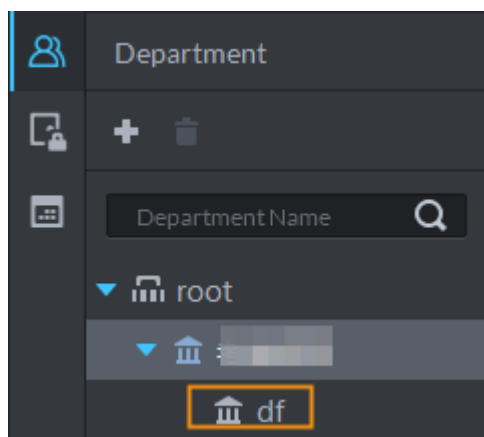
Step 2 Select a node from the department list on the left side, and then click .



Figure 4-318 Add a department



Step 3 Enter department name and click **OK**.

Figure 4-319 Added department



- To delete a department, select it, and then click . You cannot delete a department with personnel.
- To rename a department, select it, and then click .

4.19.1.2 Adding Personnel

Add personnel and authorize them to unlock doors. When adding personnel, system uploads the collected personnel information to the server for proper protection.



- Person ID shall be the same on the platform and access control devices; otherwise person

data could be wrong.

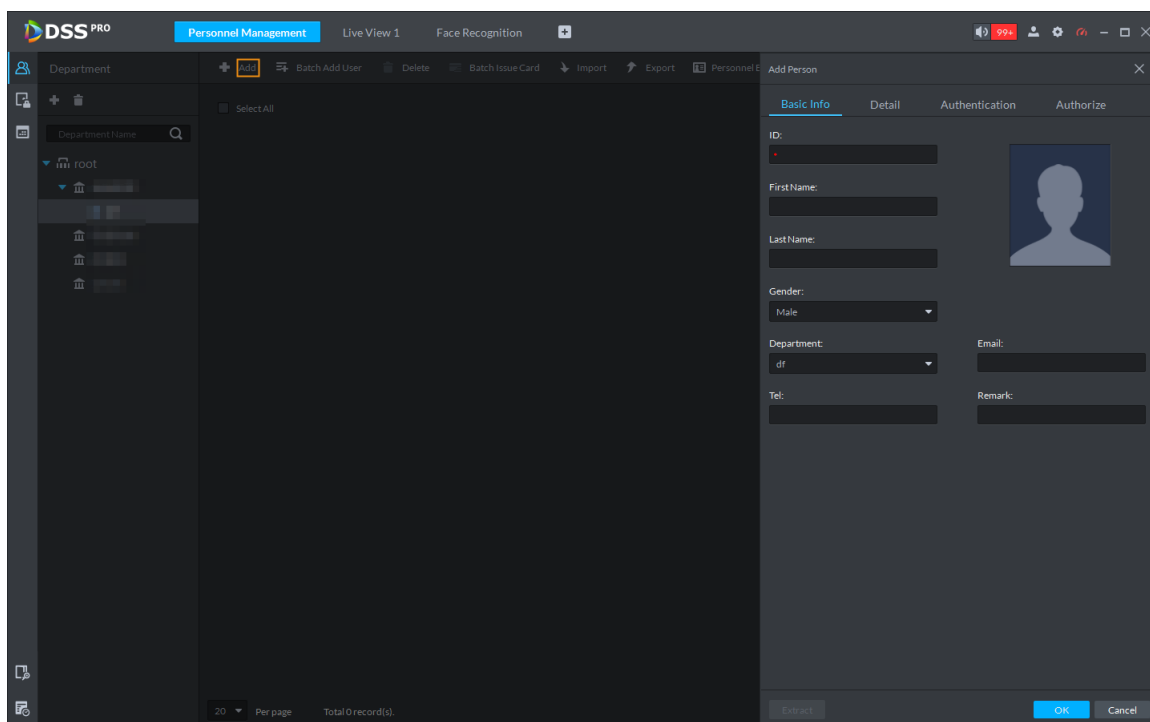
- To collect fingerprints or card No., connect a fingerprint collector or card reader first.
- IR face feature code is obtained from the access control device when editing person information.

4.19.1.2.1 Adding a Person

Step 1 Log in to the Control Client, click , and then select **Personnel Management**.


Step 2 Click **Add**.

Figure 4-320 Add a person



Step 3 Click the **Basic Info** tab to configure person information.

- 1) Hover over the profile, and then click **Upload Picture** to select a picture or click **Snapshot** to take a photo.

Click  on the **Snapshot** interface, and then you can select camera, pix format, resolution, and image quality. This is only effective with the current client.

- 2) Fill in personnel information as necessary. ID is required and must be unique, and others are optional.




If the personnel information is already on the device, you can enter the ID number, and then click **Extract** to obtain the information.

Step 4 Click the **Detail** tab, and then set person details as required.

Step 5 Click the **Authentication** tab, and then set validity period and access control information.

Figure 4-321 Authentication

Table 4-60 Authentication parameters

Parameter		Description
Term of Validity	Validity Time	Effective time of the access control permission.
	Expiration	Expiration time of the access control permission.
Access Control	Property	Set person types.  If the person has the permission of First Card Unlock, you need to select General in the Property drop-down list.
	Device Manager	Personnel include common people and system managers. A device manager has the device operation permission. This function is only effective when the person information is applied to the second-generation devices.

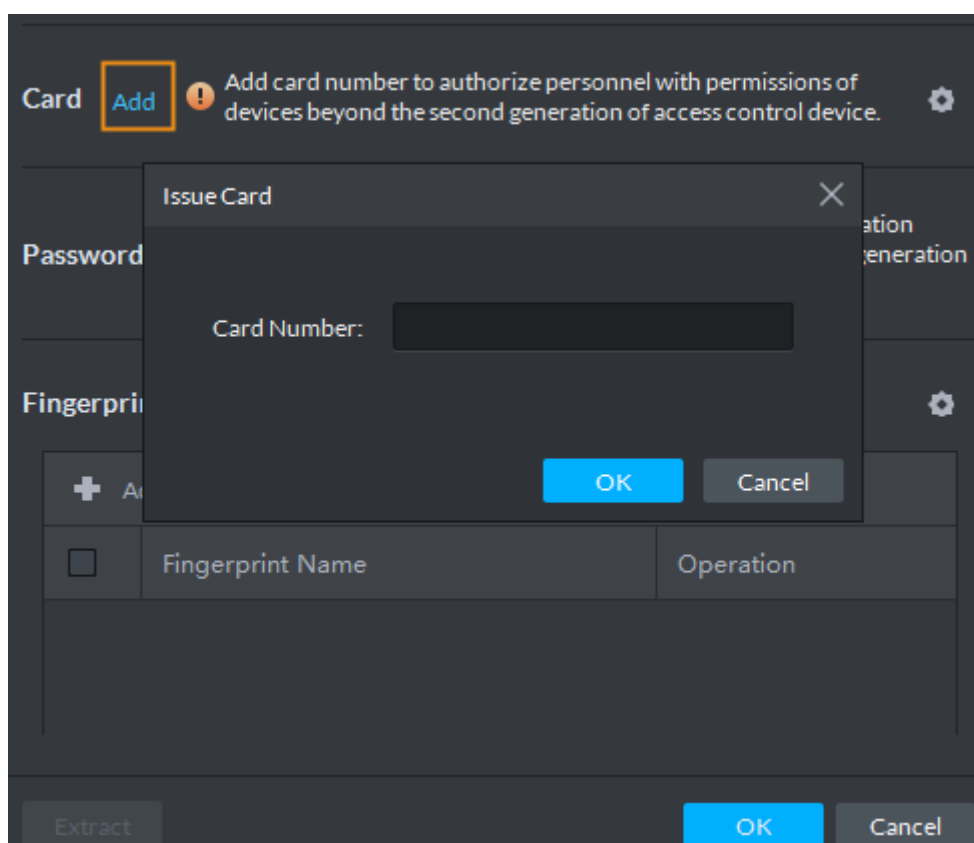
Parameter		Description
Resident Information	Room No.	Room No. is the number of the apartment in which this person lives. The room No. is displayed in the access records and video intercom operation records. Access permission of the corresponding VTO is also included when authorizing access control permission to this person.
	Householder	When several people live in one apartment, you can set one of them as the householder. The householder will be taken as the only contact of video intercom.

Step 6 Issue cards to personnel.

One person can have up to 5 cards. There are two ways to issue cards: by entering card No. and by card reader. Card No. can contain 8 or 16 numbers. 16-digit card No. is only available with the second-generation access control devices. When a card No. is less than 8 or 16 numbers, the system will automatically add zeros prior to the No. to make it 8 or 16 digits. For example, if the provided No. is 8004, it will become 00008004; if the provided No. is 1000056821, it will become 0000001000056821.

- By entering card No.
 - 1) Click **Add** next to **Card**.

Figure 4-322 Issue card by entering card No.



- 2) Enter card number and click **OK**.

Figure 4-323 Added card

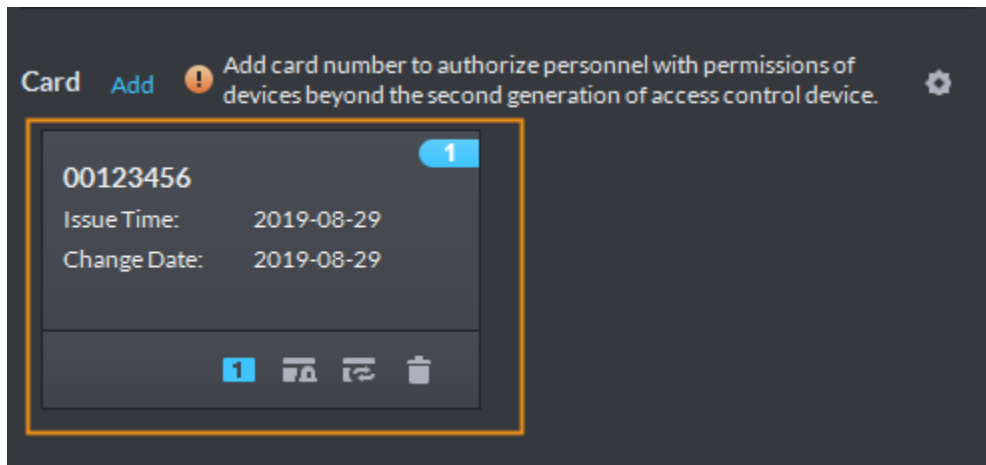


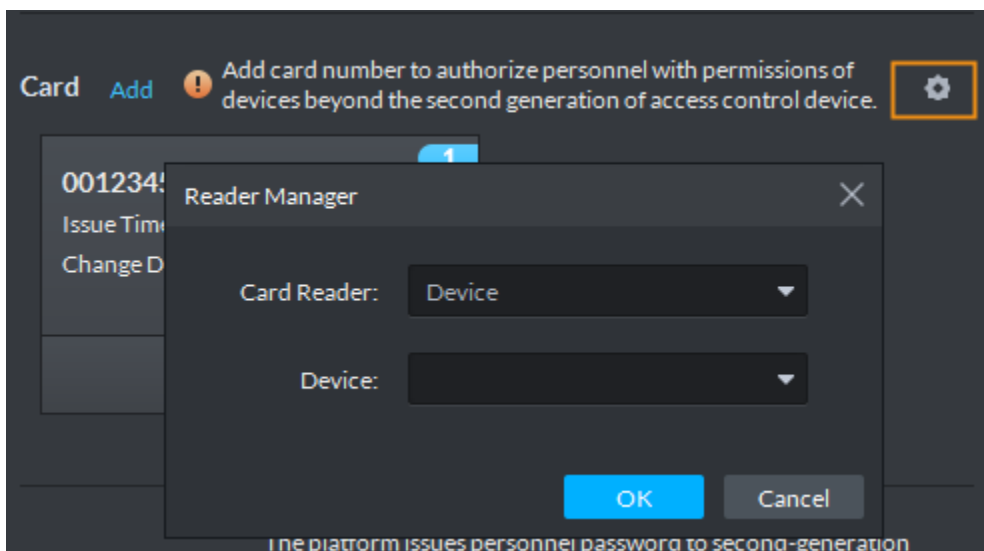
Table 4-61 Card operations

Icon	Description
	<p>If a person has more than one card, only the main card can be issued to the first-generation access control device. The first card of a person is the main card by default.</p> <p>Click on an added card, the icon turns into , which indicates that the card is a main card. Click to cancel the main card setting.</p>
	<p>Set a card as duress card. When opening door with a duress card, there will be a duress alarm.</p> <p>Click this icon, it turns into , and a icon is displayed at upper right, which indicates that the card is set as a duress card. To cancel the duress setting, click .</p>
	<p>Change card for the person when the current card does not work.</p>
	<p>Remove the card, and then it has no access permission.</p>

- By card reader

1) Click .

Figure 4-324 Issue card by card reader



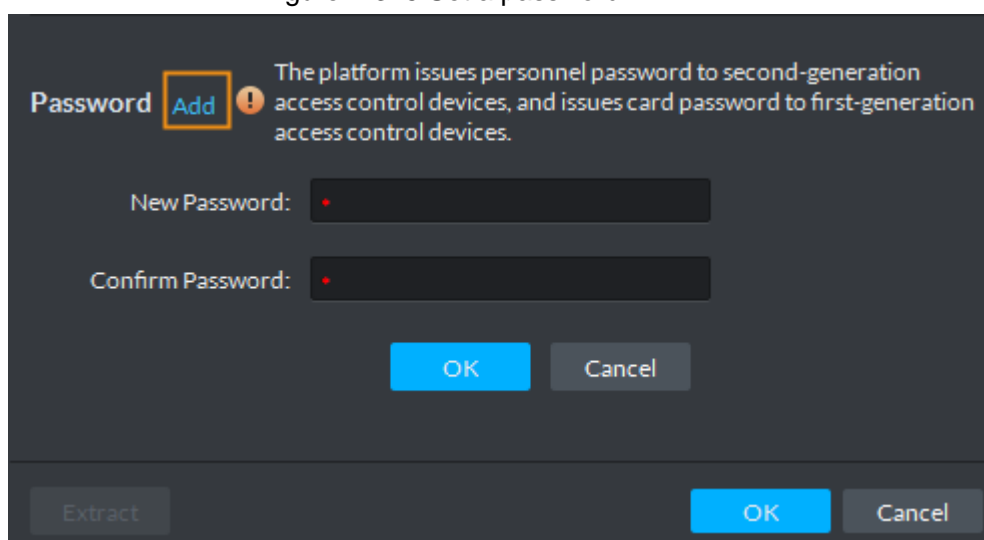
- 2) Select a reader from the **Card Reader** drop-down list or a device from the **Device** drop-down list, and then click **OK**.
- 3) Swipe card on the card reader or device.

Step 7 Set access password.

To open door with password, you need to set passwords for personnel, and then one can open door by entering person ID and password.

- 1) Click **Add** next to **Password**.

Figure 4-325 Set a password



- 2) Enter the password, and then click **OK**.

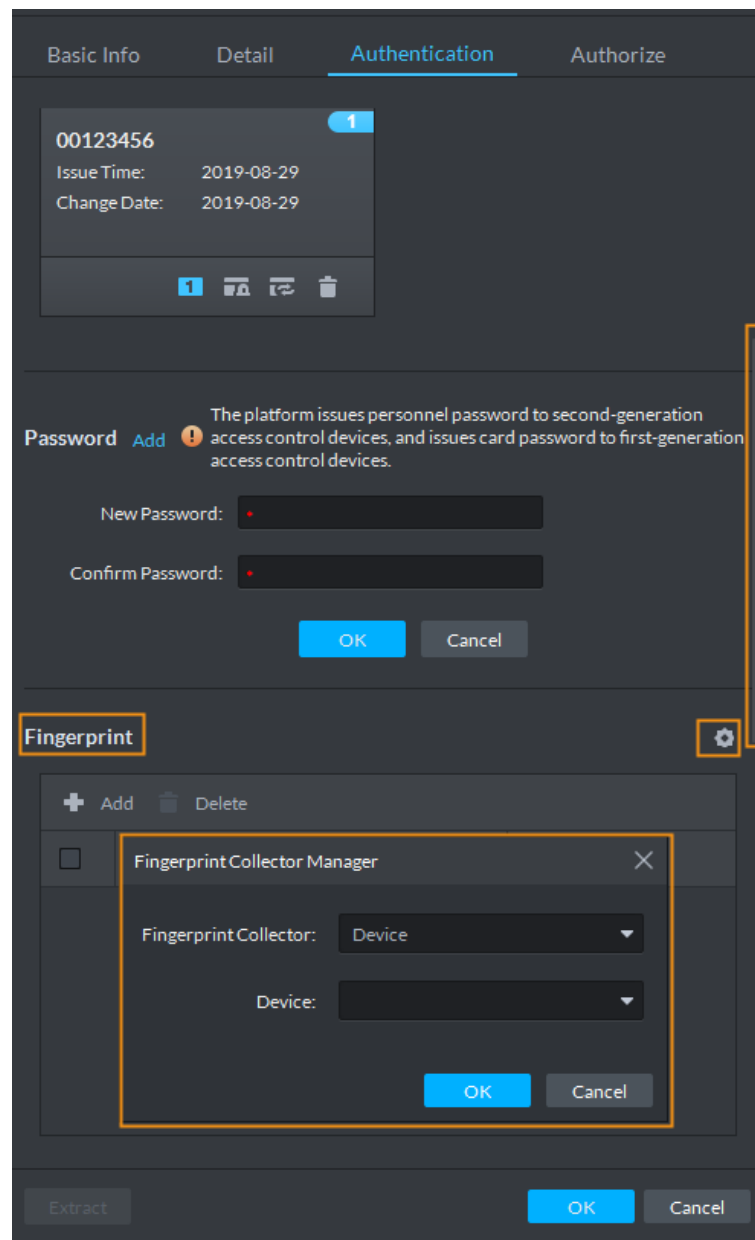
Step 8 Collect fingerprint.

To open door with fingerprint, you need to collect personnel fingerprints. A person can have up to 2 fingerprints.

- 1) Scroll down the **Authentication** page, and then in the **Fingerprint** section, click

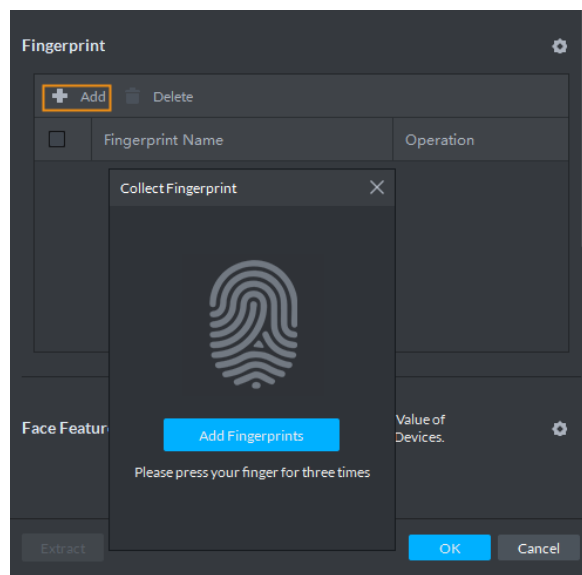


Figure 4-326 Fingerprint collector manager



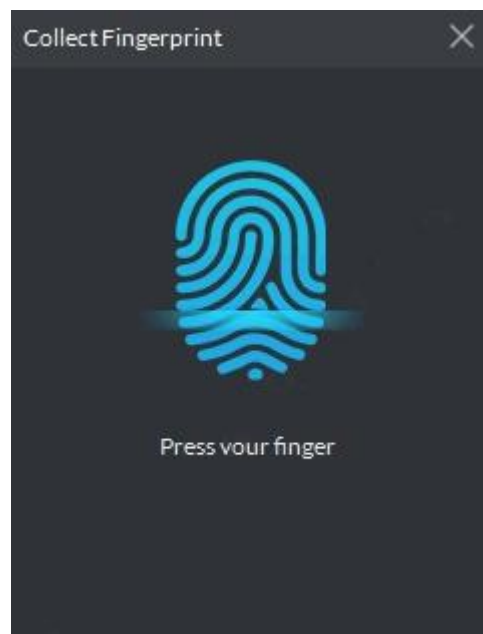
- 2) Select a fingerprint collector from the **Fingerprint Collector** drop-down list, and then click **OK**.
- 3) Click **Add**.

Figure 4-327 Collect fingerprint



- 4) Click **Add Fingerprints**.

Figure 4-328 Collect fingerprint



- 5) Keep your finger on the reader till you hear the beep sound. Repeat this three times to finish fingerprint collection.

Figure 4-329 Collecting fingerprint



Figure 4-330 A collected fingerprint

Fingerprint		
<input type="checkbox"/>	Fingerprint Name	Operation
<input type="checkbox"/>		

Table 4-62 Fingerprint operations

Icon	Description
	One can have 10 fingerprints, but only these fingerprints can be issued to devices. Click this icon, and then it turns into , which indicates that this fingerprint has been set as a main one. To cancel the main fingerprint setting, click
	Set a fingerprint as duress fingerprint. When opening door with a duress, there will be a duress alarm. Click this icon, it turns into , which indicates that the fingerprint has been set as a duress fingerprint. To cancel the duress setting, click
	Modify fingerprint name.
	Remove the fingerprint, and then it has no access permission.

Step 9 Collect face feature code.

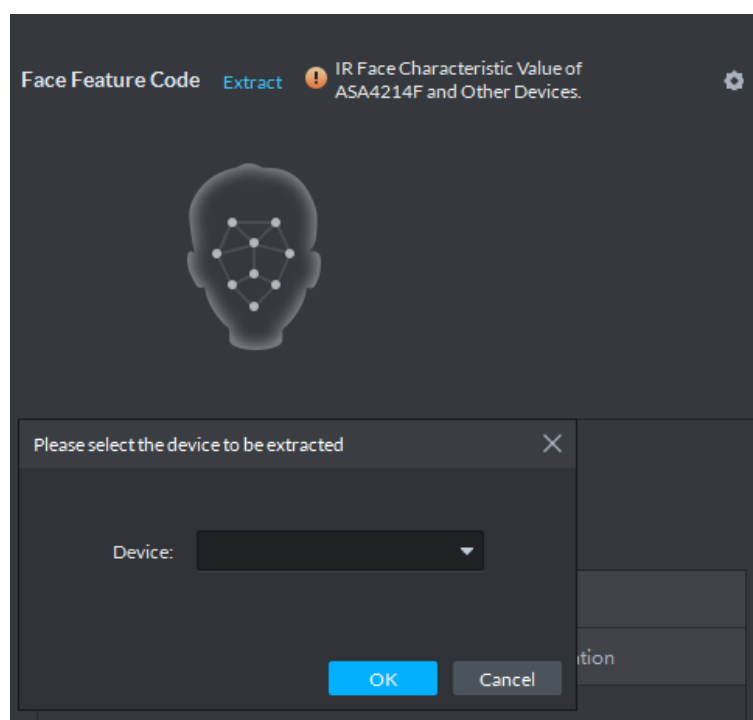
When the IR face attendance device is used, you can collect IR face feature codes through the device for face recognition, face attendance and access control.



Make sure that there is face feature codes on the IR face attendance device.

- 1) Click in the **Face Feature Code** section.

Figure 4-331 Select a device



- 2) Select an IR face attendance device, and then click **OK**.

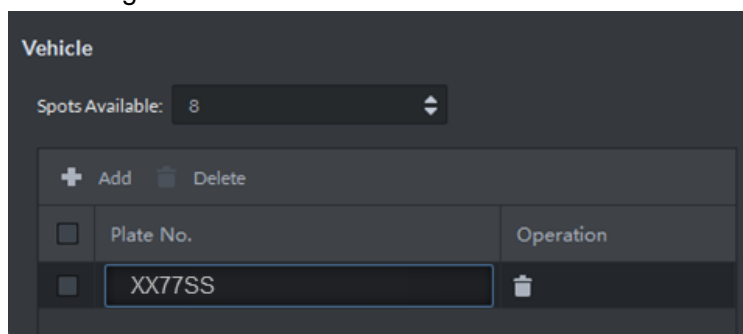
3) Click **Extract**.

Step 10 Add vehicle information.

Add vehicle information to a person, so as to enable vehicle access permission for this person.

Enter the maximum parking space number to the person, click **Add**, and then enter license plate numbers.

Figure 4-332 Add vehicle information

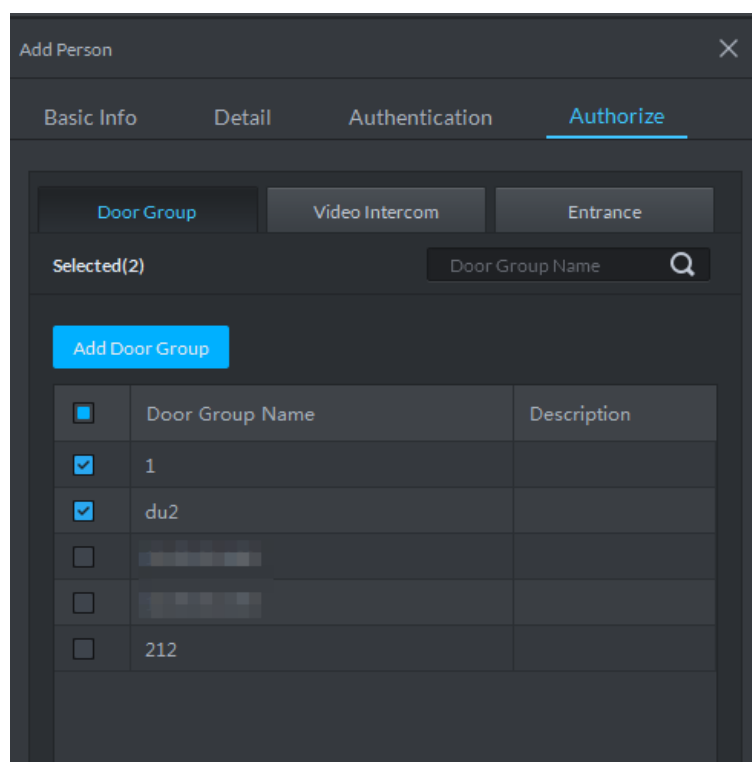


Step 11 Click the **Authorize** tab, and then select the target door groups, entrance & exit channels and video intercom channels.



A door group contains a group of doors which can be authorized in batches. To add a door group, click **Add Door Group**.

Figure 4-333 Authorize



Step 12 Click **OK**.



- To edit person information such as basic details, passwords, fingerprints, IR face feature codes and face pictures, see "4.19.1.6 Editing Personnel Information."


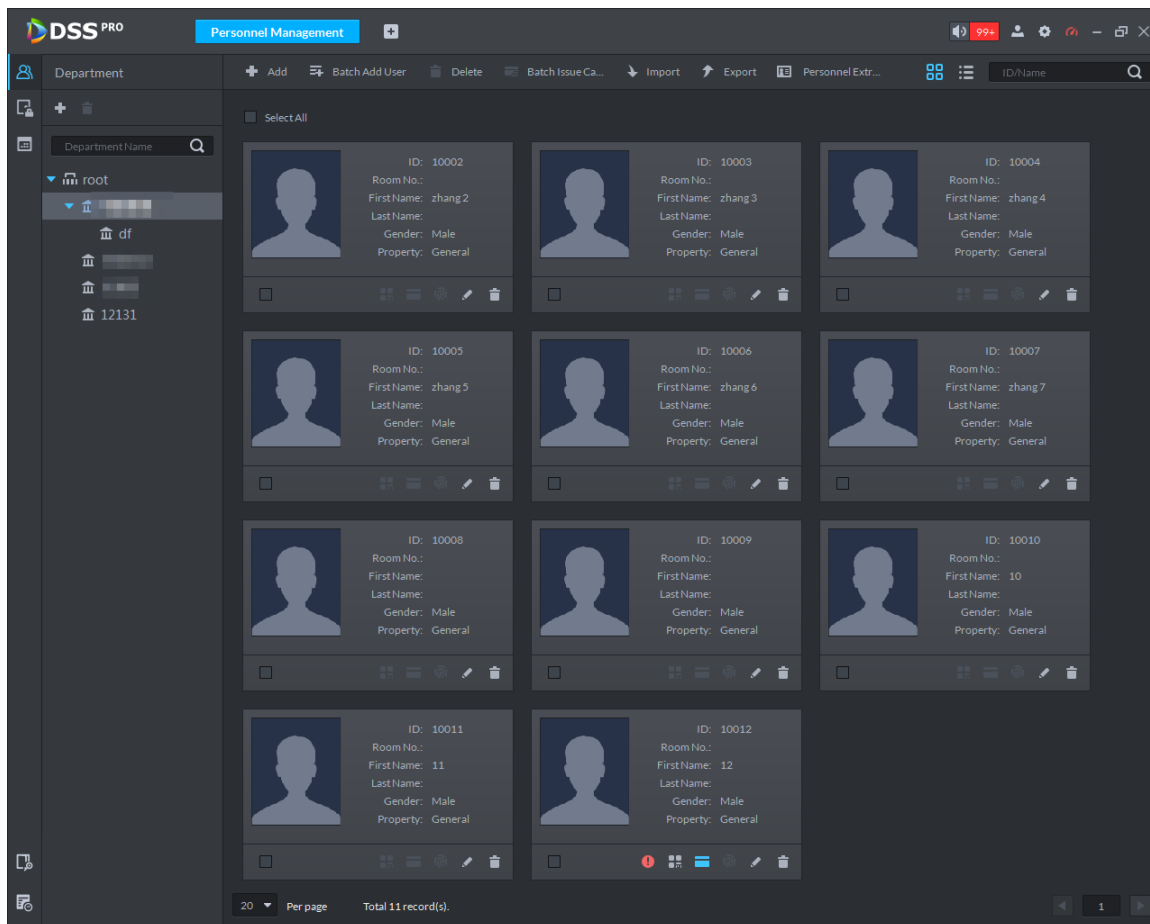
- To delete a person, you can select the person, and then click ; to delete all people on this page, select the **Select All** check box, and then click **Delete**.

Figure 4-334 Added people



4.19.1.2.2 Adding Personnel in Batches

If multiple people are added at one time, you can authorize them by issuing cards only. You cannot authorize password and fingerprint in batches. If necessary, you can authorize password and fingerprint by editing personnel authorization separately.


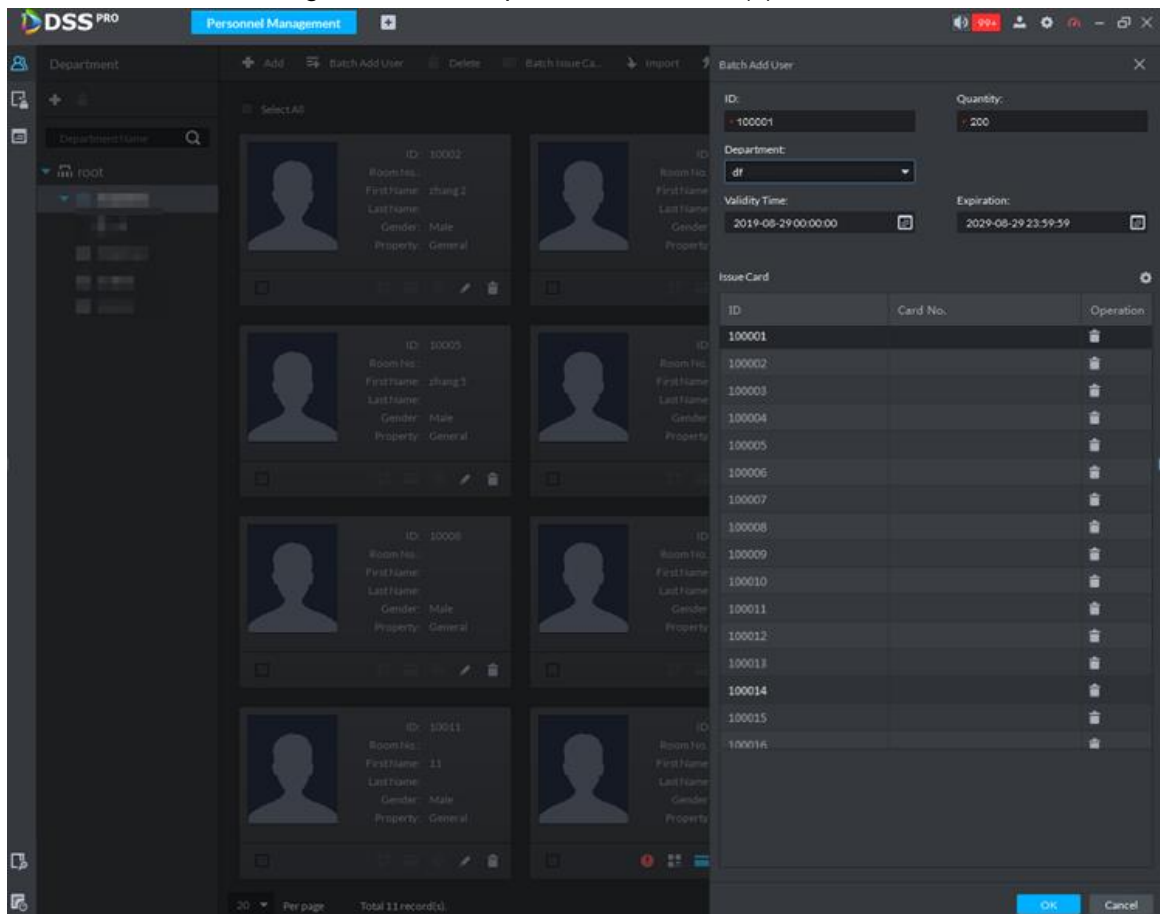
- Step 1** Log in to the Control Client, click , and then select **Personnel Management**.
- Step 2** Click **Batch Add User**.
- Step 3** Enter personnel information.

Figure 4-335 Add personnel in batch (1)

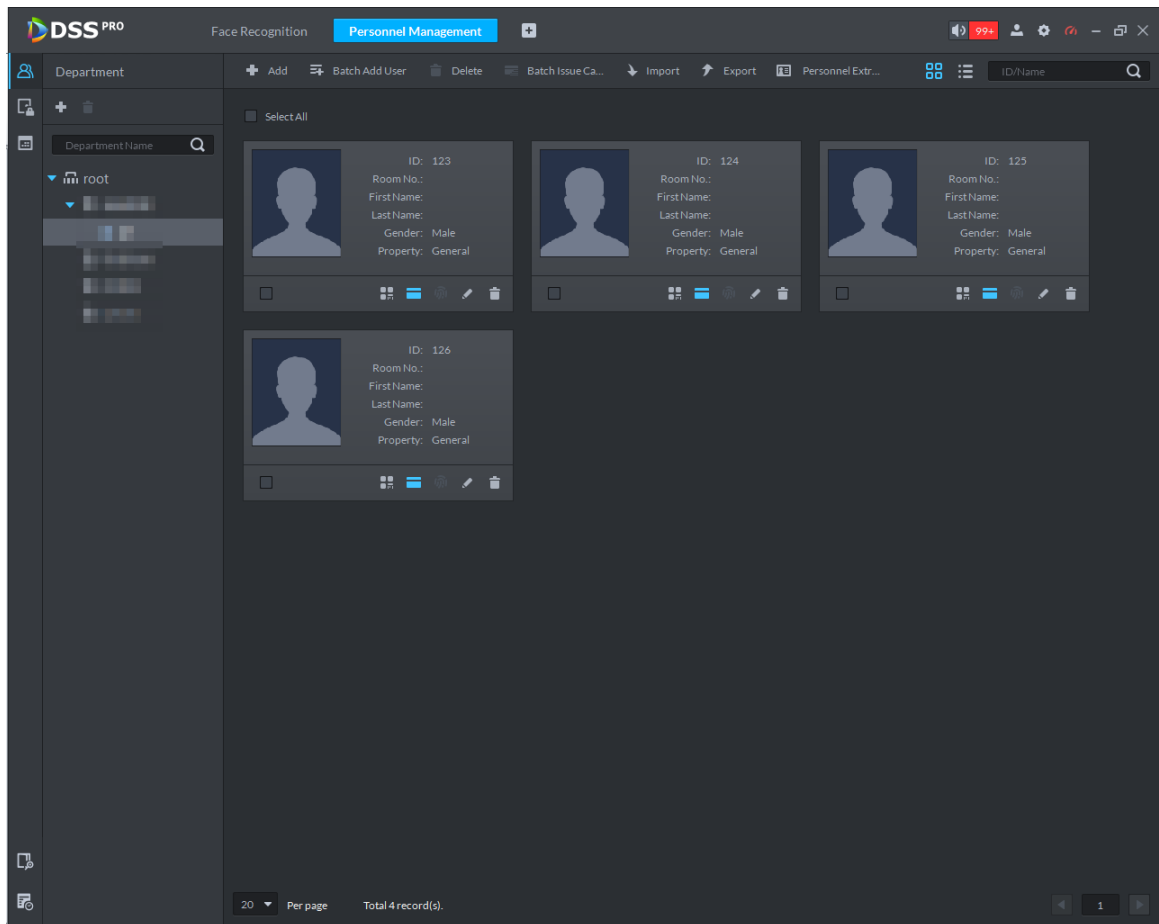


Step 4 Issue cards.

You can issue cards by entering card numbers or by using a card reader.

- By entering card numbers
 - 1) Double-click the **Card No.** cells, and then enter a card numbers one by one.
 - 2) Click **OK**.

Figure 4-336 Newly added people




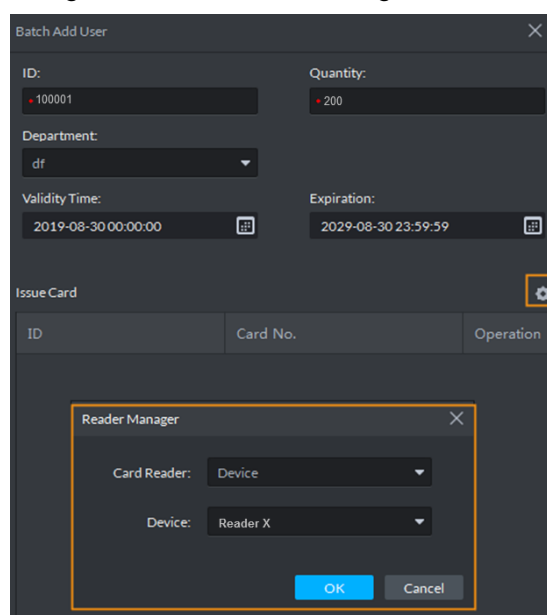
- By using card reader.
- 1) On the **Batch Add User** interface, click .
 - 2) Select a card reader or a device, and then click **OK**.

Figure 4-337 Reader manager



- 3) Select people, and then swipe cards on the card reader or device.
- 4) Click **OK**.

Step 5 Bind cards to people or authorize access control permissions.

- To bind cards to people and authorize one by one, or edit people information, see "4.19.1.6 Editing Personnel Information."
- To bind cards to people and authorize in batches, see "4.19.1.3 Issuing Cards in Batches" and "4.19.1.4 Quick Authorization."

4.19.1.2.3 Importing Personnel

To quickly add a number of personnel, you can download a personnel template, fill in it and then import it to the platform. You can also import an existing personnel file.

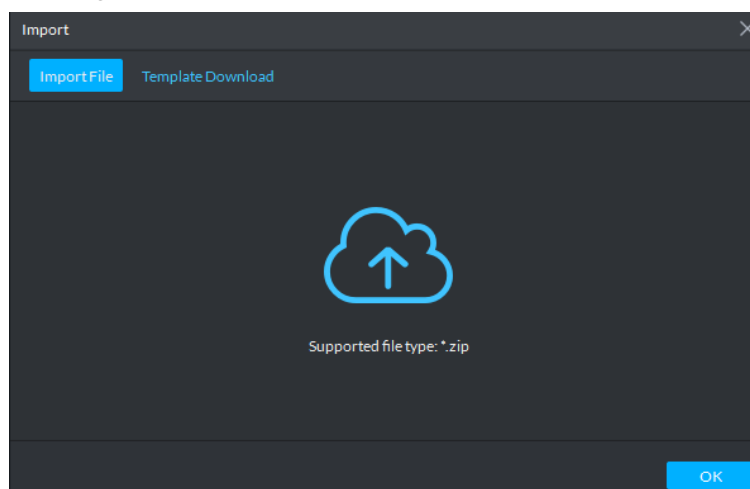


- Personnel file shall be a zip package which includes an .xlsx file and face pictures (optional). Support up to 10000 pieces of person information. A personnel file shall not be larger than 1 GB.
- Support importing personnel file exported from SmartPSS.
- For a person with First Card Unlock permission, the person attribute shall be set as **General**.

Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

Step 2 Click **Import**.

Figure 4-338 Import personnel information



Step 3 Import the personnel information file.



If there is no personnel information file, click **Template Download** and follow the instructions on the interface to create personnel information.

Step 4 Click **OK**.

The following cases might occur during an import:

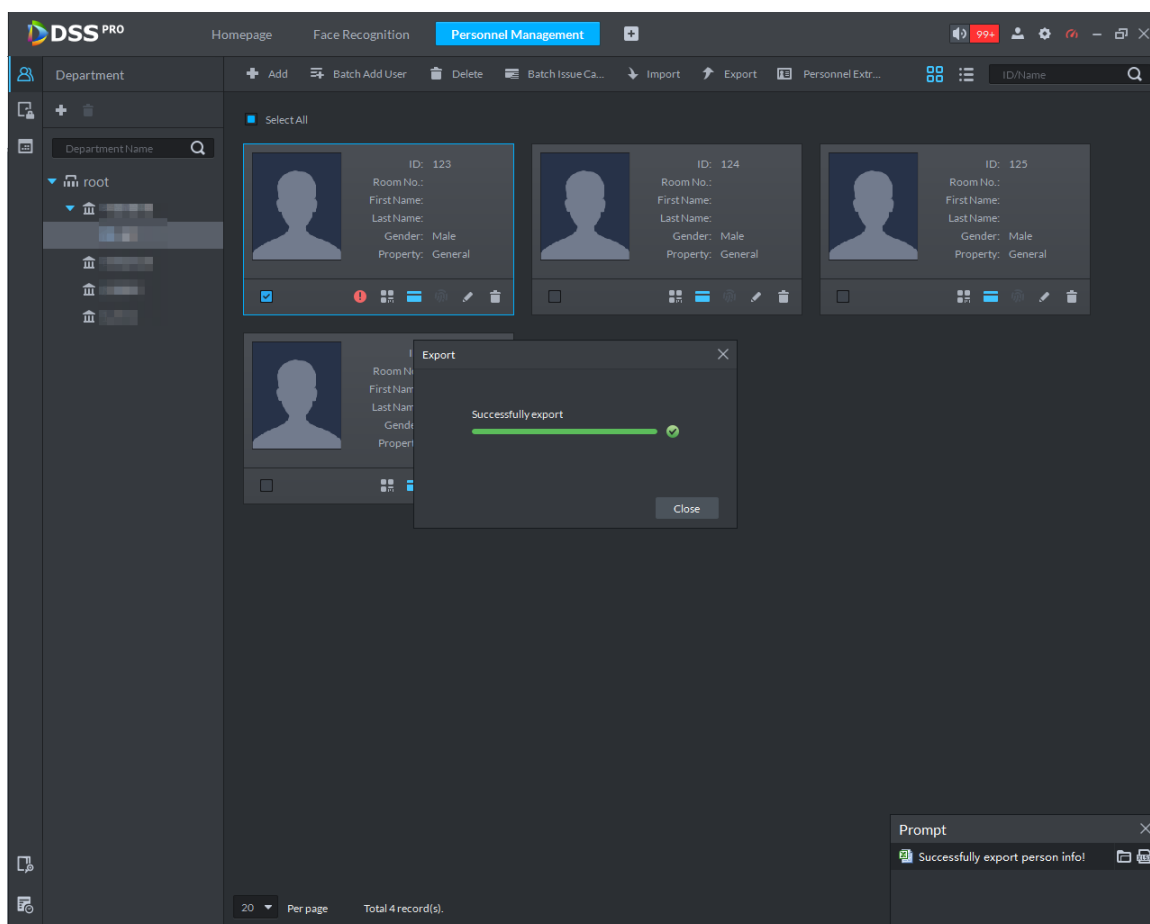
- If there are failures, you can download the failures list to view details.
- A person does not exist and the department does not exist, either. A new department will be created under the root node; if the department exists, the person is created under the department; department information matches by name.
- Cannot read the contents with a parsing error reported directly.

Other Operations

- Export personnel information.

On the left side of the **Personnel Management** interface, select an organization, click **Export**, and then follow the instructions on the interface to save the exported information to a local disk.

Figure 4-339 Export progress



- Download template

To add personnel information in batches, you can download the template, fill in and import it.

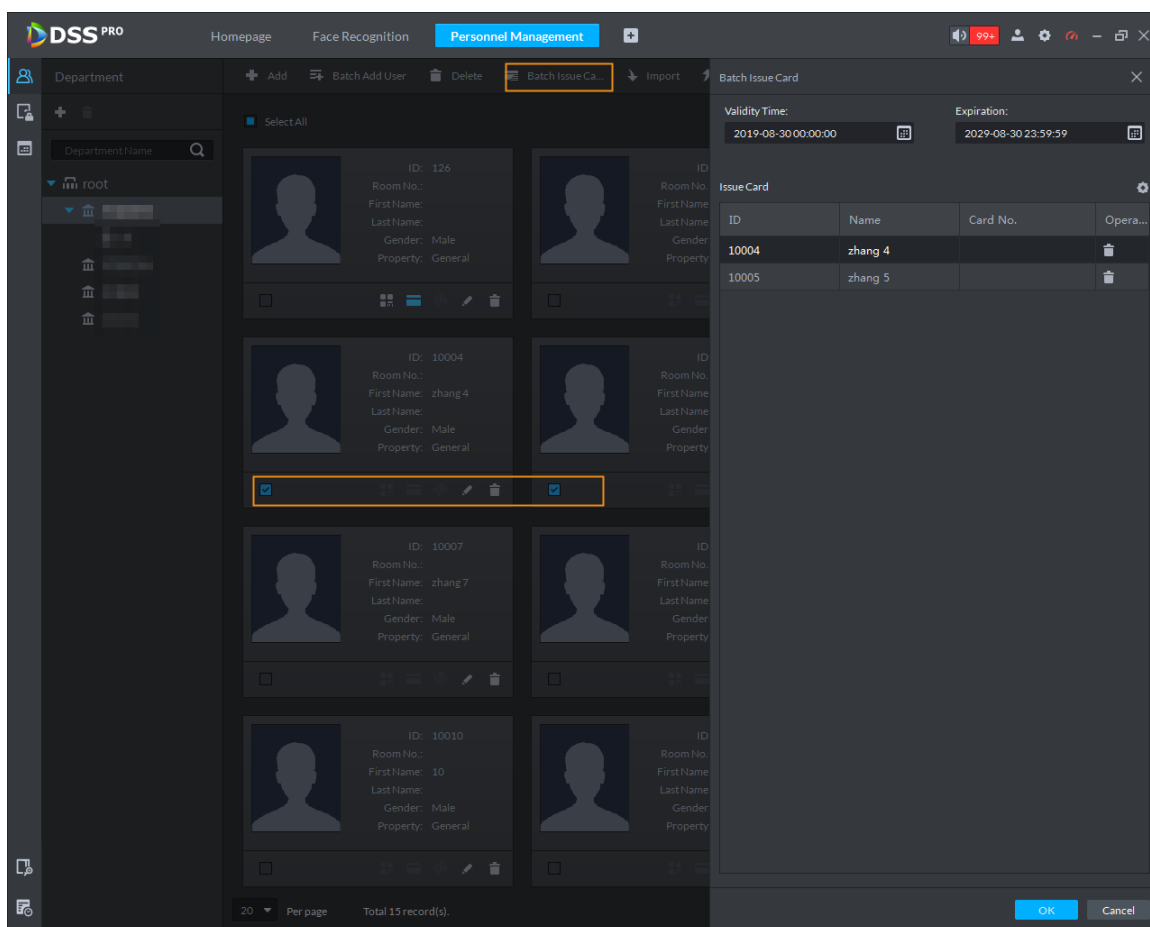
On the **Personnel Management** interface, click **Import**, download and then fill in the template before importing it.

4.19.1.3 Issuing Cards in Batches

Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

Step 2 Select the people to issue card to, and then click **Batch Issue Card**.

Figure 4-340 Issue card in batch



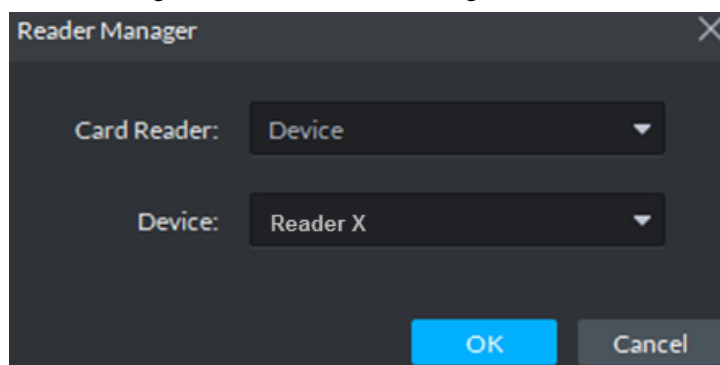
Step 3 Set term of validity.

Step 4 Issue cards to personnel.

Support issuing cards by entering card number or by using a card reader.

- By entering card number
 - 1) Double-click the Card No. cells to enter card numbers one by one.
 - 2) Click **OK**.
- By using a card reader
 - 1) Click
 - 2) Select a card reader or device, and then click **OK**.

Figure 4-341 Reader manager



- 3) Select people one by one and swipe cards respectively until everyone has a card number.
- 4) Click **OK**.

4.19.1.4 Quick Authorization

Configure access permissions in a fast way.

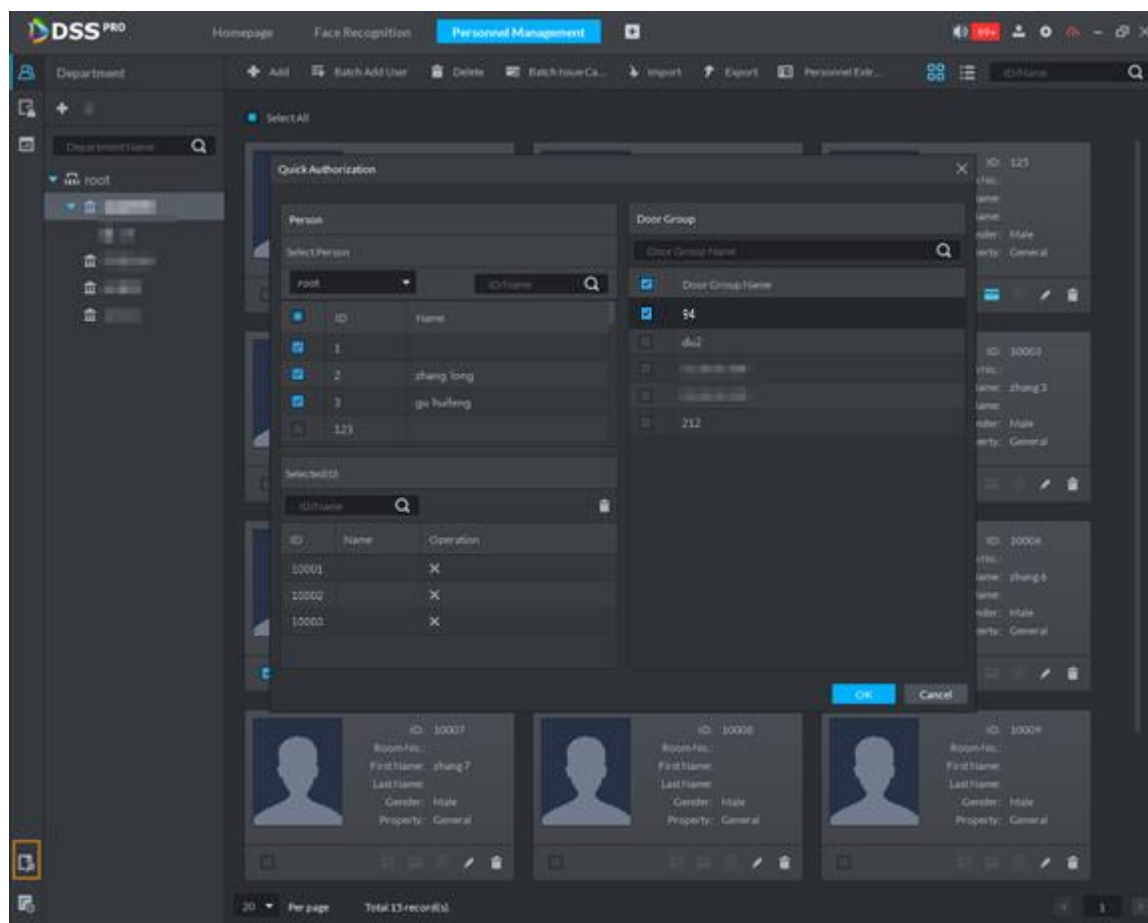
Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

Step 2 Click .

Step 3 Select personnel from the personnel list.


Step 4 Select door groups from the door group list.

Figure 4-342 Quick authorization



Step 5 Click **OK**.



Click  to view authorization progress.

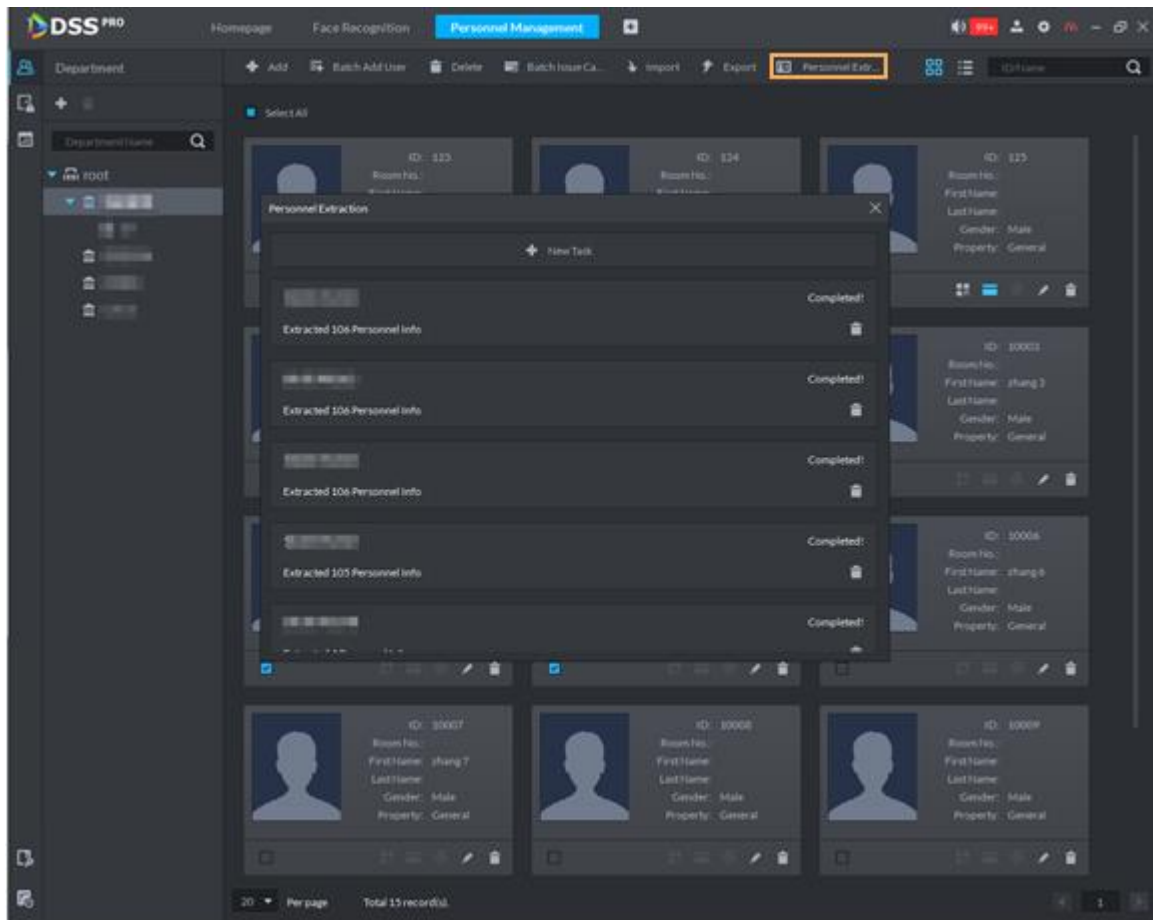
4.19.1.5 Extracting Personnel Information

When personnel information has been configured on the devices, you can directly synchronize personnel information from the devices.

Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

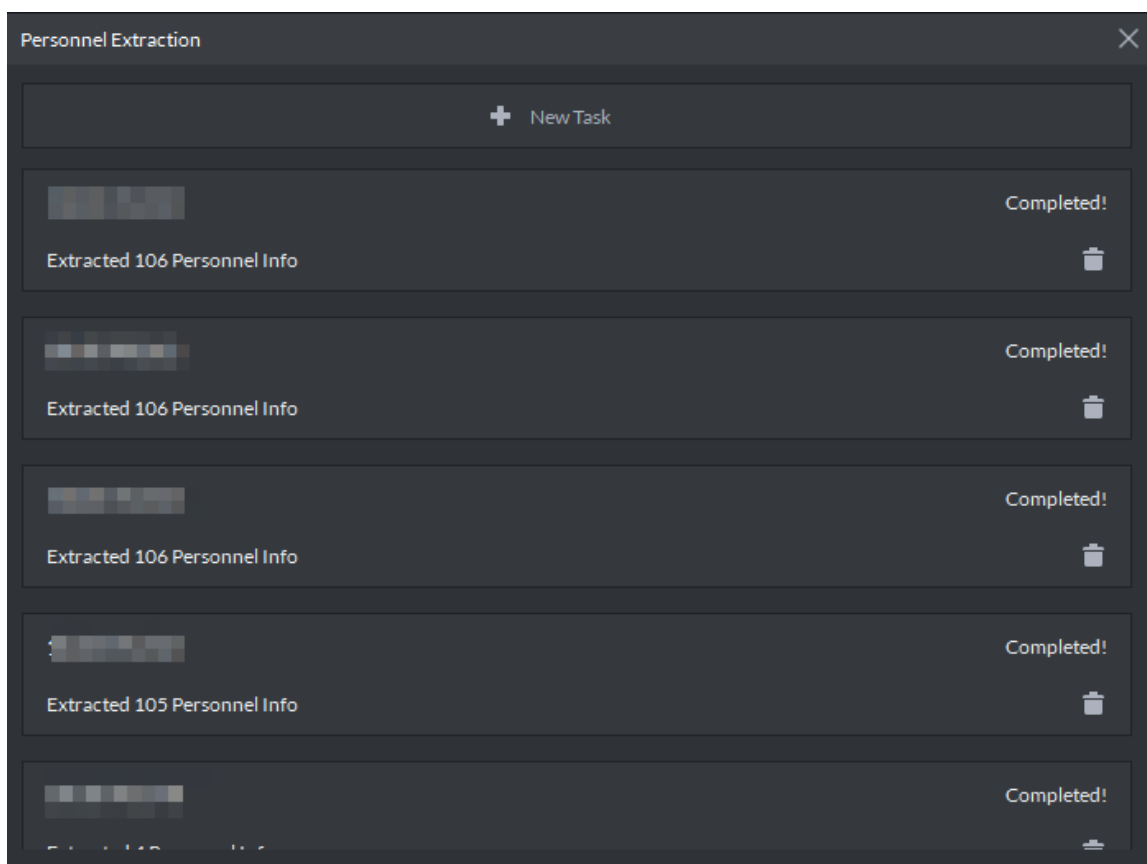
Step 2 Click **Personnel Extraction**.

