

General Surveillance Management Center

User's Manual

V1.0.4






Foreword

General

This user's manual (hereinafter referred to be "the manual") introduces the functions and operations of the DSS general surveillance management center (hereinafter referred to as "the system") 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
V1.0.4	V1.001.0000001.1	<ul style="list-style-type: none">Deleted POS, attendance and thermal module.Modified personnel management, and access control.	June 2020
V1.0.3	V1.001.0000001	<ul style="list-style-type: none">Added visitor management, alarm controller, electronic focus, smart search, and intelligent analysis configuration.Optimized licensing,	December 2019

Document Version	Software Version	Revision Content	Release Time
		device configuration, face recognition, personnel management and access control.	
V1.0.2	V1.001.0000000	<ul style="list-style-type: none"> Added the deployment configuration section. Modified system configuration. Deleted business flow chart. 	October 2019
V1.0.1	V1.001.0000000	<ul style="list-style-type: none"> Added new functions such as RAID group config, personnel management, access control management, thermal, target detection, device config, entrance, attendance management and video intercom. Modified contents such as edit device, flow analysis, plate recognition. Deleted business function. 	April 2019
V1.0.0	–	First release	September 2018

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 refer to 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 refer to our final explanation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	I
1 Overview	1
1.1 Introduction	1
1.2 Highlights	1
2 Deployment Methods	2
2.1 Configuring Single-server Deployment.....	3
2.2 Configuring Distributed Deployment.....	6
2.3 Configuring N+M.....	7
2.4 Configuring Hot Spare	10
3 Configuring Basic Settings	11
3.1 Login and Password Initialization	11
3.2 Quick Guide	12
3.3 Segment Setup	17
3.4 CMS	17
3.5 Basic.....	17
3.5.1 Manage Account.....	17
3.5.2 Maintenance	18
3.5.3 Time Setup.....	19
3.5.4 Route Setup.....	20
3.5.5 Ping Check.....	21
3.5.6 URL Detect	22
3.5.7 Log.....	23
3.6 Security Setup.....	23
3.6.1 SSH Connection Setup.....	23
3.6.2 HTTPS Setting.....	24
3.6.3 Enabling TLS	25
3.7 Self-check	25
3.8 Advanced Setting	27
3.8.1 Configuring Master/Slave	27
3.8.2 Configuring Hot Spare	28
3.9 Upgrade System	31
4 Manager Operations	32
4.1 Logging in to Web Manager.....	32
4.2 System Settings	33
4.2.1 Setting System Parameters.....	33
4.2.2 Setting Mail Server	35
4.3 Adding Organization.....	36
4.4 Adding Role and User	37
4.4.1 Adding User Role.....	37
4.4.2 Adding User	39

4.4.3 Setting Domain User.....	41
4.5 Adding Devices	44
4.5.1 Adding Devices Manually	44
4.5.2 Adding Devices through Auto Search.....	46
4.5.3 Importing Video Intercom Device	47
4.5.4 Editing Devices	49
4.5.5 Binding Resources.....	52
4.6 Configuring Record Plan.....	54
4.6.1 Configuring Storage Disk.....	54
4.6.2 Setting Disk Group Quota.....	59
4.6.3 Adding General Plan.....	60
4.6.4 Adding Backup Record Plan.....	62
4.6.5 Adding Time Template	63
4.7 Configuring Event	65
4.8 Configuring Map.....	75
4.8.1 Adding Map.....	76
4.8.2 Marking Devices	81
4.9 Adding Video Wall	82
4.10 Configuring Face Recognition	84
4.10.1 Creating Face Database.....	84
4.10.2 Arming a Face Recognition Channel.....	90
4.11 Adding Vehicle Blacklist	92
4.12 Video Intercom Management.....	95
4.12.1 Configuring Building/Unit.....	95
4.12.2 Synchronizing Contacts.....	96
4.12.3 Setting Private Password	97
4.12.4 APP User	98
4.13 System Maintenance	99
4.13.1 Server Management	99
4.13.2 Backup and Restore	101
4.13.3 Log	107
4.13.4 Overview	108
5 Client Functions	114
5.1 Client Installation and Login.....	114
5.1.1 PC Requirements	114
5.1.2 Downloading and Installing Client	114
5.1.3 Logging in to Client.....	117
5.2 Local Configuration	119
5.3 Live Video.....	125
5.3.1 Preparations	125
5.3.2 Live View.....	126
5.3.3 Device Configuration	132
5.3.4 PTZ	149
5.3.5 Fisheye-PTZ Smart Track.....	155
5.3.6 Bullet-PTZ Smart Track	158
5.3.7 Electronic Focus	165
5.3.8 View Tour	167

5.3.9 Region of Interest (RoI)	168
5.4 Configuring Intelligent Analysis	169
5.4.1 Intelligent Analysis Configuration Interface	169
5.4.2 IVS	170
5.4.3 Face Detection	191
5.4.4 People Counting	198
5.4.5 Heatmap	205
5.5 Record	210
5.5.1 Preparations	210
5.5.2 Record Playback	211
5.5.3 Search Thumbnail	217
5.6 Record Download	220
5.6.1 Preparation	220
5.6.2 Timeline	220
5.6.3 File List	222
5.6.4 Label	223
5.7 Event Center	224
5.7.1 Preparations	224
5.7.2 Configuring Alarm Parameters	225
5.7.3 Searching and Processing Real-Time Alarm	226
5.8 Video Wall	230
5.8.1 Preparations	230
5.8.2 Video Wall Display	232
5.8.3 Video Wall Plan	234
5.9 Emap	237
5.9.1 Preparations	237
5.9.2 Opening Emap in Live View	237
5.9.3 Viewing Map	239
5.9.4 Alarm Flashing on the Map	241
5.10 Flow Analysis	242
5.10.1 Preparations	242
5.10.2 Heatmap	243
5.10.3 People Counting Report	245
5.11 Human Face Recognition	246
5.11.1 Preparations	246
5.11.2 Real-Time Human Face Video	246
5.11.3 Face Search	248
5.11.4 Face Recognition Record Search	253
5.11.5 Statistics Report	256
5.12 Number Plate Recognition Applications	257
5.12.1 Preparations	257
5.12.2 Number Plate Recognition	258
5.12.3 Searching Passed Vehicle	259
5.12.4 Vehicle Track	262
5.12.5 Vehicle Alarms	264
5.13 Target Detection	267
5.13.1 Preparations	267

5.13.2 View Real-time Detection	268
5.13.3 Searching for Snapshot Targets	270
5.13.4 Statistical Report.....	272
5.14 Personnel Management.....	273
5.14.1 Configuring Personnel Information	273
5.14.2 Configuring Door Groups.....	307
5.14.3 Configuring Super Passwords.....	309
5.14.4 Configuring Time Templates	311
5.14.5 Configuring Holiday Schedules	312
5.15 Access Control	314
5.15.2 Adding Access Control.....	315
5.15.3 Personnel Management	318
5.15.4 Advanced Function	319
5.15.5 Setting Record Plan.....	333
5.15.6 Access Control Application	334
5.15.7 Device Maintenance	345
5.16 Entrance.....	347
5.16.1 Preparations	348
5.16.2 Adding Device.....	348
5.16.3 Personnel Management	354
5.16.4 Configuring Alarm Scheme.....	354
5.16.5 Configuring Parking Lot.....	355
5.16.6 Vehicle Management	362
5.16.7 Overview	364
5.16.8 License Plate Recognition.....	366
5.16.9 Info Query	367
5.17 Video Intercom	372
5.17.1 Preparations	372
5.17.2 Call Management.....	373
5.17.3 Video Intercom Application	378
5.18 Visitor Management	386
5.18.1 Preparations	386
5.18.2 Visitor Appointment.....	387
5.18.3 Visit Registration.....	388
5.18.4 End Visit Registration	394
5.18.5 Searching for Visit Records	395
5.19 Alarm Controller	397
5.19.1 Preparations	397
5.19.2 Alarm Controller Interface.....	398
5.19.3 Updating Alarm Controller Status	400
5.19.4 Alarm Controller Operation	401
5.20 Time Synchronization.....	407
5.20.1 Device Time Synchronization	407
5.20.2 Time Synchronization on the Client.....	407
Appendix 1 Service Module Introduction	410
Appendix 2 Cybersecurity Recommendations	412

Important Safeguards and Warnings

This Chapter describes the contents covering proper handling of the Device, hazard prevention, and prevention of property damage. Read these contents carefully before using the Device, comply with them when using, and keep it well for future reference.

Operation Requirement

- Do not place or install the Device in a place exposed to sunlight or near the heat source.
- Keep the Device away from dampness, dust or soot.
- Keep the Device installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the Device, and make sure there is no object filled with liquid on the Device to prevent liquid from flowing into the Device.
- Install the Device in a well-ventilated place, and do not block the ventilation of the Device.
- Operate the device within the rated range of power input and output.
- Do not disassemble the Device.
- Transport, use and store the Device under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Device; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

1 Overview

1.1 Introduction

DSS is a type of video surveillance platform which is flexible, easily-extendable, highly-reliable and more professional. DSS platform is able to meet the requirements of large and medium-sized projects via distributed extension. In addition to basic video surveillance business, DSS platform supports target detection and a series of AI functions, such as face recognition, license plate recognition, people counting, etc. It can also expand functions like business analysis and access control via value-added modules. These rich functions enable DSS platform to be widely used in chain supermarket, casino, safe city, medium and large-sized campus surveillance and some other scenarios.

1.2 Highlights

- Easily extendable
 - ◇ Supports system performance extension.
 - ◇ Supports feature extension with add-on functions.
- More professional
 - ◇ Supports maintenance of services, devices, time and other basic system information.
 - ◇ Separate Web Manager that makes management more convenient and professional.
 - ◇ Supports object detection, face recognition, number plate recognition, people counting and other AI functions, access control, and retail functions, making DSS platform more powerful.
- Highly reliable
 - ◇ Supports hot standby, which makes DSS platform more stable.
 - ◇ Supports automatic and manual backup of system data to avoid data loss caused by system crash.
- More open
 - ◇ Supports connection through standard ONVIF protocol and active registration.
 - ◇ Open SDK for third-party integration.

2 Deployment Methods

The DSS platform supports multiple deployment methods, such as single-server deployment, hot spare, distributed deployment and N+M. The server is equipped with platform software on delivery. This chapter is going to introduce the configuration and commissioning of hot spare, distributed deployment and N+M.

Figure 2-1 Single-server deployment

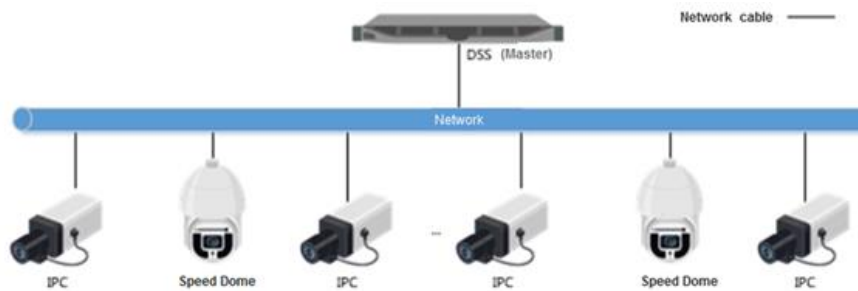


Figure 2-2 Hot spare

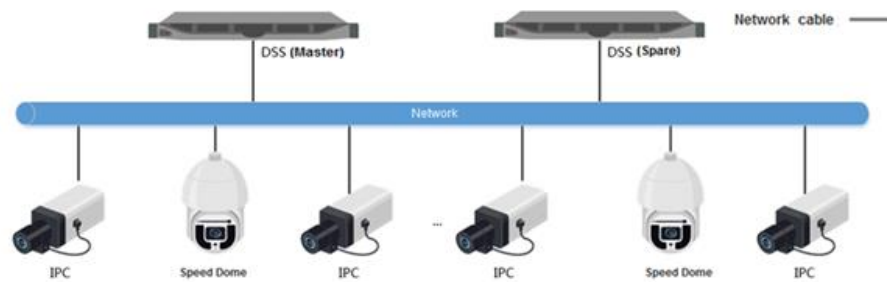


Figure 2-3 Distributed deployment

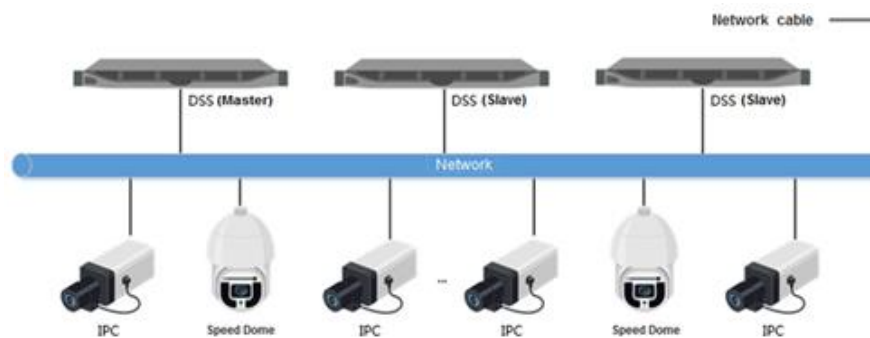
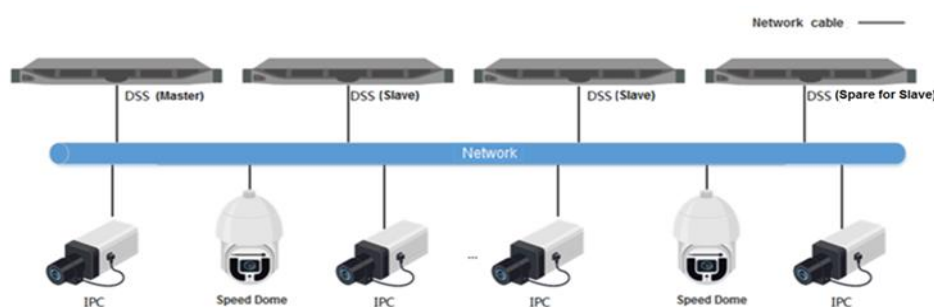


Figure 2-4 N+M





For N+M deployment, you can add one more master server for hot spare of the master server.
For details, see "2.3 Configuring N+M" and "2.4 Configuring Hot Spare."

2.1 Configuring Single-server Deployment

For each server, configure network settings and server working mode before doing the deployment configuration as mentioned in the previous chapter.

Step 1 Log in to the configuration system.

- 1) Enter *DSS IP address/config*, and then press **Enter**.
- 2) Enter username and password. Click **Login**.

The default username is *admin*, password *123456*.



You are required to modify the password for the first-time login. Follow the onscreen instructions to do it.

Step 2 Configure network.

- 1) Click Quick Guide.

Figure 2-5 Network card config

The screenshot shows a configuration page for a network card. At the top, there are two dropdown menus: 'Network Mode' set to 'Multi-address' and 'Default Network Card' set to 'Network card 1[eth0] [1000Mbps]'. Below these is a section titled 'Select network card.' with a dropdown menu also set to 'Network card 1[eth0] [1000Mbps]'. Underneath are several input fields: 'MAC Address' (displayed as a series of grey squares), 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS' (which is highlighted with a blue border).

- 2) Configure parameters of network card.

Table 2-1 Network card parameter description

Parameter	Description
Network Mode	<ul style="list-style-type: none"> Multi-address Multiple network card (hereinafter referred to as NIC) mode. You can configure different network parameters for different NICs to achieve high network reliability. For example, to configure hot spare, the NIC 2 can be used to set spare server IP. This can also be used in iSCSI storage expansion solution. When setting iSCSI storage expansion, NIC 1 can be used for communication, NIC 2 is reserved and NIC 3 and NIC 4 can be used for iSCSI storage. Fault-tolerant Multiple NICs share one IP. Normally, one of them works. When the working NIC fails, another one will automatically take over the job to ensure network stability. Load Balancing Multiple NICs share one IP and work at the same time to share the network load, providing greater network capacity than the single NIC mode. When one of them fails, the network load will be re-distributed among the rest NICs to ensure network stability. Link Aggregation Bind NICs so that all the bound NICs work at the same time and share network load. For example, bind two NICs and set multi-address for the other two NICs. Then the server has three IPs. The bandwidth of the two bound NICs is 2K and the other two are 2K respectively. This is applicable to stream forwarding, not storage.
Add Network Card	When the network mode is fault tolerance, load balance or link aggregation, you need to add network card. Select NIC to bind. You can bind 2 NICs as needed.
Default Network Card	Select default NIC. This NIC will be used as a default NIC to forward data package between non-consecutive network segments such as WAN or public network.
Select Network Card	After NIC is selected or added, its information will be displayed.
MAC Address	Displays the MAC address of the server.
IP Address	After selecting NIC, you can set its IP address, subnet mask, default gateway and DNS server address.
Subnet Mask	
Default Gateway	
Preferred DNS	
Alternate DNS	

3) Click **Save and Reboot** to save configuration and reboot server.

Step 3 Set server time.

Set server time zone and time.



If hot spare is enabled, you need to set NTP time synchronization.

1) Select **Basic > Time Setup**.

Figure 2-6 Time setting

2) Set time parameters.

Table 2-2 Parameters description

Parameter	Description
DST	Select DST to enable DST (Daylight Saving Time).
Time Zone	Select time zone of the server.
Date/Time	System provides three ways to set date and time.
Sync PC	<ul style="list-style-type: none"> Click the box to select date and time. Click Sync PC to sync PC time with system time. Synchronize NTP server time, so as to achieve regular synchronization of platform server time. To manually synchronize time, click Manual Update. <p>For the distributed deployment, N+M mode, and hot spare mode of the platform, you need synchronize NTP server time.</p>
NTP Setup	Select the check box of NTP Setup to enable NTP time synchronization.
NTP Server	Enter NTP server domain or IP and click Manual Update to synchronize time.
Manual Update	
Update Period	Interval of time synchronization between NTP server and platform server. The maximum interval is 65535 minutes.

3) Click **Apply**.

Step 4 Configure server work mode.

- For single-server deployment and hot spare deployment, set the work mode to be **Master**.
- For distributed deployment and N+M deployment, set the work mode to be **Slave**.

1) Select **Advanced Setting > Distribute Config**.

- 2) Select **Master** or **Slave** according to actual config.

Figure 2-7 Configure server mode (master)

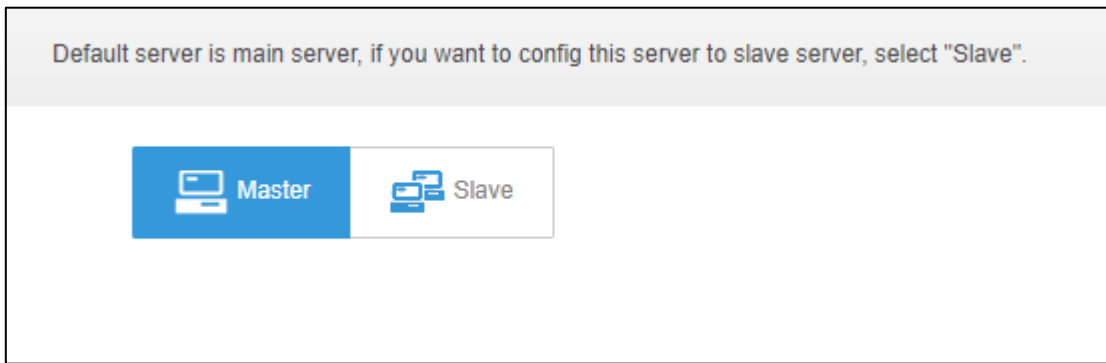
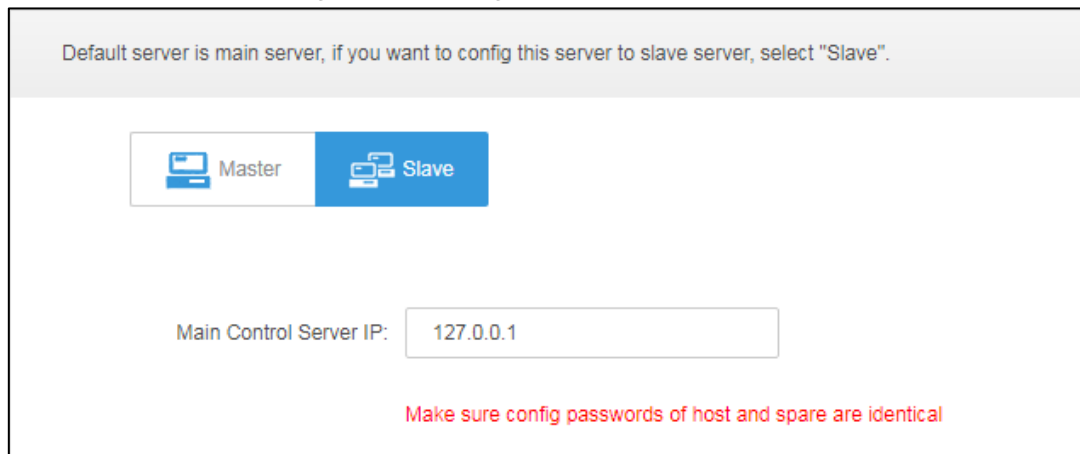


Figure 2-8 Configure server mode (slave)



Step 5 (Optional) If the server is set as **Slave**, enter master server IP address in the **Main Control Server IP** box.

Step 6 Click **Apply**.

2.2 Configuring Distributed Deployment

After each server is correctly configured, the servers automatically complete networking. Enable slave servers on the master server to finish the distributed deployment configuration.

Step 1 Log in to the web interface of the master server.

- 1) In the address bar of browser, enter DSS IP address of the master server, and then press Enter.
- 2) Enter username and password. Click **Login**.
The default username is *system*.



You are required to modify password for the first-time login.

Step 2 Click **+**, and then select **Server Management**.

Step 3 Click the **Server Config** tab.

Slave servers are disabled by default.

Figure 2-9 Server configuration

Name	IP Address	Type	Running Status	Enable Status	Operation
Center Server		Master Server	Running	Enable	⚙️
		Slave Server	Offline	OFF	👁️ ⚙️ ✖️
		Alternate Server	Offline	OFF	👁️ ⚙️ ✖️

Step 4 Click **OFF** of 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**.

2.3 Configuring N+M

After each server is correctly configured, the servers automatically complete networking. Enable slave servers on the master server and confirm the relation between slave servers and spare servers.

Step 1 Log in to the Web interface of the master server.

- 1) In the address bar of browser, enter DSS IP address of the master server, and then press Enter.
- 2) Enter username and password. Click **Login**.

The default username is *system*.



You are required to modify password for the first-time login.

Step 2 Click **+**, and then select **Server Management**.

Step 3 Click the **Server Config** tab.

Slave servers are disabled by default.

Figure 2-10 Server configuration

Name	IP Address	Type	Running Status	Enable Status	Operation
Center Server		Master Server	Running	Enable	⚙️
		Slave Server	Offline	OFF	👁️ ⚙️ ✖️
		Alternate Server	Offline	OFF	👁️ ⚙️ ✖️

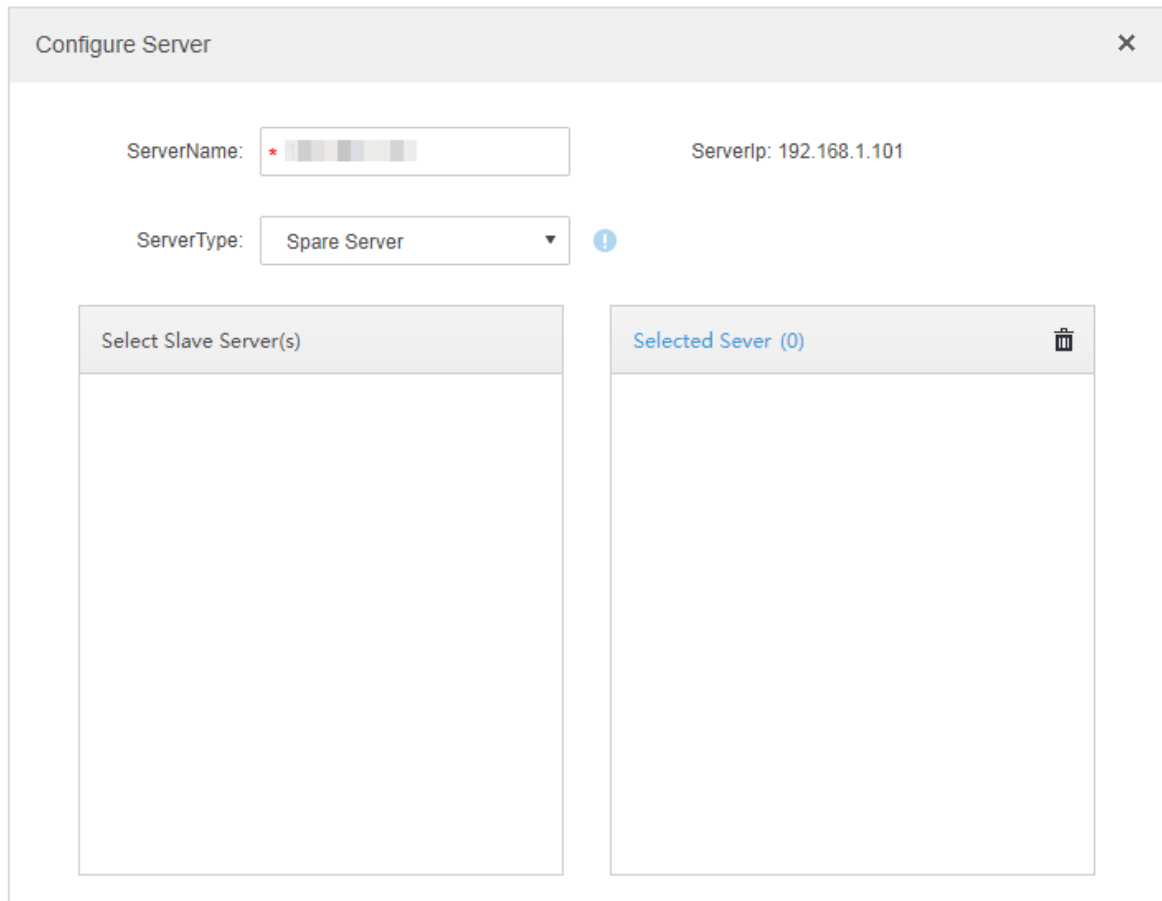
Step 4 Click **OFF** next to each slave server to enable all the slave servers.

When disabled, server status is shown as **Offline**; when enabled and if the server works normally, its status is shown as **Running**.

Step 5 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 2-11 Configure server (1)



Step 6 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.

2) Select one or more spare servers in the **Select Spare Server(s)** list.



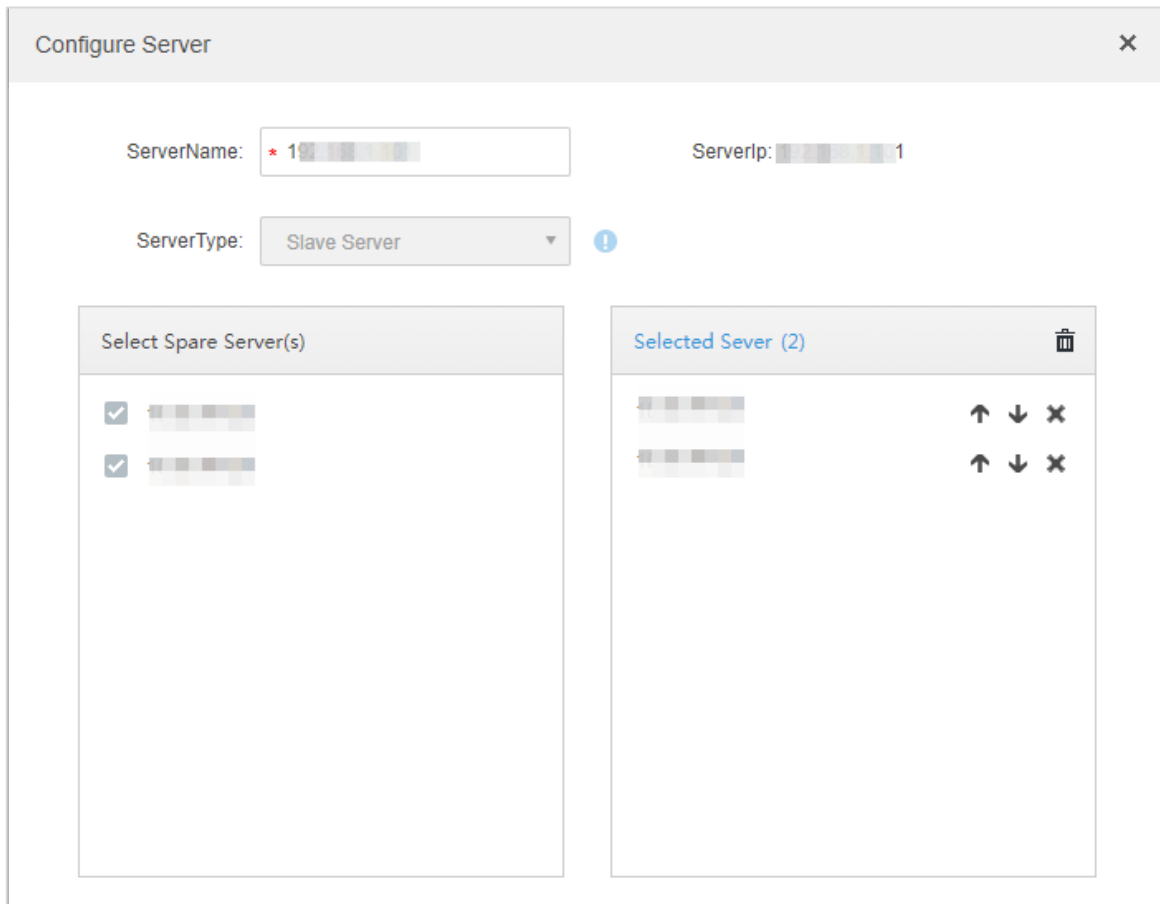

The selected servers are listed on the right. Click   to adjust the priority.

Figure 2-12 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.
- 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 2-13 Configure server (3)

Configure Server

ServerName: * [Masked]

ServerIp: [Masked]

ServerType: Spare Server ⓘ

Select Slave Server(s)

Selected Sever (0) 🗑️

3) Click **OK**.

2.4 Configuring Hot Spare

Configure hot spare server so that when the main server fails, the spare server can take over the job and ensure system stability. For details, see "3.8.2 Configuring Hot Spare."

3 Configuring Basic Settings

Log in to the Config system (configuration system) to quickly configure network parameters, basic parameters, safety parameters and hot spare, as well as system upgrade and self-check.



Make sure that device installation and deployment has been completed before logging into the Config system. For detailed deployment procedures, see *DSS General Surveillance Management Center Applications and Deployment Guide* for more details.

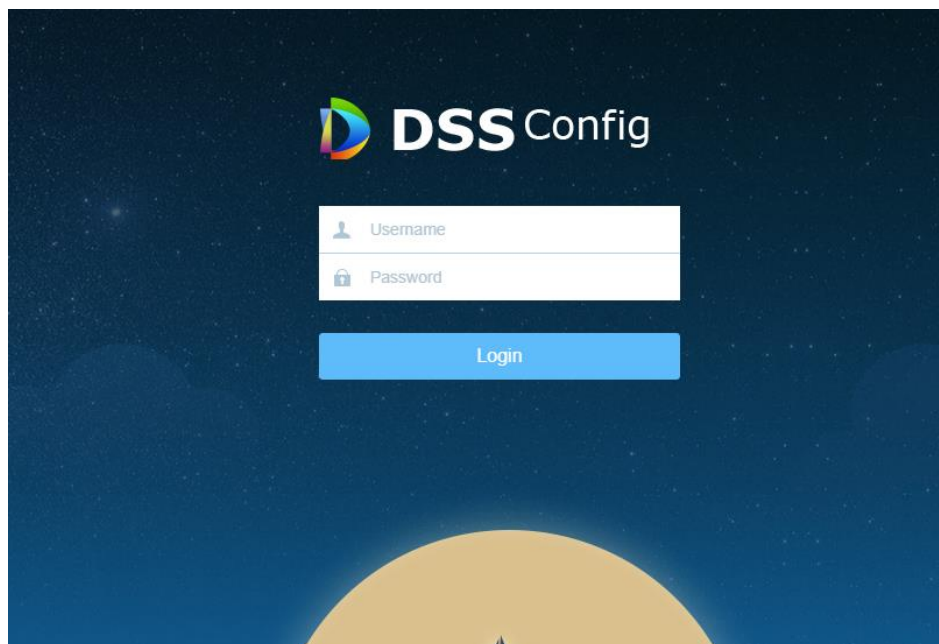
3.1 Login and Password Initialization



Make sure that the PC and server are in the same network segment. If not, please change the IP address of the PC. The default IP address of the server is 192.168.1.108.

Step 1 Enter *DSS platform IP address/config* into the browser, press Enter.

Figure 3-1 Log in to Config system



Step 2 Enter username and password (Default user name is admin, default password is 123456), click **Login**. The reset password interface is displayed.

Figure 3-2 Reset password

Reset Password

Reset Password

Old Password:

New Password:

Confirm:

Security Question

Security Question 1:

Answer:

Security Question 2:

Answer:

Security Question 3:

Answer:

OK

Step 3 Enter old password, new password and set three security questions.

Step 4 Click **OK** to complete initialization.

Service is restarted and you need to log in to the system again.

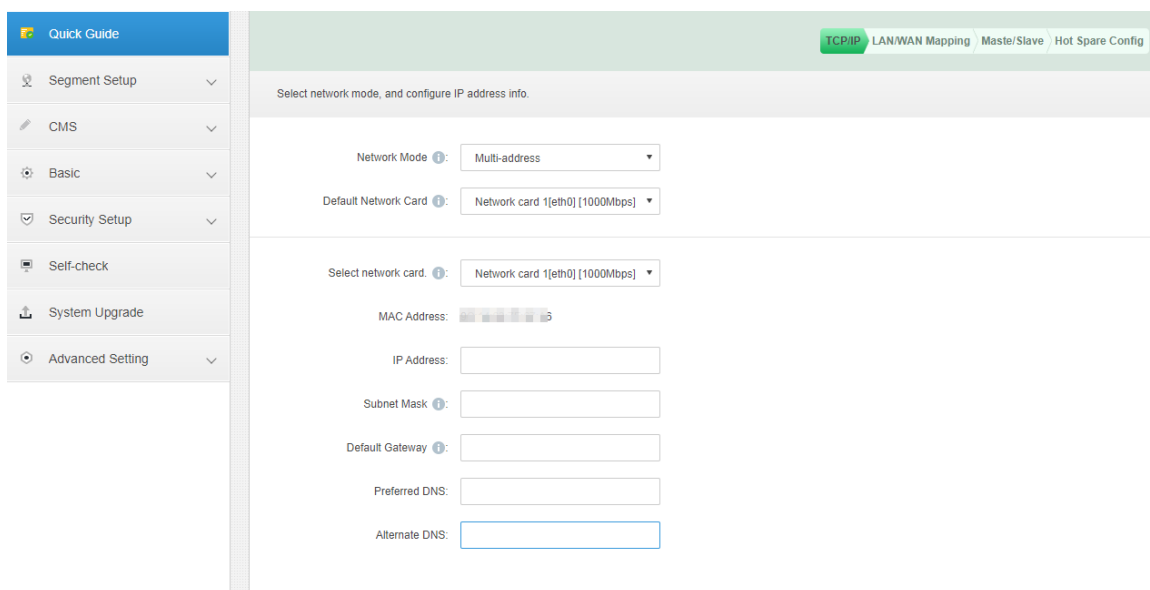
3.2 Quick Guide

Users can quickly configure the platform's network, LAN/WAN network mapping and hot spare through quick guide.

Step 1 Log in to the configuration system.

Step 2 Click **Quick Guide**.

Figure 3-3 Network card config



Step 3 Configure parameters of network card.

Table 3-1 Network card parameter description

Parameter	Description
Network Mode	<ul style="list-style-type: none"> Multi-address Multiple network card (hereinafter referred to as NIC) mode. You can configure different network segments for multiple NICs. This mode is suitable for scenarios that require high network reliability. For example, to configure hot spare, the NIC 2 will be used to set spare server IP; it can also be used in ISCSI storage expansion solution. When setting ISCSI storage expansion, NIC 1 can be used for communication, NIC 2 is reserved and NIC 3 and NIC 4 can be used for ISCSI storage. Fault-tolerant Multiple NICs share one IP. Normally, one of them works. When the working NIC is fails, another one will automatically take over job to ensure network stability. Load Balancing Multiple NICs share one IP and work at the same time to share the network load, providing greater network capacity than the single NIC mode. When one of them fails, the network load will be re-distributed among the rest NICs to ensure network stability. Link Aggregation Bind NIC for network communication. All bound NICs work at the same time and share network load. For example, bind two NICs and set multi-address for the other two NICs. Then the server has three IPs. The bandwidth of the two bound NICs is 2K and the other two

Parameter	Description
	are 2K respectively. This is applicable to stream forwarding, not storage.
Add Network Card	When the network mode is fault tolerance, load balance or link aggregation, you need to add network card. Select NIC to bind. You can bind 2 NICs as needed.
Default Network Card	Select default NIC. This NIC will be used as a default NIC to forward data package between non-consecutive network segments such as WAN or public network.
Select Network Card	After NIC is selected or added, its information will be displayed.
MAC Address	Displays the MAC address of the server.
IP Address	After selecting NIC, you can set its IP address, subnet mask, default gateway and DNS server address.
Subnet Mask	
Default Gateway	
Preferred DNS	
Alternate DNS	

Step 4 Click **Save and Restart**, save network card config and restart server.

Step 5 After server restarts, use **DSS Platform IP Address/Config** to visit Config system again. The IP address has been configured.

Step 6 Click **Quick Guide** and click **Skip**.

Figure 3-4 LAN/WAN mapping

Step 7 Configure WAN address and port info.

Table 3-2 Network card parameter description

Parameter	Description
IP Address	Sets the address of DSS platform.
Web Service Port	Default web service port is 80, it needs to use IP: Port to access WEB if it is not 80. For example, port 81; enter http://172.7.54.35:81/config to access Config system.
Router Address	Sets WAN access IP address of router.
CMS	Center management service, which is responsible for registration and signaling scheduling of other services, it is 9010 by default.

Parameter	Description
SS	Storage playback service, which is in charge of video storage, query and playback, it is 9320 by default.
ARS	Active registration service, which is responsible for actively registering the device to monitor, log in and forward stream to MTS, it is 9500 by default.
MQ	MQ service, which is responsible for information interaction, it is 61616 by default.
DMS	Device management service, which is responsible for logging into the front-end encoder, receiving alarm, forwarding alarm and sending timing command, it is 9200 by default,
ADS	Alarm distribution service, which is responsible for sending alarm information to different objects according to the plan, it is 9600 by default.
MGW	Media gateway, which is responsible for sending MTS address to decoding device, it is 9090 by default.
WEB	Web application service, responsible for administrator config, providing web service interface, providing client embedded function, it is 801 by default.
MTS	Media distribution service, which is responsible for acquiring audio and video streams from front-end devices and distributing them to SS, client and decoder devices. It is 9100 by default.
PES	Power environment surveillance service, which is responsible for managing MCD (including alarm host, access control and so on), it is 9400 by default.
PTS	Picture transmission service, which is responsible for receiving, storing and forwarding ANPR pictures, it is 8081 by default.
OSSHTTP	Picture storage service, which is responsible for receiving, storing and forwarding general pictures, 50000 by default.
OSSHTTPS	Picture storage service which is safer than OSSHTTP, responsible for receiving, storing and forwarding general pictures, 50001 by default.

Step 8 Click **Save and Next**.

Figure 3-5 Server mode (Master)

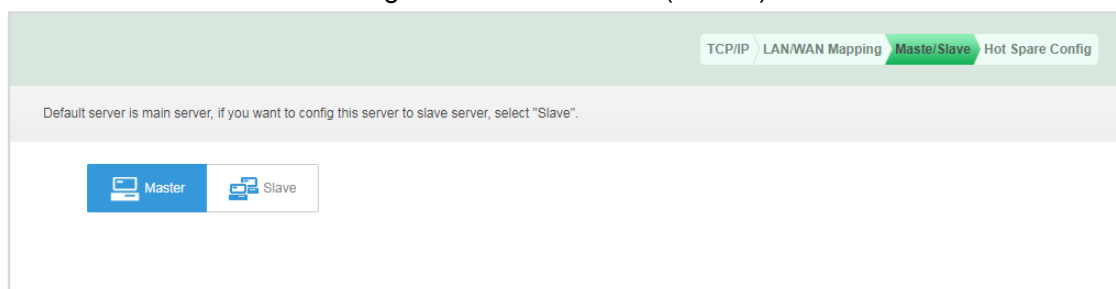


Figure 3-6 Server mode (Slave)


Step 9 Select **Master** or **Slave**.

Step 10 Click **Save and Next**.

Figure 3-7 Hot spare config

Step 11 Configure the parameters of hot spare server.

Table 3-3 Hot spare parameter description

Parameter	Description
Virtual IP	After setting virtual IP, then it can have access to platform via the virtual IP.
Mask	It is in accordance with the mask of network port 1.
Spare Business IP	IP address of spare server network port 1.
Spare Beat IP	IP address of spare server network port 2.
Spare Config System Username	It is the login username and password of spare server Config system.
Spare Config System Password	 The master/spare device need to keep the login password of Config system the same, the password cannot be changed after setting dual hot spare is set.
One-key Check	Click One-key Check to confirm username and password.
Clear Alarm Data	After it is selected, it will clear all alarm data.

Step 12 Click **Save and Next**, save settings and restart the server.

3.3 Segment Setup

In this chapter, you can set network card and LAN/WAN mapping, please refer to "3.2 Quick Guide" for more details.

3.4 CMS

When a device is registering to the platform through Auto Register, the system performs verification. According to the load-balance rule, the server replies re-position. The device registers to the server node after the device receives re-position.

Step 1 Select **CMS > Auto Register re-position**.

Step 2 Enter the re-position port.



To restore to the default port 9005, click **Restore Default**.

Figure 3-8 Reposition port

Quick Guide	Auto register re-position port: 9005	Restore Default
Segment Setup		
CMS		
Auto register re-position		

Step 3 Click **Apply**.

3.5 Basic

3.5.1 Manage Account

You can modify the login password of admin user.



It will restart all services after modifying password. Please make sure if the services have been restarted successfully during use.

Step 1 Select **Basic > Manage Account**.

Figure 3-9 Manage account

Quick Guide

Segment Setup

Basic

> Manage Account

Maintenance

Time Setup

Route Setup

PING Check

URL Detect

Log

Security Setup

Self-check

System Upgrade

Advanced Setting

All services will restart after the new password is changed!

Old Username: admin

Old Password:

New Password:

Confirm:

Step 2 Enter **Old Password**, **New Password** and **Confirm Password**.

Step 3 Click **Apply** and complete modification.



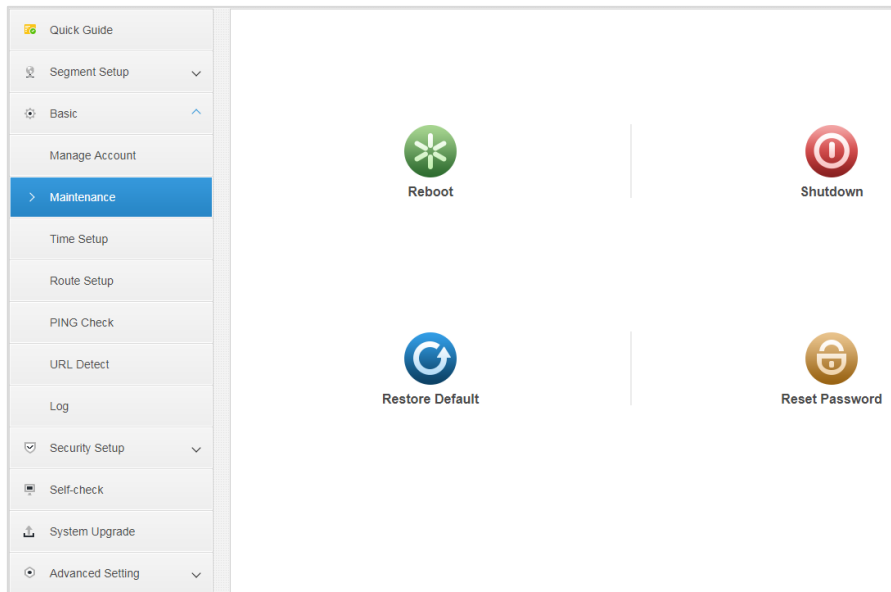
It will restart all the services after the password is modified, please confirm if all the services restart successfully after restart.

3.5.2 Maintenance

In this chapter, you can reboot device, shut down device and restore device to default status. You can also reset password.

Step 1 Select **Basic > Maintenance**.

Figure 3-10 Maintenance



Step 2 Click relevant operation to realize corresponding functions.

- Reboot: Server reboots.
- Shutdown: Server shuts down.
- Restore Default: Restore server to default status.
- Reset Password: Restore the login password of server Config system back to default 123456.

3.5.3 Time Setup

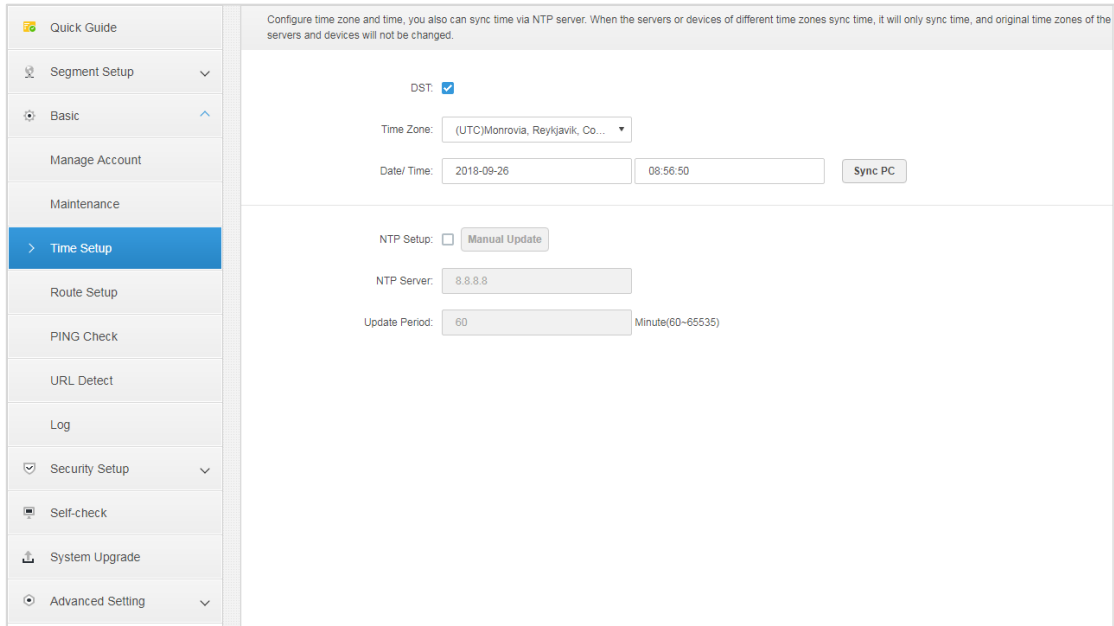
Set time zone and time where the server is located.



If the system enables dual hot spare or sets master slave server, it has to set NTP server for time sync.

Step 1 Select **Basic > Time Setup**.

Figure 3-11 Time setup



Step 2 Configure time parameter.