Figure 4-343 Personnel extraction



Step 3 Click **New Task**, select a device, and then click **OK**.

Figure 4-344 Personnel extraction results



Step 4 Double-click a result to view the detailed information.

Step 5 Synchronize personnel information to the platform, or export information.

- To add all the personnel information to the platform, click **Synch All to Platform**.
- To add part of the information, select the people of interest, and then click **Sync Selected to Platform**.
- To export all the information, click **Export All**.
The login password is the one for logging in to the platform.
- To export part of the information, click **Export Selected**.


4.19.1.6 Editing Personnel Information

Modify personnel information including basic information, authentication details, and authorization. Person ID cannot be modified.



Make sure that the corresponding devices are well-connected before collecting fingerprints, card numbers or face pictures from fingerprint collectors, card readers, or IR face attendance devices.

Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

Step 2 Double-click a person or click  to edit information. For details, see "4.19.1.2.1 Adding a Person."

4.19.1.7 Tracing Back Person Access Path

You can check all door unlocking records of a person and view the access path.



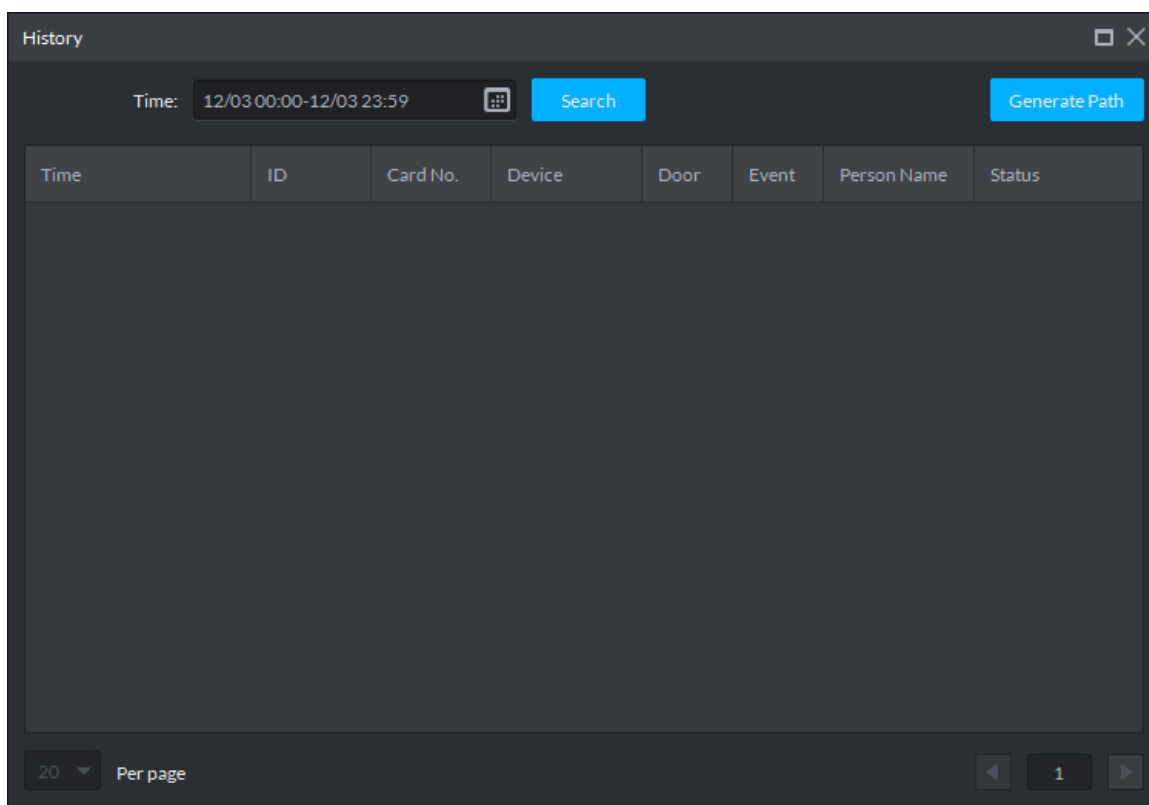
To view the generated path, you have to drag the access control devices to the map in advance.

Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

Step 2 Click  or .

Step 3 Set search time, and then click **Search**.

Figure 4-345 History



Step 4 Click **Generate Path**.

The map interface which shows the corresponding path is displayed.

Step 5 Click **Export**, and then drag to select a region to save the path as a picture to the local disk.

4.19.2 Configuring Door Groups

Configure door groups so that you can quickly assign permissions by door groups.

Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

Step 2 Click .

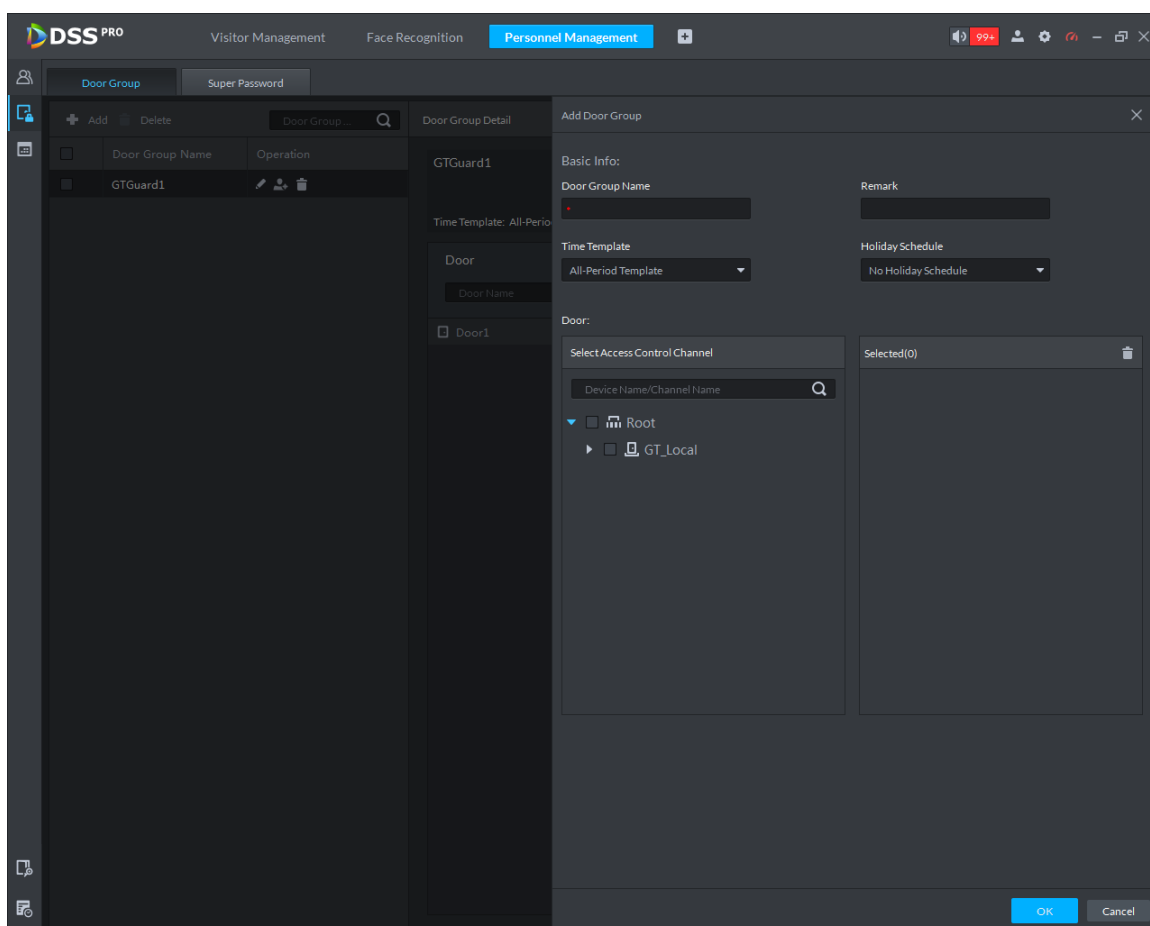
Step 3 Create a door group.

- 1) Click the **Door Group** tab.
- 2) Click **Add**.
- 3) Enter the group name, select a time template and a holiday schedule, select a device channel, and then click **OK**.

After the time template and device channel is selected, the permission assigned to personnel is valid only for period of the selected time template of the selected device channel.

- ◇ To create a new time template, select **Manage time template** in the **Time Template** drop-down list. For details, see "4.19.4 Configuring Time Templates."
- ◇ To create a new holiday schedule, select **Add Holiday Schedule** in the **Holiday Schedule** drop-down list. For details, see "4.19.5 Configuring Holiday Schedules."

Figure 4-346 Add a door group



Step 4 Authorize.


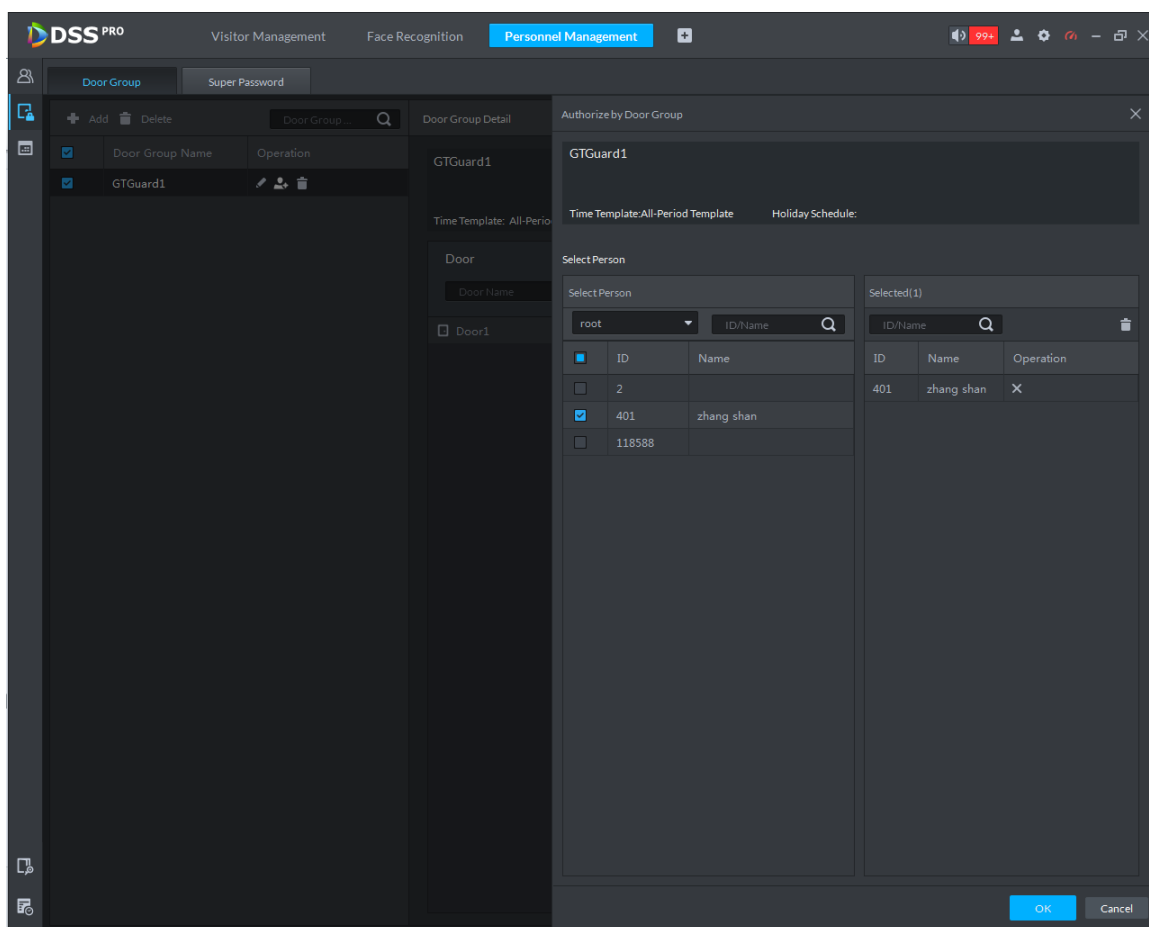
- 1) On the **Door Group** interface, select a door group, and then click the corresponding  icon.
- 2) Select personnel, and then click **OK**.

Figure 4-347 Authorize by door group



4.19.3 Configuring Admin Passwords

You can unlock the door using admin password only if admin password is configured and supported on the model of access control device.

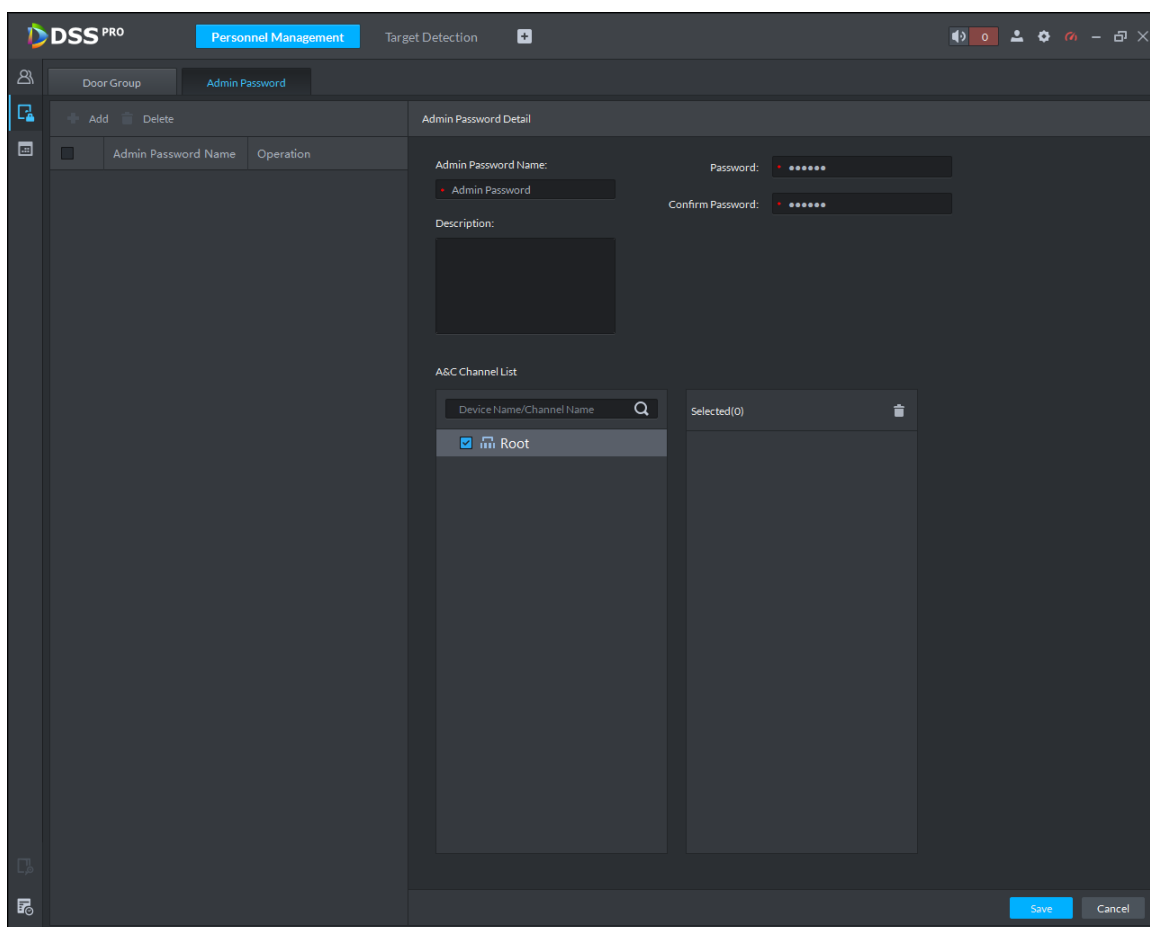
Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

Step 2 Click .

Step 3 Click the **Admin Password** tab.

Step 4 Click **Add**, set password, and select the access controller channels.

Figure 4-348 Add a super password



Step 5 Click **Save**.

4.19.4 Configuring Time Templates

Configure time templates for access control. A permission is only valid within the selected time period.

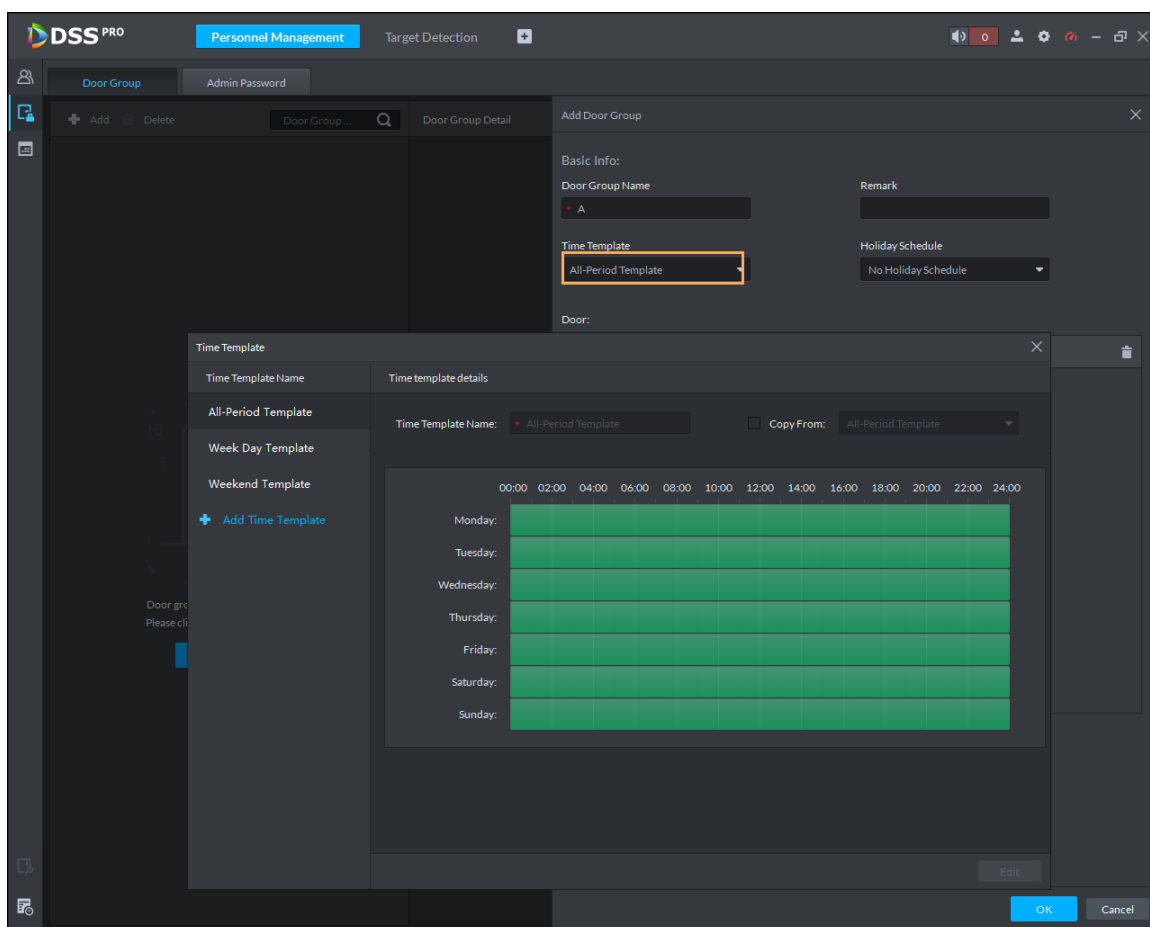
Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

Step 2 Click .

Step 3 Click the **Door Group** tab.

Step 4 Select **Manage time template** in the **Time Template** drop-down list when adding or editing a door group.

Figure 4-349 Time template






Step 5 Click Add Time Template.


Step 6 Enter the template name, set time periods, and then click **OK**.

Two ways to set time periods:

- Drag your mouse cursor on the time bars to select time sections. To remove a selected time section, click on the time bar and drag, the unneeded sections are removed.



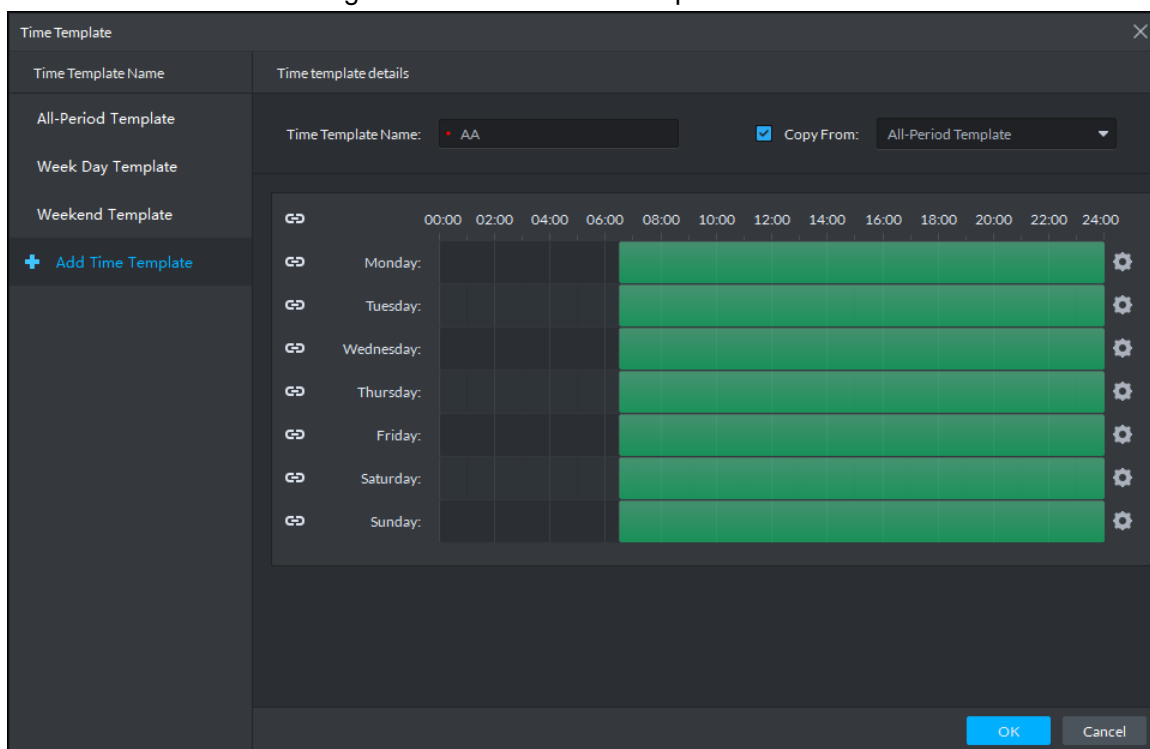
To configure time periods for multiple days, click the corresponding  icons, and then the icons have turned into , which means the days are selected. Drag on the time bars to set time sections for the selected days. To select all days, click the first  icon.

- Click , and then set time periods in the **Period Setup** dialog box. Up to 6 periods can be added.



To use an existing template, select the **Copy From** check box and then select a template in the drop-down list.

Figure 4-350 Add a time template




4.19.5 Configuring Holiday Schedules

Configure holiday schedules.

4.19.5.1 Setting Holidays

Set holidays before configuring holiday schedules. Support up to 16 holidays.

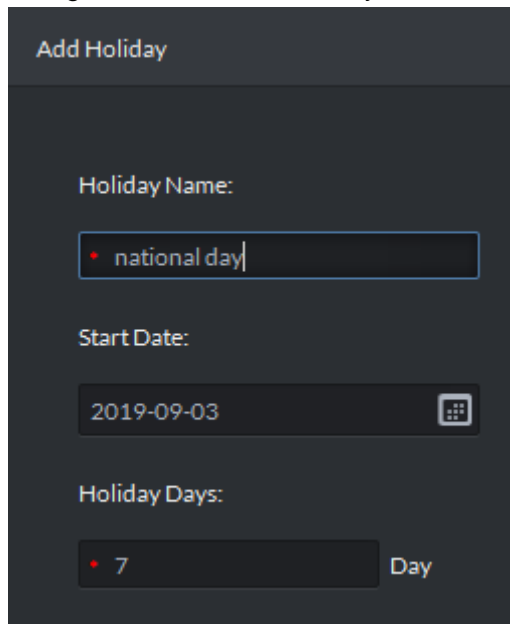
Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

Step 2 Click .

Step 3 Click the **Holiday** tab.

Step 4 Click **Add**, and then set a holiday.

Figure 4-351 Add a holiday




Step 5 Click **OK**.

4.19.5.2 Configuring Holiday Permissions

Set access control schedules for the holidays. Up to 4 schedules can be added.

Step 1 Log in to the Control Client, click , and then select **Personnel Management**.

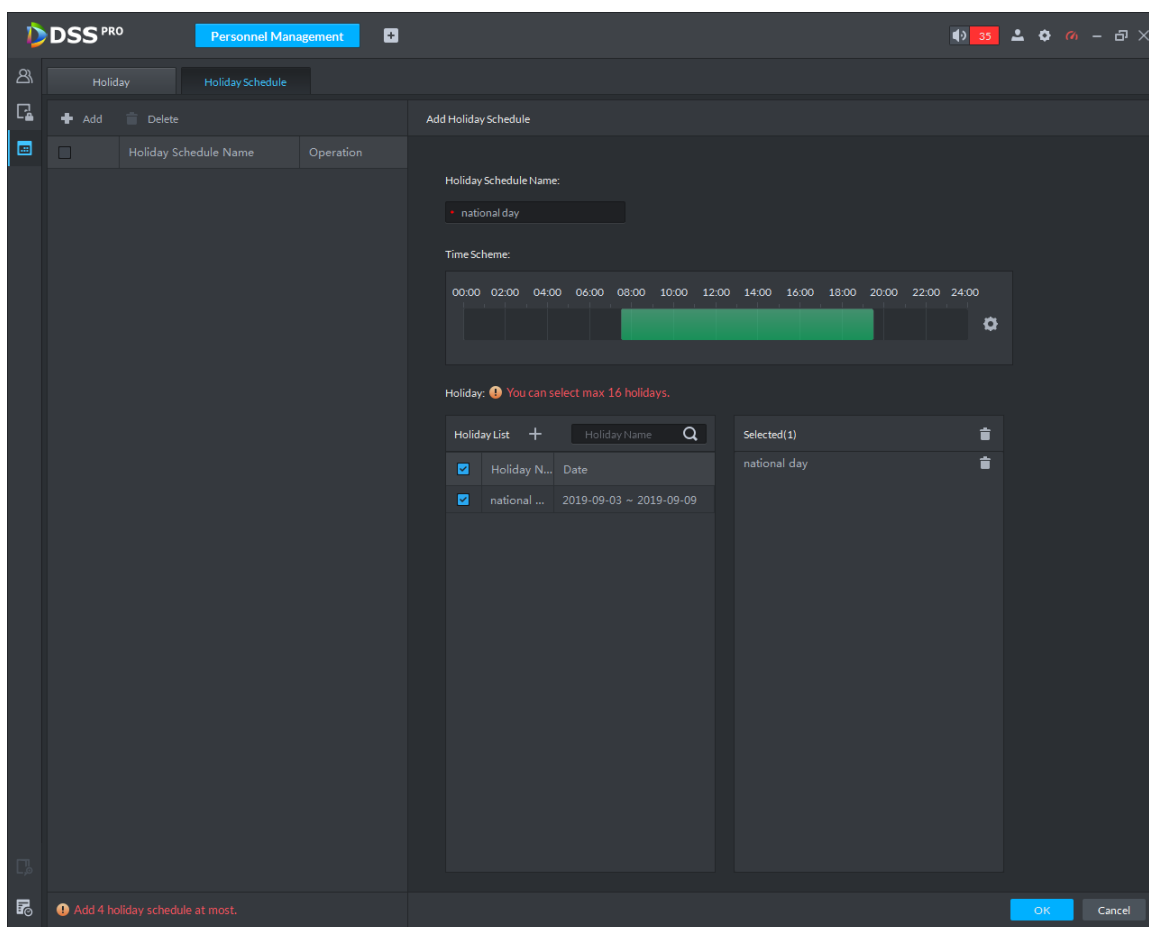
Step 2 Click .

Step 3 Click the **Holiday Schedule** tab.

Step 4 Click **Add**.

Step 5 Set the parameters as required, and then click **OK**.

Figure 4-352 Add a holiday schedule

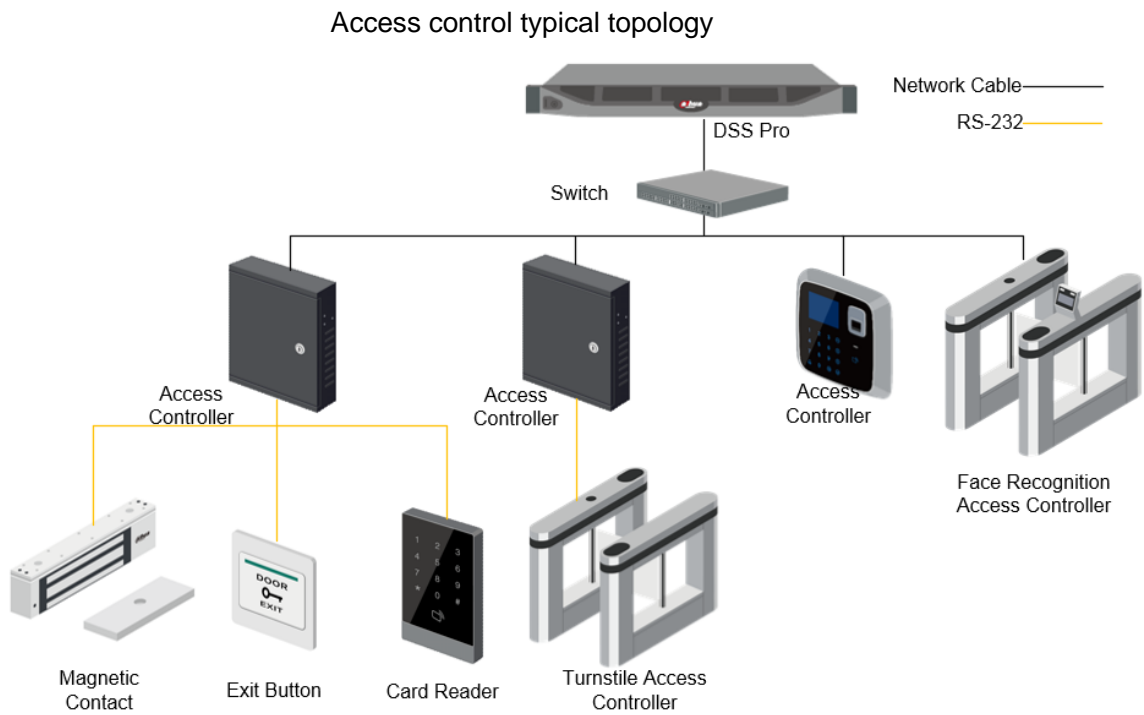


4.20 Access Control

Use the platform to achieve remote access control, view access videos and events, as well as configure advanced functions such as First-card Unlock and Multi-card Unlock.

- **Access control**
Issue cards, collect fingerprints and face data, and apply permissions, so that the authorized people can open door by using card, face or fingerprint.
- **Advanced functions**
Configure advanced access control rules such as First-card Unlock, Multi-card Unlock, Anti-pass Back and Interlock to enhance security.

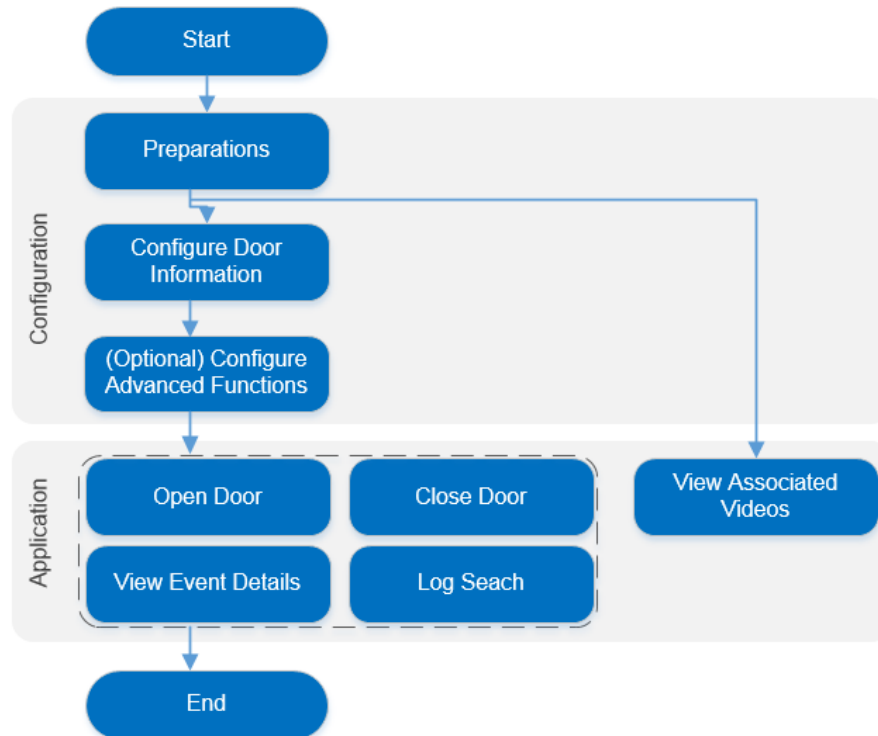
4.20.1 Typical Topology



- Access control devices are used to control doors or barriers.
- The platform centrally manages all devices.

4.20.2 Business Flow

Figure 4-353 Access control business flow



4.20.3 Configuring Access Control

4.20.3.1 Preparations

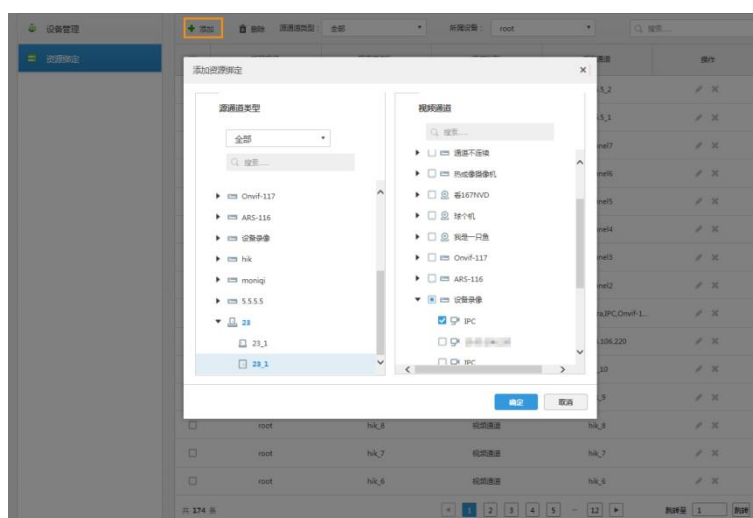
Make sure that the following preparations have been made:

- Access control devices are correctly deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding access control devices on the **Device** interface of Web Manager, select **Access Control** for device category.

Figure 4-354 Add device

- ◇ (Optional) On the **Bind Resource** interface, bind video channels for access control channels.

Figure 4-355 Bind video channels for access control channels



- ◇ Personnel information is added correctly. For details, see “4.19 Personnel Management.”

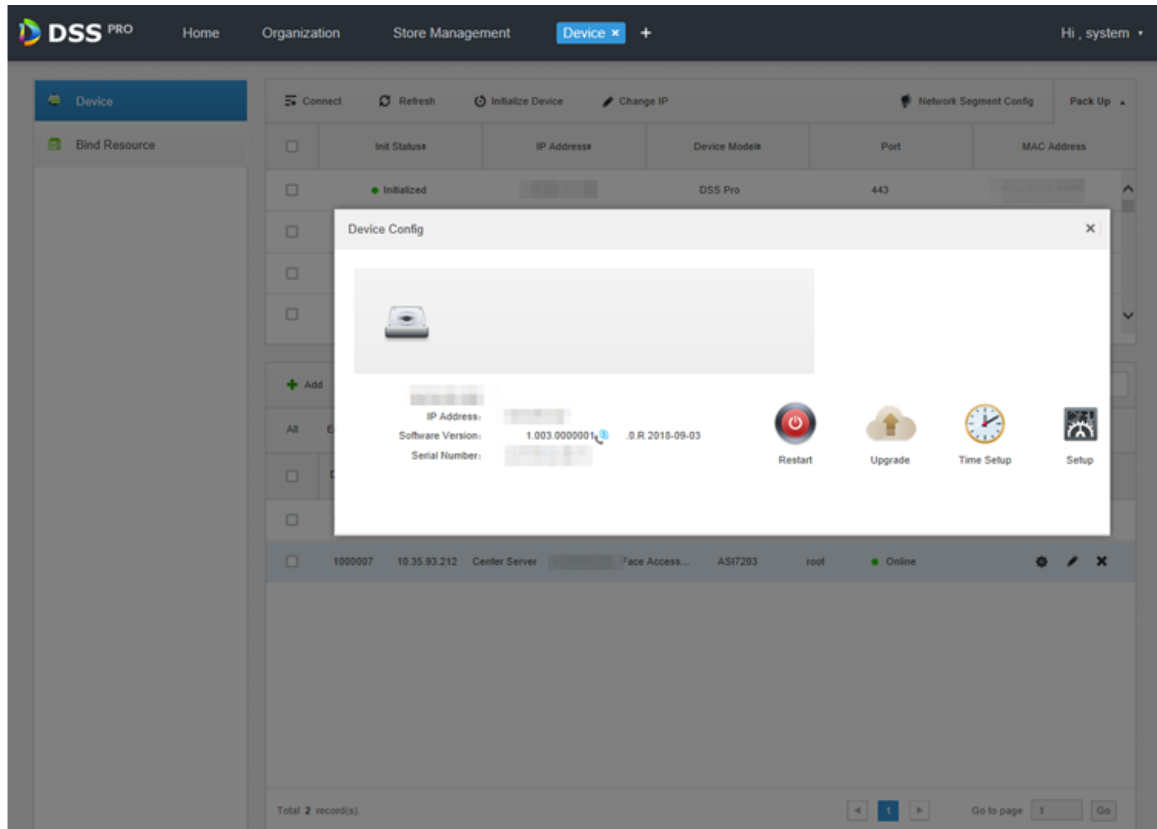
4.20.3.2 Configuring Access Control Devices

After an access control device is added, and if it is online, you can restart and upgrade it, and synchronize device time.

Step 1 Click . On the **New Tab** interface, select **Device**.

Step 2 Click of an access control device.

Figure 4-356 Device configuration



Step 3 Configure access control devices.

- Restart device

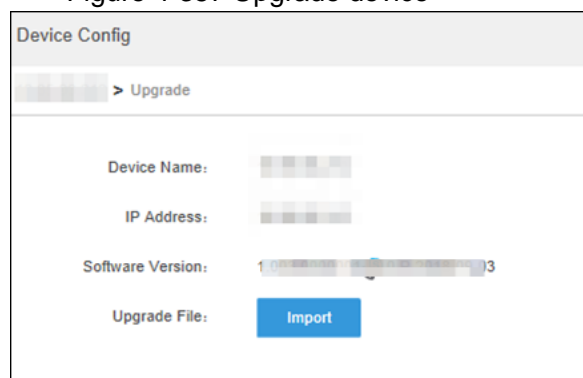
Click to restart.

- Upgrade device

Prepare the new firmware in advance.

- Click .

Figure 4-357 Upgrade device



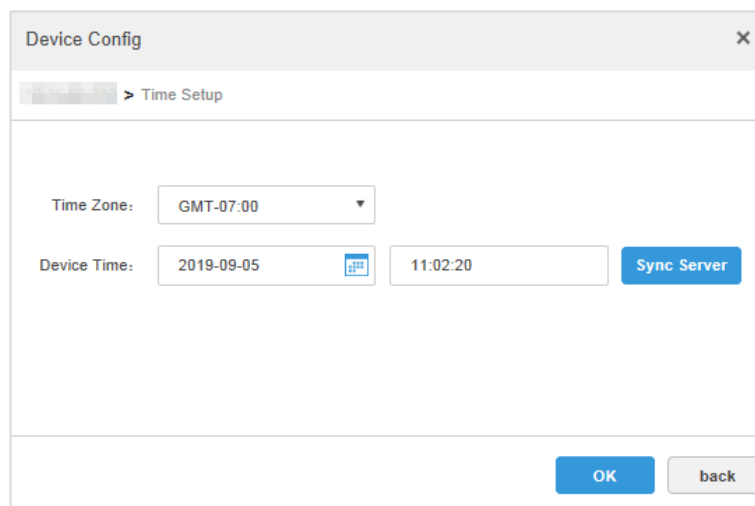
- Click **Import**, and then follow the onscreen instructions to complete upgrading.


- Click **Back** or to exit the upgrade dialog box.

- Synchronize device time
Synchronize device time to make it the same as the platform server time.

- 1) Click .

Figure 4-358 Synchronize device time



- 2) Click Sync Server.
The device time on the interface is refreshed.
- 3) Click **OK**.
Device time is synchronized.
- 4) Click **Back** or  to exit the dialog box.



To go to the local configuration interface of access controller, click .

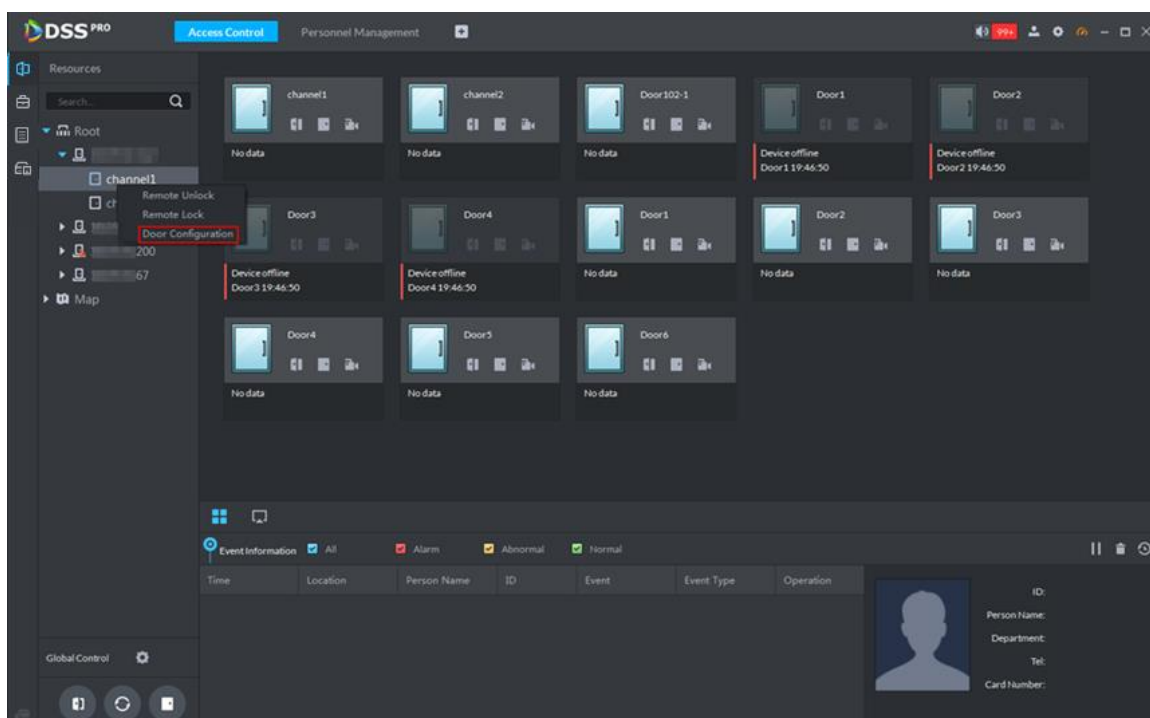
4.20.3.3 Configuring Door Information

Support configuring door status, Always-Open or Always-Close period, alarm and more.

Step 1 Click  on the Control Client, and then select **Access Control**.

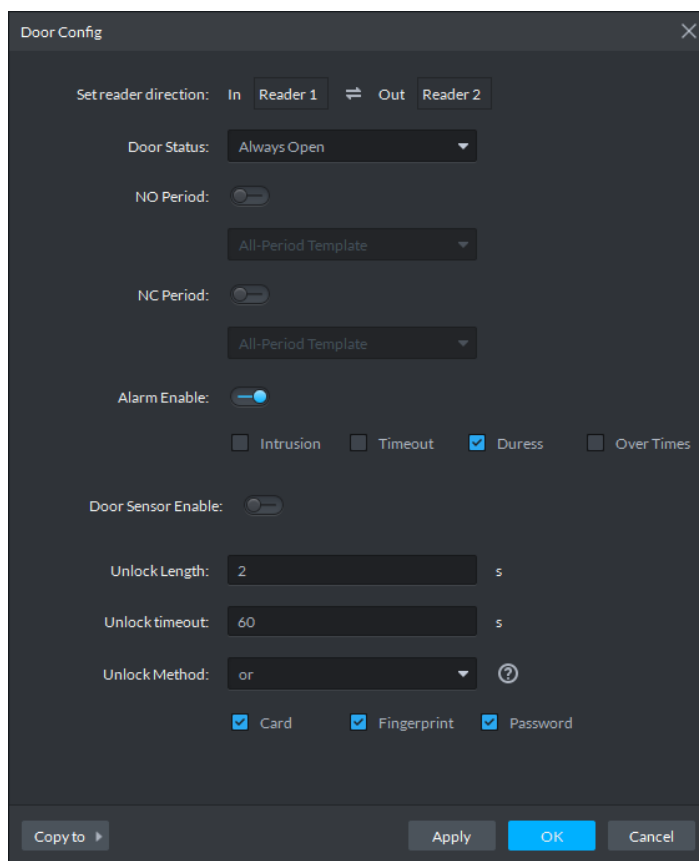
Step 2 Click .

Figure 4-359 Console



Step 3 On the left side of the interface, right-click an access control channel in the device tree. In the popup menu, select **Door Configuration**.

Figure 4-360 Door configuration



Step 4 Configure door information and click **OK**.



The interface might vary depending on different access control devices connected. The actual interfaces shall prevail.

Table 4-63 Parameters

Parameter	Description
Set reader direction	Indicates the in/out reader based on the wiring of ACS.
Door Status	Sets the access control status to Normal, Always Open, or Always Close.
NO Period	If enabled, you can set up a period during which the door is always open.
NC Period	If enabled, you can set up a period during which the door is always close.
Alarm Enable	<ul style="list-style-type: none"> • If the door is not unlocked by configured method, the door contact is split and triggers an intrusion alarm. • Entry with the duress card, duress password, or duress fingerprint triggers a duress alarm. • Unlock duration timeout triggers a timeout alarm. • Swiping an illegal card for more than five times triggers a malicious alarm.
Door Sensor Enable	Enables the door sensor. The intrusion alarm and timeout alarm take effect only when door sensor is enabled.
Unlock Length	Sets up the duration of door unlocking. The door is automatically locked when the duration is over.
Unlock timeout	Unlock duration exceeding the Unlock timeout triggers a timeout alarm.
Unlock Method	You can use any one of the methods, card, fingerprint, face, and password, or any of their combinations to unlock the door.
Inter-door Lock	Indicates whether to enable Inter-door Lock.
Malicious Alarm	Swiping an unauthorized card for five times continuously within 50s triggers a malicious alarm. In the next 50s, every swipe of the card triggers a same alarm.

4.20.3.4 Configuring Advanced Functions

4.20.3.4.1 First Card Unlock

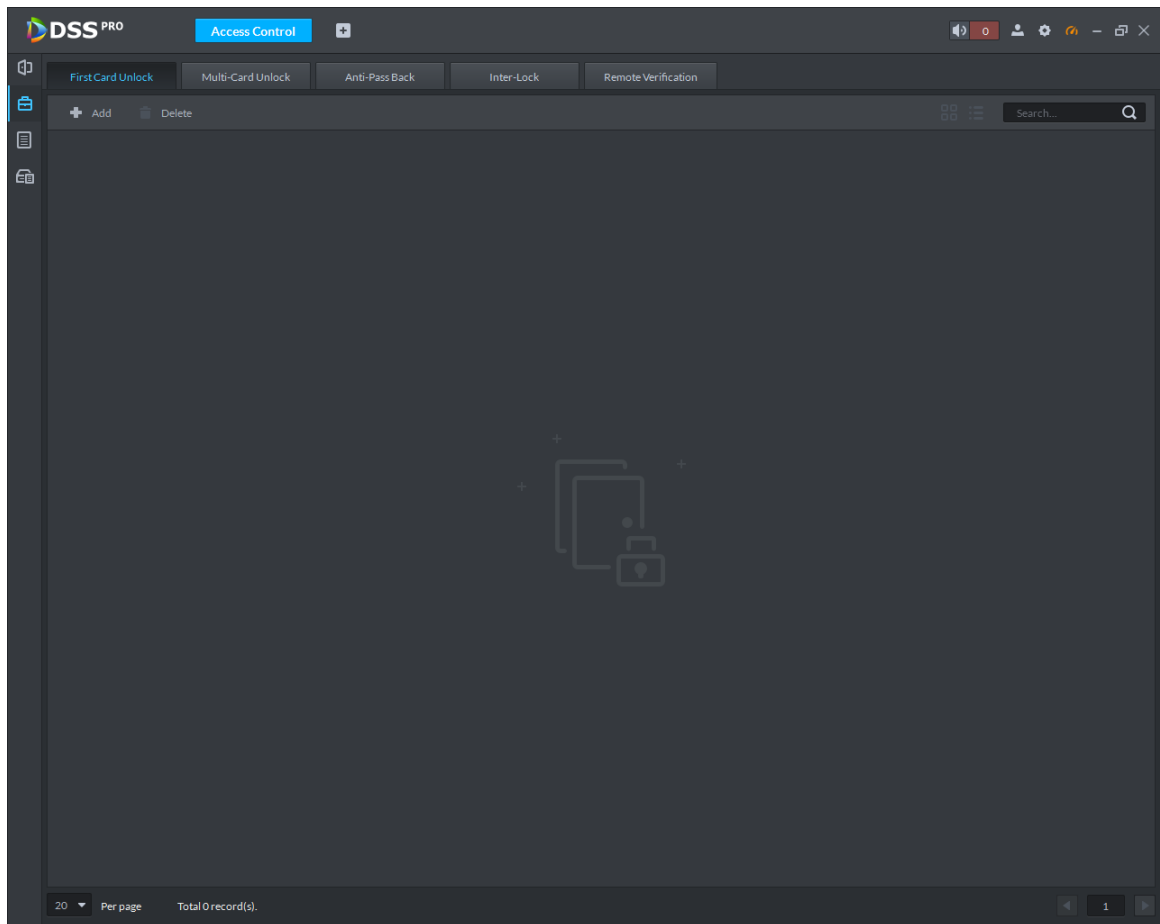
Only after the specified first-card user swipes the card every day can other users unlock the door with their cards. You can set up multiple first cards. Only after any one of the users swipes the first card can other users without first cards unlock the door with their cards.



For a person to be issued with the first card unlock permission, you need to select **General** in the **Property** drop-down list when adding this person.

Step 1 On the **Access Control** interface, click .

Figure 4-361 Advanced Function



Step 2 Click the **First Card Unlock** tab.

Step 3 Click **Add**.

Figure 4-362 First card unlock configuration

First Card Unlock Configuration

Door: Time Template: All-Period Template

Status: Normal

User List

Root Search...

ID	Name
<input type="checkbox"/>	1
<input type="checkbox"/>	4 ic4
<input type="checkbox"/>	1010 dd xx
<input type="checkbox"/>	1011 dd xx
<input type="checkbox"/>	1012 dd xx
<input type="checkbox"/>	1013 dd xx
<input type="checkbox"/>	1014 dd xx
<input type="checkbox"/>	1015 dd xx
<input type="checkbox"/>	1016 dd xx

Selected(0)

ID	Name	Department	Operation
----	------	------------	-----------

OK Cancel

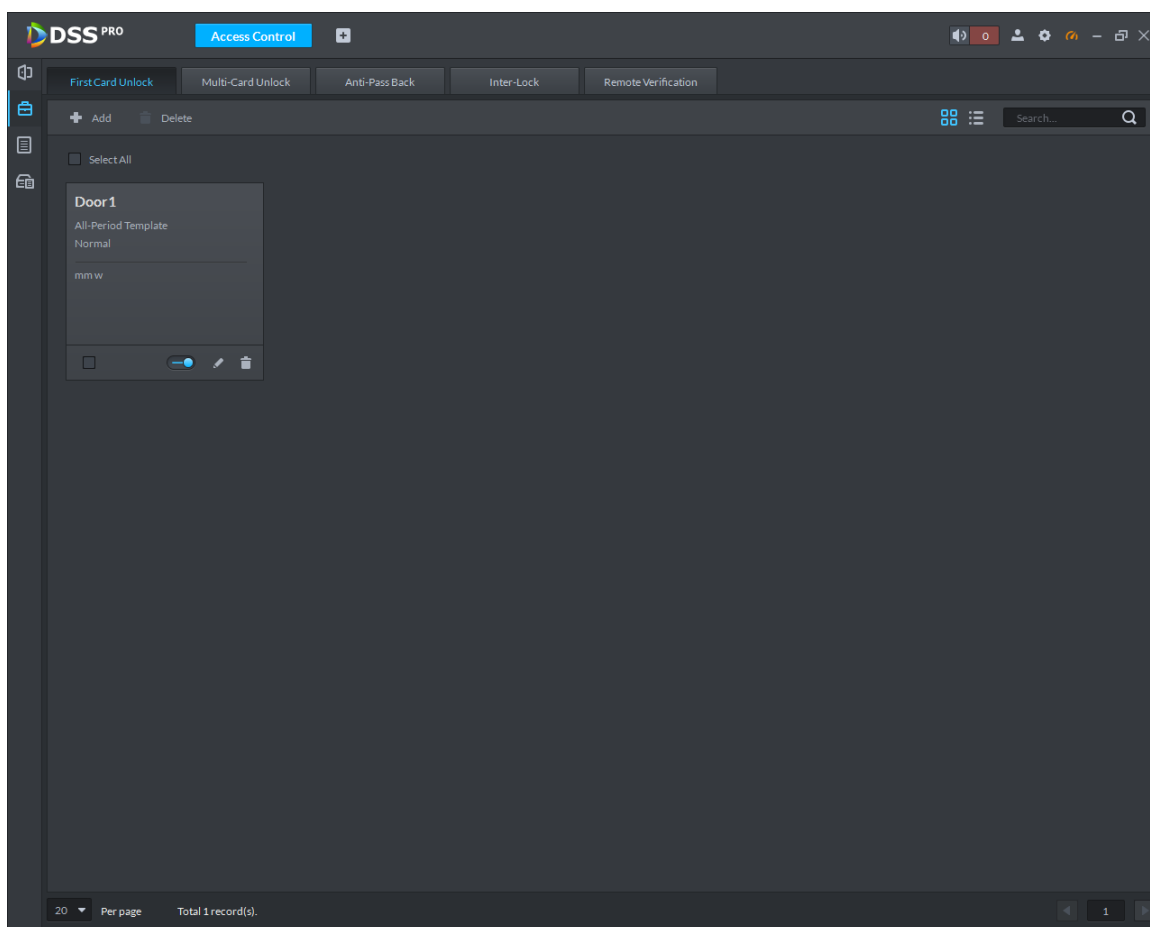
Step 4 Configure the **First Card Unlock** parameters and click **OK**.

First Card Unlock is enabled by default.

Table 4-64 Parameters

Parameter	Description
Door	You can select the target access control channel to configure the first card unlock.
Time Template	First Card Unlock is valid in the time period of the selected time template.
Status	After First Card Unlock is enabled, the door is in either the Normal mode or Always Open mode.
User	You can select the user to hold the first card. Supports selecting a number of users to hold first cards. Any one of them swiping the first card means first card unlock is done.

Figure 4-363 First card unlock information



Step 5 Click .

The icon changing into  indicates **First Card Unlock** is enabled.

4.20.3.4.2 Multi-Card Unlock

In this mode, one or multiple groups of users have to swipe cards for an access control channel in an established sequence to unlock the door.



- One group can have up to 50 users, and one person can only belong to one group.
- With Multi-Card Unlock enabled for an access control channel, there can be up to four groups of users being on site at the same time for verification. The total number of users can be 50 at most, with up to 5 valid users.
- First Card Unlock has higher priority than Multi-Card Unlock, which means if the two rules are both enabled the system performs First Card Unlock first.
- It is not advised to add people with First Card Unlock permission to the Multi-Card Unlock group.
- Do not set the VIP or Patrol type for people in the person group. For details, see "4.19 Personnel Management."