Table 3-4

Parameter	Description
DST	After selecting DST , it enables DST function.
Time Zone	Selects the time zone where the device is located.
Date/Time	The system provides two methods to set data and time. <ul style="list-style-type: none"> Click display box to select data and time.
Sync PC	<ul style="list-style-type: none"> Click Sync PC and it synchronizes system time to local PC time.
NTP Setup	Selects NTP Setup and then it enables the function of NTP timing update time.
NTP Server	Enter NTP server domain name or IP address; click Manual Update to synchronize the time of NTP time.
Manual Update	
Update Period	The interval between platform server and NTP server sync time. The maximally updates period is 65535 minutes.

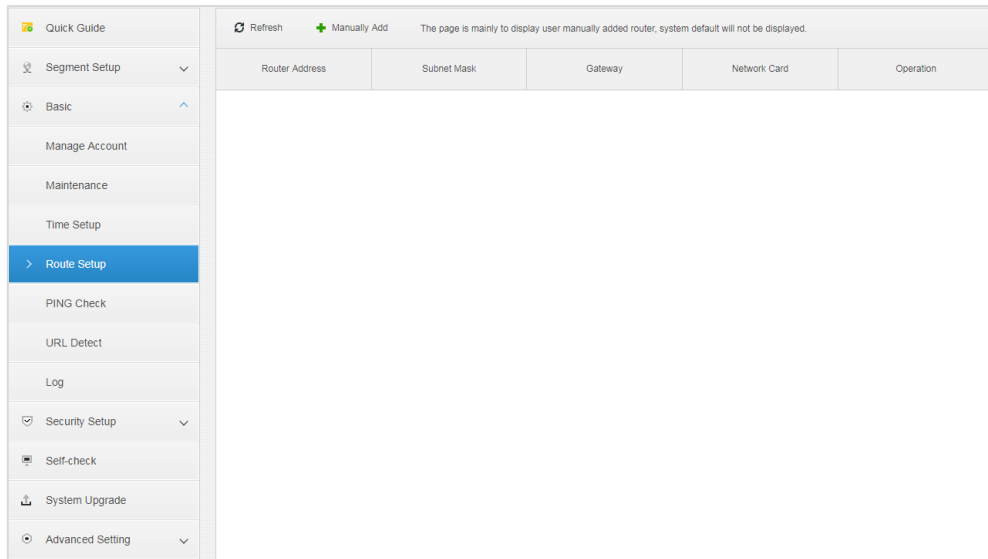
Step 3 Click **Apply** to complete setting.

3.5.4 Route Setup

Add static route and realize the access of LAN and WAN.

Step 1 Select **Basic > Route Setup**.

Figure 3-12 Route setup



Step 2 Click **Manually Add**.

Figure 3-13 Add statistic router

The screenshot shows a dialog box titled 'Add Static Router' with a close button (X) in the top right corner. Inside the dialog, there are three input fields: 'Router Address:', 'Subnet Mask:', and 'Gateway:'. At the bottom right of the dialog, there are two buttons: 'OK' and 'Cancel'.

Step 3 Enter router IP address, subnet mask and default gateway.

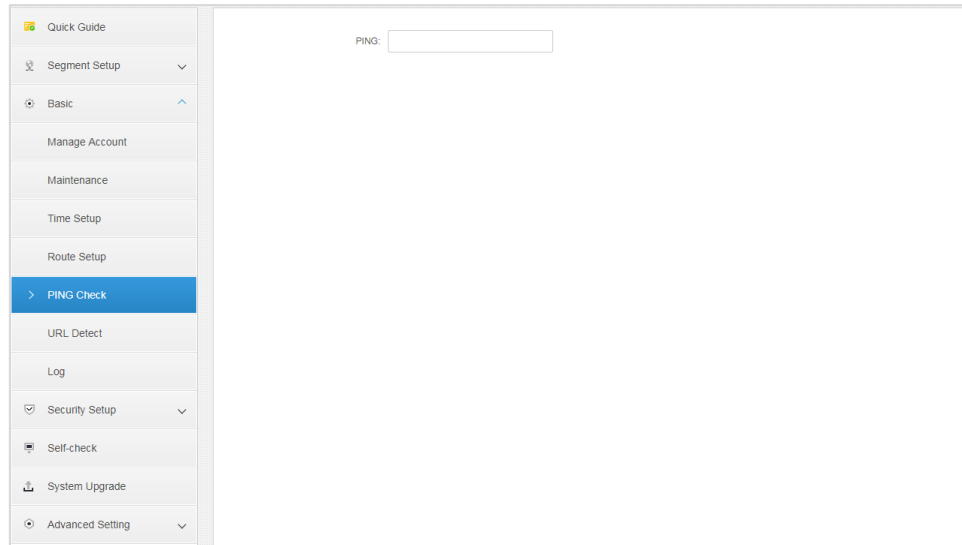
Step 4 Click **OK**.

3.5.5 Ping Check

Check if the platform is interconnected with IP network.

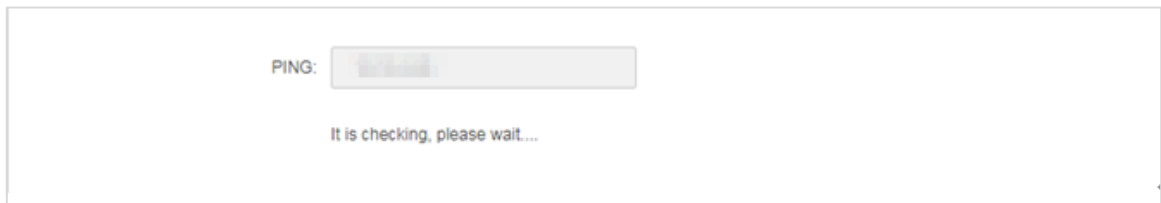
Step 1 Select **Basic > Ping Check**.

Figure 3-14 PING check



Step 2 Enter IP address, click **Apply**.

Figure 3-15 IP

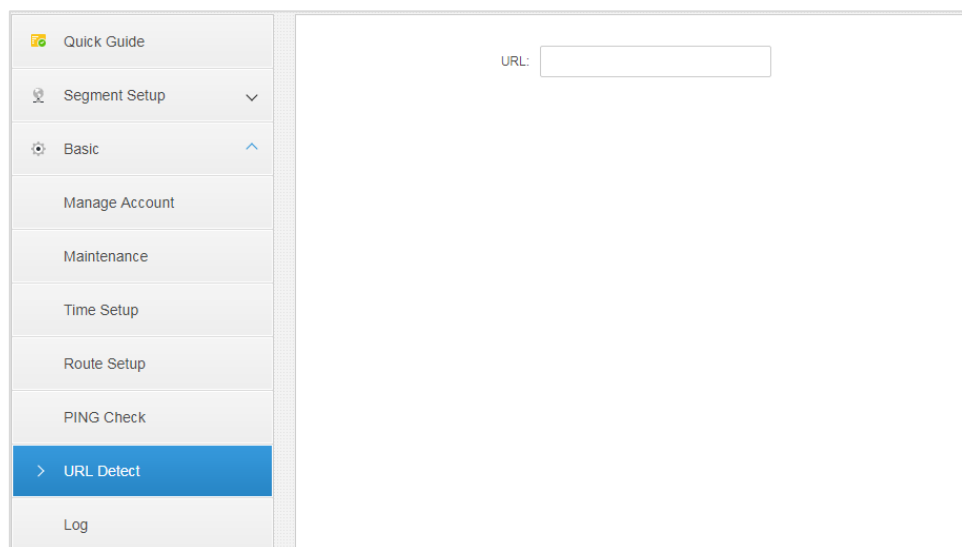


3.5.6 URL Detect

Detect if the platform is interconnected with URL address network.

Step 1 Select **Basic > URL Detect**.

Figure 3-16 URL detection



Step 2 Enter URL address, and then click **Apply**.

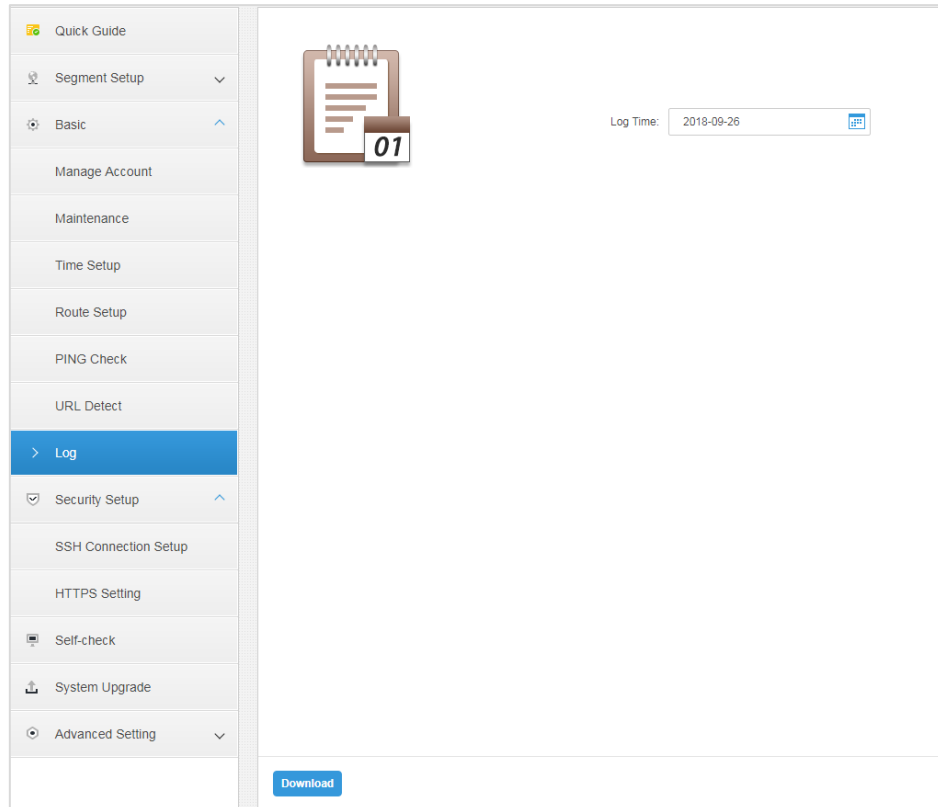
Start to detect if the platform is interconnected with the URL address.

3.5.7 Log

The system supports to download CMS, DMS, MTS, SS and other service logs.

Step 1 Click **Log**.

Figure 3-17 Log



Step 2 Select date, and click **Download** to download log file.

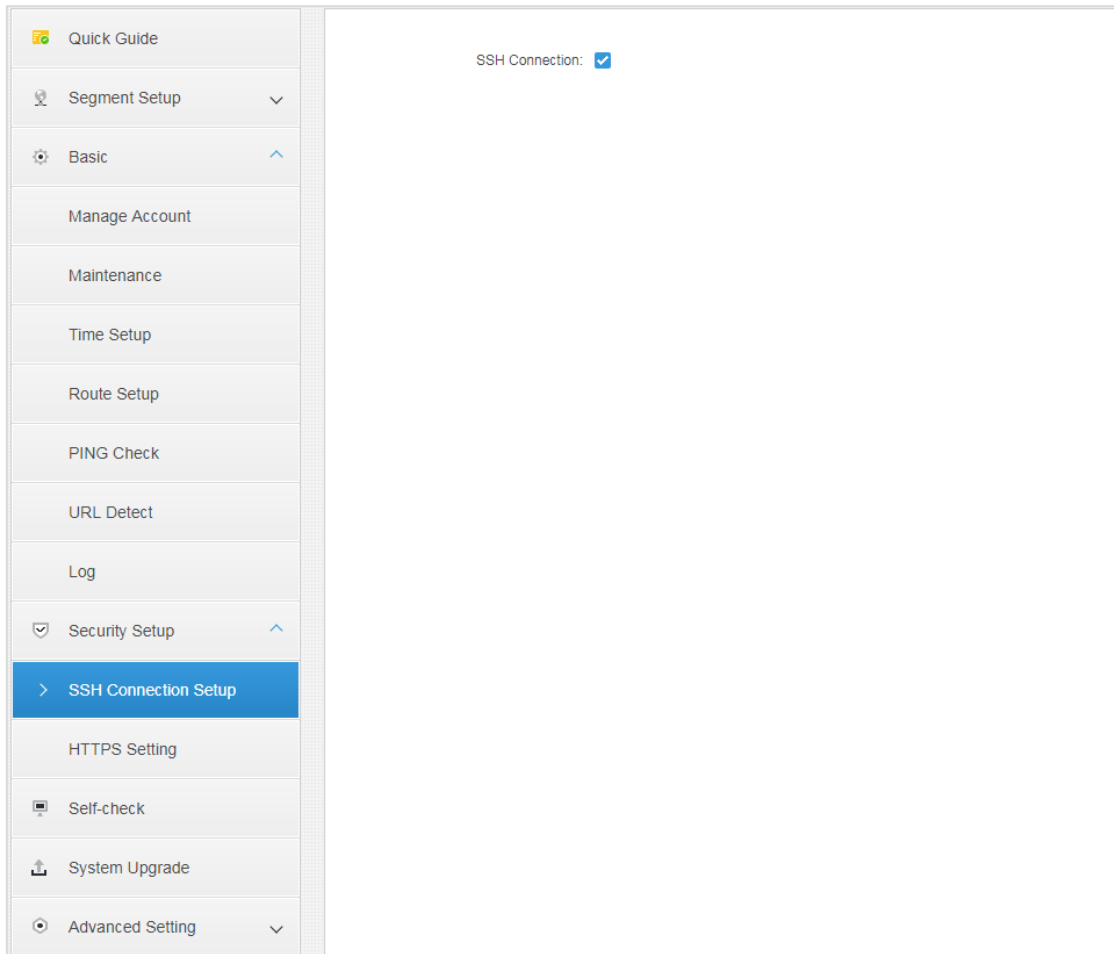
3.6 Security Setup

3.6.1 SSH Connection Setup

After enabling SSH connection, the debugging terminal can log in platform server to debug device via SSH protocol.

Step 1 Select **Security Setup > SSH Connection Setup**.

Figure 3-18 SSH connection



Step 2 Select **SSH Connection**.

Step 3 Click **Apply** to complete setting.

3.6.2 HTTPS Setting

After configuring HTTPS, it can make PC log in platform normally via HTTPS; meanwhile it can guarantee the safety of communication data.

Step 1 Select **Security Setup > HTTPS**.

Figure 3-19 Configure HTTPS

The image shows a configuration form for HTTPS. It contains three input fields: 'Port' with the value '443', 'Import Certificate' with a 'Browse...' button to its right, and 'Password'. The form is enclosed in a light gray border.

Step 2 Enter port (default port is 443), import certificate and enter password.



If the default port number is modified, then it needs to enter the modified port when the user visits platform and logs in the client.

Step 3 Click **Apply** to complete setting.

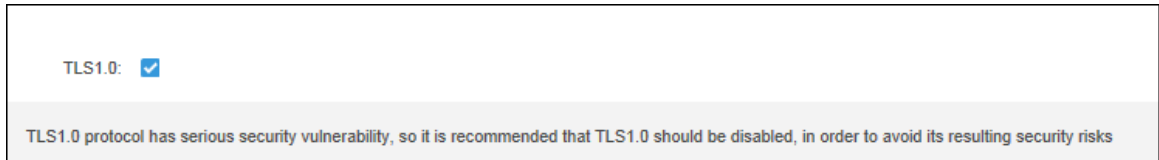
3.6.3 Enabling TLS

To enable the browser to visit the platform through TLS1.0, you need to enable TLS1.0. TLS1.0 has safety risks. Be aware.

Step 1 Select **Security Setup > TLS Setting**.

Step 2 Select the TLS1.0 check box.

Figure 3-20 Enable TLS1.0



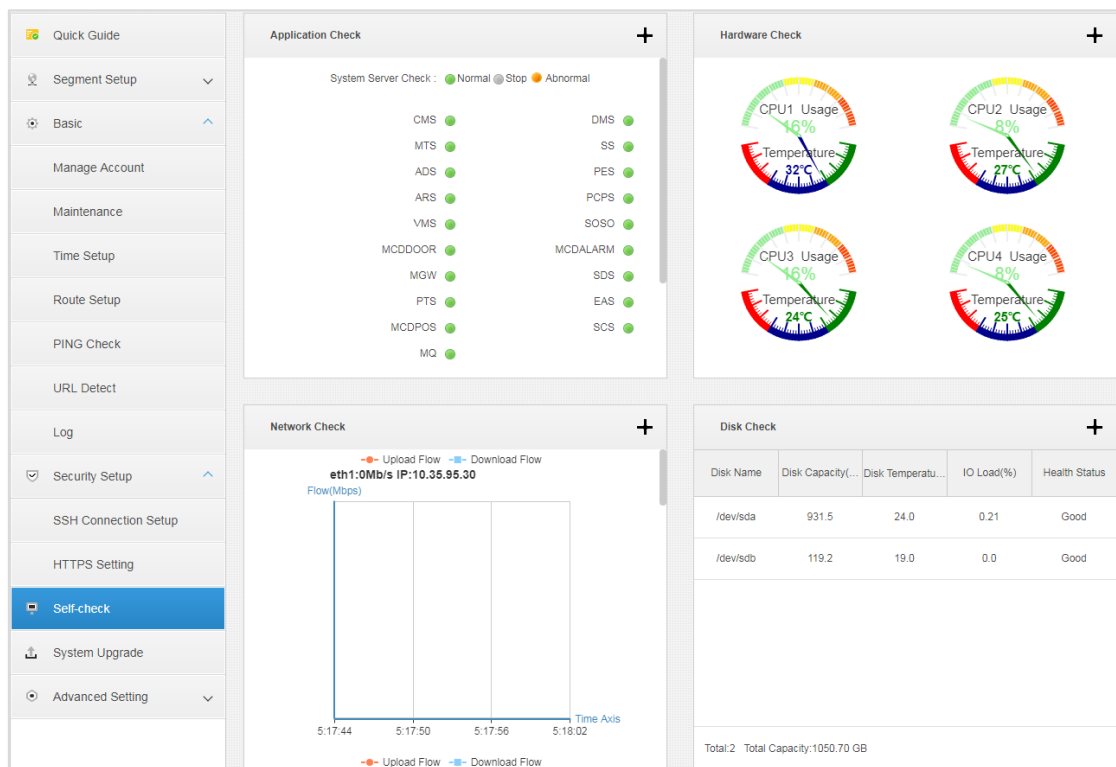
Step 3 Click **Apply**.

3.7 Self-check

Check the detection results of background application, CPU module, network and disk.

- Click Self-check and the system will display the interface of self-check result.

Figure 3-21 System self-check



- Click the + on the upper right corner of each module or click the icon



on the top left corner of the interface, and then the detection result interface is displayed.

Figure 3-22 Application check result

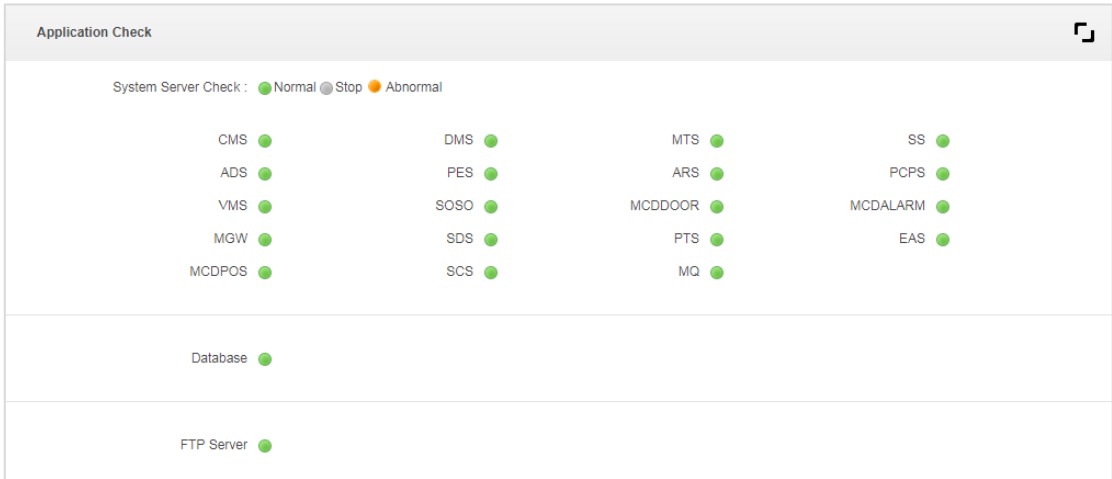


Figure 3-23 CPU check result

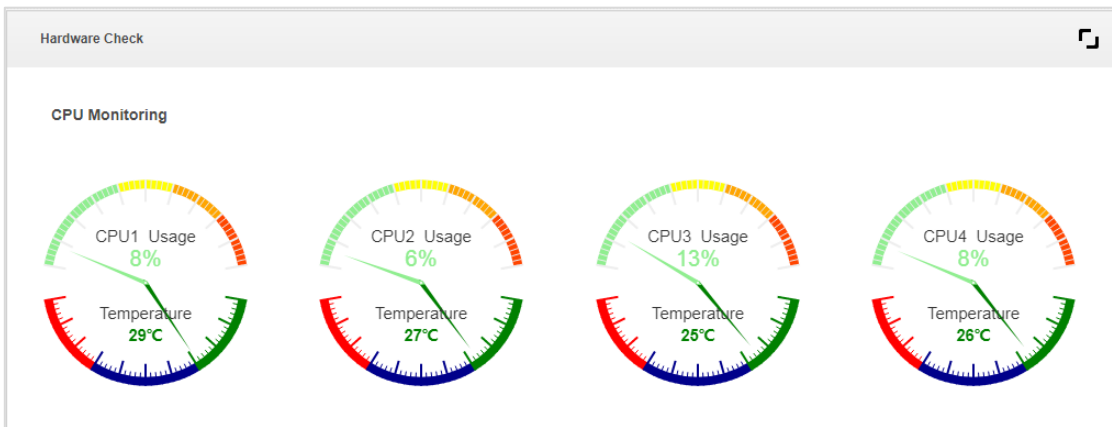


Figure 3-24 Network detection result

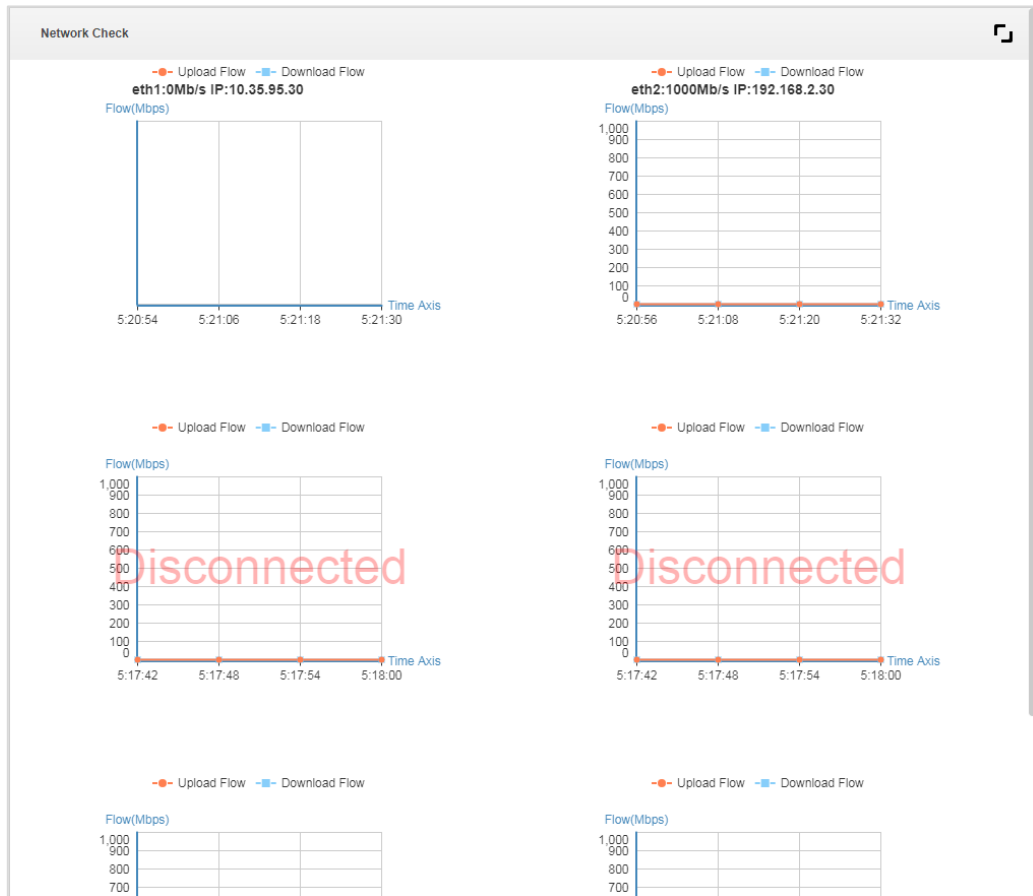


Figure 3-25 Disk detection result

Disk Name	Disk Capacity(GB)	Disk Temperature(°C)	IO Load(%)	Health Status
/dev/sda	931.5	24.0	0.00	Good
/dev/sdb	119.2	19.0	0.00	Good

3.8 Advanced Setting

In addition to the single-server deployment, the platform also supports hot spare, distributed deployment, and N+M deployment. In the **Advanced Setting** interface, you can configure the work mode of the servers for hot spare, distributed deployment, and N+M deployment.

3.8.1 Configuring Master/Slave

When configuring distributed deployment or N+M deployment, set the server to be master or slave according to the actual situation.

Step 1 Select **Advanced Setting > Distribute Config**.

Step 2 Select **Master** or **Slave** according to actual config.

Figure 3-26 Configure server mode (master)

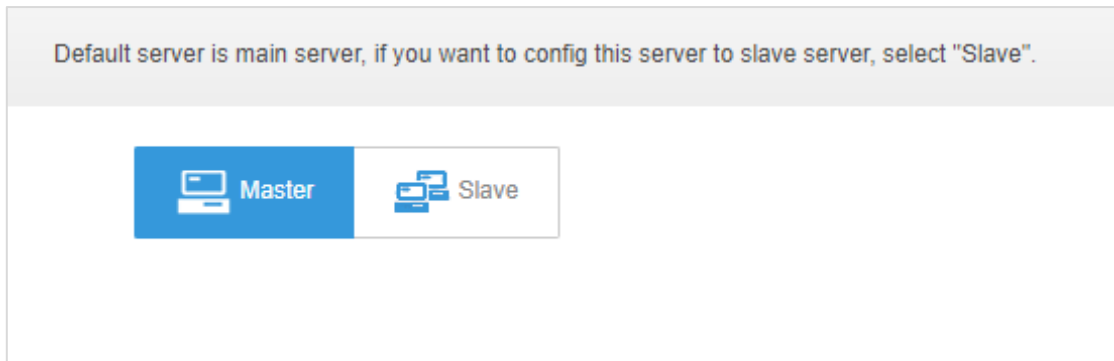
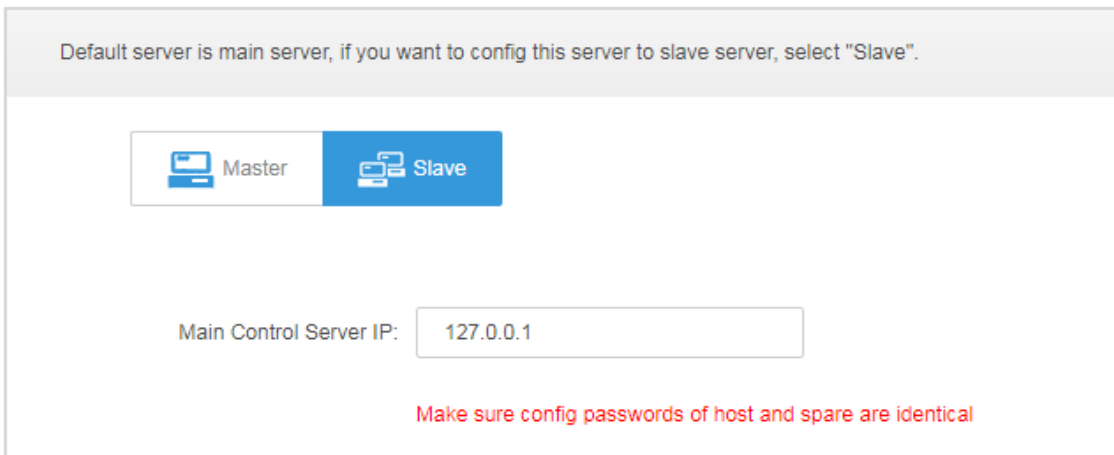


Figure 3-27 Configure server mode (slave)



Step 3 (Optional) If the server is set as **Slave**, enter master server IP address in the **Main Control Server IP** box.

Step 4 Click **Apply**.

3.8.2 Configuring Hot Spare

Configure hot spare server so that when the main server fails, the spare server can take over the job and ensure system stability.

Preparation before Operation

- Physical cable connection

Step 1 Take network port 1 as business network port, configure the IP of network port 1 as the IP of the same segment, and make it connect to the same LAN via switch, VIP and IP of network port 1 need to be in the same segment.

Step 2 Take network port 2 as heartbeat network port, which is used to keep data sync of both two machines. Configure that the IP of network port 1 is not in the same segment of network port 1 IP, but the IP of network port 2 of both two machines need to be in the same segment, you can check and configure IP address of network port 2 from network card config.

- Time sync



Please make sure both master server and spare server have enabled NTP server time correction function and sync with NTP server clock before configuring hot spare.

- Attention
 - ◇ Dual hot spare needs to use one virtual IP address, which is VIP (Virtual IP) .The VIP is chosen to, allocate an unused IP address in the business network. After the configuration is completed, the IP addresses of two DSSs do not need to log in; it only needs to log in VIP.
 - ◇ If dual hot spare need to deploy linked SMS and linked email function, you need to log in Config system of two machines first and then complete config respectively, then deploy the hot spare.
 - ◇ Before configuring dual hot spare, it needs to set the FTP password of two servers as the same password.
 - ◇ Hot spare is a synchronization of the databases of the two machines. Any two machines that involve non-database modifications, such as ports and configuration files of each service, must be modified to be consistent before the hot spare configuration.
 - ◇ When removing the hot spare, you need to log in to the configuration system that is currently activating the simulated machine, remove the hot spare option, click next, and then click Apply. Then log in to the configuration system of another machine and do the same.
 - ◇ For the upgrade of two machines with hot spare, the heartbeat network of the two machines will exchange data continuously, so direct upgrade will lead to database confusion. Therefore, to upgrade the hot spare, you need to disconnect the heartbeat network of the two hot spare machines on the site (break the network cable of the network port 2 at the back of the machine)

Operation Steps

Step 1 Select **Advanced > Hot Spare**.

Figure 3-28 Hot spare

If you want another server to replaces this main server and maintain system operation after main server finish downtime, please configure a hot spare service for this main server, fill in the following info and save.

Virtual IP:

Mask:

Spare IP:

Spare beat IP:

Spare config username:


Spare config password:

Clear Alarm Data To shorten preparation time for basic data, all alarm data will be cleared.

Make sure config passwords and ftp passwords of host and spare are identical, otherwise data sync and failure switch may fail

Step 2 Configure the parameters of hot spare server.

Table 3-5 Hot spare parameter description

Parameter	Description
Virtual IP	After setting virtual IP, then it can have access to platform via the virtual IP.
Mask	It is in accordance with the mask of network port 1.
Spare Business IP	IP address of spare server network port 1.
Spare Beat IP	IP address of spare server network port 2.
Spare Config System Username	It is the login username and password of spare server Config system.
Spare Config System Password	 The master/spare device need to keep the login password of Config system the same, the password cannot be changed after setting dual hot spare is set.
One-key Check	Click “One-key Check” to confirm if the username and password are correct.
Clear Alarm Data	After it is selected, it will clear all alarm data.

Step 3 Click **Execute Dual Host Spare** to enable the function of dual hot spare.

Click **Remove Hot Spare** to disable hot spare.

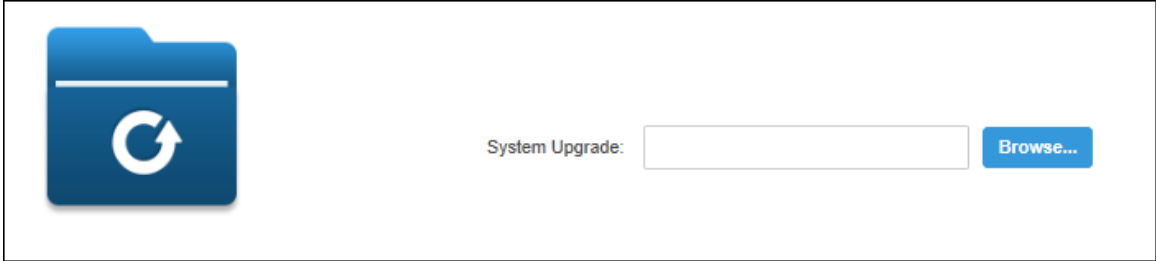
3.9 Upgrade System

Before upgrading your system, make sure that you have got the software package.

Step 1 Click the **System Upgrade** tab.

Step 2 Click **Browse**, and then select the upgrade package.

Figure 3-29 Upgrade



Step 3 Click **Apply**.

4 Manager Operations

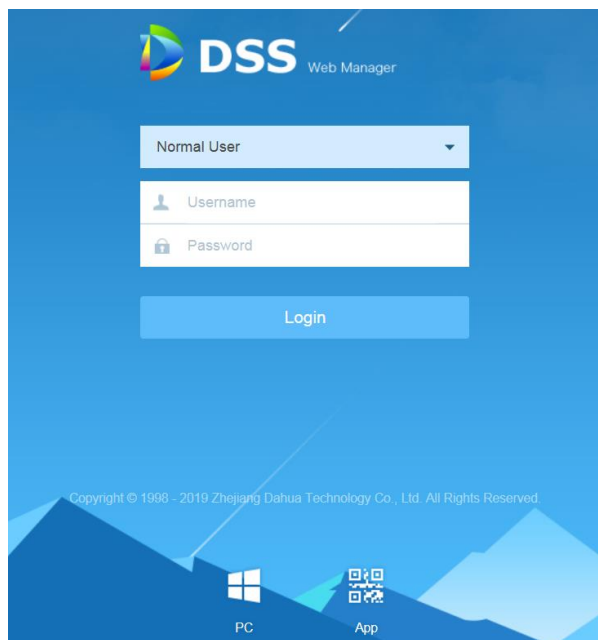
DSS Web Manager supports configuring system information, user information and record plan etc. It is recommended to use Google Chrome 40 and newer version, Firefox 40 and later version.

4.1 Logging in to Web Manager

You can log in to the Web Manager of platform server via browser, and realize remote configuration of relevant business by administrator.

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

Figure 4-1 Log in to the Web Manager



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

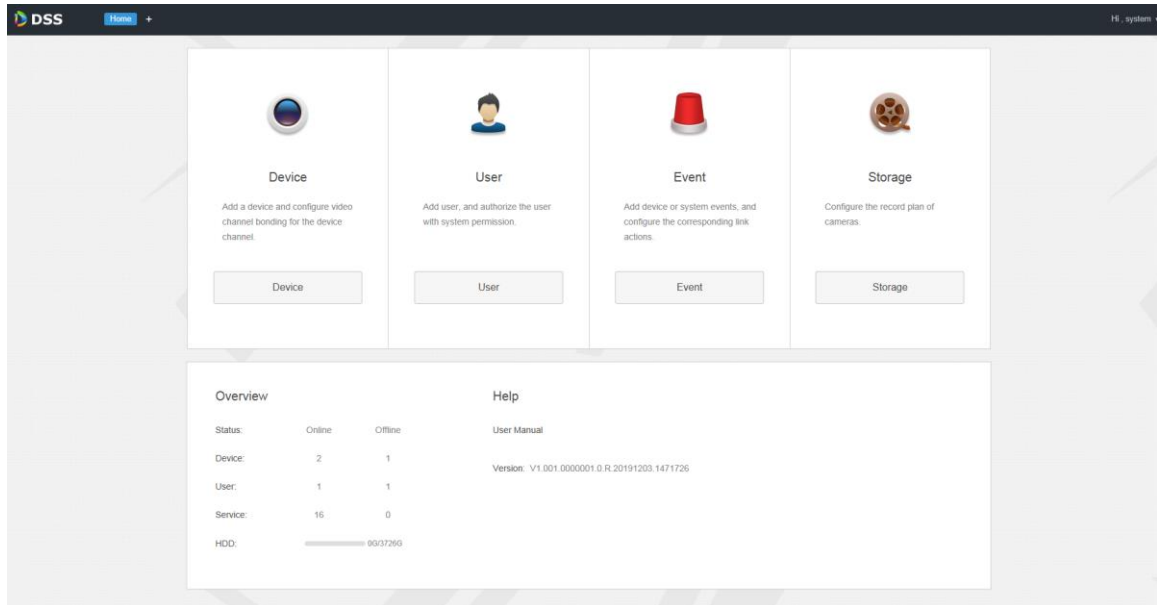
The default username is *system*.




- 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.

The homepage is displayed.

Figure 4-2 Homepage



- Hover over 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.
- Authorization: Check authorization details, purchase authorization document step by step according to requirements.
- Help: Check *User's Manual* and version information.

4.2 System Settings


4.2.1 Setting System Parameters

Configure system parameters when logging in to DSS system for the first time, which is to make sure that the system runs normally.

Step 1 Click , select **System** on the **New Tab** interface.

Figure 4-3 Set message storage time

Table 4-1 Parameters

Parameter	Description	
Message Storage Time Setup	Log	Set the longest retention time of log; it is 30 days by default.
	Alarm Info	Set the longest retention time of alarm info; it is 30 days by default.
	GPS Info	Set the longest retention time of GPS info; it is 30 days by default.
	Heatmap	Set the retention time for heatmap data.
	Face Recognition	Set the longest retention time of face recognition info; it is 180 days by default.
	Passed Vehicle Record	Set the longest retention time of passed vehicle record; it is 180 days by default.
	Access Snapshot	Set the longest retention time of entrance snapshot record.
	Customer Analysis	Set the longest retention time of people flow statistics record.
Time Sync	Scheduled Time Sync	Select it to enable scheduled time synchronizaton for devices except access control.
	Start Time	Set start time of time sync.
	Sync Interval	The time of server shall prevail; synchronize the time of device and server. It is 2 hours by default, the system is based on the server time every 2 hours, and then it is to synchronize the time of both device and server.  The time between device and server is synchronized via SDK.
	Immediately	Click the button to start time sync immediately.

Parameter		Description
Mail Server	–	Set mail server IP, port, encryption type, username/password, sender, test recipient etc. Send email to users when the administrator configures the alarm linkage and the client handles the alarm.
Activity Directory	–	Set domain information.
HTTPS	–	Enable HTTPS for higher web security level.
Login Mode Settings		In order to ensure safe use of devices, the platform supports two ways to log in to devices: Compatibility mode and security mode. You are recommended to select the Security Mode as the Compatibility Mode has potential security risks.

Step 2 Configure corresponding parameters.

Step 3 Click **Save**.

4.2.2 Setting Mail Server

4.2.2.1 Application Scenarios

You can select to send mail to user when the administrator is configuring alarm linkage and client handling alarm, at this moment, it needs to configure mail server first.

4.2.2.2 Configuration

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

Step 2 Select the **Mail Server** tab, check **Enable** to enable mail configuration.

Figure 4-4 Set mail server

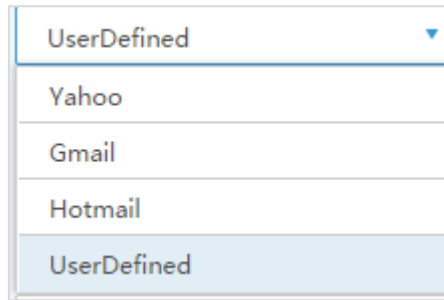
The screenshot shows the 'Mail Server' configuration page. At the top left, there is a title 'Mail Server' and an 'Enable' checkbox which is checked. Below this, there are several input fields and dropdown menus:

- 'SMTP Server Type' is a dropdown menu currently showing 'UserDefined'.
- 'SMTP Server' is a text input field containing 'xxxxxxxx'.
- 'Port' is a text input field containing '25'.
- 'Encryption Type' is a dropdown menu showing 'TLS Encrypt'.
- 'Sender Mail Address' is a text input field containing 'xxxx@xxx.com'.
- 'Password' is a text input field with all characters masked by dots.
- 'Test Recipient' is a text input field containing 'xxxx@xxx.com'.

A 'Mail Test' button is located at the bottom right of the configuration area.


Step 3 Select the type of mail server in the drop-down box.

Figure 4-5 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.

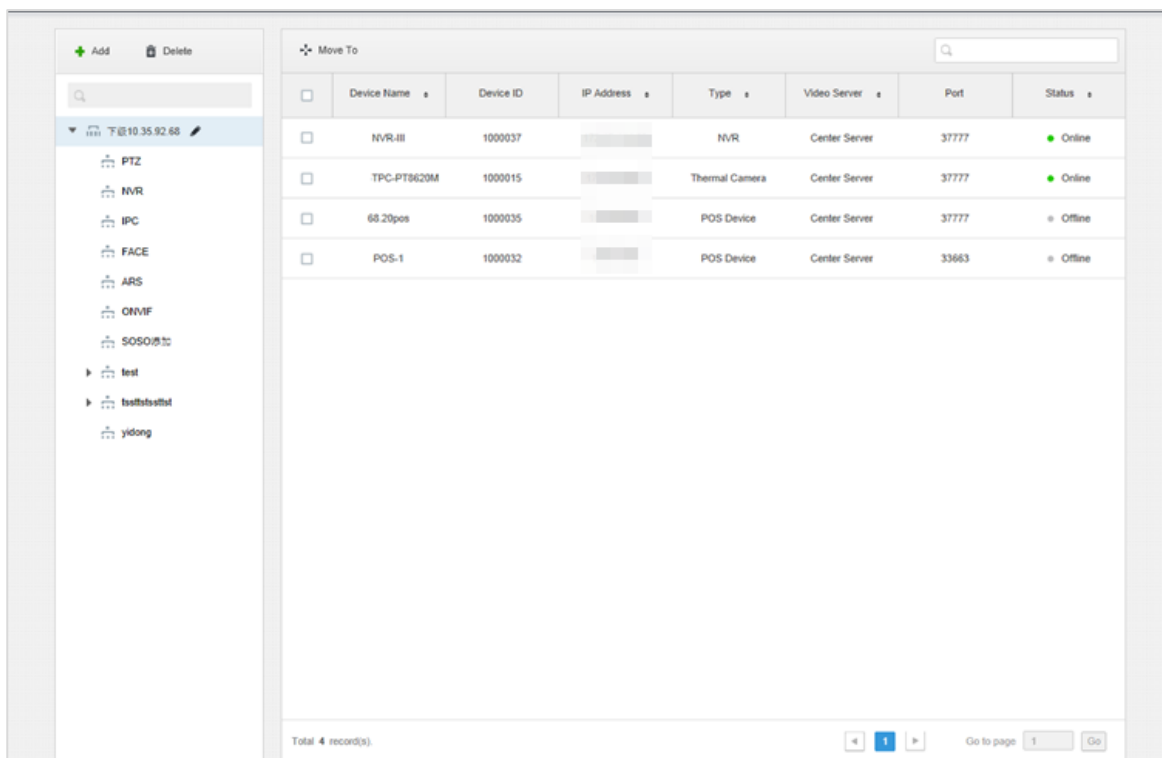
4.3 Adding Organization

Adding organizations is to deploy the hierarchy of organization or device, which is to make it easy to manage. It doesn't have to add organizations, the added users or devices are classified to the default organization.

The default first level organization of the system is Root, the newly-added organization is displayed at the next level of root.

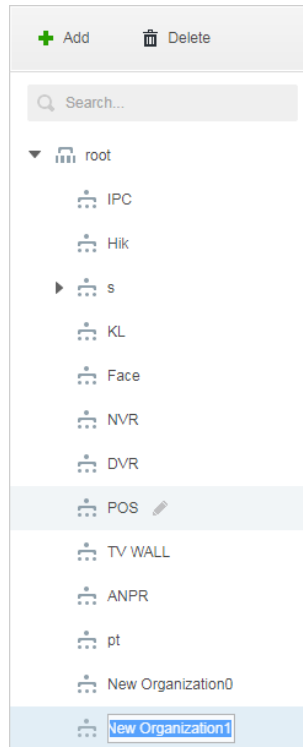
Step 1 Click  and select **Organization** on the **New Tab** interface.

Figure 4-6 Set organization



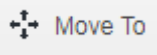

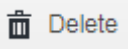
Step 2 Select root organization, click **Add**.

Figure 4-7 Add an organization



Step 3 Enter organization name, press Enter.

Operations

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

4.4 Adding Role and User

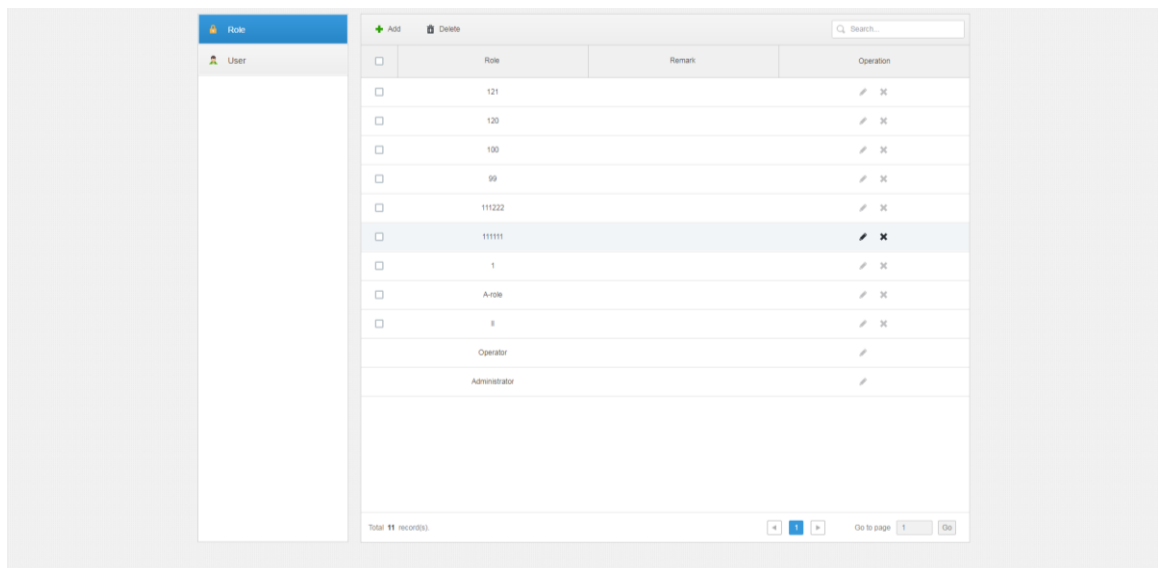
4.4.1 Adding User Role

You can create user role and add user. The created user can log in both admin and client. Different user roles decide users to have different operation permissions.

The operation permission of user role includes device permission, management menu permission and operation menu permission. First it needs to grant permissions to these operations and then it can implement corresponding operations.

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

Figure 4-8 User information interface



Step 2 Click **Add** under the **Role** tab.

Step 3 Enter **Role Name**.



If it selects Copy from next to the Role Name and select some role in the drop-down list, then it can copy the configuration information into the selected roles and realize quick configuration.

Step 4 Select **Device Permission** and **Operation Permission**.

Figure 4-9 Add a role

Add Role

Basic Info

Name: Copy from

Remark:

Device Permissions

Search...

- root
 - IPC
 - Hik
 - s
 - KL
 - Face
 - NVR

Control Permissions

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

User

<input type="checkbox"/>	Username
<input type="checkbox"/>	system
<input type="checkbox"/>	Imx
<input type="checkbox"/>	21396
<input type="checkbox"/>	chenjie
<input type="checkbox"/>	A

OK **Cancel**



If it fails to select corresponding device permission or menu permission, then the users under the role has no corresponding device or menu operation permission.