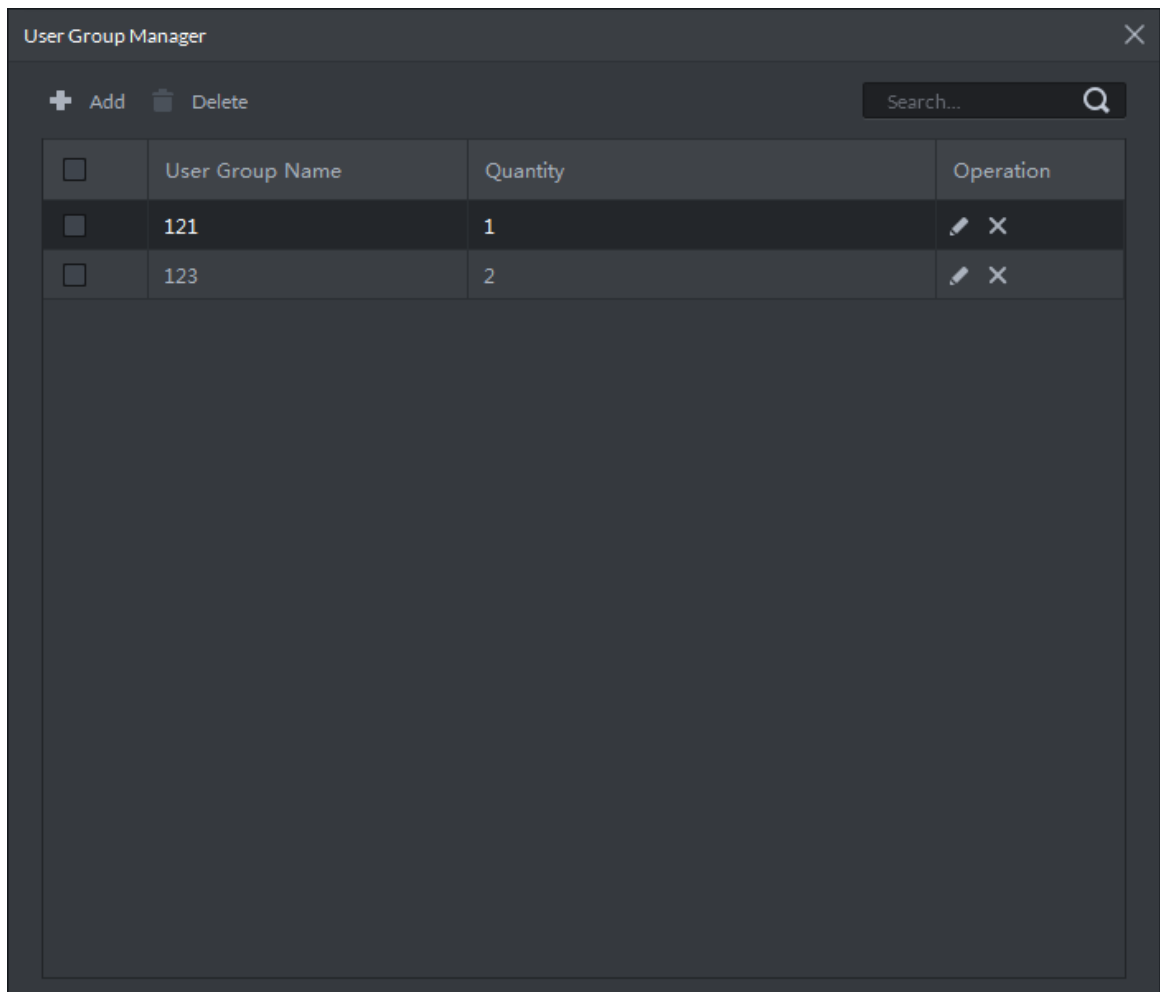
Step 1 On the **Access Control** interface, click .

Step 2 Click the **Multi-Card Unlock** tab.

Step 3 Add user group.

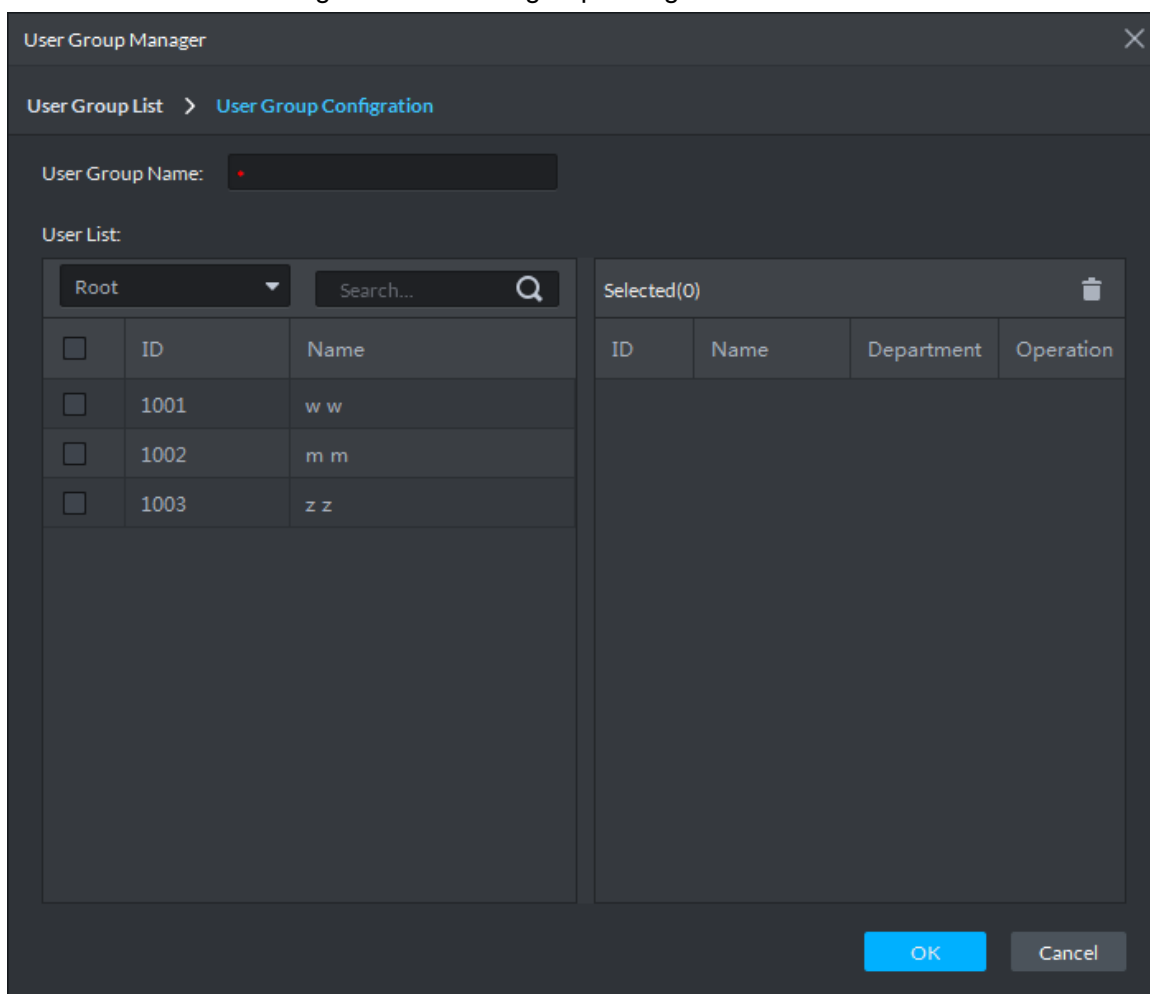
- 1) Click Person Group.


Figure 4-364 User group manager



- 2) Click **Add**.

Figure 4-365 User group configuration

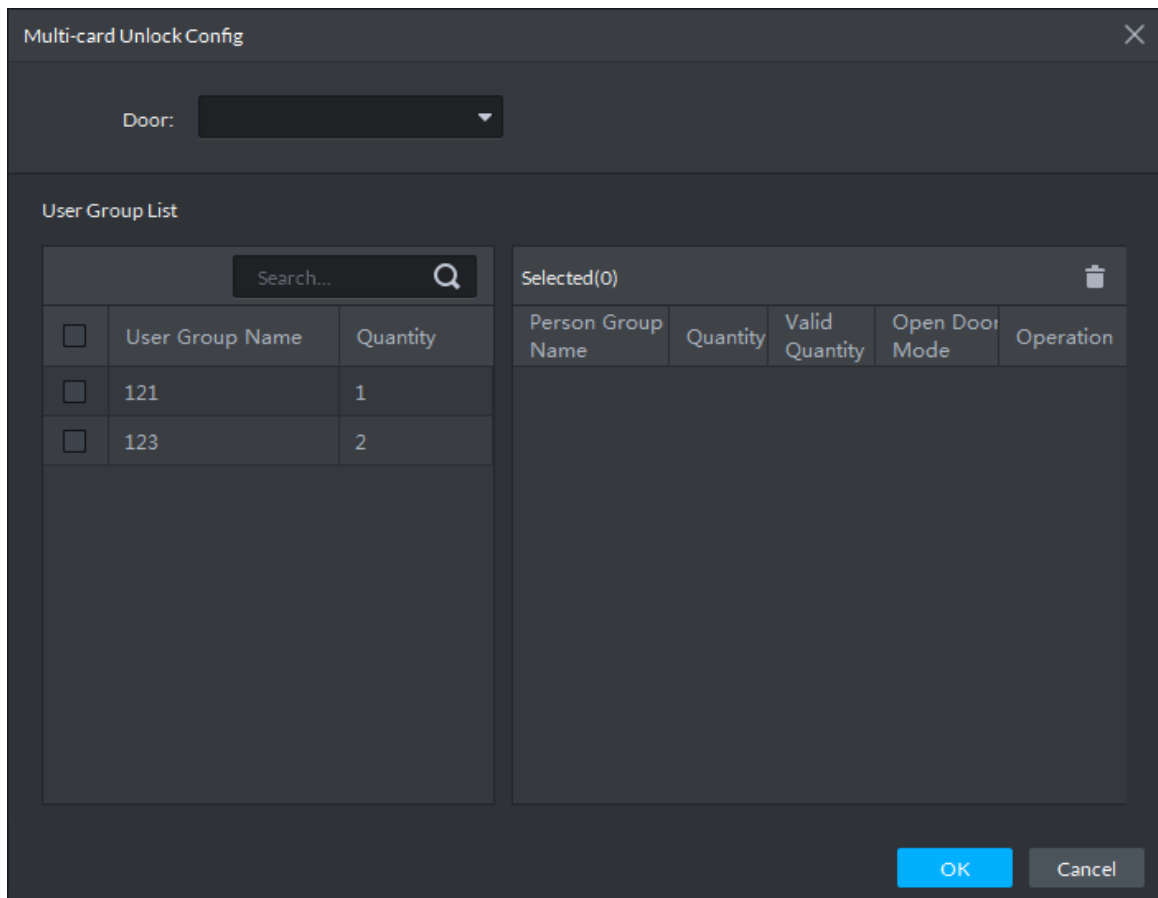


- 3) Set up **User Group Name**. Select users from **User List** and click **OK**. You can select up to 64 users.
- 4) Click  in the upper right corner of the **User Group Manager** interface.

Step 4 Configure Multi-Card Unlock.

- 1) Click **Add**.

Figure 4-366 Multi-card unlock configuration



Multi-card Unlock Config

Door:

User Group List

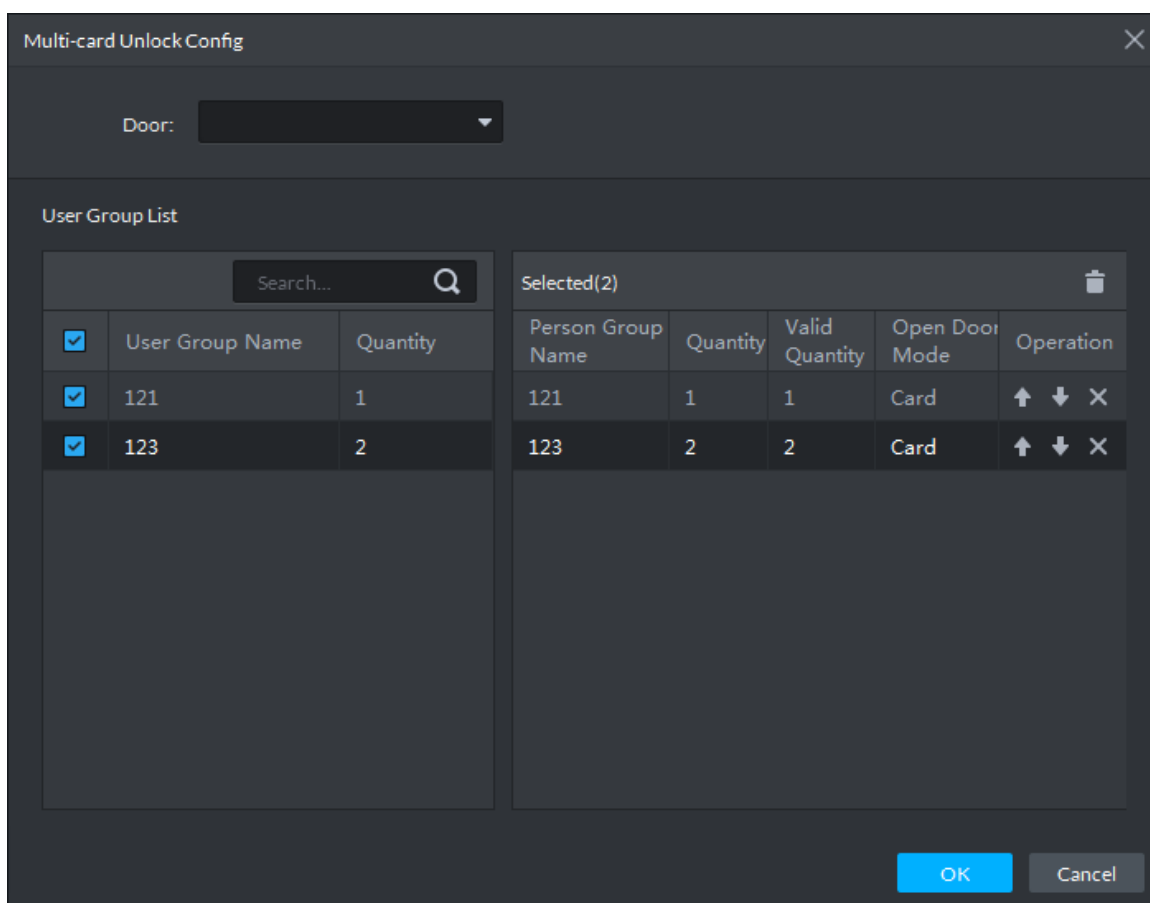
<input type="checkbox"/>	User Group Name	Quantity
<input type="checkbox"/>	121	1
<input type="checkbox"/>	123	2

Selected(0)				
Person Group Name	Quantity	Valid Quantity	Open Door Mode	Operation

OK Cancel

- 2) Select the door to set Multi-Card Unlock.
- 3) Select the user group. You can select up to four groups.

Figure 4-367 User group information



- 4) Fill in the **Valid Quantity** for each group to be on site and the **Open Door Mode**.

Click  or  to adjust the group sequence to unlock the door.

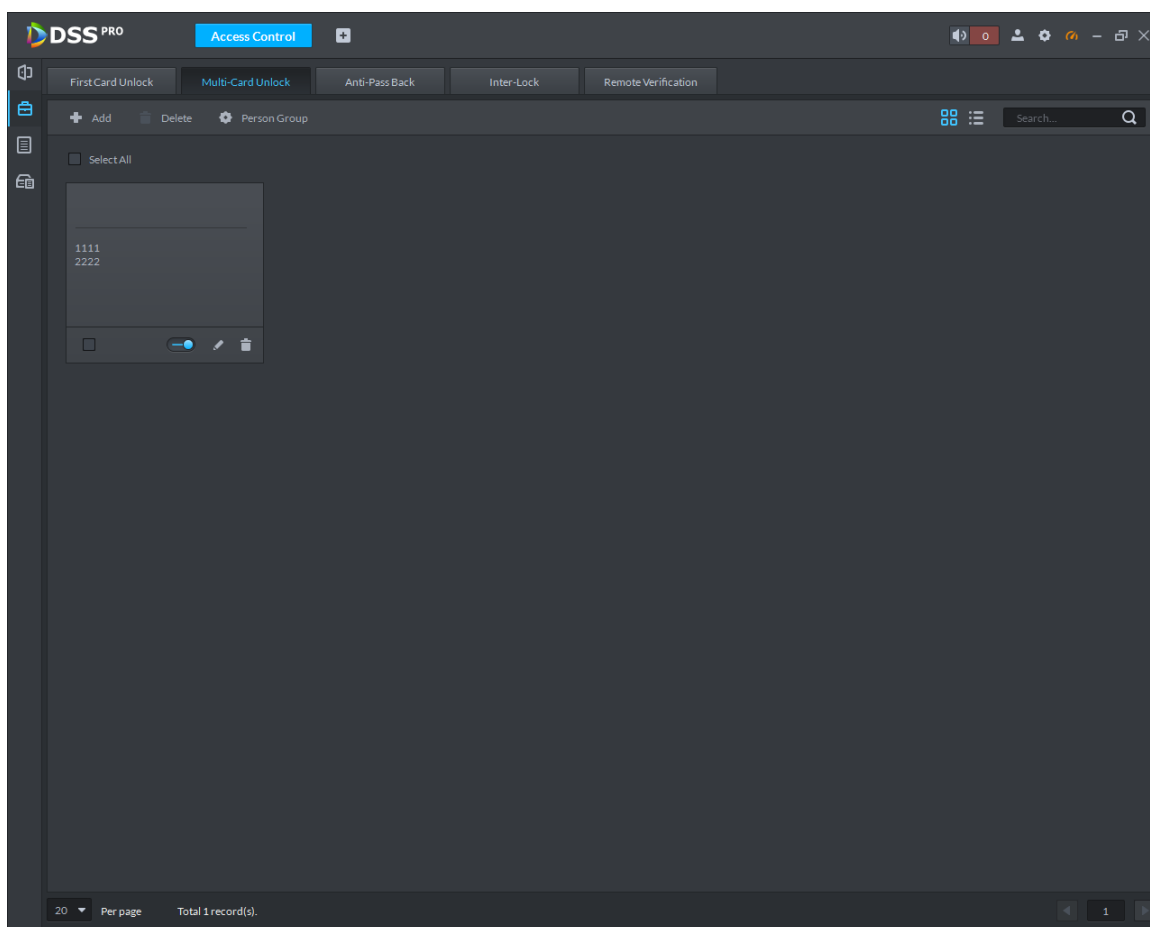
The valid quantity refers to the number of users in each group that must be on site to swipe their cards.




Up to five valid users are allowed.

- 5) Click **OK**.

Figure 4-368 Multi-card unlock details



Step 5 Click .

The icon changing into  indicates Multi-Card Unlock is enabled.

4.20.3.4.3 Anti-passback

The Anti-passback feature requires a person to exit from the specific doors. For the same person, an entry record must pair with an exit record. If someone has entered by tailing someone else, which means there is no entry record, this person cannot unlock the door for exit.

Step 1 On the **Access Control** interface, click .

Step 2 Click the **Anti-passback** tab.

Step 3 Click **Add**.

Figure 4-369 Anti-passback configuration

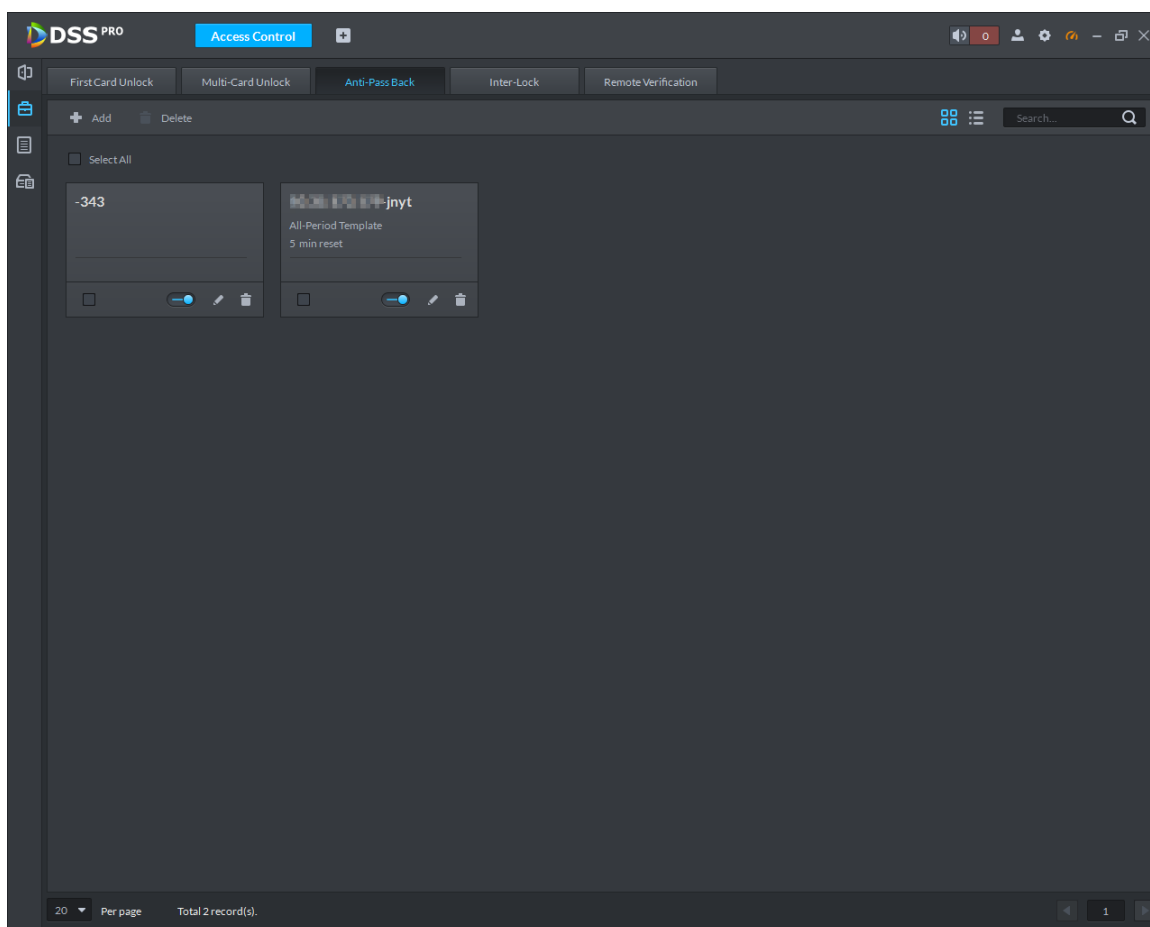
Step 4 Configure the anti-passback parameters and click **Next Step**.

Table 4-65 User selection information description

Parameter	Description	
Device	You can select the device to configure the anti-passback rules.	
Anti-passback name	You can customize the name of an anti-passback rule.	
Reset Time(min)	The access card becomes invalid if an anti-passback rule is violated. The reset time is the invalidity duration.	<p>When the selected device is a multi-door controller, you must set up these parameters.</p>
Time Template	You can select the time periods to implement the anti-passback rules.	
Remark	Description information.	
Group X	The group sequence here is the sequence for swiping cards. You can add up to 16 readers for each group.	
X is a number.	Each group can swipe cards on any of the readers.	

Step 5 Select people, and then click **OK**.

Figure 4-370 Anti-passback information



Step 6 (Optional) Click .

The icon  indicates that Anti-passback is enabled.

4.20.3.4.4 Inter-door Lock

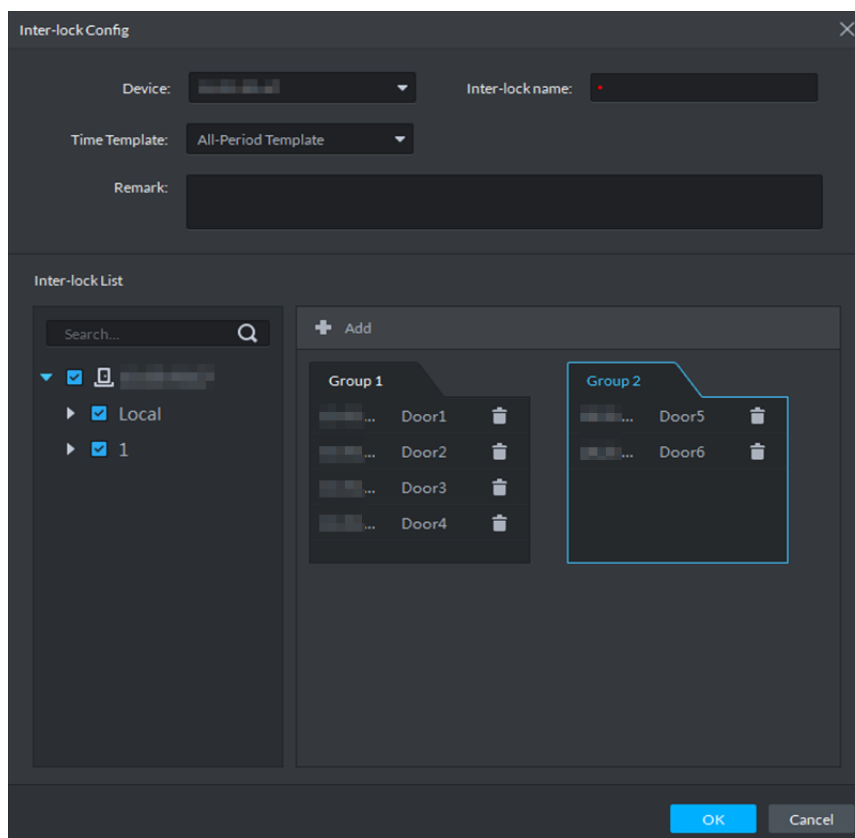
A regular access controller employs inter-lock within the group. To open one of the access control channels (under normal access control), the other corresponding access control channels must be closed; otherwise the door cannot be unlocked. The A&C Central Controller employs inter-group inter-lock, where the access control channels are independent of the inter-lock and can all be opened. However, whenever an access control channel in a group is opened, no channels of other groups can be opened. The configuration steps in this chapter are for an A&C Central Controller.

Step 1 On the **Access Control** interface, click .

Step 2 Click the **Inter-Lock** tab.

Step 3 Click **Add**.

Figure 4-371 Inter-door lock configuration

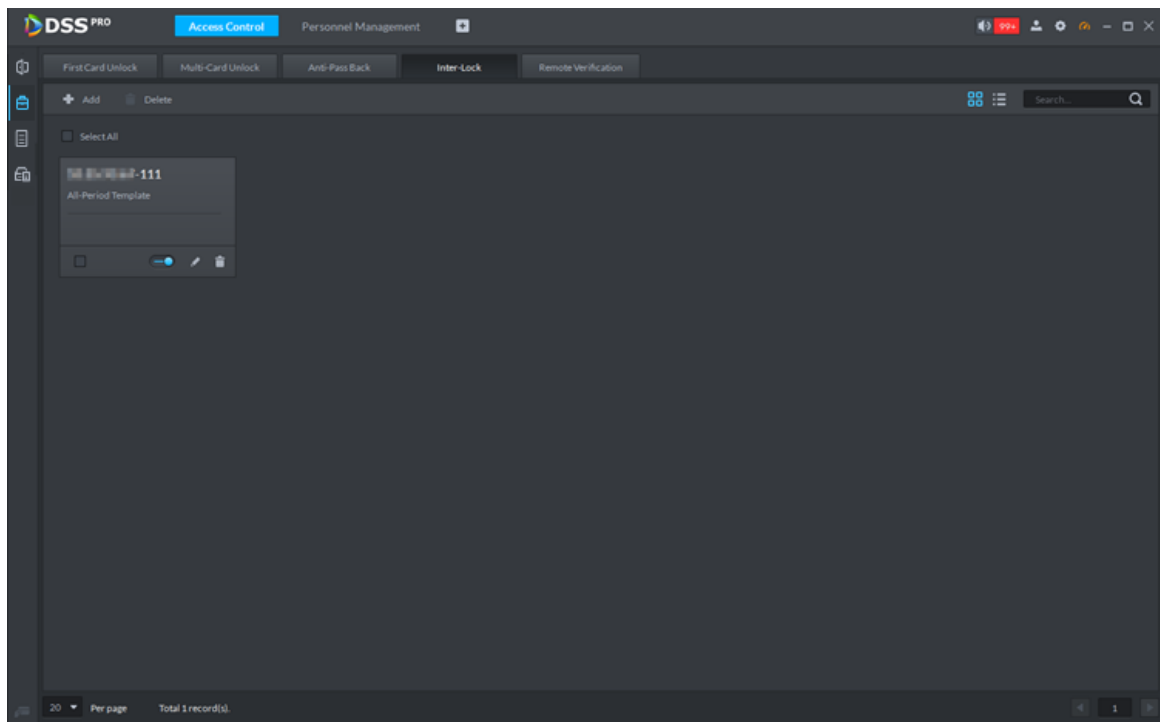


Step 4 Configure inter-lock parameters and click **OK**.


Table 4-66 Parameters

Parameter	Description	
Device	You can select the device to set up inter-lock.	
Inter-lock name	You can customize the name of the inter-lock rule.	
Time Template	You can select the time period to implement inter-lock.	When the selected device is a multi-door controller, you must set up these parameters.
Remark	Description information.	
Group X X is a number.	You can set up inter-lock across different door groups. If a door in Group 1 is opened, no doors can be opened in Group 2 until all doors in Group 1 are closed. Supports up to 16 door groups, with up to 16 doors in each group.	

Figure 4-372 Inter-door lock information



Step 5 Click .

The icon  indicates the function is enabled.

4.20.3.4.5 Remote Verification

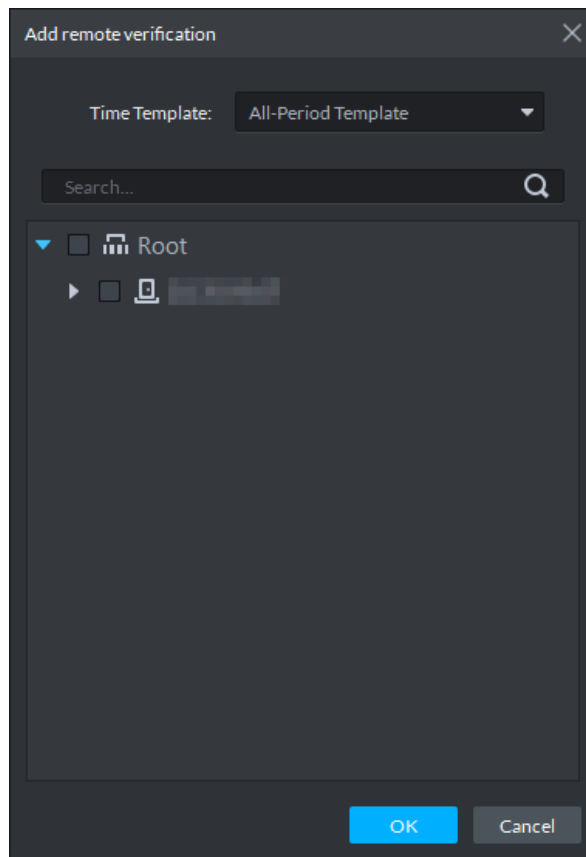
For devices with remote verification, when users unlock the doors with card, fingerprint, or password in the specified time period, it must be confirmed on the platform client before the access controller can be opened.

Step 1 On the **Access Control** interface, click .

Step 2 Click the Remote Verification tab.

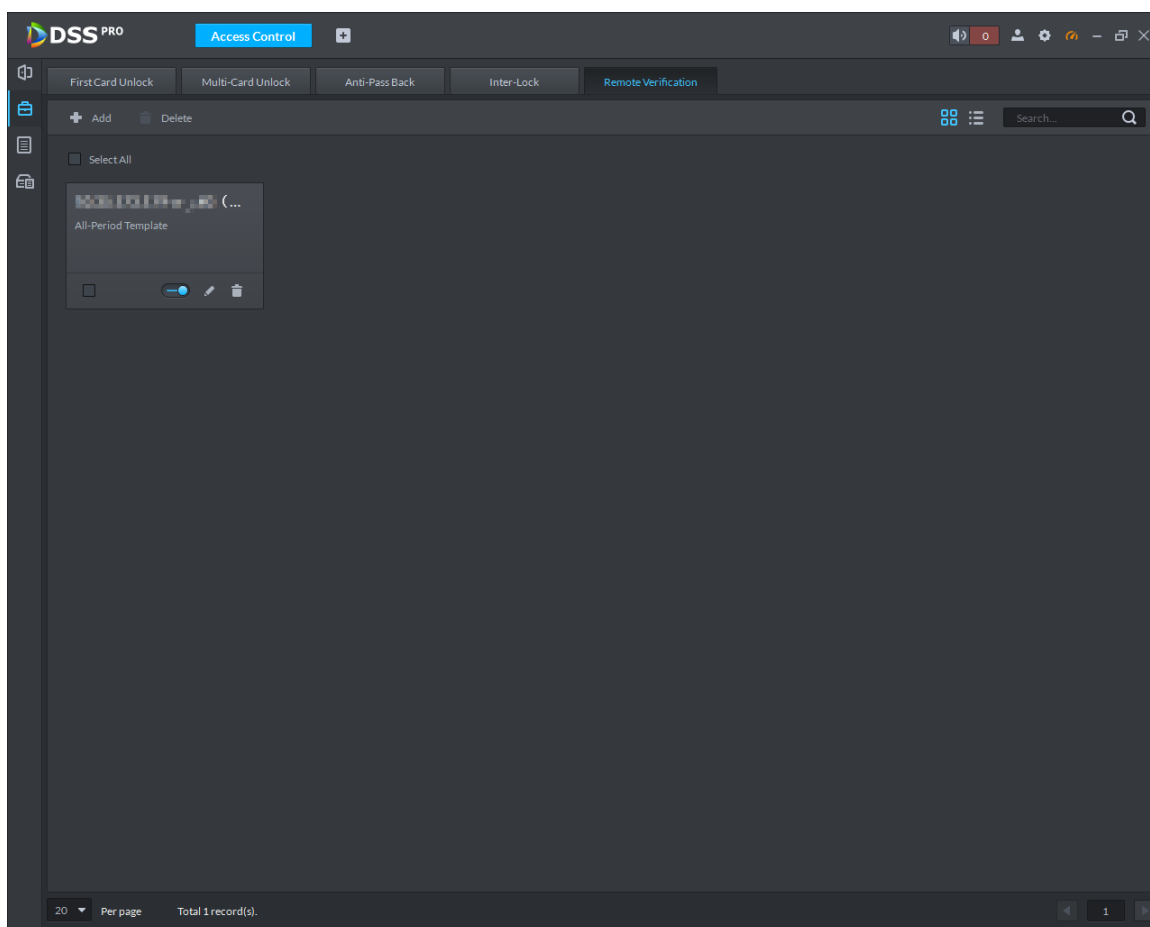
Step 3 Click **Add**.

Figure 4-373 Add remote verification



Step 4 Select **Time Template** and access control channel, and click **OK**.

Figure 4-374 Remote verification information



Step 5 Click .

The icon  indicates **Remote Verification** is enabled.

After the setup, door unlocking by card, fingerprint, or password that takes place in the corresponding access control channel triggers a pop-up on the client.


You can choose to unlock the door or ignore it by clicking the corresponding button, and the popup automatically disappears.

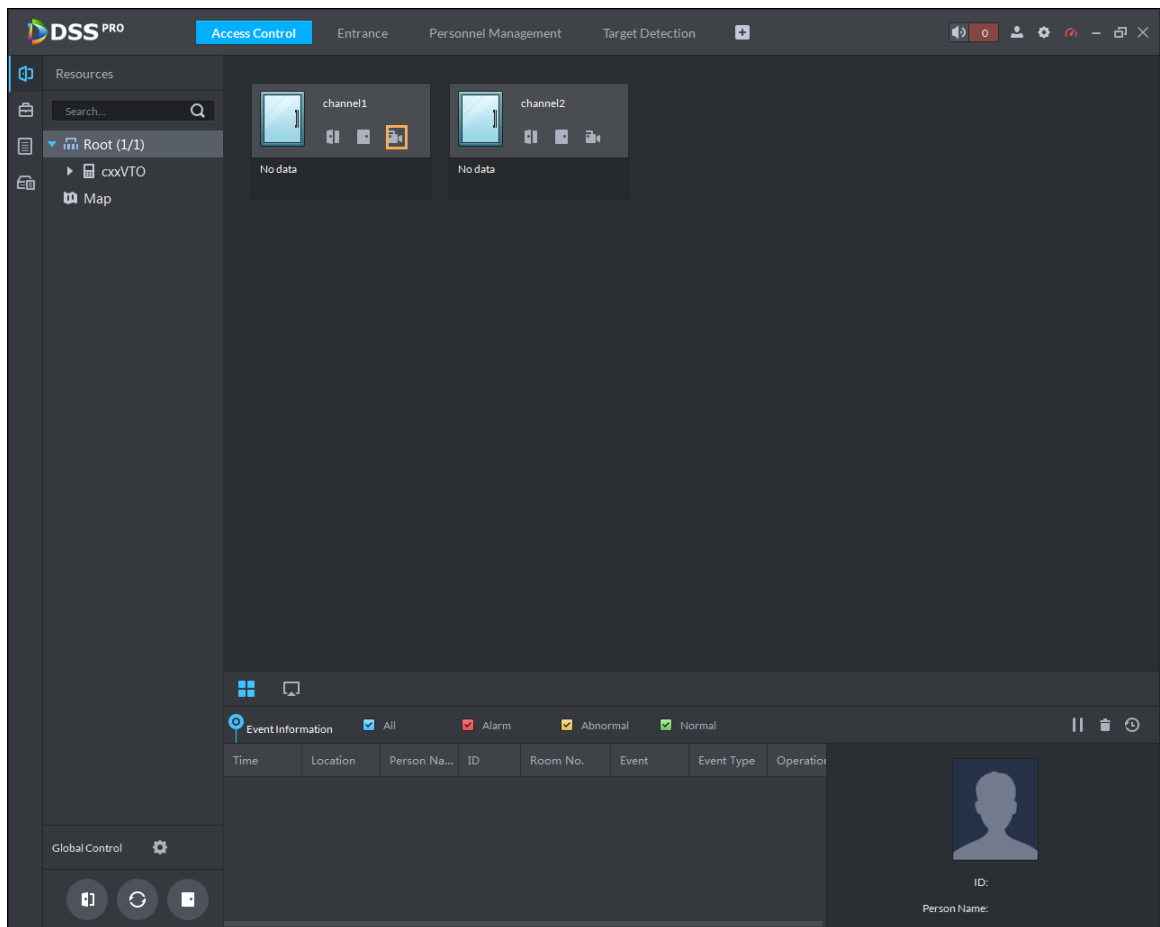
4.20.4 Access Control Applications

4.20.4.1 Viewing Videos

If you have already bound a video channel to the access control channel, you can view the real-time videos of the channels on the console. To bind video channels, see "3.4.6 Binding Resource."

Log in to the Control Client, select **Access Control > Console**, and then view videos in the following ways.

- On the right side of the console interface, click  in the access control channel list. The system displays videos in real time.




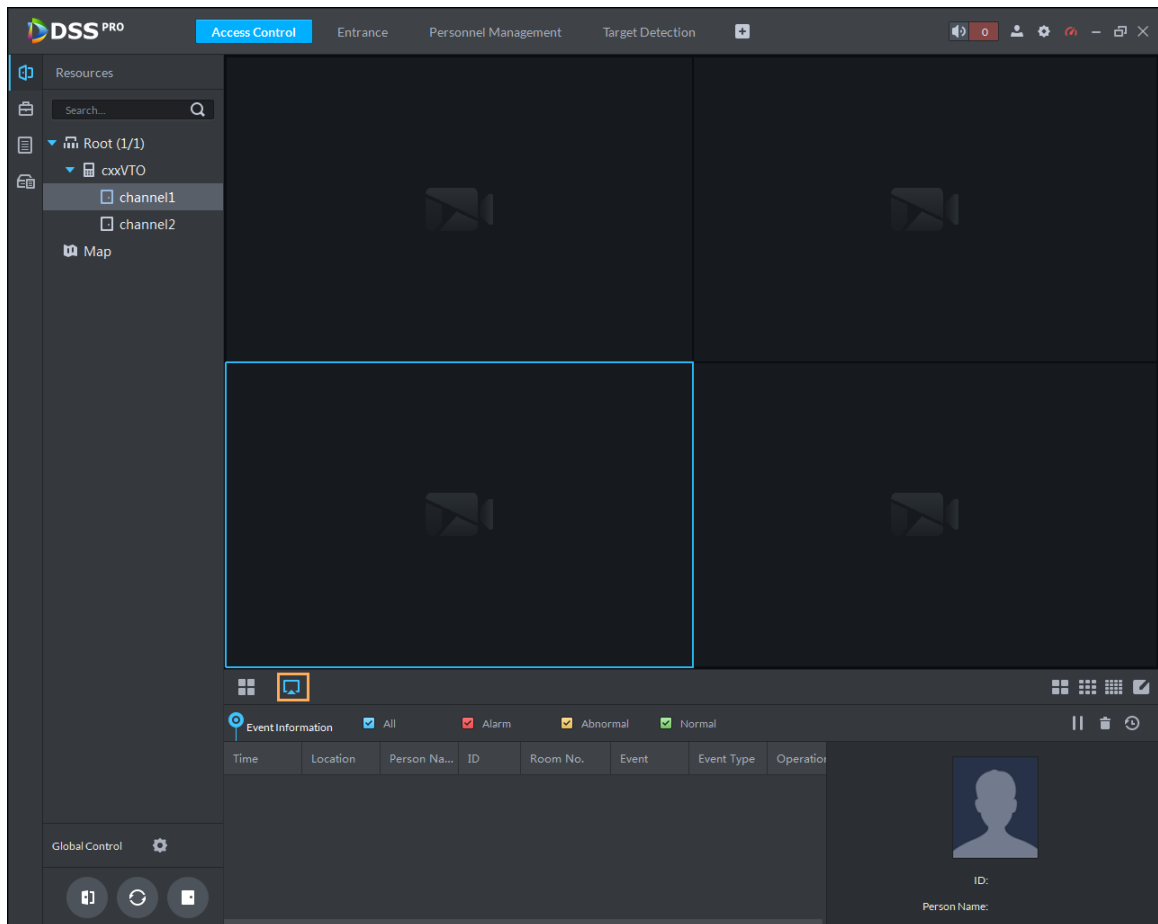
- Click  on the console interface. The system displays the video interface. Drag the access control channel on the left side of the screen to the live view interface on the right side. The system displays videos in real time.

Figure 4-375 Real-time video



4.20.4.2 Unlocking Door

In addition to Always Open or linked unlock in specified periods, the console also supports unlocking by manually controlling the access control channel. After unlock, the door automatically locks up after a specified period (5 s by default, and 10 s in this example) set up in Door Config.

You can unlock the door in the following ways:


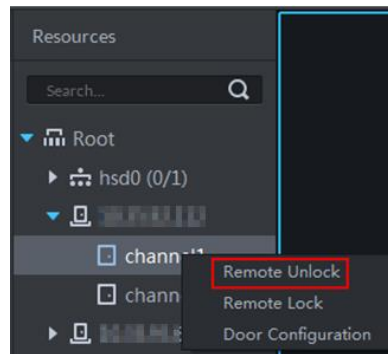
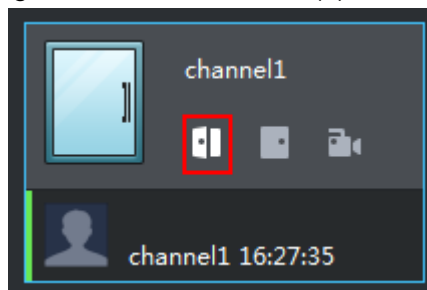
- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Unlock** in the popup menu. After unlocking, the door status in the access control channel list on the right side of the interface changes to open, as .

Figure 4-376 Unlock door (1)



- Click  on the door channel interface to unlock the door.

Figure 4-377 Unlock door (2)




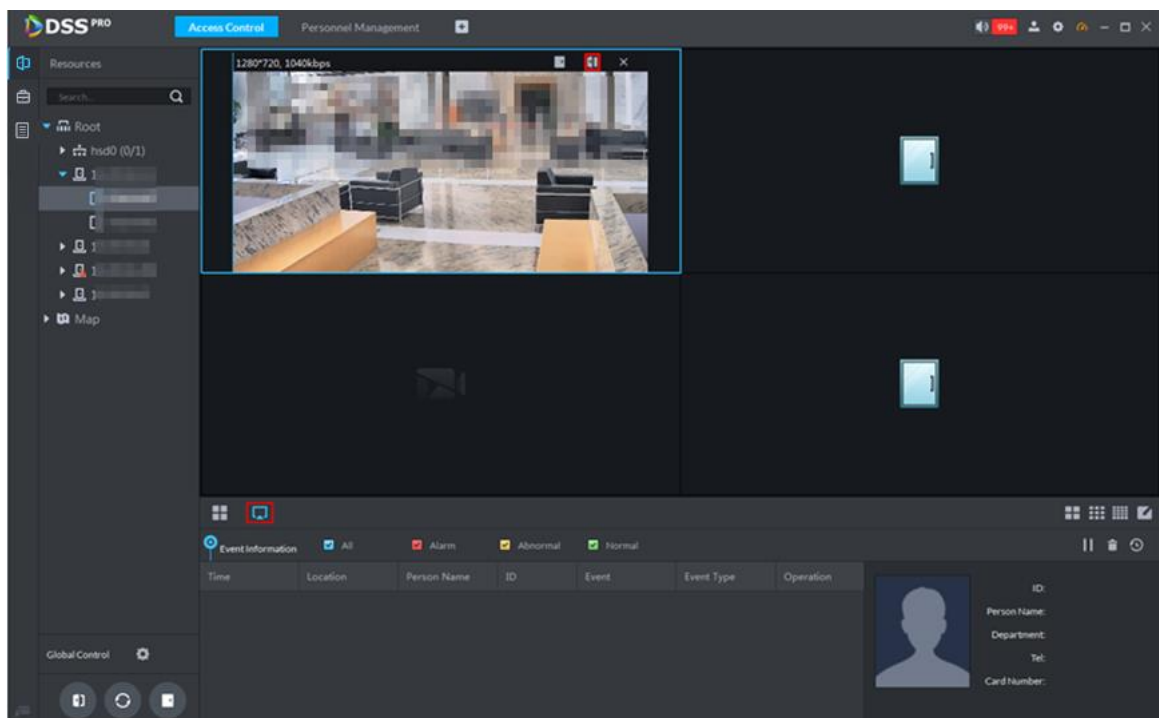
- When viewing videos bound to the channel, click  on the video interface to unlock the door.

Figure 4-378 Unlock door (3)



- Temporary Always Open of multiple doors
Select door channels through global control, and then you can set the door to be Always Open.

Step 1 Click  on the lower left of the console interface of the **Access Control** module.

Step 2 Select an access control channel to be set to Always Open via global control, and click **OK**.


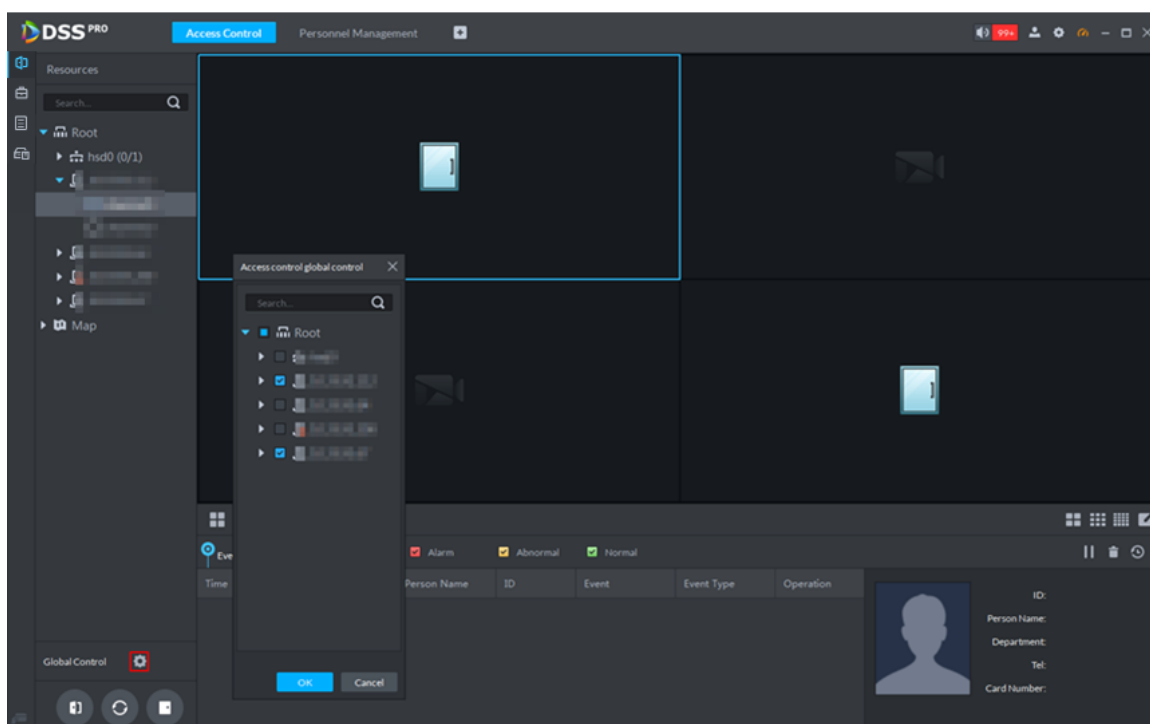
Step 3 Click  on the lower-left corner of the interface.


Figure 4-379 Global control



Step 4 Enter current user's password, and click **OK**.

All the doors of the selected access control channels are set to Always Open.



Click  to restore the door from the Always Open or Always Closed status before the scheduled door control or face-recognition access control takes effect.

4.20.4.3 Locking Door

In addition to Always Close or linked lock in specified periods, the console also supports locking by manually controlling the access control channel. You can lock the door in the following ways:

- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Lock** in the popup menu. After locking, the door status in the access


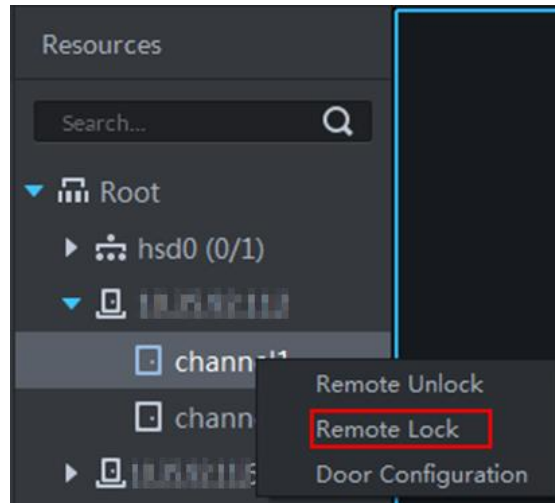
control channel list on the right side of the interface changes to closed, as .

Figure 4-380 Lock door (1)




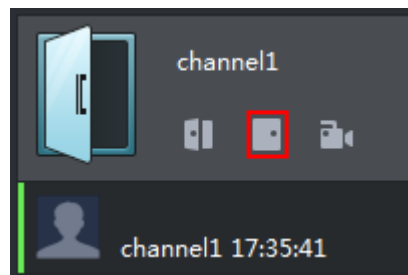
- Click  on the door channel interface to lock the door.

Figure 4-381 Lock door (2)




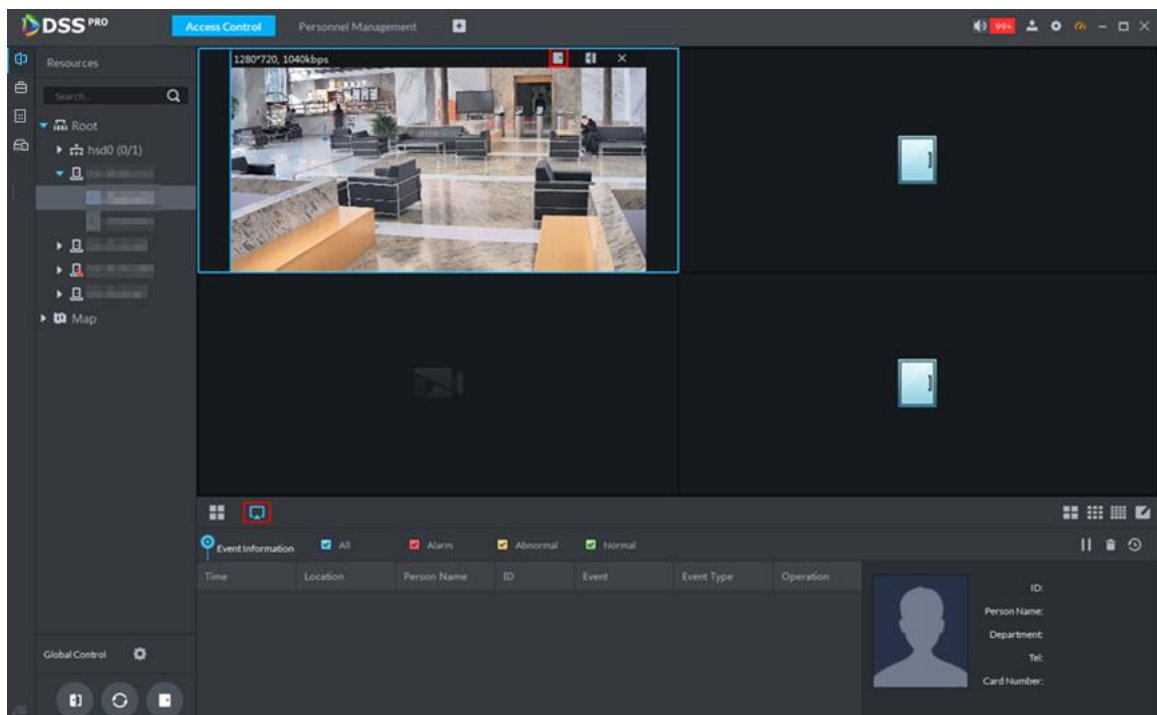
- When viewing videos bound to the channel, click  on the video screen to lock the door.

Figure 4-382 Lock door (3)



- Temporary Always Close of multiple doors
Select a door channel through global control and you can set the door to be Always Close.

Step 1 Click  on the bottom left of the console interface.

Step 2 Select an access control channel to be set to Always Close via global control, and click **OK**.


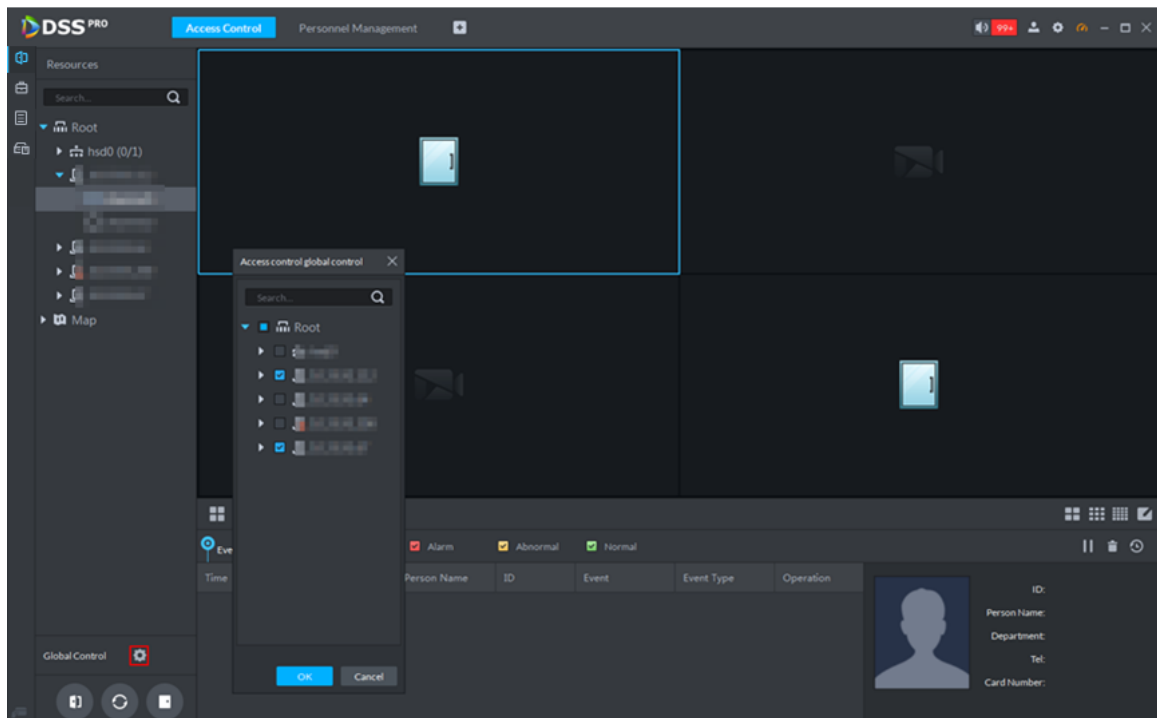
Step 3 Click  at lower left of the interface.


Figure 4-383 Global control



Step 4 Enter current user's password, and click **OK**.

All the doors of the selected access control channels are set to Always Close.




Click  to restore the door from the Always Open or Always Closed status before the scheduled door control or face-recognition access control takes effect.

4.20.4.4 Viewing Event Details

View details of the events reported on door locking and unlocking, including: Event Info, Live View, Snapshot, and Recording.



- Live view is only available when a video channel is bound to the access control channel. To bind video channels, see "3.4.6 Binding Resources."
- To see snapshots and videos of access control, you need to configure video linkage action for the access control channels. For details, see "4.4 Event and Alarm."

Step 1 In the event list below the console interface, click  next to the event records.



For a face recognition controller, the face snapshots will be displayed in the records; for other controllers, the records display people profiles.

Figure 4-384 Event information

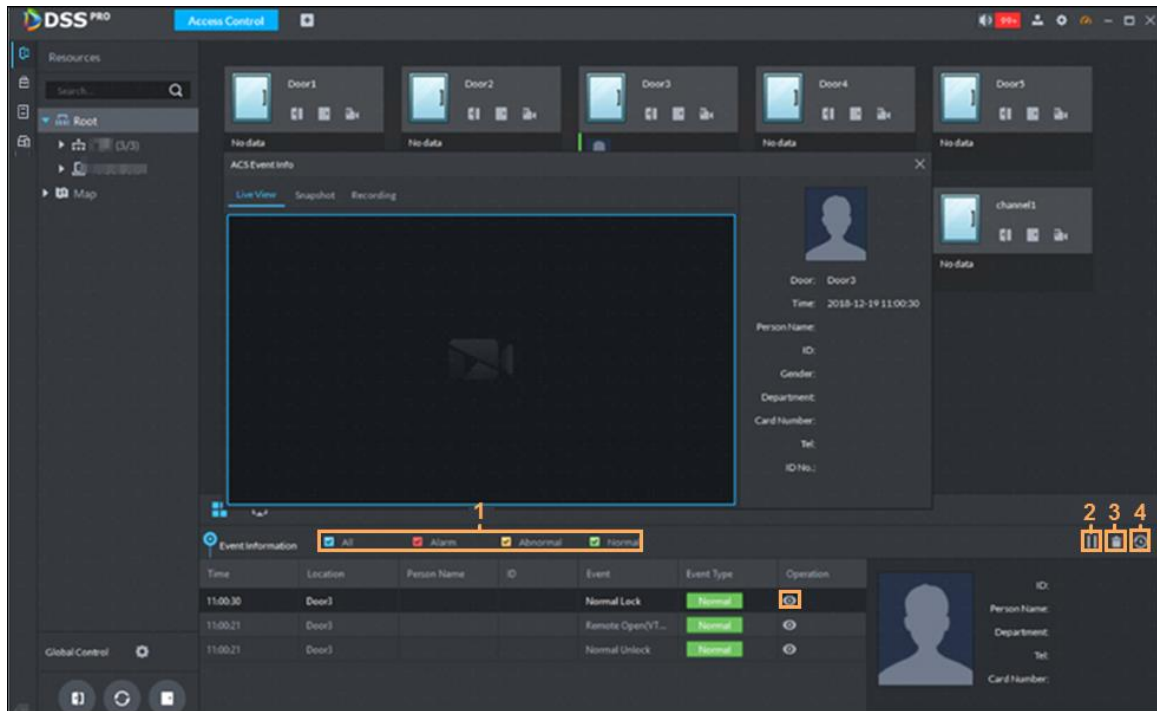


Table 4-67 More operations

No.	Description
1	You can choose to view the events of certain event types. For instance, if you select Normal , the list only displays normal events.
2	<ul style="list-style-type: none"> Click to stop displaying reported event information. In this case, the interface no longer displays the reported new events. After clicking, the button changes to . Click to start refreshing reported event information. The interface does not display events during the stopping period. After clicking, the button changes to .
3	Clear the events from the current event list without removing them from the log.
4	Click to view access control records.

Step 2 Click the corresponding tab to view the live view, snapshots, and video recordings of the linked video channel.

4.20.4.5 Viewing Access Control Records

You can view access control records. There are two types of records:

- Online records


The access control records stored on the platform.

- Offline records

The access control records stored in the device when it was disconnected from the platform. After the device gets reconnected to the platform, you can retrieve the records generated during the disconnection.

4.20.4.5.1 Online Records

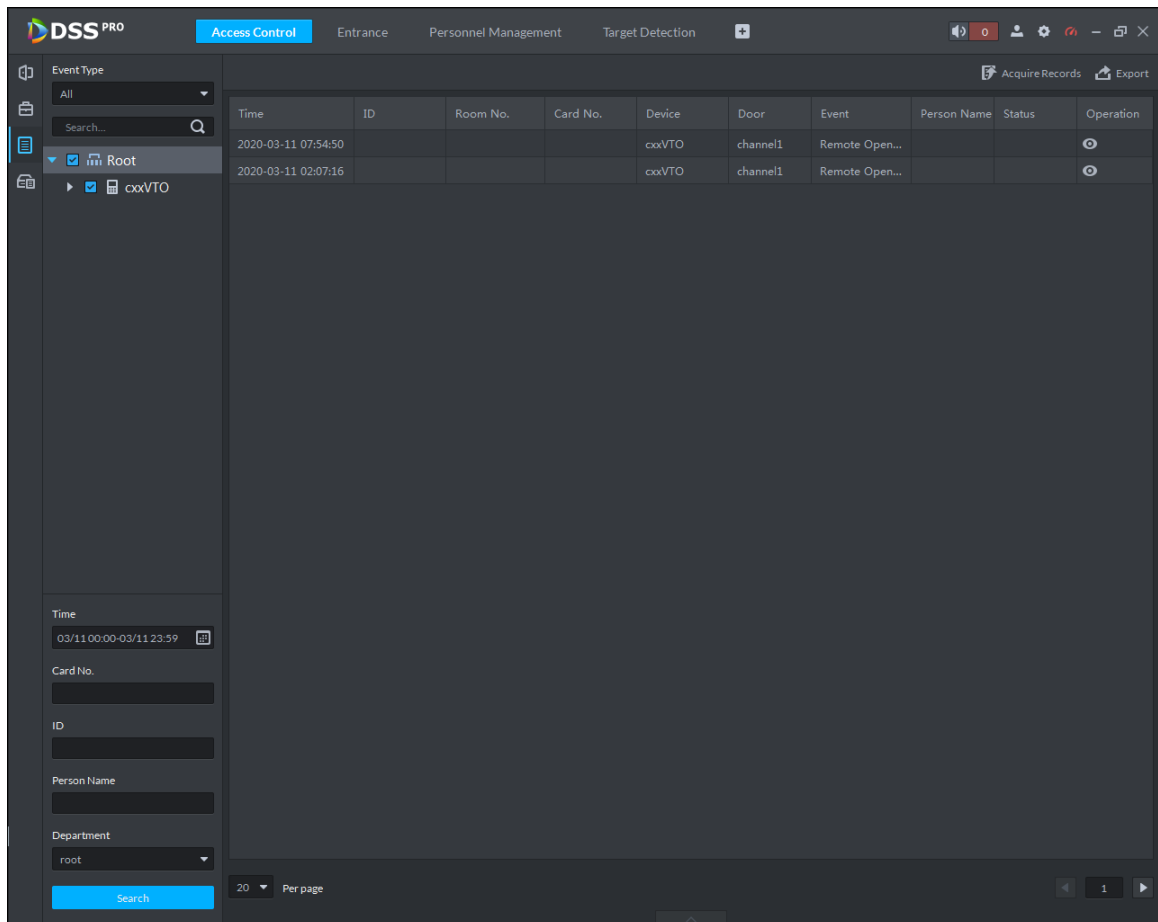
Step 1 Log in to the Control Client, and then select **Access Control**.

Step 2 Click .

Step 3 Set search conditions such as event type, channel, and time, and then click **Search**.

To export the searches, click **Export** at the upper-right corner of the interface. The required password is the one for logging in to the platform.

Figure 4-385 Log search



4.20.4.5.2 Offline Records

Step 1 Log in to the Control Client, and then select **Access Control**.

Step 2 Click .

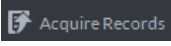
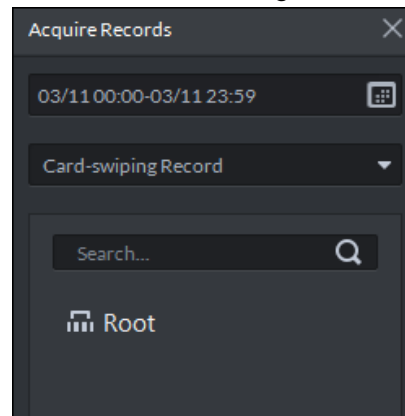

Step 3 Click  at the upper-right corner.

Figure 4-386 Extract records during disconnection



Step 4 Click  to set period.

Step 5 Click  to select a record type.

Step 6 Select a channel.

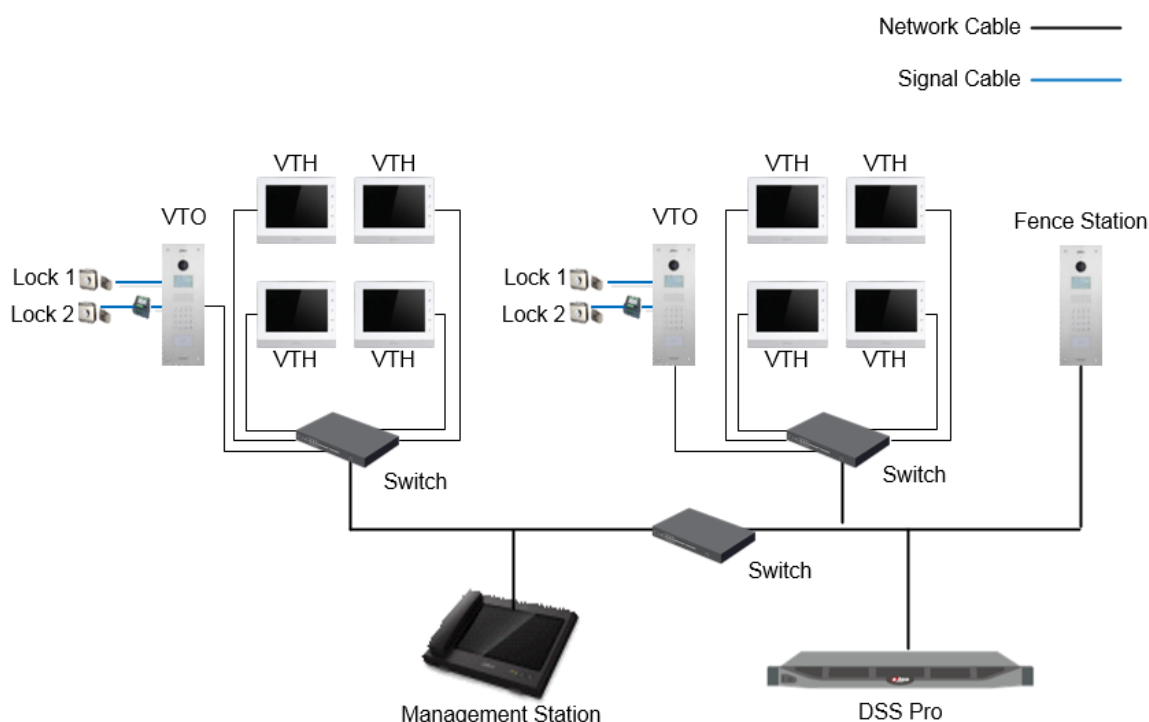
Step 7 Click **OK**.

4.21 Video Intercom

Video intercom plays an important role in modern community management. It enables convenient communication and door control between visitors and residents.

4.21.1 Typical Topology

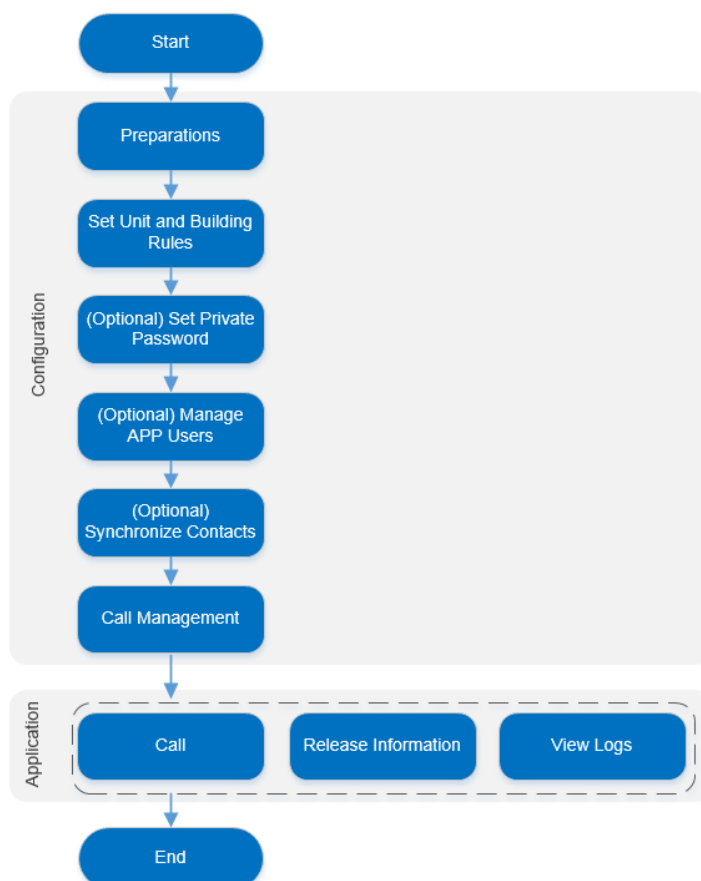
Figure 4-387 Access control typical topology



- VTH (indoor monitor) is installed in home for receiving visitor calls from VTO (door station) or fence station, or security center (VTS or the DSS platform), calling other homes (VTHs) or the security center, viewing videos at the door, and opening door.
- VTO is installed at the building door for the visitor to call homes.
- Locks are mounted on the door for door control.
- Fence station is installed at the gate for the visitor to call the host.
- Management station is deployed in the security center for receiving calls from visitors or residents.
- The platform centrally manages all devices (VTH, VTO, management station and fence station), speaks with the devices, and provides record search.

4.21.2 Business Flow

Figure 4-388 Video intercom business flow



4.21.3 Configuring Video Intercom

4.21.3.1 Preparations

Make sure that the following preparations have been made:

- Access control devices are correctly deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations." When adding video intercom devices on the **Device** interface of Web Manager, select **Video Intercom** for device category.



- ◇ The enable status of unit and building on the VTO must be consistent with that on the platform. Or else you might fail to add VTO. For details, see "4.23.3.2 Configuring Building and Unit."
- ◇ The system creates personnel information automatically when you add VTH. It extracts room number from VTH SIP. This number is used as person ID. You can view and modify personnel information on the interface **Personnel Management** interface.

- ◇ Any configuration modification on the device will not be reported to the platform. You need to go to the device modification interface of Web Manager to manually synchronize the modification.

Figure 4-389 Adding video intercom device

4.21.3.2 Configuring Building/Unit

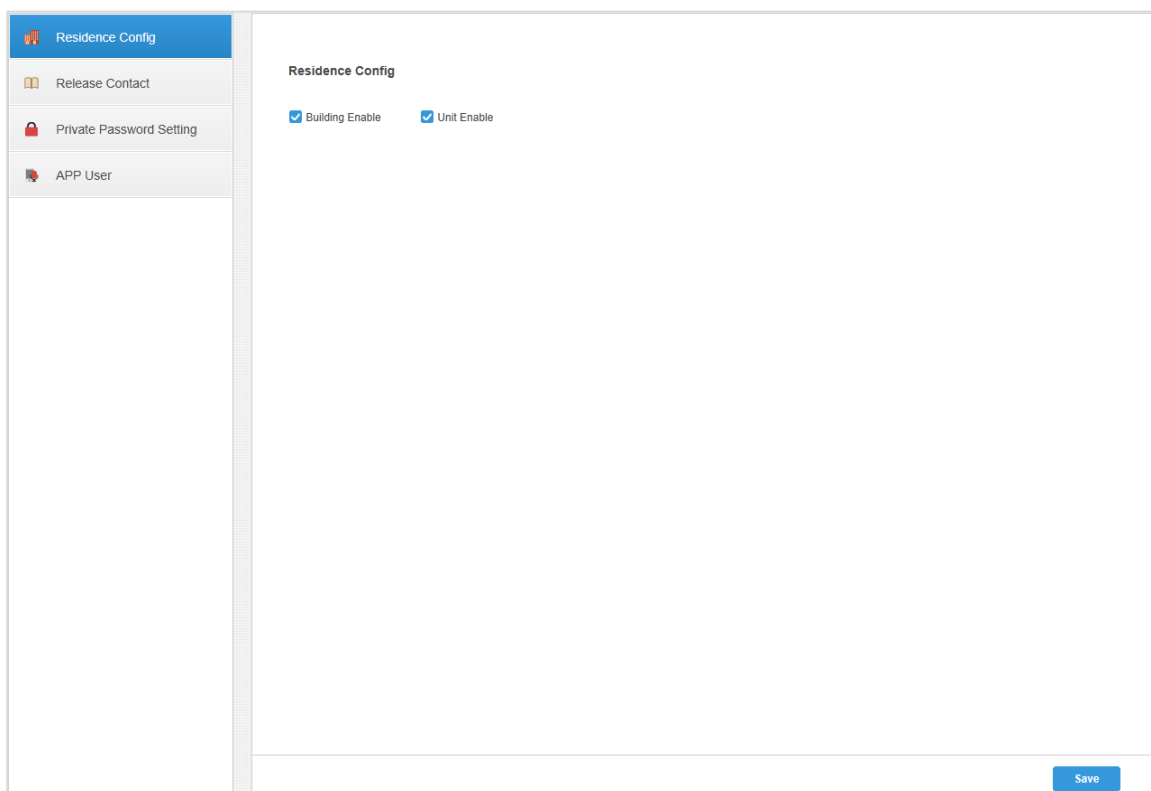
Make sure that the enable status of building and unit is in accordance with the device; otherwise, the device is offline after being added. That also affects the dialing rule. Take room 1001 unit 2 building 1 as an example, the dialing rule is as follows after it is enabled.

- If building is enabled while unit is not, the room number is "1#1001".
- If building is enabled, and unit is enabled as well, the room number is "1#2#1001".
- If building is not enabled, and unit is not enabled either, the room number is "1001".

Step 1 Click on the Web Manager, and then select **Video Intercom Management**

Step 2 Click **Residence Config**.


Figure 4-390 Residence configuration



Step 3 Enable or disable building and unit as required, and then click **Save**.

4.21.3.3 Synchronizing Contacts

Synchronize contacts information to VTO and then you can view contacts on the VTO display screen or WEB interface.

Step 1 Click  on the Web Manager, and then select **Video Intercom Management**.

Step 2 Click **Release Contact**.

Step 3 Select an organization node (VTO), and then click **Release Contact**.

Step 4 Select VTH and click **Save**.


You can view contact on the VTO display screen or WEB interface after releasing is completed.

4.21.3.4 Setting Private Password

Set room door passwords so that the room door can be opened by entering password on the VTO (outdoor station).

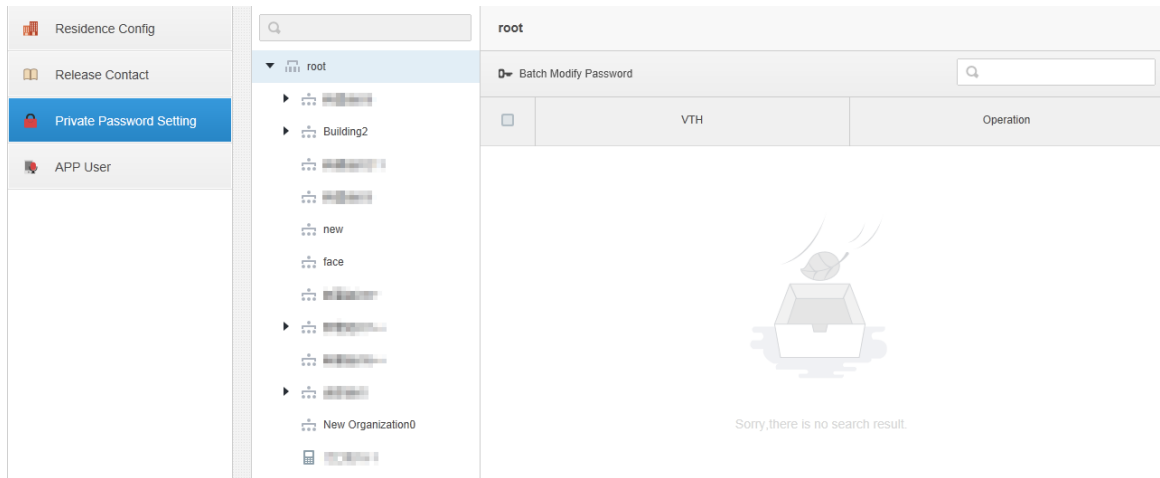


Make sure that contacts are released to VTO; otherwise it will fail to set private password.

Step 1 Click  on the Web Manager, and then select **Video Intercom Management**.

Step 2 Click **Private Password Setting**.

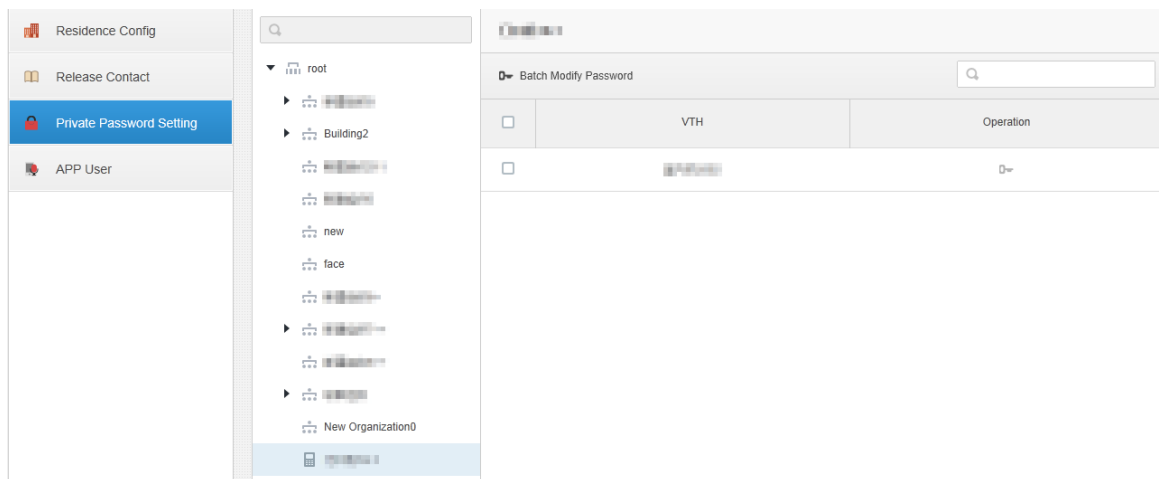
Figure 4-391 Set private password (1)



Step 3 Select a VTO.

The VTHs bound to this VTO are displayed.

Figure 4-392 Set private password (2)



Step 4 Select a VTH, click **Batch Modify Password** or select several VTHs, click **Batch Modify Password**.

Figure 4-393 Change password

Change Password
✕

! Please release the contacts of the selected VTH device to the VTO device, or else password modification is invalid.

New Password :

Confirm :

OK
Cancel

Step 5 Enter password, and then click **OK**.

You can use the new password to unlock on the VTO.

4.21.3.5 APP User

View information of APP users, freeze user, modify login password and delete user.



APP user can register by scanning the QR code on VTH. For details, see *DSS APP User's Manual*.

Step 1 Click **+** on the Web Manager, and then select **Video Intercom Management**.

Step 2 Click **APP User**.

Figure 4-394 App user

Delete							
<input type="checkbox"/>	Username	VTH Info	SIP Code	Last Login Time	Right Status	Last Password Res..	Operation
<input type="checkbox"/>	lyca		10#1#5502#101	2019-03-25 13:37:15	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	lycl		10#1#5502#177	2019-03-25 12:02:48	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	zxy		10#1#5502#191	2019-03-26 10:05:23	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	zxy1		10#1#5502#130	2019-03-26 11:54:56	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	ljl1		10#1#5502#139	2019-03-26 11:32:47	<input checked="" type="checkbox"/>		

Table 4-68 Parameters

Operation	Description
Freeze APP user	<p>The APP user cannot log during 600 s after being frozen.</p> <p> means normal status; means freezed. Click this icon to switch between the two statuses.</p> <p></p> <p>The account will be frozen when invalid password attempts exceeds 5 by APP user.</p>
Modify APP login password	<p>Click and enter new password on the interface of Reset Password. Click OK.</p> <p></p> <ul style="list-style-type: none"> The password shall be between 8 and 16 characters, including number and letter. means password can be seen while means password is protected. Click icon to switch.
Delete APP user	<p>Click or select APP user (several users can be selected); click Delete and the selected users will be deleted according to the interface tips.</p>

4.21.3.6 Call Management

Create device group, management group and relation group respectively and define restricted call relations. This function is only available for the system account user.



Click on the interface of device group, management group or relation group, the system will restore management group and relation group to original status.

4.21.3.6.1 Device Group Config

Realize mutual call only when VTO and VTH are added into the same device group. Pro will automatically generate corresponding device group when VTO, verifying VTO and fence station are added to Pro.

- Add VTO and automatically generate a device group, add VTH of the unit into the group, and realize mutual call between VTH and VTO within the group.
- Add verifying VTO and automatically generate a device group, add it to the group together with the VTH of the same room, and realize mutual call between VTH and verifying VTO within the group.
- Add fence station and automatically generate a device group, add all the VTH into the group. Realize mutual call between fence station and all the VTH.

- Add VTH, if the VTH is automatically connected to unit VTO, verifying VTO, fence station, and then it will be automatically added to the device group, and realize mutual call among unit VTO, verifying VTO or fence station.



Call between VTH is not restricted by device group; mutual call can be realized among VTH in different device groups.

4.21.3.6.2 Adding Management Group

Management group is to make groups for administrators, and realize relation binding of one to one, one to many or many to many. Administrators include Pro administrator and VTS. If there is default management group, VTS will be automatically added to management group when it is added.



- Before configuring management group, it needs to create user, select video intercom menu permission and device permission, and add new users into management group.
- Use system user to configure group relation, need to switch to new user for login. If system logs onto many devices, then it cannot be used as administrator.


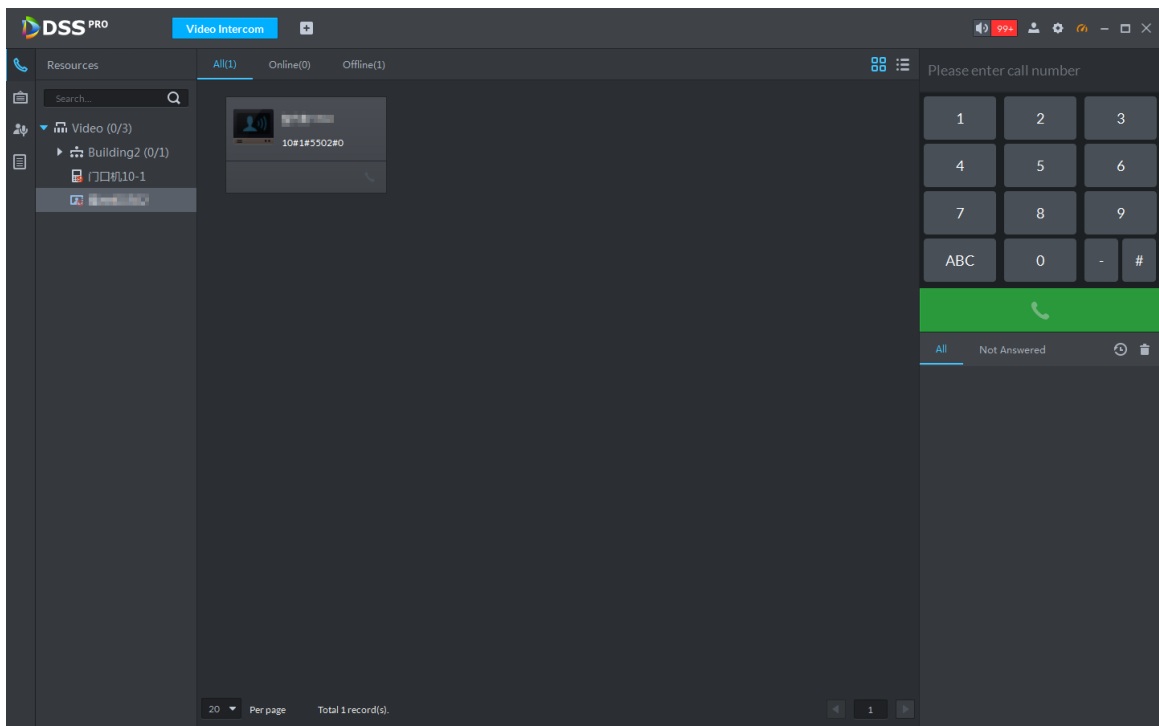

Step 1 Click  on the Control Client, and then select **Video Intercom**.

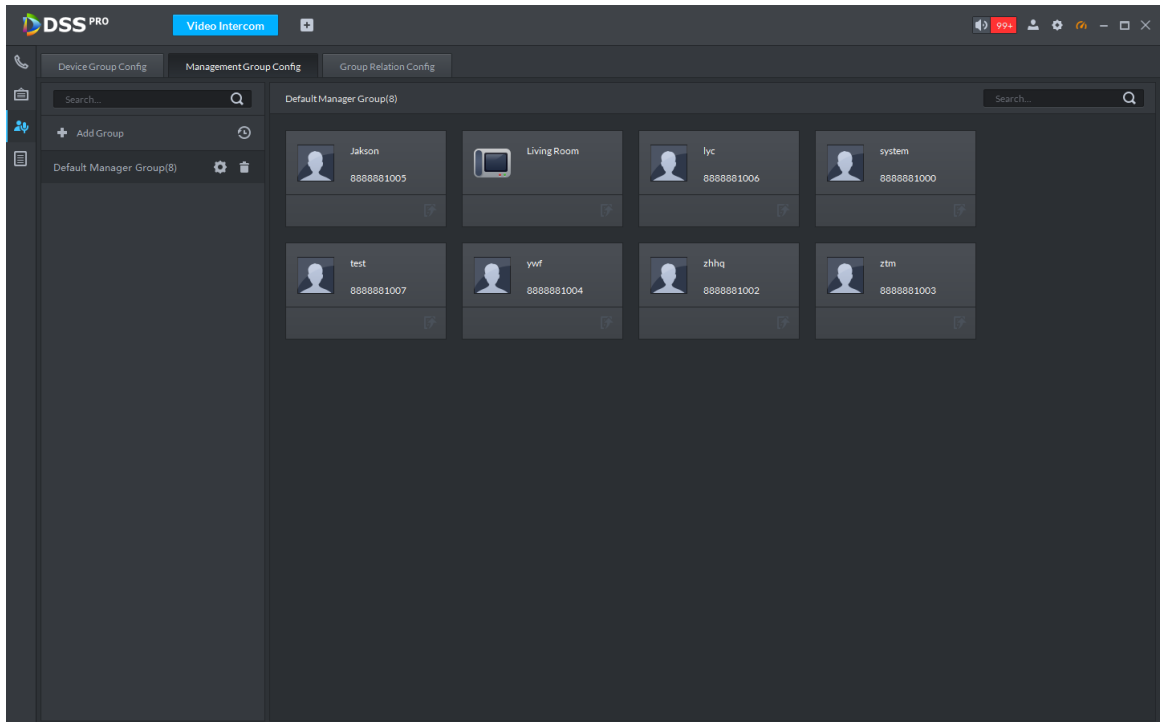
Figure 4-395 Video intercom



Step 2 Click .

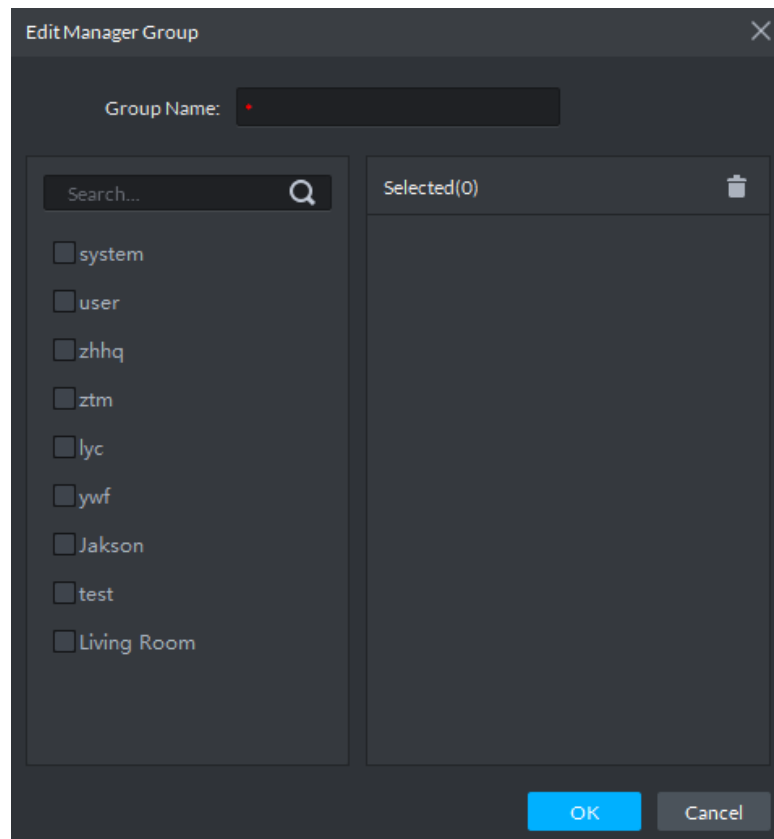
Step 3 Click **Management Group Config**.

Figure 4-396 Management group configuration



Step 4 Click **Add Group**.

Figure 4-397 Edit manager group



Step 5 Enter group name, select administrator account or VTS, and click **OK**.
The added management group is displayed in the list.





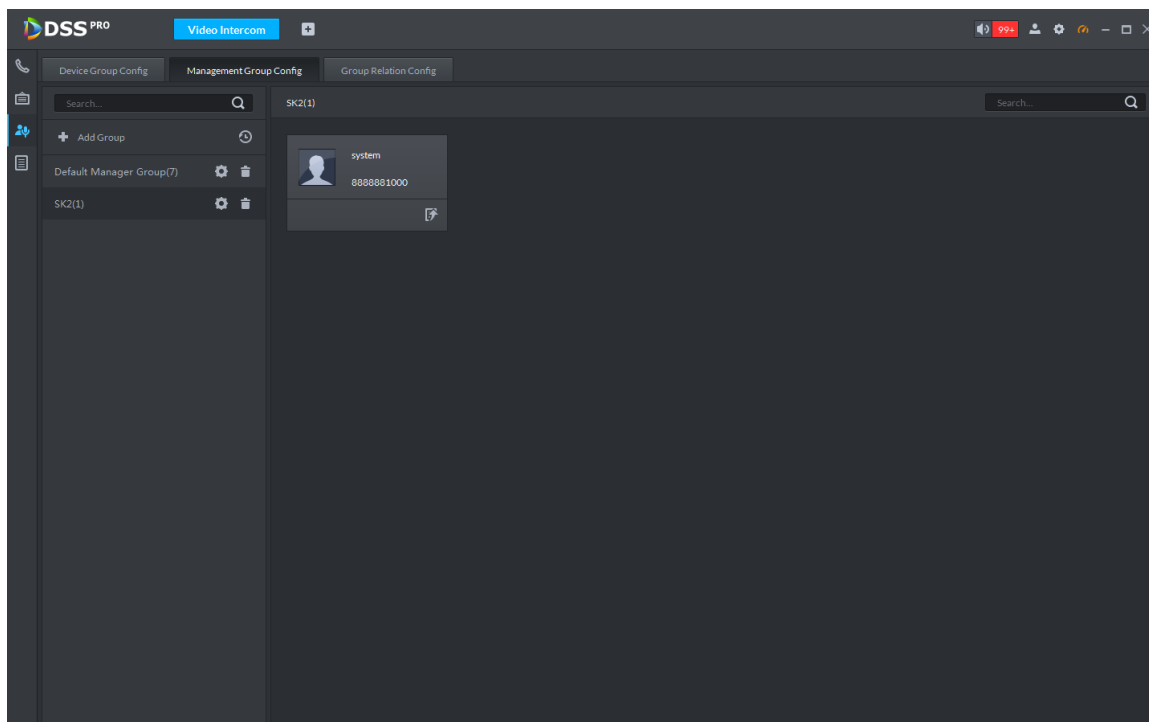
- To transfer members, click  and move the member to the group.
- To manage group members, click  to add or delete group member.



Figure 4-398 Added management group



4.21.3.6.3 Group Relation Config

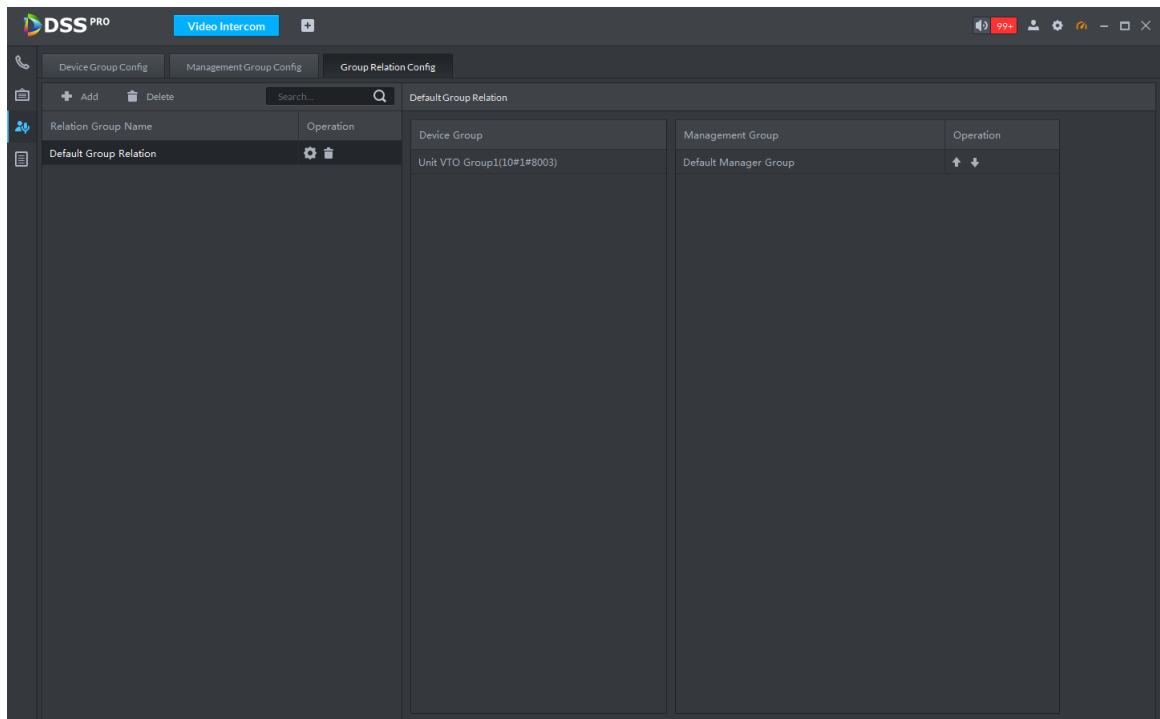
There are two situations for relation binding

- Device group only binds one management group
Any device in the group can call administration with one click, all the bound administrators within the management group will generate ring bell. At this moment, all other ring bell will stop as long as there is on administrator answers. The device call request can be rejected as long as all the administrators reject to answer.
- Device group binds several management groups
There is priority among several management groups. When any device in the group calls administrator with one click, and all the online administrators of management group with highest priority will generate ring bell. If none of these administrators answer, then it will call next management group. The interval between two calls is 30s; it can skip up to one management group. If neither of two groups answer, then the device prompts call overtime, no response.

Step 1 Click  on the Control Client, select **Video Intercom**, and then click .

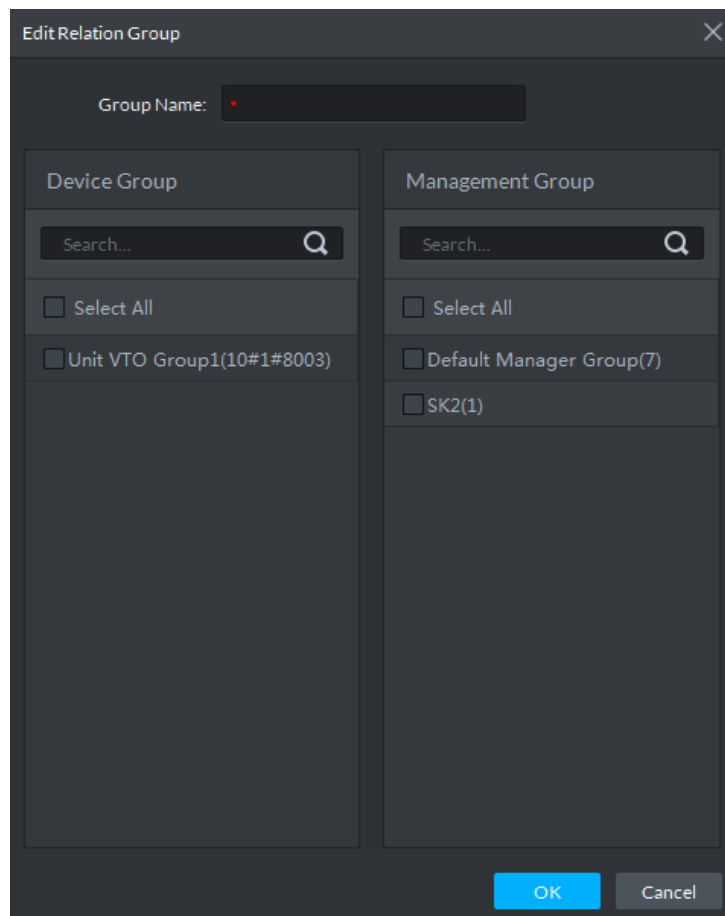
Step 2 Click **Relation Group Config**.

Figure 4-399 Relation group configuration



Step 3 Click **Add**.

Figure 4-400



Step 4 Enter name, select device group and management group, and then click **OK**.



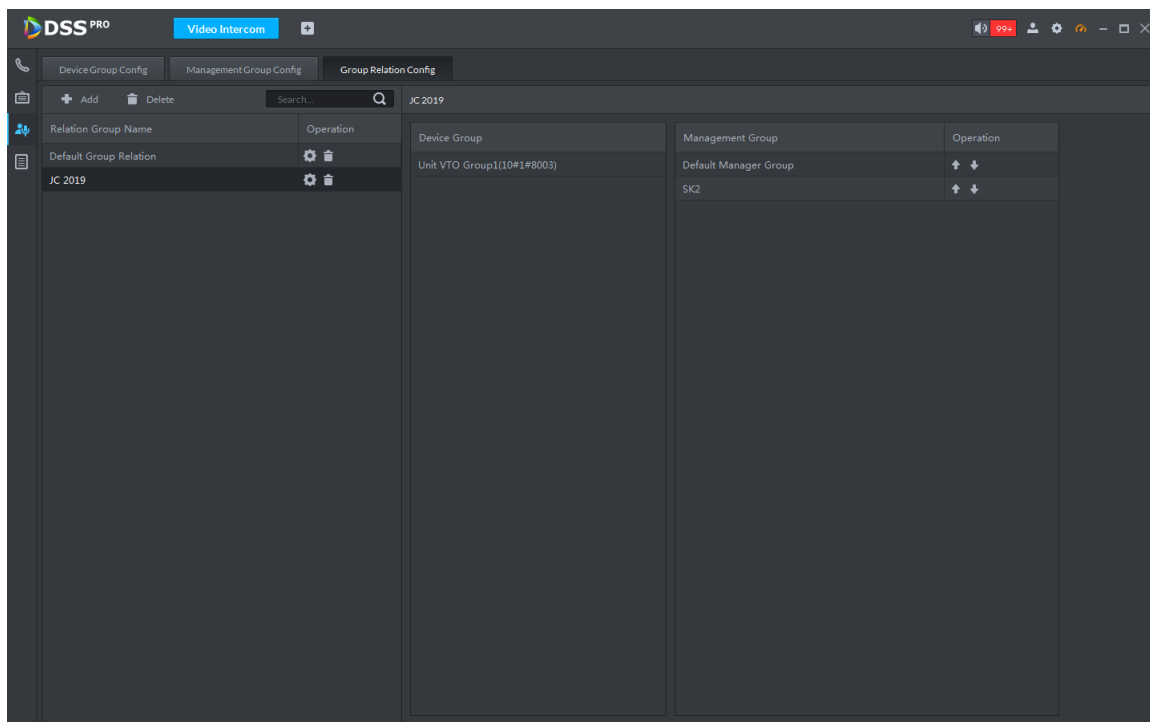
Added relation group is displayed in the list. If there are several relation groups, you can click  or  to adjust priority level. When there is call, the online administrators with high priority will generate ring bell first.

Figure 4-401 Added relation group



4.21.4 Video Intercom Applications

4.21.4.1 Call

Realize call among Pro, VTO and VTH.


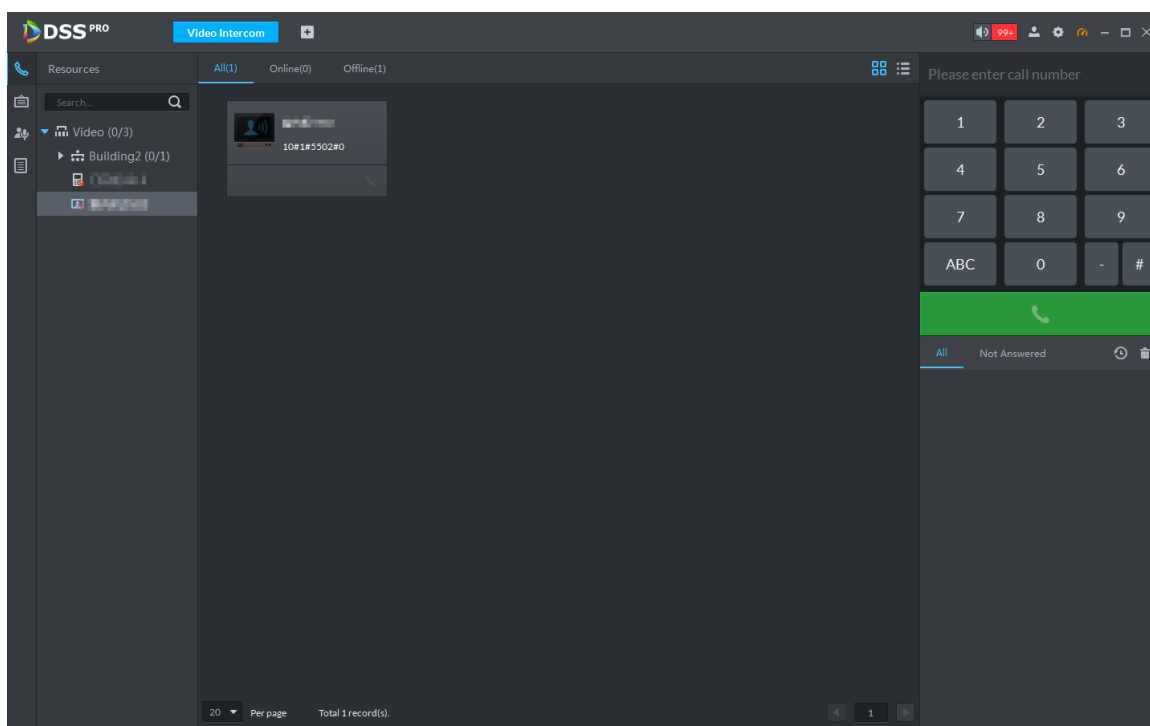

Step 1 Click  on the interface of **Video Intercom**.

Figure 4-402 Call center



Step 2 You can call VTO and VTH on the interface of **Call Center**.

- Call from the platform to VTO

Select VTO in the device list; click corresponding  of VTO and call VTO. The system pops out call interface. The following operations are support during call.





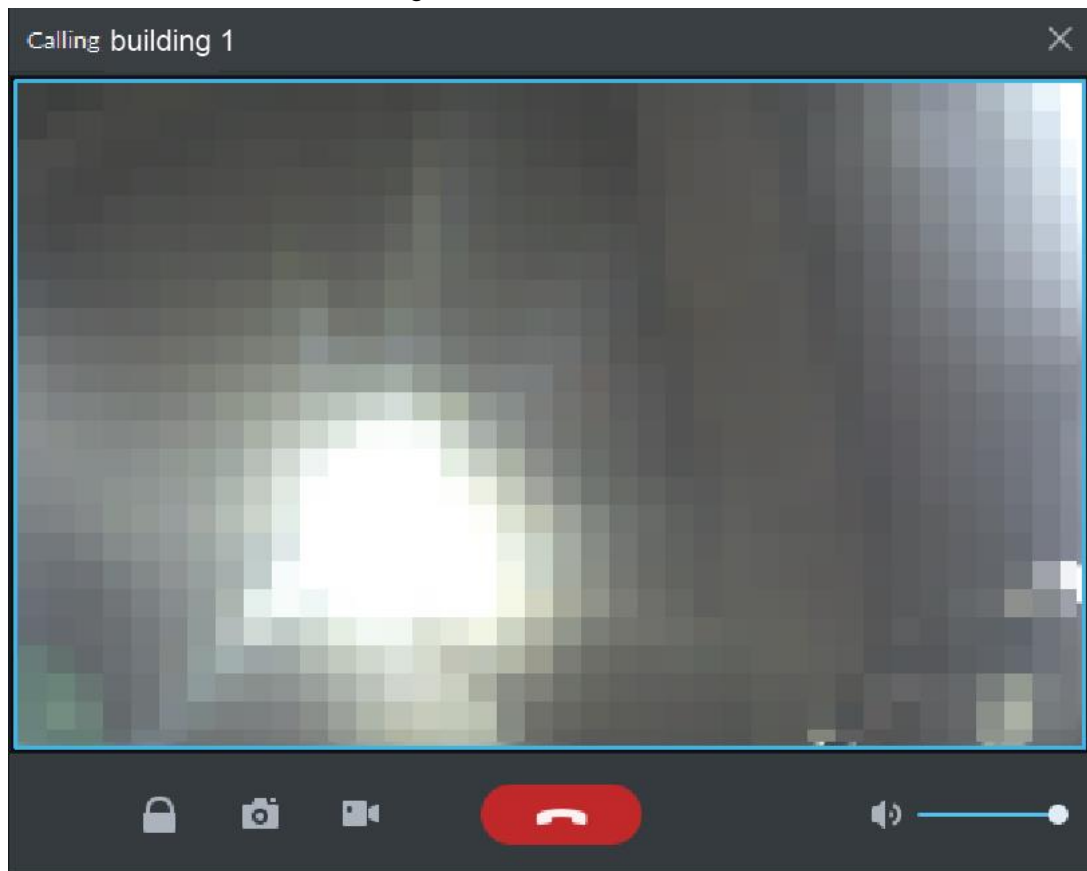

- ◇ If VTO is connected to lock, click  to unlock.
- ◇ Click  to capture picture, the snapshot is saved into the default directory installed by client. If you need to modify the save path of snapshot, see "4.1.4 Local Configuration" for more details.
- ◇ Click  to start record, click again to stop record. The video is saved in default path installed by client. If you need to modify the save path, see "4.1.4 Local Configuration" for more details.
- ◇ Click  to hang up.

Figure 4-403 Call



- Call from the platform to VTH

Select VTH from the device list, click  on the VTH or dial corresponding VTH on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait** There are two modes for answering the call.


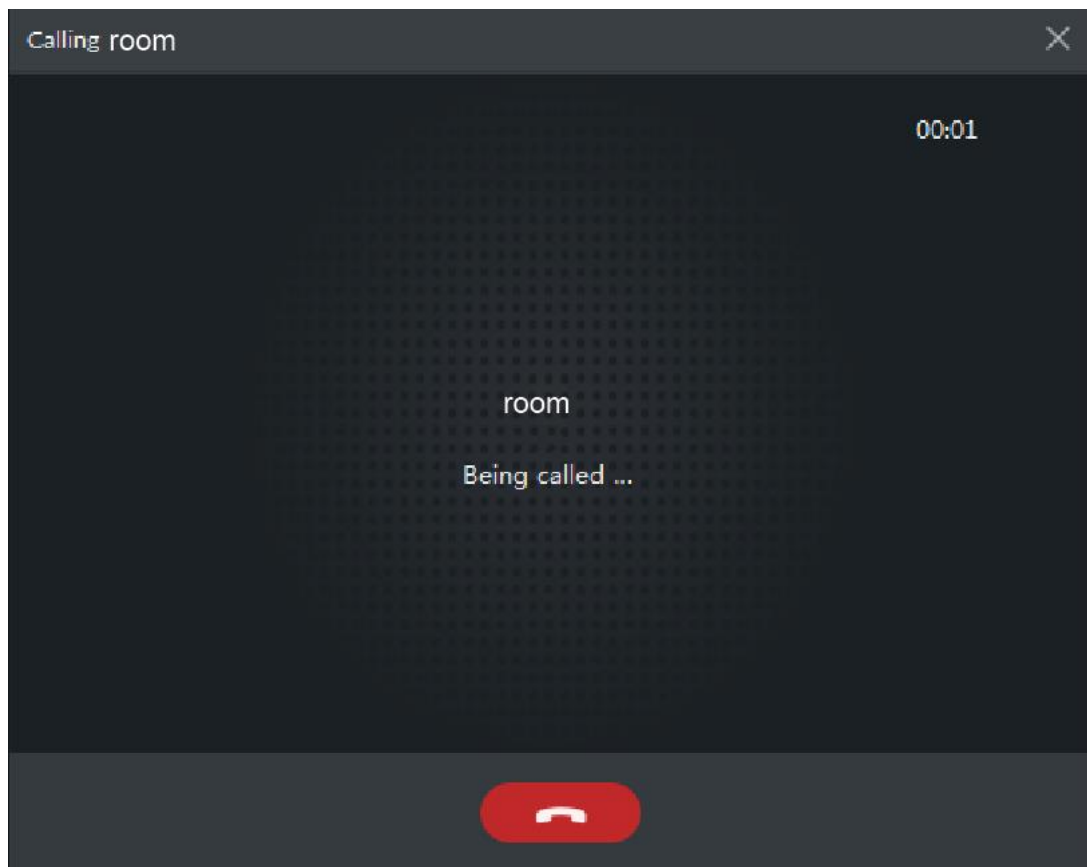
- ◇ Answer by VTH, bidirectional talk between client and VTH. Press  to hang up when you answer the call.
- ◇ If VTH fails to answer over 30s, busy or hang up directly, then it means the call is busy.

Figure 4-404 Calling






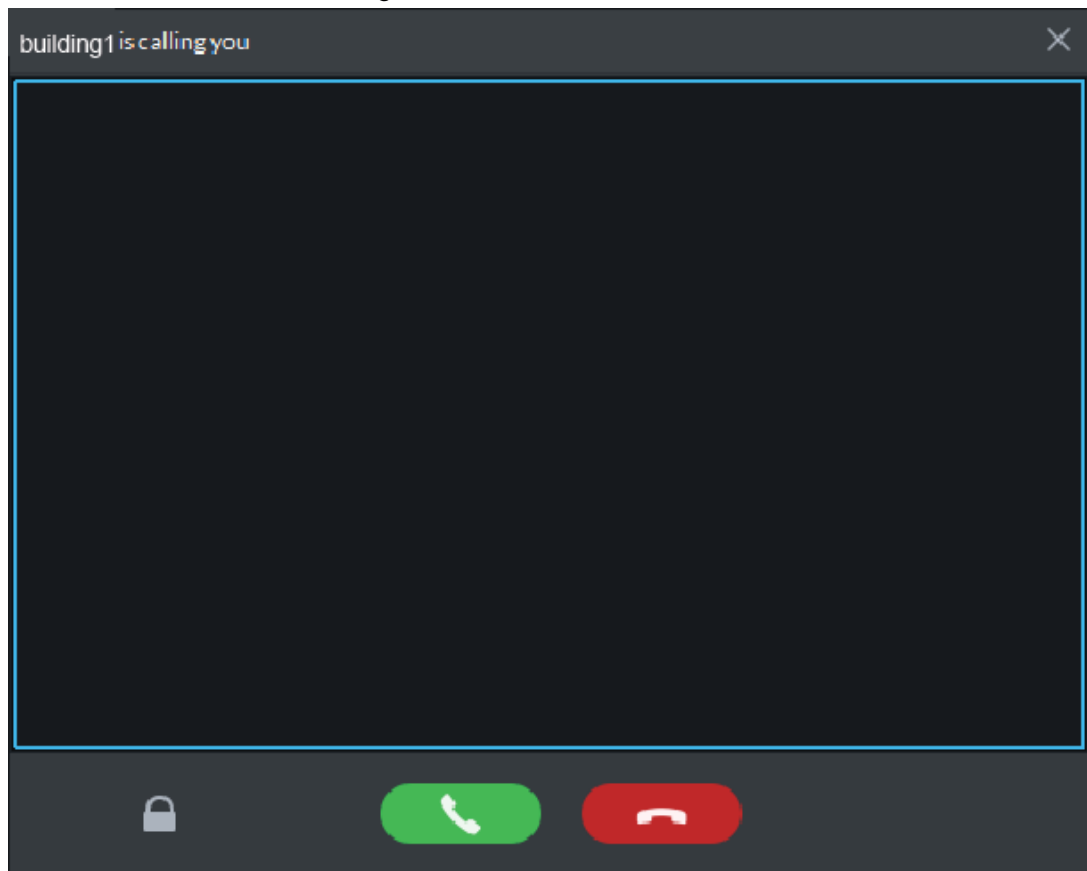

- Call from VTO to the platform
VTO calls Pro, client pops up the dialog box of VTO calling.
 - ◇ If VTO is connected to lock, click  to unlock.
 - ◇ Click  to answer VTO, realize mutual call after connected.
 - ◇ Click  to hang up.

Figure 4-405 VTO Call



- When VTH is calling the platform

The client pops out the dialog box of VTH calling. Click  to talk with VTH.



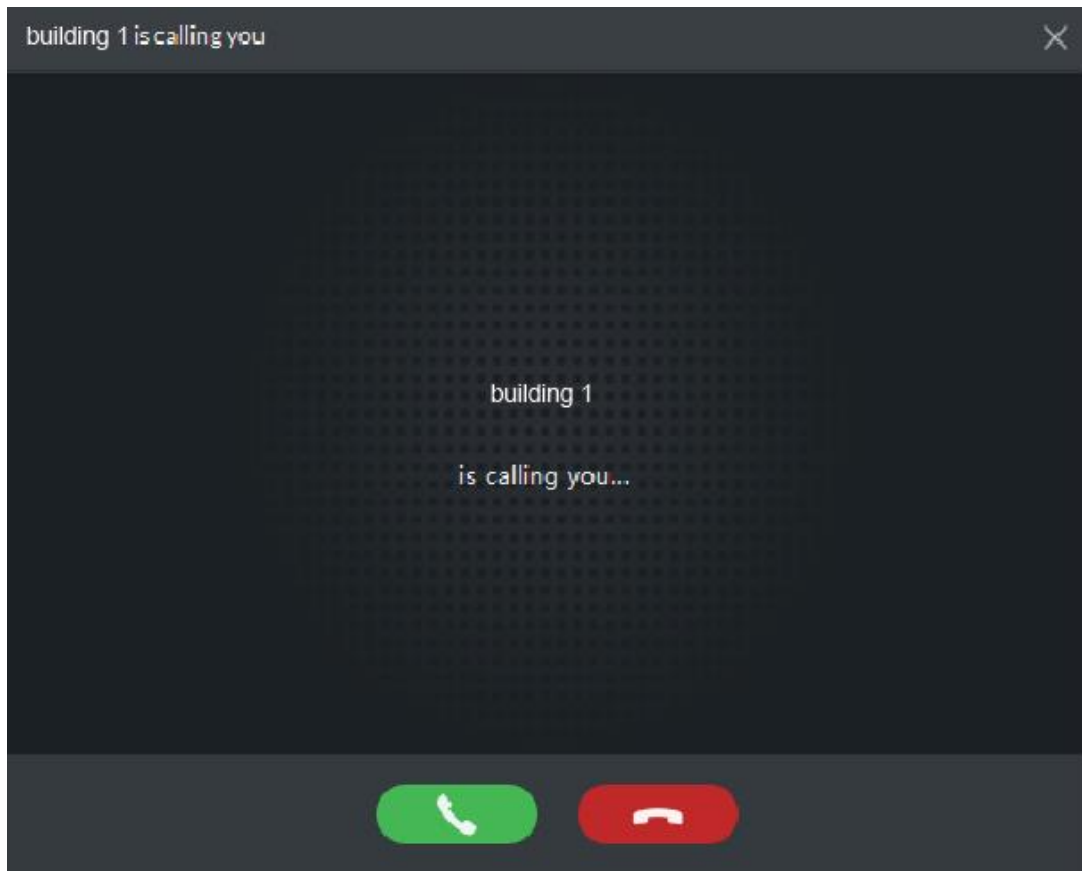
- ◇ Click  and answer VTO, realize mutual talk after connected.
- ◇ Click  and hang up.