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

4.4.2 Adding User

You can add the user of the role if you have added the user role.

Step 1 Click **User** tab.

Figure 4-10 Add a user (1)

Role		+ Add Delete Import Domain User Search...				
User		Username	Role	Status	User Type	Operation
<input type="checkbox"/>		ym	Administrator	● Online	Normal User	
<input type="checkbox"/>		asd		● Offline	Normal User	
<input type="checkbox"/>		778888111	Administrator	● Offline	Normal User	
<input type="checkbox"/>		778888	Administrator	● Offline	Normal User	
<input type="checkbox"/>		1		● Offline	Normal User	
<input type="checkbox"/>		ll	Administrator,II	● Offline	Normal User	
<input type="checkbox"/>		zhhq	Administrator	● Offline	Normal User	
<input type="checkbox"/>		testfx	Administrator,Operator,II	● 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	II	● Online	Normal User	
		system	Administrator,99,100,120,121	● Online	Normal User	

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

Step 2 Click **Add**.

Figure 4-11 Add a user (2)

Basic Info

Username: * Password Expiry:

MAC Address: PTZ Control Permission: * 5

Password: * Email Address:

Confirm: * Remark:

Role

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

Device Permissions

Search...

▼ root

Control Permissions

- ▼ All Permissions
 - ▼ Control Permissions
 - ▼ Menu Permissions
 - ▼ Administrator Menu
 - ▼ Client Menu




Step 3 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 4 Click **OK** to add the user.

Operations

- Click  to freeze user, the user which logs in the client will quit.
- Click  to modify user information except username.
- Click  to delete user.

4.4.3 Setting Domain User

The setting in this chapter is optional, please select if it is to set domain user according to the actual situation.

4.4.3.1 Application Scenario

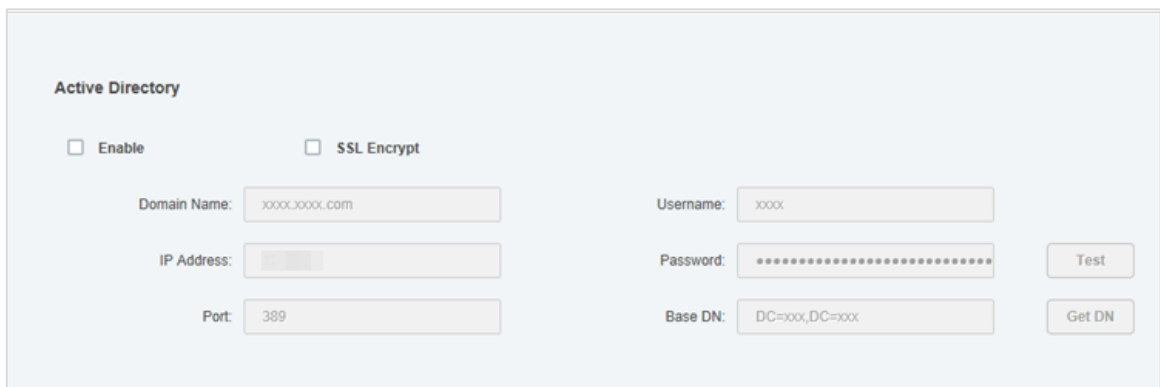
For the companies with domain information and want to use domain users as system login users, using domain user import can improve the convenience of project deployment.

4.4.3.2 Setting Domain Info

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

Step 2 Click the tab of **Active Directory** and configure domain information.

Figure 4-12 Set active directory



Step 3 After setting domain information, click **Get DN** and it will acquire basic DN information automatically.

Step 4 After getting DN information, click **Test** to test if domain information is available.

Step 5 Click **Save** to save configuration.

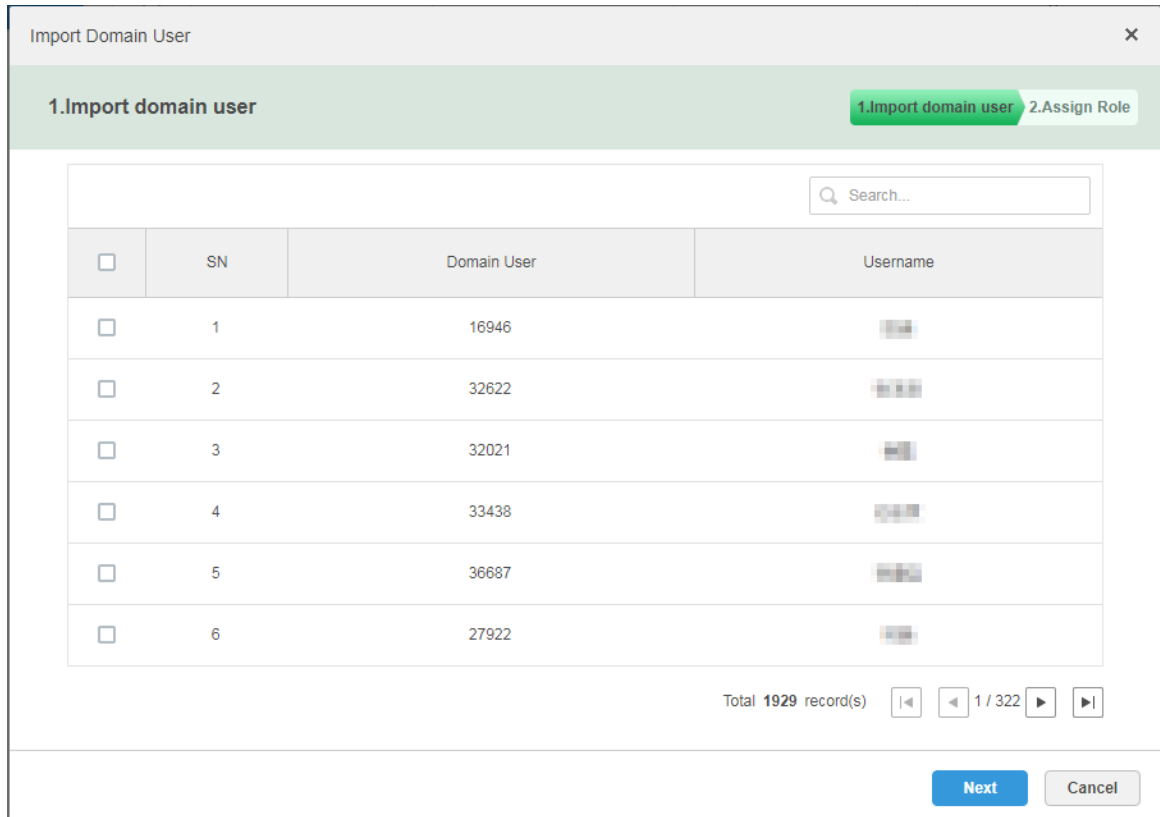
It can import domain user on the interface of **User** after it prompted successfully. Please refer to the next chapter for more operation details.

4.4.3.3 Importing Domain User

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

Step 2 Select **User** tab, click **Import Domain User** on the right of the interface.

Figure 4-13 Import domain user

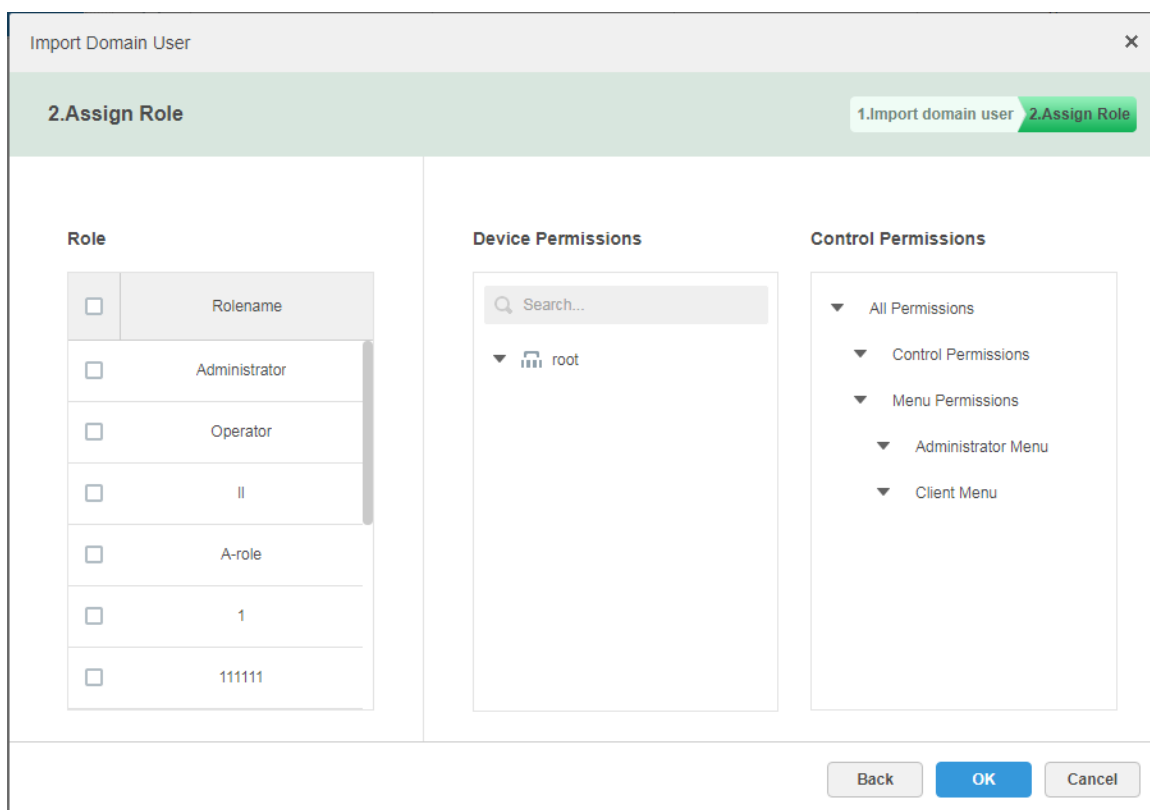


Step 3 Select the users which need to be imported from the acquired domain users. It supports searching users by entering key words in the search box.

Step 4 Click **Next**.

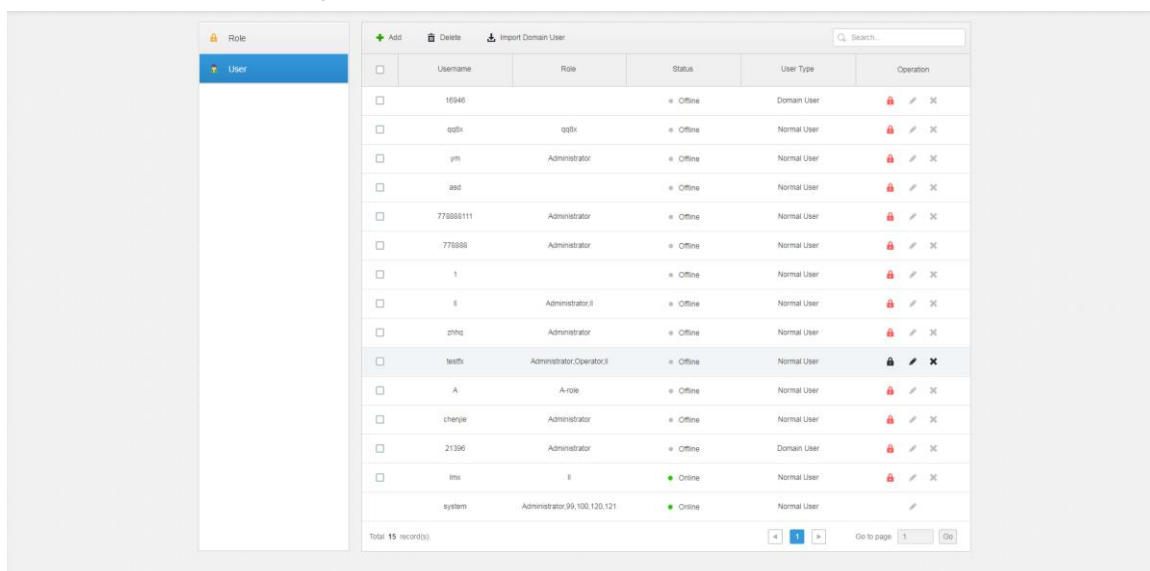
The system displays the interface of **Import Domain User**. See Figure 4-14.

Figure 4-14 Assign role to user



Step 5 Select role for domain user, it displays corresponding device information and function permission information on the right of the interface, click **OK** after it is confirmed. Make sure domain user has been successfully imported in **User Information**.

Figure 4-15 User information interface

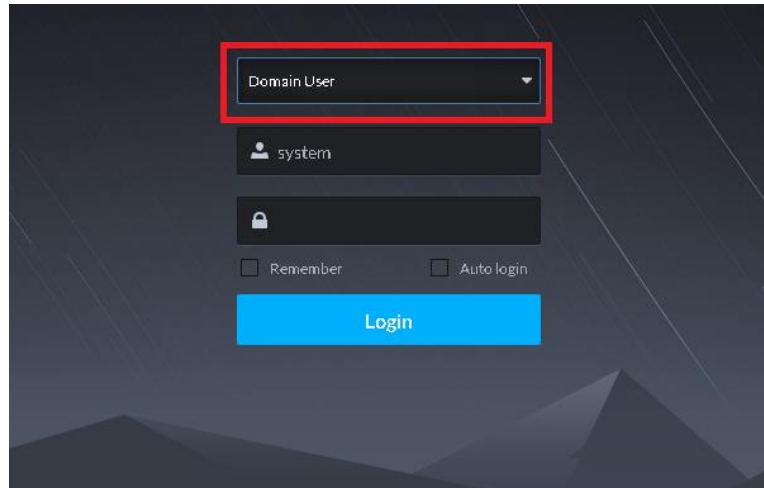


4.4.3.4 Logging in as Domain User

It can use domain user to log in client.

Step 1 Select **Domain User** in the drop-down box of **User Type** on the client login interface.

Figure 4-16 Log in as a domain user



Step 2 Enter domain username, password, server IP, port and other information, click **Login**.
The interface and function are the same as login via general user after it logged in successfully, which is not going to be repeated here.

4.5 Adding Devices

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

4.5.1 Adding Devices Manually

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

Figure 4-17 Device

The screenshot shows a web interface for device management. At the top, there are buttons for 'Connect', 'Refresh', 'Initialize Device', and 'Change IP'. Below these is a table with columns: 'Init Status', 'IP Address', 'Type', 'Port', and 'MAC Address'. Four rows are visible, all with 'Init Status' as 'Initialized'. Below the table are buttons for '+ Add', 'Delete', 'Mod...', and 'Imp...'. There is also a search bar and a dropdown for 'Org: root'. Below this is a navigation bar with tabs: 'All', 'Encoder', 'Decoder', 'Video Wall', 'ANPR', 'Matrix', 'Access Control', 'Led Device', 'Video Intercom', and 'Emergency'. The main area shows a detailed table with columns: 'Device ID', 'IP/Domain', 'Home Server', 'Device Name', 'Type', 'Org', 'Status', 'Offline Cause', and 'Operation'. Eight rows are visible, all with 'Status' as 'Offline' and 'Offline Cause' as 'Network anomaly'.

Init Status	IP Address	Type	Port	MAC Address
Initialized	[Redacted]	Unknown	37777	[Redacted]
Initialized	[Redacted]	NVR	37777	[Redacted]
Initialized	[Redacted]	NVR	37117	[Redacted]
Initialized	[Redacted]	IPC	37755	[Redacted]

Device ID	IP/Domain	Home Server	Device Name	Type	Org	Status	Offline Cause	Operation
1001896	[Redacted]	Center Server	[Redacted]	Access Snapsho...	root	Offline	Network anomaly.	[Edit] [X]
1001880	[Redacted]	Center Server	[Redacted]	EVS	root	Offline	Network anomaly.	[Edit] [X]
1001878	[Redacted]	Center Server	[Redacted]	VTH	root	Offline	Network anomaly.	[Edit] [X]
1001875	[Redacted]	Center Server	[Redacted]	Access Snapsho...	root	Offline	Network anomaly.	[Edit] [X]
1001874	[Redacted]	Center Server	[Redacted]	NVR	root	Offline	Network anomaly.	[Edit] [X]
1001873	[Redacted]	Center Server	[Redacted]	Unit VTO	[Redacted]	Offline	Network anomaly.	[Edit] [X]
1001872	[Redacted]	Center Server	[Redacted]	VTH	[Redacted]	Offline	Network anomaly.	[Edit] [X]

Step 2 Click **Add**.

Figure 4-18 Add a device (1)

The screenshot shows a dialog box titled 'Add All' with a close button (X). It has two tabs: '1. Login Information.' (selected) and '2. Device Information'. The 'Login Information' tab contains the following fields:

- Protocol: [Dropdown menu]
- Manufacturer: [Dropdown menu]
- Add Type: [Dropdown menu, value: IP Address]
- Device Category: [Dropdown menu, value: Encoder]
- IP Address: [Text input, red asterisk]
- Device Port: [Text input, value: 37777, red asterisk]
- User: [Text input, value: admin, red asterisk]
- Password: [Text input, value: ****]
- Org: [Dropdown menu, value: PTZ]
- Video Server: [Dropdown menu, value: Center Server]

At the bottom right, there are two buttons: 'Add' and 'Cancel'.

Step 3 Select **Protocol**, **Manufacturer**, **Add Type**, **Device Category**, **Organization**, **Video Server**, input **IP Address**, **Device Port** and **Username/Password**.



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

In the **Add Type** dropdown list,

- When **IP Address** is selected, enter device IP address.
- When **Auto Register** is selected, enter device registration ID. Add encoders through auto register; the ID of auto register has to be in accordance with the registered ID configured at encoder.
- When **Domain Name** is selected, the options are from the configured domain during deployment.

Step 4 Click **Add**.

Figure 4-19 Add a device (2)

The screenshot shows a window titled "Add All" with a close button in the top right corner. Below the title bar, there are two tabs: "1.Login Information" and "2.Device Information", with the second tab selected. The main area contains the following fields:

- Device Name: (required, indicated by a red asterisk)
- Type: (dropdown menu)
- Device SN:
- Role:
- Video Channel: (required, indicated by a red asterisk)
- Alarm Input Channel:
- Alarm Output Channel:

At the bottom of the window, there are three buttons: "Back", "Continue to add", and "OK".

Step 5 Select Device Type and enter Device Name, Alarm input/output channel, and so on.

Step 6 Click **OK**.

Please click **Continue to add** if it continues to add device.

4.5.2 Adding Devices through Auto Search

Channels on the 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 Click **Search Again** on the **Device** interface.



Click **Network Segment Config** to configure IP segment again, click **Search Again** to search the devices whose IP addresses are within the range.

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

The system will pop out the **Batch Add** interface. See Figure 4-20.

Figure 4-20 Batch add

A screenshot of a 'Batch Add' dialog box. The dialog has a title bar with 'Batch Add' and a close button (X). Inside, there are four input fields: 'Org:' with a dropdown menu showing 'root', 'Video Server:' with a dropdown menu showing 'Center Server', 'User:' with a text input field containing '* admin', and 'Password:' with a text input field containing '*****'. At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (grey).

Step 4 Select Organization and Video Server, enter User and Password.

User and **Password** are the username and password which are used to log in the device; both are **Admin** by default.

Step 5 Click **OK**.

The system will add the devices into corresponding organization.

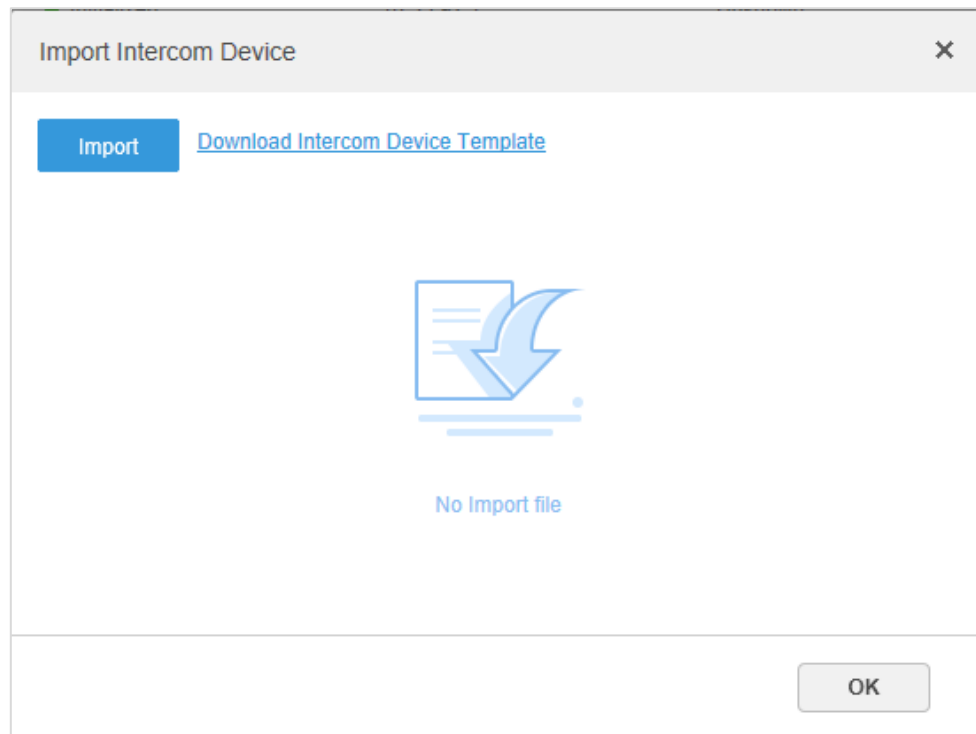
4.5.3 Importing Video Intercom Device

Fill in intercom device information in the template, you can batch add intercom devices via importing template.

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

Step 2 Click **Import**.

Figure 4-21 Import video intercom devices (1)

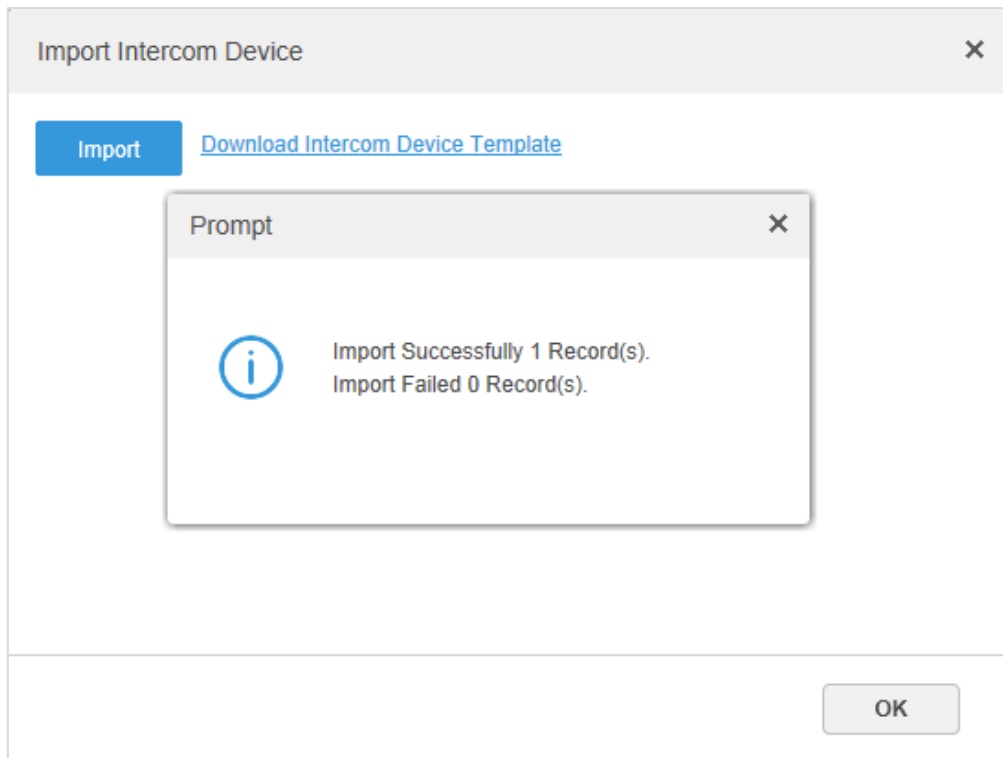



- Step 3 Click **Download Intercom Device Template** and save the template to PC according to interface tips.
- Step 4 Fill in the template according to the actual networking situation and then save the information.
- Step 5 Click **Import** and select the completed template according to interface instructions. You can view the added device in the device list.



If the device is already added to DSS platform 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 4-22 Import video intercom devices (2)



Step 6 Click  and close the prompt box.

Step 7 Click **OK**.

4.5.4 Editing Devices

It needs to edit device after adding devices, set relevant channel information.

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

Step 2 Click the corresponding  of device list.



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

Figure 4-23 Basic information

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

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



- Different types of device have different interfaces of features; the actual interface shall prevail. Device features include intelligent alarm, fisheye, face detection, face recognition and more. Select device features as needed.
- The Features setting is not available for a third-party device.

Figure 4-24 Set video channel features

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

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



Please skip the step unless when the added devices support alarm input.

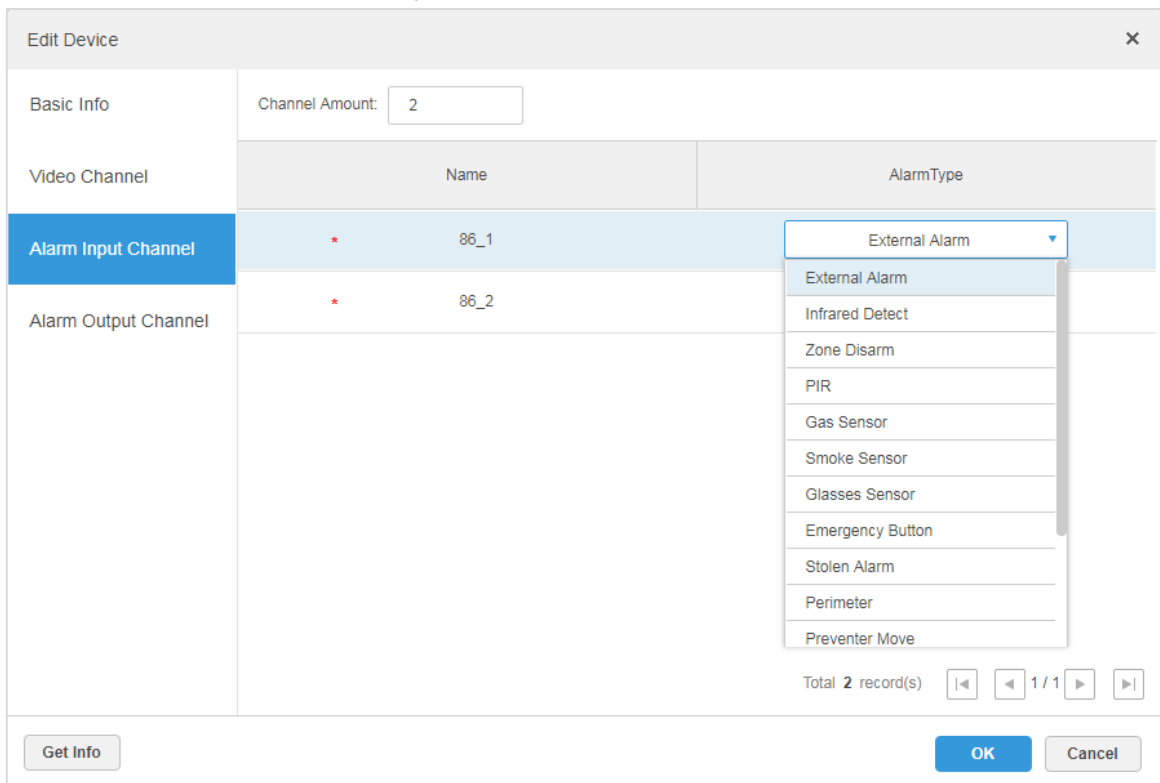
- Alarm type includes external alarm, IR detect, zone disarm, PIR, gas sensor, smoke sensor, glass sensor, emergency button, stolen alarm, perimeter and preventer move.
- Alarm type supports custom. Select **Customize Alarm Type** in the **Alarm Type** drop-down list. Click **Add** to add new alarm type. 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 be deleted but modified.
- It supports deletion if it is not used by alarm plan, after deletion, the alarm type of the alarm input channel configured with this alarm type is restored to the default value.
- 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 4-25 Alarm type



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

Figure 4-26 Modify alarm output name

Edit Device	
Basic Info	Channel Amount: <input type="text" value="2"/>
Video Channel	Name
Alarm Input Channel	* <input type="text" value="86_1"/>
Alarm Output Channel	* <input type="text" value="86_2"/>

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

Get Info OK Cancel

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

4.5.5 Binding Resources

The platform supports setting video channel, alarm input channel, ANPR channel, access control channel and video channel resource binding. It can check bound video via resource bind for businesses such as map, alarm, commercial intelligence and face etc.

Adding Resource Bind

Step 1 Click **Resource Bind**.

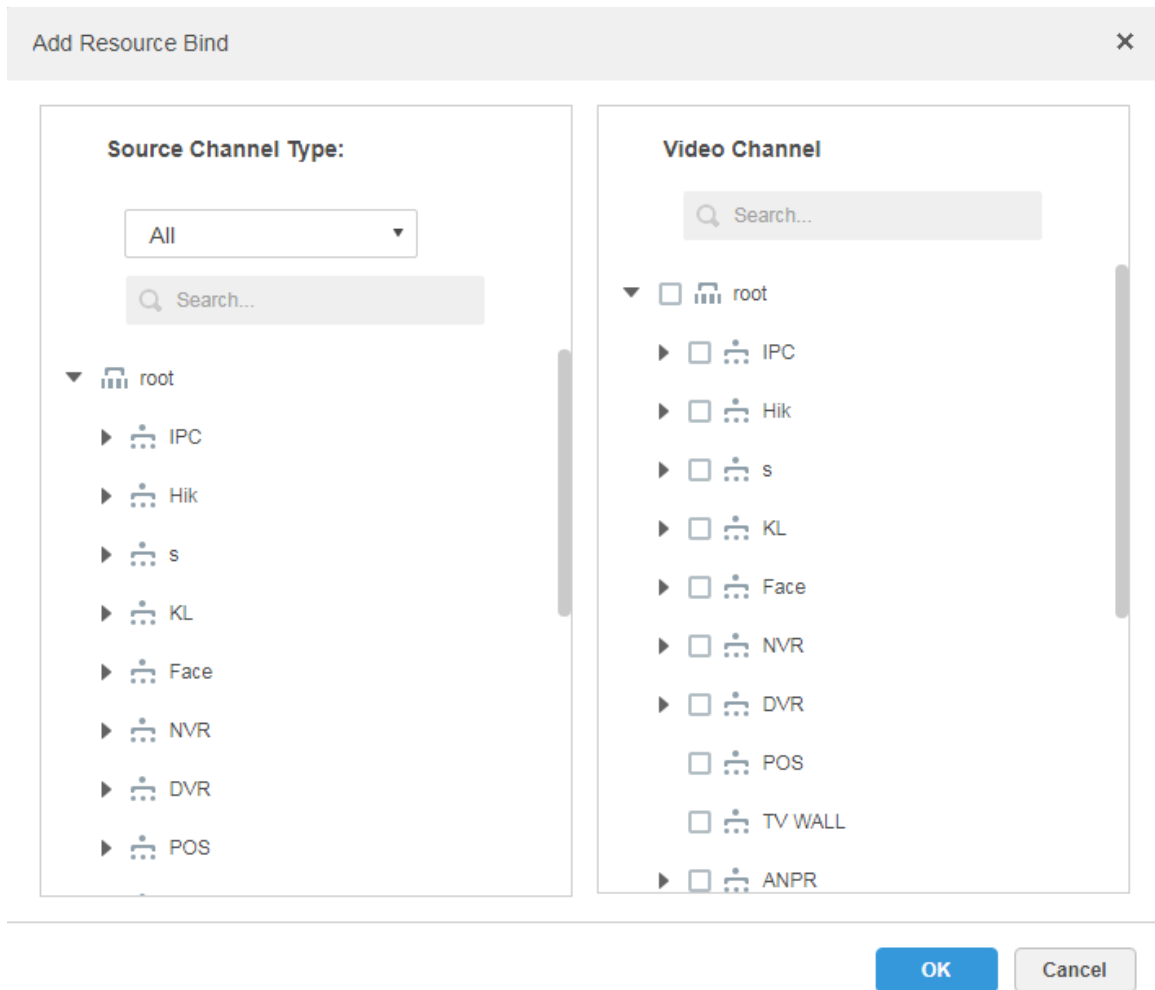
Figure 4-27 Bind resource

Device		Add	Delete	Source Chann...	Org: root	Search...
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 1

Step 2 Click **Add**.

Figure 4-28 Add resource to bind



Step 3 Select source channel and video channel respectively, and then click **OK**.

4.6 Configuring Record Plan

The platform management supports configuring record plan for video channel, which is to make front-end device record during the period which has been set.

4.6.1 Configuring Storage Disk

Add storage disk that can be used to store pictures and videos. The system supports adding net disk and local disk.

4.6.1.1 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 Click **+** and select **Storage** on the interface of **New Tab**.

Figure 4-29 Storage

Record Plan	+ Add	Delete	Search...			
Plan Name	Time Template	Position	Status	Operation		
1	All-Period Template	Store on Server	Disable	OFF [edit] [delete]		

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

Figure 4-30 Set net disk

Record Plan	Net Disk	Local Disk	+ Add	Format	All			
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	[edit] [refresh] [info] [delete]	
Center Server		20-video	50.00	26.66	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		26-1	100.00	38.44	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		26-2	100.00	0.00	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		26-3	100.00	0.00	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		26-4	100.00	19.55	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		26-5	100.00	95.95	Picture	Normal	[edit] [refresh] [info] [delete]	
Center Server		4004-s2-1	300.00	250.67	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		4004-s2-2	300.00	299.97	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		e1	32.00	4.05	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		e10	80.00	0.00	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		e13	110.00	0.00	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		e15	110.00	0.00	Video	Normal	[edit] [refresh] [info] [delete]	
Center Server		e16	120.00	0.00	Picture	Normal	[edit] [refresh] [info] [delete]	

Total 60 record(s). [page navigation] Go to page 1 [Go]

Step 3 Click **Add**.

Figure 4-31 Add net disk

Server Name:


IP Address:

Username:

Password:

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

The system will display information of all user volumes on the storage server.

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


Step 6 Select format disk type according to actual situation, click **OK** to implement formatting.

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

You can check the results of disk formatting after formatting is completed; make sure both disk size and available space are correct.



One user volume can only be used by one server at the same time. If the disk information of the list shows red, then it is already added and used by other server.

Click  and take the right to use, then the disk needs to be formatted. It will fail to take the right of use if task manager is enabled.

4.6.1.2 Configuring Local Disk

Configure local disk to store different types of files, including videos, ANPR pictures and general pictures. General pictures are all the snapshot pictures except ANPR pictures. Meanwhile, DSS platform supports external disks which can be used after formatting. You can configure individual disk storage or RAID storage.

Configuring Individual Disk

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

Figure 4-32 Storage

Record Plan	+ Add Delete							
	<input type="checkbox"/>	Plan Name	Time Template	Position	Status	Operation		
Backup Record Plan	<input type="checkbox"/>	1231	All-Period Template	Store on Server	Enable	<input type="checkbox"/>		
Group Quota	<input type="checkbox"/>	GDPR	All-Period Template	Store on Server	Enable	<input type="checkbox"/>		
Storage Config	<input type="checkbox"/>	123	All-Period Template	Store on Server	Enable	<input type="checkbox"/>		

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

Figure 4-33 Local disk

Record Plan	Net Disk Local Disk								
	<input type="checkbox"/>	Server Name	Disk Name	Capacity(GB)	Free Capacity(GB)	Disk Type	Health Status	Disk status	Operation
Backup Record Plan	<input type="checkbox"/> <td>Center Server</td> <td>C:\</td> <td>731.00</td> <td>562.00</td> <td>Not set</td> <td>OK</td> <td>Normal</td> <td></td>	Center Server	C:\	731.00	562.00	Not set	OK	Normal	
Group Quota	<input type="checkbox"/> <td>Center Server</td> <td>D:\</td> <td>200.00</td> <td>84.00</td> <td>Not set</td> <td>OK</td> <td>Normal</td> <td></td>	Center Server	D:\	200.00	84.00	Not set	OK	Normal	
Storage Config	<input type="checkbox"/> <td>Center Server</td> <td>E:\</td> <td>485.00</td> <td>456.00</td> <td>Common picture</td> <td>OK</td> <td>Normal</td> <td></td>	Center Server	E:\	485.00	456.00	Common picture	OK	Normal	

Step 3 Configure local disk.




- Click  and configure disk type according to interface prompt.
- Select disk and click **Format**, or click  next to disk information and format the disk according to interface prompt and configure disk type. Only external disk supports formatting. Hot spare
Set disk as backup disk of RAID group, replace the damaged disk of RAID group.
- Click  and set parameters, click **OK**.

Figure 4-34 Set hot spare

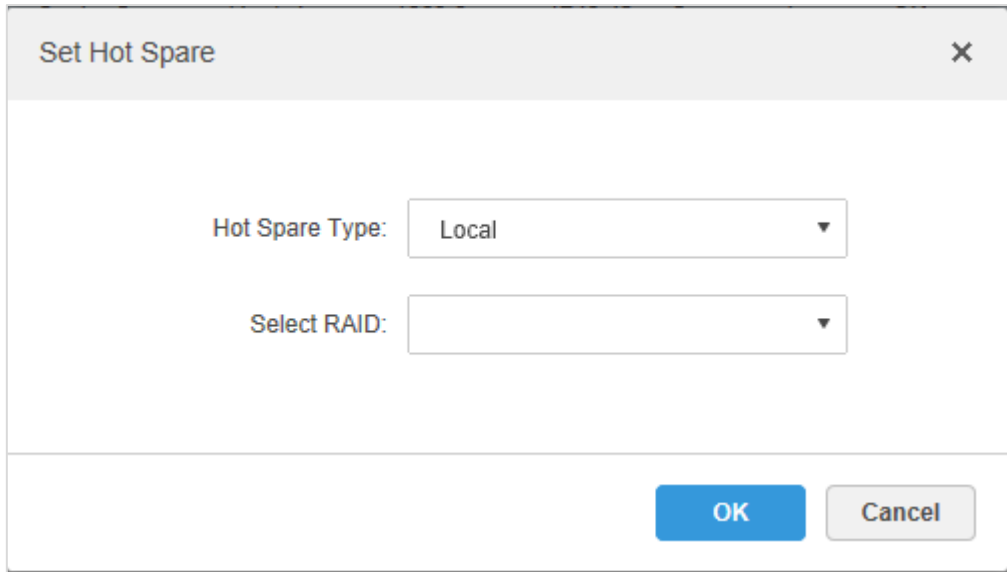


Table 4-2 Hot spare parameter description

Parameter	Description
Hot Spare Type	<p>Supported types include:</p> <ul style="list-style-type: none"> ● Local Set disk as backup disk of designated RAID group. Recreate system immediately when disk error happens in the RAID group. ● Global Set disk as backup disk of all RAID group. Recreate system immediately when disk error happens in any RAID group.

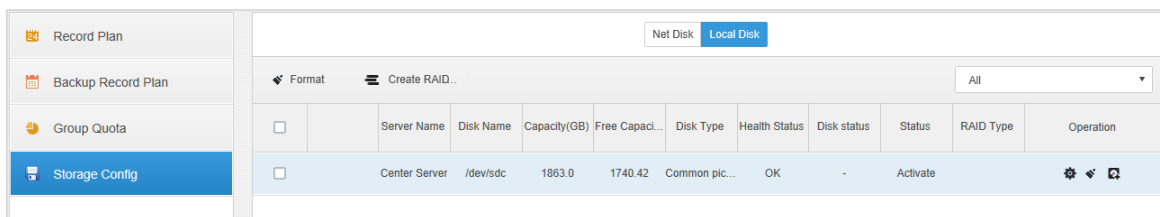
Configuring RAID Group

Create RAID group for higher storage performance and data redundancy.

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

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

Figure 4-35 Local disk



Step 3 Click **Create RAID**.

Figure 4-36 Create RAID

✕
Create RAID Type

RAID Type: raid0

<input type="checkbox"/>	Server Name	Status	Disk Name	Slot No.	Capacity(GB)
<input type="checkbox"/>	Center Server	Activate	/dev/sdb	2	2794.5

Total 2 record(s).

Go to page

Step 4 Select a **RAID Type**, select disks, and then click **OK**.

Figure 4-37 RAID group info

<input type="checkbox"/>	Server Name	Disk Name	Capacity(GB)	Free Capaci...	Disk Type	Health Status	Disk status	Status	RAID Type	Operation
<input type="checkbox"/>	Center Server	/dev/sdb	2794.5	2793.28	Picture	OK	Normal	Activate		⚙️ ⚡ 🗑️
<input type="checkbox"/>	Center Server	/dev/sdc	2794.5	2605.71	Common pic...	OK	-	Activate		⚙️ ⚡ 🗑️

Step 5 Configure RAID group.

- Set disk type.

Click and follow the onscreen instructions to configure disk type. Different type of disk stores different data.


- Format disk. Only external disk supports formatting.



All the data in the disk will be deleted after disk formatting. Please use the function with care.

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

- Delete RAID group



Click  next to disk information, and delete RAID group according to system prompt.

4.6.2 Setting Disk Group Quota

Operate on a single server, divide storage disks into several groups, and designate the storage path of the video channel to a fixed packet disk. On the one hand, directional storage is realized through the grouping and binding method; on the other hand, timed storage is realized through the proportional relation between disk capacity and channel.

Step 1 Click the tab of **Group Quota**.

Figure 4-38 Server status

	Name	Status	Operation
 Record Plan	172.22.151.19	● Online	
 Backup Record Plan	10.35.92.65	● Offline	
 Group Quota	10.35.92.19	● Offline	
 Storage Config	Center Server	● Online	


Step 2 Click  next to the online/offline of status server.

Figure 4-39 Edit disk groupb (1)

Edit Disk Group ×

1. Set Group. 1. Set Group 2. Allocate Channel

Not Allocated


<input type="checkbox"/>	Disk Name	Total Capacity(GB)	Used capacity (GB)
<input type="checkbox"/>	\\.\PhysicalDrive6	150	150
<input type="checkbox"/>	\\.\PhysicalDrive16	500	500

>
<

Group List

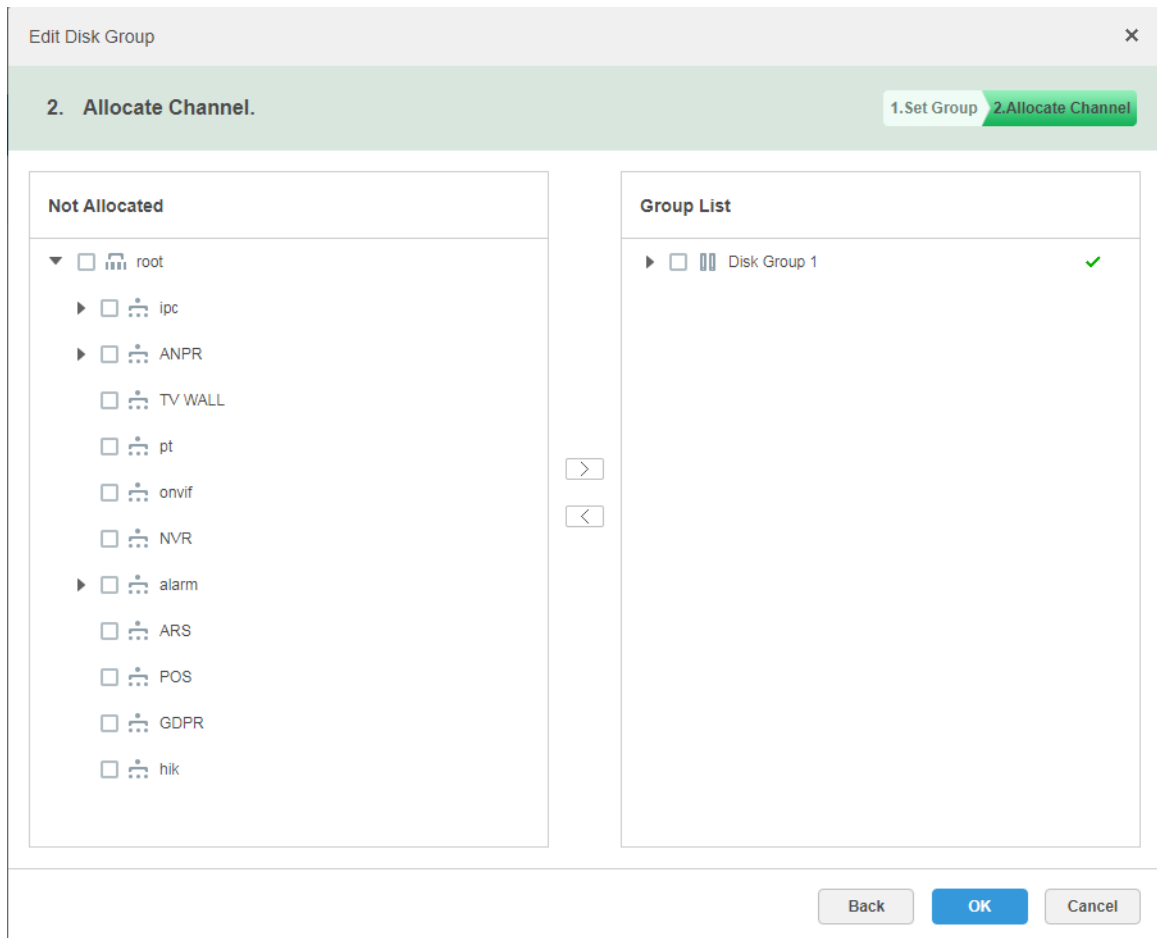
<input type="checkbox"/>	Group Name	Total Capacity(GB)	Contain


Next
Cancel

Step 3 Select the undistributed disks on the left, click  and add it to the disk group list on the right.

Step 4 Click **Next** to distribute channels for disk group.

Figure 4-40 Edit disk groupb (2)



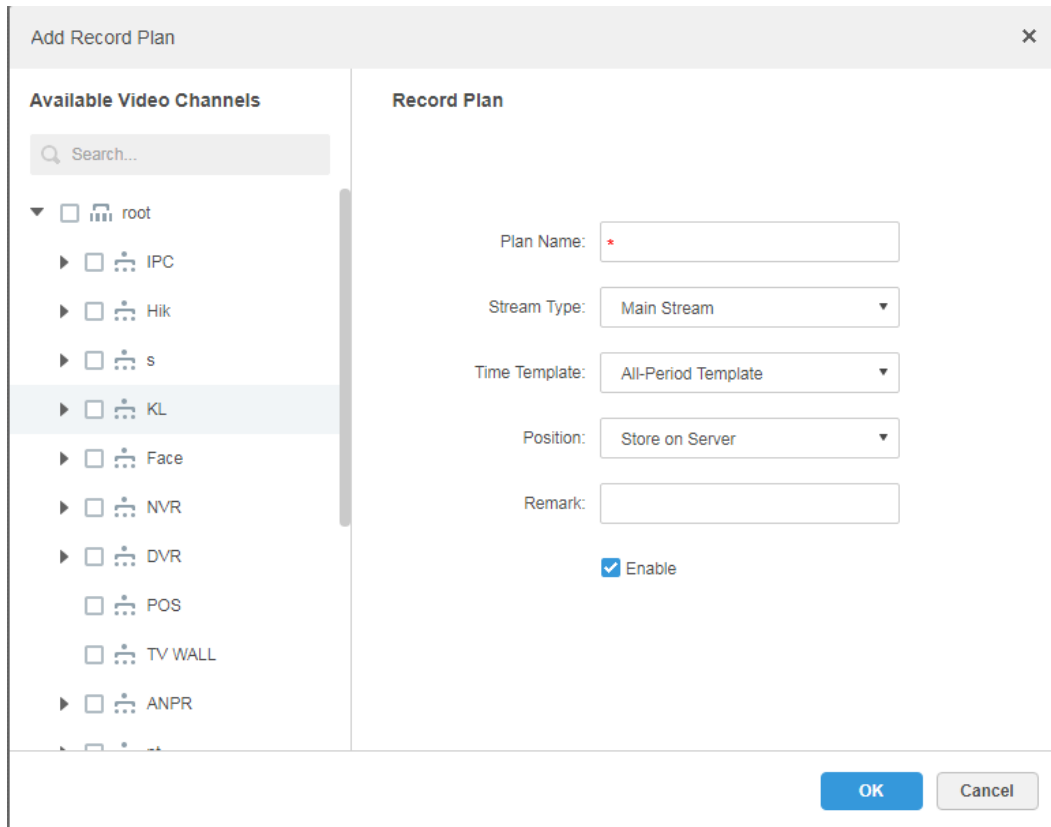
Step 5 Select channels in the device list on the left, click  to add it to the disk group on the right.