Figure 4-406 VTH call









- Call through call records
All the call records are displayed in the **Call Record** at the lower right corner of the interface of **Video Intercom**. Move the mouse pointer to the record, click  and call back.

Figure 4-407 Call records

All	Not Answered		
	4#4#401#0	00:00	2018-07-02 13:57:28
	4#4#402#0	00:00	2018-07-02 13:56:55
	4#4#401#0 (2)	00:00	2018-07-02 13:56:44
	4#4#8001 (4)	00:06	2018-07-02 13:53:43
	4#4#402#0	00:00	2018-07-02 13:43:19

4.21.4.2 Information Release

Send message to designated VTH.


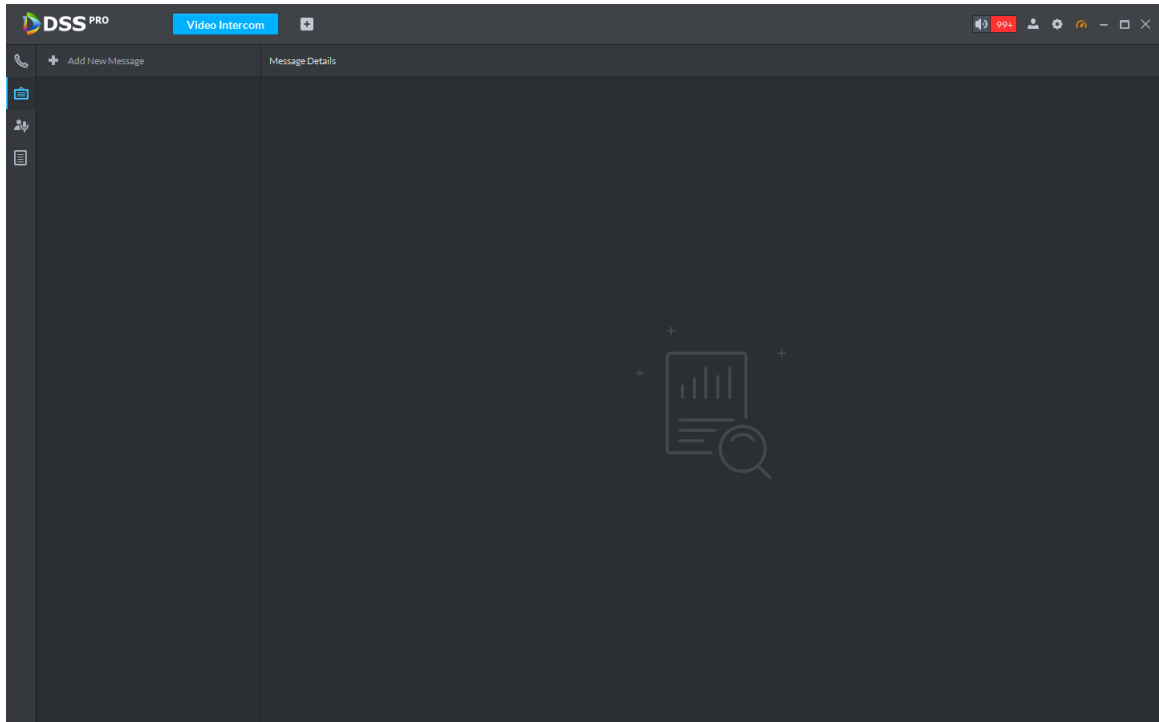
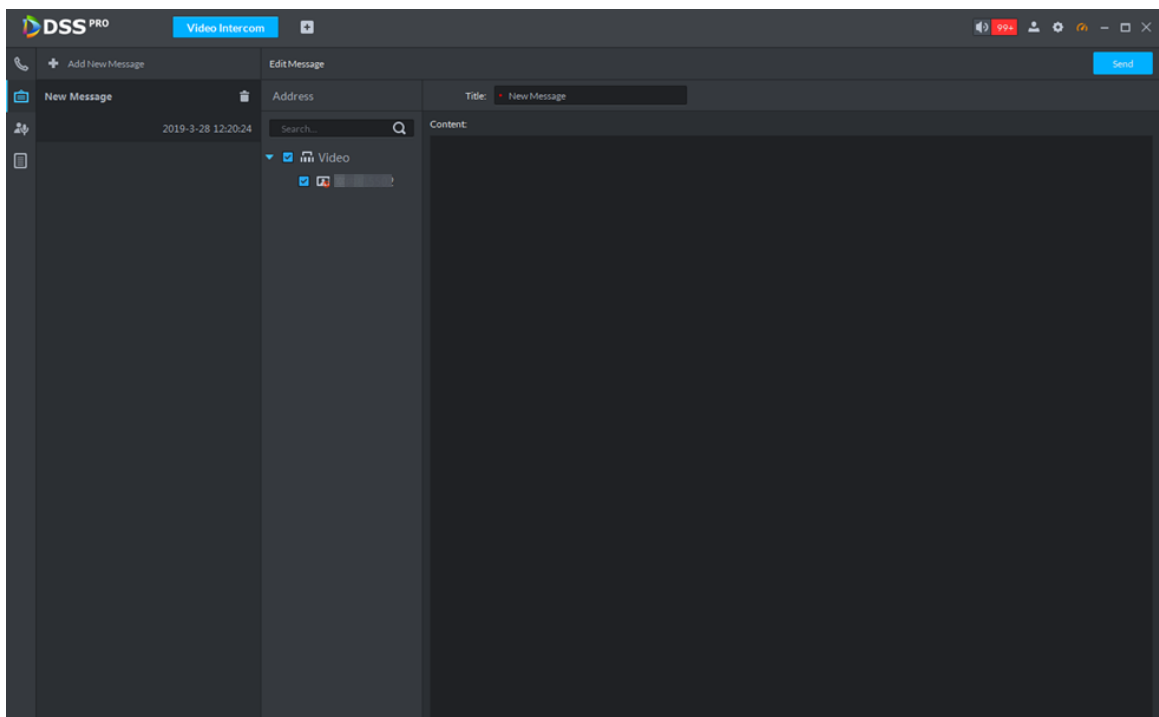
Step 1 Click  on the interface of **Video Intercom**.

Figure 4-408 Release interface



Step 2 Click **Add New Message**, select VTH and add release information.

Figure 4-409 Add new message



Step 3 Click **Send**.

The VTH will receive the message after it is sent successfully.

4.21.4.3 Video Intercom Logs

View log records and you can trace recorded calls.

Step 1 Enter the interface of video intercom log.



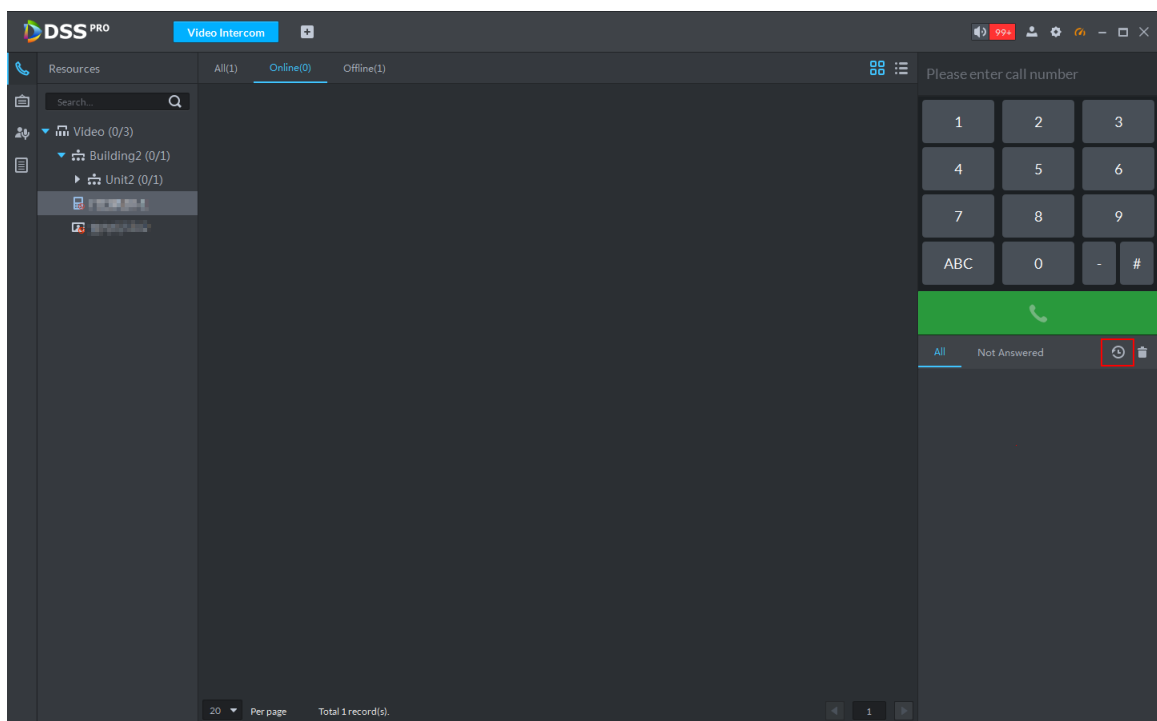
- Click  on the interface of **Video Intercom**.
- Click  and enter console on the interface of **Video Intercom**.

Figure 4-410 Enter console



Step 2 Set conditions, and then click **Search**.

Figure 4-411 Logs

Device Name	Call Type	Room No.	Start Time	Talk Time	End Status
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:34:05	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:30:57	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:30:46	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:30:00	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:28:22	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:28:05	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:25:42	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:24:50	00:00	Missed
[REDACTED]	Incoming	10#1#8003	2019-03-25 20:24:38	00:09	Received
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:20:50	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:19:55	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:18:34	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 20:18:18	00:00	Missed
[REDACTED]	Outgoing	10#1#5502#0	2019-03-25 20:02:49	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 19:55:12	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 19:55:02	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 19:54:41	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 19:48:18	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 19:48:06	00:00	Missed
[REDACTED]	Incoming	10#1#5502#0	2019-03-25 19:47:59	00:00	Missed

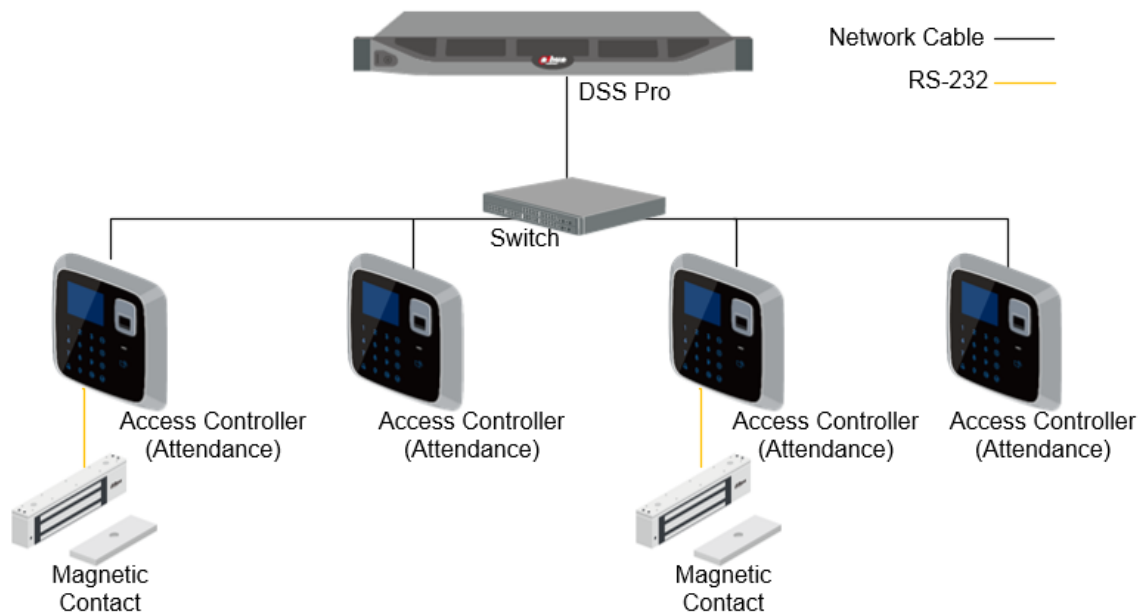
Step 3 Click **Export** and the logs will be saved locally according to system prompt.

4.22 Attendance Management

Configure attendance settings such as attendance devices, attendance shifts and periods, so as to manage attendance records and reports.

4.22.1 Typical Topology

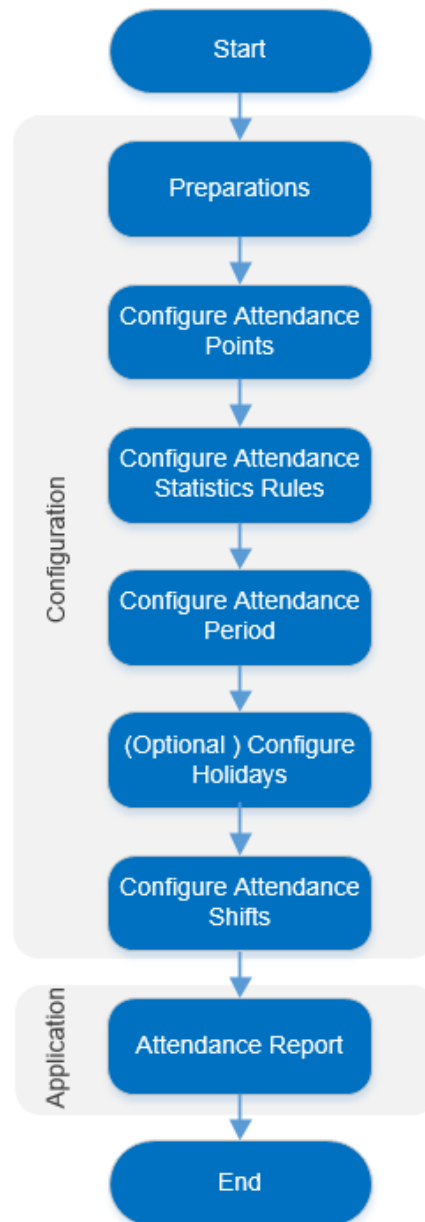
Figure 4-412 Attendance management typical topology



- Attendance devices are used for recording checking in or out in the way of face recognition, swiping card or more.
- The platform centrally manages all devices and attendance rules, and provides attendance analysis.

4.22.2 Business Flow

Figure 4-413 Attendance business flow



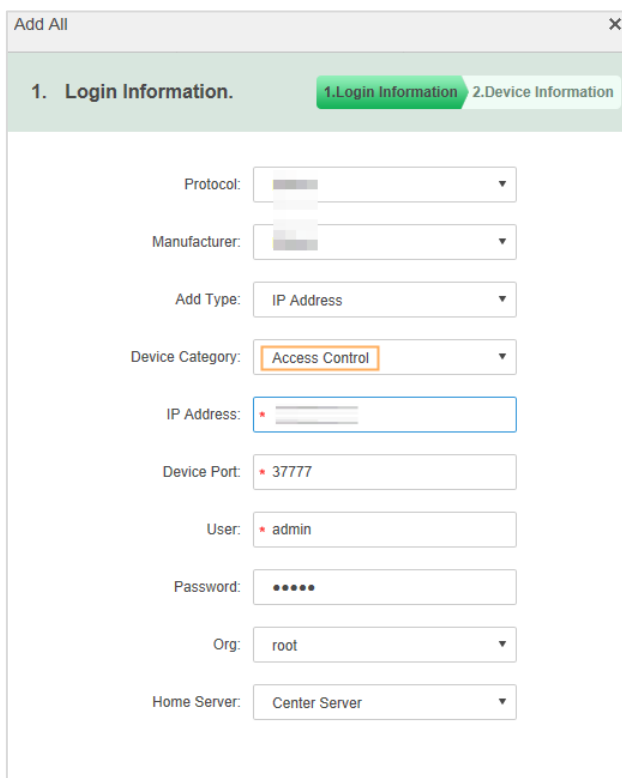
4.22.3 Configuring Attendance

4.22.3.1 Preparations

Make sure that the following preparations have been made:

- Attendance devices are correctly deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding attendance devices on the **Device** interface of Web Manager, select **Access Control** for device category.

Figure 4-414 Add device



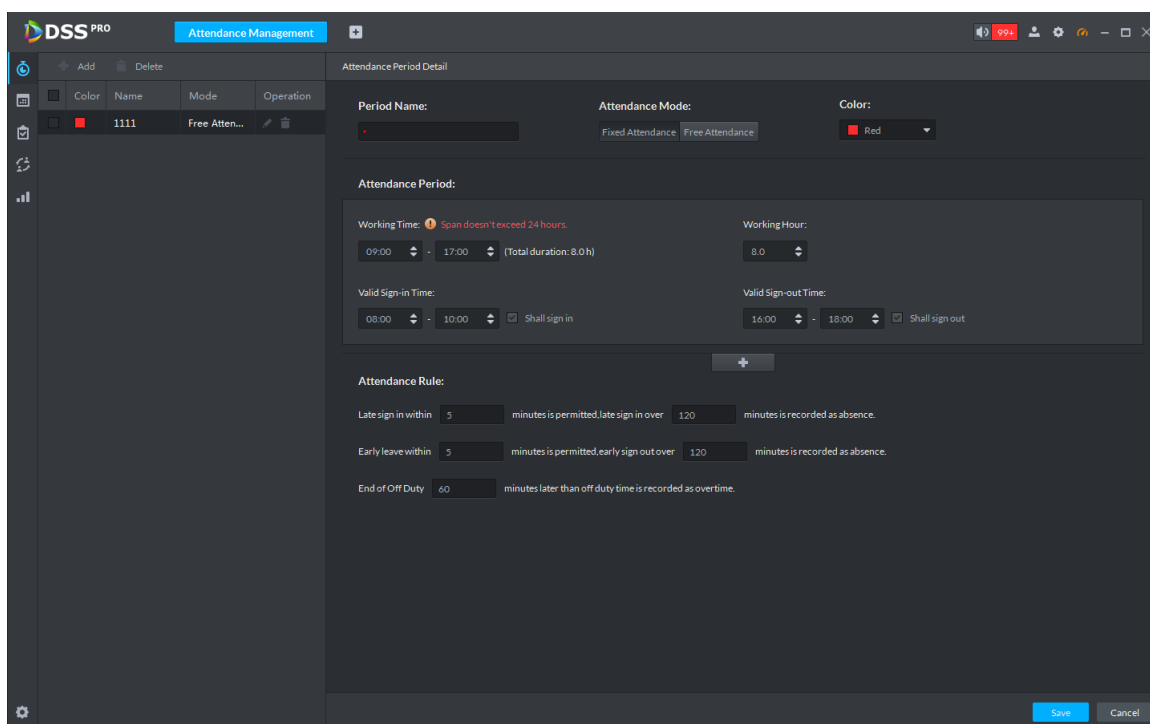
- ◇ Personnel information is added correctly. For details, see "4.19 Personnel Management."

4.22.3.2 Setting Attendance Terminal

Make sure that access controller is used as attendance device for check-in and check-out, recording attendance information, and uploading attendance data.

Step 1 Click  and select **Attendance Management**.

Figure 4-415 Attendance management




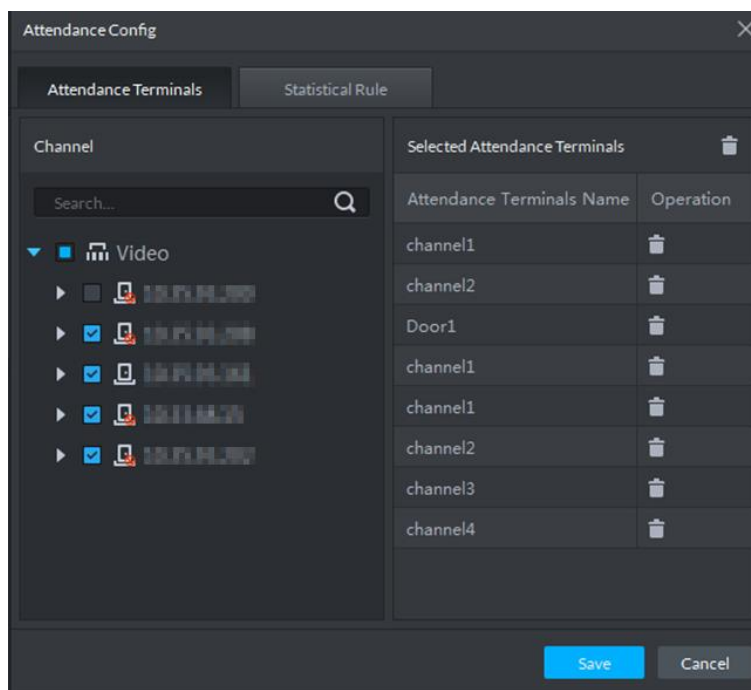
Step 2 Click  at the lower-left corner of the interface, and then select **Attendance Terminals**.

Figure 4-416 Attendance terminal



Step 3 Select access control channel from the left list, and then click **Save**.



You can find needed devices by search. The system supports fast search.

4.22.3.3 Setting Statistics Rule

Minimum timing unit of swiping card is minute, the statistics rule of dealing with second is round up and round down. For example, swipe card at 09:00:01, if the rule is set as round down, then the time of swiping card is 09:00; if the rule is set as round up, then the time of swiping card is 09:01.


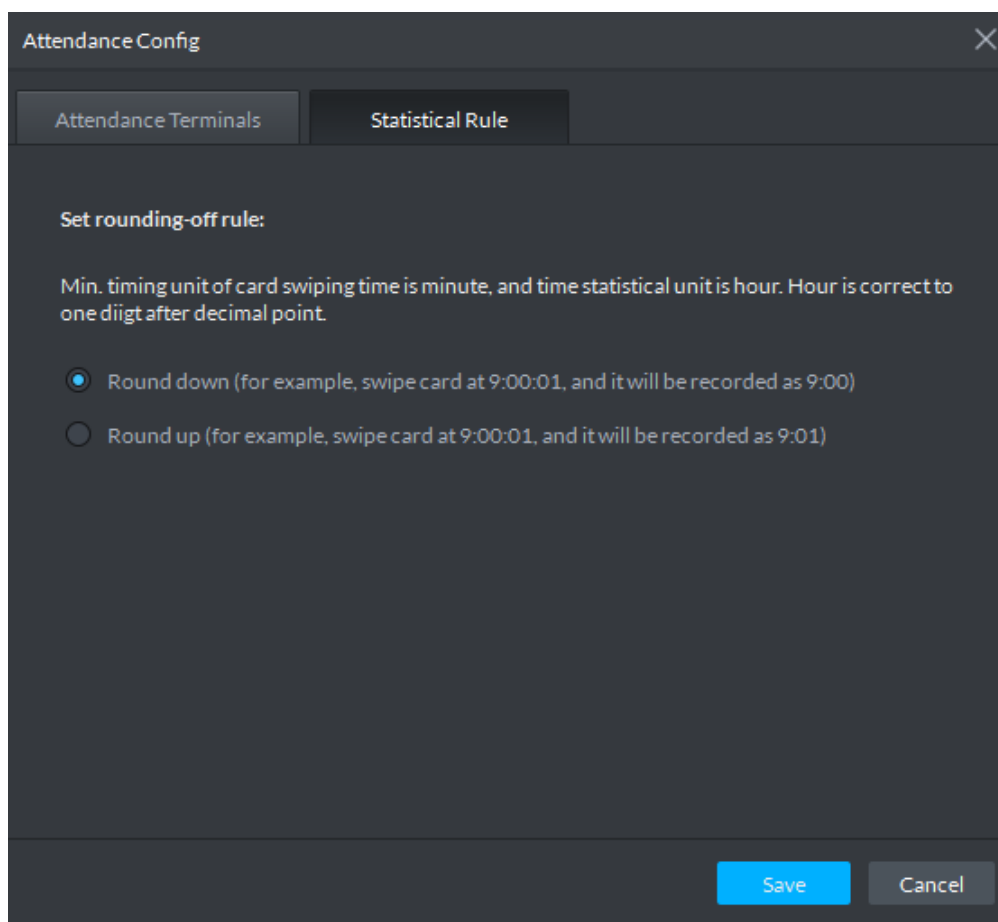
Step 1 Click  at the lower left corner on the interface of **Attendance Management**, select **Statistics Rule**.

Figure 4-417 Statistical rule



Step 2 Select rule and click **Save**.

4.22.3.4 Setting Attendance Period

Set attendance period, which can be used as time evidence to judge if people attend, arrive late or leave early.


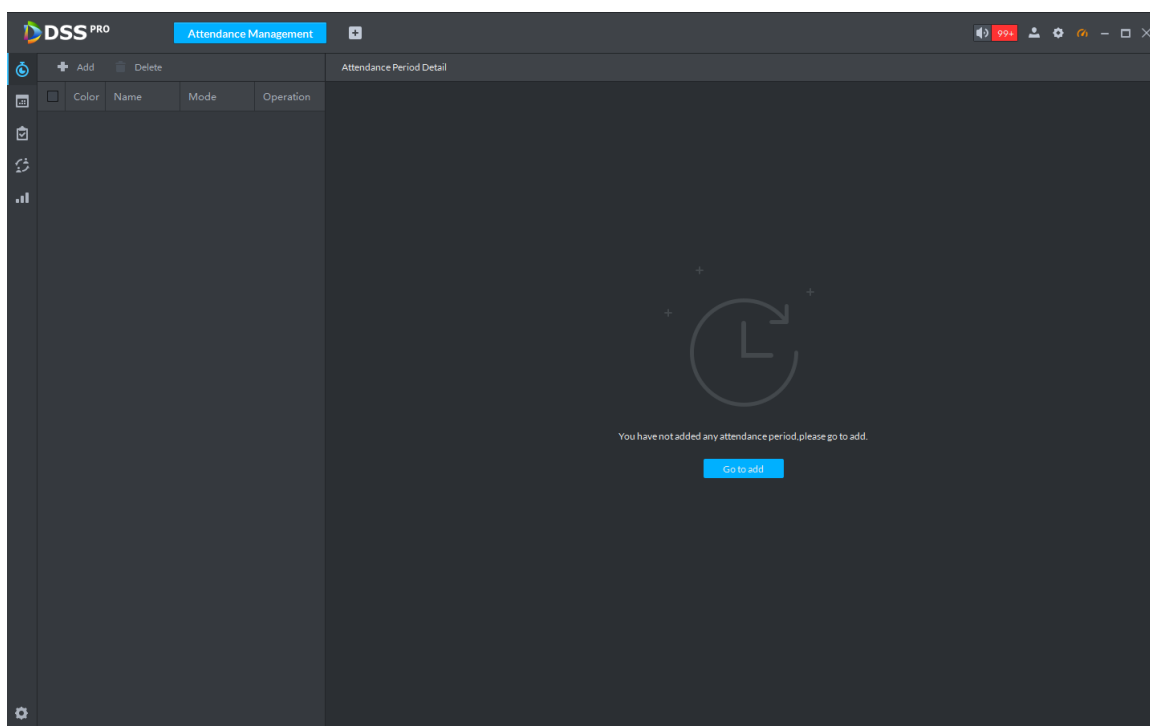

Step 1 Click  on the interface of **Attendance Management**.

Figure 4-418 Attendance period



Step 2 Click  on upper-left corner of the interface.

The new attendance period interface is displayed.

Step 3 Set parameters of attendance period.



The priority of rules set by Pro is higher than that of the device itself.

There are two types of attendance according to different attendance modes and different configurations.

- Fixed attendance requires you to sign in and sign out during the fixed hours.

Figure 4-419 Set attendance time (one working period)



The screenshot shows the 'Attendance Management' window in DSS PRO. The 'Attendance Period Detail' form is active. It includes fields for 'Period Name', 'Attendance Mode' (Fixed Attendance, Free Attendance), and 'Color' (Red). The 'Attendance Period' section contains two rows of settings: 'Working Time' (09:00 - 17:00, Total duration: 8.0h) and 'Working Hour' (8.0). Below this, 'Valid Sign-in Time' is set to 08:00 - 10:00 with a 'Shall sign in' checkbox, and 'Valid Sign-out Time' is set to 16:00 - 18:00 with a 'Shall sign out' checkbox. The 'Attendance Rule' section has three rows: 'Late sign in within 5 minutes is permitted, late sign in over 120 minutes is recorded as absence.', 'Early leave within 5 minutes is permitted, early sign out over 120 minutes is recorded as absence.', and 'End of Off Duty 60 minutes later than off duty time is recorded as overtime.' The interface includes a sidebar with navigation icons and a bottom bar with 'Save' and 'Cancel' buttons.

Figure 4-420 Set attendance time (two working periods)

This screenshot is similar to Figure 4-419 but shows two 'Attendance Period' rows. The first row has 'Working Time' 09:00 - 17:00 (8.0h) and 'Working Hour' 8.0. The second row has 'Working Time' 09:00 - 17:00 (8.0h) and 'Working Hour' 8.0. The 'Valid Sign-in Time' for the second row is 08:00 - 10:00 with 'Shall sign in' checked. The 'Valid Sign-out Time' for the second row is 16:00 - 18:00 with 'Shall sign out' checked. The 'Attendance Rule' section remains the same as in Figure 4-419. The interface includes a sidebar with navigation icons and a bottom bar with 'Save' and 'Cancel' buttons.

Table 4-69 Fixed attendance parameters

Parameter	Description
Period Name	Custom period name, used to recognize period, such as early shift and night shift.
Color	Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly

Parameter	Description
	recognize shift information.
Attendance Mode	Set as Fixed Attendance .
Working Time	<p>Set corresponding working hour of period. Attendance time supports cross-day, but not exceeds 24 hours. One attendance period supports max two types of attendance time.</p>  <ul style="list-style-type: none"> ● If attendance time needs to be split into twice, such as morning and afternoon, then it needs to click , set second working time and sign-in sign-out period. ● If you set two types of attendance time, then it needs to sign in and sign out according to the configured attendance time, which can be considered as normal attendance.
Working Hour	Please fill in according to actual situation.
Valid Sign-in Time	<p>If working time is set from 09:00-18:00, then valid sign-in time can be set as 08:00-10:00, valid sign-out time can be set as 16:00-18:00. Configuration rules are as follows:</p> <ul style="list-style-type: none"> ● The start time of valid sign-in time is earlier than or equal to start working time (09:00), the end time of valid sign-in time should be later than start working time (09:00), earlier than start time of valid sign-out time. If there are several sign-in records within valid sign-in time, then the earliest record is considered as sign-in time. ● The start time of valid sign-out time is later than the end time of valid sign-in time, earlier than end working time (18:00), the end sing-in time of valid sign-out time is later than or equal to end working time (18:00). If there are several sign-out records within valid sign-out time, then the earliest record is considered as sign-out time.
Valid Sign-out Time	
Shall sign in	If you set two working time, then the second working time can cancel sign in, you don't have to sign in when you work at the second working time, and the start time of working time can be used as sign-in time.
Shall sign out	If you set two working time, then the first working time can cancel sign in, you don't have to sign out when you finish work at the second working time, and the end time of working time can be used as sign-out time.
Late sign-in within _minutes is permitted	Define the rules for being late, absence and early leave.
Late sign-in over _minutes recorded as absence	Suppose set Work sign-in over __minutes recorded as late as 5 minutes; Late sign-in over _minutes recorded as absence is set as 60 minutes; Off duty _minutes in advance recorded as early leave is set as 10 minutes; Early leave exceeds _minutes recorded as absence is set as 30 minutes.

Parameter	Description
Early leave within _ minutes is permitted Early Sign out over _ minutes is recorded as absence	Details are as follows. <ul style="list-style-type: none"> ● Late When work sign-in is later than start time of working time, and 5 minutes < period ≤ 60 minutes, then it is recorded as late. ● Early leave When off duty sign-out time is earlier than end time of working time, and 10 minutes < period ≤ 30 minutes, then it is recorded as early leave. ● Absence When work sign-in time is later than start time of working time, and period > 60 minutes, then it is recorded as absence. When off duty sign-out time is earlier than end time of working time, and period > 30 minutes, then it is recorded as absence.
End of Off Duty _minutes later than off duty time is recorded as overtime	Define overtime rule. Suppose Off duty sign-out over __minutes recorded as overtime is set as 120 minutes, off duty sign-out time is later than end time of working time, and period > 120 minutes, then it is recorded as overtime, overtime period is Period – 120 minutes .

- Free attendance just calculates whether the daily working hours of a person meets the rule according to the sign-in/out time.

Figure 4-421 Configure free attendance

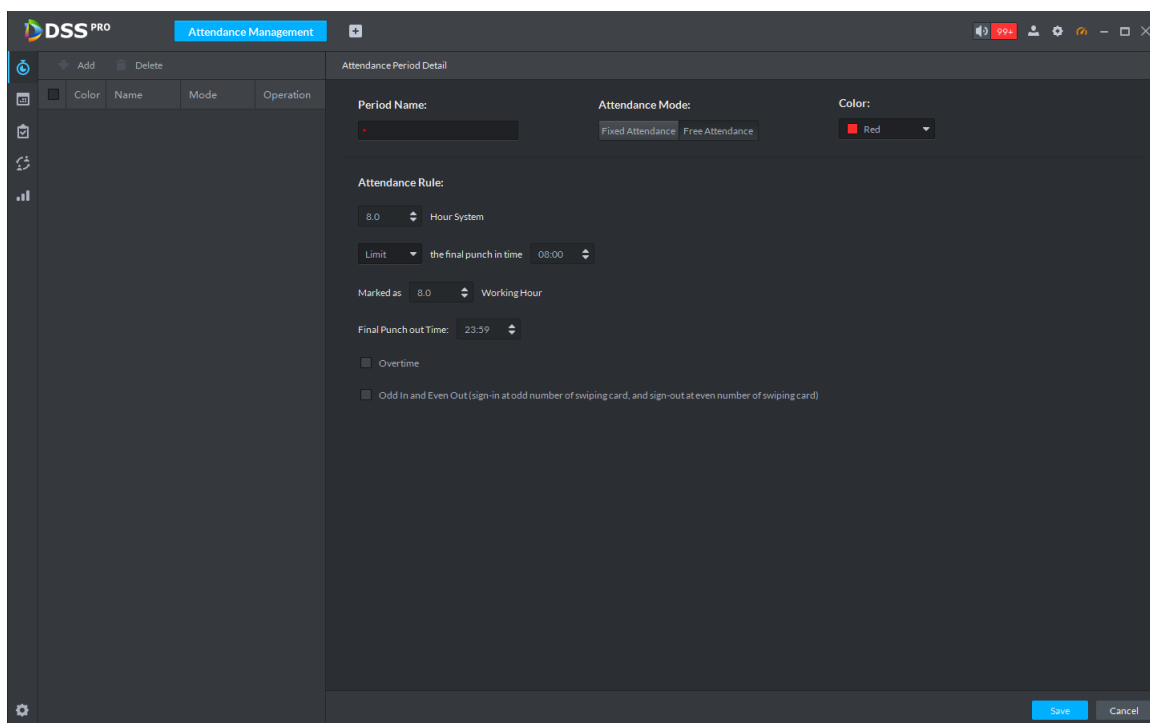


Table 4-70 Free attendance parameters

Parameter	Description
Period name	Custom period name, used to recognize period, such as flexible attendance.

Parameter	Description
Attendance mode	Set as Free Attendance .
Color	Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly recognize shift information.
Hour system	Set how many hours you have to work a day. For example, if you set 8, then it means you are required to work 8 hours.
Final punch in time	Sign in after restricted time is recorded as late.
Mark as_working hour	Fill in working hour according to actual situation.
Final punch out time	You are required to sign out before the designated time, otherwise no sign out is recorded.
Overtime	Working over__ hours is recorded as overtime. For example, working hour is 8 hours a day, and if you work overtime for 2.5 hours, then it is recorded as overtime, then you can set 10.5 here.
Work over_hours recorded as overtime	
Odd in even out	Swipe card at odd number is recorded as sign-in. For example, the first card-swiping is sign-in. Swipe card at even number is recorded as sign-out. For example, the second card-swiping is sign-out. It is recorded as twice card-swiping when the interval of continuous twice card swiping is bigger than the threshold.
Continuous twice card swiping interval \geq _minutes	

Step 4 Click **Save** and save period configuration.



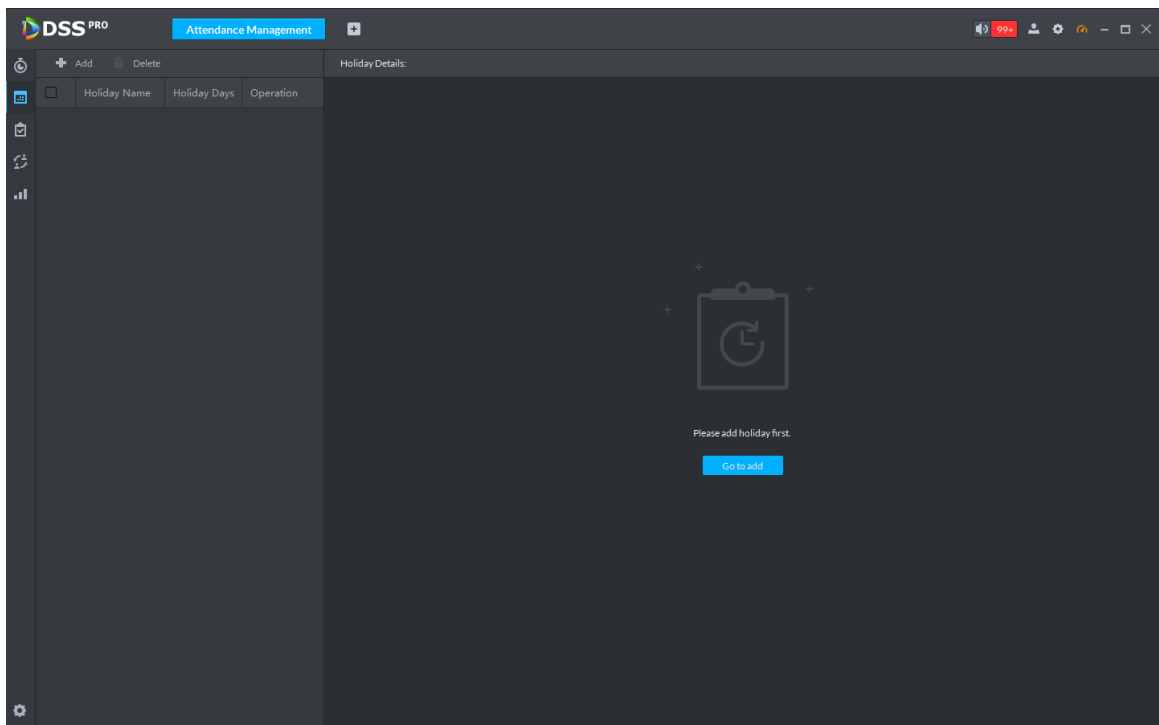
If attendance period is already applied to attendance shift, then before deleting attendance period, enter the interface of **Attendance Shift**, modify attendance shift, and delete attendance period.

4.22.3.5 Setting Holidays

Set holiday time, used to judge overtime type during attendance statistics.

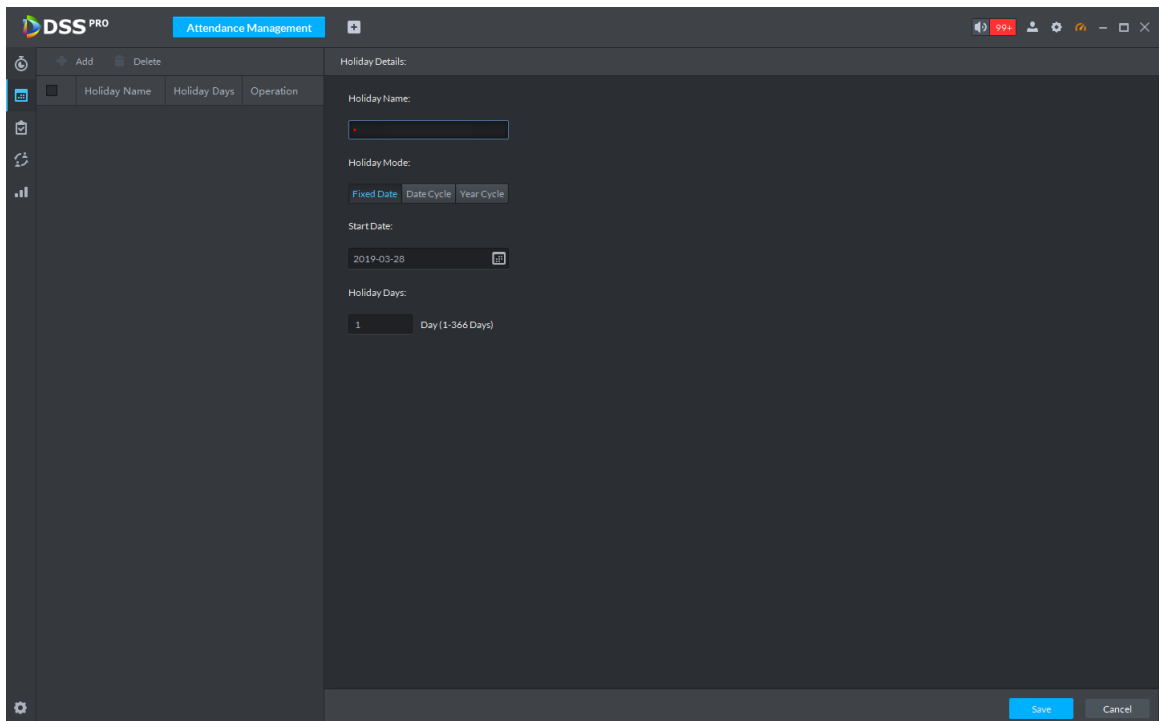
Step 1 Click  on the interface of **Attendance Management**.

Figure 4-422 Holiday management



Step 2 Click  at the upper-left corner of the interface.

Figure 4-423 Add a holiday



Step 3 Set holiday details, three modes available.

Table 4-71 Holiday parameters

Holiday mode	Description
Fixed Date	Set some specific date as holiday. For example, set June 7, 2019 (Dragon

Holiday mode	Description
	Boat Festival) as holiday, and lasts for 1 day, then set Start Date as June 7, 2019 and Holiday Days as 1.
Date Cycle	If the holiday is the fixed weekday of some week in some specific month, and it cycles according to year, which can be configured as date cycle. For example, if you want to set Mother's Day as holiday, and it lasts for 1 day, then you can set Start Date as the second Sunday in May, and Holiday Days as 1.
Year Cycle	If the holiday is fixed date and it cycles according to year, which can be configured as year cycle. For example, set New Year's Day as holiday, and it lasts for 1 day, then you can set Start Date as January 1 and Holiday Days as 1.

Step 4 Click **Save**.

4.22.3.6 Setting Attendance Shift

Set attendance shift according to attendance period, used for department and personnel shift.


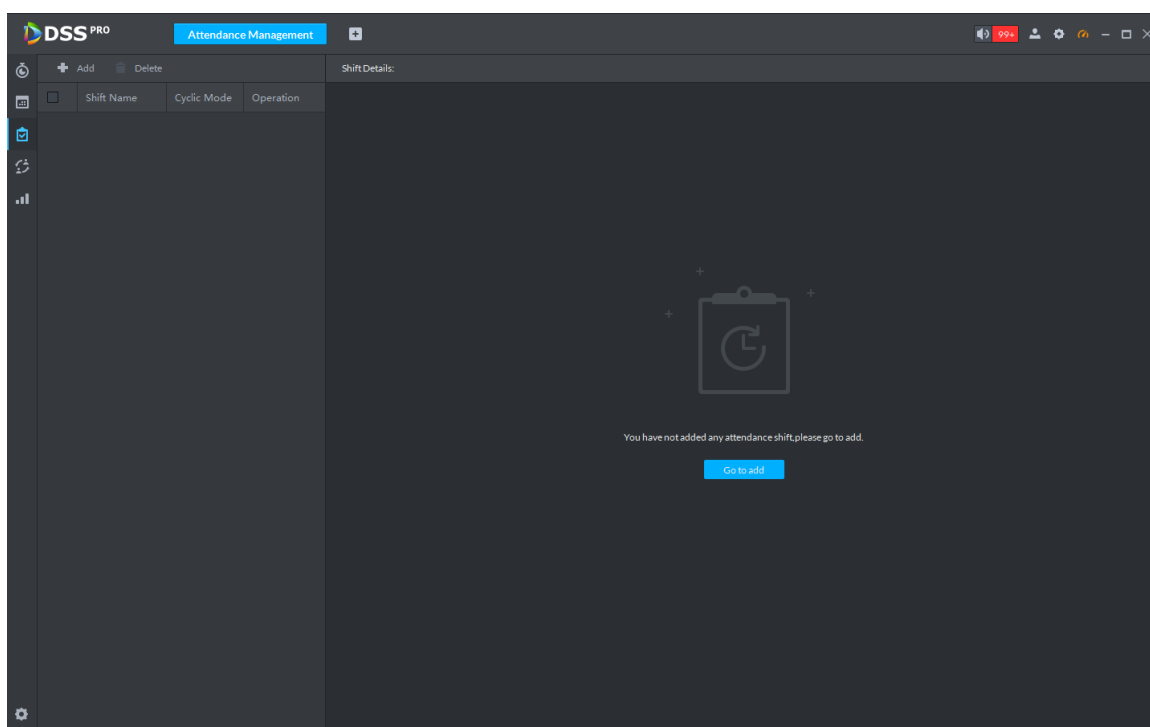
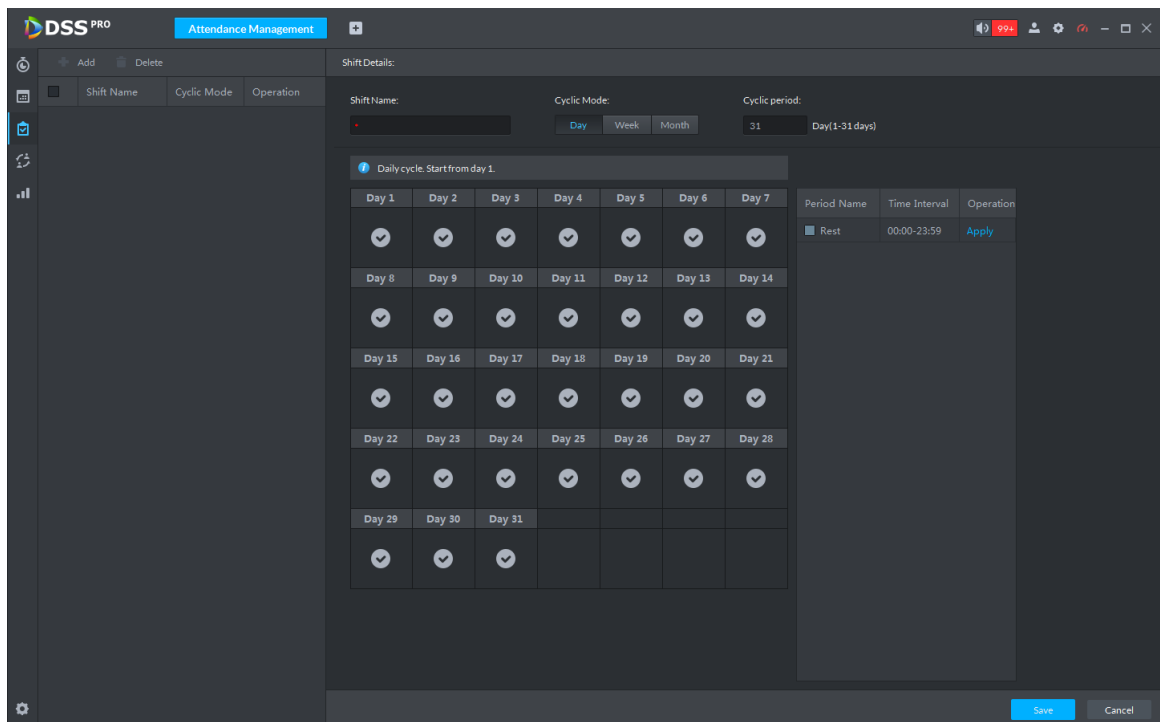
Step 1 Click  on the interface of **Attendance Management**.

Figure 4-424 Attendance shift



Step 2 Click  on the upper-left corner of the interface.

Figure 4-425 Configure attendance shifts (1)



Step 3 Set shift details, select date, click **Apply** to arrange attendance period for date.

Figure 4-426 Configure attendance shifts (2)

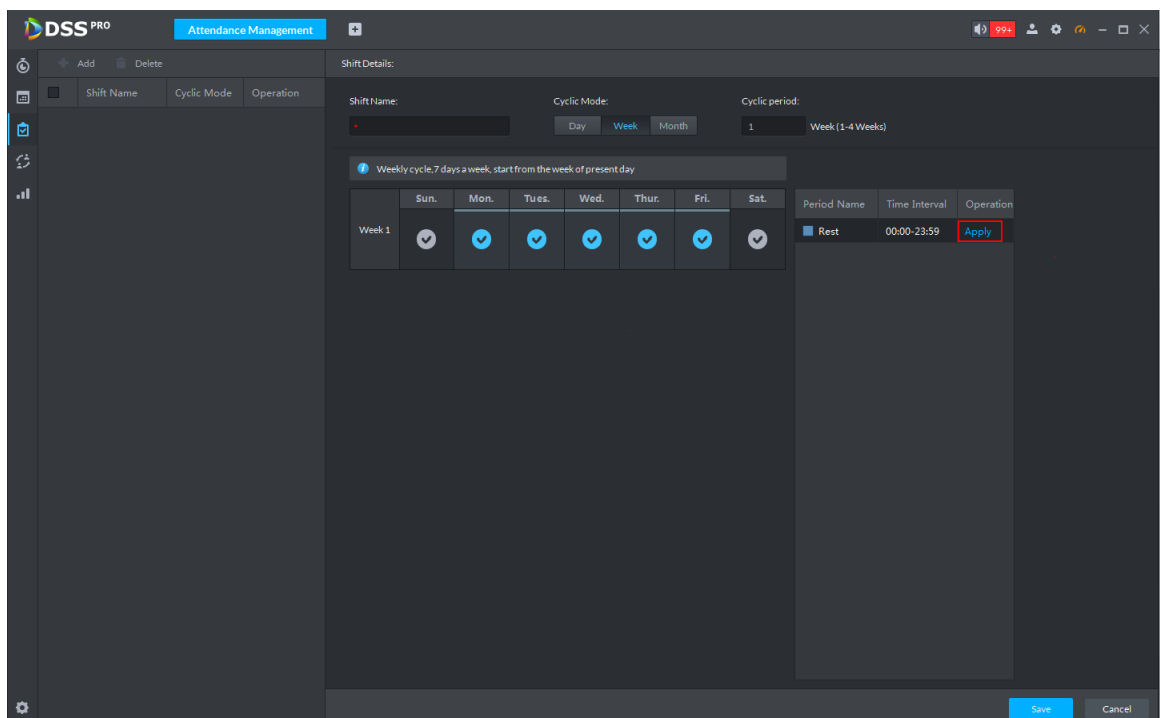


Table 4-72 Attendance shift parameters

Parameter	Description
Shift name	Custom period name, used to recognize shift.

Parameter	Description
Cycle mode	Day: Start cycle from the first day, cycle period can be set as any number from 1 to 31 according to day. For example, if you set 2, then the cycle period is 2 days.
Cycle period	Week: There are 7 days in a week by default, it starts cycle from Sunday, and so Sunday is required to be set as the first day. Cycle period can be set as any number from 1 to 4. For example, if you set 2, then 2 weeks can be a cycle period. Month: There are 31 days in a month by default, it starts cycle from the current day (If the date does not exist, then it will be deleted during shift arrangement), cycle period can be set as any number from 1 to 3 according to month. For example, if you set 2, then 2 months can be a cycle period.

Step 4 Click **Save** to save shift configuration.



Delete in-use attendance shift: Go to the **Personnel Shift Arrangement** interface, check if there are shifts to be deleted; if yes, remove the relation, and then delete.

4.22.3.7 Shift Management

Make shifts for personnel or department, meanwhile it makes temporary shift for personnel. The shift priority is temporary shift > holiday > personnel shift > department shift.

4.22.3.7.1 Personnel/Department Shift Arrangement

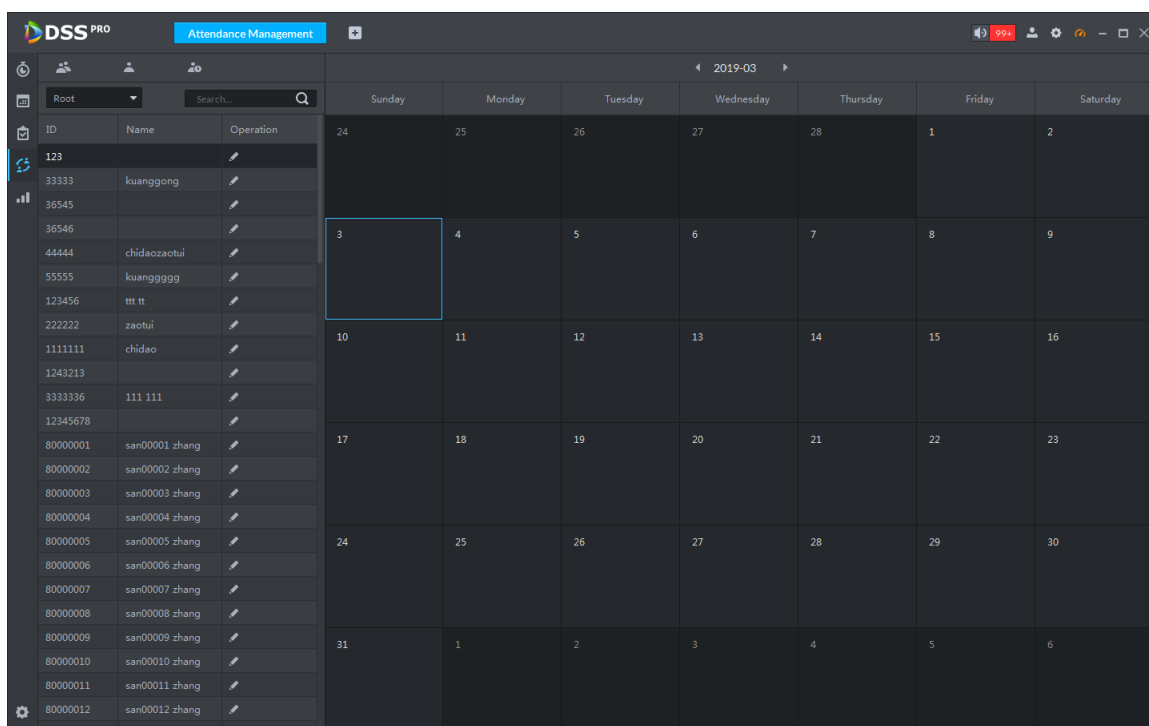
The operations over both personnel shift and department shift are similar, in this chapter; it takes personnel shift as an example to introduce configuration.



- If you configure department shift, then all the personnel of the department need to conform to the shift.
- If both personnel and department are configured with shift, then the latest personnel shift shall prevail. For example, after configuring the personnel shift, and the corresponding department is configured as well, then personnel shift is based on the latest department shift.
- If the department where new personnel belong to is configured with shift, then the shift of new personnel should conform to department shift.

Step 1 Click  on the interface of **Attendance Management**.

Figure 4-427 Personnel shift arrangement (1)



Step 2 Click  on the upper-left corner of the interface.





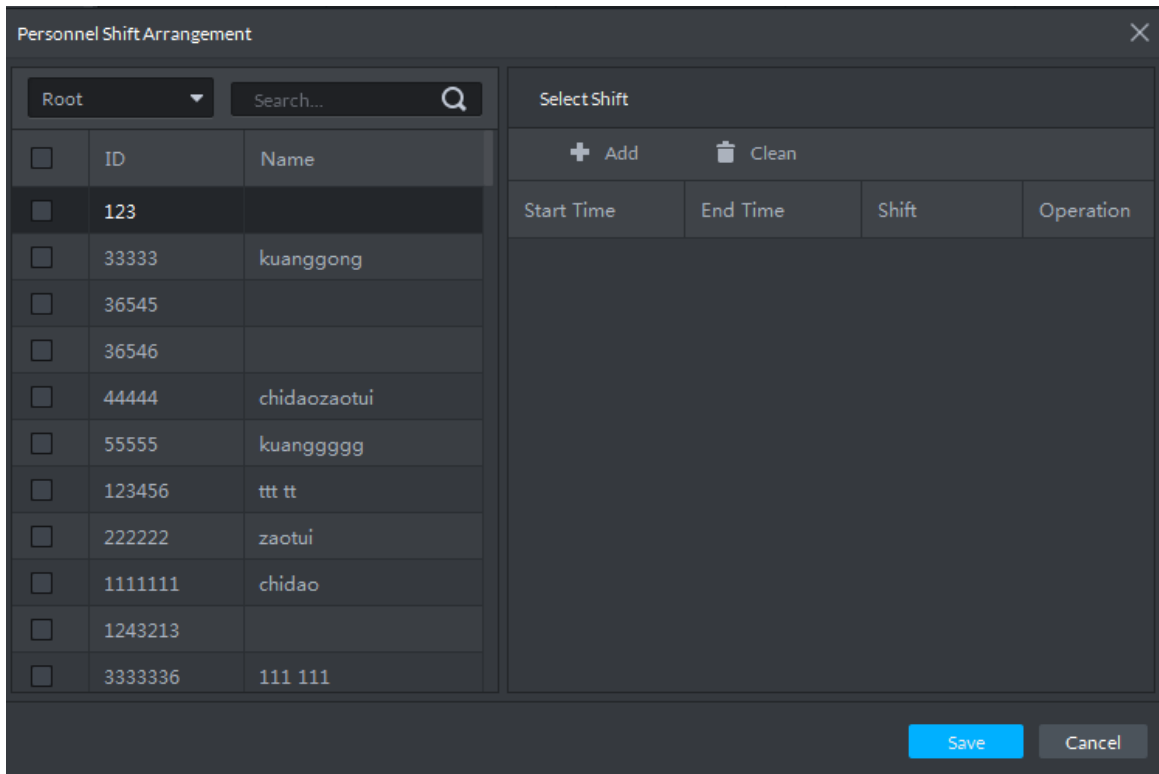
- If you need to configure shift for department, click  on the upper-left corner and enter the interface of department shift arrangement. The following operation is the same as personnel shift arrangement.
- On the interface of personnel shift arrangement, select personnel and view the shift situation.
- Click  next to the personnel and you can view the shift details.