Step 6 Click **OK**.

4.6.3 Adding General Plan

Step 1 Click the tab of **Record Plan**, click **Add**.

Figure 4-41 Add recording plan



Step 2 Select the video channel which needs to configure record plan, set **Plan Name**, **Stream**, select **Time Template** and **Position**.





- Stream type includes: Main stream, sub stream 1, sub stream 2.
- Time template can select the system default template or new template created by users, refer to "4.6.5 Adding Time Template" for details of adding time template.
- Storage position can select server or recorder.

Step 3 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 a general plan, click  **Delete** to delete plans in batches.

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

4.6.4 Adding Backup Record Plan

The system supports backup recording over the devices 3 days ago, the implementation time of backup plan can span the day, the condition of backup record is time/Wi-Fi optional.



- Backup video comes for the local record of the camera.
- Backup Condition can select time and Wi-Fi. If it selects time, sets backup plan time, it will make backup record automatically after the time reaches; If it selects Wi-Fi, then it will make backup record automatically after the device is connected to Wi-Fi mode.

Step 1 Click the tab of **Backup Record Plan**.

Figure 4-42 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 2 Click **Add** to add backup plan.

Step 3 Select corresponding devices on the left device tree, and enter plan name.

Step 4 Set backup conditions.

- Take time as condition.

Figure 4-43 Add backup plan

Add Backup Record Plan
✕

Available Video Channels

Search...

- ▶ 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

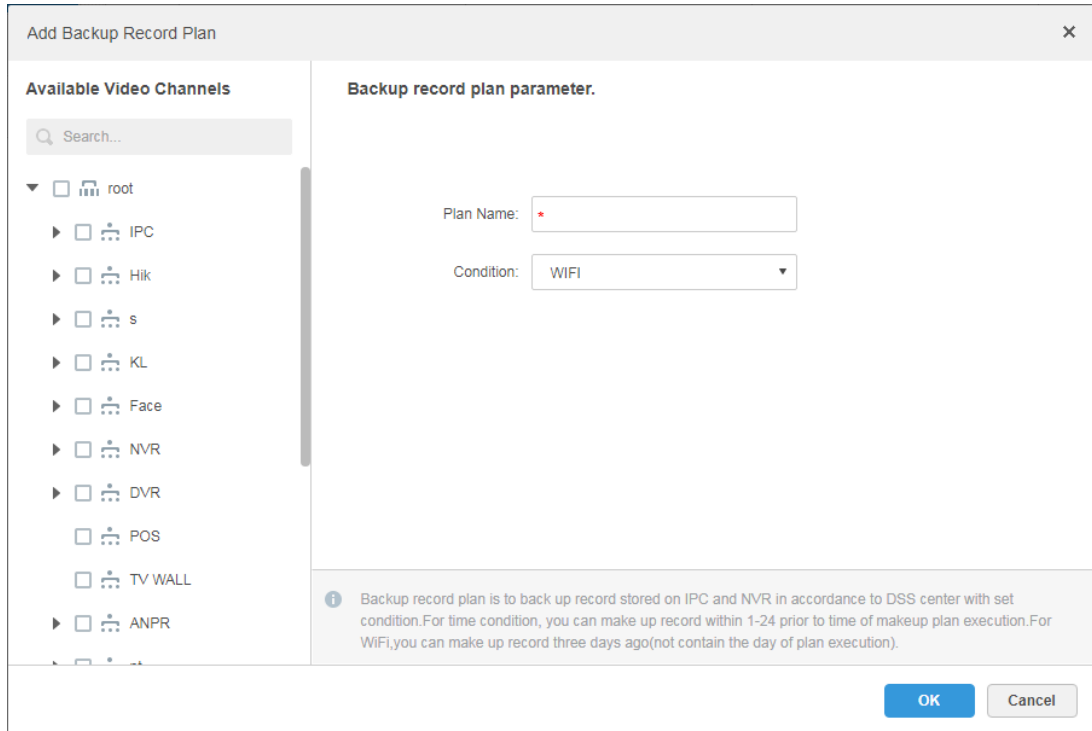
Backup Record Length: * Hour

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).

OK
Cancel

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

Figure 4-44 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 backup record plan

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

- Delete backup record plan

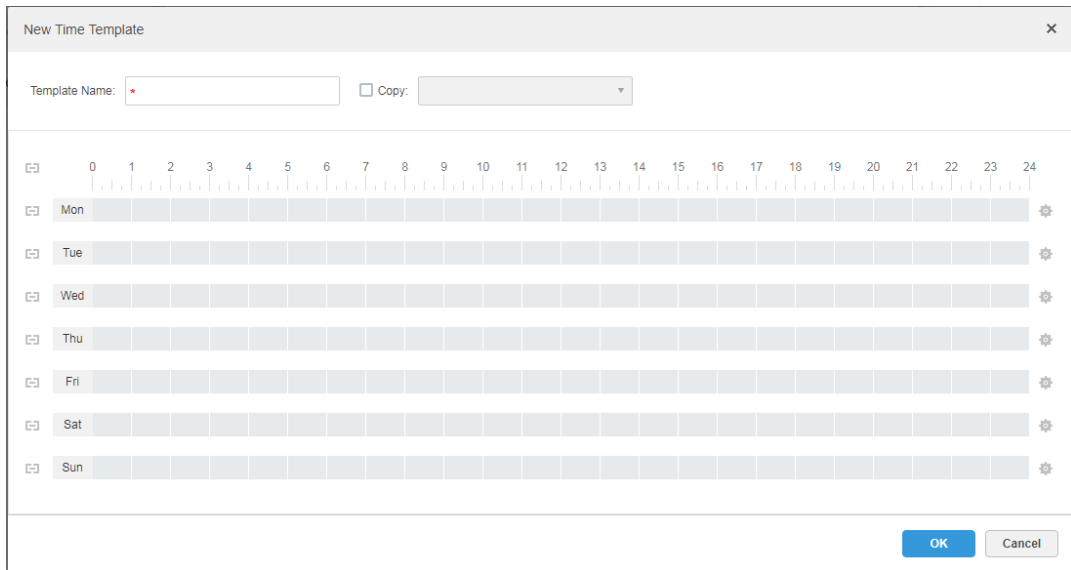
◇ Select backup record plan, click  **Delete** to delete plan in batch.

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

4.6.5 Adding Time Template

Step 1 Select **New Time Template** in the drop-down box of **Time Template**.

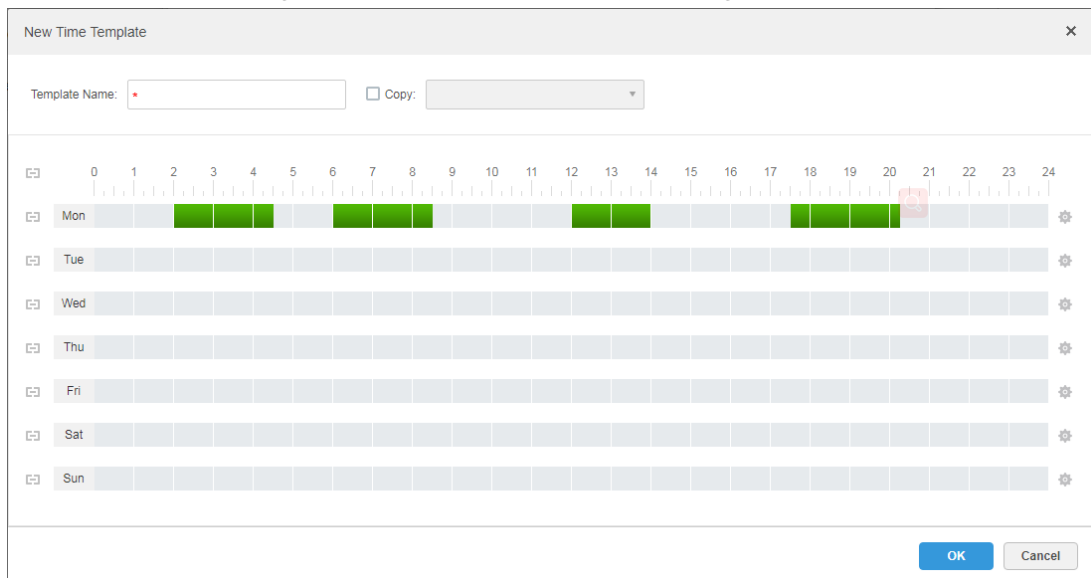
Figure 4-45 New time template



Step 2 Sets template name and time period.

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

Figure 4-46 Set time period by drawing




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

Figure 4-47 Set time period by selecting

Period Setup

Period1 02:00:00 — 04:30:00 + ×

Period2 06:00:00 — 08:30:00 + ×

Period3 12:00:00 — 14:00:00 + ×

Period4 17:30:00 — 20:15:00 + ×

All

Mon Tue Wed Thu Fri Sat Sun

OK Cancel



It can set max 6 periods in one day.

Step 3 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.

4.7 Configuring Event

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.
































Step 1 Click  on the Web Manager, select **Event** on the **New Tab** interface.

Figure 4-48 Event

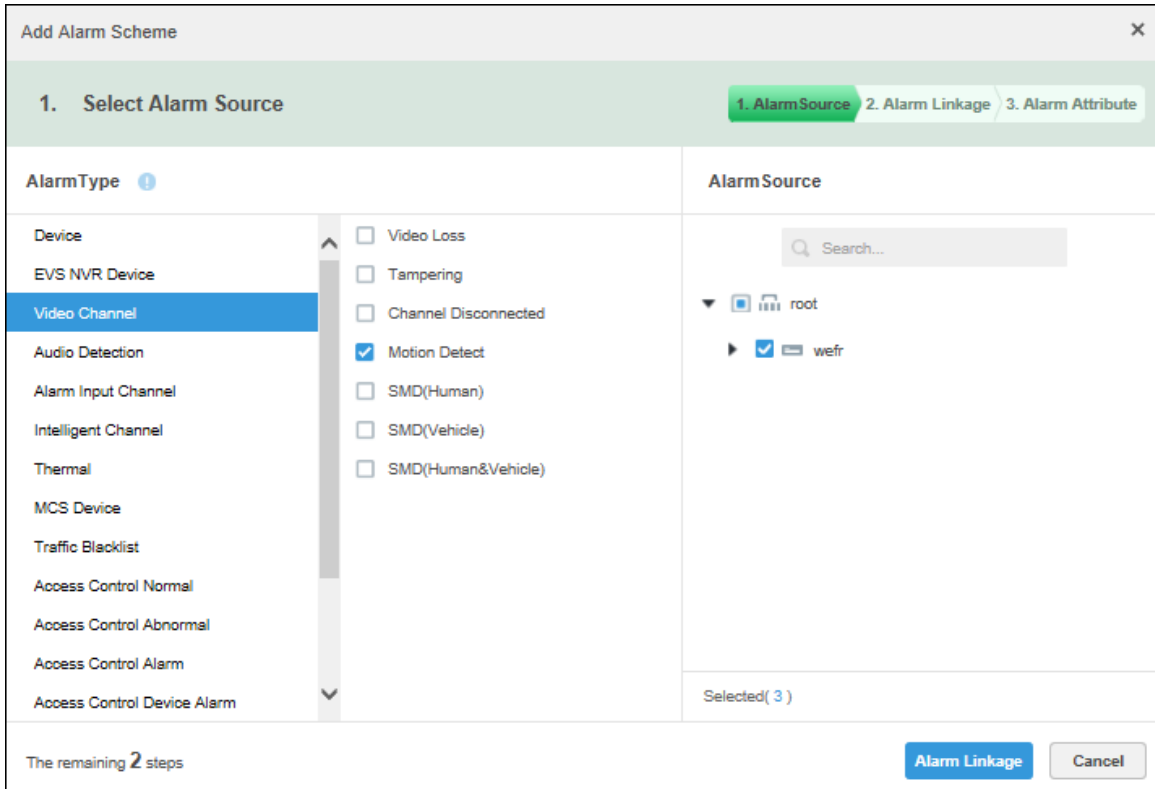
<input type="checkbox"/>	Name	Plan	Type	Priority	Remark	Scheme Status	Operation
<input type="checkbox"/>	duanxian	All-Period Template	Channel Disconnected	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	lmx	All-Period Template	Tripwire,Intrusion	Medium		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx196	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx195	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx194	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx193	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx192	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx191	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx190	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx189	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx188	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx187	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx186	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx185	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	fx184	All-Period Template	Tampering	High		Enable	<input type="checkbox"/> ON  

Total 200 record(s).

Navigation: < 1 2 3 4 5 ... 14 > Go to page 1 Go

Step 2 Click **Add**.

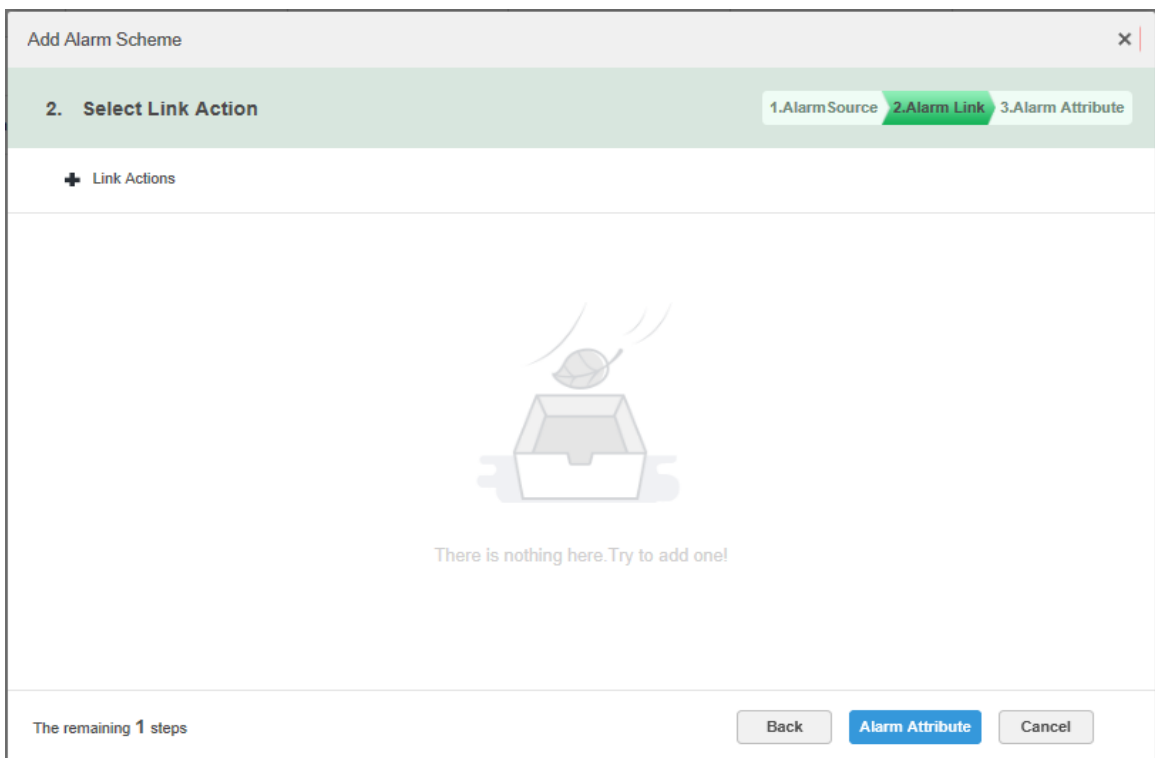
Figure 4-49 Edit alarm scheme



Step 3 Configure alarm source.

- 1) Select alarm type and alarm source.
- 2) Click Alarm Link.

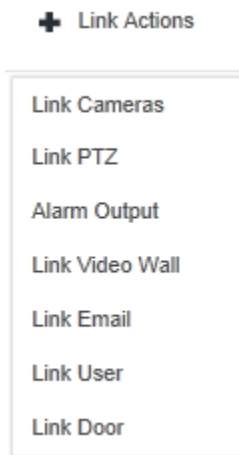
Figure 4-50 Add alarm scheme



Step 4 Configure alarm link.

- 1) Click **+**, the **Link Actions** list is displayed.

Figure 4-51 Link actions



2) Select linkage actions.

- ◇ Click **Link Cameras**, and then set parameters. See Figure 4-52. Please refer to Table 4-3 for more details about parameters.

Figure 4-52 Link camera

Add Alarm Scheme
×

2. Select Link Action

1.Alarm Source
2.Alarm Link
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

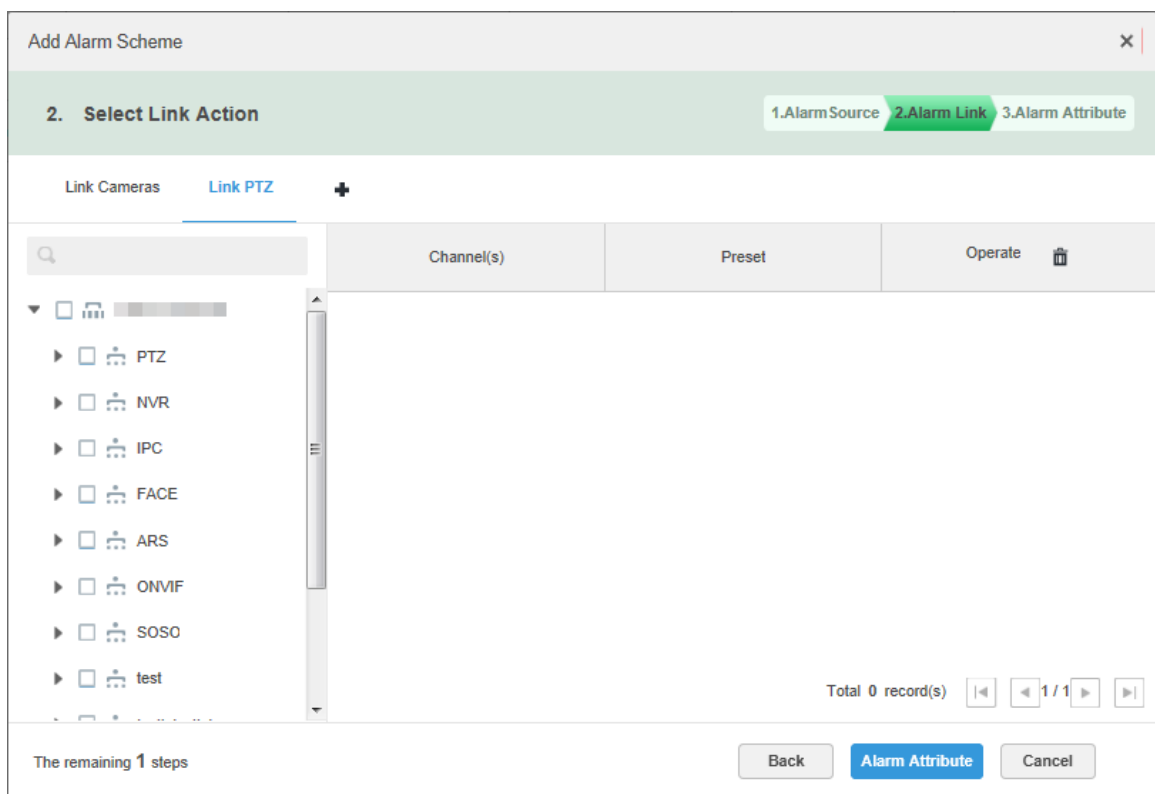
Table 4-3 Parameters

Parameter	Description
<input checked="" type="radio"/> Link Bind Camera <input type="radio"/> Select Camera !	<ul style="list-style-type: none"> Bind camera: Video channel has been bound with the alarm source. It is to quickly configure event scheme via resource binding. Select a camera for linkage: manually select a camera to link with the alarm.
Position	It is to set whether to store the video on server or device.
Stream Type	It is to set the stream type of recording video. Main stream has

Parameter	Description
	higher quality than sub stream, but consumes more storage and bandwidth than sub stream.
Record Time	It is to set the duration of video recording.
Prerecord Time	It is 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.
Open camera video on client when alarm is triggered.	Confirm if it opens camera video window on the client during alarm.

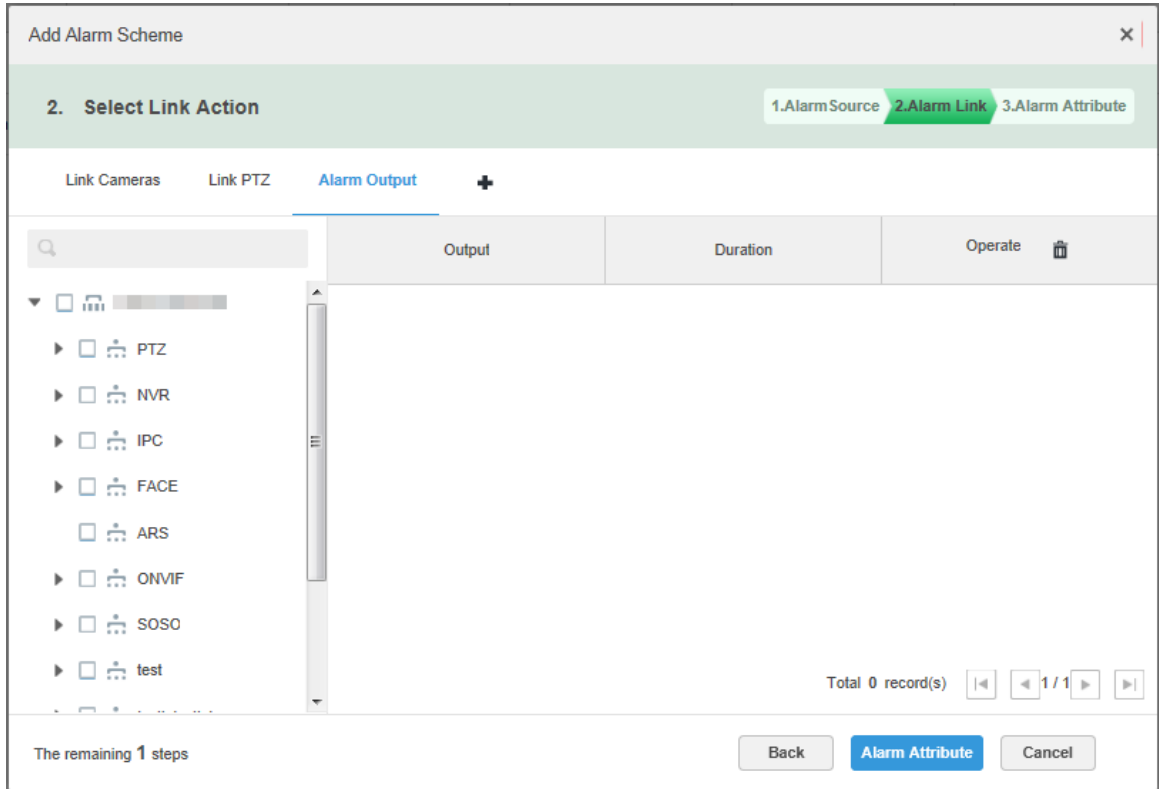
- ◇ Click **Link PTZ**, select the channels which need PTZ to link device, and then set prerecord actions. See Figure 4-53.

Figure 4-53 Link PTZ



- ◇ Click **Alarm Output**, select alarm output channel, and then set duration. See Figure 4-54.

Figure 4-54 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. See Figure 4-55. 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. See Figure 4-56.

Figure 4-55 Link video wall (1)

Add Alarm Scheme ✕

2. Select Link Action 1.AlarmSource **2.Alarm Link** 3.Alarm Attribute

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

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.

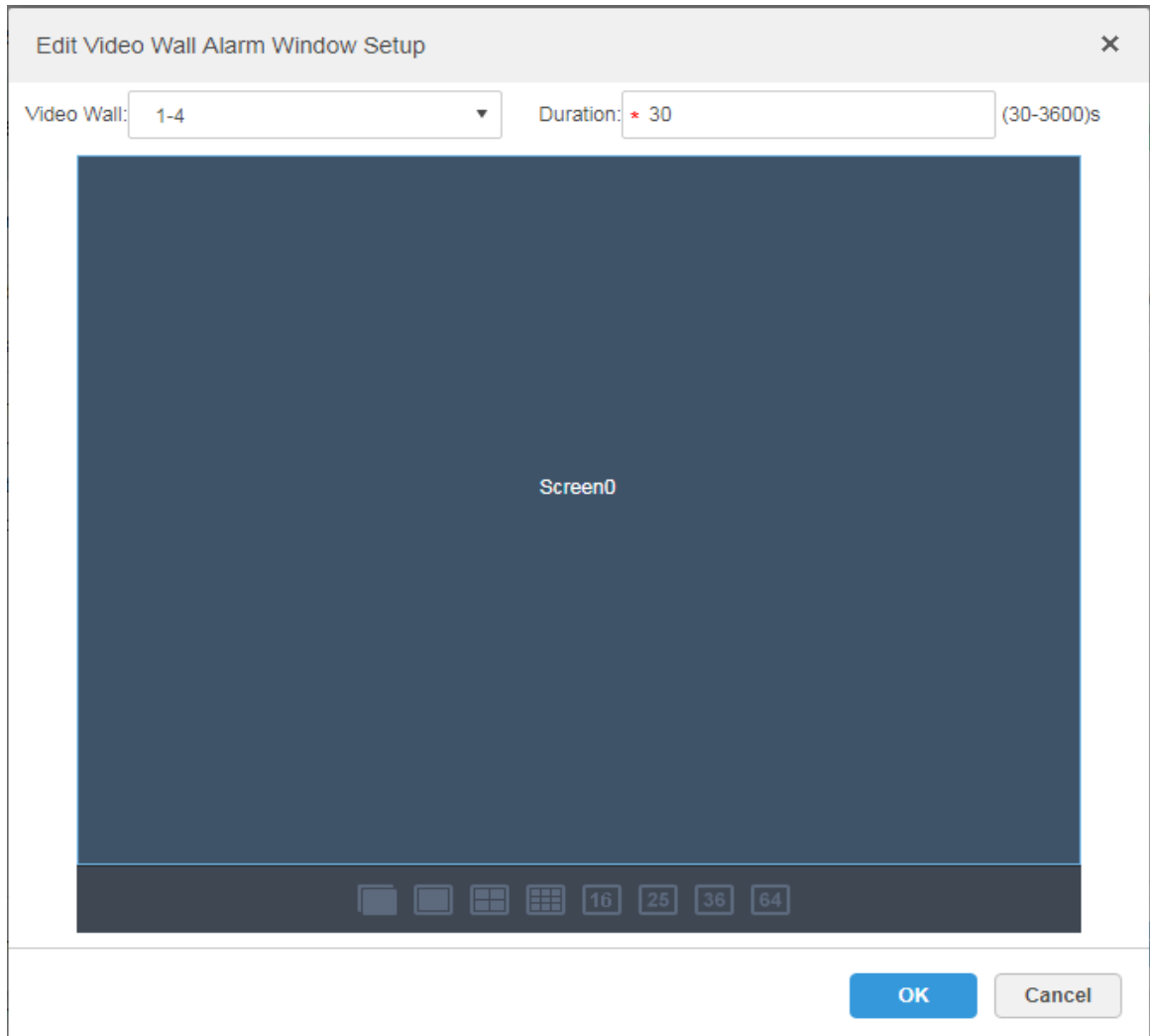
Video Wall: 1-4 Video Wall Alarm Window Setup

Screen0

The remaining **1** steps

Back **Alarm Attribute** Cancel

Figure 4-56 Link video wall (2)



- ◇ Click **Link Email**, select email template and recipient. See Figure 4-57.
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 4-57 Link email

Add Alarm Scheme

2. Select Link Action

1.Alarm Source 2.Alarm Link 3.Alarm Attribute

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

Email Template: Default

Address: +

Subject: Event time Event source Event type

Send event image ⓘ

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

Time: Event time

Location: Org name

Event Source: Event source

The remaining 1 steps

Back Alarm Attribute Cancel

Figure 4-58 Set email template

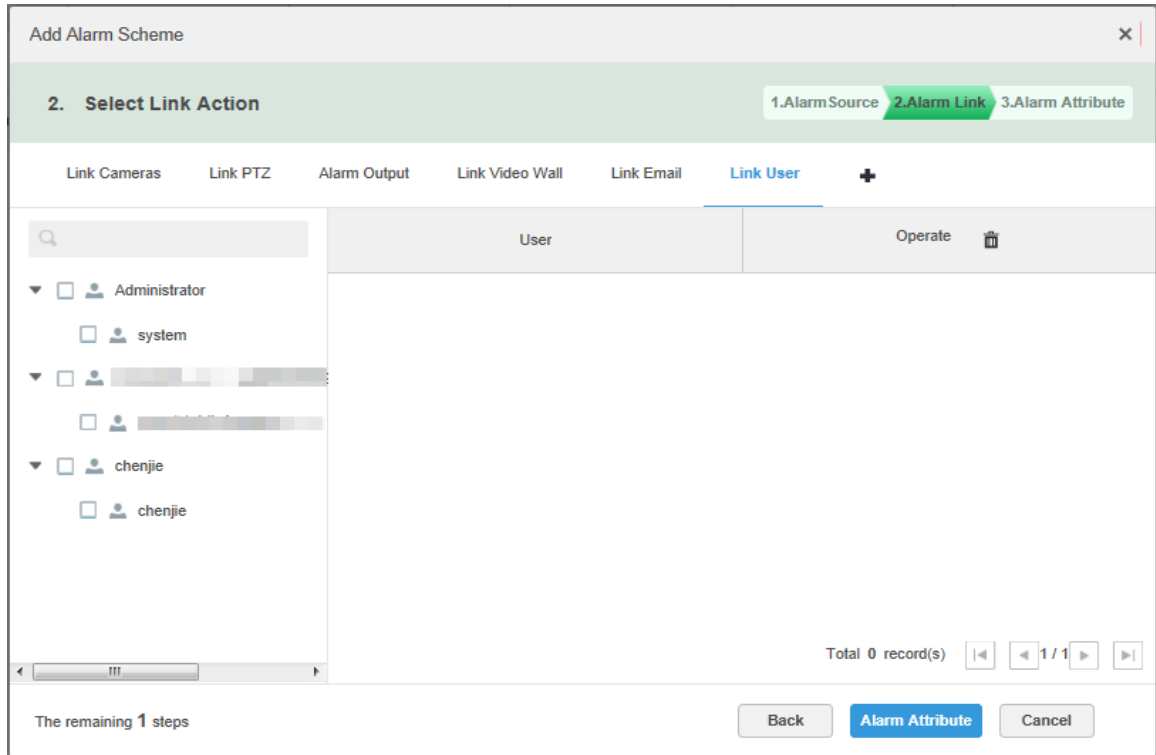
Add Alarm Scheme

Template Name	Mail Content:
Default	Template Name:
test	
12	Event time Org name Event source Event type
+ New Template	Subject:
	Mail Content:

OK Cancel

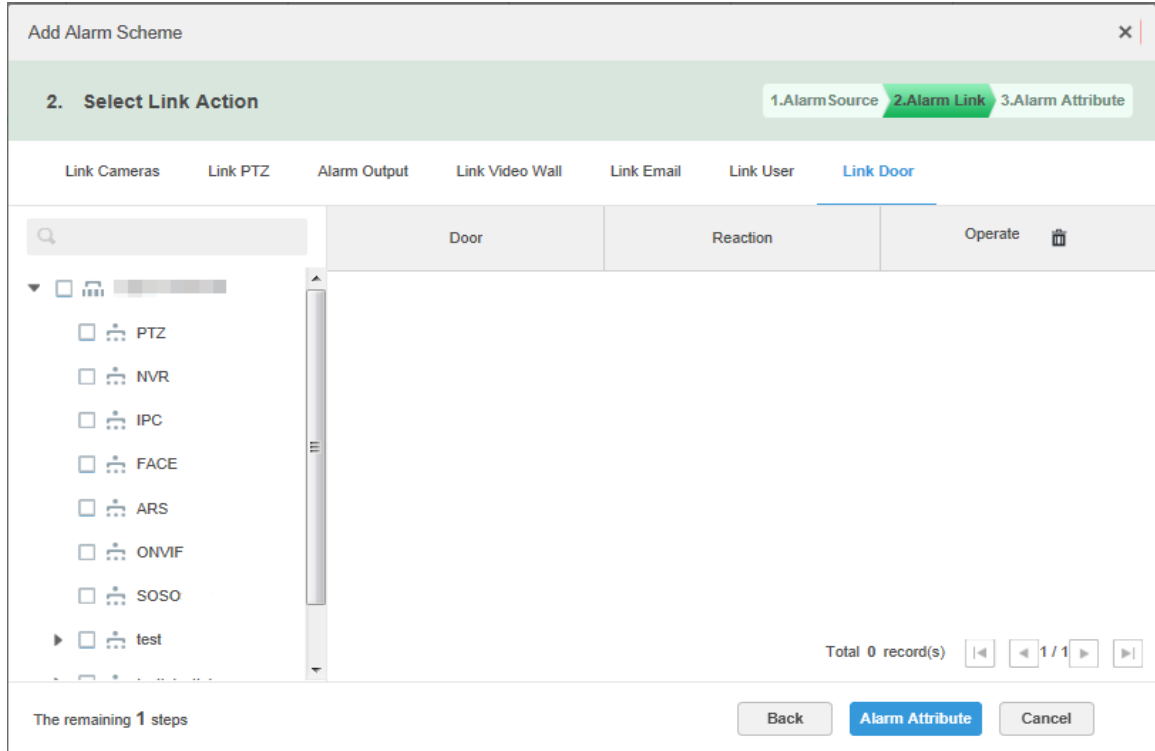
- ◇ Click **Link User**, select the users to be informed.

Figure 4-59 Link user



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

Figure 4-60 Link door



Step 5 Click **Alarm Attribute**.

Figure 4-61 Configure alarm attribute

The screenshot shows a window titled "Add Alarm Scheme" with a close button in the top right corner. Below the title bar, there are three tabs: "1.Alarm Source", "2.Alarm Link", and "3.Alarm Attribute", with the third tab being active. The main area contains the following fields:

- Name:
- Time Template:
- Priority:
- Remark:

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




Step 6 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 7 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.

4.8 Configuring Map

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



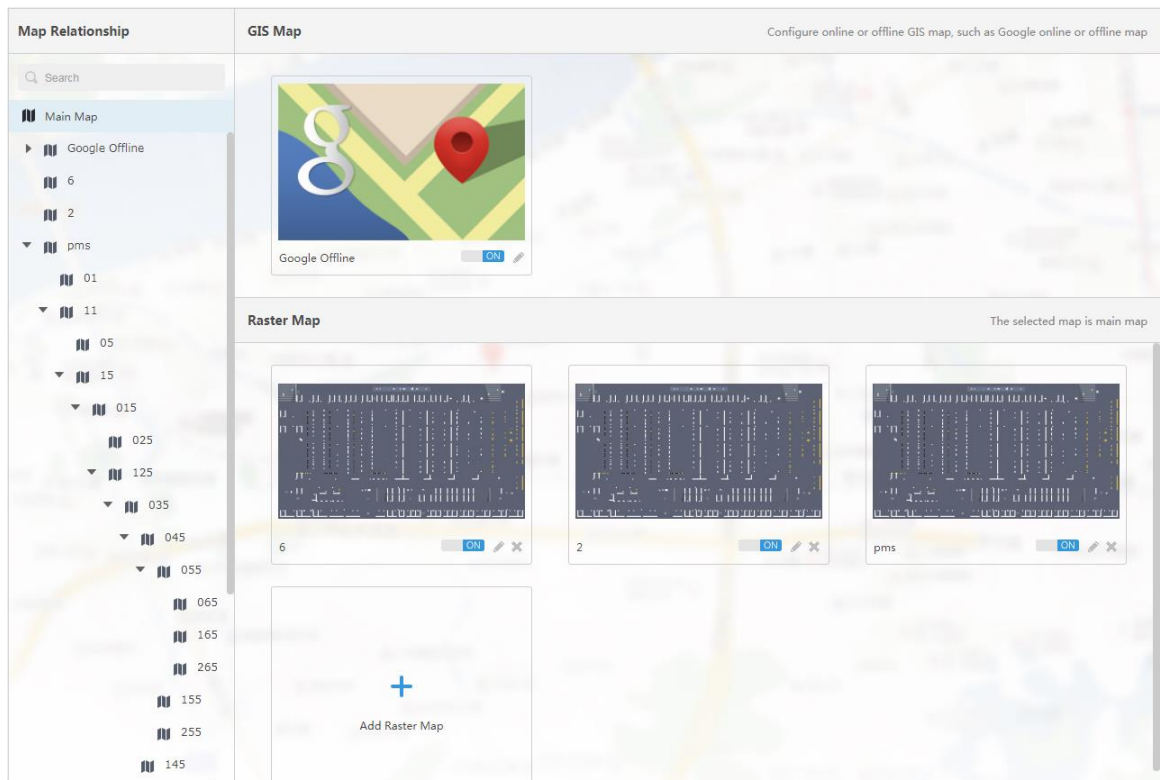
- A raster map is a floor plan or a picture of a place. The server enables raster map by default.
- GIS map includes Google online map and Google offline map.

4.8.1 Adding Map

4.8.1.1 Adding GIS Map

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

Figure 4-62 Map




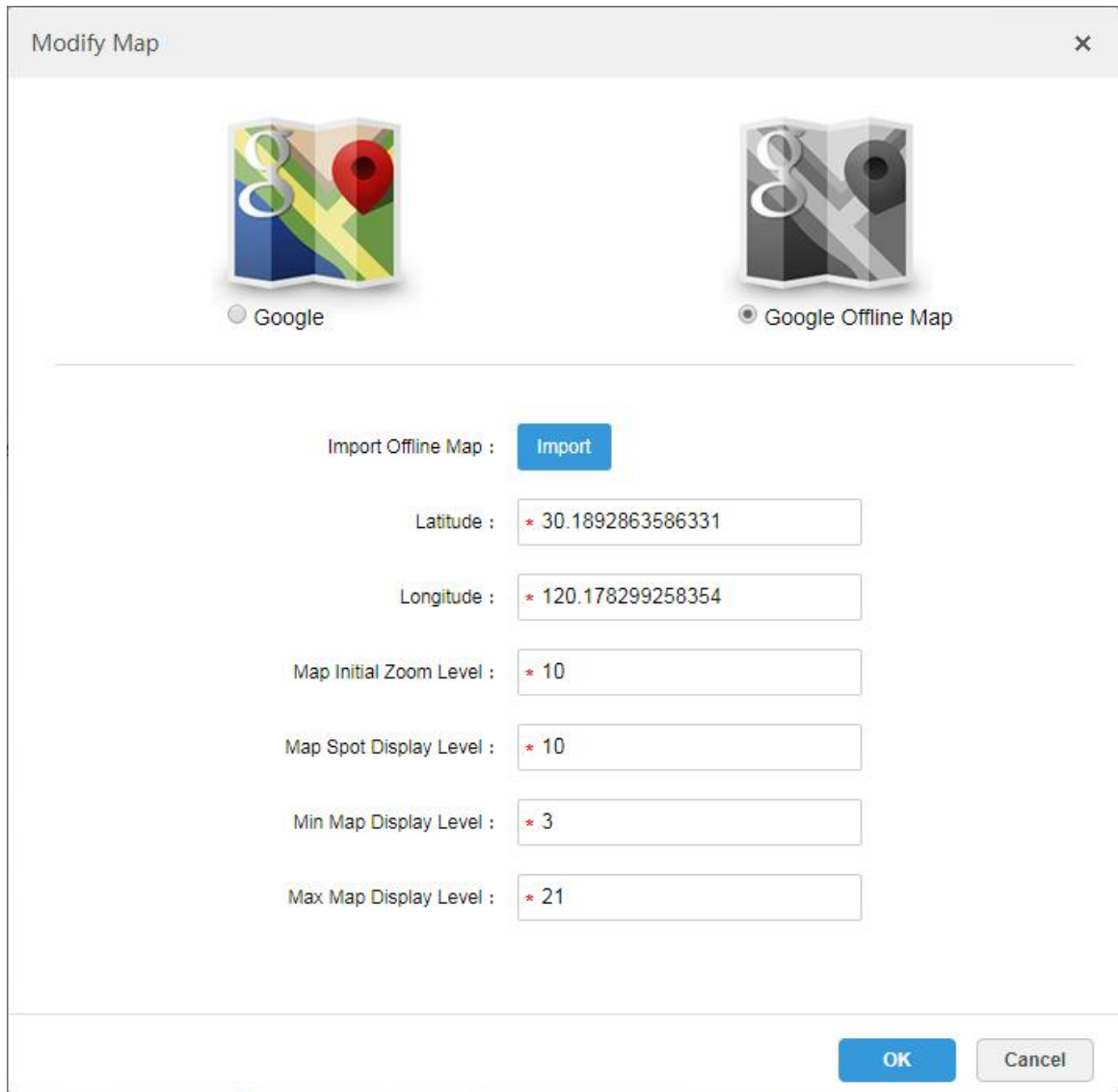
Step 2 Click  on the Google map.

Figure 4-63 Map configuration



Step 3 Select a map type, and then set parameters

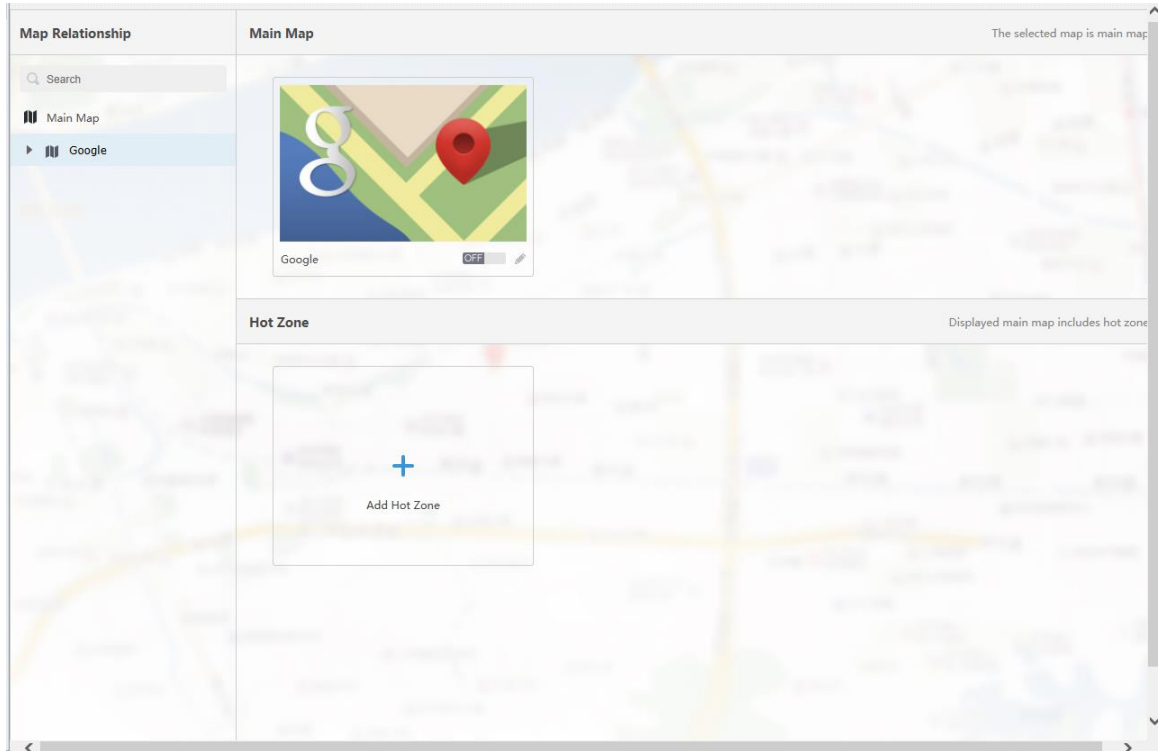
- Google online map
 - 1) Select Google online map.
 - 2) Configure map information, and then click **OK**.
- Google offline map
 - 1) Select Google offline map.
 - 2) Click **Import** and import offline map.
 - 3) Configure map information, and then click **OK**.

Step 4 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.

Figure 4-64 GIS map



2) Click Add Hot Zone.

Figure 4-65 Adding hot zone

The 'Add Hot Zone' dialog box contains the following fields and controls: a 'Name:' text box with a red asterisk; a 'Picture:' text box with a blue 'Browse' button; a 'Preview:' area showing a map icon and the text 'Import raster map, support PNG, JPG, JPEG'; and a 'Remark:' text box. At the bottom are 'Next' and 'Cancel' buttons.

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.

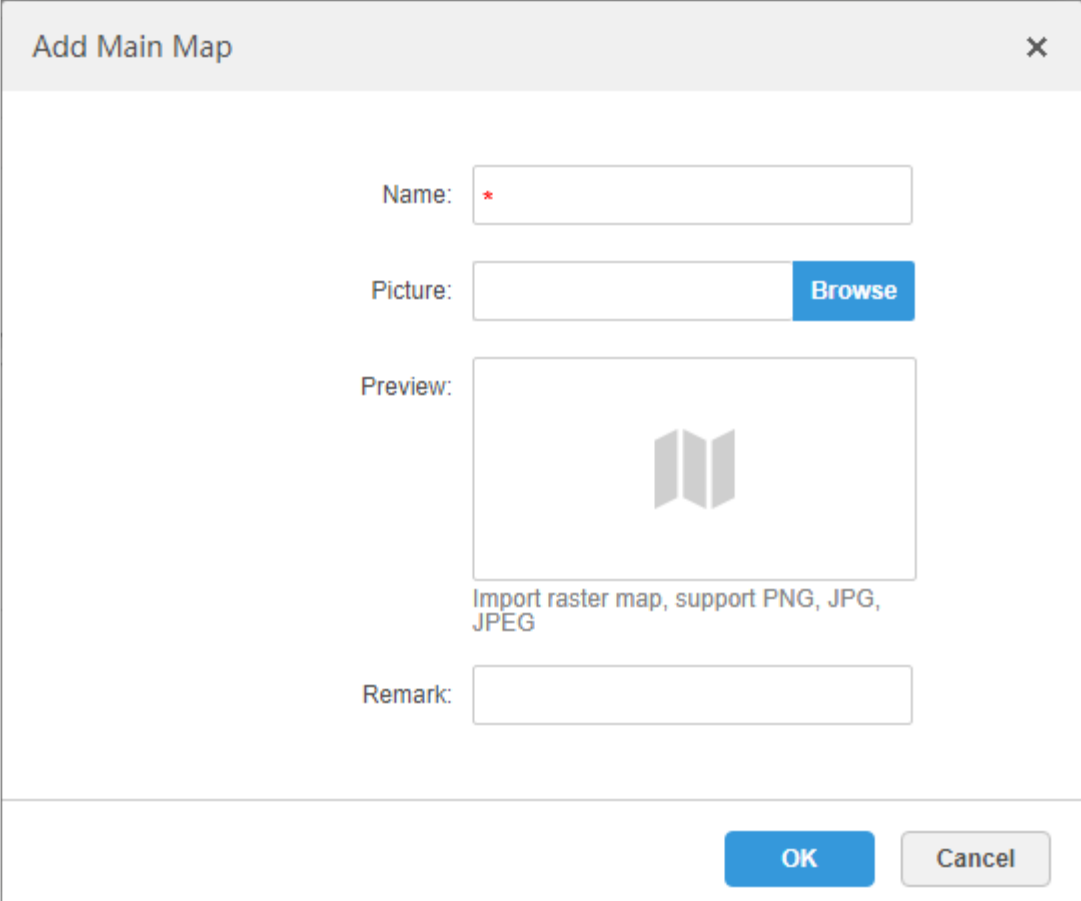
4.8.1.2 Adding Raster Map

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 Click **+** and select **Map** on the **New Tab** interface.

Step 2 Click **Add Raster Map**.

Figure 4-66 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 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 the preview area, the text "Import raster map, support PNG, JPG, JPEG" is displayed.
- Remark:** A text input field.
- Buttons:** At the bottom right, there are two buttons: a blue "OK" button and a gray "Cancel" button.

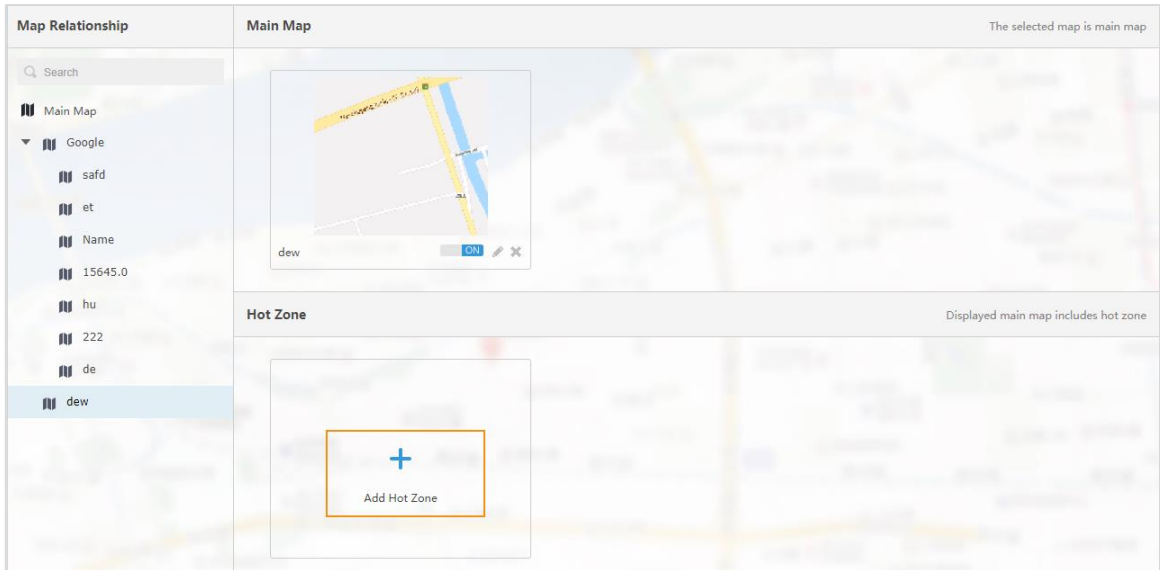
Step 3 Enter the map name, select the picture and then click **OK**.

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

Step 4 Add a hot zone.

- 1) Click the added GIS map or raster map in the map list. The **Hot Zone** interface is displayed.

Figure 4-67 Adding hot zone



2) Click Add Hot Zone.

Figure 4-68 Adding hot zone

The 'Add Hot Zone' dialog box has a title bar with a close button. It contains the following fields and controls:

- 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 map icon. Below it, the text reads: 'Import raster map, support PNG, JPG, JPEG'.
- Remark:** A text input field.

At the bottom right, there are two buttons: a blue 'Next' button and a grey 'Cancel' button.

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

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

4.8.2 Marking Devices

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



You do not need to link mobile devices to the map, because they report their locations automatically in real time.

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

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

Figure 4-69 Map

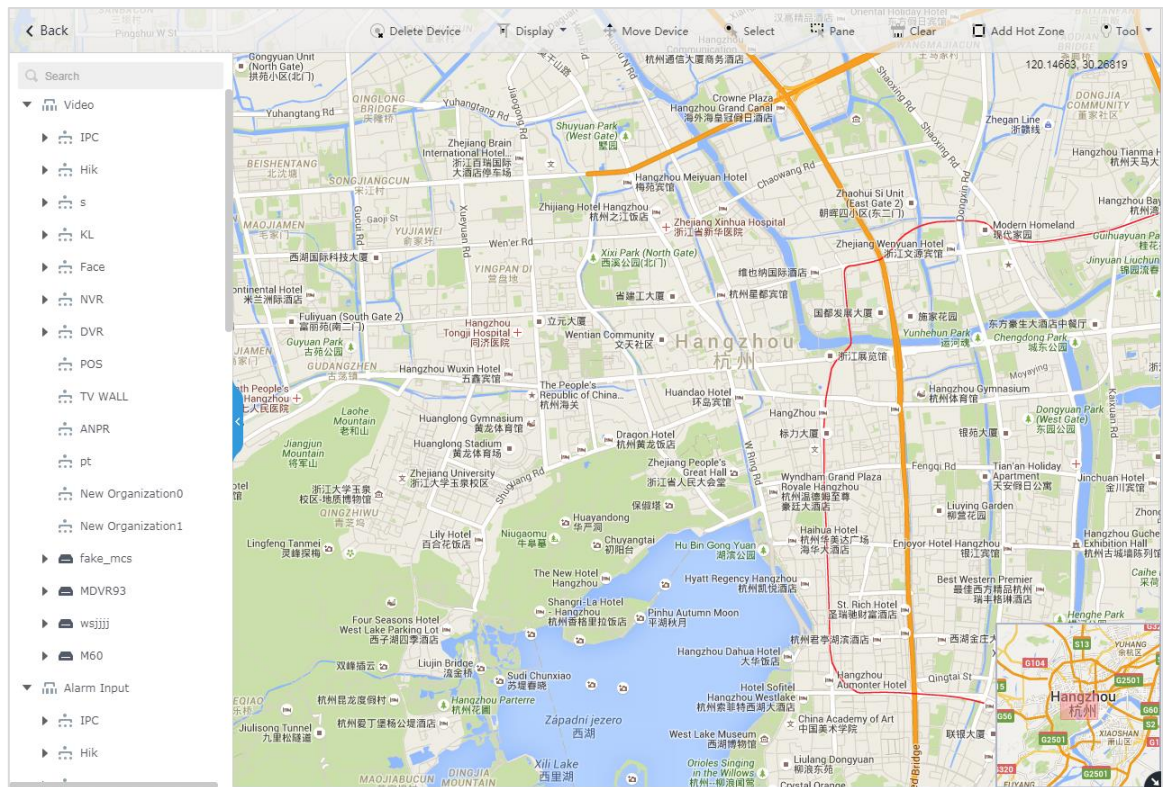


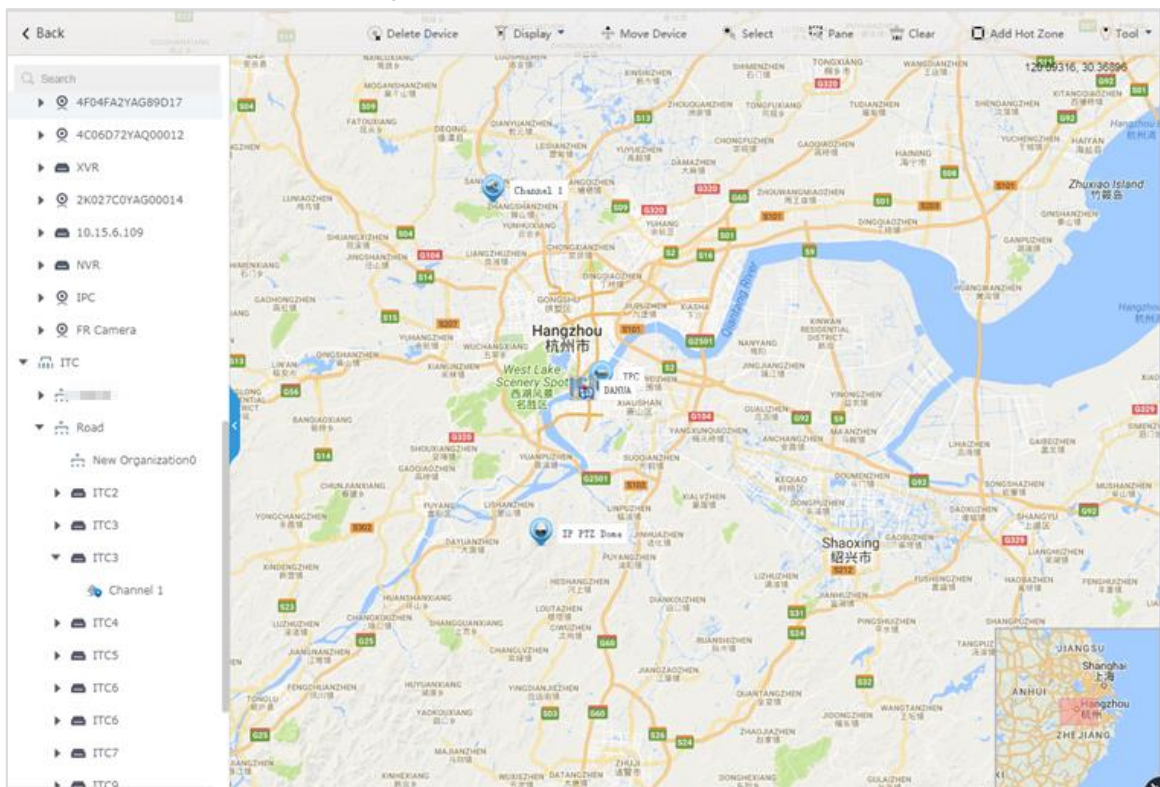
Table 4-4 Description

Parameter	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 boxing trace on the screen.
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 4-70 Add a channel

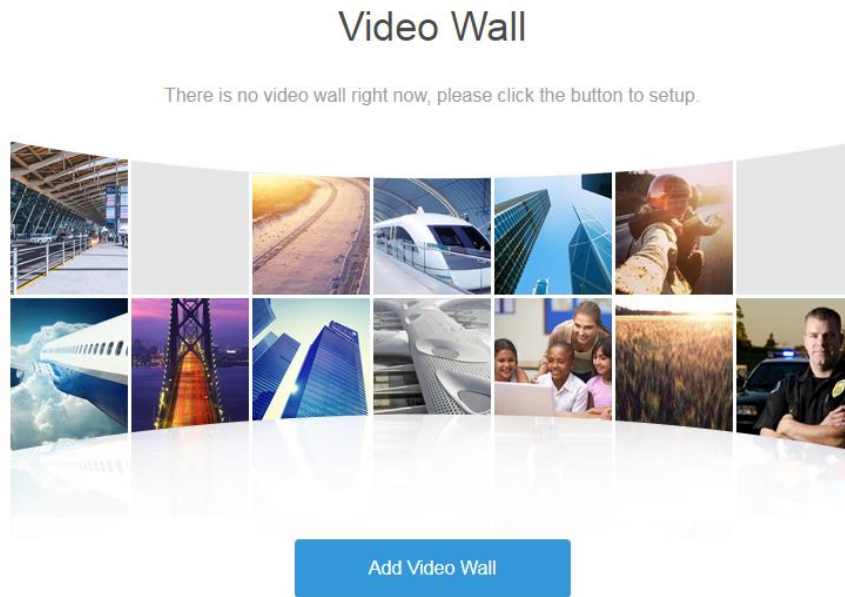


4.9 Adding Video Wall

Add a video wall layout on the platform.

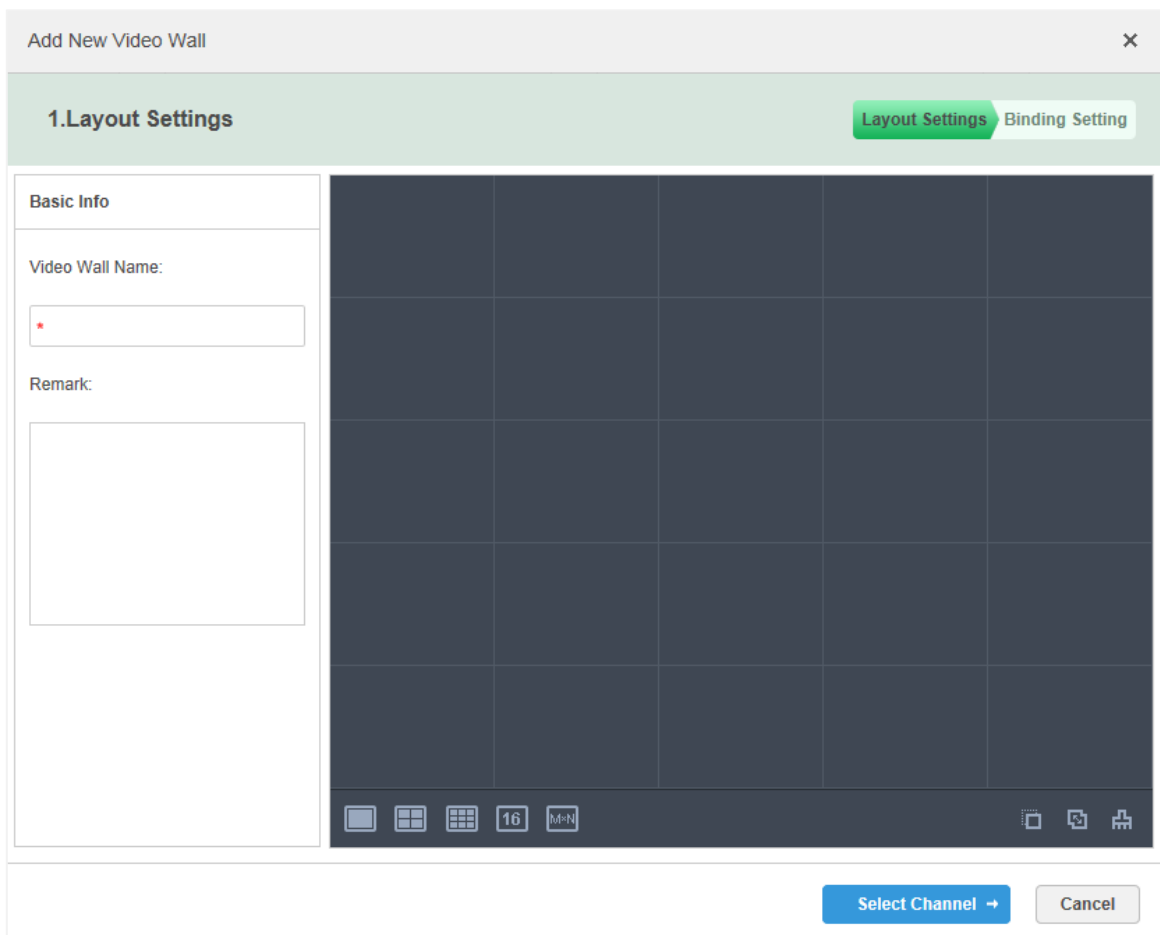
Step 1 Click **+** and select **Video Wall** on the **New Tab** interface.

Figure 4-71 Video wall configuration interface



Step 2 Click **Add Video Wall**.

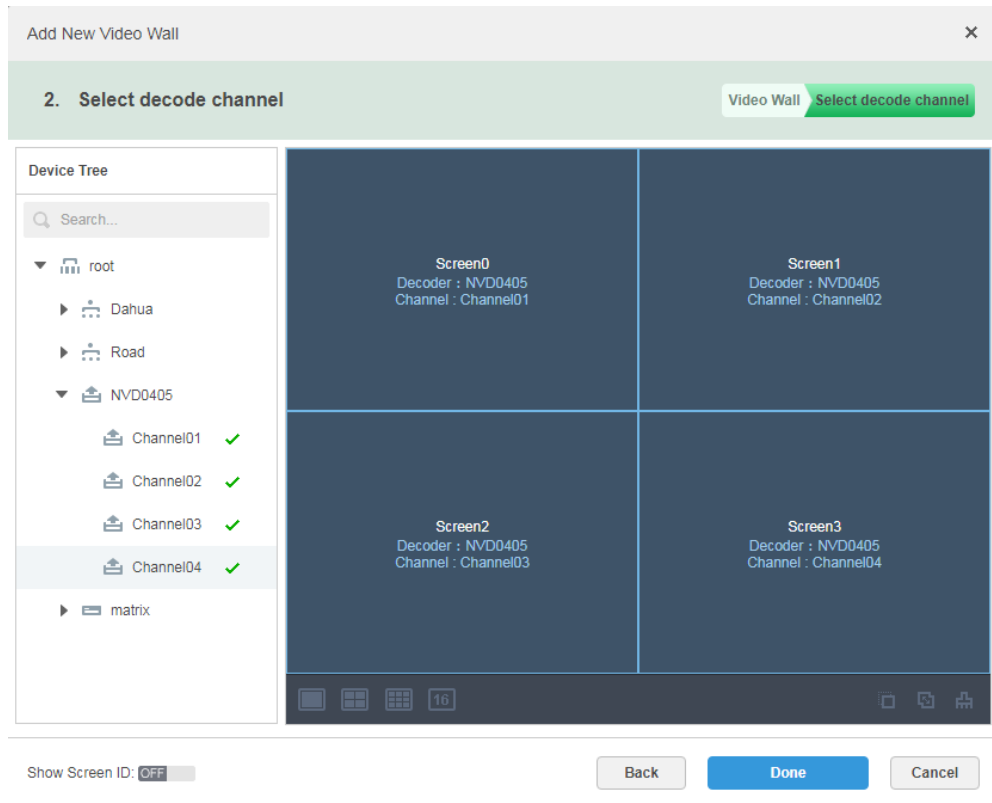
Figure 4-72 Add a video wall



Step 3 Enter **Video Wall Name**, select window distribution.

Step 4 Click **Select Channel**.

Figure 4-73 Select a decoding channel



It 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.

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

Step 6 Click **Done**.

4.10 Configuring Face Recognition

You can refer to the following chapter if it is to realize the function of face recognition.

4.10.1 Creating Face Database

It supports creating face library, managing face information in the library, and add face images to the library as references for comparison.

4.10.1.1 Adding Face Database

Face library is used to store staff information, which is convenient to deploy or search staff.


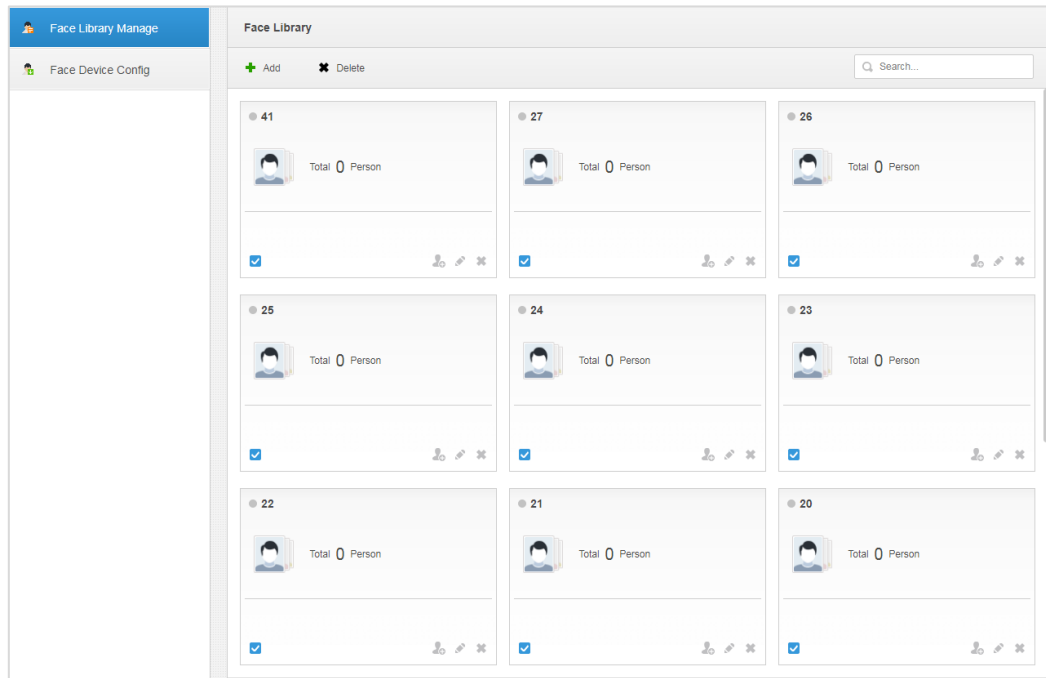
Step 1 Click  and select **Face Database**.

Figure 4-74 Face library



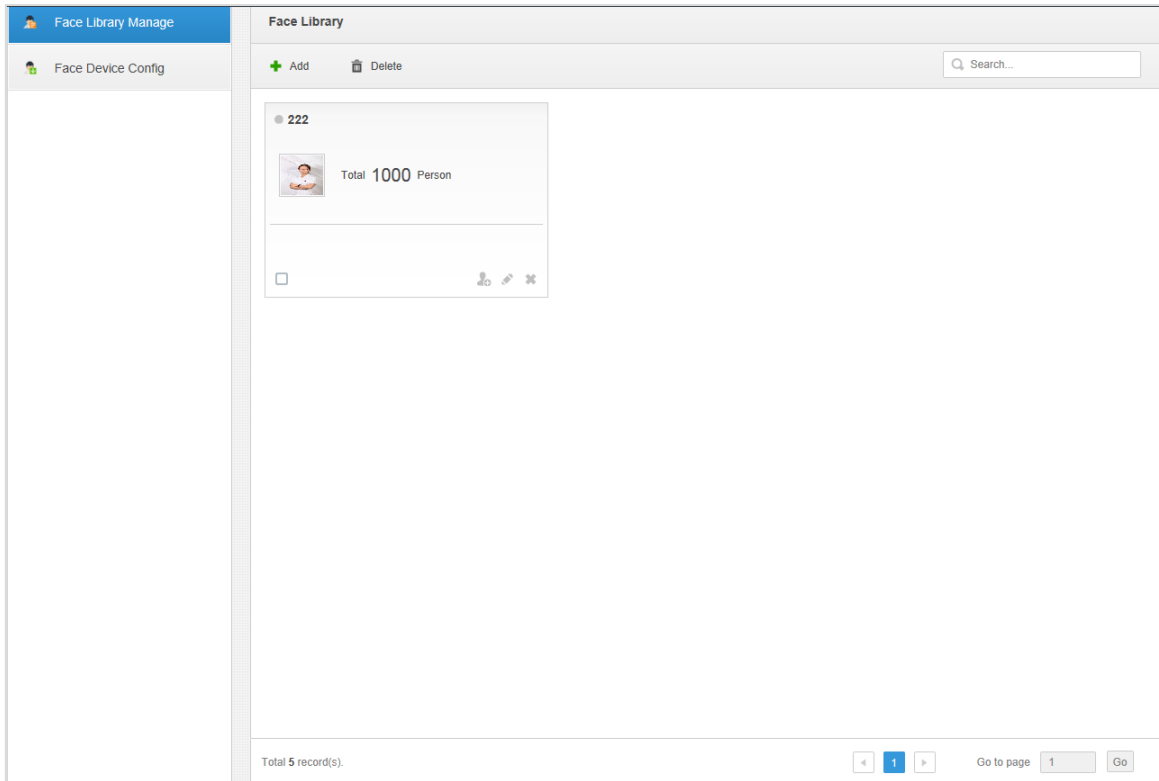
Step 2 Click **Add**.

Figure 4-75 Add a face library




The dialog box is titled "Add Face Library" and has a close button (X) in the top right corner. It contains three input fields: "Library Name" with a red asterisk indicating it is required, "Library Color" with a dropdown menu currently set to "Gray", and "Remark". At the bottom right, there are two buttons: "OK" (highlighted in blue) and "Cancel".

Step 3 Enter library name, select library color, and then click **OK**.

Figure 4-76 Added face library



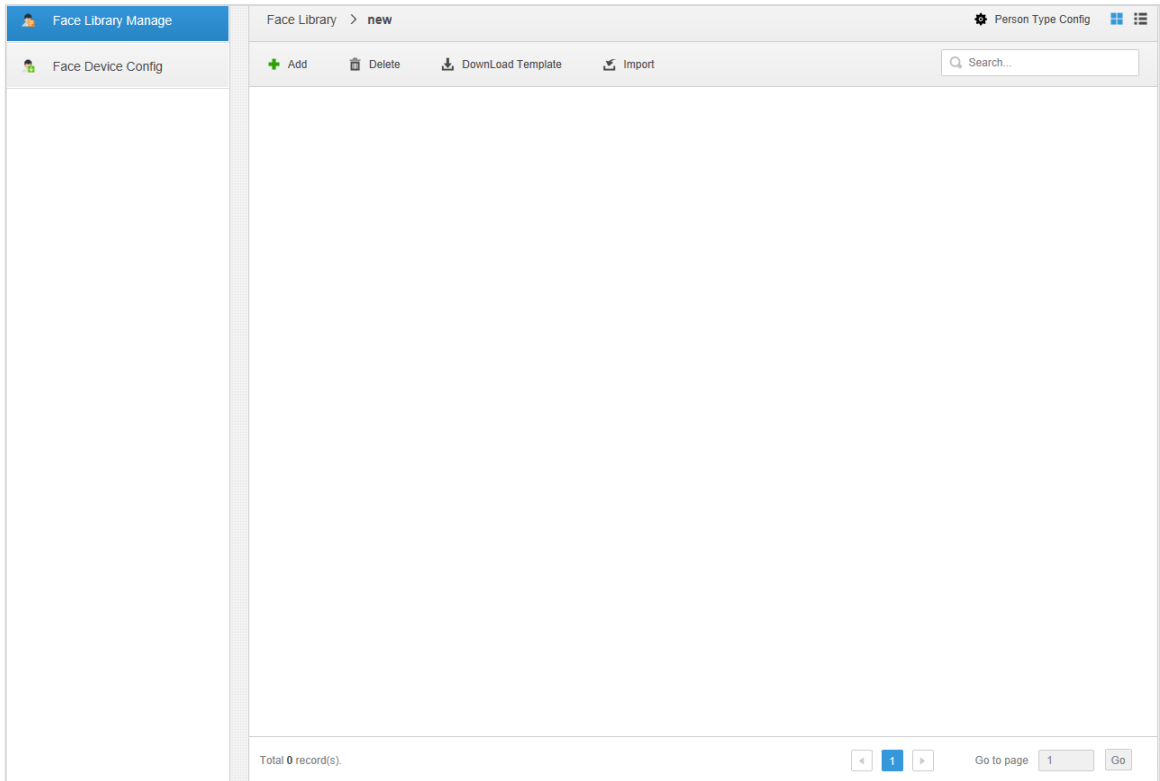
Other Operations

- Search library
Filter the library via face library type or keyword.
- Add face library
Click  to add staff information. Please refer to "4.10.1.3 Adding Face Library Information."
- Modify staff Library
Click  to modify library name and library description.
- Delete staff Library
Click  to delete face library only when there is no face information under the library.

4.10.1.2 Configuring Person Type

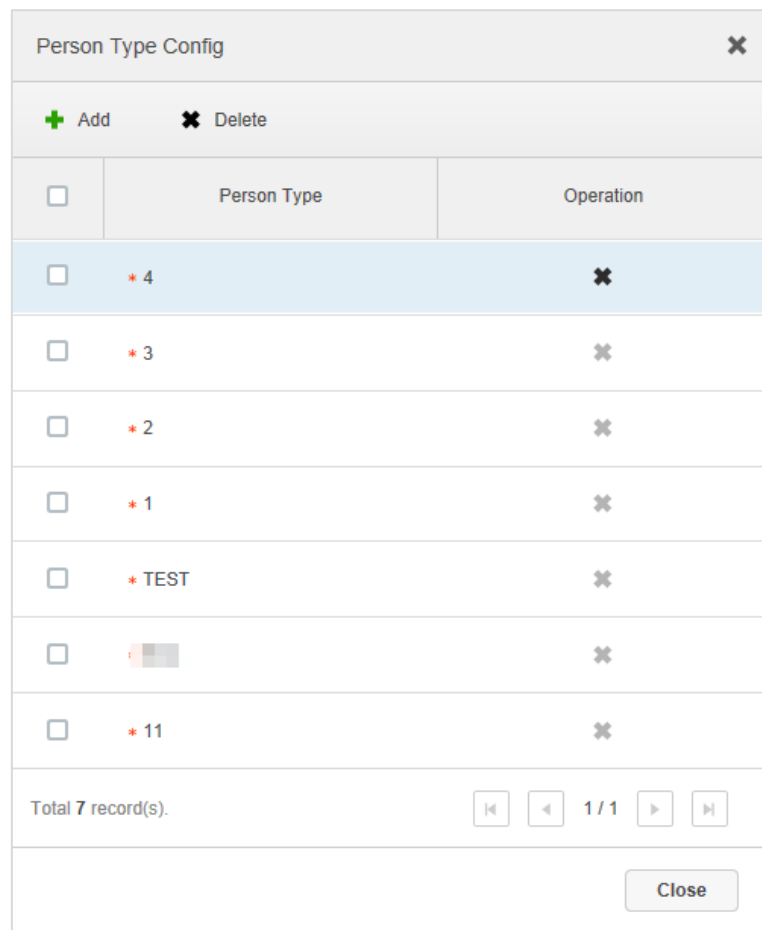
Step 1 Click the face library which needs to be added with person on the **Face Library Manage** interface.

Figure 4-77 Set face library




Step 2 Click **Person Type Config**.

Figure 4-78 Set person types



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.

4.10.1.3 Adding Face Database Information

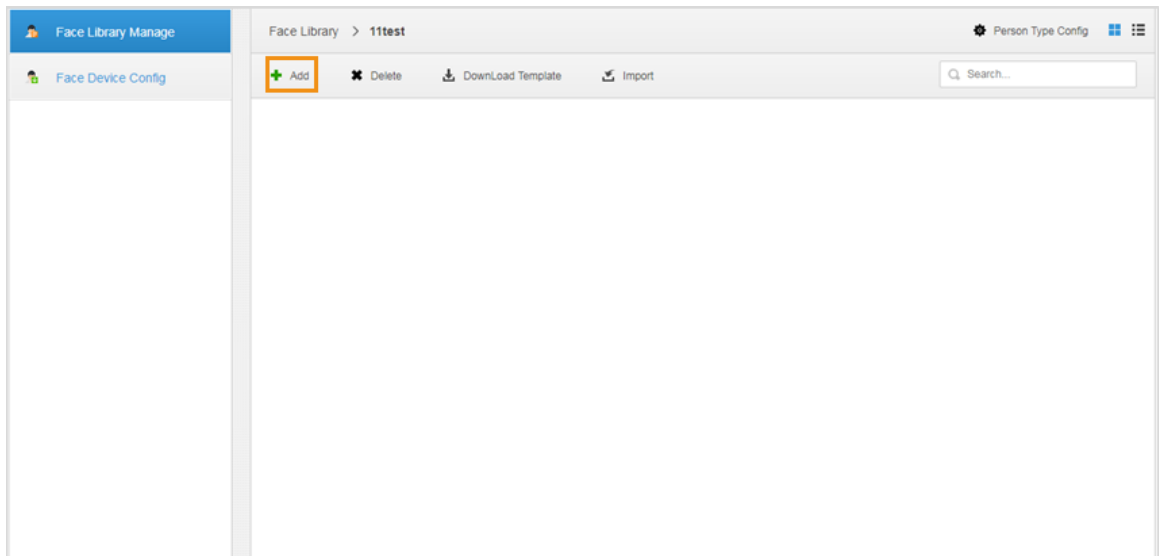
It can add person information via adding individual person and importing in batches.

4.10.1.3.1 Manual Add

Step 1 Enter the adding person interface in two ways:

- Click the library which needs to be added with people on the **Face Library Manage** interface.

Figure 4-79 Add a face library




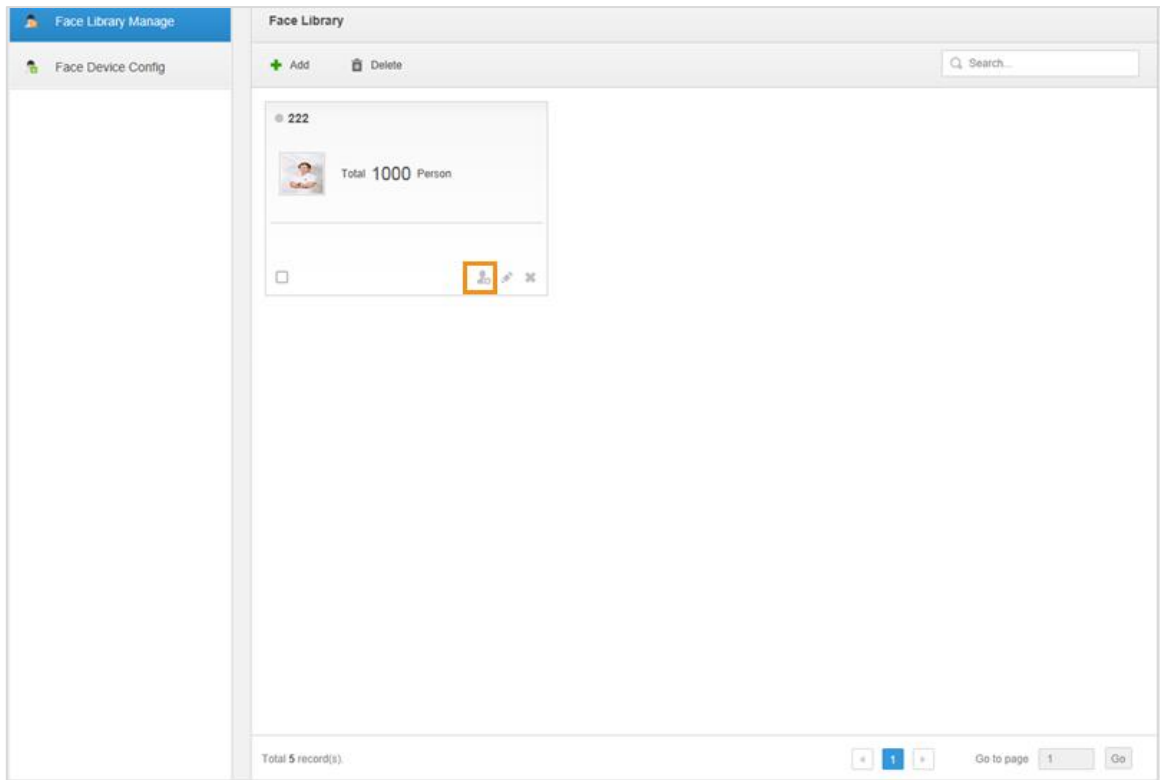
- Click  on the person library card.

Figure 4-80 Set person details





Step 2 Enter person information.

Step 3 Click profile photo and upload a face picture.

Step 4 Click **OK**.

Operations

- Query person
Enter key words into the query text box, press Enter or click  to query person.
- Delete person
 - ◇ Click  on person interface and then you can delete person individually.
 - ◇ Select person, click **Delete** to delete person in batches.

4.10.1.3.2 Batch Import

Prepare face pictures in advance if you want to import in batches, and compress it into zip files. Currently batch import supports max 1000 pictures at one time.

Figure 4-81 Zip file

The screenshot shows a file explorer window with a list of files. The files are 'Face.jpg' and 'face-EN.xls'. The table below represents the data shown in the screenshot.

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...

Figure 4-82 Table

*Person Name	*Certificate No.	*Person Type	*Gender	Birthday	Region	Remark	*Face Image
Jerry	35125	Staff	Female	2018/05/26	China	Joined on October 2th	Face.jpg

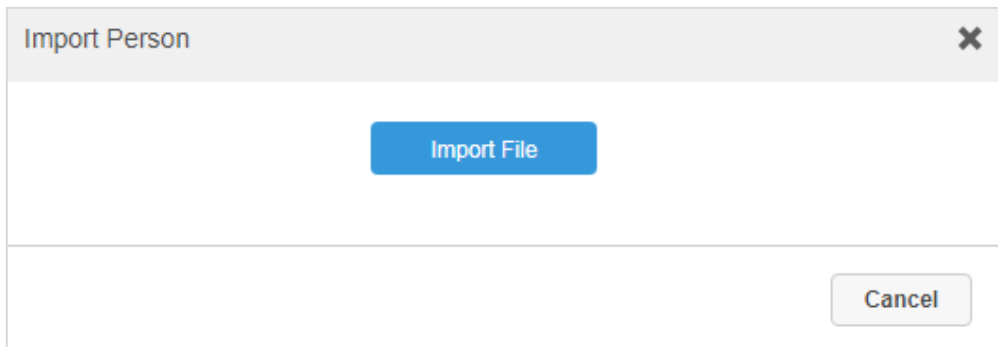
Fill Requirements :

- 1.* indicates this blank must be filled and a maximum of 1000 persons each time.
- 2.Person Name: Can only contain letter, number, Chinese character -_:#() < > @[] plus sign of half angle and plus sign of fully angle and space among letters.
- 3.Certificate No.: Can only contain letter and number.
- 4.Person Type: Fill in the type created on the web manager.
- 5.Gender: "Male" or "Female", you can select it from drop-down box.
- 6.Birthday: Year/Month/Day
- 7.Region: You can select it from drop-down box.
- 8.Remark: Can only contain letter, number, Chinese character -_:#() < > [] plus sign of half angle and plus sign of fully angle and space among letters.
- 9.Face Image: It must be jpg format, name in the blank must keep same with picture's name. The picture is less than 1000 pixels * 1000 pixels.

Step 1 Click the library to add person on the **Face Library Manage** interface.

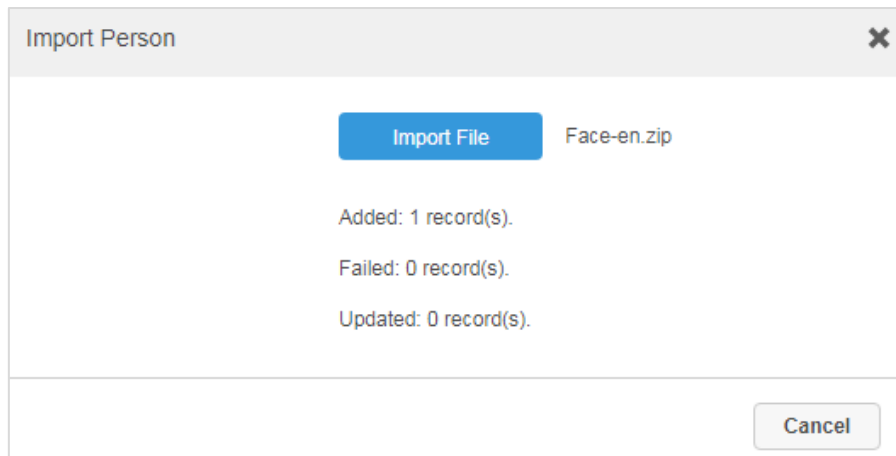
Step 2 Click **Import**.

Figure 4-83 Import faces in batches (1)



Step 3 Click **Import File** and upload compressed package according to prompt.

Figure 4-84 Import faces in batches (2)



Other Operations

Other operations are the same as those in "4.10.1.3.1 Manual Add."

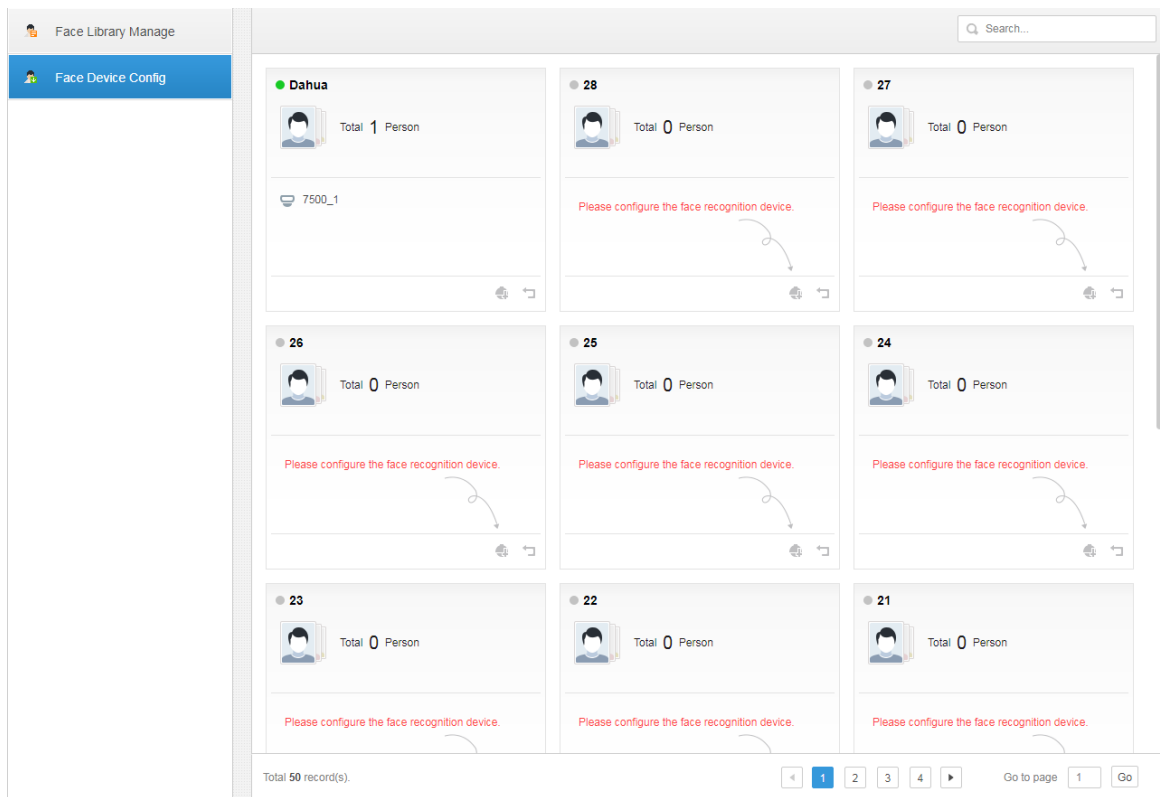
4.10.2 Arming a Face Recognition Channel

Arm means real-time comparison between capture image and face database image; it will trigger real-time alarm when the similarity reaches the value which has been set. It can make arm upon the face database where the person exists if it needs to take real-time surveillance over the designated person.

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

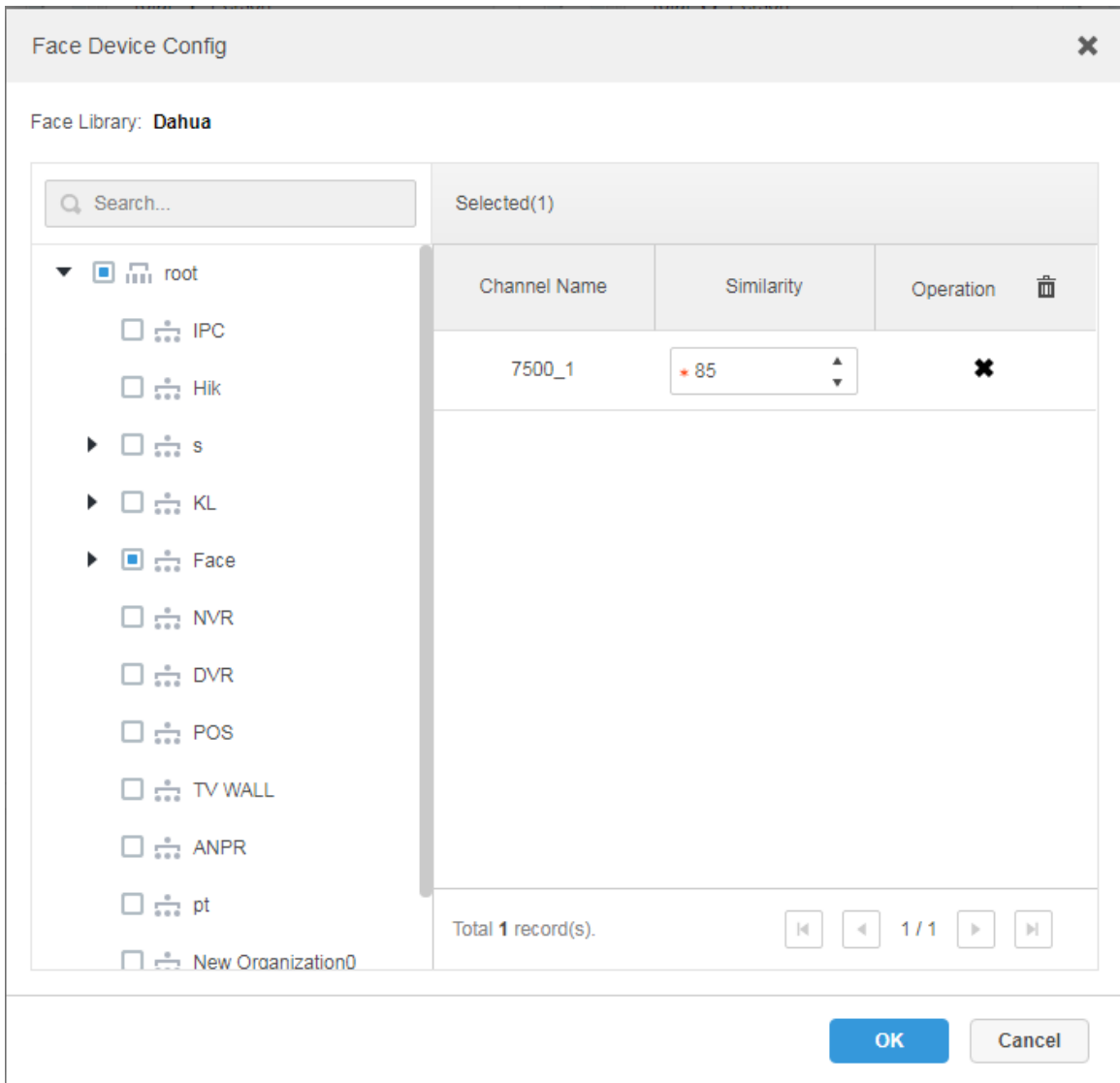
Step 2 Click **Face Device Config** on the left of navigation bar.

Figure 4-85 Face device configuration



Step 3 Click  to start arm.



Figure 4-86 Select a channel



Step 4 Select arm channel and set similarity.

Step 5 Click **OK** to complete arm.

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 **Arm Manage** interface to disarm.































4.11 Adding Vehicle Blacklist

Arm means monitoring vehicles, it will trigger alarm when it takes snapshot and recognizes the vehicle with designated license plate. Arm management includes adding vehicle blacklist, arming and disarming.

It can refer to the chapter when it needs to realize the business of road surveillance.

Step 1 Click  and select **Vehicle Blacklist** on the interface.

Figure 4-87 Vehicle blacklist

<input type="checkbox"/>	Plate No.	Arm Type	Start Time	End Time	Arm Status	Armed Person	Operate
<input type="checkbox"/>	121111111	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

Step 2 Click **Add**.

Figure 4-88 Add a vehicle

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

- Plate No. : (with a red asterisk indicating a required field)
- Start Time : (with a red asterisk and a calendar icon)
- End Time : (with a red asterisk and a calendar icon)
- Vehicle Type : (dropdown menu)
- Plate Color : (dropdown menu)
- Vehicle Logo : (dropdown menu)
- Vehicle Color : (dropdown menu)
- Arm Type : (dropdown menu)

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


Step 3 Set armed vehicle information, including plate number, start time, vehicle type, plate color, vehicle logo, vehicle color and arm type.