Figure 4-428 Personnel shift arrangement (2)




Step 3 Select shift personnel, click  to add shift information.

Figure 4-429 Select shifts

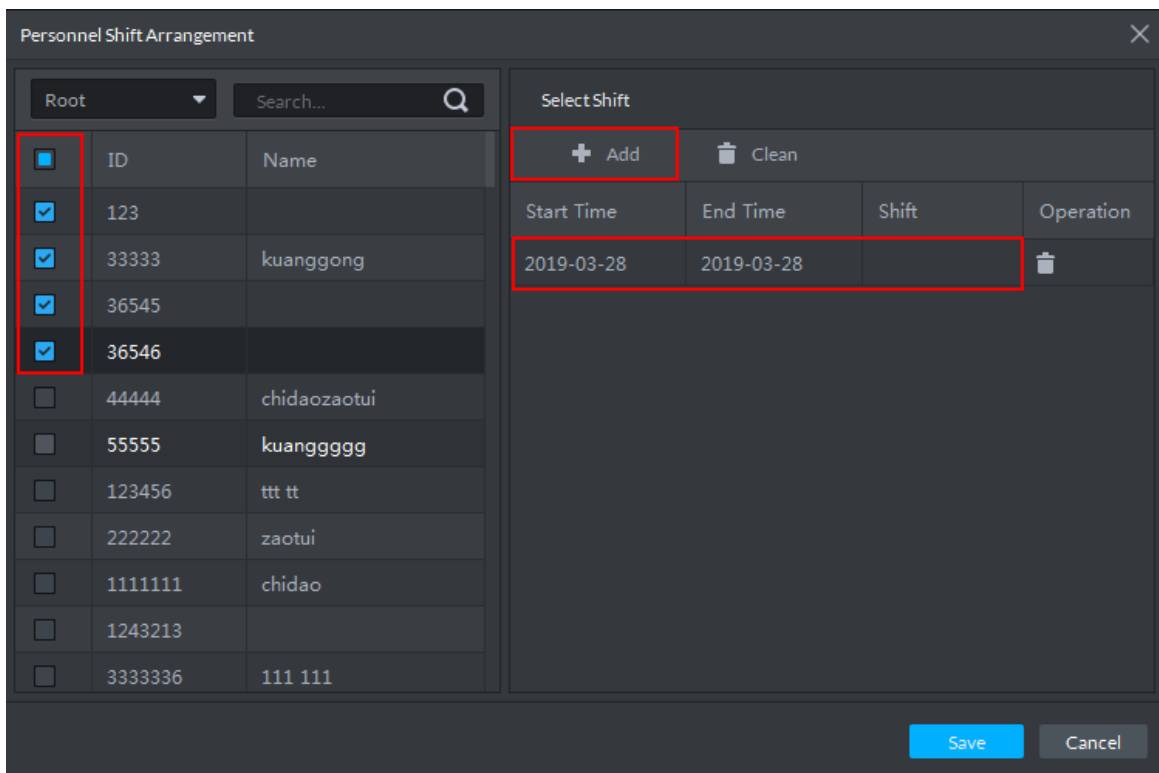


Table 4-73 Shift parameters

Parameter	Description
Start time	Set start date and end date of personnel shift. Click the column of Start Time and display calendar, select date and time, and then click OK to complete date setting
End time	
Shift	Select needed shifts. Shift range means all the attendance shifts set in "4.22.3.6 Setting Attendance Shift."

Step 4 Click **Save**.

4.22.3.7.2 Temporary Shift

Temporary shift is needed when work changes temporarily.


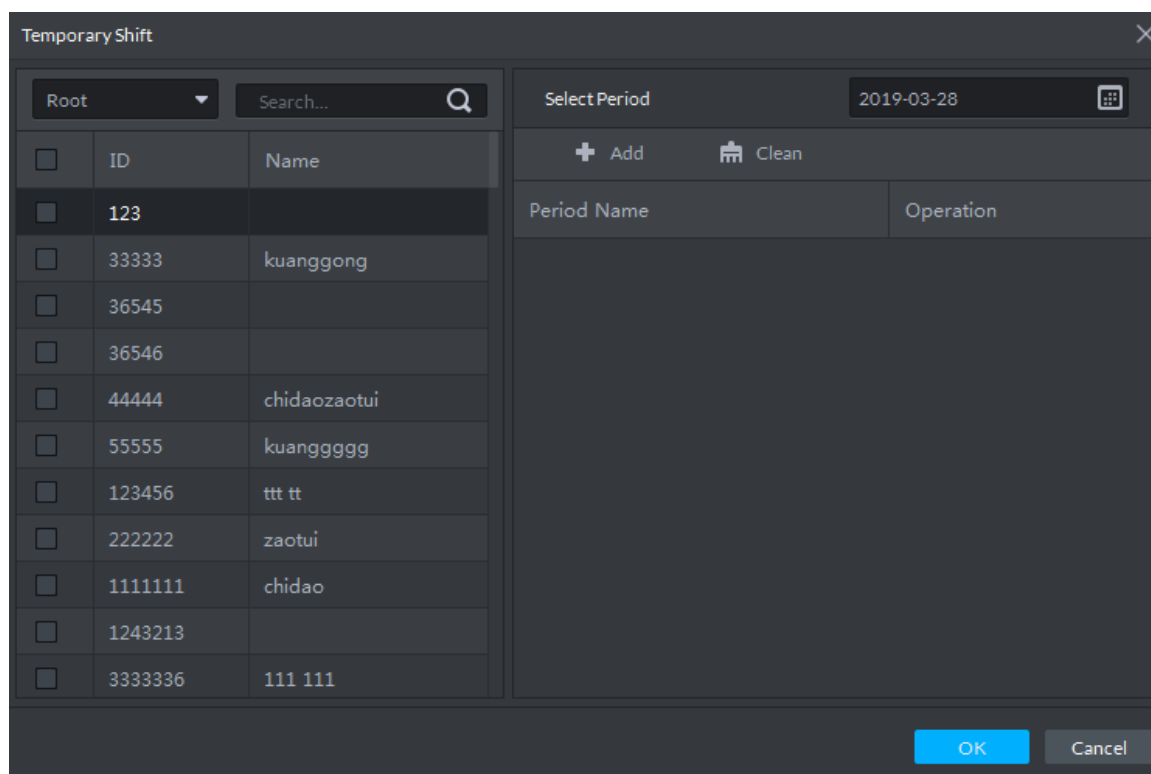
Step 1 Click  on the interface of **Attendance Management** or select personnel on the right, Double-click date on the left.

Figure 4-430 Temporary shift interface




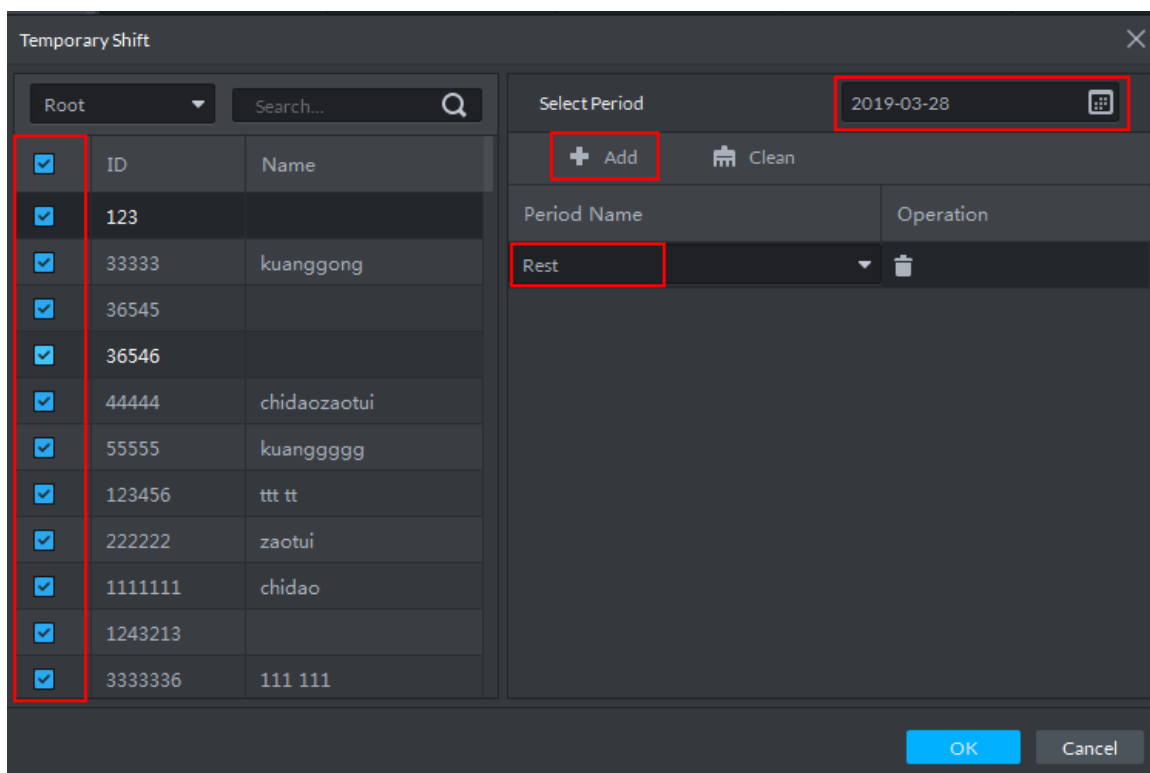
Step 2 Select personnel and date, click  and select temporary attendance period. You can add max. 2 attendance periods and 1 free attendance period.

Figure 4-431 Temporary shift



Step 3 Click **OK** and save shift information.



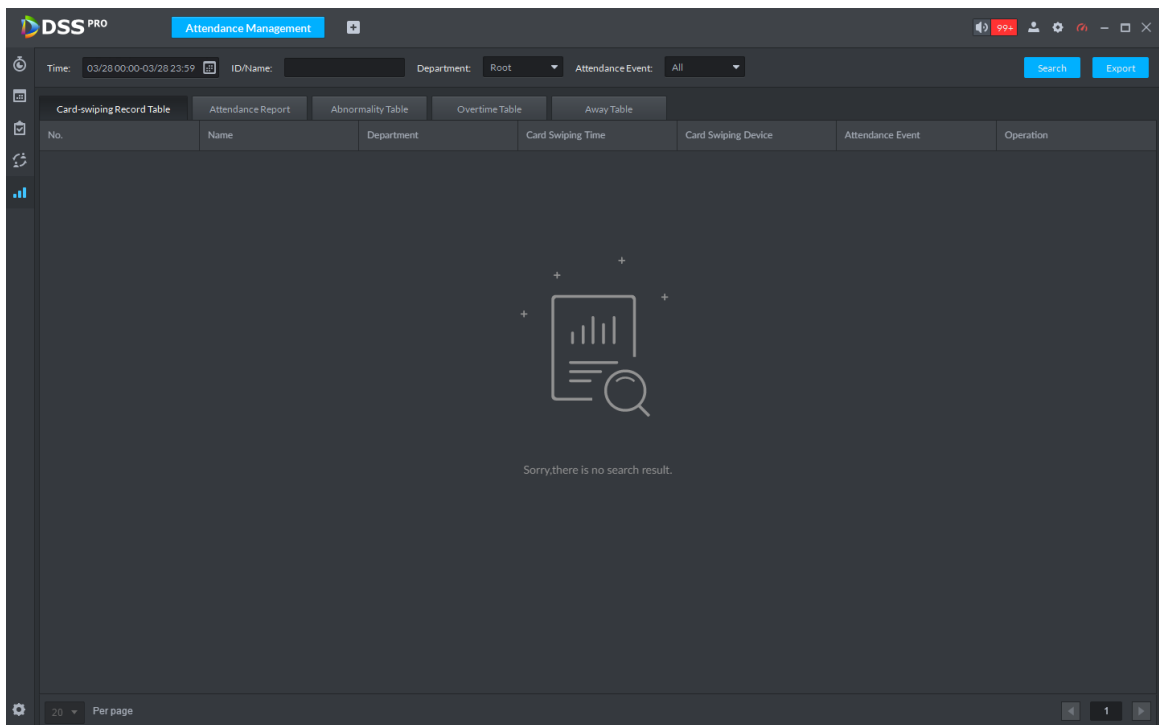
Temporary shift can be deleted, right-click the date which is configured with temporary shift, and delete temporary shift according to system prompt.

4.22.4 Viewing Attendance Report

View attendance data, displayed in the form of report, including card swiping record table, attendance report, abnormality table, overtime table and away table.

Step 1 Click  on the interface of **Attendance Management**.

Figure 4-432 Attendance report



Step 2 Click corresponding tab, set search condition, click **Search**.


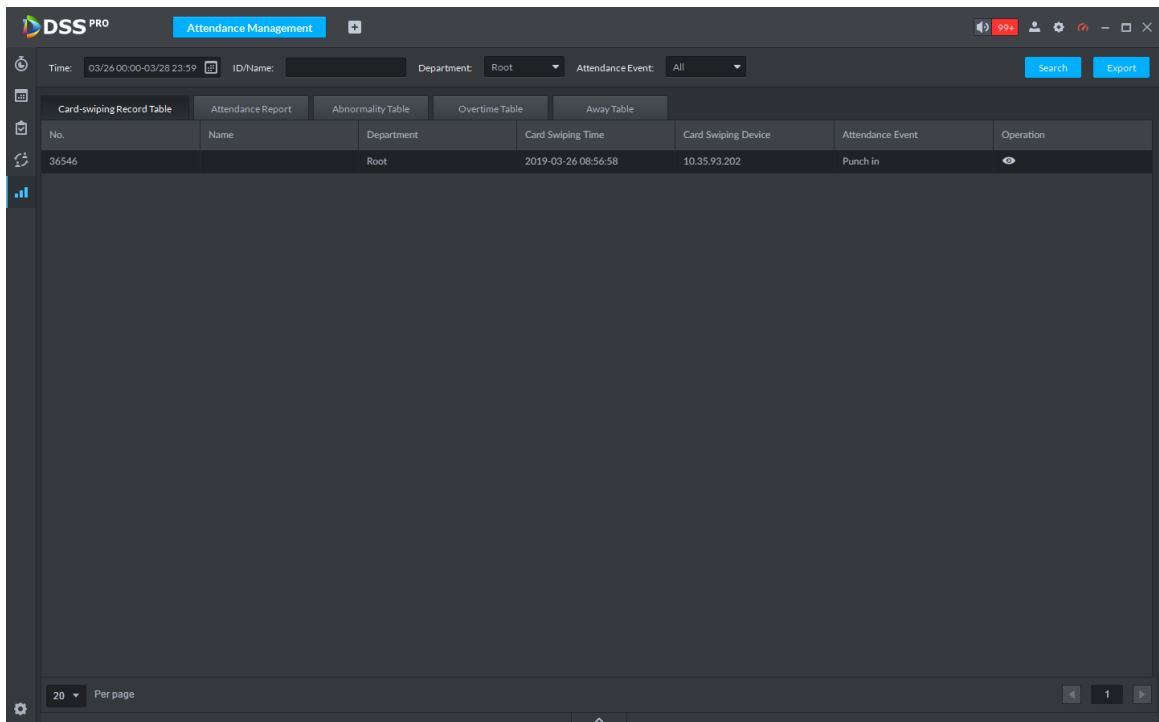
- Card swiping records. Click  and view more details of the person who swipes card.

Figure 4-433 Card-swiping records



- Attendance report

Figure 4-434 Attendance report

DSS PRO Attendance Management

Time: 03/26 00:00-03/28 23:59 ID/Name: Department: Root Search Export

Card-swiping Record Table Attendance Report Abnormality Table Overtime Table Away Table

Date	No.	Name	Department	Sign-in Time	Sign-out Time	Week	Away Duration	Working Period	Overtime Duration
2019-03-26	36546		Root	08:56		Tuesday	0.0 Hour(s)	0.0 Hour(s)	0.0 Hour(s)

20 Per page 1

- Abnormity table

Figure 4-435 Abnormity table

DSS PRO Attendance Management

Time: 03/26 00:00-03/28 23:59 ID/Name: Department: Root Abnormal Type: All Search Export

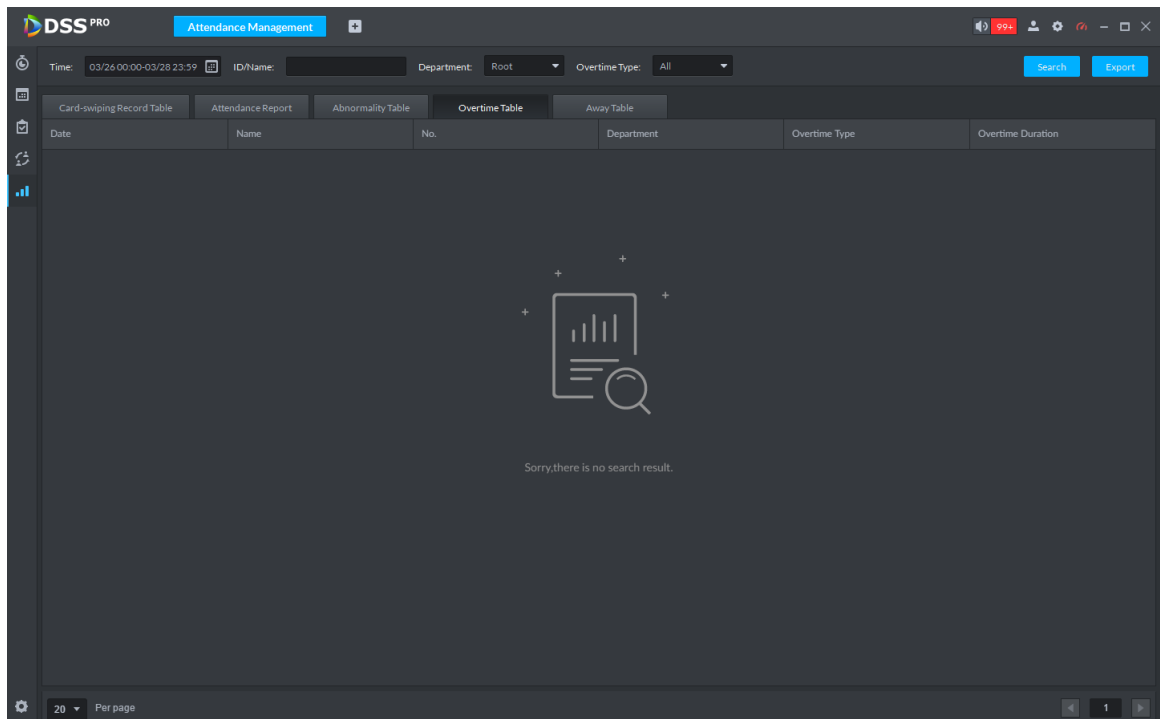
Card-swiping Record Table Attendance Report Abnormality Table Overtime Table Away Table

Date	No.	Name	Department	Sign-in Time	Sign-out Time	Abnormal Type
2019-03-26	36546		Root	08:56		Late

20 Per page 1

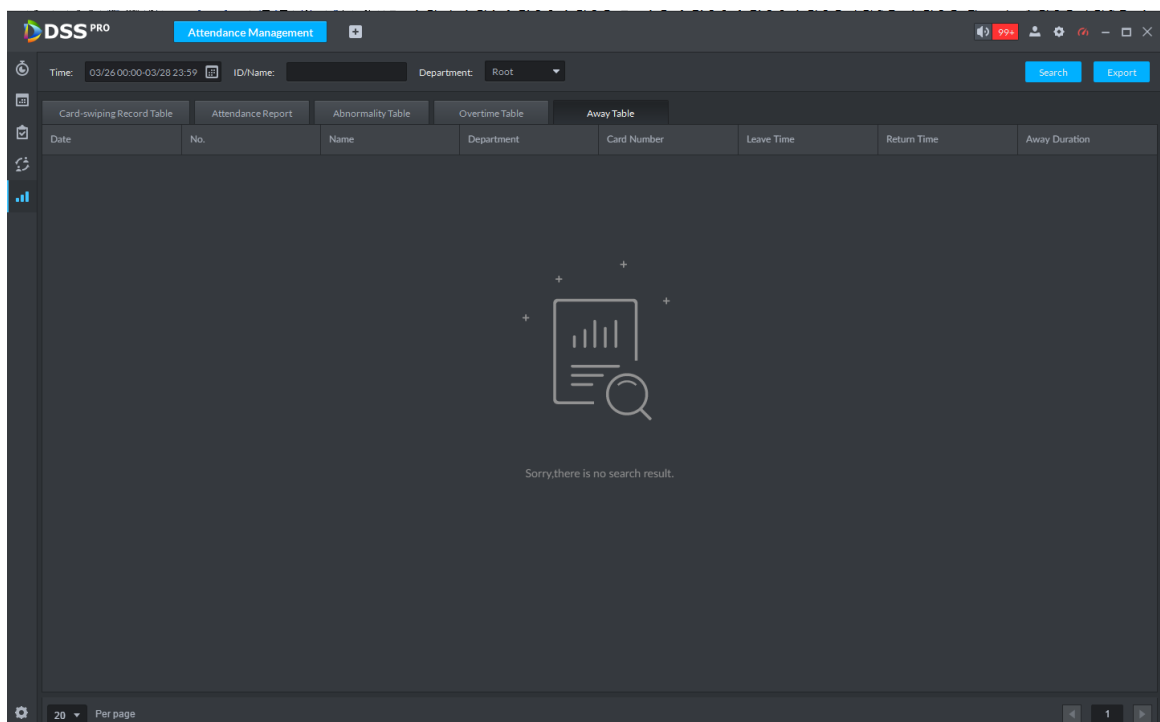
- Overtime table

Figure 4-436 Overtime table



- Away table

Figure 4-437 Away table



4.23 Visitor Management

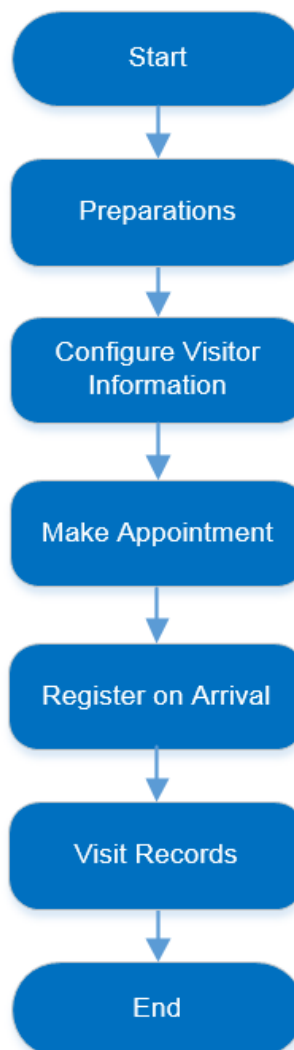
After appointment is made on platform, and visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves.

4.23.1 Preparations

- Access control devices have been added into the system. For details, see "3.4 Managing Device."
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."

4.23.2 Business Flow

Figure 4-438 Visitor management business flow



4.23.3 Configuring Visit Settings

Configure the default parameters of visit, including, automatic visit, automatic leave, and default permissions.

Step 1 Log in to the client, click , and then select **Visitor Management**.

Step 2 Click .

Step 3 Set parameters.

Figure 4-439 Set visit parameters

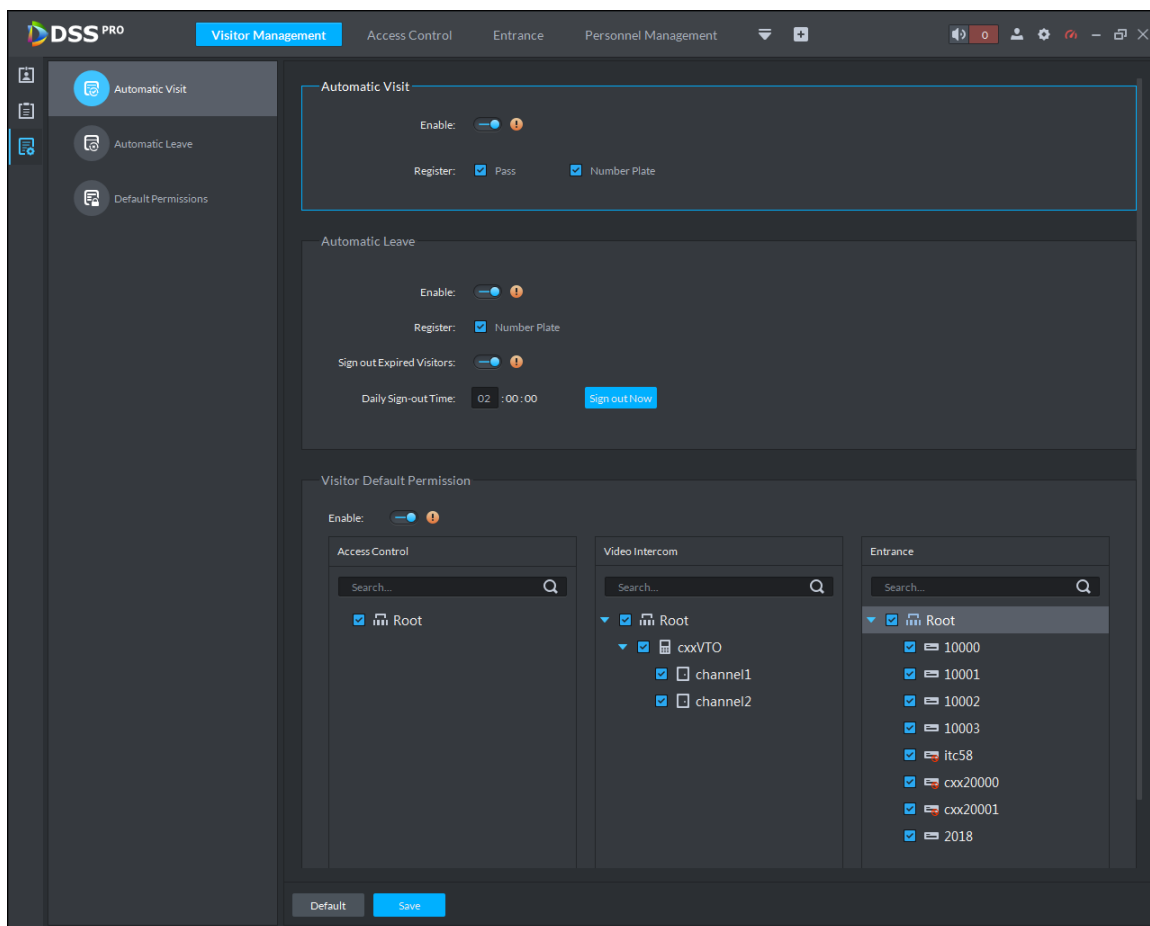



Table 4-74 Description

Parameter		Description
Automatic Visit	Enable	If enabled, in the appointed period, the visitor can show the pass to get in or drive in (based on ANPR), without having to register. Beyond the appointed period, the visitor still needs to register.
	Register	
Automatic Leave	Enable	After Automatic Leave and Number Plate enabled, in the valid period, the visitor can leave without registering.
	Register	
	Sign out Expired Visitors	The system automatically signs out the expired visitors at the defined time point.
	Daily Sign-out Time	For those who have not visited as appointed before the daily automatic sign-out time, the appointments will be cancelled.

Parameter		Description
	Sign out Now	Sign out the expired visitors right now.  For those who have not visited as appointed, the appointments will be cancelled.
Visitor Default Permissions	Enable	Set the default access permissions for visitors.
	Access Control	
	Video Intercom	
	Entrance	

Step 4 Click **Save**.

4.23.4 Visitor Appointment

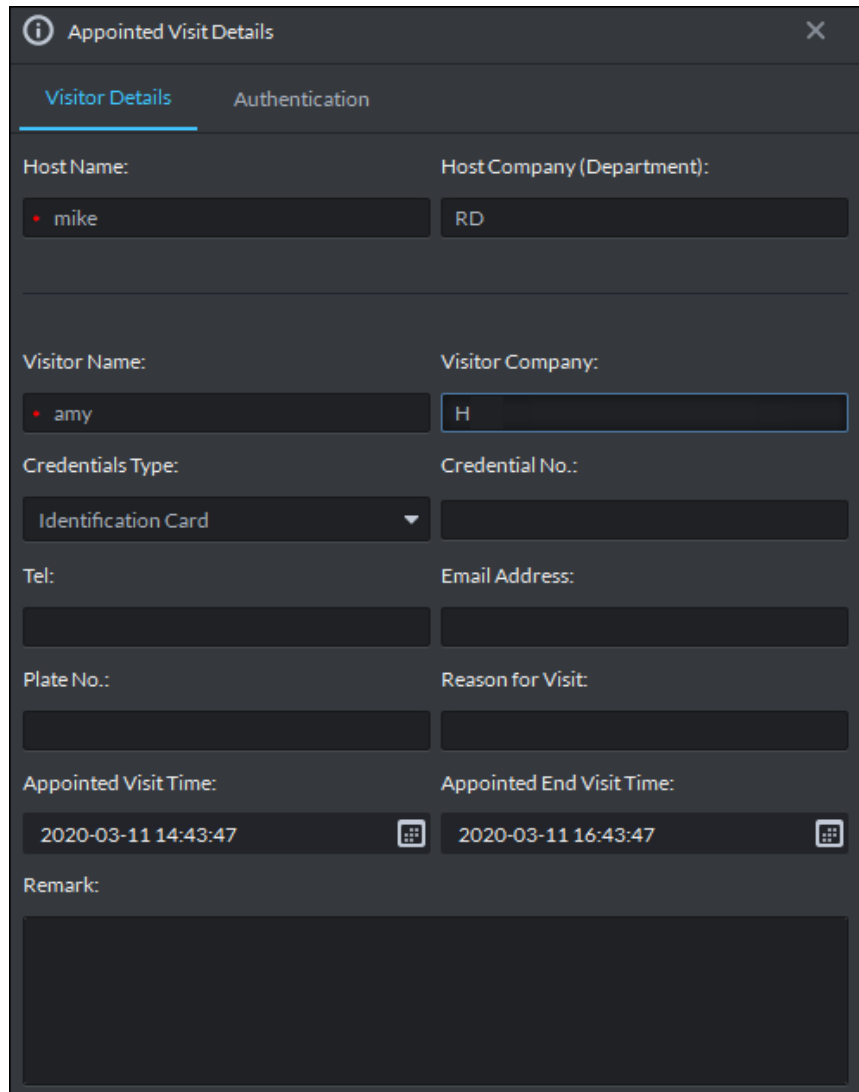
Register visitor information on the platform.

Step 1 Log in to the Control Client, click , and then select **Visitor Management**.

Step 2 Click **Appointment Registration**.

Step 3 Click the **Visitor Details** tab, enter the information of the visitor and the one to be visited.

Figure 4-440 Appointment registration



i Appointed Visit Details
✕

Visitor Details
Authentication

Host Name:

Host Company (Department):

Visitor Name:

Visitor Company:

Credentials Type:

Credential No.:

Tel:

Email Address:

Plate No.:

Reason for Visit:

Appointed Visit Time:

Appointed End Visit Time:

Remark:

Step 4 (Optional) Click the **Authentication** tab, select the room number to be visited, and then click **Generate** to generate the QR code of the pass.



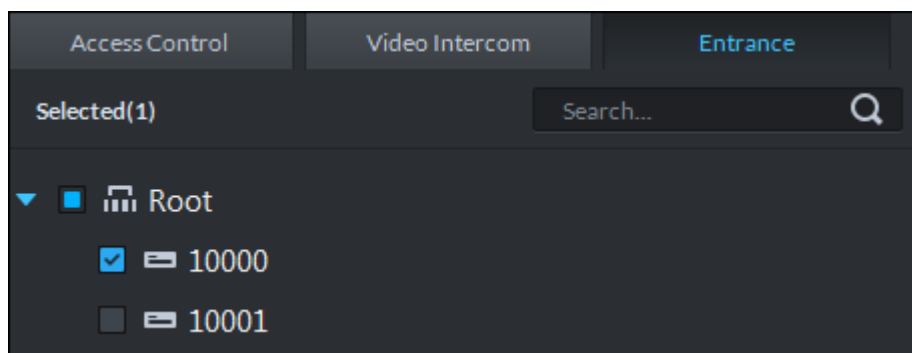
You can click  to download the QR code, and click  to send it to the visitor by email.

Figure 4-441 Visitor authentication



Step 5 Click the **Authorize** tab to select the access channels for the visitor.

Figure 4-442 Authorize visitor



Step 6 Click **OK**.

4.23.5 Checking In

When an appointed visitor comes to visit, you need to confirm person information and give access permission. On-site registration is supported when there is a walk-in visitor. Visitors can get access by swiping card or face recognition.

Step 1 Log in to the Control Client, click  and then select **Visitor Management**.

Step 2 Click .

Step 3 Record visitor details.

- 1) Go to the visit registration information interface.
 - ◇ If a visitor is appointed


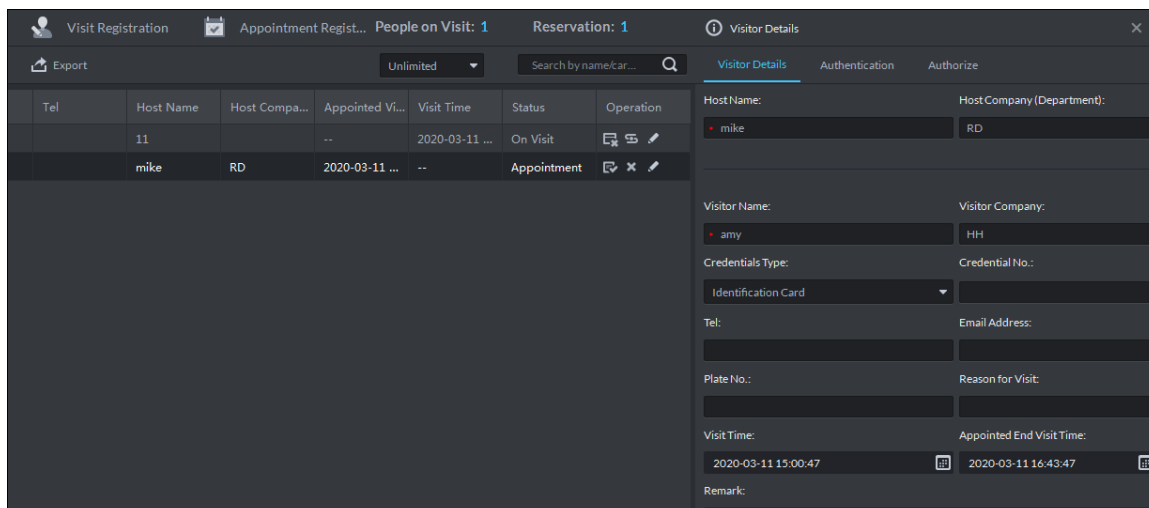
- Find the visitor information, and then click .
- ◇ If a visitor is not appointed
Click **Visit Registration**.
- 2) Confirm or enter visitor information.

Figure 4-443 Visit information



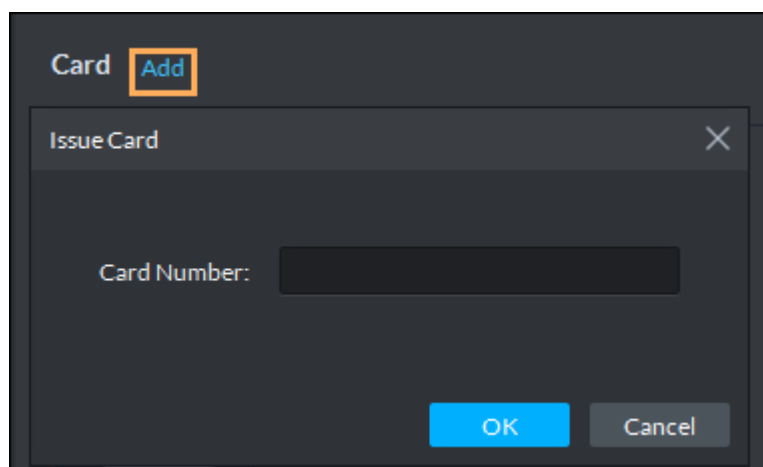
Step 4 Click the **Authorization** tab, and then set authorization information.

- 1) Select the room number.
- 2) Issue cards.

You can issue cards by entering card No. manually or by using a card reader. Card No. supports 8 and 16 digits. If the card No. is less than 8 or 16 digits, the platform adds 0 by default to meet the digit number requirement. For example, if you enter card number 8004, then the platform will change it to 00008004. If you enter card number 1000056821, then the platform will change it to 0000001000056821.

- ◇ Issue cards by entering card No. manually
Click **Add** next to **Card**, enter the card number, click **OK**.

Figure 4-444 Issue card



- ◇ Issue card by using a card reader


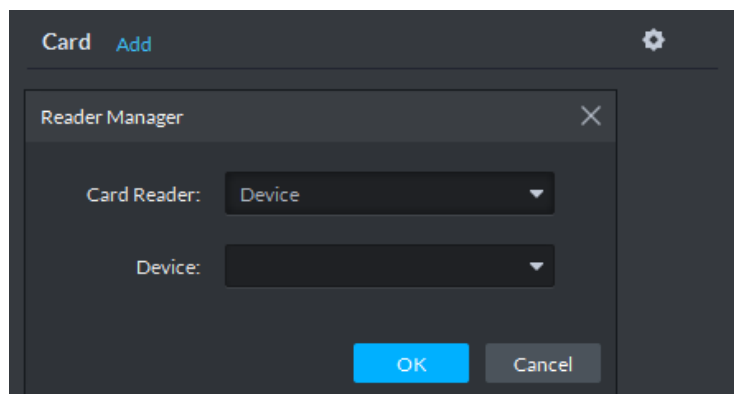
Click , select a card reader or device, and then click **OK**. Swipe card on reader or device, and card is issued.

Figure 4-445 Reader manager



- 3) Set face pictures. Hover over the face snapshot area, click **Upload Picture** to select a picture or click **Snapshot** to take a photo.


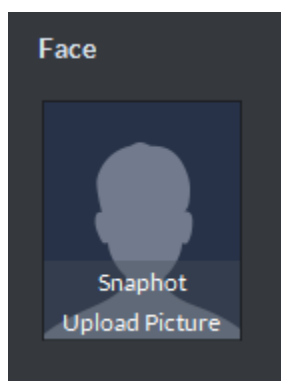


Click , and then you can select snapshot camera, pixel format, resolution and set image quality. This is only effective with the current client.

Figure 4-446 Take a face snapshot

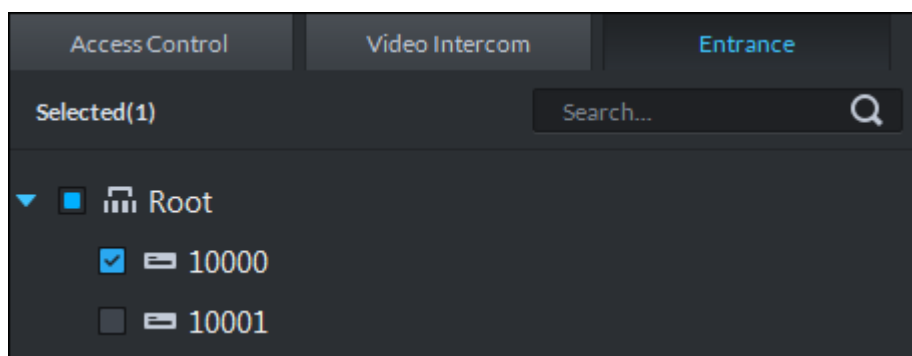


4. Click **Generate** to generate the QR code pass.

You can click  to download the QR code, or click  to send the code to the visitor by email.

Step 5 Click the **Authorize** tab to select the access channels for the visitor.

Figure 4-447 Authorize visitor



Step 6 Click **OK**.



- Click to end visit.
- Click to view visitor card swiping records.

4.23.6 Checking Out

When visitors are leaving, close their access permissions.

Step 1 On the **Visitor Management** interface, click .

Step 2 Find the appointment record of the visitor, and then click .

Figure 4-448 End visit

Step 3 Click **OK** to close the access permission.

If you have issued a card to visitor, Make sure that the card is returned when the visitor leaves.

4.23.7 Searching for Visit Records

Search for visit records, and view visitor details and the card swiping records.

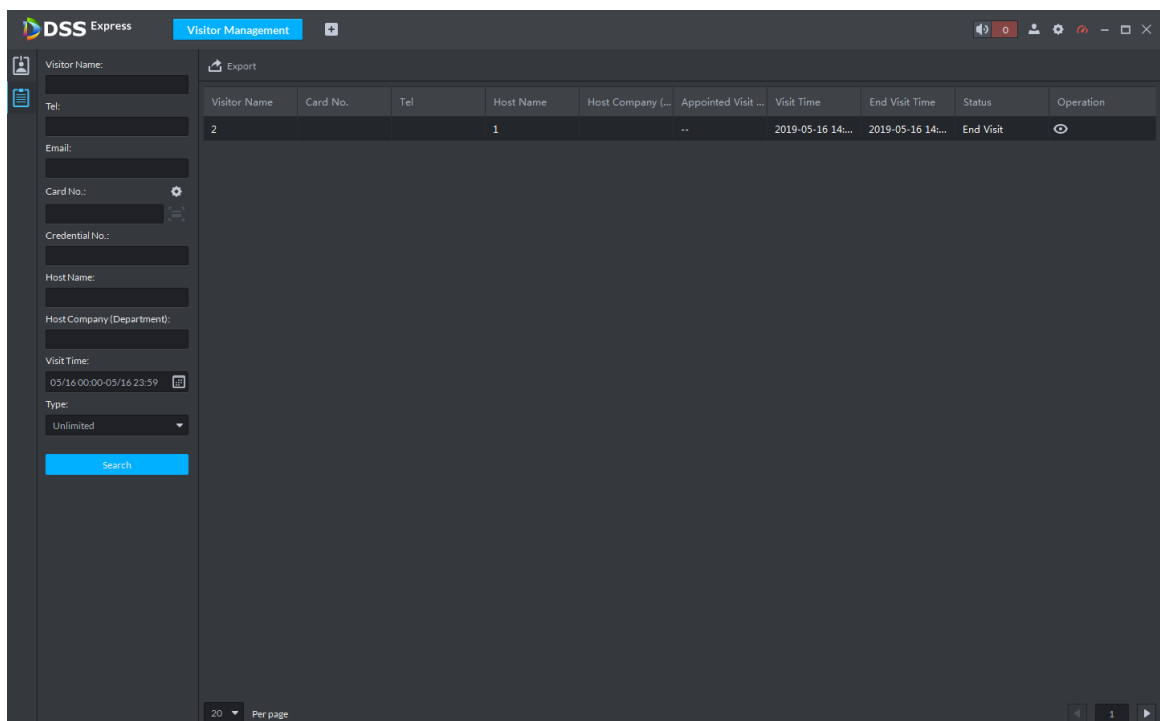
Step 1 On **Visitor Management** interface, click

Step 2 Set search conditions, and then click **Search**.
The results are displayed.



In addition to entering card number manually, you can also click , select a card reader and then get the card number by swiping card.

Figure 4-449 Search visit result



Step 3 Click to view visitor details and card swiping records.

4.24 Business Intelligence

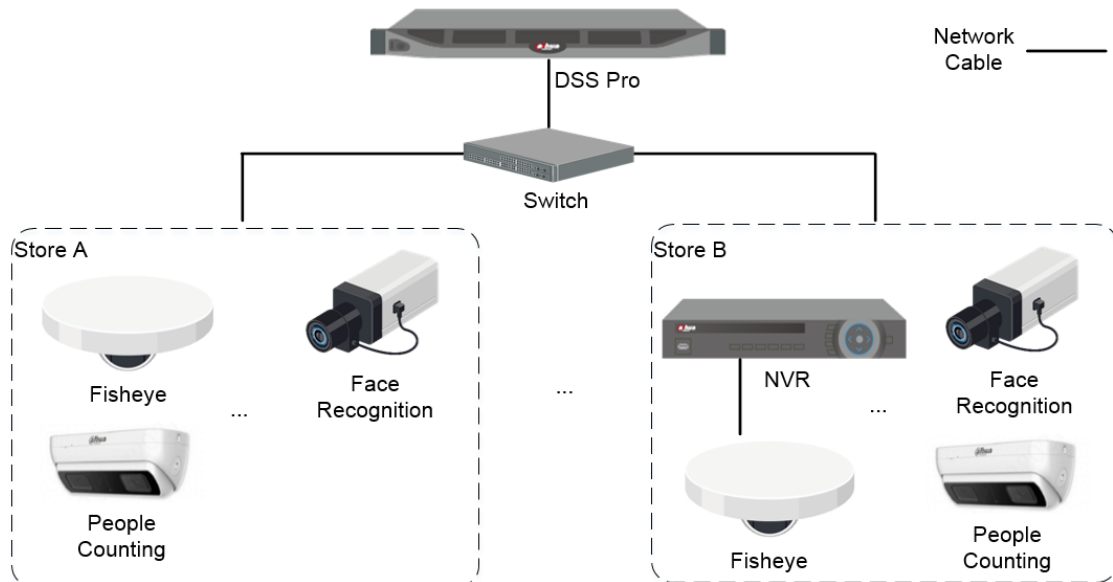
Analyze customer flow in your store so that you can optimize your business strategy accordingly.

- Entrance analysis
View the entry and exit numbers of customers.
- Customer analysis
Analyze customer flow by gender and age.
- Indoor analysis

View customer numbers and stay numbers on each floor.

4.24.1 Typical Topology

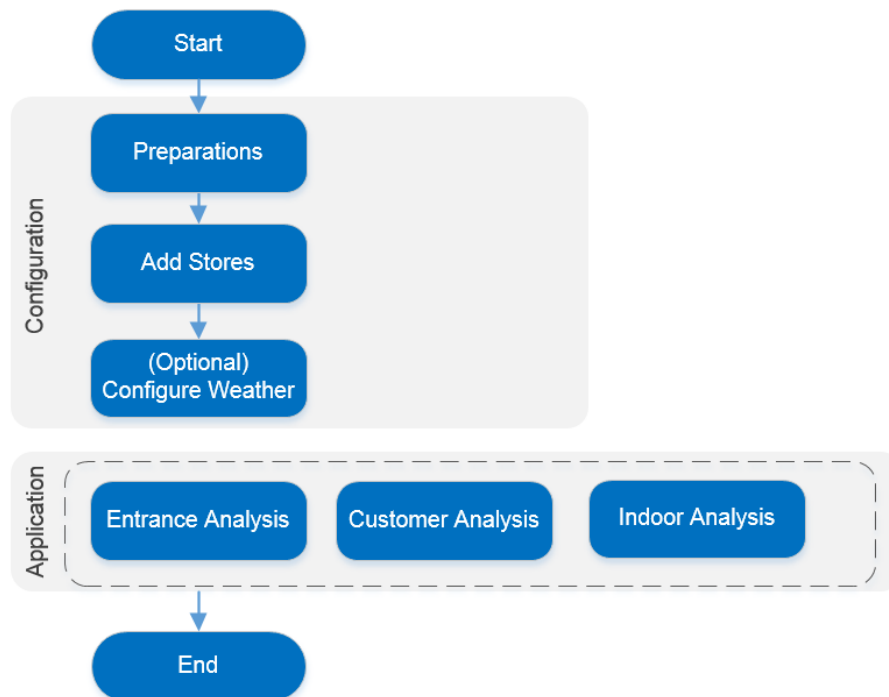
Figure 4-450 Business intelligent typical topology



- Fisheye and people counting cameras count people numbers and provide full views of areas.
- Face recognition cameras detect and recognize people faces.
- (Optional) NVR can be used for managing fisheye camera.
- The platform centrally manages the devices and provides videos and record search.

4.24.2 Business Flow

Figure 4-451 Business intelligence business flow



4.24.3 Configuring Business Intelligence

4.24.3.1 Preparations

Make sure that the following preparations have been made:

- Fisheye, face recognition, and people counting cameras are well deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding cameras on the **Device** interface of Web Manager, select **Encoder** for device category.

Figure 4-452 Add device


- After the fisheye camera or people counting camera is added, click , and then select **People Counting for Features.**

Figure 4-453 Edit camera features (1)

Video Channel	Name	Camera Type	Features	SN	KeyBoard Code
Alarm Input	Channel0	Fixed Camera	Fisheye, People Cou...		



- After the face recognition camera is added, click , and then select **Face Detection** or **Face Recognition** for **Features**.

Figure 4-454 Edit camera features (2)

Video Channel	Name	Camera Type	Features	SN	KeyBoard Code
Channel0	Channel0	Fixed Camera	Face Detection		

4.24.3.2 Adding Stores

- Step 1** Log in to the Web Manager, click , and then select **Store Management**.
- Step 2** Click **Add** to open the **Add Store** interface.
- Step 3** Name the store, select an organization, and then click **Upload Map** to upload a store map.
- Step 4** Select the fisheye camera, drag it from the device tree to the map, and then select **People Counting** for **Camera Type**.

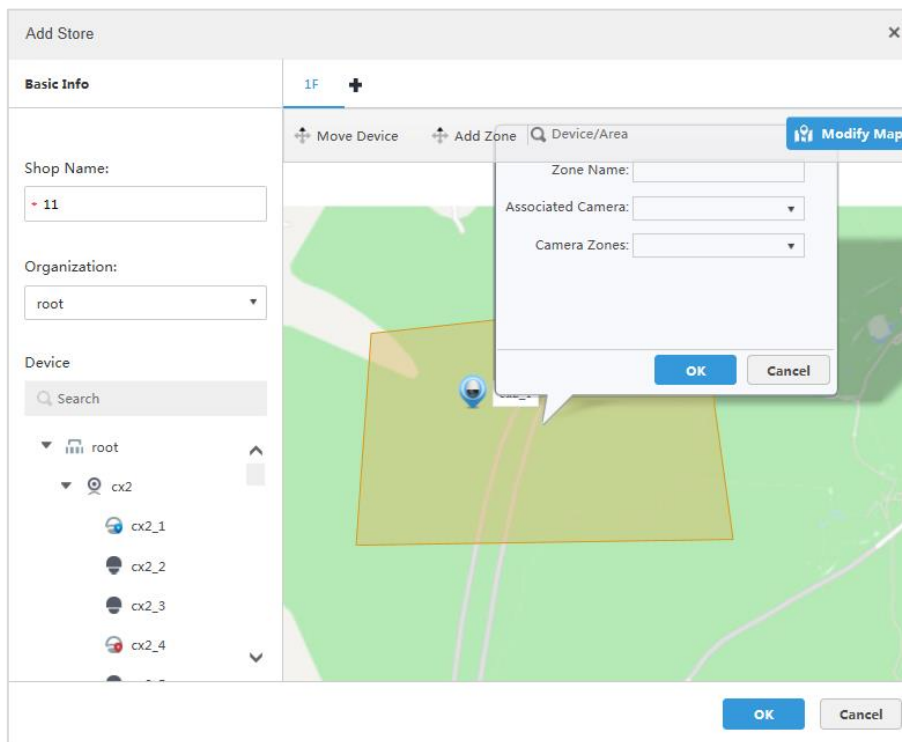


Double-click the camera on the map to modify camera type.

- Step 5** Draw detection regions.
Support passenger flow analysis region and angle analysis region.
- Passenger flow analysis.
 - Select **Add Zone > Passenger flow Analysis**, and then draw a region on the map.
 - Set a zone name, select a fisheye camera and the camera zone, and then click **OK**.

In this way, the fisheye camera zone and the store area is bound, and then data displayed in the store areas come from the bound fisheye camera zone. After the configuration, store information is displayed in the store list. See Figure 4-457.

Figure 4-455 Configure passenger flow zone



- Angle analysis
 - Analyze the number of people going to different shelves inside the store.
- 1) Select **Add Zone > Passenger flow Analysis**, and then draw a zones on the map according to the people flow directions.
- 2) Set a zone name, select a fisheye camera and the camera zone, adjust the direction, and then click **OK**.

In this way, the fisheye camera zone and the store area is bound, and then data displayed in the store areas come from the bound fisheye camera zone. After the configuration, store information is displayed in the store list. See Figure 4-457.

Figure 4-456 Configure angle analysis zone

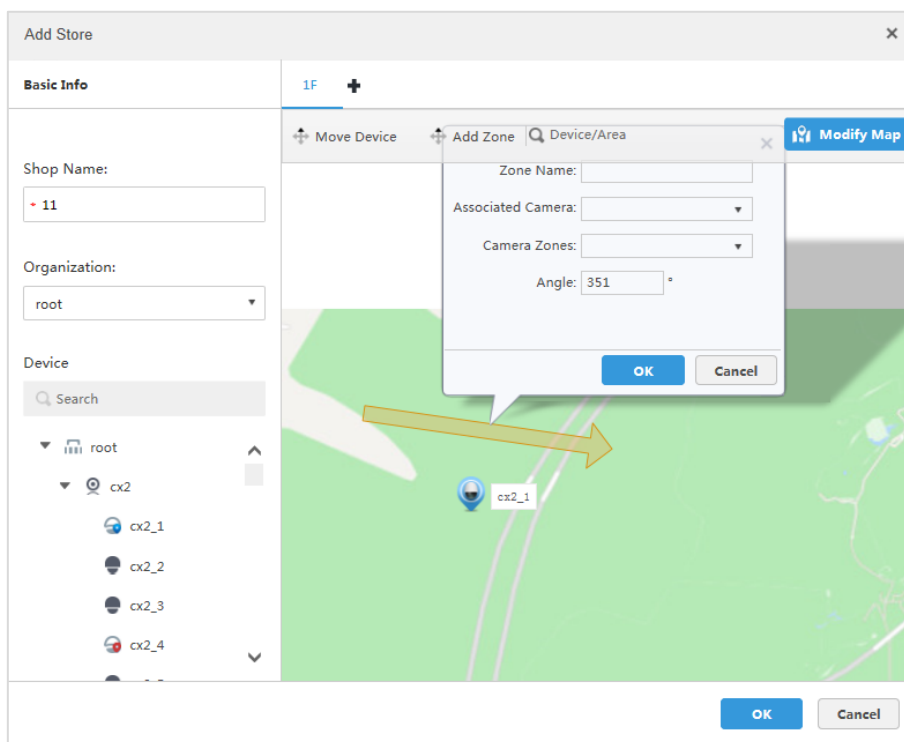
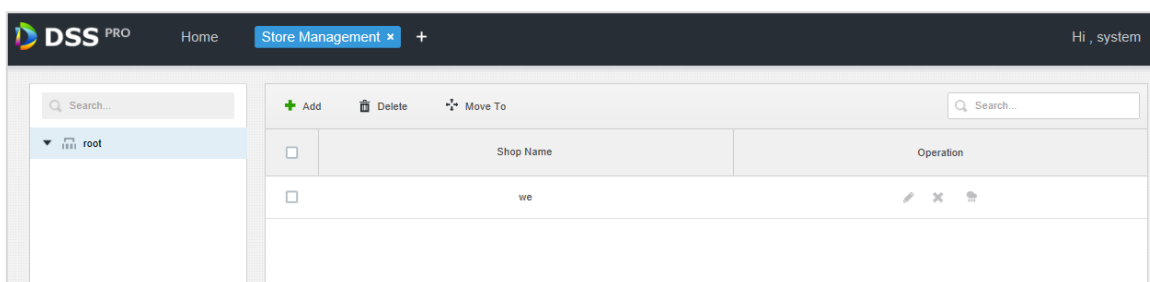


Figure 4-457 Store details



Step 6 (Optional) click **+**, add multiple floors, and then repeat the previous steps to complete adding the store maps.

Up to 10 floors can be added.

Step 7 Click **X**, follow the onscreen instructions, and then click **OK**.



Other Operations

- Edit a store

Click of a store, and then edit store details. Support modifying the map.

- Delete a store

◇ Select the stores to be deleted. Click . The stores are deleted in batches.

- ◇ Click , and then you can delete a single store.
- Move a store to another organization
 - Select the store, click , select an organization, and then click **OK**. The store is moved to the new organization.

4.24.3.3 (Optional) Configuring Weather Report



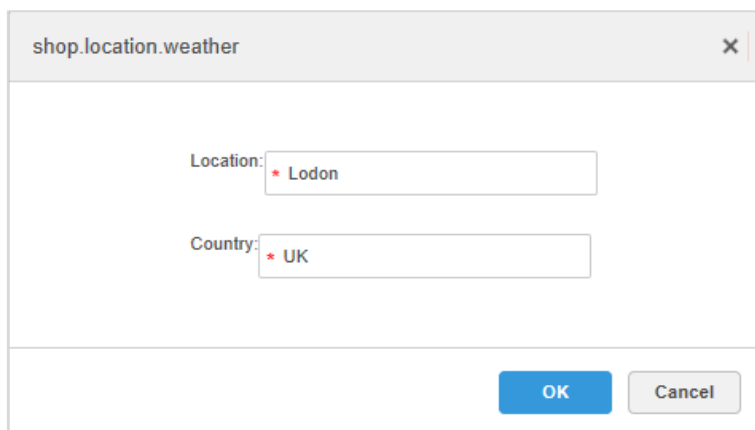
- Step 1 If your platform is connected to the Internet, you can view weather report.
- Step 2 Log in to the Web Manager, click , and then select **Store Management**.
- Step 3 Click  of a store in the store list, enter store location and country, and then click **OK**.