Step 4 Click **OK**.


The system prompts that it has added successfully. It is armed by default.

Operations

- Modify vehicle blacklist

Click  of corresponding vehicle in the list, and then you can edit relevant information of vehicle arm.

- Delete vehicle blacklist

Click  of corresponding vehicle arm information in the list, or select vehicle arm information, click Delete to delete vehicle arm information.

- Arm/Disarm

Select vehicle arm information, click **Arm** to arm the vehicle; Click **Disarm** to disarm the vehicle.

- **Import**

Click **Import** and it can import vehicle arm information according to template.



It can download import template in the Import interface after clicking Import.

- **Export**

Select vehicle arm information, click **Export Selected** to export the selected vehicle arm info; click **Export All** to export all the vehicle arm information in the list.

4.12 Video Intercom Management

4.12.1 Configuring Building/Unit

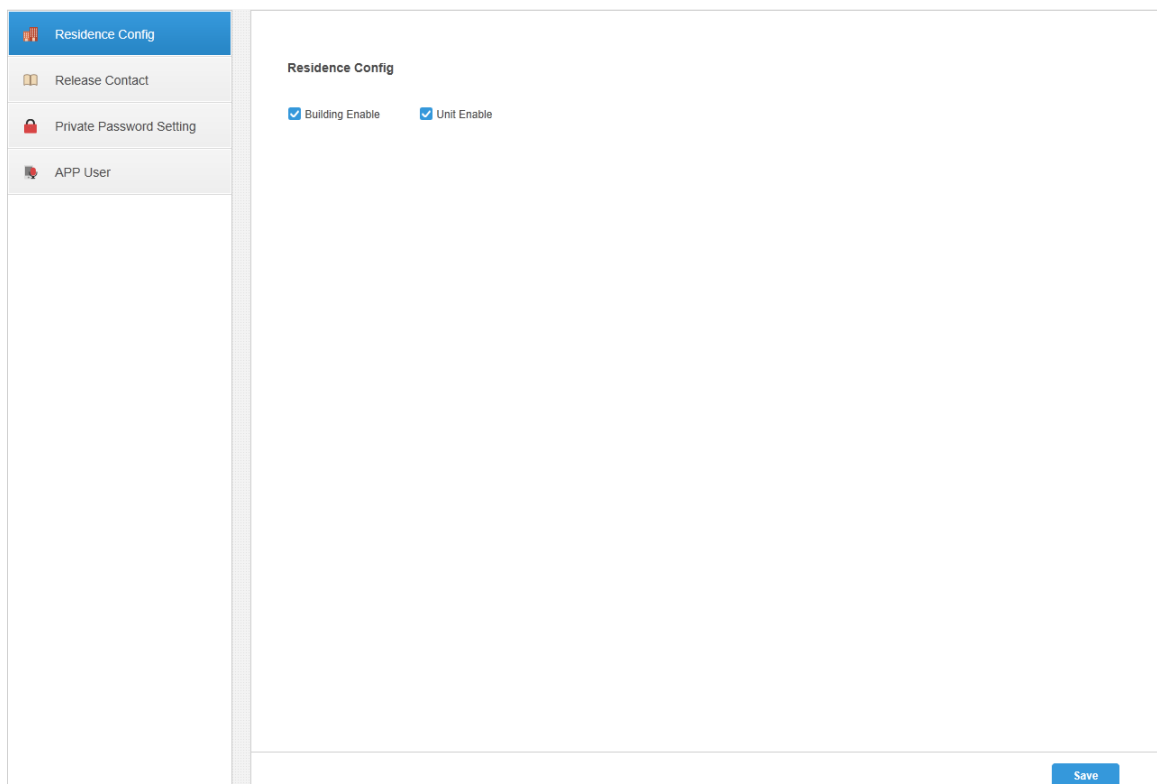
It needs to make sure the enable of building and unit is in accordance with the device if you want to use the video talk module of the platform, otherwise, the device is offline after adding device. The setting of building and unit affects the dialing rule. Take room 1001 unit 2 building 1 as an example, the dialing rule is shown as follows after it is enabled.

- If building is enabled, unit is not enabled, and then the number is "1#1001".
- If building is enabled, unit is enabled as well, and then the number is "1#2#1001".
- If building is not enabled, unit is not enabled either, and then the number is "1001".

Step 1 Click  and select **Video Intercom Management** on the interface. The system displays the **Video Intercom Management** interface.

Step 2 Click the tab of **Residence Config**.

Figure 4-89 Residence configuration



Step 3 Enable or disable building and unit according to the actual situation, it is required to be in accordance with that of the device, click **Save** and complete configuration.

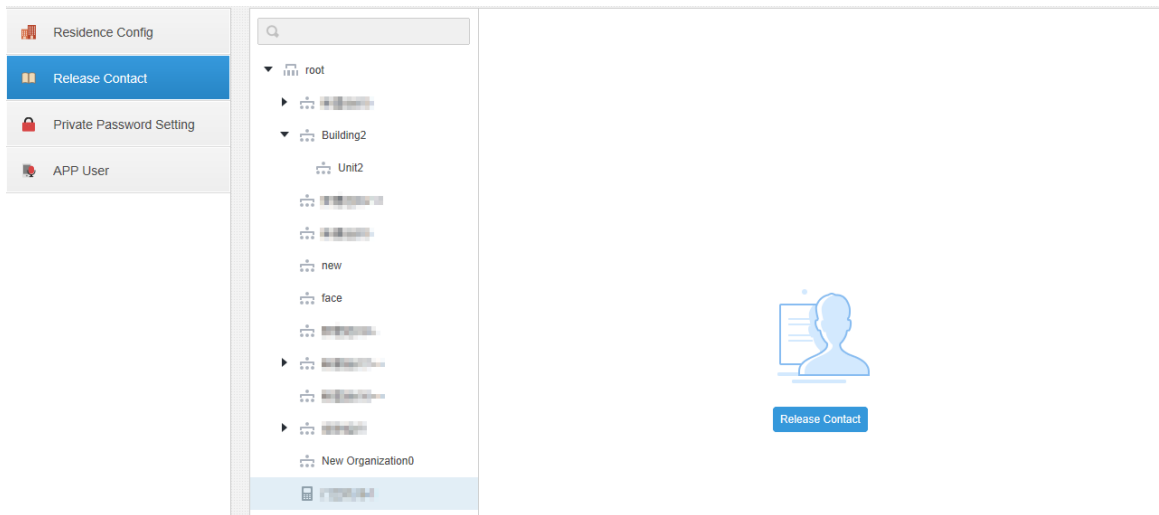
4.12.2 Synchronizing Contacts

Synchronize contacts information to VTO and then you can view contacts on the VTO display screen or WEB interface.

Step 1 Click **+** and select **Video Intercom Management** on the interface.

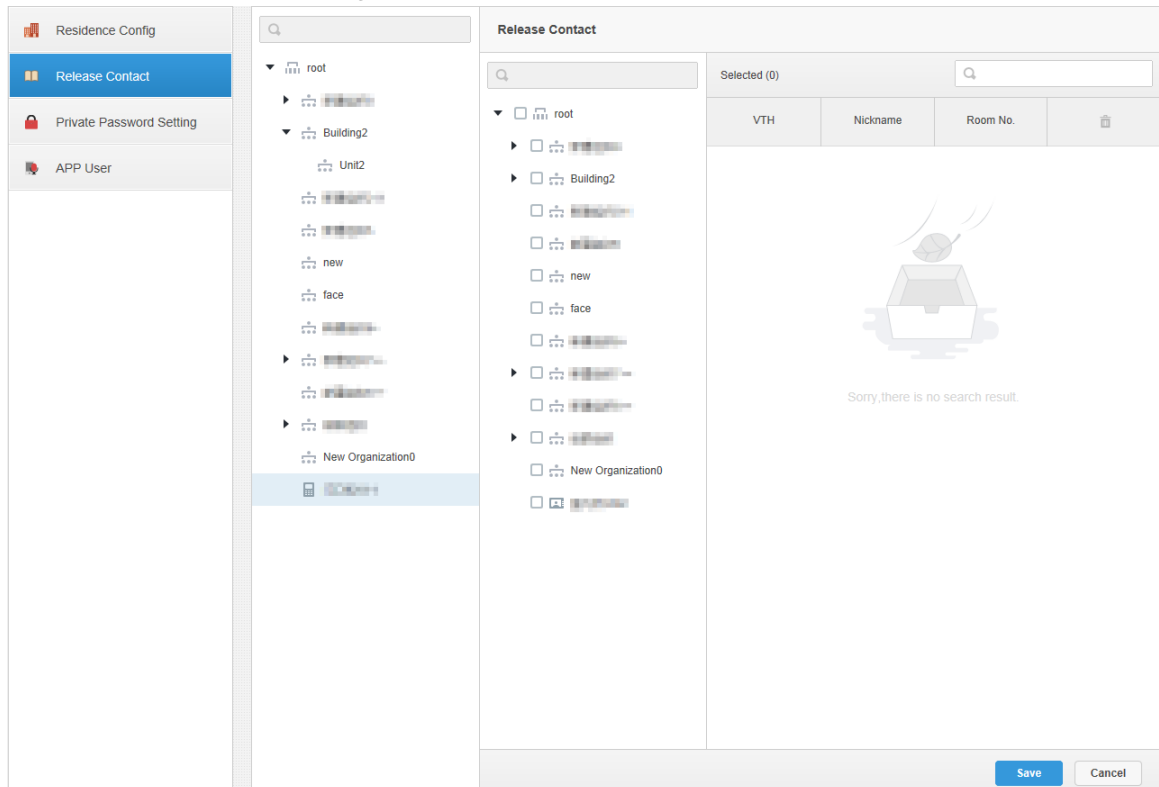
Step 2 Click the tab of **Release Contact**.

Figure 4-90 Release contact (1)



Step 3 Select organization node (VTO) and click **Release Contact**.

Figure 4-91 Release contact (2)



Step 4 Select VTH and click **Save**.

You can view contact on the VTO display screen or Web interface after releasing is completed.

4.12.3 Setting Private Password

It sets the unlock password of corresponding VTO bound by VTH.

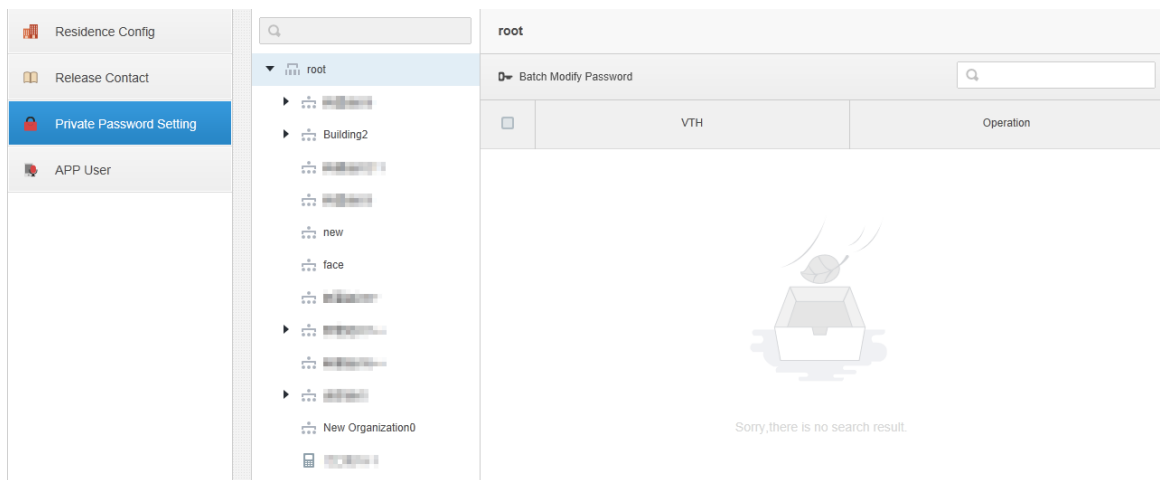


Contacts is required to be released to VTO, otherwise it fails to set private password.

Step 1 Click  and select **Video Intercom Management** on the interface.

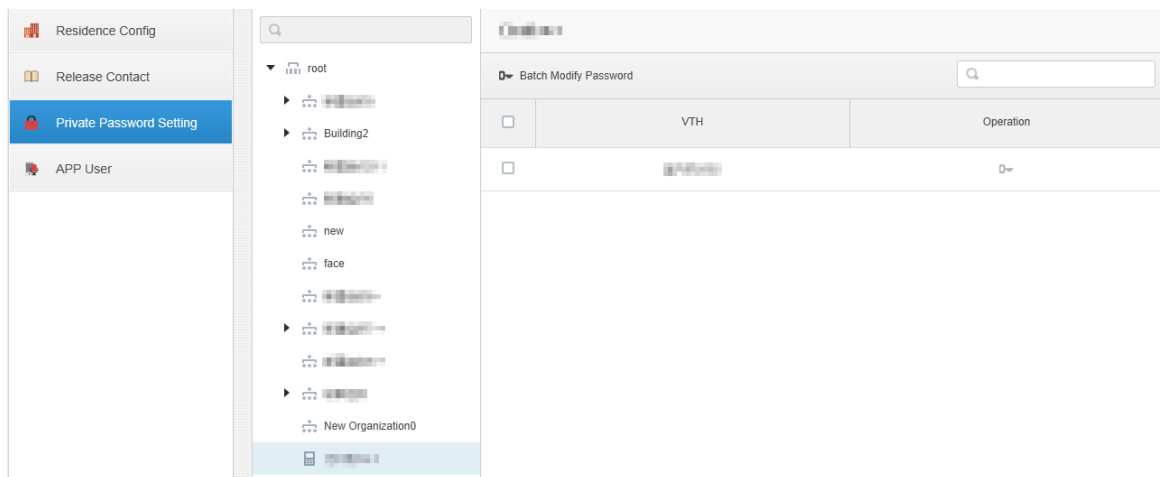
Step 2 Click the tab of **Private Password Setting**.

Figure 4-92 Set private password (1)



Step 3 Select organization node (VTO).

Figure 4-93 Set private password (2)



Step 4 Select VTH, click  or select several VTH, click **Batch Modify Password**.

Figure 4-94 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, click **OK**.

You can use the new password to unlock on the VTO.

4.12.4 APP User

It supports to view information of APP users, freeze user, modify login password and delete user.



APP user can register by scanning QR code on the VTH; refer to APP user manual for more details.

Step 1 Click + and select **Video Intercom Management** on the interface.






Step 2 Click the tab of **APP User**.

Figure 4-95 App user

		Username	VTH Info	SIP Code	Last Login Time	Right Status	Last Password Res...	Operation
<input type="checkbox"/>	<input type="checkbox"/>	lyca		10#1#5502#101	2019-03-25 13:37:15	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	lycl		10#1#5502#177	2019-03-25 12:02:48	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	zxy		10#1#5502#191	2019-03-26 10:05:23	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	zxy1		10#1#5502#130	2019-03-26 11:54:56	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>	ijl1		10#1#5502#139	2019-03-26 11:32:47	<input checked="" type="checkbox"/>		

Table 4-5 Parameters

Operation	APP user	Description
Freeze	APP user	After APP user is frozen, it fails to log in within 600s. ON means normal status, OFF means freezes status, both statuses can be switched The account will be frozen when invalid password attempts exceeds 5

Operation	Description
	by APP user.
Modify APP user login password	<p>Click  and enter new password on the Reset Password interface. 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 user	Click  or select APP user (several users can be selected); click Delete and the selected users will be deleted according to the interface tips.

4.13 System Maintenance

4.13.1 Server Management

Server management supports managing server information, adjusting server or superior server of the device.

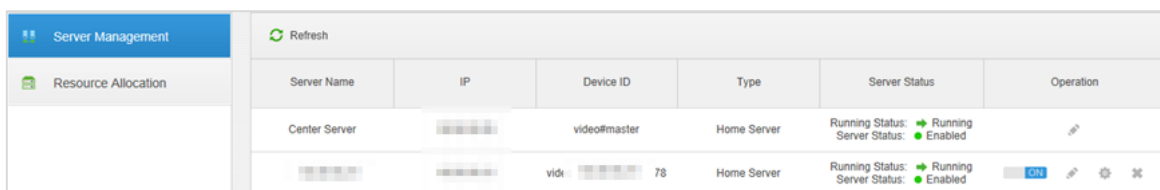
4.13.1.1 Server Management

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 **New Tab** interface.

Step 2 Click tab of **Server Management**.

Figure 4-96 Server management



Step 3 The management server supports following operations:

- Click  and edit the server information.
- OFF means the server is not enabled; Click the icon and it becomes ON, means the server is already enabled.
- Click  and allocate the server type.
- Click  and delete the server information.

4.13.1.2 Resource Allocation

Adjust the device server during distributed deployment.

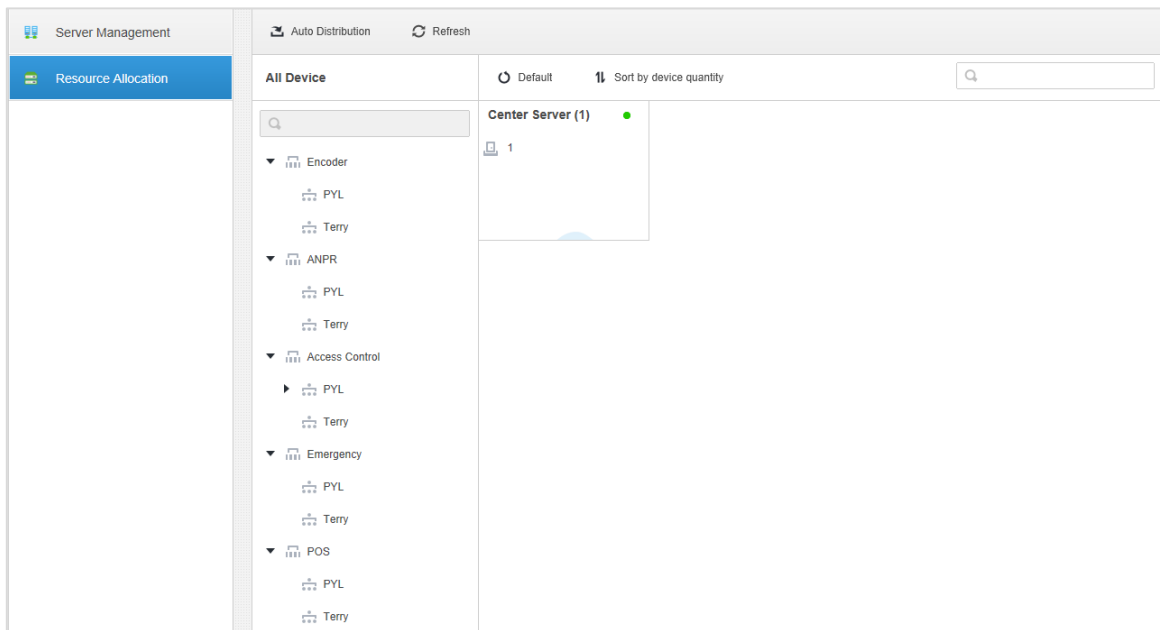
Step 1 Click  and select **Server Management** on the **New Tab** interface.

Step 2 Click the tab of Resource Allocation.



- 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 4-97 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 4-98 Auto distribution

Auto Distribution

Device Type :

Select Server

<input type="checkbox"/>	Server Name
<input type="checkbox"/>	Center Server

i Distribute devices evenly to selected server.

OK Cancel

- 2) Select Device Type, several types can be selected.
- 3) Select server where the device will be distributed to, several servers can be selected.
- 4) Click OK and complete configuration.

4.13.2 Backup and Restore

DSS platform supports backup of configured information and save it to local PC, meanwhile it supports restoring system via backup file, which is convenient for system maintenance and guarantee system security.



Only system user supports backup and restore. It can implement system backup and restore only when it logs in DSS management via system account.

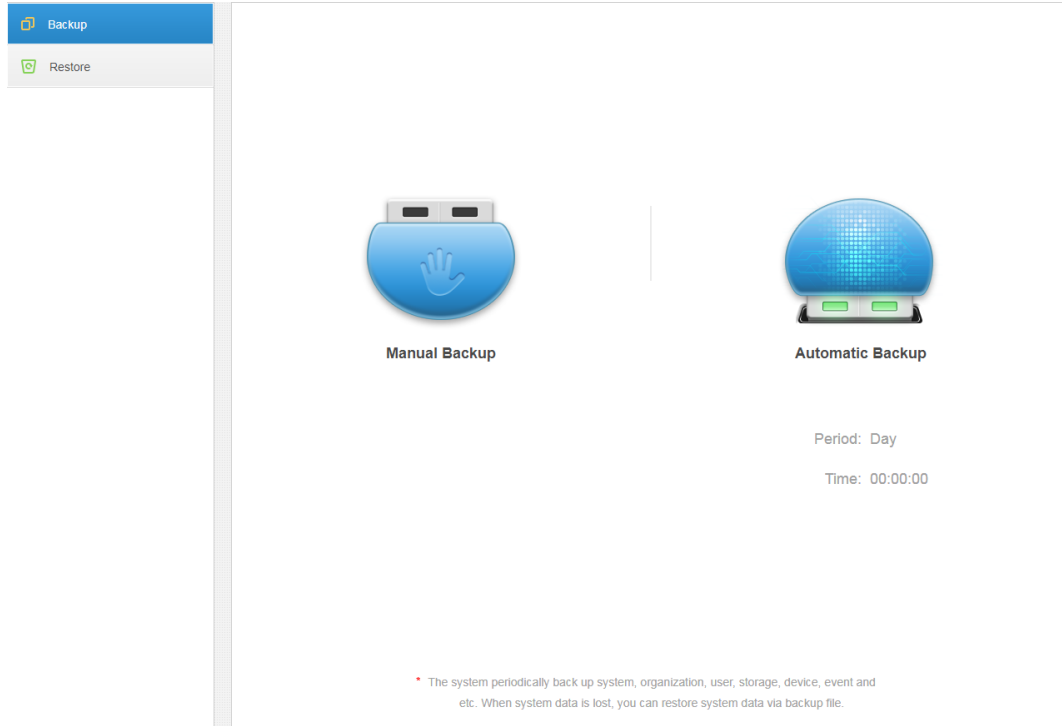
4.13.2.1 System Backup

In order to guarantee the security of user data, DSS platform system provides data backup function. The backup includes manual backup and automatic backup.

Manual Backup

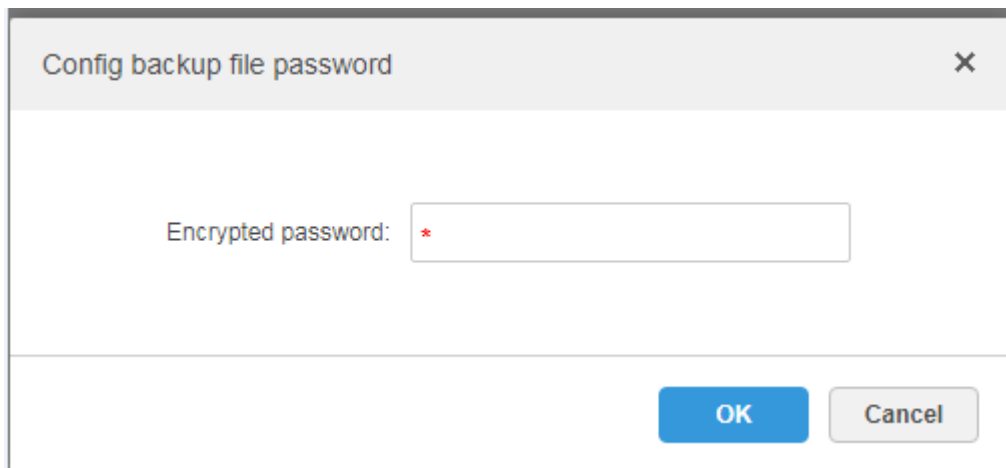
Step 1 Click  and select **Backup and Restore** on the **New Tab** interface.

Figure 4-99 Backup



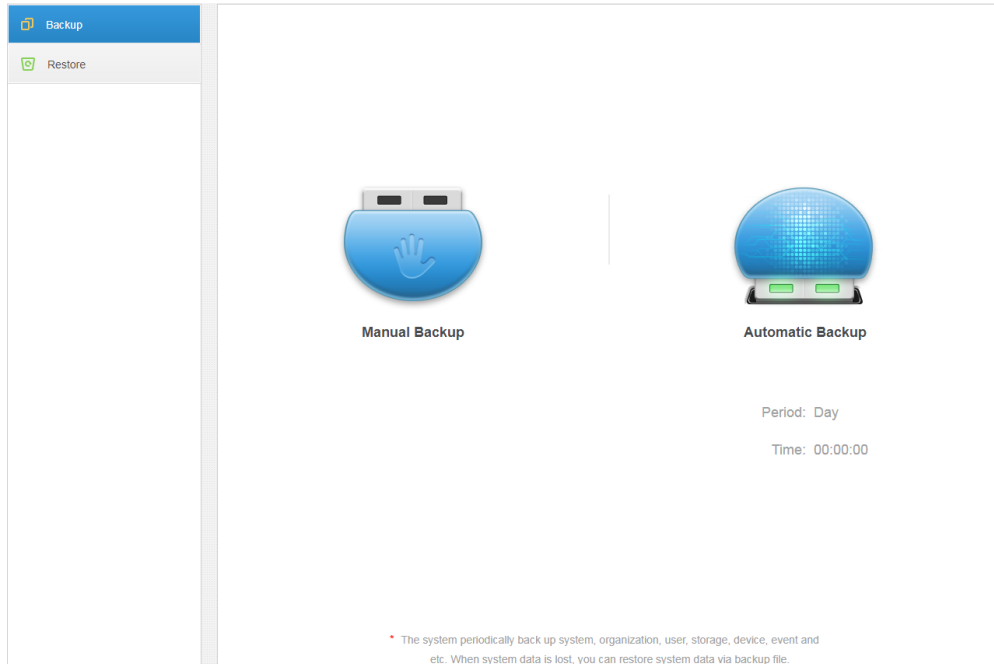
Step 2 Click **Manual Backup**.

Figure 4-100 Configure backup file password



Step 3 Enter encrypted password, click **OK**.

Figure 4-101 Backup

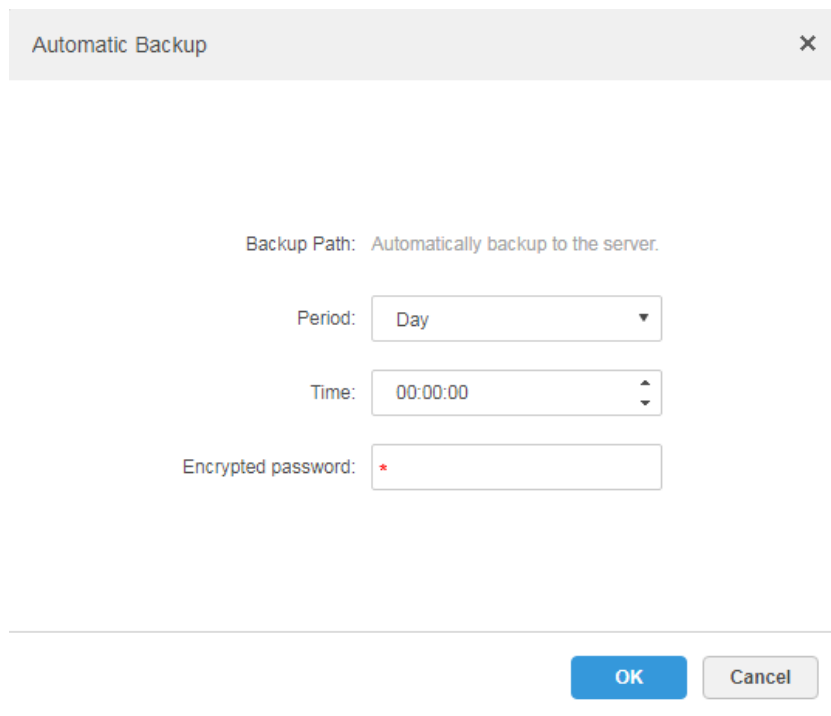


Automatic Backup

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

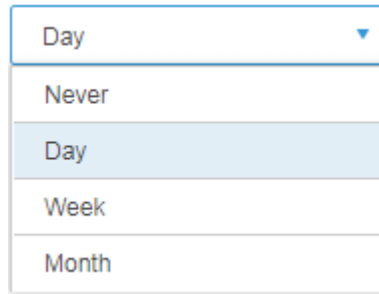
Step 2 Click Automatic Backup.

Figure 4-102 Automatic backup



Step 3 Select backup period, it includes: never, day, week, and month.

Figure 4-103 Backup period

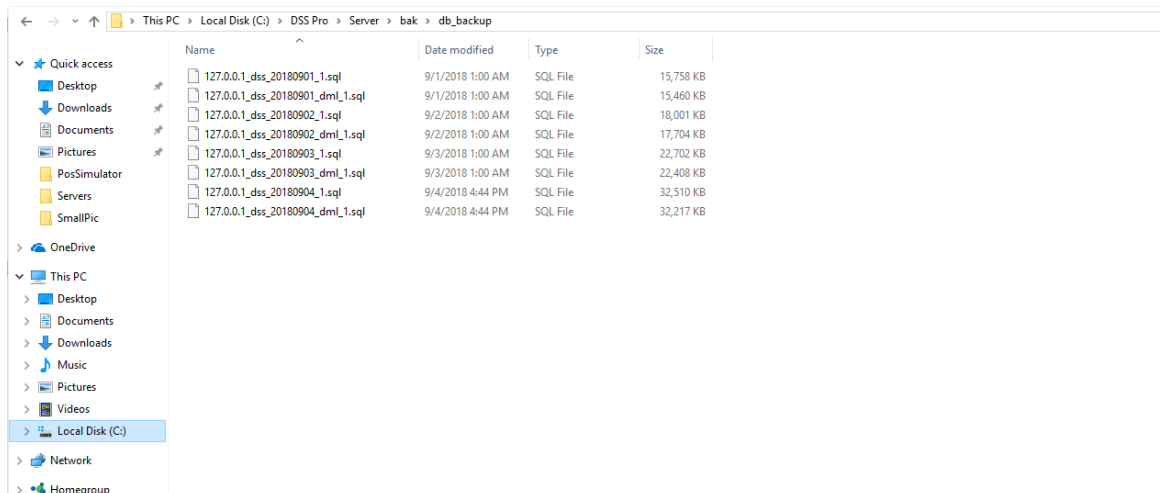


Step 4 Click **OK** to save configuration.

The system will automatically back up the file onto the server according to the period and time which have been set.

Step 5 Check the auto-backup file on the server, the default backup path is -Servers-bak-db_backup.

Figure 4-104 Backup path



4.13.2.2 System Restore

It can use system restore function to restore the data back the time point of the latest backup when the user database becomes abnormal. It can quickly restore the user's DSS system and lower user loss.



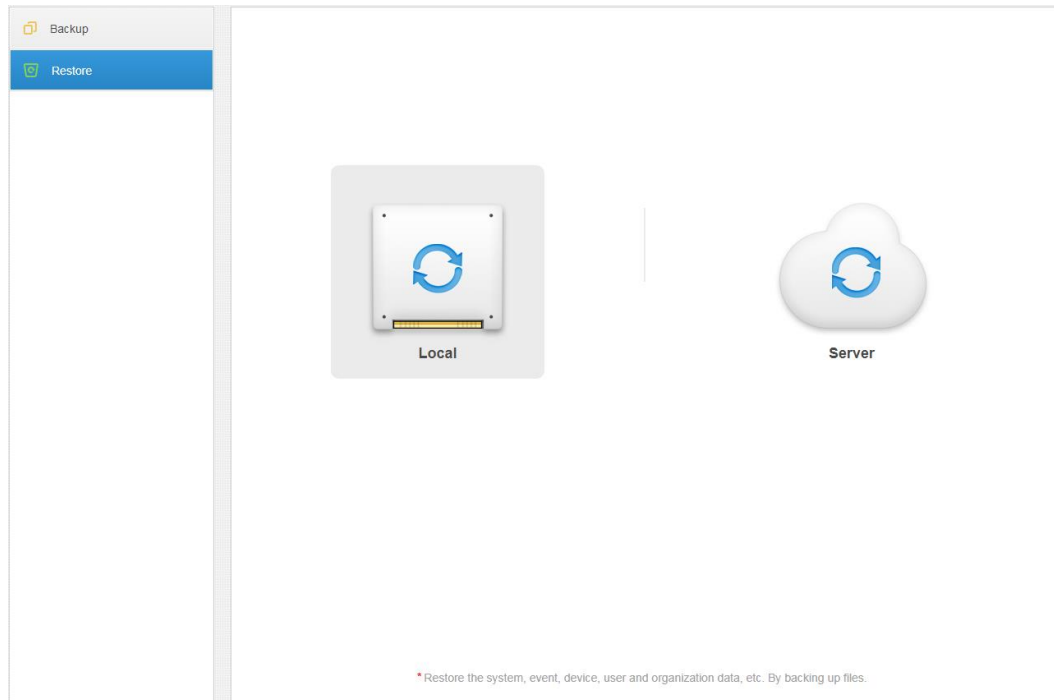
It needs to stop other users using DSS system when implementing system restore. Please be cautious when using the function because it may change data information.

Local

In general, local file restoration means restoring manual backup fills onto the server.

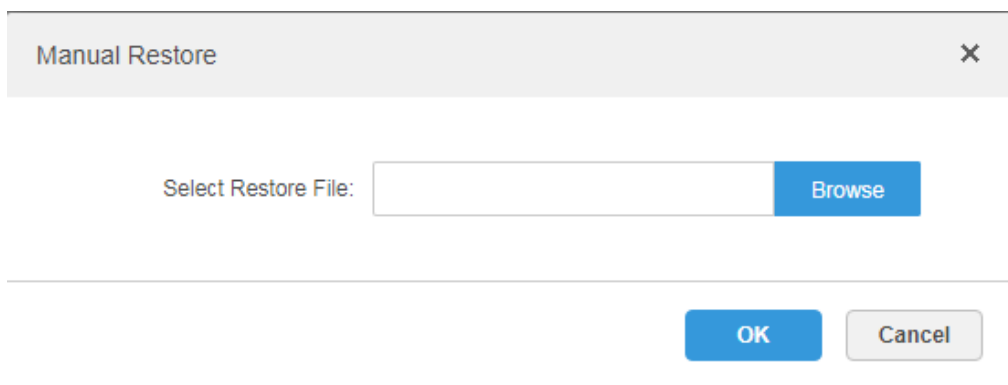
Step 1 Select **Restore** tab.

Figure 4-105 Restore



Step 2 Click **Local**.

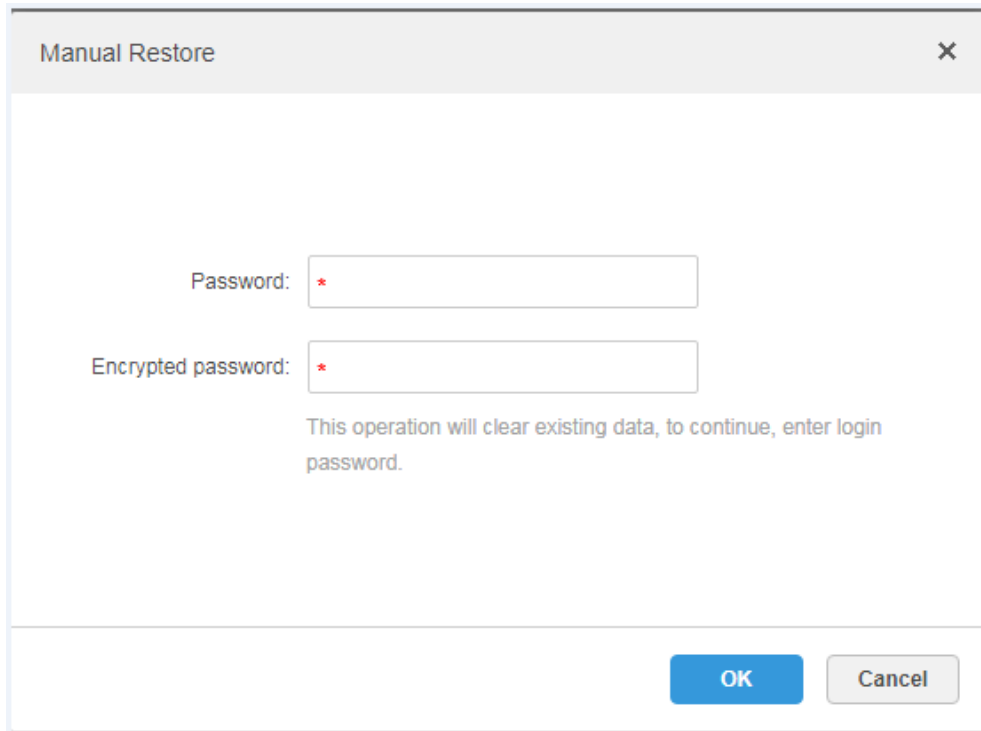
Figure 4-106 Manually restore (1)



Step 3 Click **Browse**, select file and then click **OK**.

Step 4 Enter administrator login **Password** and backup file **Encrypted Password**..

Figure 4-107 Manually restore (2)



The image shows a 'Manual Restore' dialog box with a title bar containing the text 'Manual Restore' and a close button (X). The main area contains two input fields: 'Password:' and 'Encrypted password:', each with a red asterisk indicating a required field. Below these fields is a message: 'This operation will clear existing data, to continue, enter login password.' At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (grey).

Step 5 Click **OK**.

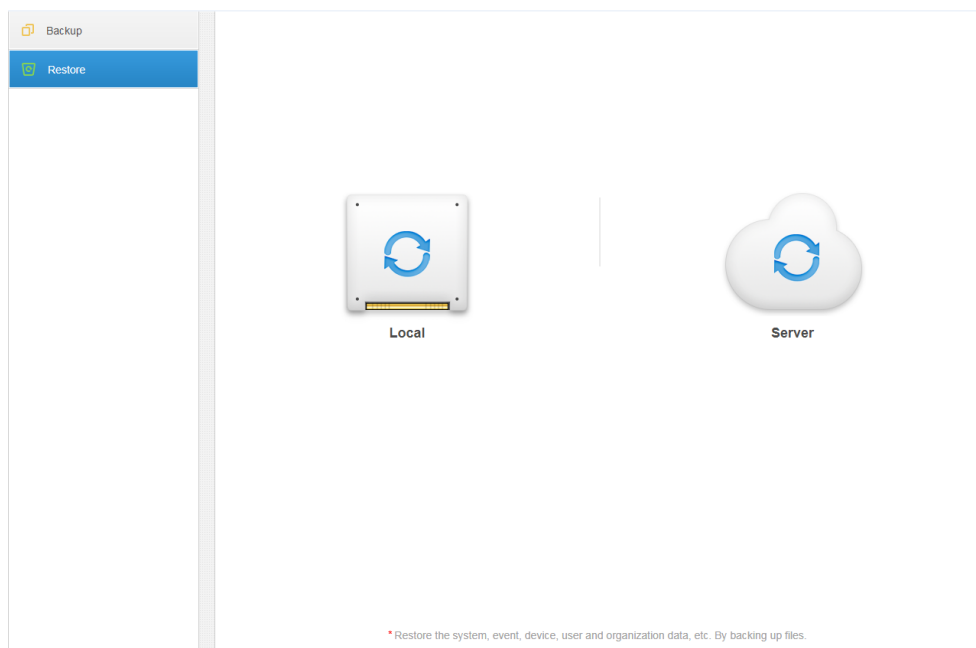
The data is being restored; it will display the restoration percentage via progress bar. The system will start again after it is completed.


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 4-108 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.

4.13.3 Log

The system supports inquiring management configuring log, client setting configuration and system log. It can filtrate type, select period and search via key word during query. It can inquire log export as well (it is PDF by default).

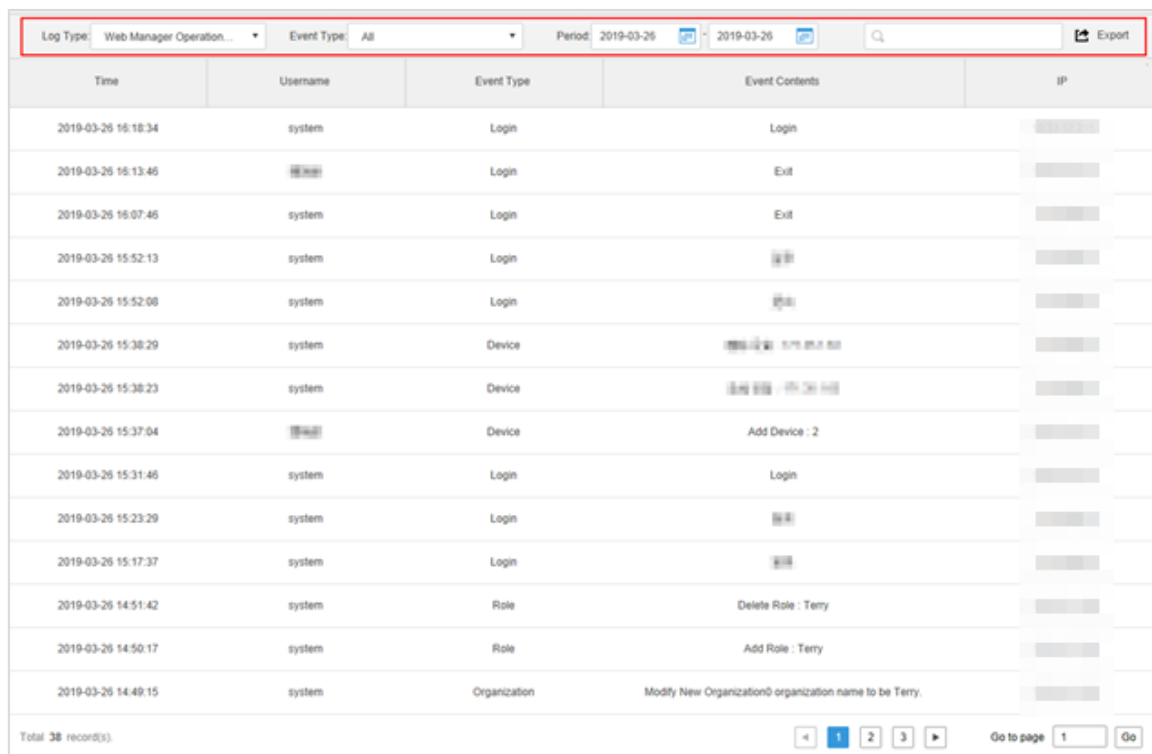
Take **Management Configuring Log** for an example.

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

Step 2 Select Log Type, Event Type or Query time.

The system displays query results; it will display the total records on the lower left corner.

Figure 4-109 Log



Time	Username	Event Type	Event Contents	IP
2019-03-26 16:18:34	system	Login	Login	
2019-03-26 16:13:46	system	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		
2019-03-26 15:38:23	system	Device		
2019-03-26 15:37:04	system	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)

Go to page 1 Go

Step 3 Click **Export** and export log information.

Step 4 Log exports results to check, the currently exported log package is displayed in the lower left corner of the browser, and you can also check it in the download section of your browser.

Step 5 Check log final record results.

Figure 4-110 Exported Log

Time	Username	Event Type	Event Contents	IP
2018-09-04 16:48:43	system	Preview	Request Main Stream video of IPC channel.	
2018-09-04 16:48:20	system	Preview	Request Main Stream video of IPC channel.	
2018-09-04 16:47:29	system	Preview	Request Main Stream video of IPC channel.	
2018-09-04 16:46:50	system	Preview	Request Main Stream video of IPC channel.	
2018-09-04 16:45:45	system	Preview	Request Main Stream video of IPC channel.	
2018-09-04 16:45:17	system	Preview	Request Main Stream video of IPC channel.	
2018-09-04 16:44:57	system	Preview	Request Main Stream video of	

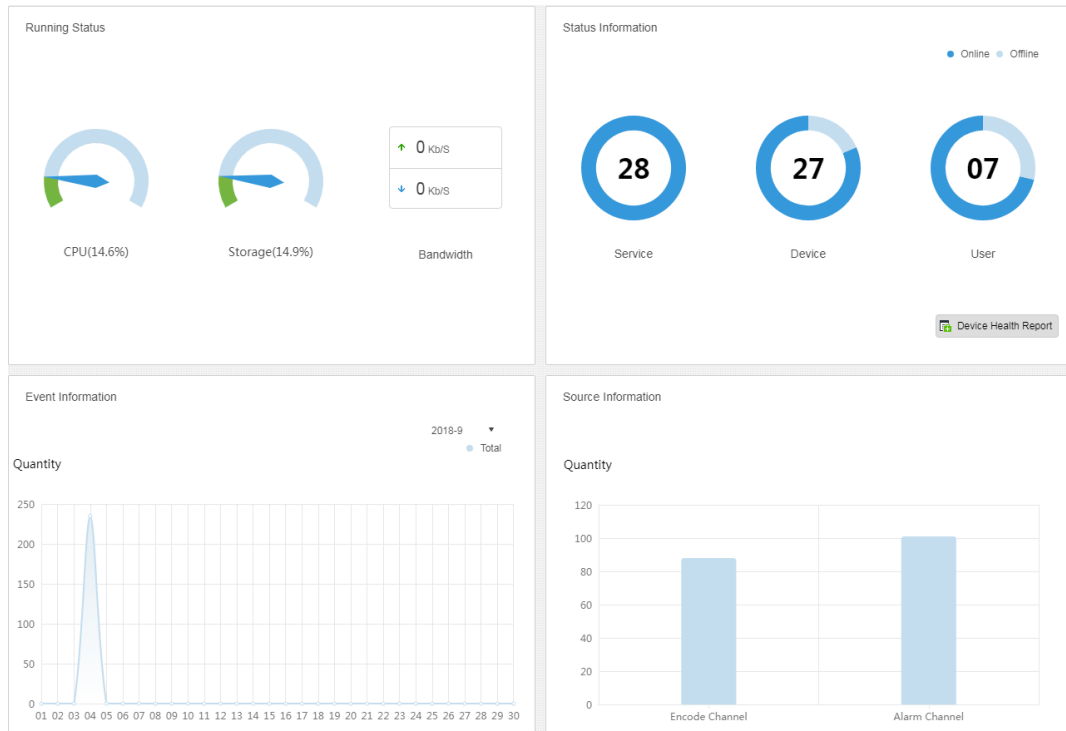
4.13.4 Overview

DSS platform supports function of inquiring system operation and maintenance statistics, which is to know the system running situation in time.

4.13.4.1 Overview

Click  and select **Overview** on the **New Tab** interface.