Figure 4-458 Configure weather parameters



The screenshot shows a dialog box titled "shop.location.weather" with a close button (X) in the top right corner. Inside the dialog, there are two input fields. The first is labeled "Location:" and contains the text "Lodon" with a red asterisk to its left. The second is labeled "Country:" and contains the text "UK" with a red asterisk to its left. At the bottom right of the dialog, there are two buttons: a blue "OK" button and a grey "Cancel" button.

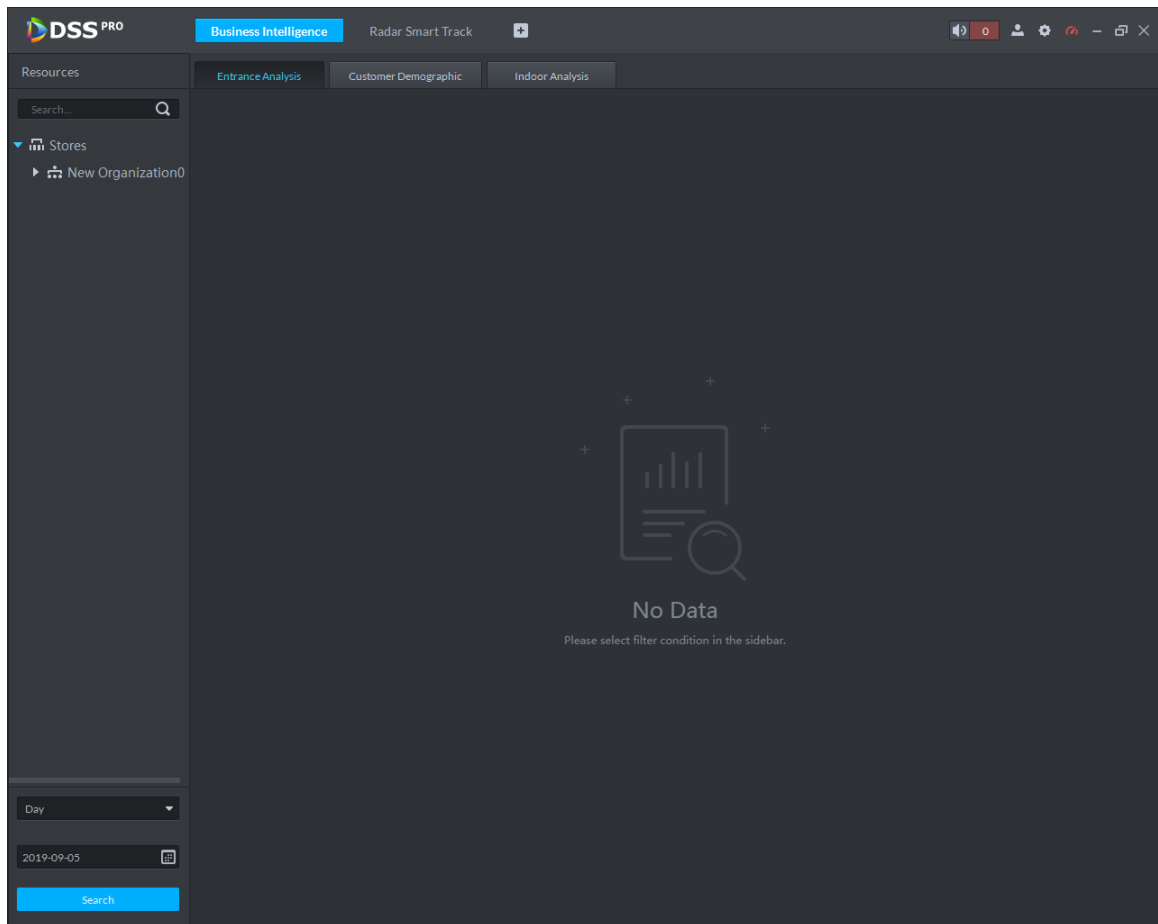
4.24.4 Business Intelligence Applications

4.24.4.1 Entrance Analysis

View the entry and exit numbers of customers.

- Step 1 On the **Homepage** interface of the Control Client, select **Business Intelligence**.
- Step 2 Click the **Entrance Analysis** tab.

Figure 4-459 Entrance analysis



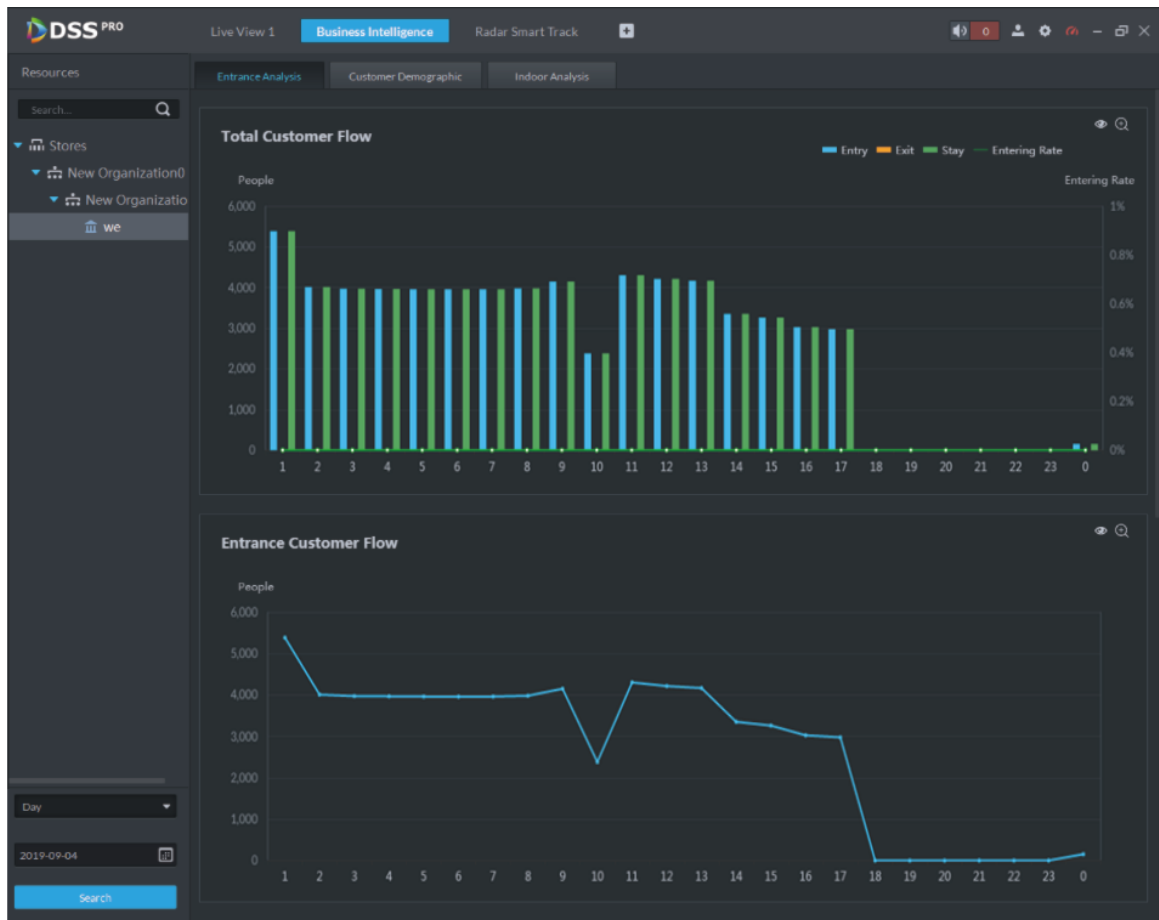
Step 3 Select a store from the organization tree, and then set search time.

Support searching by year, month and day.

Step 4 Click **Search**.

- The statistics data is classified by **Entry**, **Exit**, **Stay** and **Entering Rate**.
- The result includes the total customer flow data and entrance flow data.

Figure 4-460 Entrance analysis



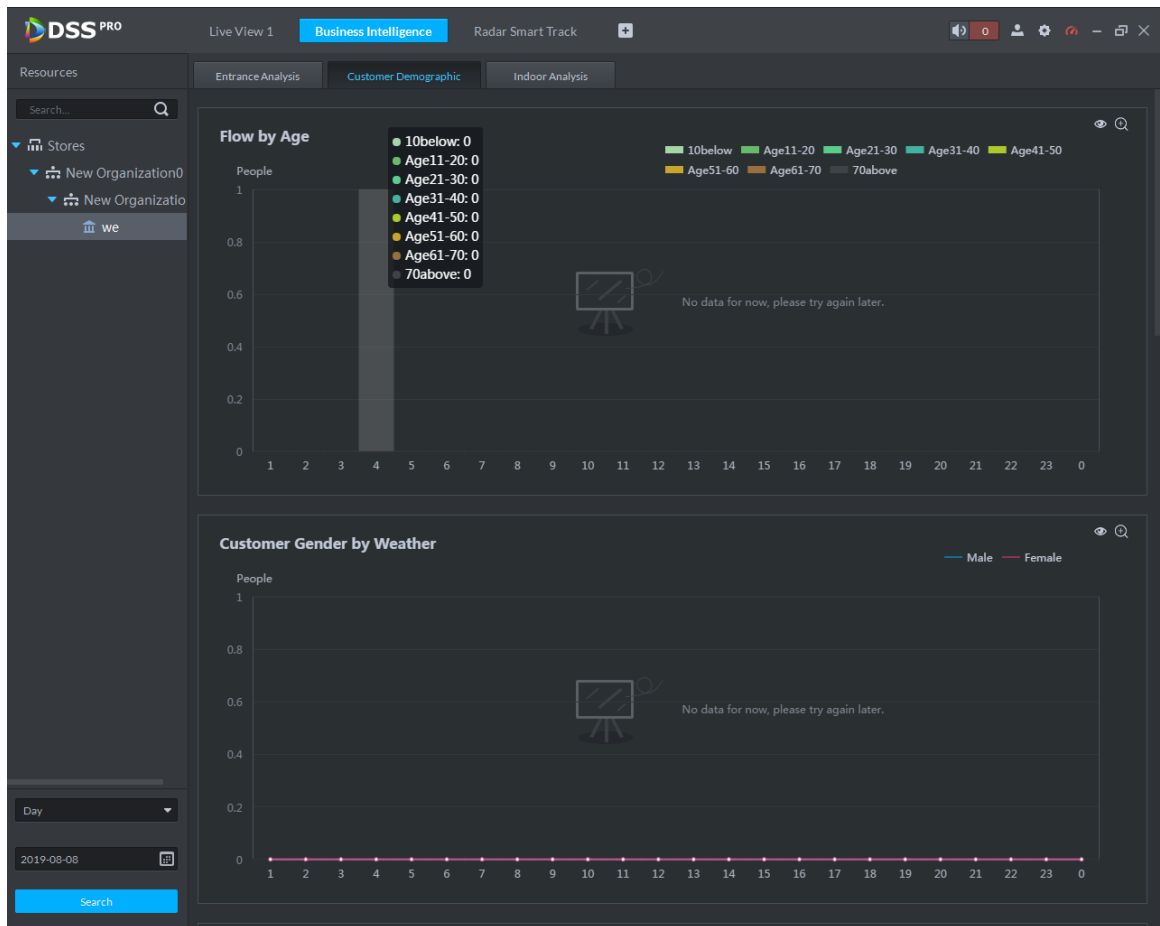
4.24.4.2 Customer Analysis

Analyze customer flow by gender and age.

Step 1 On the **Homepage** interface of the Control Client, select **Business Intelligence**.

Step 2 Click **Customer Demographic**.

Figure 4-461 Customer statistics



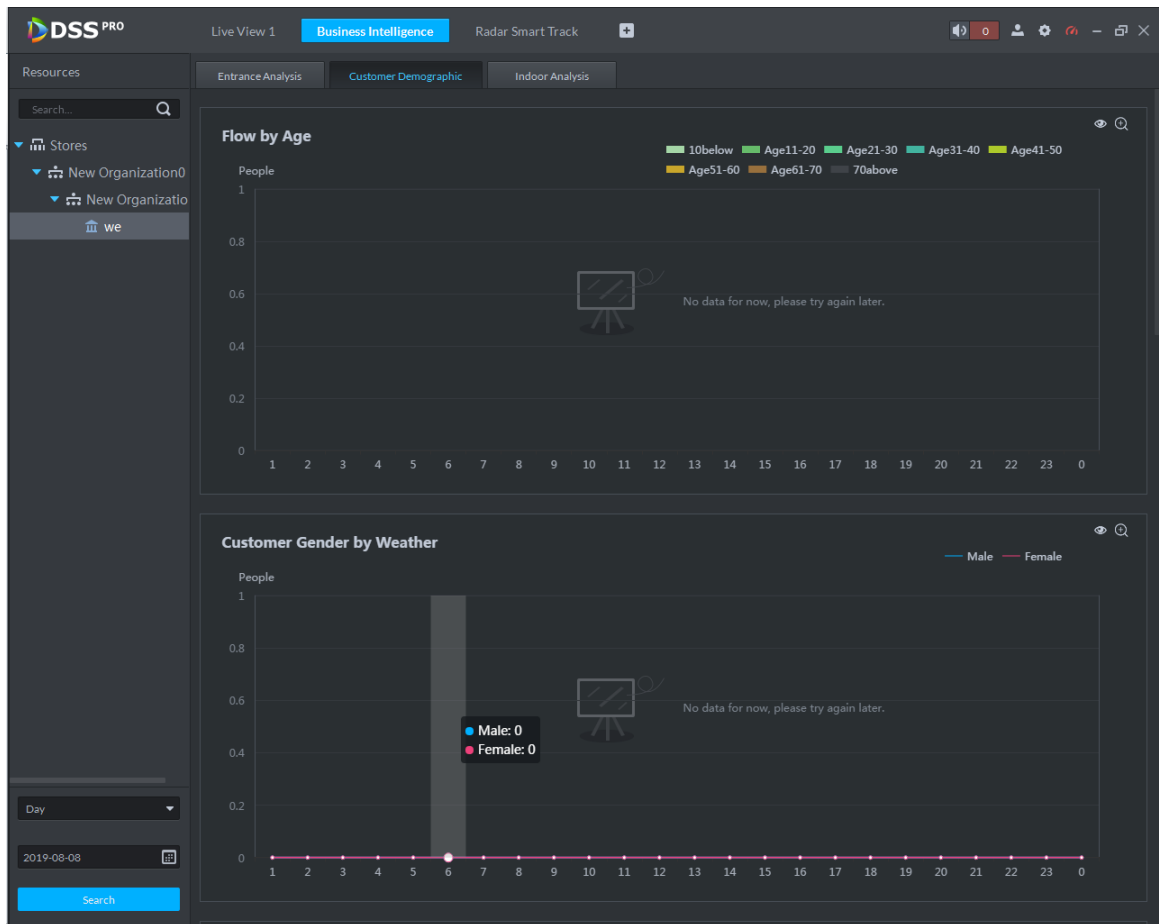
Step 3 Select a store from the organization tree, and then set search time.

Support searching by year, month and day.

Step 4 Click **Search**.

The result displays statistics data by customer age sections and by gender-weather relation.

Figure 4-462 Customer statistics



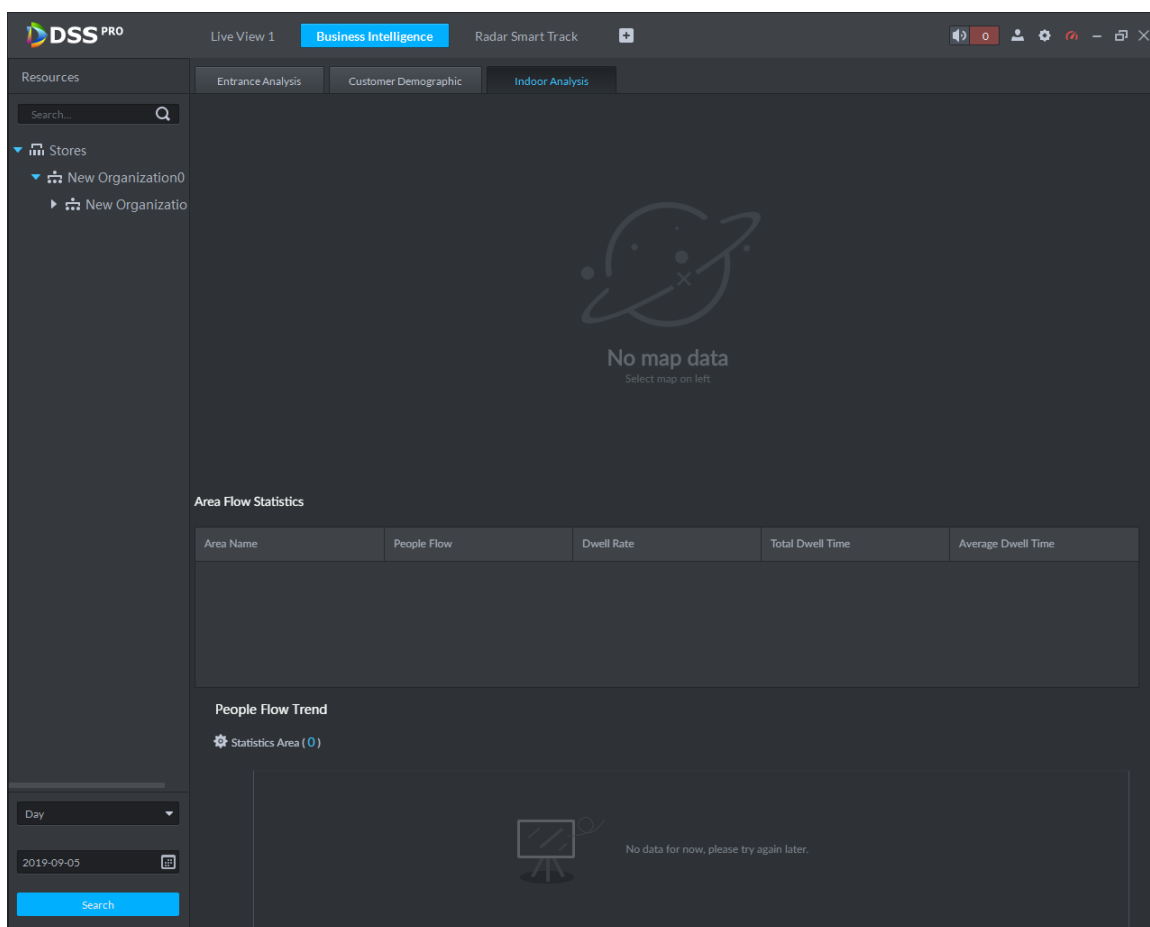
4.24.4.3 Indoor Analysis

View customer numbers and stay numbers on each floor.

Step 1 On the **Homepage** of the Control Client, select **Business Intelligence**.

Step 2 Click **Indoor Analysis**.

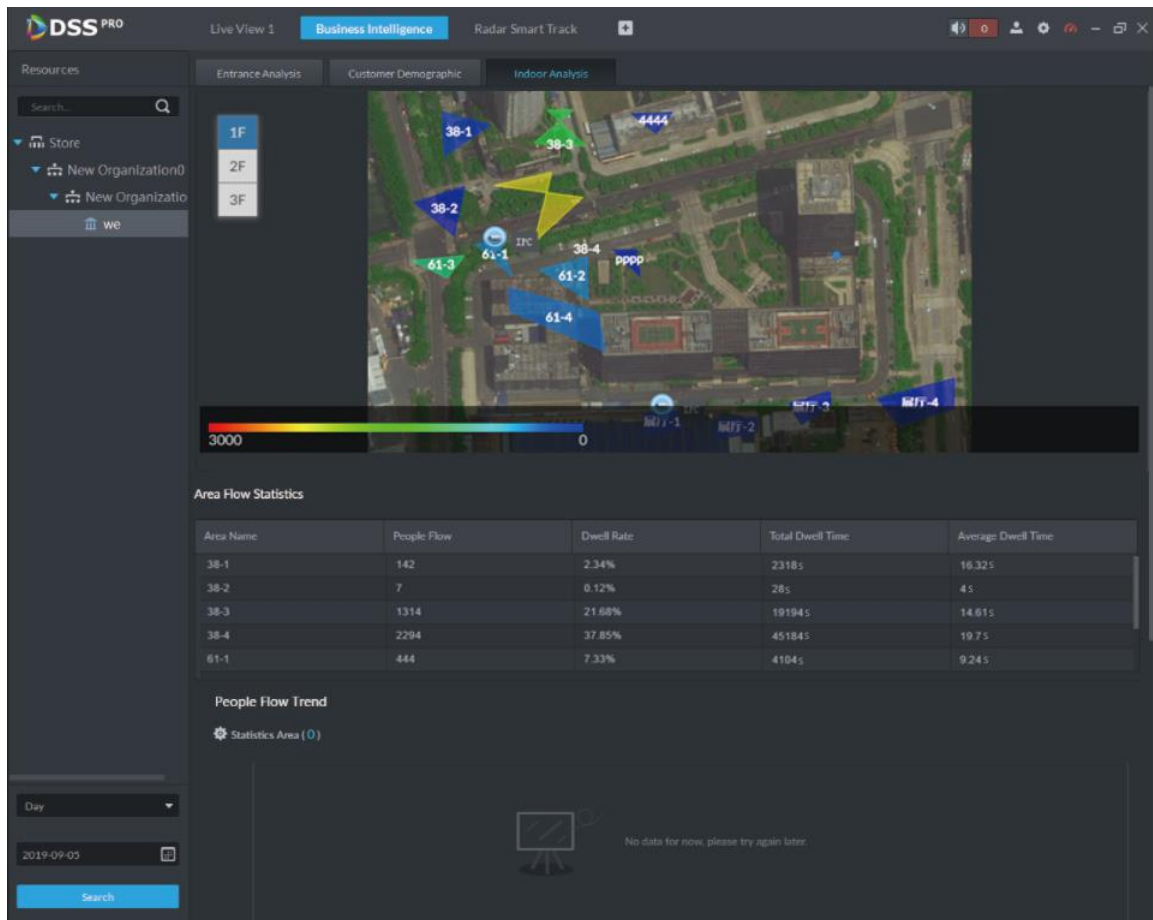
Figure 4-463 Indoor analysis interface



Step 3 From the organization tree on the left, select a store, set search time, and then click **Search**.

- Click the floor name to switch to another floor and view the corresponding data.
- The **Area Flow Statistics** section shows flow statistics data. If there is no data in an area, it will not show this area.
- In the **People Flow Trend** section and **Dwell Time Trend** section, you can click **Statistics Area** to select an area to be displayed. The section only displays data of the selected floor. If there are more than 10 statistics areas, only the top 10 areas will be displayed.

Figure 4-464 Indoor analysis



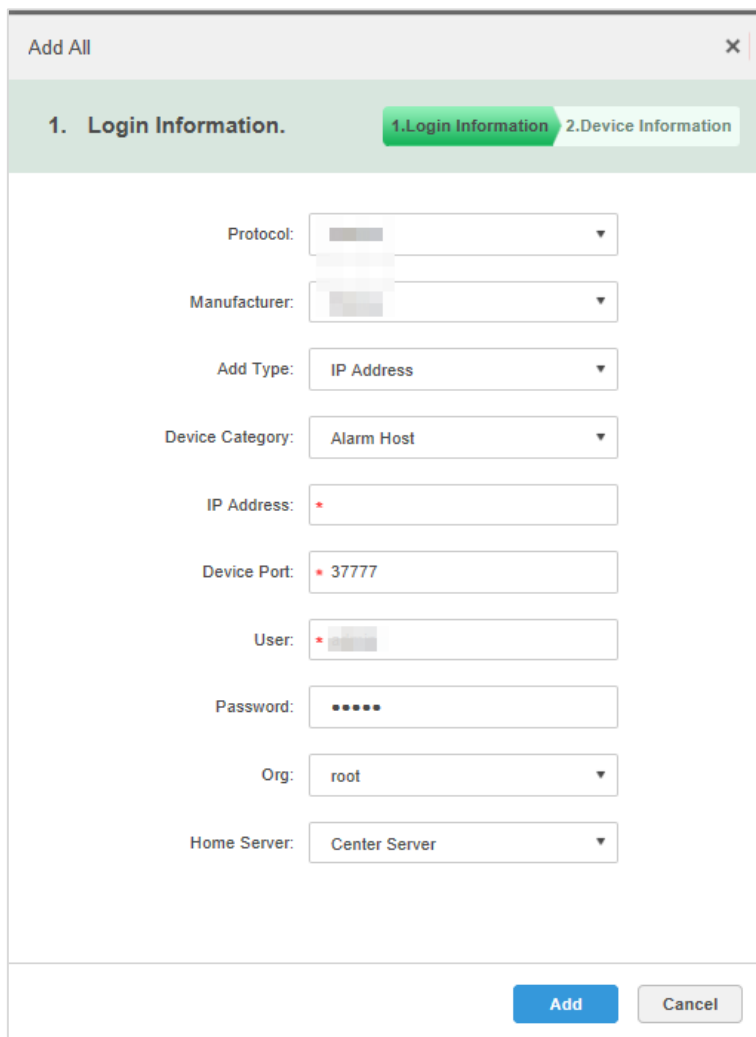
4.25 Alarm Controller

After adding alarm controllers to platform, you can manage and configure alarm zones and sub systems centrally.

4.25.1 Preparations

- Alarm controllers have been added into the system. For details, see "3.4 Managing Device."
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations."
 - ◇ When adding alarm controllers on the **Device** interface of Web Manager, select **Alarm Host** for device category.

Figure 4-465 Add an alarm controller




- After adding alarm controllers, Modify zone types, click  to modify the features of zones. For example, for a smoke detection zone, select **Smoke Sensor** as the alarm type. The alarm types can be customized. Select **Customized Alarm Type** in the **Alarm Type** drop-down list and then set the type details as needed. After alarm type configuration, you can configure the corresponding event types for the zones.

Figure 4-466 Set zone type

Edit Alarm Host
✕

Basic Info	Channel Amount: <input style="width: 50px;" type="text" value="16"/>						
Zone	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="width: 5%;"></th> <th style="width: 60%;">Name</th> <th style="width: 35%;">AlarmType</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">*</td> <td>No Name</td> <td> <div style="border: 1px solid #ccc; padding: 2px;"> ▼ Host Alarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Host Alarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Infrared Detect </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Zone Disarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> PIR </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Gas Sensor </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px; background-color: #f2f2f2;"> Smoke Sensor </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Glasses Sensor </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Emergency Button </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Stolen Alarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Perimeter </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Preventer Move </div> </td></tr></tbody></table>		Name	AlarmType	*	No Name	<div style="border: 1px solid #ccc; padding: 2px;"> ▼ Host Alarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Host Alarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Infrared Detect </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Zone Disarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> PIR </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Gas Sensor </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px; background-color: #f2f2f2;"> Smoke Sensor </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Glasses Sensor </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Emergency Button </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Stolen Alarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Perimeter </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Preventer Move </div>
	Name	AlarmType					
*	No Name	<div style="border: 1px solid #ccc; padding: 2px;"> ▼ Host Alarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Host Alarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Infrared Detect </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Zone Disarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> PIR </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Gas Sensor </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px; background-color: #f2f2f2;"> Smoke Sensor </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Glasses Sensor </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Emergency Button </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Stolen Alarm </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Perimeter </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Preventer Move </div>					

*	No Name	
*	No Name	
*	No Name	
*	No Name	
*	No Name	
*	No Name	
*	No Name	

Alarm Output	<div style="text-align: right; font-size: small;"> Total 16 record(s) ◀ ▶ 1 / 3 ▶ </div>
--------------	---

Get Info
OK
Cancel

4.25.2 Alarm Controller Interface

Click , and then select **Alarm Controller** on the client homepage. The **Alarm Controller** interface is displayed.

Figure 4-467 Alarm controller interface

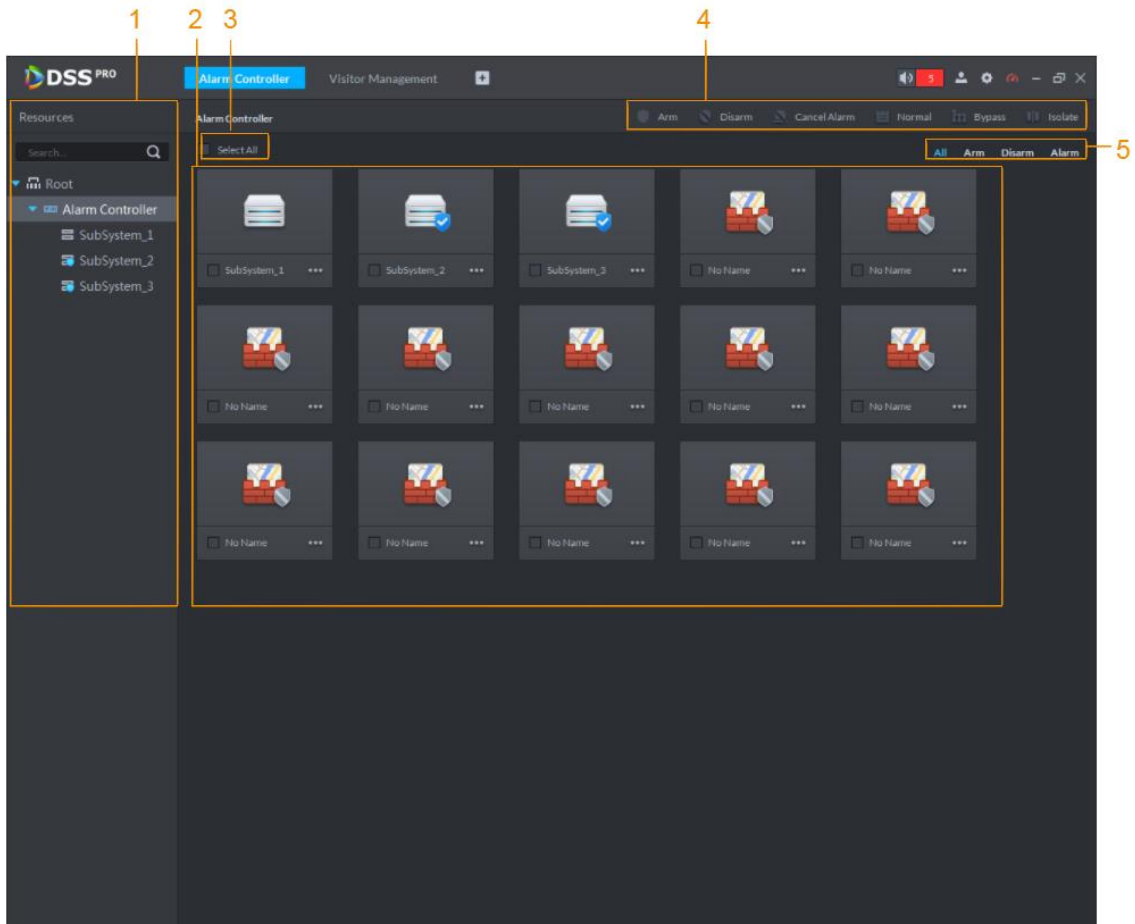













Table 4-75 Alarm controller interface description

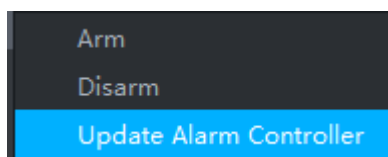
No.	Name	Description
1	Device list	<p>Display all alarm controller devices and subsystems under device. Icon status of subsystem</p> <ul style="list-style-type: none"> , no zone under subsystem. , zone exists under subsystem <p></p> <p>The subsystem and zone information displayed on platform can be acquired from device; the platform does not support config.</p>

No.	Name	Description
2	Subsystem and zone list	<ul style="list-style-type: none"> Clicking on an alarm controller name in the device tree, its subsystems and the zones not yet added to subsystems will be displayed on the right. Clicking on a subsystem name, the zones in this subsystem will be displayed on the right. <p>The description of icon status is shown as follows.</p> <ul style="list-style-type: none"> Zone status icon <ul style="list-style-type: none">  , arm.  , disarm.  , bypass.  , isolate. Subsystem status icon <ul style="list-style-type: none">  , all zones armed under subsystem.  , all zones disarmed under subsystem.  , zones are not distributed by subsystem.  , some zones under subsystem are armed.
3	Select all	Select all subsystems and zones displayed in list.
4	Operation button	Operation buttons supported by zone or subsystem.
5	Filter button	Click the button, the subsystem and zone of corresponding status are displayed in the list.

4.25.3 Updating Alarm Controller Status

In the device tree area, right-click the alarm controller that needs to be updated, and then select **Update Alarm Controller**.

Figure 4-468 Update alarm controller



4.25.4 Arming/Disarming

A zone detects and reports alarms only when it is armed. After being disarmed, a zone will not upload alarms any more.

4.25.4.1 Global Arming/Disarming

Globally arm or disarm all zones under an alarm controller.

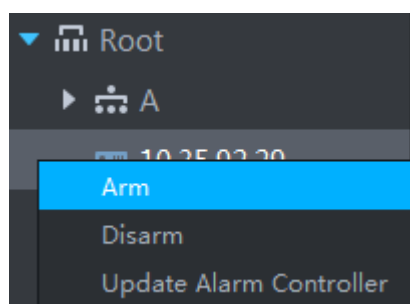
Arming

In device tree area, right-click the alarm controller that needs to be armed globally, and then select **Arm**.



The arming operation will fail when there is an alarm input in the zone. Disarm the zone if you continue to arm, clear alarms in each zone, zone with alarm input exists in bypass, and then arm again.

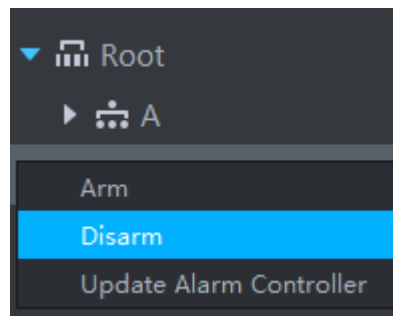
Figure 4-469 Global arm



Disarming

In device tree area, right-click the alarm controller that needs to be disarmed globally, and then select **Disarm**.

Figure 4-470 Global disarm



4.25.4.2 Arming/Disarming a Zone/Subsystem

Arm or disarm a single zone or subsystem.

Arming



- The arming operation will fail when there is an alarm input in the zone. Disarm the zone if you continue to arm, clear alarms in each zone, bypass the zone with alarm input, and then arm again.
- If a subsystem has no zone, then you cannot arm or disarm it.

You can arm by the following two methods:


- Click the zone you want to arm or  of the corresponding subsystem, and then select **Arm**.

Figure 4-471 Arm a zone

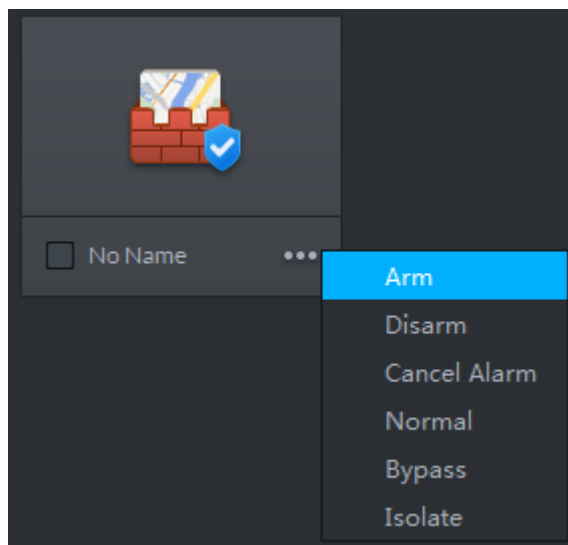
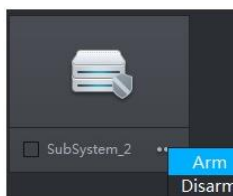
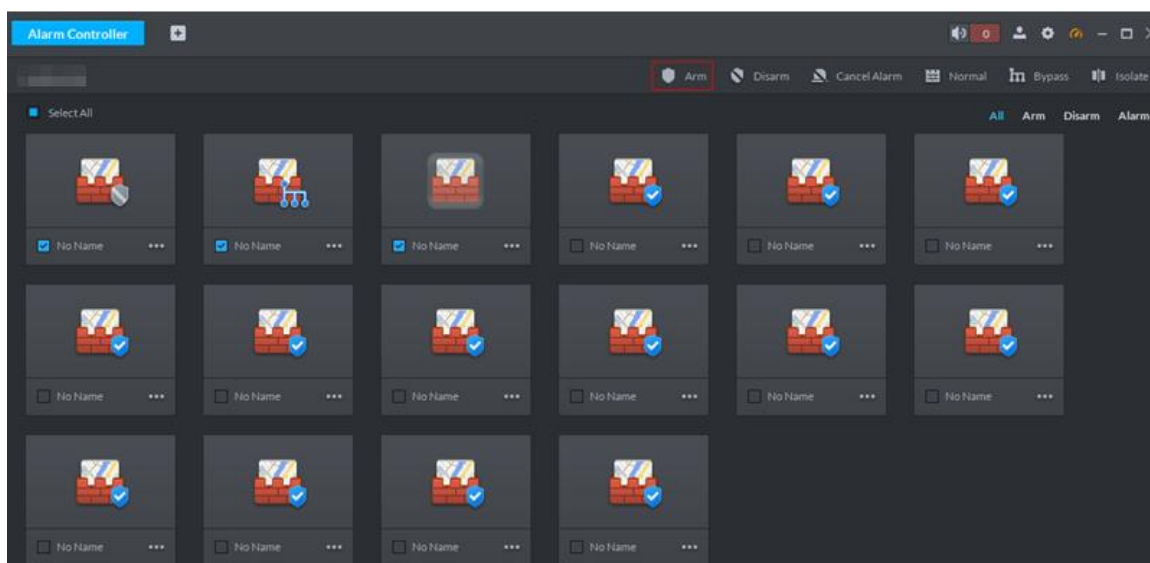


Figure 4-472 Arm a subsystem



- Select the zone or subsystem you want to arm (multiple choice supported), and then click **Arm** on the top of the interface.

Figure 4-473 Arm



Disarming

Support disarming by the following two methods.

- Click the zone you want to disarm or **...** of the corresponding subsystem, and then select **Disarm**.

Figure 4-474 Disarm a zone

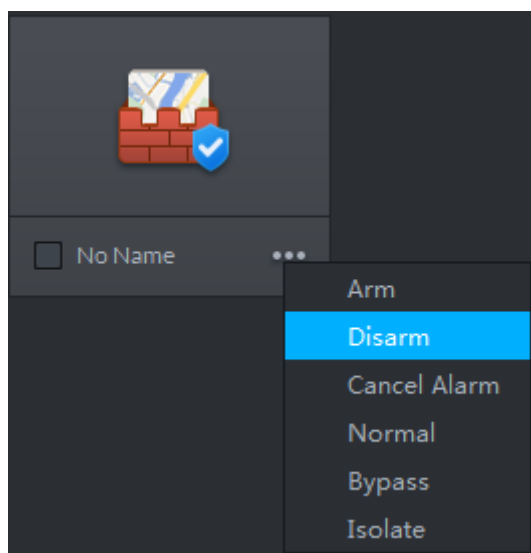
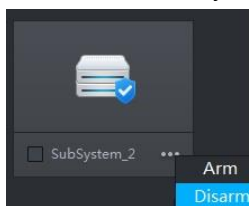
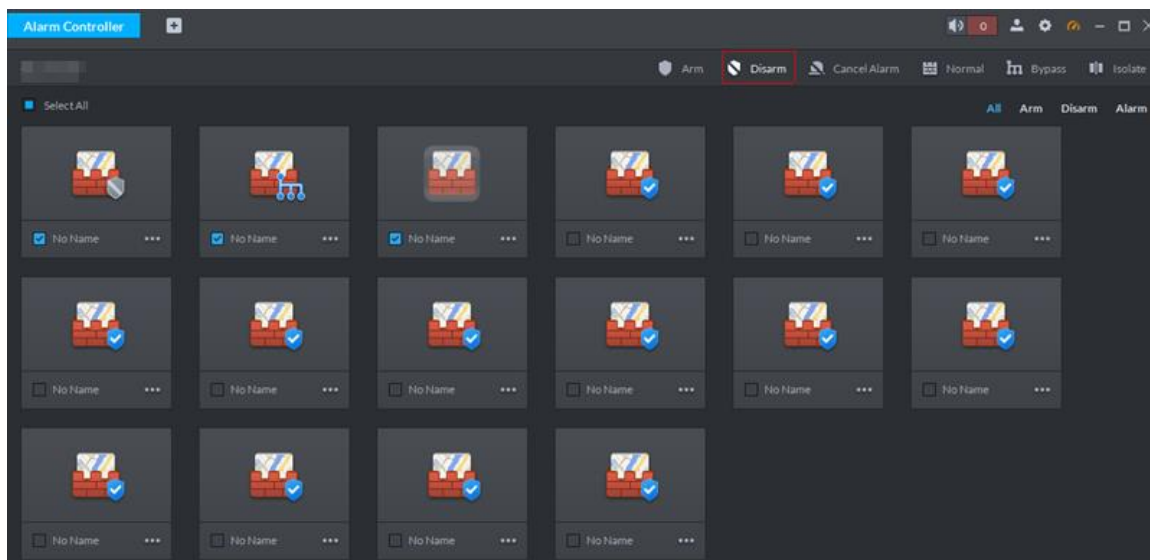


Figure 4-475 Disarm a subsystem



- Select the zone or subsystem you want to disarm (multiple choice supported), and then click **Disarm** on the top of the interface.

Figure 4-476 Disarm



4.25.5 Bypassing/Isolating/Normal

- When a zone is bypassed, the alarm controller still monitors the zone but will not forward the zone data to users. If you want to arm the bypassed zone, disarm the zone into non-bypass and arm again.
- When a zone is isolated, the alarm controller still monitors the zone but will not forward the zone data to users. When the zone is disabled or you want to disarm and arm again, the isolated zone is still disabled.
- When a zone is in the status of Normal, the zone can trigger alarms normally when it is armed.

Two ways to arm/disarm a zone:


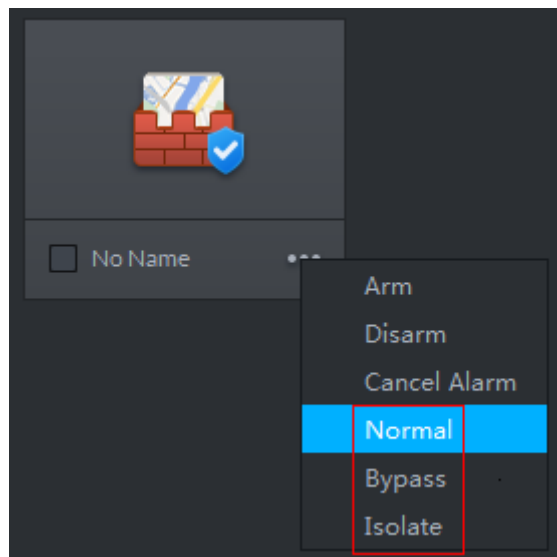
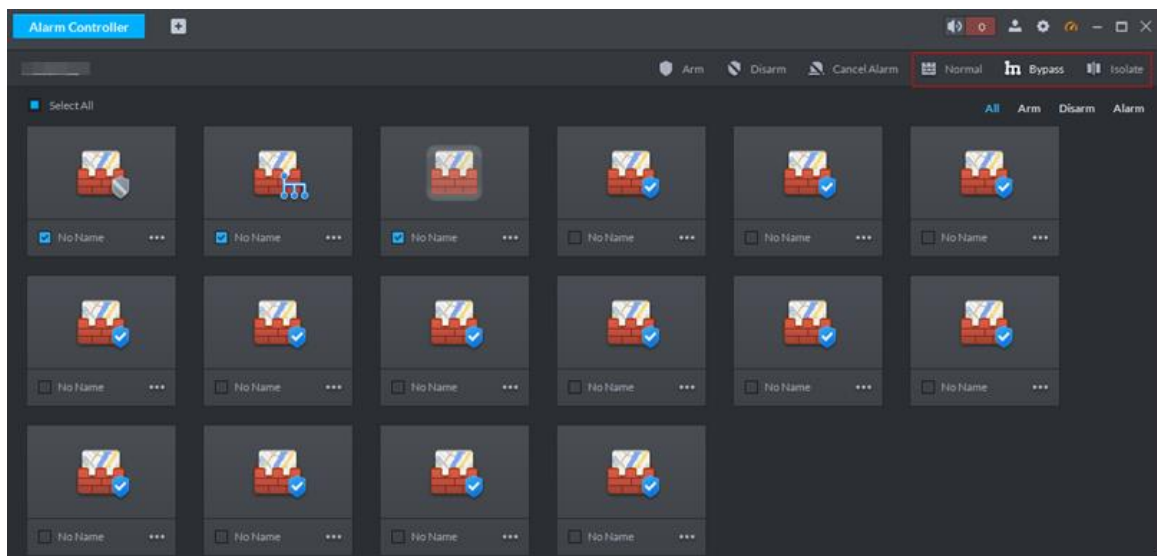
- Click  of the zone that needs to be bypassed, isolated or recovered to normal, and then select operation.

Figure 4-477 Bypass/isolate a zone (1)



- Select the zone that needs to be bypassed, isolated or recovered normal (multiple choice supported), and then click the operation buttons on the top of the interface.

Figure 4-478 Bypass/isolate zone (2)

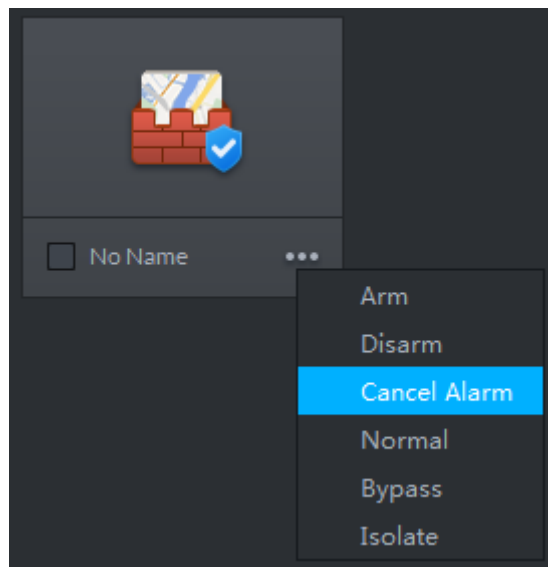


4.25.5.2 Cancelling Alarms

You can remove an alarm by **Cancel Alarm** when the alarm is triggered.

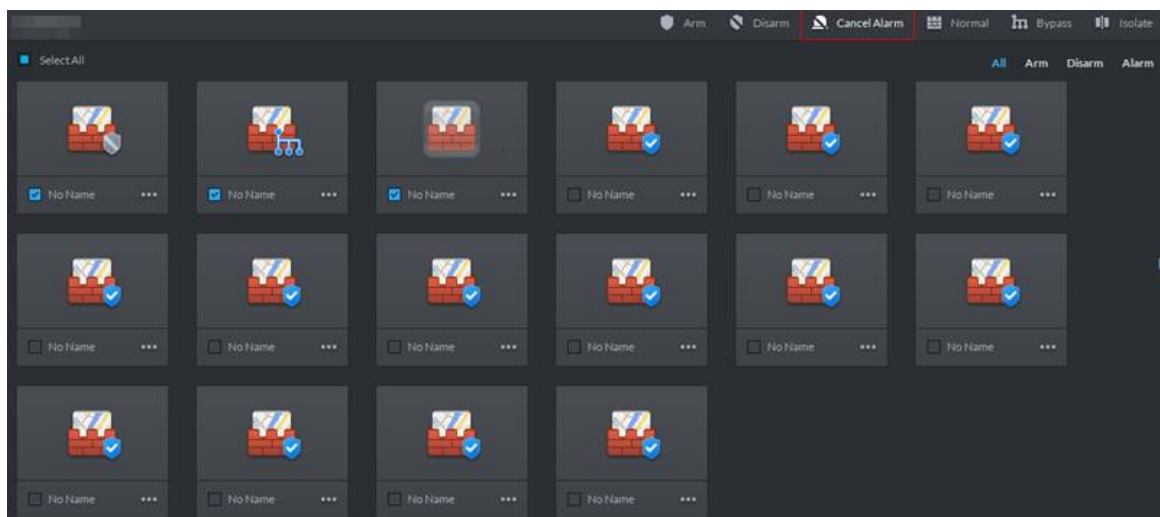
- Click the zone you want to cancel alarm, and then select **Cancel Alarm**.

Figure 4-479 Cancel alarms



- Select the zone you want to cancel alarms from (multiple choices supported), and then click **Cancel Alarm** on the top of the interface.

Figure 4-480 Cancel alarms (2)



4.26 Configuring N+M

To configure N+M, enable slave servers on the master server and confirm the relation between slave servers and spare servers.

Make sure that all servers are well deployed before starting to configure N+M.

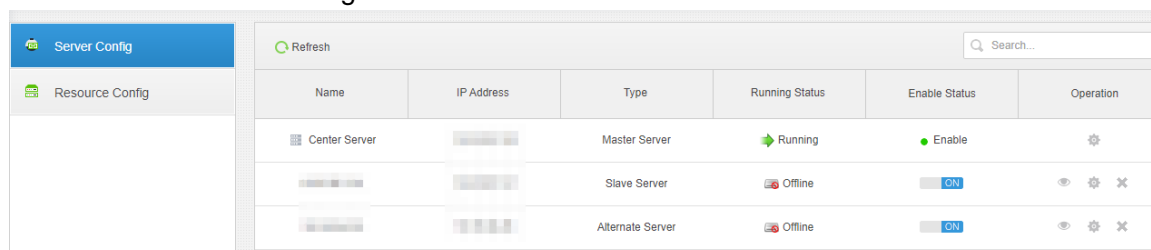
Step 1 Log in to the Web interface of the master server.








Step 2 Click , and then select **Server Management > Server Config**. Slave servers are disabled by default.

Step 3 Click  next to each slave server to enable all the slave servers.

When disabled, server status is shown as **Offline**; when enabled and if the server works normally, its status is shown as **Running**.

Figure 4-481 Enable slave servers



Name	IP Address	Type	Running Status	Enable Status	Operation
Center Server		Master Server	Running	Enable	
		Slave Server	Offline	<input checked="" type="checkbox"/>	  
		Alternate Server	Offline	<input checked="" type="checkbox"/>	  

Step 4 Set specific servers to be spare servers.


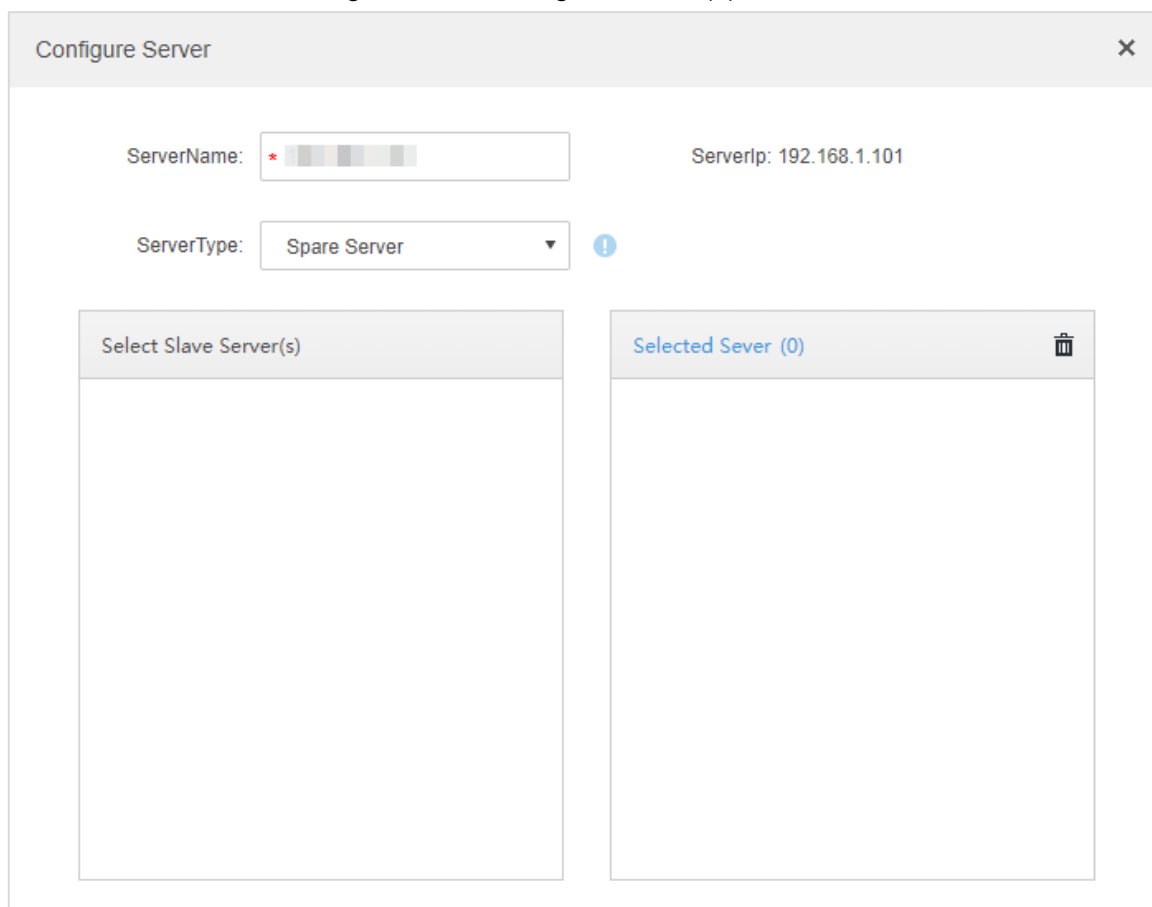

- 1) Click  of each slave server.
- 2) Select **Spare Server** in the **Server Type** dropdown list. Click **OK**.

Figure 4-482 Configure server (1)



Step 5 Configure the relationship between slave servers and spare servers.

Support the following two methods to configure.

- Go to the **Configure Server** interface of the slave server, and then select spare servers. See instructions below.
 - 1) Click  of the slave server.
The **Configure Server** interface is displayed.
 - 2) Select one or more spare servers in the **Select Spare Server(s)** list.



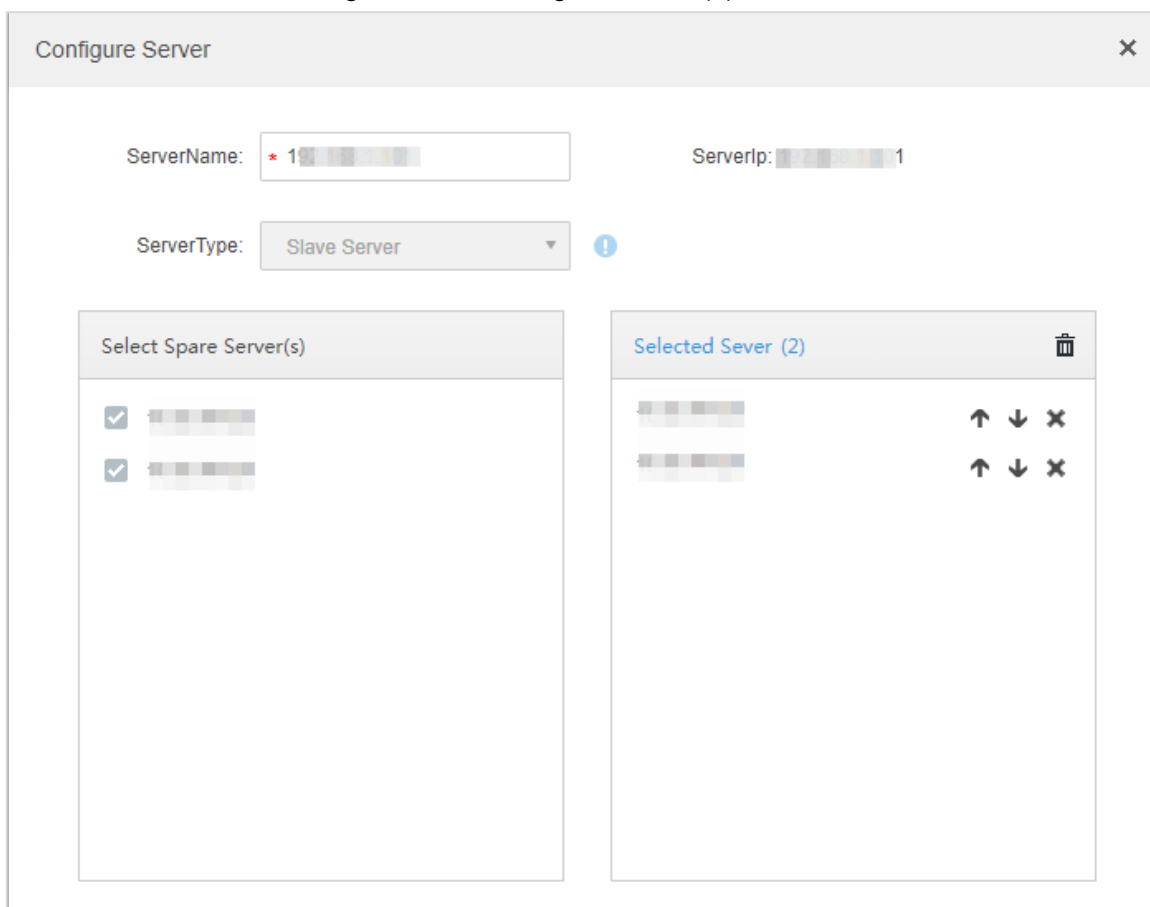
The selected servers are listed on the right. Click   to adjust the priority.

Figure 4-483 Configure server (2)






- 3) Click **OK**.
 - Go to the **Configure Server** interface of the spare server, and then select slave servers. See instructions below.
- 1) Click  of the spare server.
The **Configure Server** interface is displayed.
- 2) Select one or more slave servers from the **Select Slave Server(s)** list.
The selected servers are listed on the left. Click   to adjust the priority.

Figure 4-484 Configure server (3)

3) Click **OK**.

4.27 Cascade

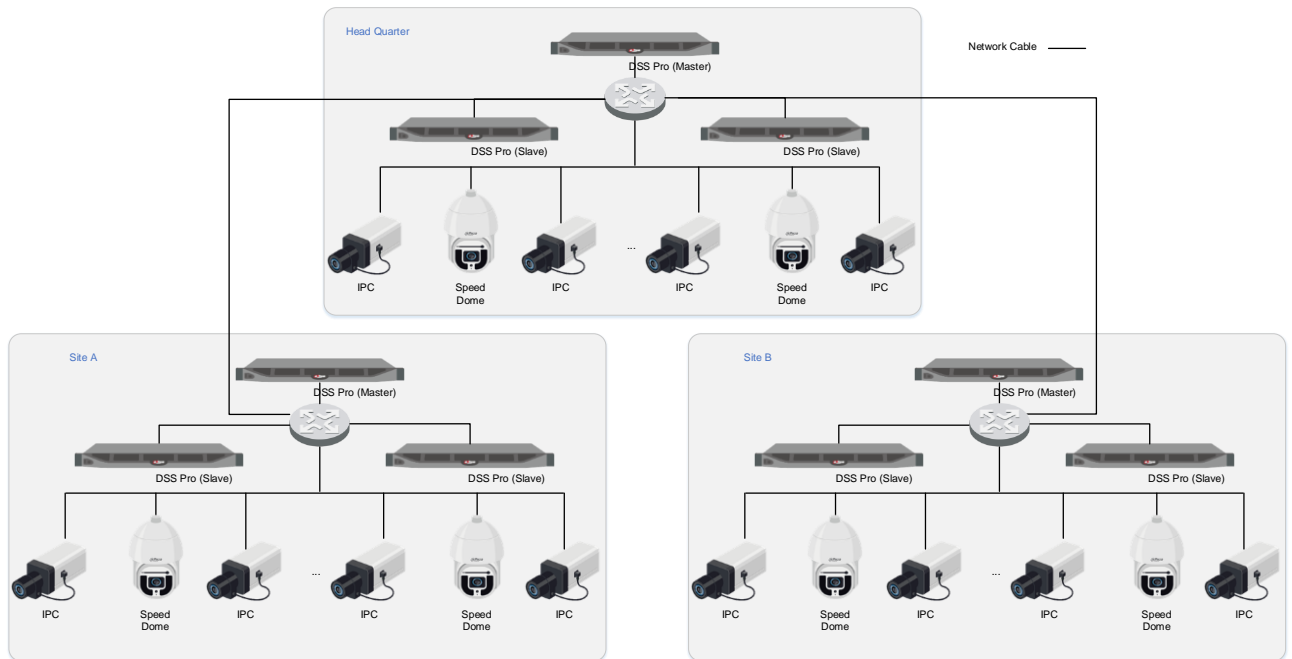
The system supports cascading. After cascading, platform of higher level can view the live video and video record of platforms of lower level. Configuring cascade refers to adding lower-level platforms to higher-level ones. The system supports up to 3 levels.



- Before configuring, make sure that the platform is deployed.
- Currently, the systems supports cascading between Pro and Express platforms. Express can only be lower-level platform.

4.27.1 Typical Topology

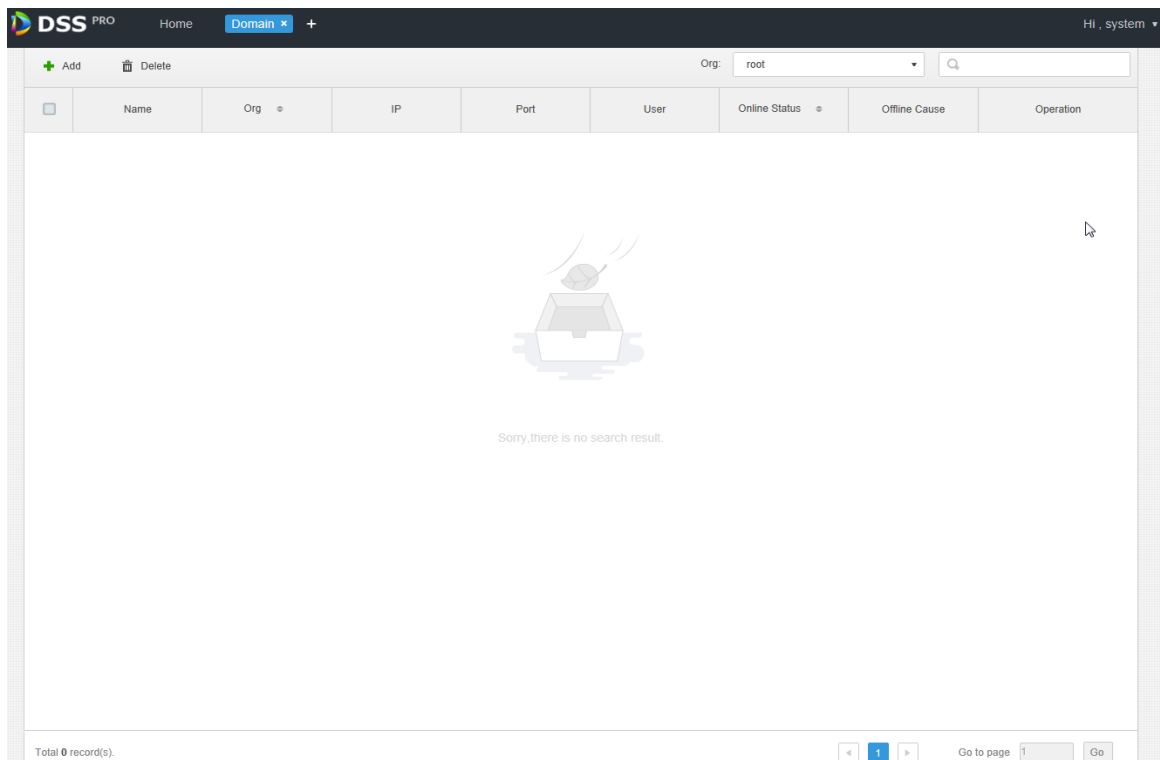
Figure 4-485 Typical topology



4.27.2 Configuring Cascade

Step 1 Click **+** on the Web Manager, and then select **Domain**.

Figure 4-486 Domain



Step 2 Click **Add**.

Figure 4-487 Add cascading

Step 3 Configure the parameters, and click **OK** to save the configuration.

Org refers to the higher-level platform that the added platform belongs to.

Step 4 If there is more than one level of platform, repeat this process.

4.28 System Configuration


Configure system settings such as email and device login mode.

4.28.1 HTTPs Certificate

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is a safe HTTP transmission protocol. It provides safe and stable guarantee of user information and device security. When HTTPS certificate is configured, you can log in to the platform through HTTPS protocol to ensure transmission security.



SSL certificate is created or purchased, and you have got the password.

Step 1 Log in to the Web Manager, click , and then select **System**.

Step 2 Click the **HTTPS** tab.

Figure 4-488 HTTPs certificate

Step 3 Click **Browse**, import SSL certificate, and then enter the password.

Step 4 Click **Save**.

4.28.2 Setting Mail Server

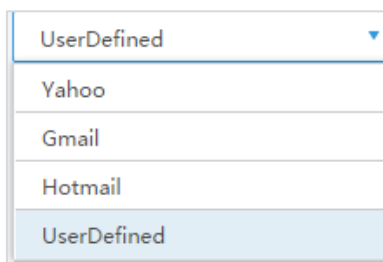
Step 1 Click  on the Web Manager, and then select **System**.


Step 2 Select the **Mail Server** tab, check **Enable** to enable mail configuration.

Figure 4-489 Set mail server

Step 3 Select the type of mail server in the drop-down box.

Figure 4-490 Set mail server type



- Step 4** Set mail server IP, port, encryption type, username/password, sender and test recipient etc.
- Step 5** Click **Mail Test** to test if the configuration of mail server is valid. Test prompt will be received if the test is successful, and the test account will receive corresponding email.
- Step 6** Click  after the test is successful, and then it can save configuration information.

4.28.3 Setting Device Login Mode

In order to ensure safe use of devices, the platform supports two ways to log in to devices: Compatibility mode and security mode.


- Step 1** Log in to the Web Manager, click , and then select **System** on the **New Tab** interface.
- Step 2** Click the **Login Mode Settings** tab.
- Step 3** Select a mode.

Figure 4-491 Select a login mode



- Step 4** Click **Save**.

4.29 Server Management

Server management supports managing server information, adjusting server or superior server of the device.

4.29.1 Server Management

Server management supports a series of operations, such as switching master/spare mode of server, modifying server name, enabling or disabling service etc.

Step 1 Click and select **Server Management** on the interface of **New Tab**.

Step 2 Click **Server Management** tab.

Figure 4-492 Server management

Server Name	IP	Device ID	Type	Server Status	Operation
Center Server		videomaster	Home Server	Running Status: Running Server Status: Enabled	
		vidt: 78	Home Server	Running Status: Running Server Status: Enabled	

Step 3 The management server supports following operations:

- Click and edit the server information.
- means the server is not enabled; Click the icon and it becomes , means the server is already enabled.
- Click and allocate the server type.
- Click and delete the server information.

4.29.2 Resource Config

Adjust the device server during distributed deployment.

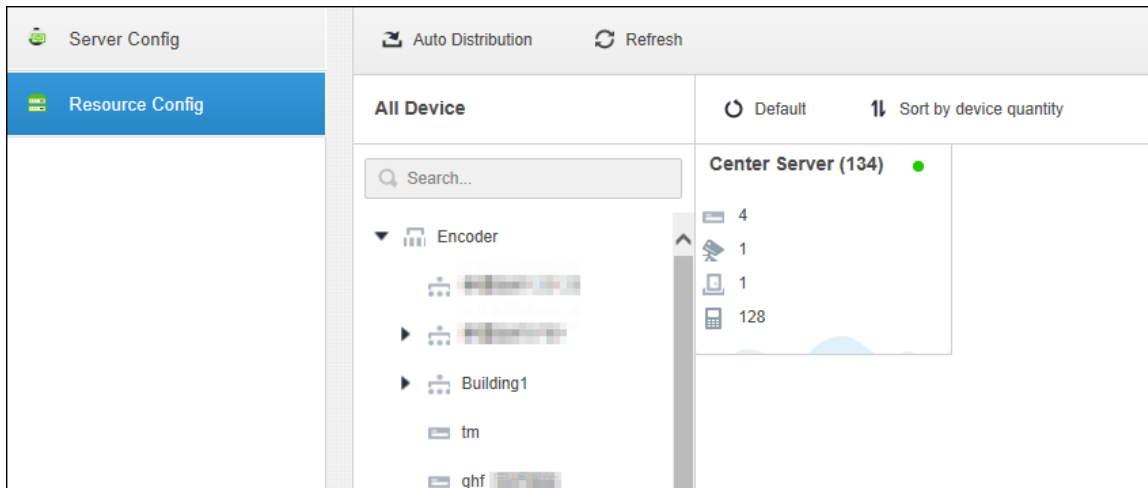
Step 1 Click and select **Server Management**.

Step 2 Click the **Resource Config** tab.



- Click **Default** and the servers will be sorted according to the time when they are added.
- Click **Sort by device quantity** and the servers will be sorted according to quantity of devices attached to them.

Figure 4-493 Resource allocation



Step 3 Adjust the attached server.

- Manual adjustment

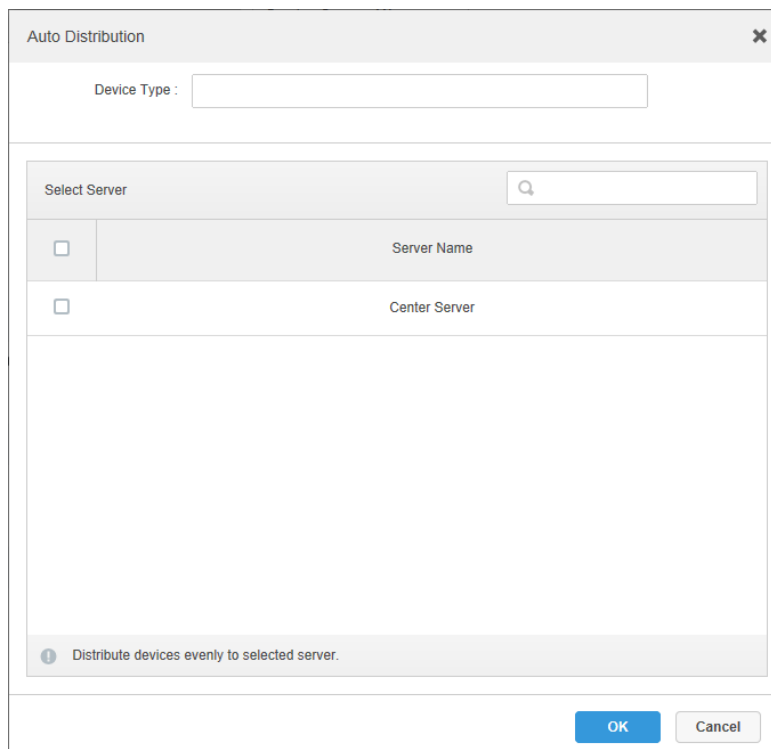
Select the device on the left and drag it to the server on the right. The device quantity of attached server will increase while the device quantity of original server will decrease.

- Auto distribution

Averagely distribute the same type of device to the server that is deployed by distribution.

- 1) Click **Auto Distribution**.

Figure 4-494 Auto distribution




- 2) Select device types.
- 3) Select servers where the device will be distributed to.
- 4) Click **OK**.

4.30 Password Maintenance

The platform supports modifying user password, and resetting system user password when it is forgotten. Only the system user can reset password. Other users, when their passwords are forgotten, can ask the system user to rmodify the passwords.

4.30.1 Modifying Password

You are advised to modify your password regularly for the sake of account safety.

Step 1 Log in to the Control Client, click  at the upper-right corner, and then select **Change Password**. You can also go to the Web Manager, hover over **Hi, system**, and then select **Change Password**.

Step 2 Enter the old password, new password, and then confirm the new password. Click **OK**.

4.30.2 Resetting Password

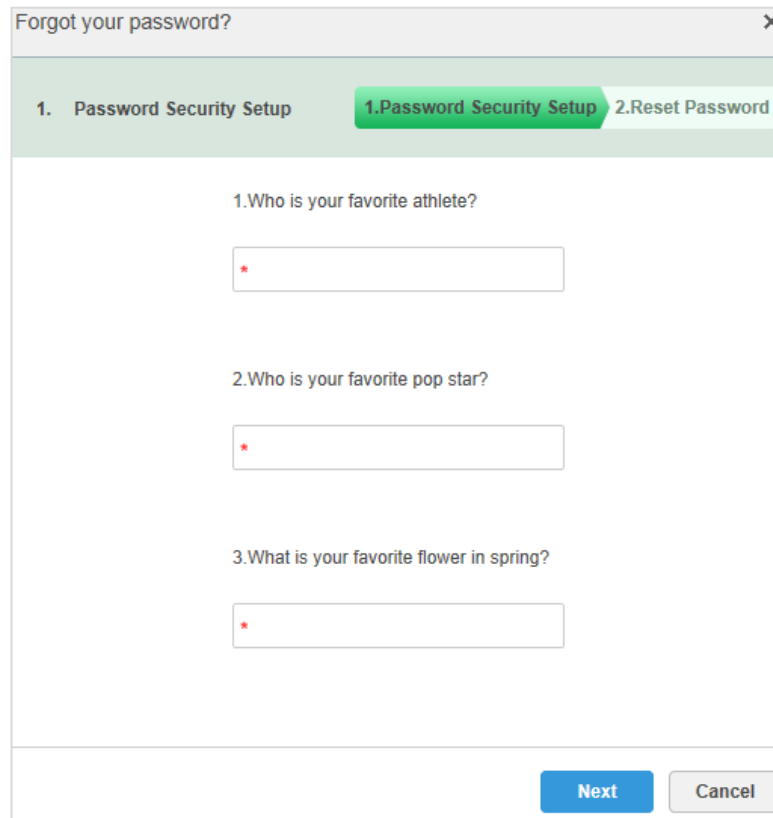
4.30.2.1 Resetting System User Password

When the system user password is forgotten, you can reset the password by answering security questions.

Step 1 When logging in to the Web Manager, enter system and a random password, and then click **Login**.

Step 2 Click **Forgot your password?**.

Figure 4-495 Security questions



Step 3 Enter the answers of the questions, and then click **Next**.

Step 4 Enter the new password, and then click **OK**.

4.30.2.2 Resetting Password of General User

Only the system user can reset password. Other users, when their passwords are forgotten, can ask the system user to reset the passwords.

Step 1 Log in to the Web Manager using the system username and password, and then click **User**.


Step 2 Click the **User** tab, select the user whose password is to be reset, and then click .

Figure 4-496 Edit user information

Edit User

Basic Info

Username: Password Expiry:

Multiple Points of Presence: OFF MAC Address:

Reset Password: ON PTZ Control Permission:

Password:

Confirm: Email Address:

Remark:

Role

<input type="checkbox"/>	Role name
<input type="checkbox"/>	Administrator
<input type="checkbox"/>	Operator

Device Permissions

Search...

▼ root

Control Permissions

- ▼ All Permissions
 - ▼ Control Permissions
 - ▼ Menu Permissions
 - ▼ Administrator Menu
 - ▼ Client Menu

Step 3 Enable **Reset Password**, enter the new password, and then confirm it. Click **OK**.

5 Maintenance

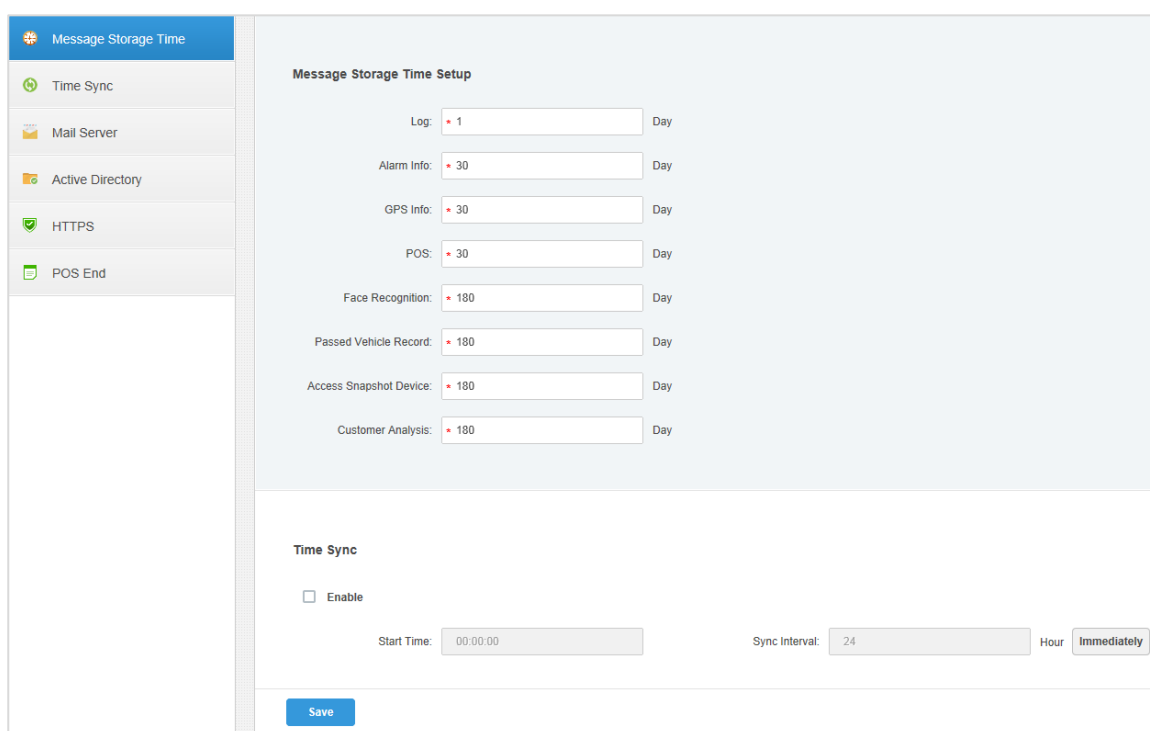
5.1 Setting System Data Retention Period

Set the retention periods for logs, alarm messages, GPS information, POS messages, vehicle records, heatmap data, face recognition records, and access snapshot records.

Step 1 Click , select **System** on the **New Tab** interface.

Step 2 Configure corresponding parameters.

Figure 5-1 Set message storage time



Step 3 Click **Save**.

5.2 Updating App Certificate

Update the App certificate when it expires. Same method for DSS Mobile 2 and DSS Mobile for VDP.

Step 1 Click , select **System** on the **New Tab** interface.

Step 2 Click the **App Certificate** tab.

Step 3 Click **Export current certificate** and save the certificate.

Step 4 Send the certificate to dss_support@dahuatach.com to get a new certificate.

Step 5 Click **Update the certificate** to import the new certificate.

Step 6 Enter App username, and then click **Send Test Message**.

The certificate is updated when you receive the message.

Step 7 Click **Save**.

5.3 Remote Log

To ensure safe use of platform, the system sends administrator and operator logs to the log server for backup at 3 A.M. every day.

Step 1 Click , select **System** on the **New Tab** interface.

Step 2 Click the **Remote Log** tab.

Step 3 Select the **Enable** check box, and then set parameters as required.

The platform number must be the same on the remote server and the platform.

Figure 5-2 Enable remote log



Remote Log :

Enable

IP Address: * 127.0.0.1

Platform Number: * 22

Port: * 514

Step 4 Click **Save**.


5.4 Time Synchronization

Synchronize the system time of all connected devices with that of the platform; otherwise the system might malfunction. For example, video search might fail. The platform supports synchronizing time of devices connected through Dahua protocol and ONVIF. You can synchronize manually or automatically.

5.4.1 Automatic Time Synchronization

Configure automatic time synchronization.

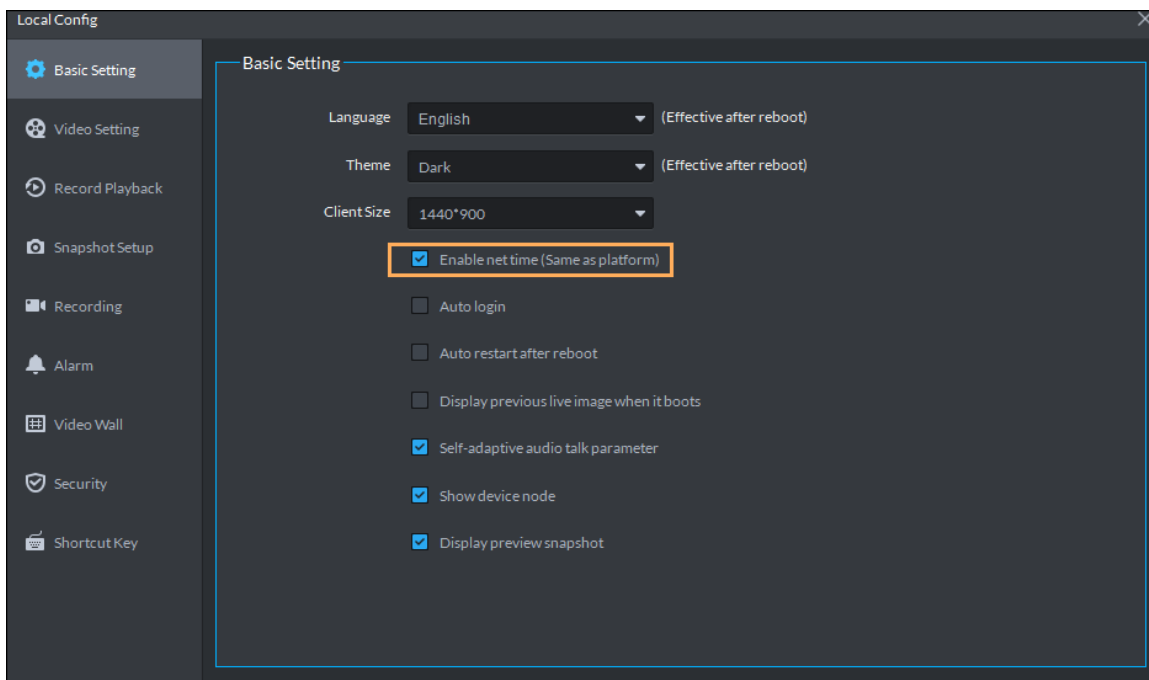
Step 1 (Optional) Enable time synchronization on Control Client.

- 1) Log in to the Control Client, and then click .
- 2) Click **Basic Setting**, select the check box next to **Enable net time (Same with platform)**, and then click **Save**.



The system immediately synchronizes time after you enable the function.

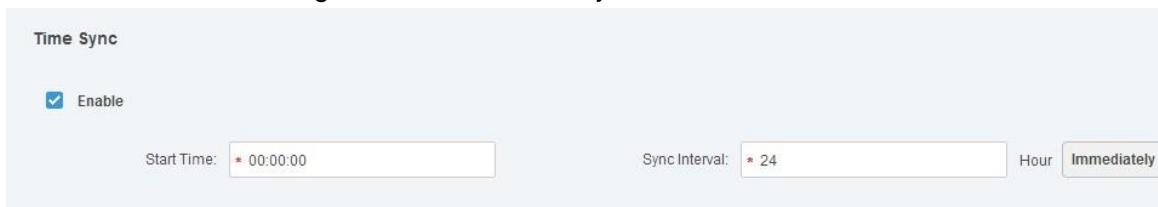
Figure 5-3 Enable net time



Step 2 Click on the Web Manager, and then select **System**.

Step 3 Click the **Time Sync** tab, and then select the check box to enable the function. Set time synchronization parameters.

Figure 5-4 Enable time synchronization



Step 4 Click **Save**.

5.4.2 Manual Time Synchronization

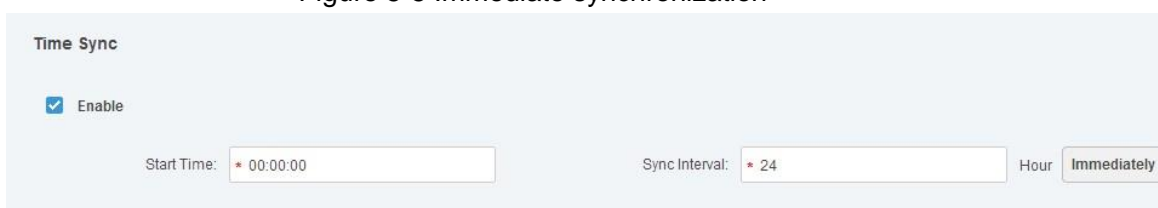
Manually synchronize system time.

Step 1 (Optional) Enable time synchronization on Control Client. For details, see "5.4.1 Automatic Time Synchronization."

Step 2 Click on the Web Manager, and then select **System**.

Step 3 Click the **Time Sync** tab, and then click **Immediately**.

Figure 5-5 Immediate synchronization



5.5 Backup and Restore

DSS Pro supports backup of configuration information and saving it to local PC, so that you can use the backup file for restoring settings.



Only system account can back up and restore.

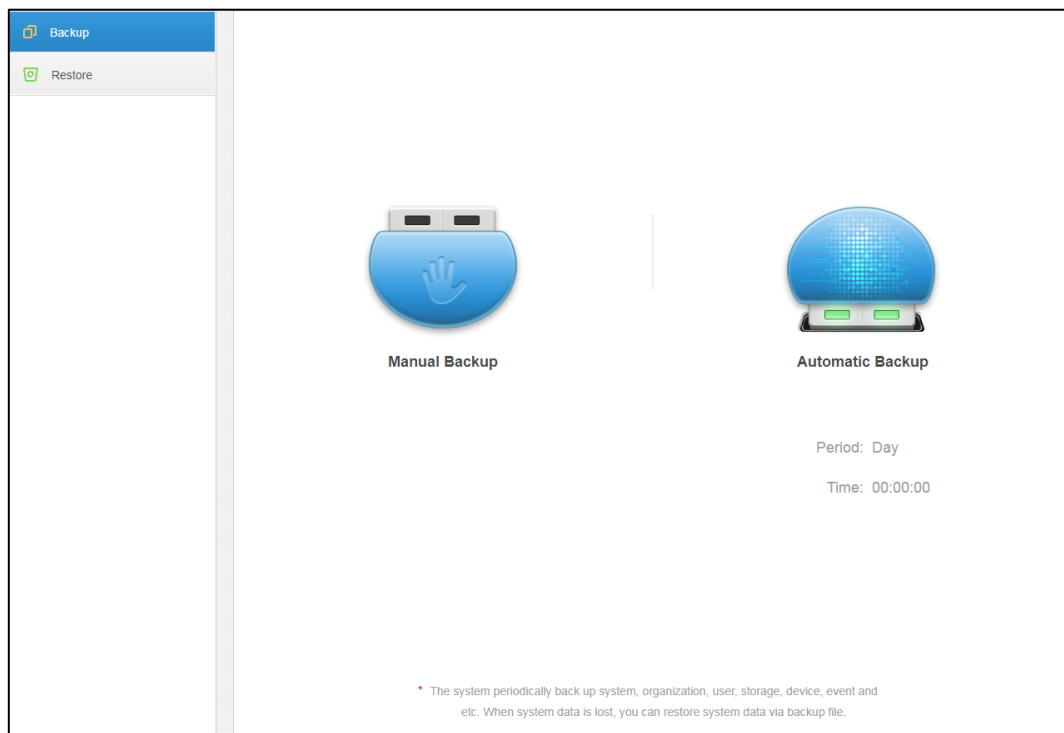
5.5.1 System Backup

In order to guarantee the security of user data, DSS Pro system provides data backup function. The backup includes manual backup and automatic backup.

Manual Backup

Step 1 Click  on the Web Manager, and select **Backup and Restore**.


Figure 5-6 Backup



Step 2 Click **Manual Backup**.

Step 3 Enter encrypted password, and then click **OK**.

Automatic Backup

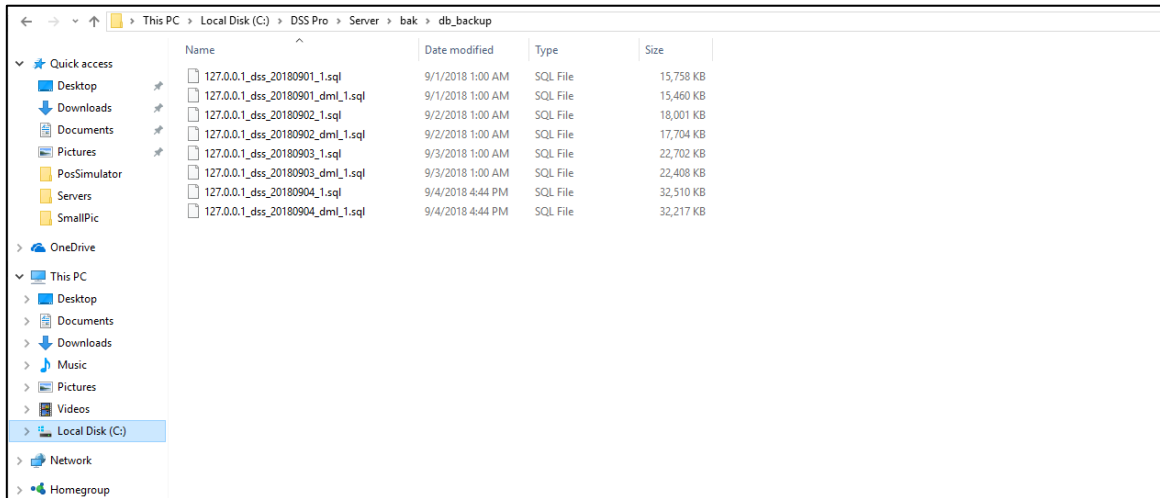
Step 1 Click  on the Web Manager, and then select **Backup and Restore**.

Step 2 Click **Automatic Backup**.

Step 3 Select a backup period, and then click **OK**.

Step 4 Check the auto-backup file on the server.

Figure 5-7 Backup path



5.5.2 System Restore

Restore the data of the latest backup when the user database becomes abnormal. It can quickly restore the user's DSS system and reduce user loss.

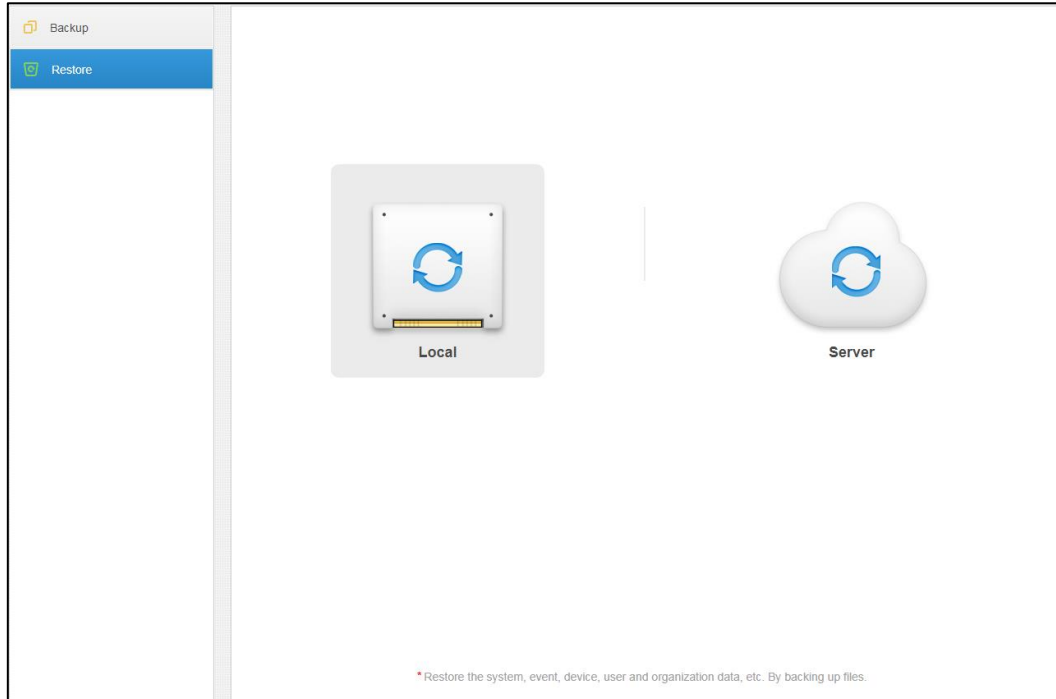


Stop other users using DSS system when implementing system restore. Be cautious when using the function because it may change data information.

Local

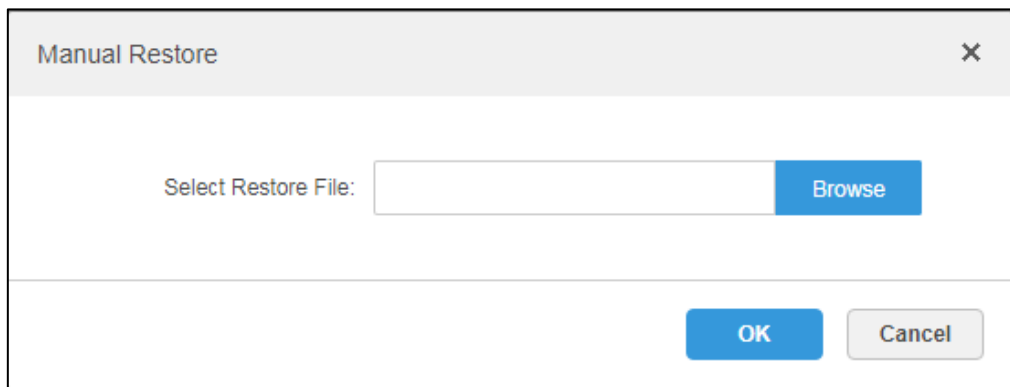
Step 1 Select **Restore** tab.

Figure 5-8 Restore



Step 2 Click **Local**.

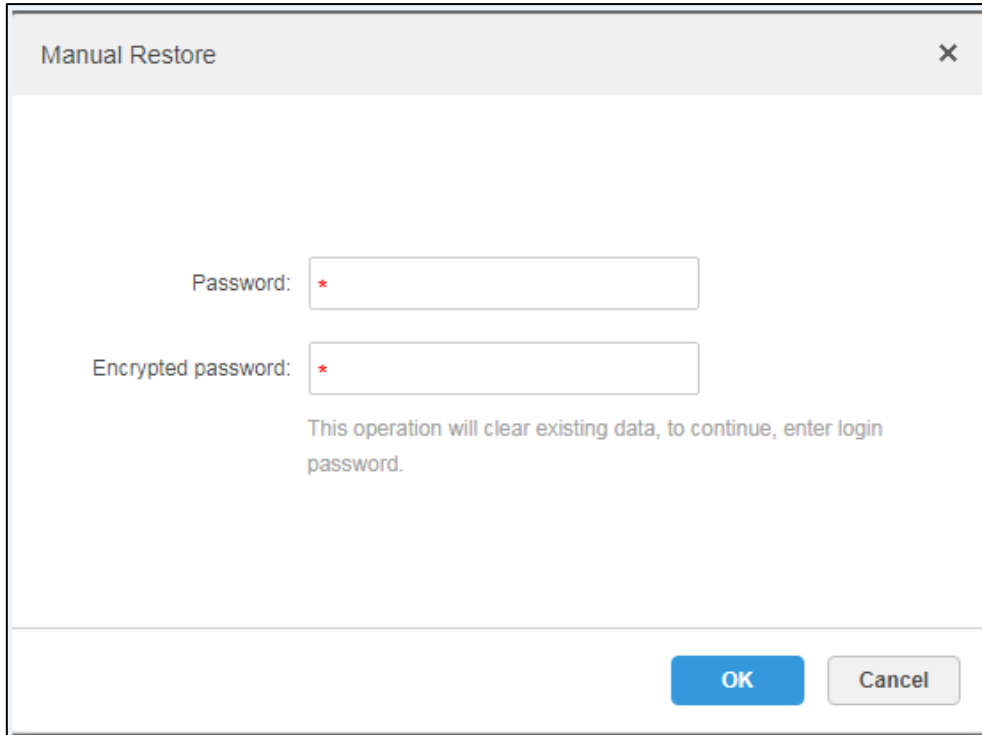
Figure 5-9 Manually restore (1)



Step 3 Click **Browse**, select file and then click **OK**.

Step 4 Enter administrator login **Password** and backup file **Encrypted Password**.

Figure 5-10 Manually restore (2)



Step 5 Click **OK**.

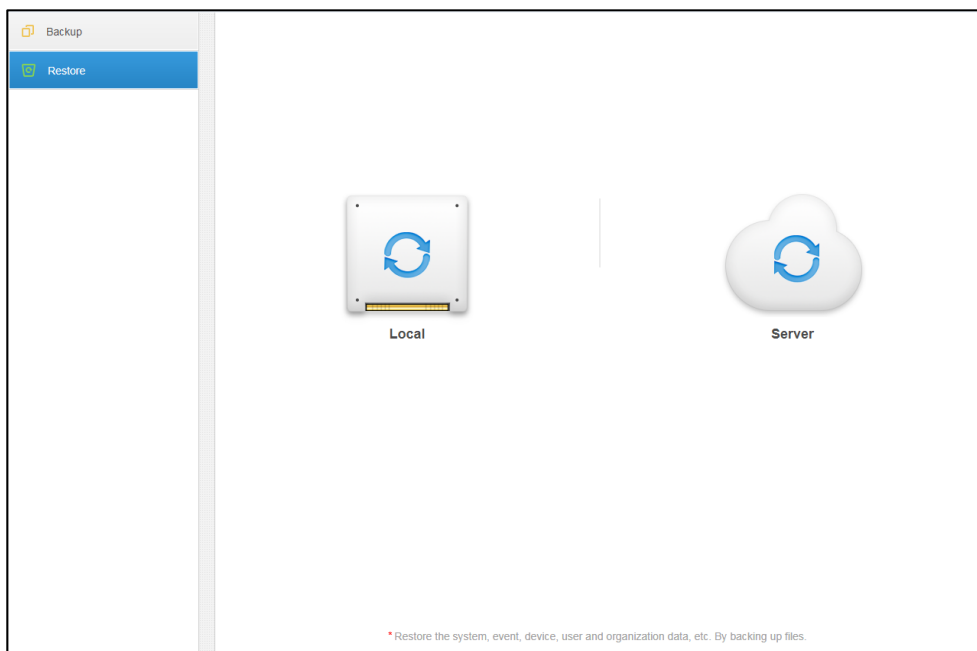
The data is being restored; it will display the restoration percentage via progress bar. The system will start again after it is completed.


Server

It selects to restore the data from the backup file on the server side. The precondition is that it needs to enable the auto backup function, the server end backs up the database according to the set period and form backup file.

Step 1 Select **Restore** tab.

Figure 5-11 Restore



Step 2 Click **Server** and click  from the list and select the file which needs to be restored.

Step 3 Enter admin password, click **OK** and restore.

The system will restart after the data is successfully restored.

5.6 Log

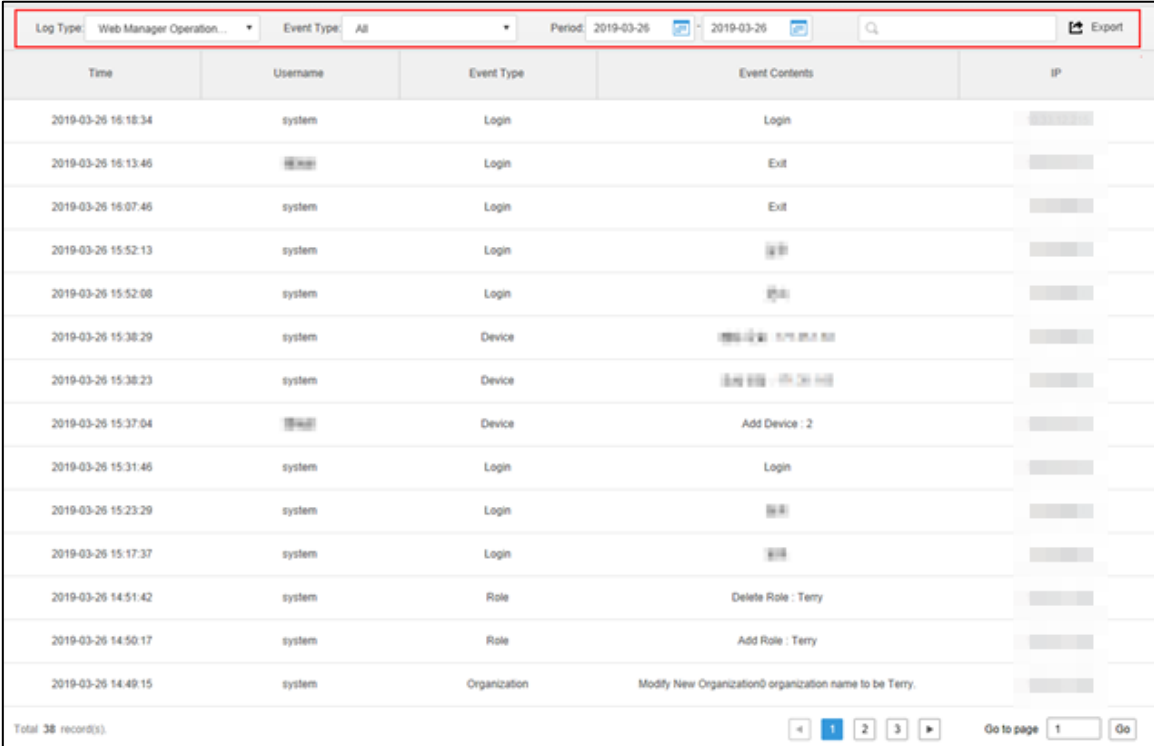
View administrator and operator operation logs. You can filter by event and time.

Take **Management Configuring Log** for an example.

Step 1 Click  and select **Log** on the **New Tab** interface.

Step 2 Select log type, event type or query time.

Figure 5-12 Log



Time	Username	Event Type	Event Contents	IP
2019-03-26 16:18:34	system	Login	Login	
2019-03-26 16:13:46		Login	Exit	
2019-03-26 16:07:46	system	Login	Exit	
2019-03-26 15:52:13	system	Login		
2019-03-26 15:52:08	system	Login		
2019-03-26 15:38:29	system	Device	删除设备: 1:15 删除成功	
2019-03-26 15:38:23	system	Device	添加设备: 1:15 添加成功	
2019-03-26 15:37:04		Device	Add Device : 2	
2019-03-26 15:31:46	system	Login	Login	
2019-03-26 15:23:29	system	Login		
2019-03-26 15:17:37	system	Login		
2019-03-26 14:51:42	system	Role	Delete Role : Terry	
2019-03-26 14:50:17	system	Role	Add Role : Terry	
2019-03-26 14:49:15	system	Organization	Modify New Organization0 organization name to be Terry.	

Total 38 record(s).

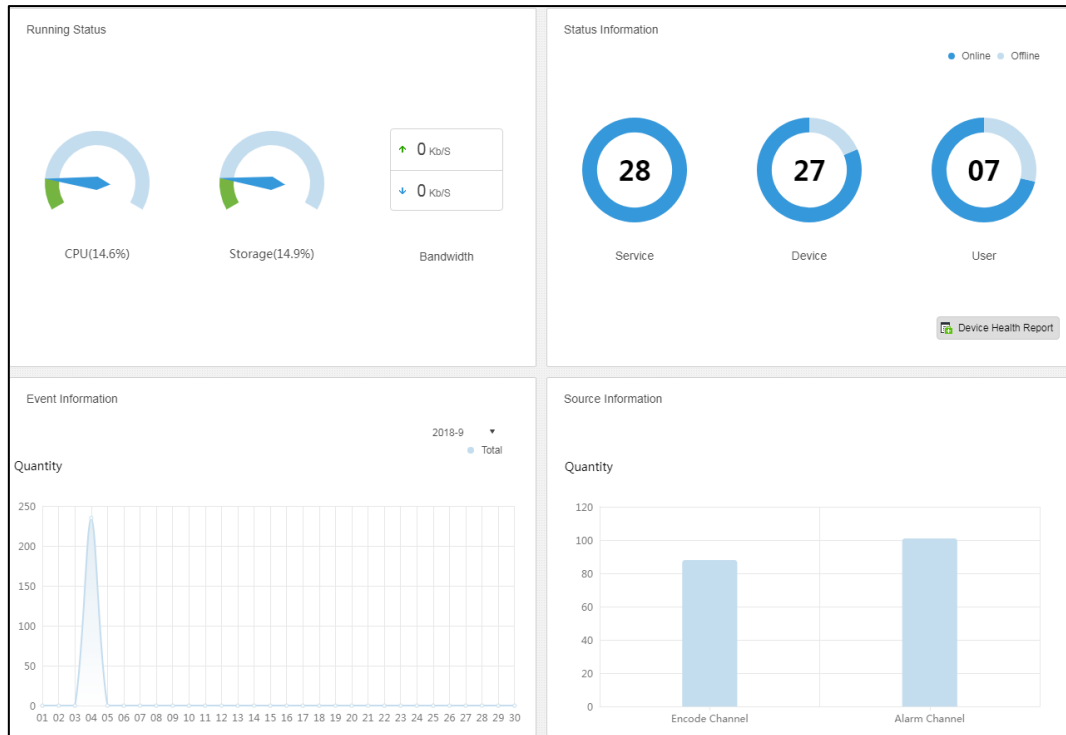
5.7 System Maintenance

View system operation and maintenance statistics to know the system running situation in time.

5.7.1 Overview

Click  on the Web Manager, and then select **Overview**.

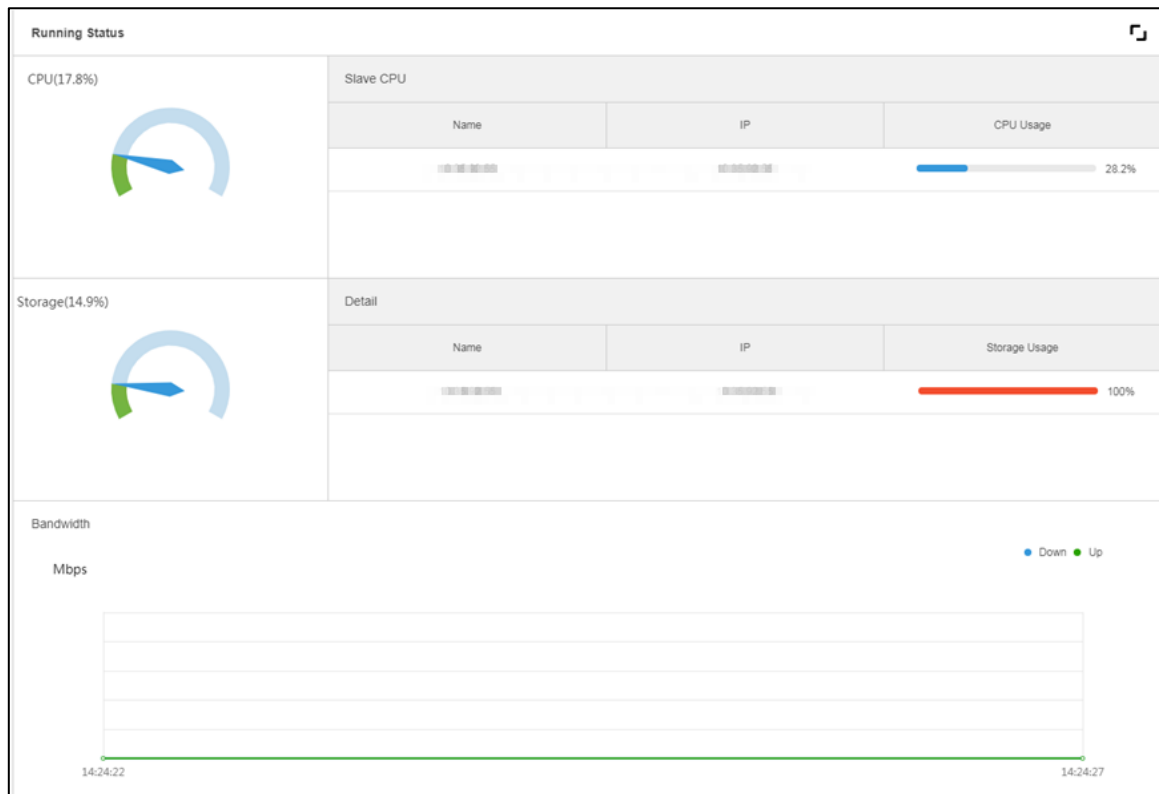
Figure 5-13 Overview



5.7.2 Running Status

Click **Running Status** to view status of CPU, storage, and bandwidth.

Figure 5-14 Running status



5.7.3 Status Information

View the status of server, devices, and users.

Service Status Information

Click on the **Service Status** interface, and then the interface displays service details.

Figure 5-15 Service status

Server Status					
	Name	IP Address	Device ID	Type	Server Status
▶	Center Server		Master	Home Server	Running Status: Running Enable Status: Enable
▶				Home Server	Running Status: Running Enable Status: Enable

Device Status Information

Step 1 Click on the Web Manager, and then select **Overview**.

Step 2 Click **Device Status**.

Figure 5-16 Real-time device status

Device Status				
Device ID	Status	Device Name	Org	IP/Domain
1000050	Online	NVR51	Terry	
1000049	Online	VTO63	Terry	
1000001	Online	FR Access Standalone	PYL	
1000048	Offline	2	root	
1000024	Offline	Decoder	root	

Step 3 Check device status.

- Click the **Real Time** tab on the device status information interface to view device real-time status.
- Click the **History** tab on the device status information interface to view device history status.

Figure 5-17 View real-time/history device status

Time	Status	Device Name	Org Name	IP/Domain
2017-04-08 11:51:45	Online		root	
2017-04-08 11:51:45	Online		root	
2017-04-08 11:51:45	Online		root	
2017-04-08 11:51:44	Online		root	
2017-04-08 11:51:17	Online		root	
2017-04-08 11:51:17	Online		root	
2017-04-08 11:51:17	Online		root	
2017-04-08 11:51:16	Online		root	
2017-04-07 01:23:22	Online		root	
2017-04-07 01:19:19	Offline		root	
2017-04-07 01:19:16	Offline		root	
2017-04-06 11:46:04	Online		root	
2017-04-06 11:42:36	Offline		root	
2017-04-06 11:42:33	Offline		root	

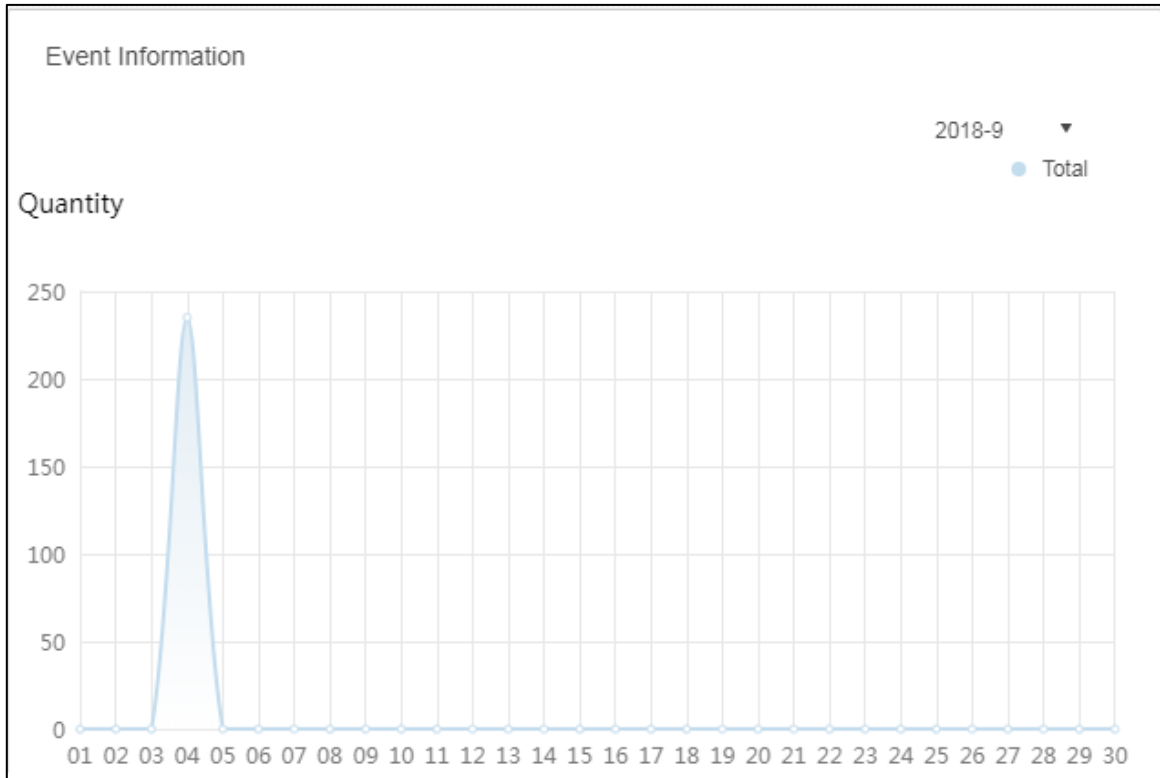
Step 4 Click **Export** to exports device real-time status information (PDF format).

Step 5 Click **User State** and **Device Health Report** to view details.

5.7.4 Event Information

View total number of alarm events and processed events by month.

Figure 5-18 Event information



5.7.5 Source Information

View the statistics of video channels and alarm channels. Click **Source Information** or the icon below to go to the detailed interface.

- View video channel details.

Figure 5-19 Video channel details

Name	Device	Org	SN	Camera Type
[blurred]	[blurred]	KL	[blurred]	Fixed Camera
[blurred]	[blurred]	ANPR	[blurred]	Fixed Camera
[blurred]	[blurred]	ANPR	[blurred]	Speed Dome
[blurred]	[blurred]	KL	[blurred]	Fixed Camera
37723_1	37723	ANPR	[blurred]	Speed Dome
Slot04-01	M70-E	TV WALL	[blurred]	Speed Dome
Slot04-02	M70-E	TV WALL	[blurred]	Speed Dome
Slot04-03	M70-E	TV WALL	[blurred]	Speed Dome
Slot04-04	M70-E	TV WALL	[blurred]	Speed Dome
Slot06-01	M70-E	TV WALL	[blurred]	Speed Dome
Slot06-02	M70-E	TV WALL	[blurred]	Speed Dome
Slot06-03	M70-E	TV WALL	[blurred]	Speed Dome
Slot06-04	M70-E	TV WALL	[blurred]	Speed Dome
[blurred]	M70-E	TV WALL	[blurred]	Speed Dome

- Click the **Alarm** tab to view the details of alarm channels.

Appendix 1 Service Module Introduction

Service Name	Service Name	Function Description	Port	Protocol Type
Center Management Service	DSS_WEB	Center management service is to manage each service and provide accessing port.	HTTPS: 443	TCP
Message Queue Service	DSS_MQ	Message queue service is to transfer messages between the platforms.	61616	TCP
DMS (Device Management Service)	DSS_DMS	Device management service is to register front-end encoder, receive alarm, transfer alarm and send out sync time command.	9200	TCP
MTS (Media Transmission Service)	DSS_MTS	Media transmission service is to get the audio/video bit stream from the front-end device and then transfer these data to the SS, client and decoder.	9100	TCP
SS (Storage Service)	DSS_SS	Storage service is to storage/search/playback record.	9320	TCP
VMS (Video Matrix Service)	DSS_VMS	Video matrix service is to login the the decoder and send out task to the decoder to output to the TV wall.	Not fixed, do not need to be mapped to the outside.	TCP
MGW (Media Gateway Service)	DSS_MGW	Media gateway service is to send out MTS service to the decoder.	9090	TCP
ARS (Auto Register Service)	DSS_ARS	Auto register service is to listen, login, or get bit streams to send to MTS.	9500	TCP
PCPS (ProxyList control Proxy Service)	DSS_PCPS	ProxyList control Proxy Service is to login Hikvision device, ONVIF device, and then get the stream and transfer the data to MTS.	5060 14509	UDP TCP
ADS (Alarm Dispatch Service)	DSS_ADS	Alarm dispatch service is to send out alarm information to different objects according to the plans.	9600	TCP

MCD (Multi-Control Device)	DSS_MCD	Deals with alarm devices access. The MCD service simulates devices and deals with access of SDK of alarm controllers, access control devices and dynamic environment monitoring devices.	30001	TCP
PES (Power Environment Server)	DSS_PES	Deals with access of dynamic environment monitoring devices.	11001	TCP
SC (Switch Center)	DSS_SC	Deals with PC client and App client login as SIP client, and also forwards the audio-talk stream.	28001	TCP
OSS (Object Storage Service)	DSS_OSS	Deals with storage of face snapshots and intelligent alarm pictures.	9901	TCP
PTS (Picture Transfer Server)	DSS_PTS	Deals with picture transmission	13001	TCP

Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. Enable Whitelist

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

11. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

14. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.

ENABLING A SAFER SOCIETY AND SMARTER LIVING