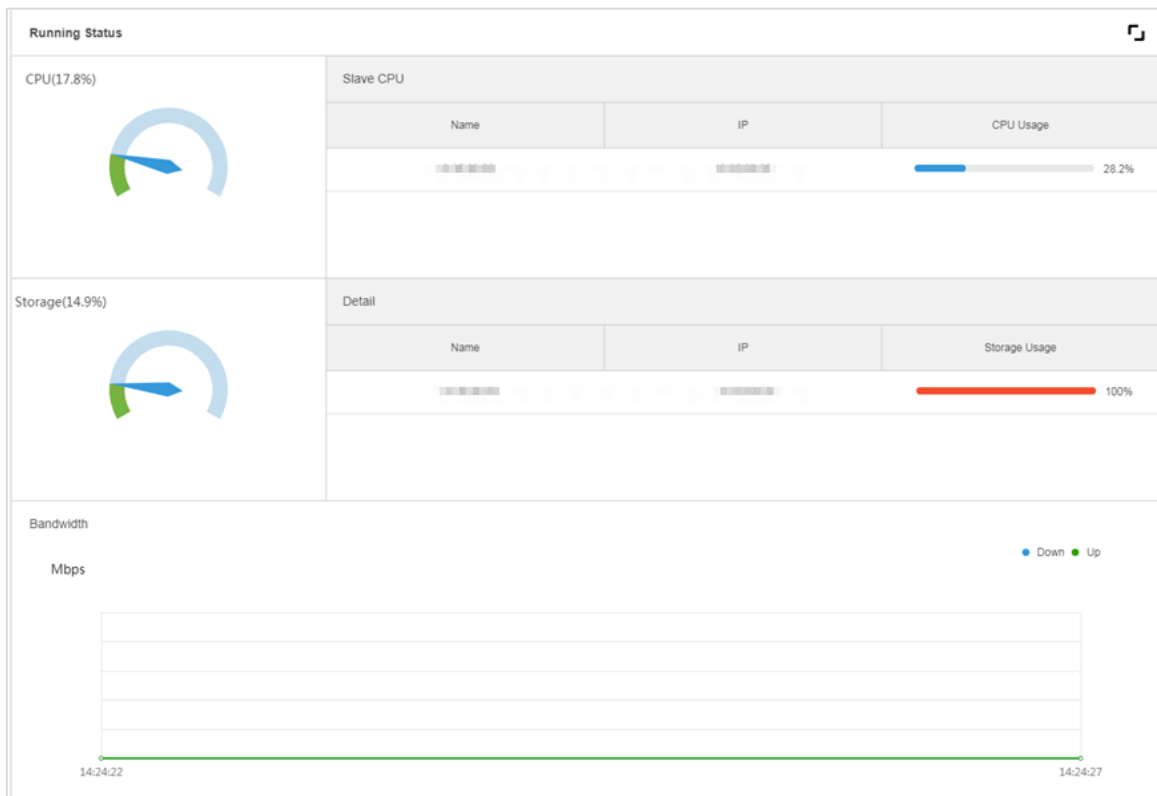
Figure 4-111 Overview



4.13.4.2 Running Status

Check CPU, storage, bandwidth and so on; click **Running Status** or the icon below and jump to the detail interface.

Figure 4-112 Running status



4.13.4.3 Status Information

Check server, device, user online/offline status statistics, click Status Information or the icon below to jump to the detailed interface.

Service Status Information


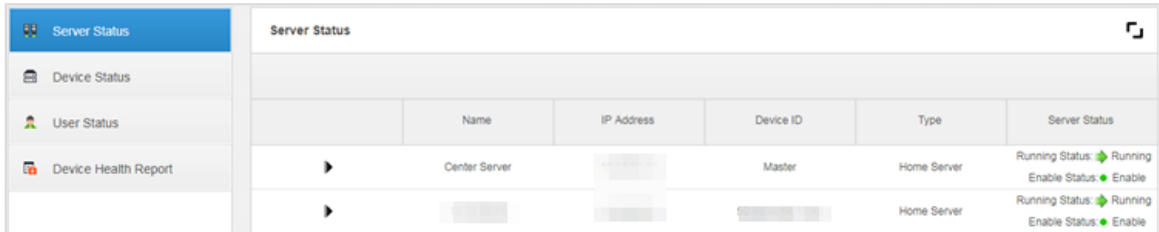
Click  on the Service Status interface, and then the interface displays service details.

Figure 4-113 Service status

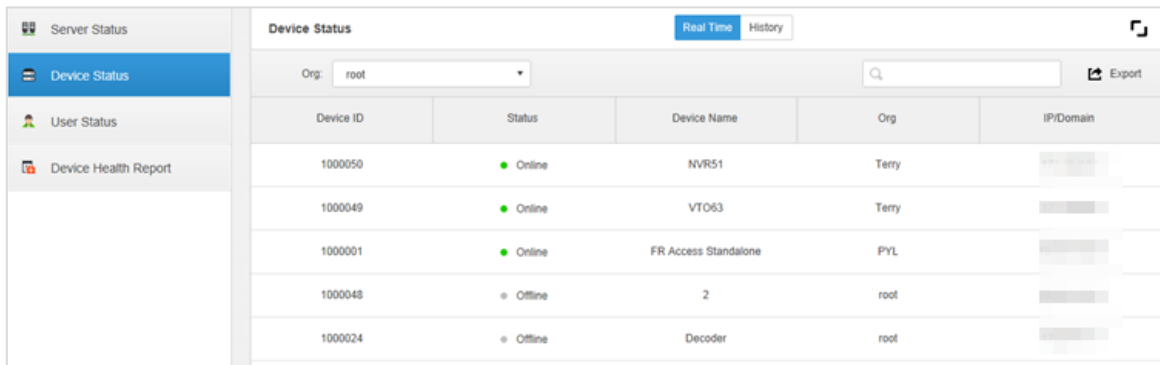


Name	IP Address	Device ID	Type	Server Status
Center Server		Master	Home Server	Running Status: Running Enable Status: Enable
			Home Server	Running Status: Running Enable Status: Enable

Device Status Information

Step 1 Click the tab of **Device Status**.

Figure 4-114 Real-time 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 2 Check device status.

- Click the **Real Time** tab on the device status information interface, check device real-time status information.
- Click the **History** tab on the device status information interface, check device history status information.

Figure 4-115 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 3 Click **Export**.

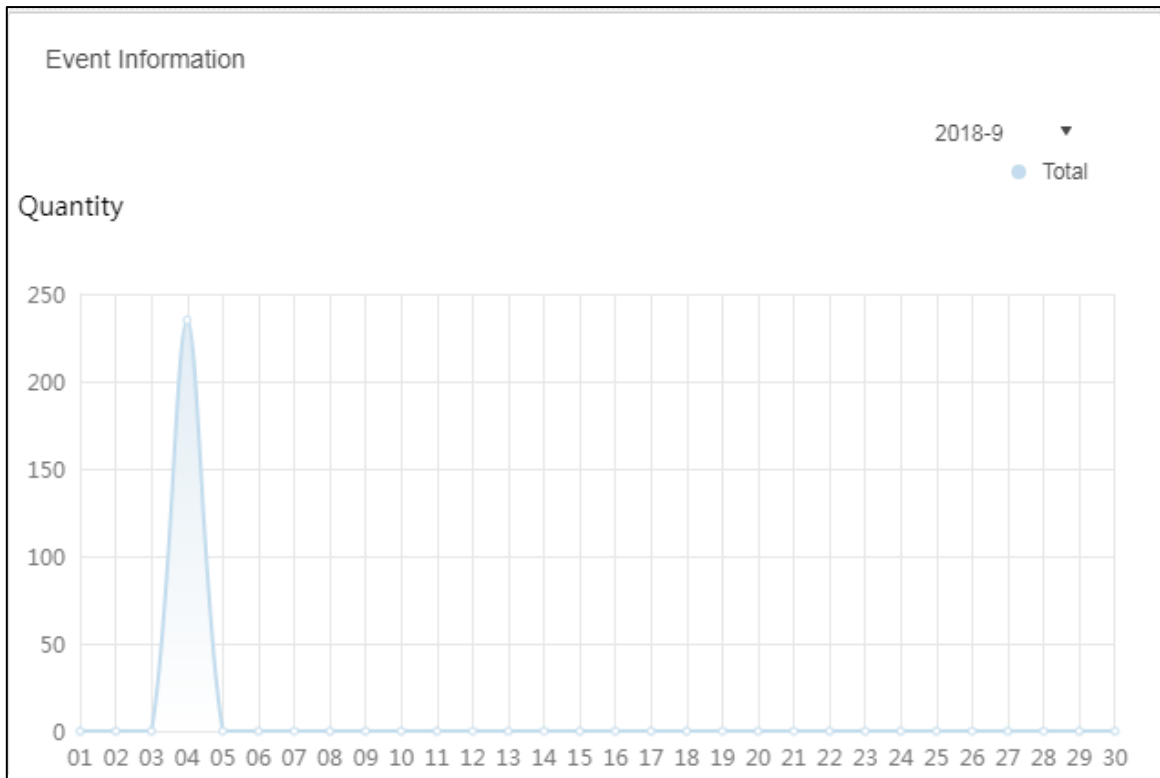
It exports device real-time status information (PDF format).

Step 4 Click **User State** and **Device Health Report** tabs to check corresponding details.

4.13.4.4 Event Information

Check total number of alarm events and processed events according to month.

Figure 4-116 Event information



4.13.4.5 Source Information

Check the statistics of encoding channel and alarm channel, click **Source Information** or the icon below to jump to the detailed interface.

- Check video channel details.

Figure 4-117 Video channel details

Name	Device	Org	SN	Camera Type
[Redacted]	[Redacted]	KL		Fixed Camera
[Redacted]	[Redacted]	ANPR		Fixed Camera
[Redacted]	[Redacted]	ANPR		Speed Dome
[Redacted]	[Redacted]	KL		Fixed Camera
37723_1	37723	ANPR		Speed Dome
Slot04-01	M70-E	TV WALL		Speed Dome
Slot04-02	M70-E	TV WALL		Speed Dome
Slot04-03	M70-E	TV WALL		Speed Dome
Slot04-04	M70-E	TV WALL		Speed Dome
Slot06-01	M70-E	TV WALL		Speed Dome
Slot06-02	M70-E	TV WALL		Speed Dome
Slot06-03	M70-E	TV WALL		Speed Dome
Slot06-04	M70-E	TV WALL		Speed Dome
[Redacted]	M70-E	TV WALL		Speed Dome

Total 89 record(s). [Page 1 of 7] Go to page 1 Go

- Click the **Alarm** tab to check the details of alarm channel.

5 Client Functions

Configure various functions and rules by DSS platform client and then display results. DSS platform client includes PC client and mobile phone APP. In this chapter, it takes DSS platform client (hereinafter referred to as client) as an example to introduce each function.

5.1 Client Installation and Login

5.1.1 PC Requirements

To install the DSS Client, the PC shall meet the following requirements.

Table 5-1 PC hardware requirements

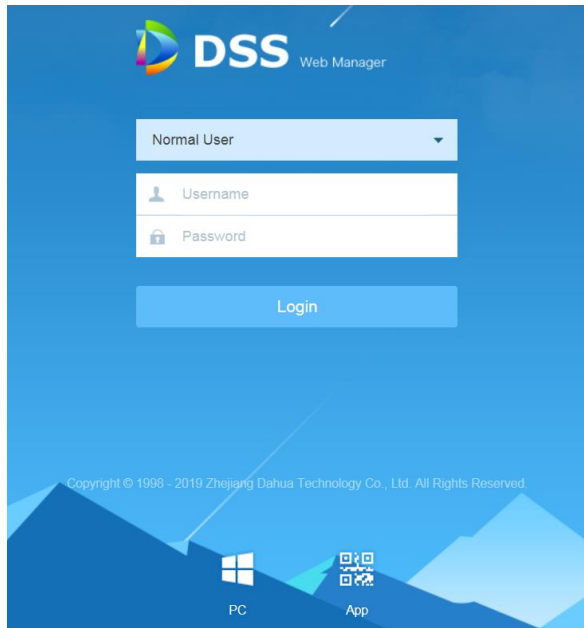
Parameters	Description
Recommended Configuration	<ul style="list-style-type: none">• CPU: i5-6500• Main frequency: 3.20GHz• Memory: 8 GB• Graphics: Inter HD Graphics 530• Network adapter:1 Gbps• HDD Type: HDD 1T• DSS client installation space:200 GB
Min. Configuration	<ul style="list-style-type: none">•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


5.1.2 Downloading and Installing Client

5.1.2.1 Installing PC Client

Step 1 Input IP address of DSS platform into the browser and then press **Enter**.

Figure 5-1 Log in to the web manager



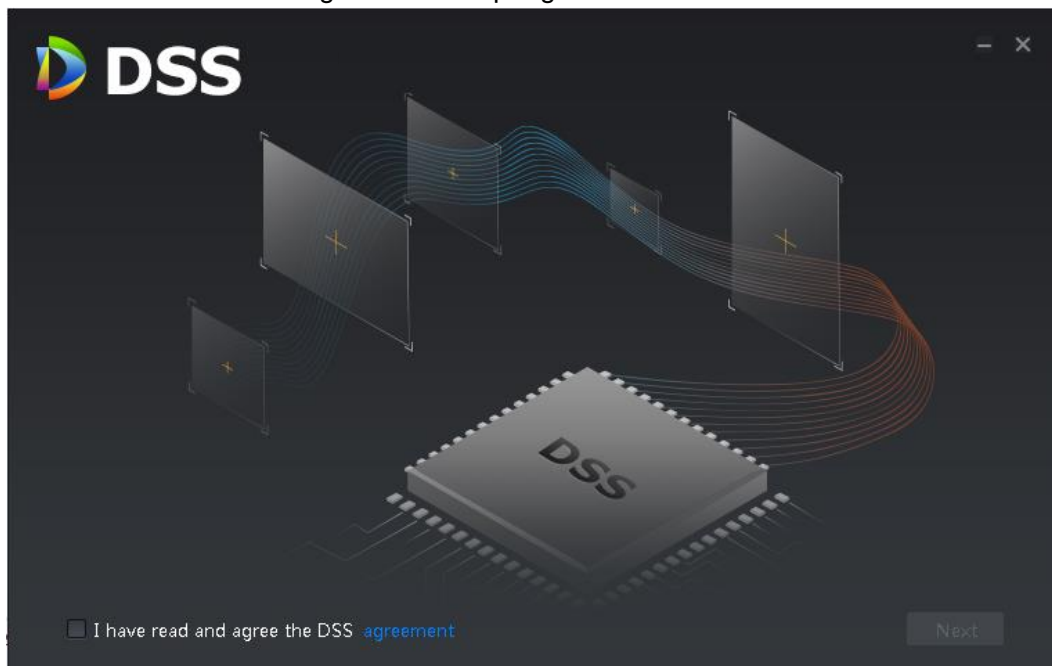
Step 2 Click  to download the client.

System pops up the **File Downloads** dialogue box.

Step 3 Click **Save** to download and save the DSS client software on the PC.

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

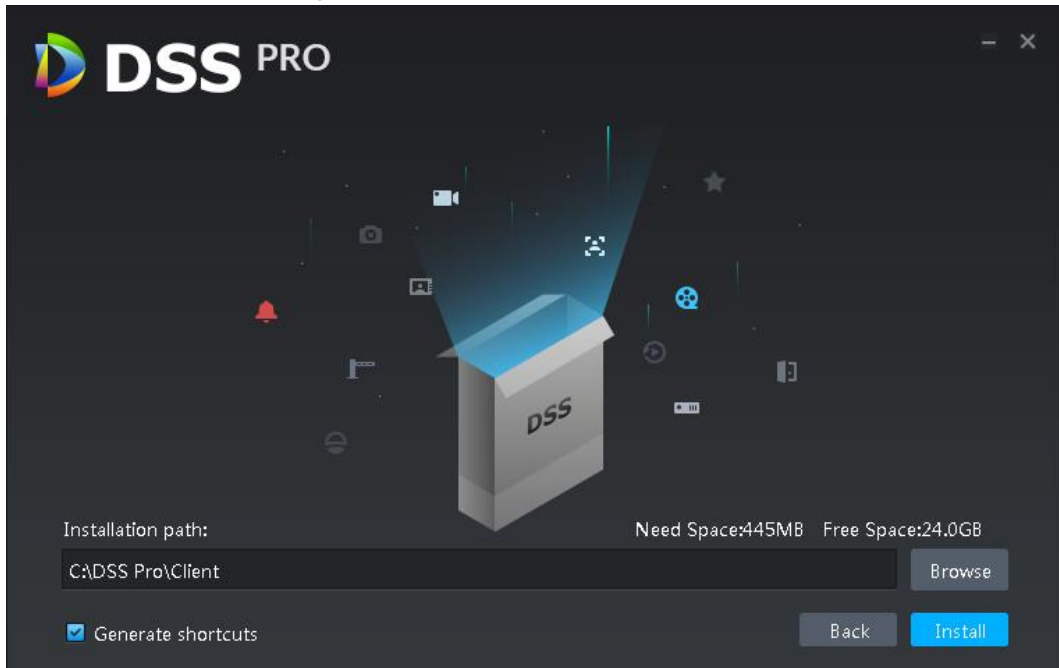
Figure 5-2 Accept agreement



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

Step 6 Select installation path.

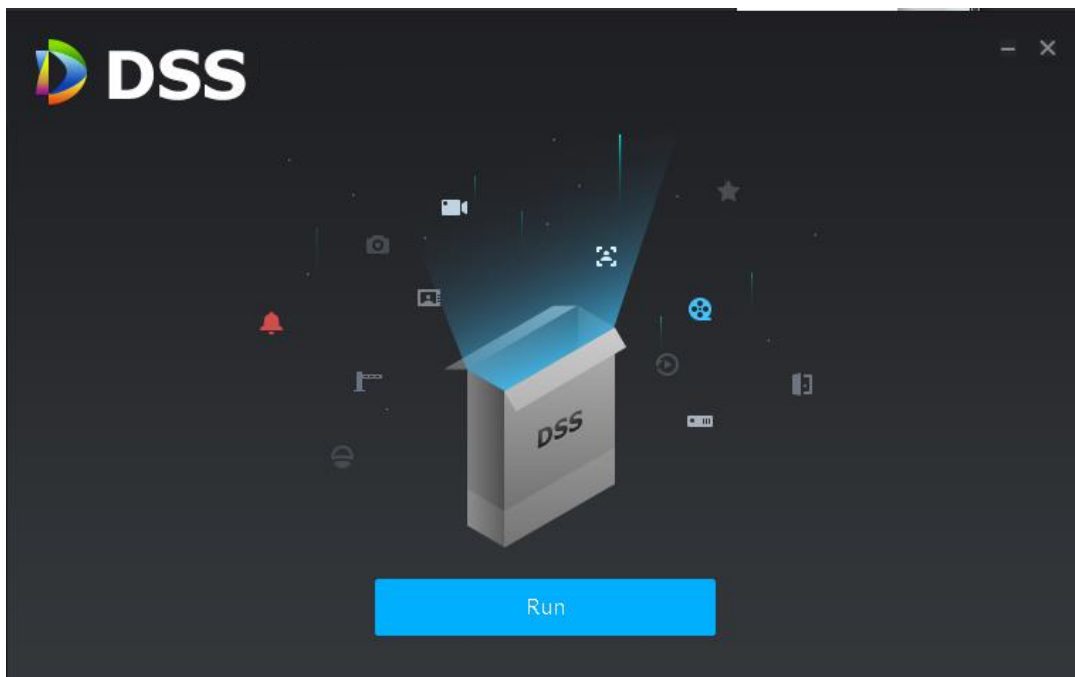
Figure 5-3 Set installation path



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

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

Figure 5-4 Installation completed



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

5.1.2.2 Mobile Phone App

Step 1 Input IP address of DSS platform into the browser and then press **Enter**.


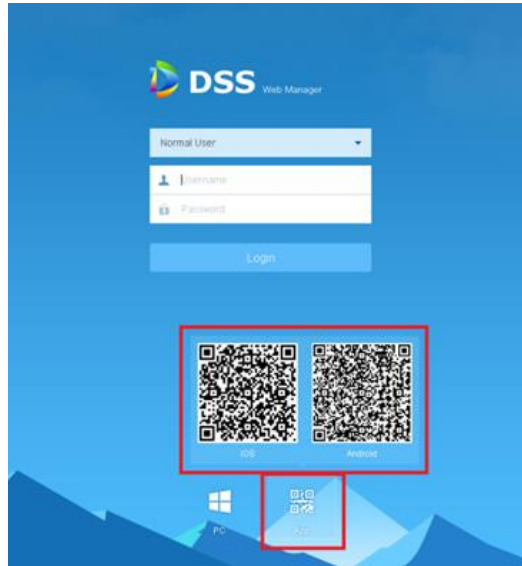
Step 2 Click  to view QR code of mobile phone APP. Currently it supports iOS and Android.

Figure 5-5 Download App by scanning QR code



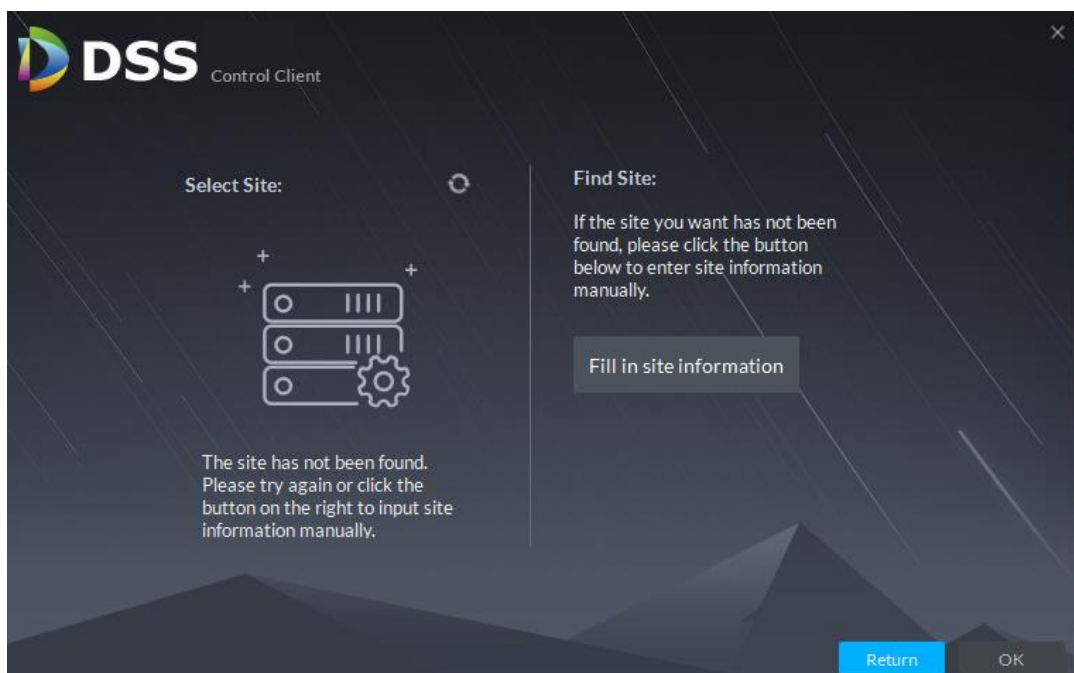
Step 3 Scan the QR code and then download the mobile phone App.

5.1.3 Logging in to Client

Step 1 Double-click DSS client icon on the desktop.

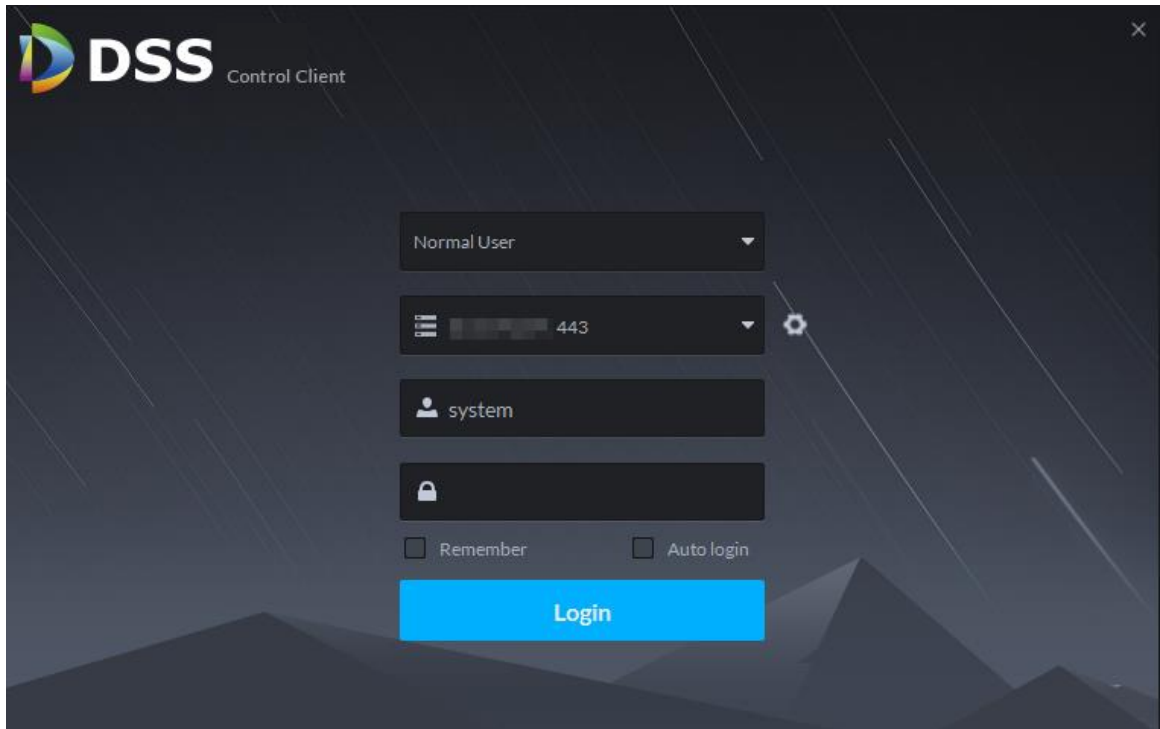
The first time you log in, the following interface is displayed, which proceeds to Step 2.

Figure 5-6 First-time login



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

Figure 5-7 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 platform server or PC, Port is 443 by default.
- Step 4** Click **Login**.

Figure 5-8 Homepage

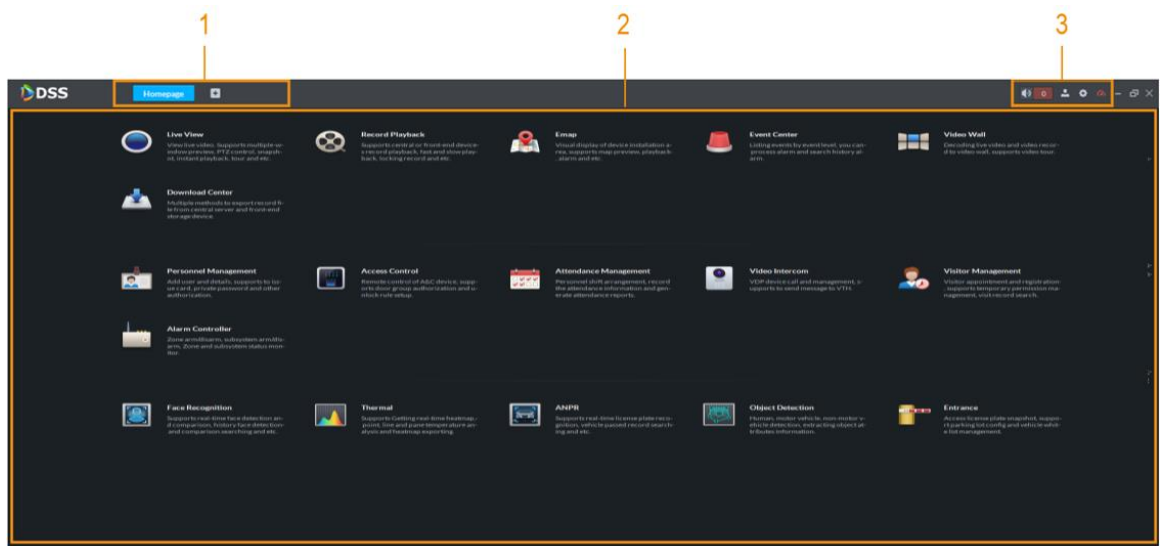








Table 5-2 Description

No.	Name	Function
1	Tab	Display all valid tabs. Click  and you can open the module you want.

No.	Name	Function
2	Applications	Go to each application by clicking the icon.
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, and alarm shortcut settings. Refer to "5.2 Local Configuration" for details. ● : View system status, including network status, CPU status, and memory status.

5.2 Local Configuration

After logging into the client for the first time, you need to configure the system parameters. It includes General, Video, Playback, Snapshot, Record, Alarm and the Shortcut Key.


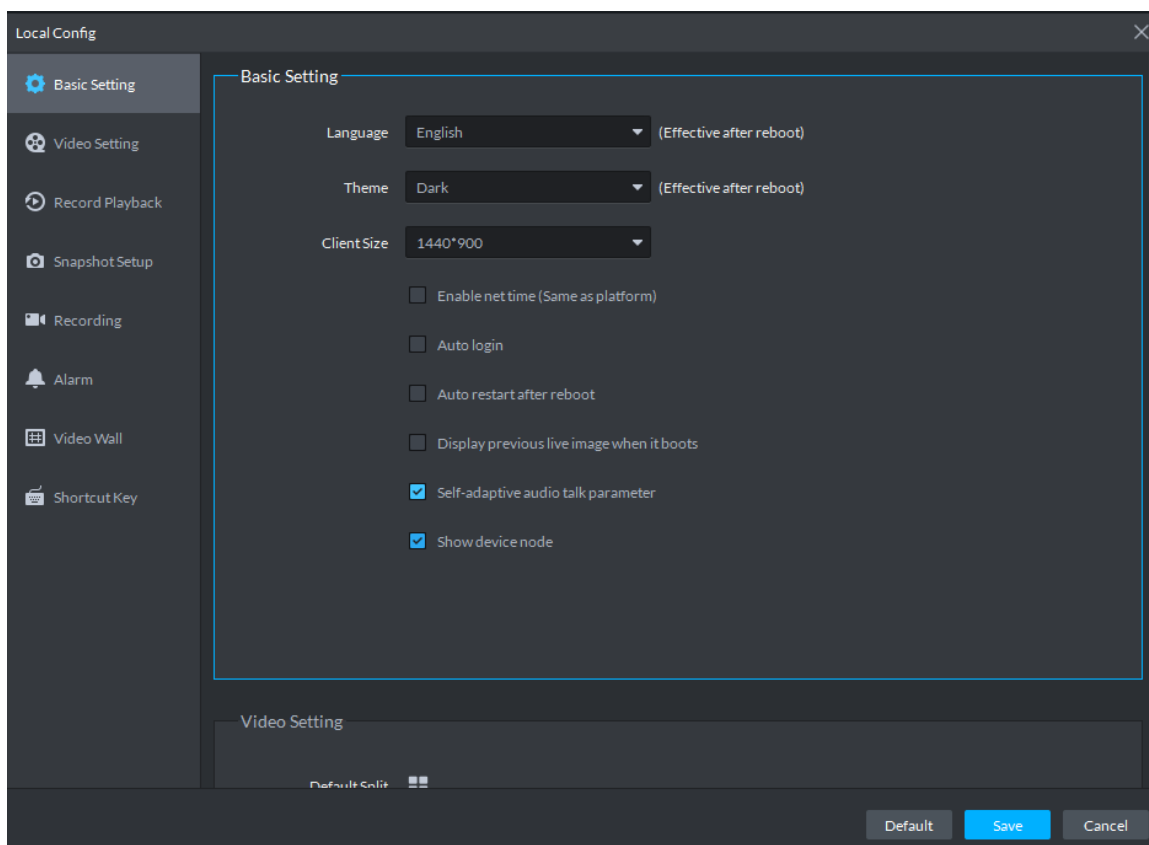
Step 1 Click  at the upper-right corner on the homepage.

Figure 5-9 Local configurations



Step 2 Click **Video Setting** and set relevant parameters.

Table 5-3 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	It is to set client display size.
Enable net time	If checked, the client starts to synchronize network time with the server. It is to complete time synchronization.
Auto Login	If checked, auto login is allowed when Client starts running.
Auto Reboot	If checked, auto reboot of the Client is allowed when the PC power is on.
Display Previous live Image when it boots	If checked, system displays the last Live video automatically after rebooting the client.

Parameters	Description
Self-adaptive Audio Talk Parameter	If checked, the system will adapt to Sampling Frequency, Sampling Bit, and Audio Format to the device automatically during audio talk.
Show Device Node	Check the box, system displays device node.

Step 3 Click **Video Setting** to set parameters.

Table 5-4 Configure video settings

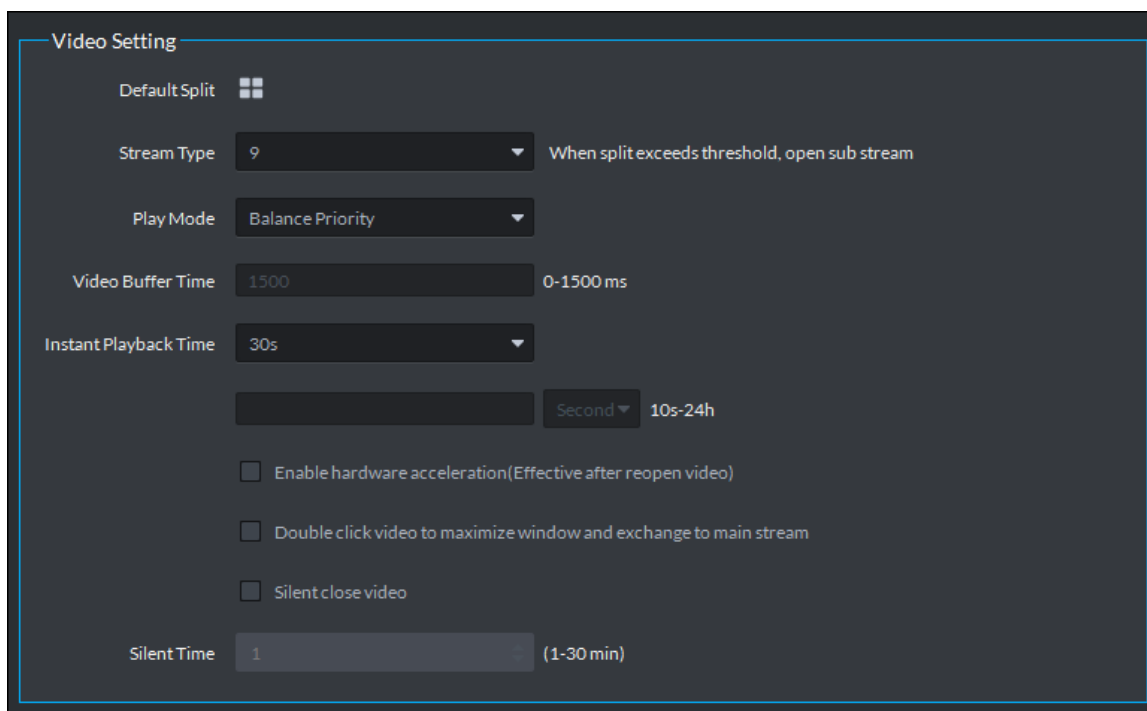


Table 5-5 Parameters

Parameters	Description
Default Split	Set split mode of the video window.
Stream type	Defines bit stream type for video transmission. With main bit stream as default, the auxiliary bit stream will be used when number of window splits is greater than the value selected here.
Play Mode	Play mode to be selected as required, including Real Time Priority, Fluency Priority, Balance Priority, as well as user-defined modes.
Video buffer time	Set video buffer time. It is only valid when play mode is customized.
Instant playback time	Select instant playback time and then click Instant playback on the Live view interface, you can view the record of current

Parameters	Description
	period.
Enable hardware acceleration (effective after reopen the video)	Check the box to enable the function. It is to use hardware module to enhance acceleration features.
Double-click video to maximize window and exchange to main stream	Check the box to enable the function.
Slilent close video	After being enabled, if the time of no operation for the Live interface exceeds the set value, the system will close Live automatically.

Step 4 Click **Record Playback** to set parameters.

Figure 5-10 Configure record playback settings

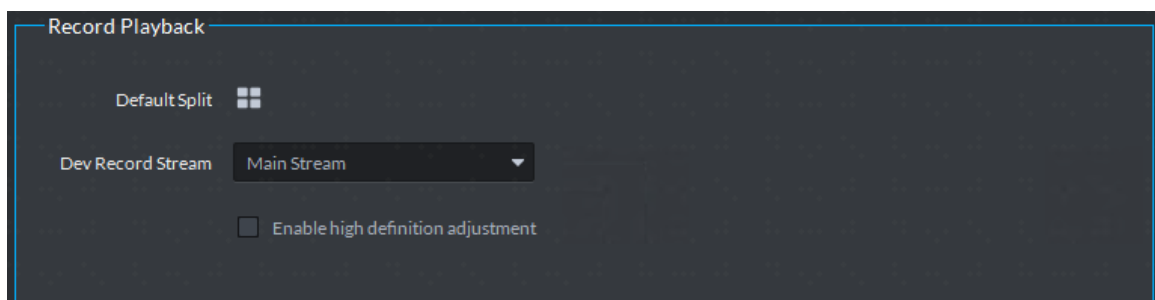


Table 5-6 Parameters

Parameters	Description
Default Split	Set default split mode of the playback window.
Device record stream	It is to select record playback bit stream.
Enable high definition adjustment	Check the box to enable the function. In high definition, big bit stream playback mode, system reserves I frames only to guarantee video fluency and reduce high decoding pressure.

Step 5 Click **Snapshot Setup** to set parameters.

Figure 5-11 Configure snapshot settings

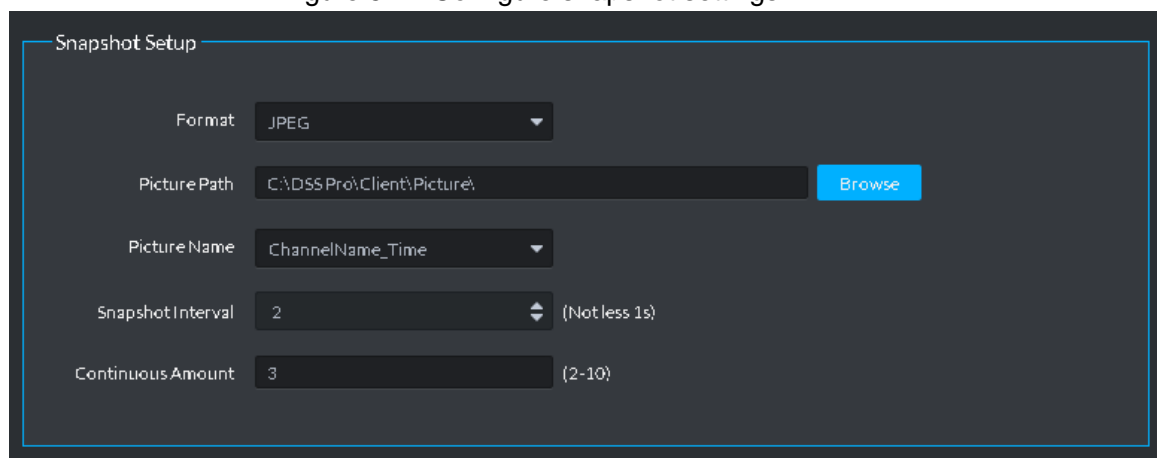


Table 5-7 parameters

Parameters	Description
Format	It is to set snapshot image format.

Parameters	Description
Picture path	It is to set snapshot storage path. The default path: C:\DSS platform\Client\Picture\.
Picture name	It is to select picture name rule.
Snapshot interval	It is to set snapshot interval. System snapshot once after the specified period.
Continuous amount	It is to snapshot amount at each time.

Step 6 Click **Recording** to set parameters.

Figure 5-12 Configure recording settings

The screenshot shows the 'Recording' configuration window. It contains three main settings:

- Record Path:** A text input field containing 'C:\DSS Pro\Client\Record\' with a 'Browse' button to its right.
- Record Name:** A dropdown menu currently showing 'ChannelName_Time'.
- Max Size of Record:** A text input field containing '1024' with '(10-1500M)' in smaller text to its right.

Table 5-8 Parameters

Parameters	Description
Record path	It is to set record storage path. The default path: C:\DSS platform\Client\Record\.
Record name	It is to set record file name rule.
Max. record size	It is to set record file size.

Step 7 Click **Alarm** to set parameters.



Figure 5-13 Configure alarm settings

The screenshot shows the 'Alarm' configuration window. It includes several settings:

- Play alarm sound:** A checked checkbox.
- Loop:** A checked checkbox.
- Alarm Type:** A dropdown menu set to 'Video Loss'.
- Sound Path:** A text input field containing '.\Sound\sound_en\video lost.wav' with 'Browse' and 'Play' buttons.
- Map flashes when alarm occurred:** A checked checkbox.
- Alarm Type (second):** A dropdown menu set to 'Video Loss'.
- Display alarm link video when alarm occurred:** A checked checkbox.
- Video Opening Type:** Radio buttons for 'Pop Up' (selected) and 'In Preview'.

Table 5-9 Parameters

Parameters	Description
Play alarm sound	Check the box, system generates a sound when an alarm occurs.
Loop	Check the box; system plays alarm sound repeatedly when an alarm occurs.

Parameters	Description
	 <p>This item is only valid when Play alarm sound function is enabled.</p>
Alarm Type	<p>It is to set alarm type. System can play sound when corresponding alarm occurs.</p>  <p>This item is only valid when Play alarm sound function is enabled.</p>
Sound Path	It is to select alarm audio file path.
Map flashes when alarm occurred	Check the box and then select alarm type. When the corresponding alarm occurs, the device on the emap can flash.
Display alarm link video when alarm occurred	Check the box, system automatically opens linkage video when an alarm occurs.
Video opening type	System automatically opens linkage video when an alarm occurs. You can view on the pop-up window or on the preview interface.

Step 8 Click **Video Wall** to set parameters.

Figure 5-14 Configure video wall settings

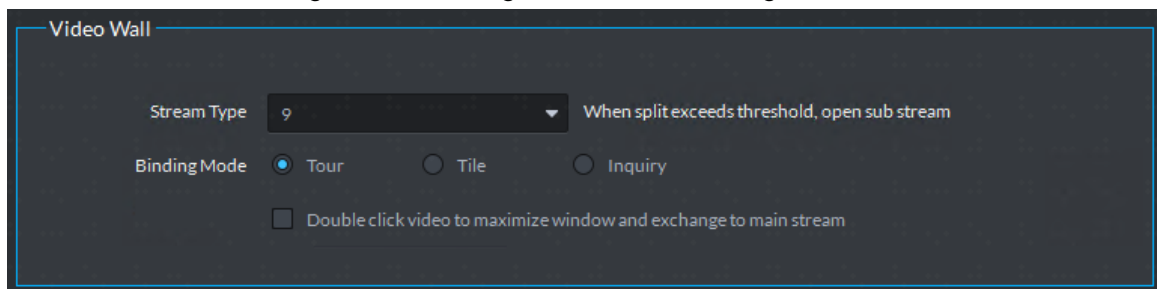


Table 5-10 Parameters

Parameters	Description
Stream type	When split exceeds threshold, open substream.
Binding mode	<ul style="list-style-type: none"> ● Tour: Device nodes are displayed on 1 window by tour. ● Tile: Device nodes are displayed on windows of current screen by tile. ● Inquiry: When dragging the device nodes to the window, the systems prompts whether tour or tile.
Double-click video to maximize window and exchange to main stream	Double-click the video screen to maximize the window, and the stream change to main stream.

Step 9 Click **Shortcut Key** to set parameters.

Figure 5-15 Configure shortcut keys

Shortcut Key

Keyboard Type Joystick USB NKB PC Keyboard

Function	Shortcut Key	Function	Shortcut Key
Move Window Up	Up	Lock Client	Ctrl+L
Move Window Down	Down	Snap Single Window	P
Move Window Left	Left	One-click Snapshot	Ctrl+P
Move Window Right	Right	Local Record	Ctrl+R
Aperture-	Insert	Preset 1	1
Aperture+	Delete	Preset 2	2
Focus-	Home	Preset 3	3
Focus+	End	Preset 4	4
Zoom-	PgUp	Preset 5	5
Zoom+	PgDn	Preset 6	6
Open Single Window	Enter	Preset 7	7
Close Single Window	Enter	Preset 8	8
Open Full Screen	Ctrl+F	Preset 9	9
Exit Full Screen	Esc	Preset 10	0

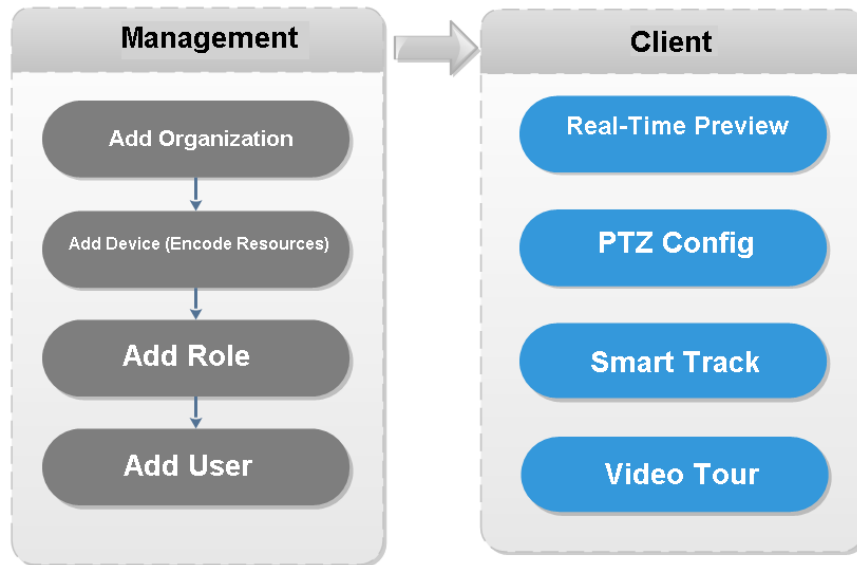
Step 10 Click **Save**.

5.3 Live Video

5.3.1 Preparations

Before the operation, refer to "4.5 Adding Device" to add devices on the manager.
Refer to Figure 5-16 for live view flows information.

Figure 5-16 Live view business flow



5.3.2 Live View

5.3.2.1 Live Video View

Step 1 Click **+**. On the **New Tab** interface, select **Live View**. The **Live view** interface is displayed.

Step 2 View real-time video.

- Select channel from the device list on the left side of the **Live View** interface.
- Double-click or drag it to the video window. If you double-click the device, then all channels of the device will be opened.
- Select the preview window(s) on the right side of interface.
- On the device list, right-click to select **Tour**, and you can choose the time. The system will play (in loops) videos of all channels for selected devices within the set time, which is the play time.

Real-time monitoring interface is displayed in the video window. See Figure 5-17. Refer to Table 5-11 to set parameters.

Figure 5-17 Live view

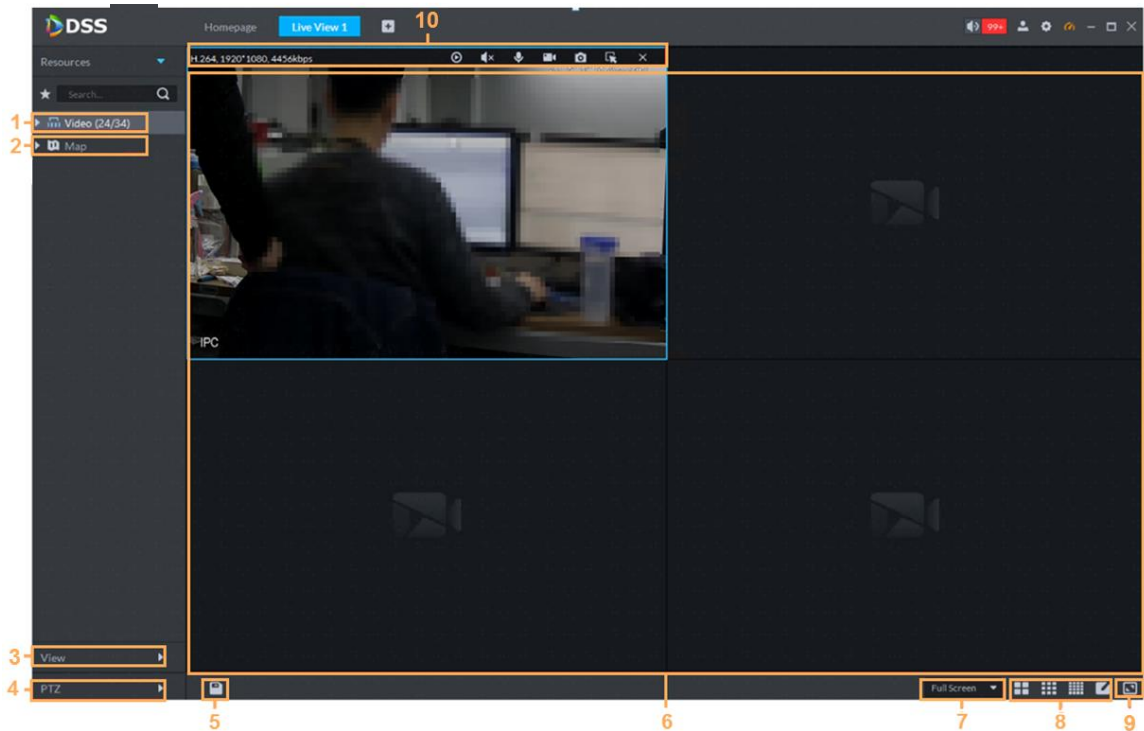






Table 5-11 Description

No.	Name	Function
1	Favorites and Device Tree Search	<ul style="list-style-type: none"> From Local Config > General, if you enable Show device node, device tree displays all channels of current device. If you cancel the box, system display all channels of all device. Search is supported by input device name or channel name in <input type="text" value="Search.."/> here. : Add, Delete or Rename Favorite. Favorite Tour supported.
2	Map Resource	Map can be opened in preview window, both GIS map and Raster map.
3	View	Live video window can be saved as View. Three-level directory is adopted for view, with level one as root node, level two for group and level three for view. Video Tour is supported from root node and group node, with tour intervals selected from 10s, 30s, 1min, 2min, 5min and 10min. Maximum of 100 views can be created.
4	PTZ	More information about PTZ of PTZ camera, refer to "5.3.4 PTZ."
5	Save view	Click  to save current video window as a view.
6	Video play	Displays real-time video play. Put the mouse on the video play window, and you can scroll forward to zoom in and backward

No.	Name	Function
		to zoom out.
7	Display mode	Aspect ratio of the video window, selected from two modes for video play: actual scale and fit in window.
8	Window Split Mode	Select from modes among 1 to 64 to set window split mode, or click  to define split mode.  If the real-time channel is more than the number of windows, then you can turn page(s) at the bottom-middle side of the interface.
9	Full Screen	Switch the video window to full screen mode. To exit full screen, press the Esc key, or right-click to select exit full screen.
10	Bit Stream and Quick Start	Quick operations. Refer to "5.3.2.3 Window Shortcut Menu" for detailed information.

5.3.2.2 Right-click Shortcut Menu

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



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

Figure 5-18 Live video operation menu

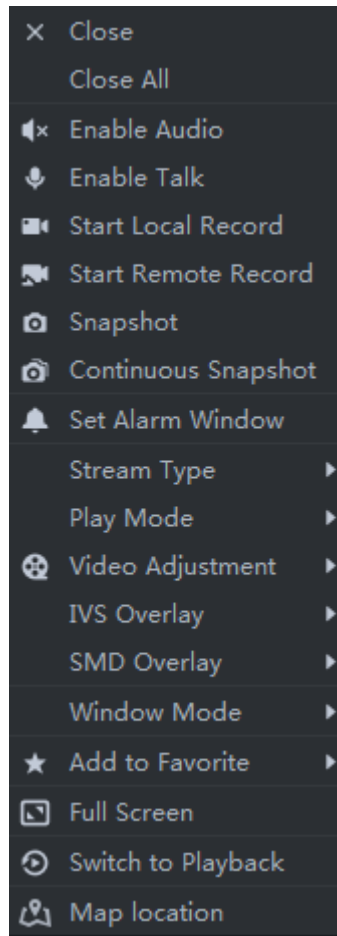










Table 5-12 Description

Parameters	Description
Close	Close active video window.
Close All	Close all video windows.
Enable Audio	Same as  , to enable or disable camera audio.
Enable Talk	Same as  , to enable or disable audio talk of corresponding device. Check 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.  Support audio talk with NVR. Right-click an NVR in the device tree and then select Audio Talk to start talking.
Start Local Record	Same as  , to record audio/video of the active video window and save them in local PC.
Start Remote Record	Click to start remote record. The item becomes Stop remote record. Click Stop remote record, system stops record. If the platform has configured video storage HDD, the record file is saved on the platform server.
Snapshot	Same as  , to save image of the active video window as picture (one picture for each snapshot).
Continuous	To save image of the active video window as picture (three snapshots

Parameters	Description
Snapshot	each time by default).
Set Alarm Window	Set the current window as the alarm window. Alarm videos are displayed on this window when alarms are triggered. An alarm window is marked with a red frame.
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 custom defined mode.
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 only effective to the current selected channel.
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 only effective to the current selected channel.
Open crowd density map	 This function is only available for multisensor panoramic camera + PTZ camera. 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.
Installation mode	 For fisheye camera only. The installation mode has three types:ceiling mount, wall mount and ground mount. Select corresponding installation mode according to the actual situation, the real-time video can automatically dewarp according to the installation mode.
Fisheye view mode	 For fisheye camera only. When changing the video stream, the fisheye view mode keeps the configuration before the stream is changed. It refers to current video display mode (system supports original video mode by default.). System supports following display modes according to different installation mode. <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.
Split mode	It supports standard mode, 1+3 mode, 1+5 mode.
Alarm output control	Turn on/off alarm output.

Parameters	Description
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	You can switch between live view interface and playback interface quickly, without going back to homepage first.
Map location	After enabling map location, a map that centers on the device will be displayed.

5.3.2.3 Window Shortcut Menu

Move the mouse to the video window, you can see the shortcut menu at the upper right

Figure 5-19 Shortcut menu

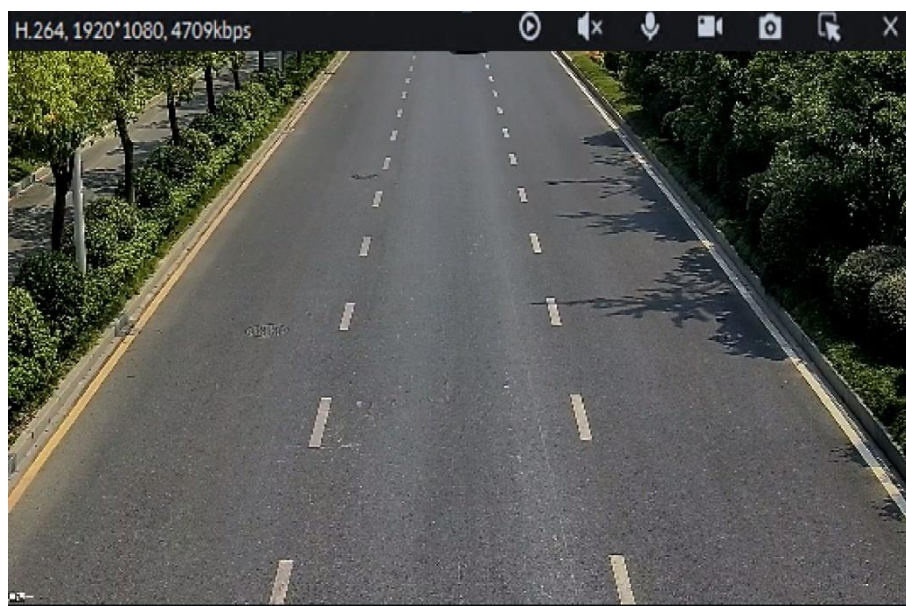


Table 5-13 Description

Icon	Name	Description
	Instant playback	Open/close instant playback. Go to Local config>General to set instant playback time. Make sure there is a record on the platform or the device.
	Audio	Open/close audio.
	Audio talk	Open/close bidirectional talk.
	Local record	Click it, system begins record local file and you can view the record time at the upper left. Click again, 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.

5.3.3 Device Configuration

Configure the camera properties, video stream, snapshot, video overlay, and audio configuration for the device channel on the platform.



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

5.3.3.1 Configuring Camera Properties

Support configuring the property files in the modes of **Daytime**, **Night**, and **Regular**. The system switches between different modes based on the preset time to ensure image quality collected by the camera.

5.3.3.1.1 Configuring Property Files

Step 1 On the **Live View** interface, right-click the video device and select **Device Config**.



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

Figure 5-20 Select Device Config

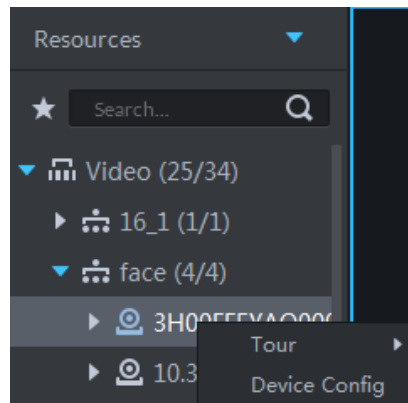
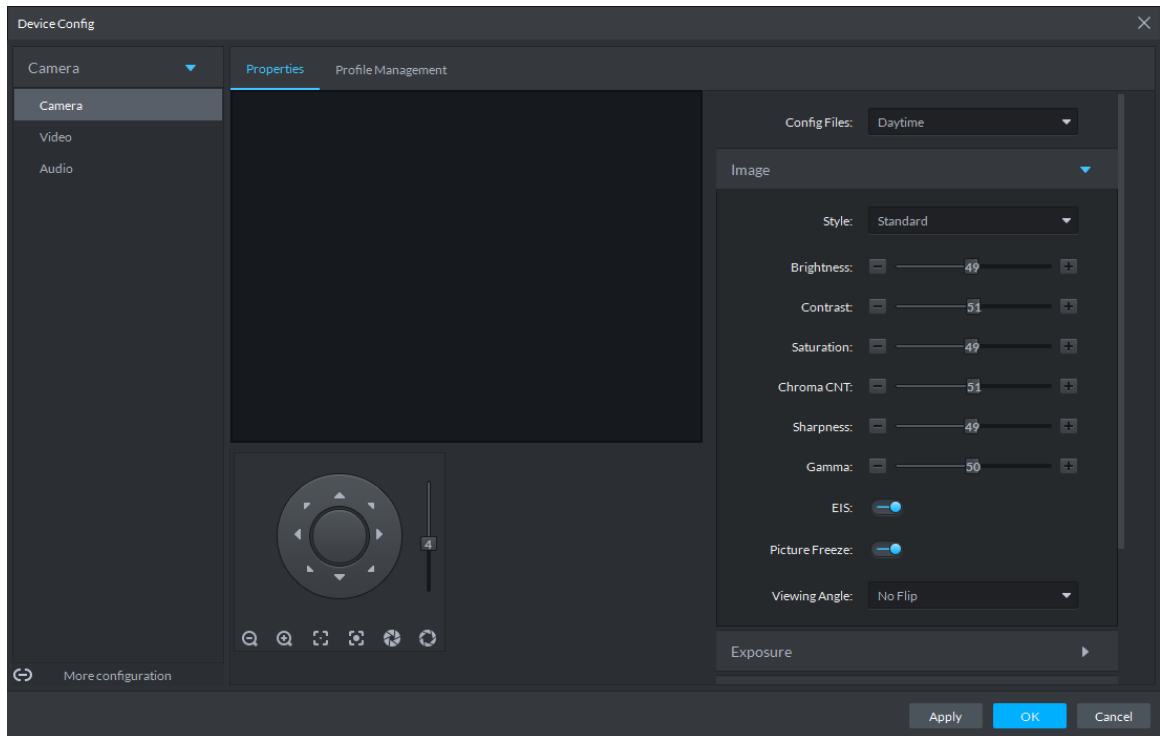


Figure 5-21 Device Config interface



Step 2 Select **Camera > Camera > Properties > Image**.

Step 3 Select **Profile Management**.

Step 4 Click **Image**.

Table 5-14 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.
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 5 Click **Exposure** to set up relevant parameters.



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

Figure 5-22 Exposure

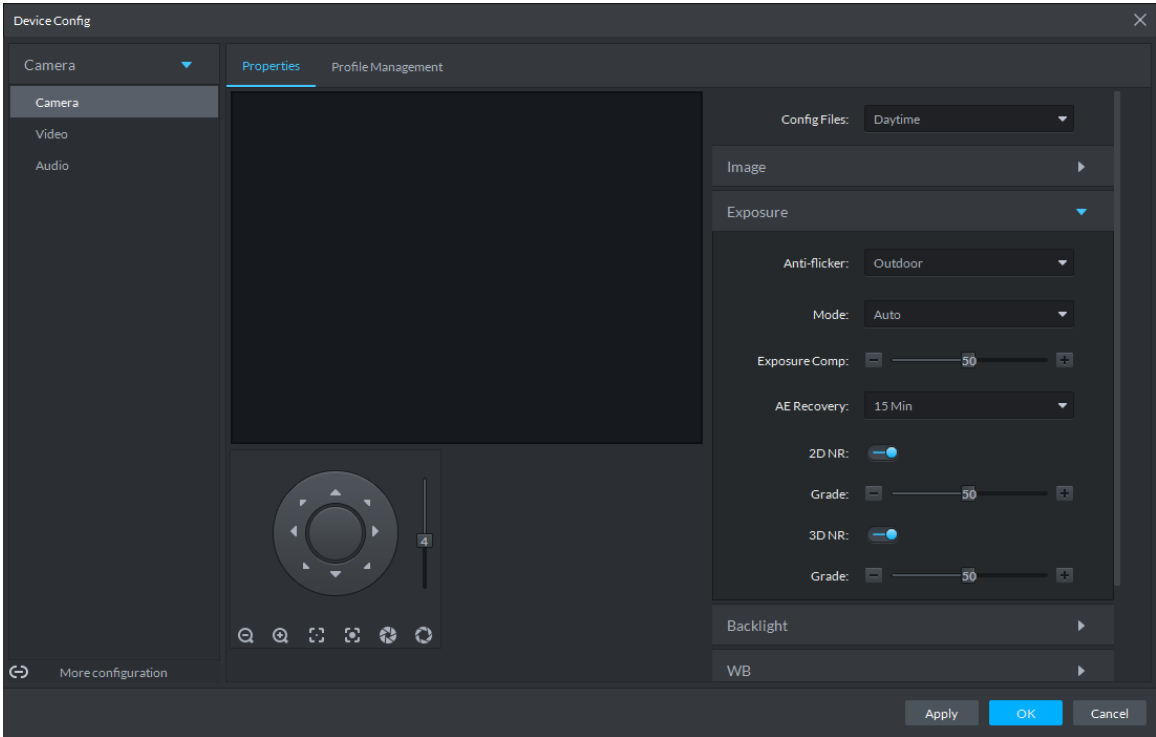



Table 5-15 Exposure parameters

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.
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 6 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 5-23 Backlight

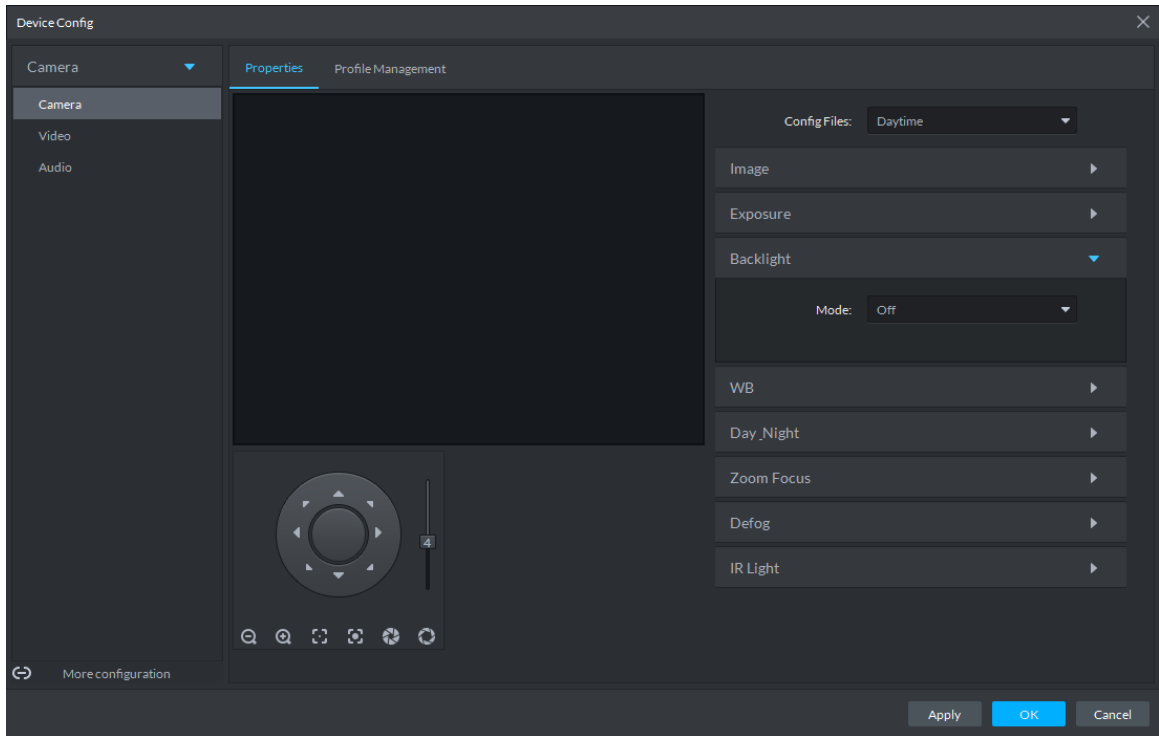



Table 5-16 Backlight parameters

Backlight mode	Description
SSA	The system adjusts image brightness automatically based on the environmental lighting conditions to show image details clearly.
Backlight Correction	<p>You can select Default mode or Custom mode.</p> <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	<p>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.</p> <p> The camera might lose seconds of video recordings when switching from a non-wide dynamic mode to Wide Dynamic.</p>
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 7 Click **WB** to set up 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 5-24 WB

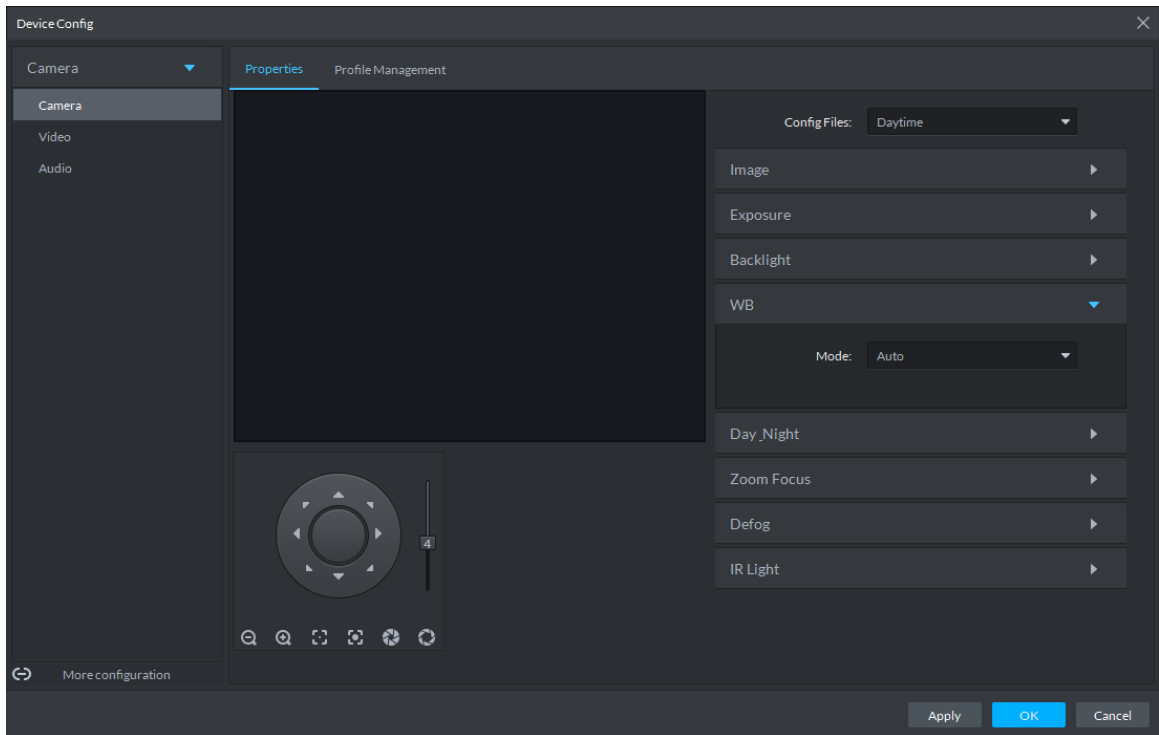


Table 5-17 WB parameters

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 8 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 5-25 Day & night

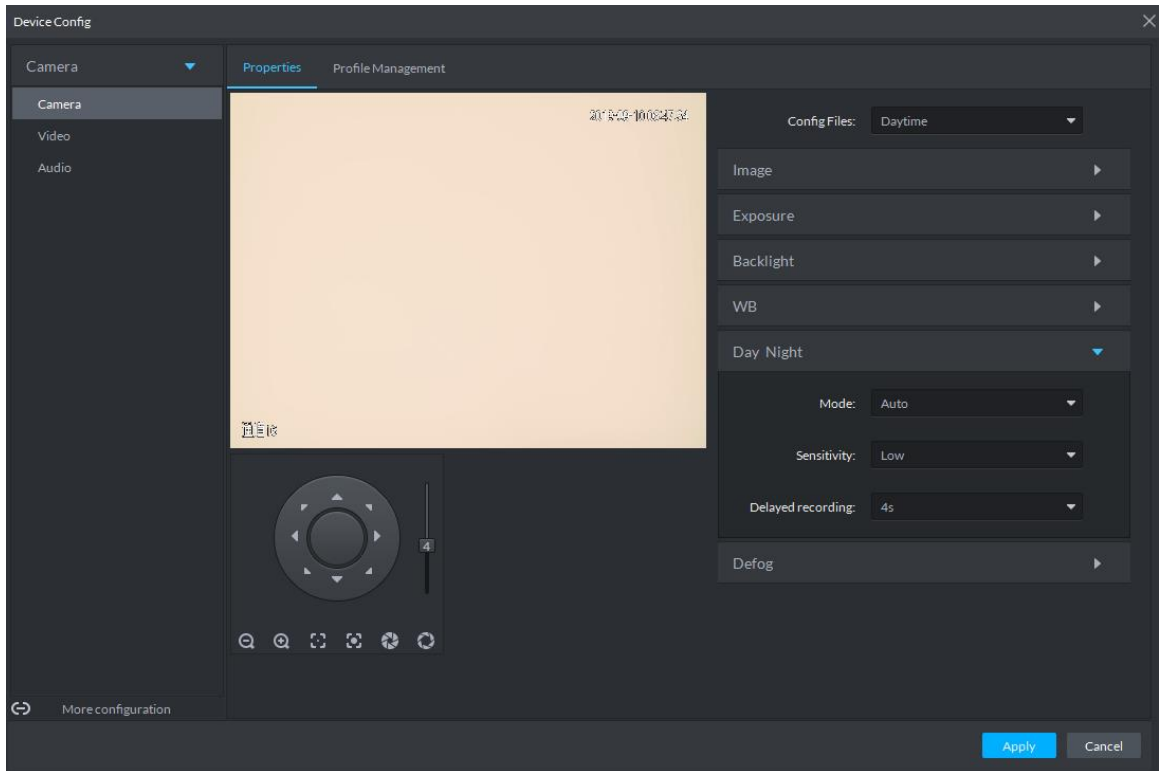



Table 5-18 Day & night parameters

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></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.</p> <p>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.</p> <p>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 9 Click **Defog** to set up relevant parameters.

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 5-26 Defog

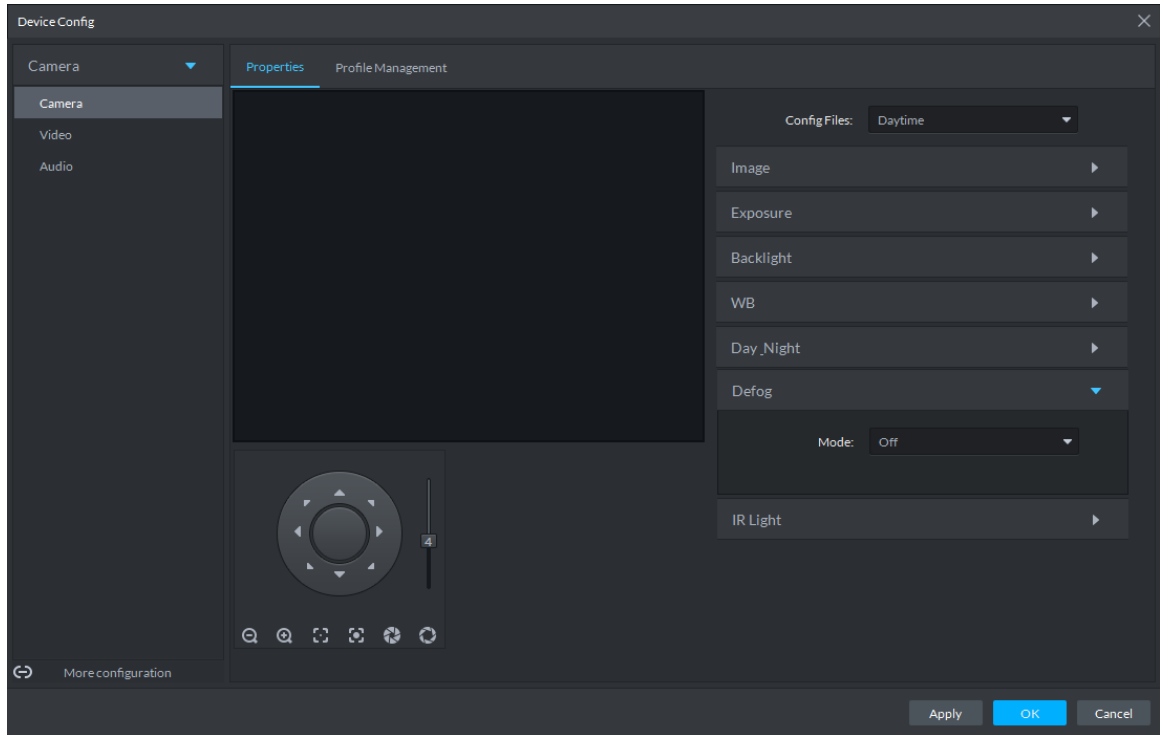


Table 5-19 Defog parameters

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 10 Click **IR Light** to set up relevant parameters.

Figure 5-27 IR light

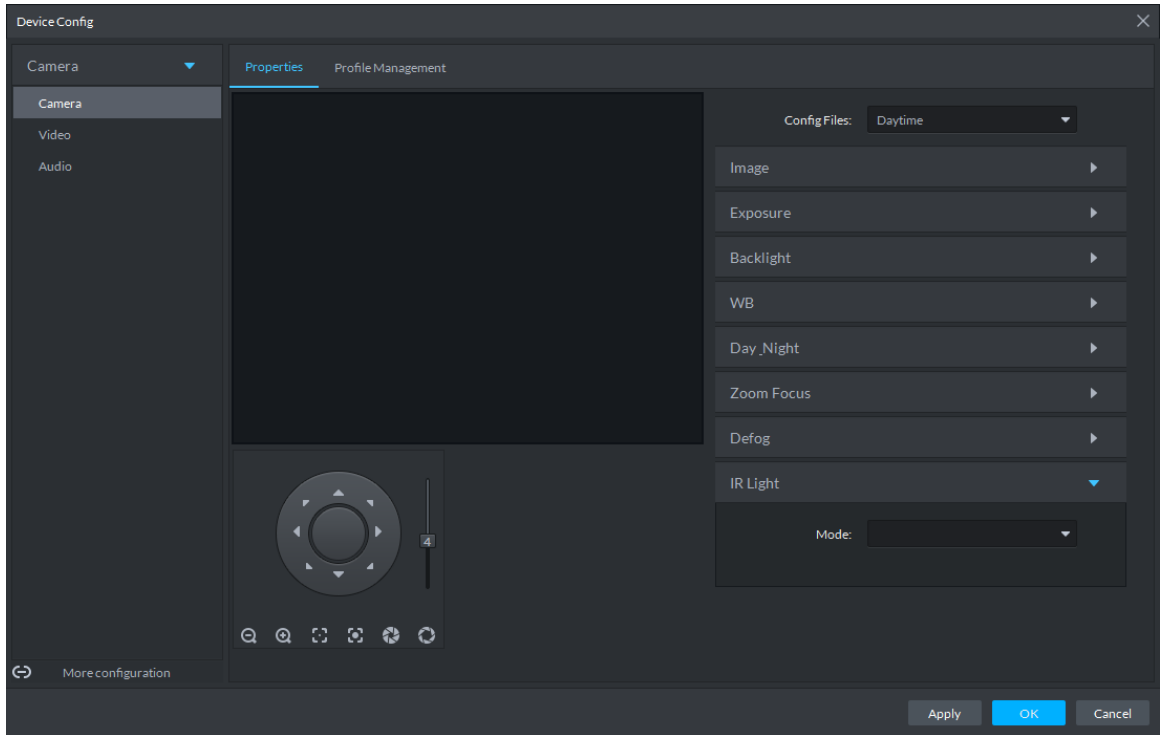


Table 5-20 IR light parameters

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	<p>The system adjusts the IR Light automatically to adapt to the brightness changes in the environment.</p> <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 11 Click **OK**.

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

5.3.3.1.2 Applying Configuration Files

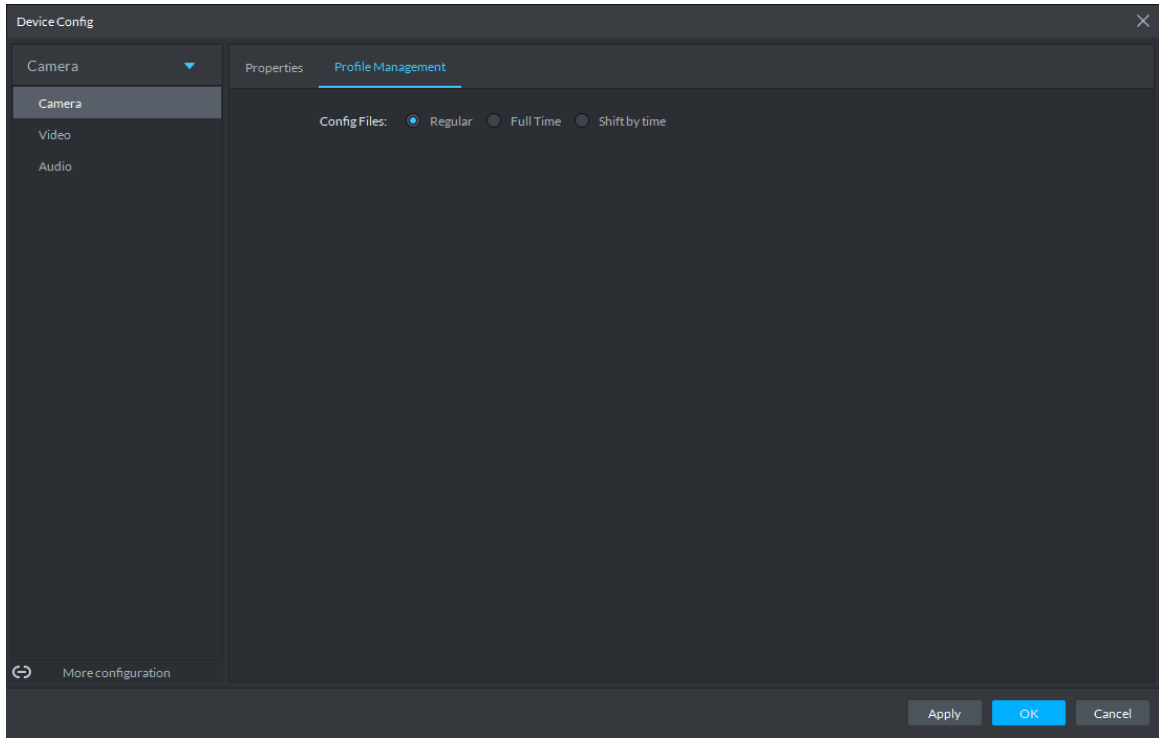
The system monitors the objects in different time periods based on the preset configuration files modes.

Step 1 Select **Camera > Camera > Properties > Profile Management**.

Step 2 Setting up configuration files.

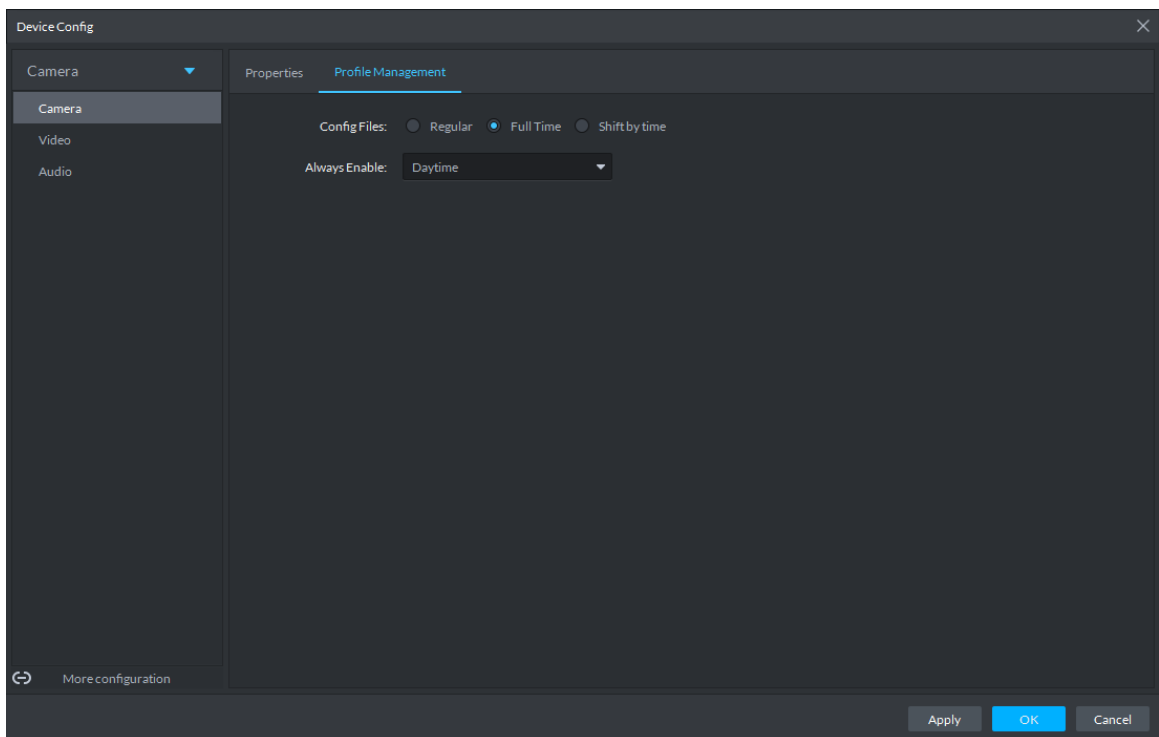
- When **Config Files** is set to **Regular**, the system monitors the objects as per regular configurations.

Figure 5-28 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.

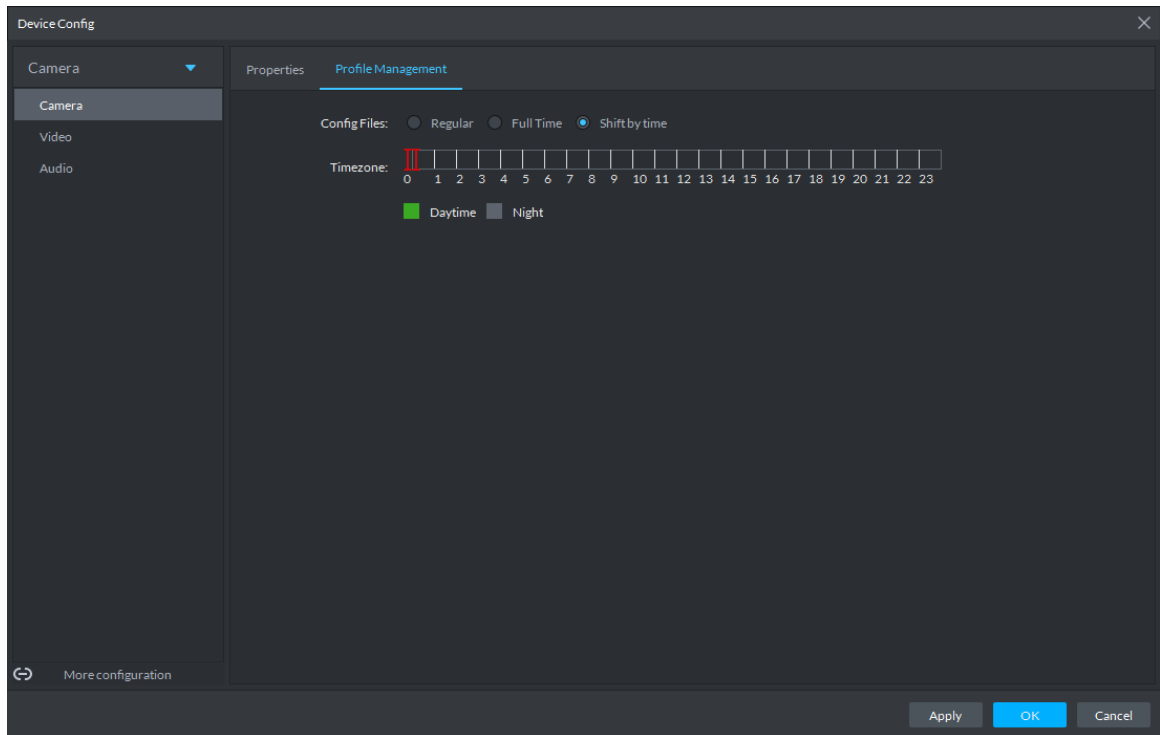
Figure 5-29 Set configuration files as full time



- 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 5-30 Set configuration files as shift by time



Step 3 Click **OK** to save the configurations.

5.3.3.2 Video

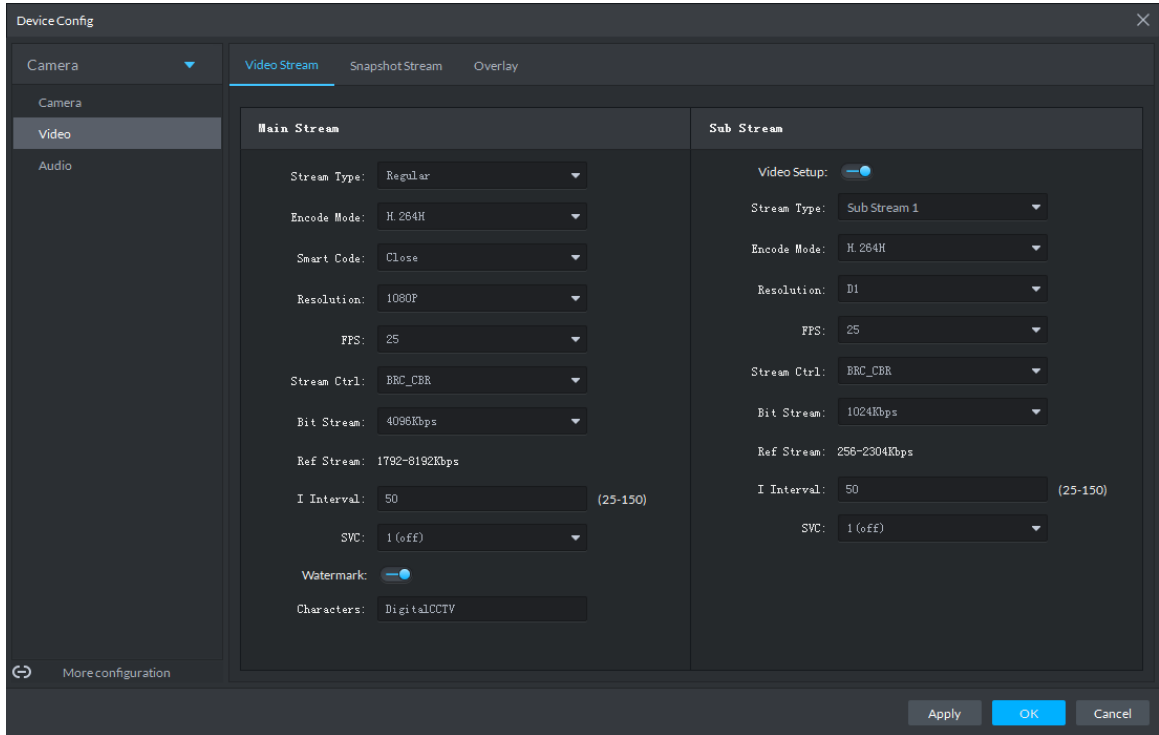
You can set some video parameters, including Video Stream, Snapshot Stream, Overlay, ROI, Save Path, and Video Encryption.

5.3.3.2.1 Video Stream

You can set up some video stream parameters, including Stream Type, Encode Mode, Resolution, FPS, Stream Ctrl, Bit Stream, I Interval, SVC, Watermark, and more.

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

Figure 5-31 Configure video stream settings



Step 2 To set **Video Stream**, see Table 5-21 for the details of various parameters.



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

Table 5-21 Video stream parameters

Parameter	Description
Video Setup	Indicates whether to set up the Sub Stream parameters.
Encode Mode	The following video encoding modes are available: <ul style="list-style-type: none"> ● H.264: Main Profile. ● H.264H: High Profile. ● H.265: Main Profile.
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>

Parameter	Description
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 dropdown 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. The default value is 1, that is non-layered encoding.
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.

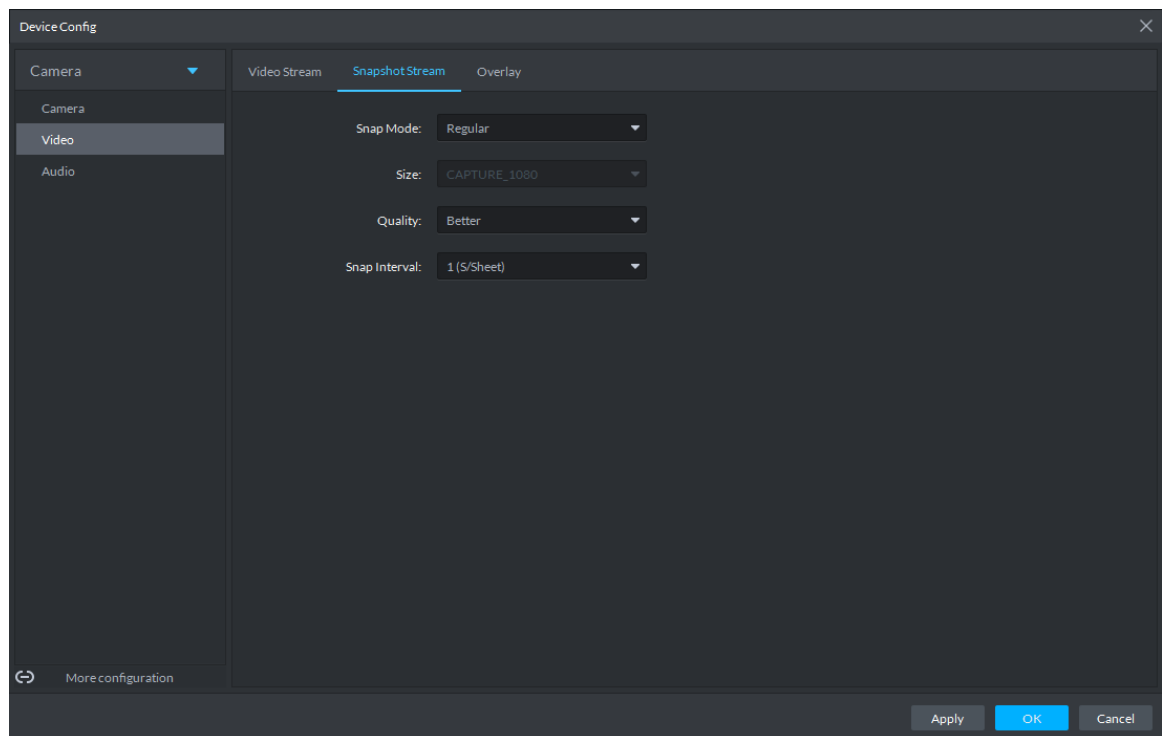
Step 3 Click **OK** to save the configurations.

5.3.3.2.2 Snapshot Stream

You can set up some stream parameters for snapshots, including Snap Mode, Size, Quality, and Snap Interval.

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

Figure 5-32 Configure snapshot stream settings



Step 2 To set up **Snapshot Stream**, see Table 5-22 for the details of various parameters.

Table 5-22 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** to save the configurations.

5.3.3.2.3 Overlay

You can set up video overlay, including Tampering/Privacy Mask, Channel Title, Period Title, Geographic Position, OSD Overlay, Font, and Picture Overlay.

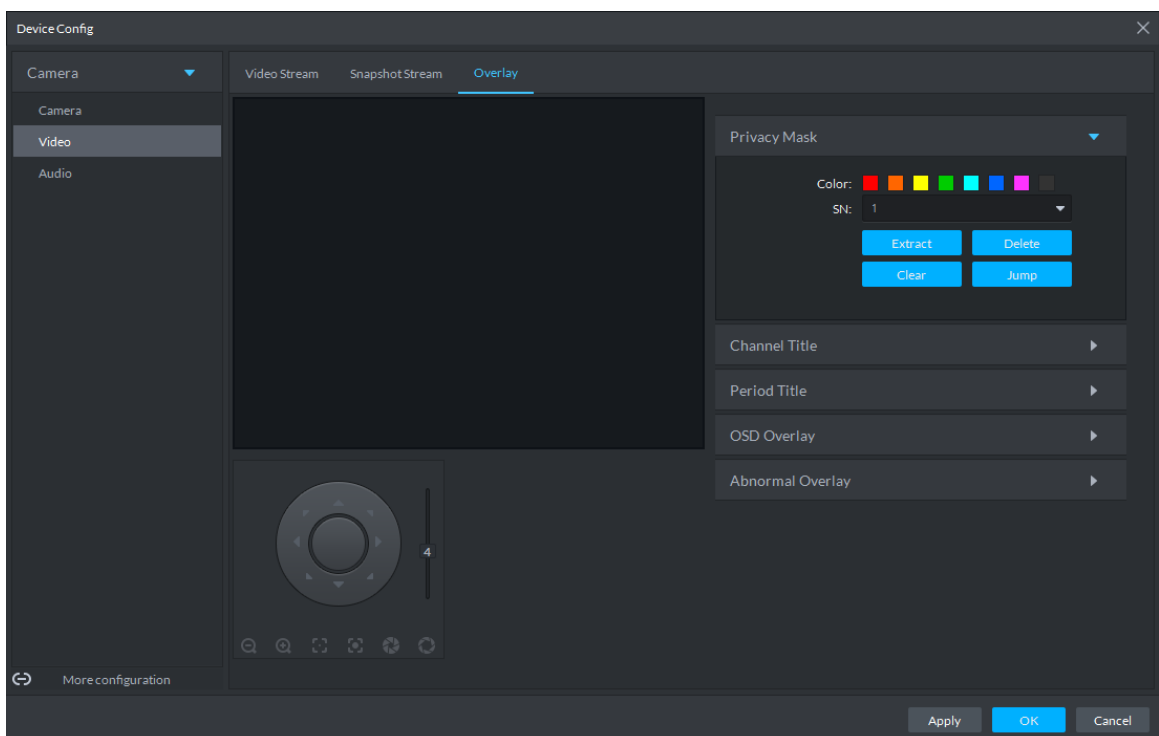
Step 1 On the **Device Config** interface, select **Camera > Video > Overlay**.

Step 2 (Optional) Set up Privacy Mask.

Tampering is useful in case that privacy protection is needed for some parts of the video images.

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

Figure 5-33 Configure overlay settings



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



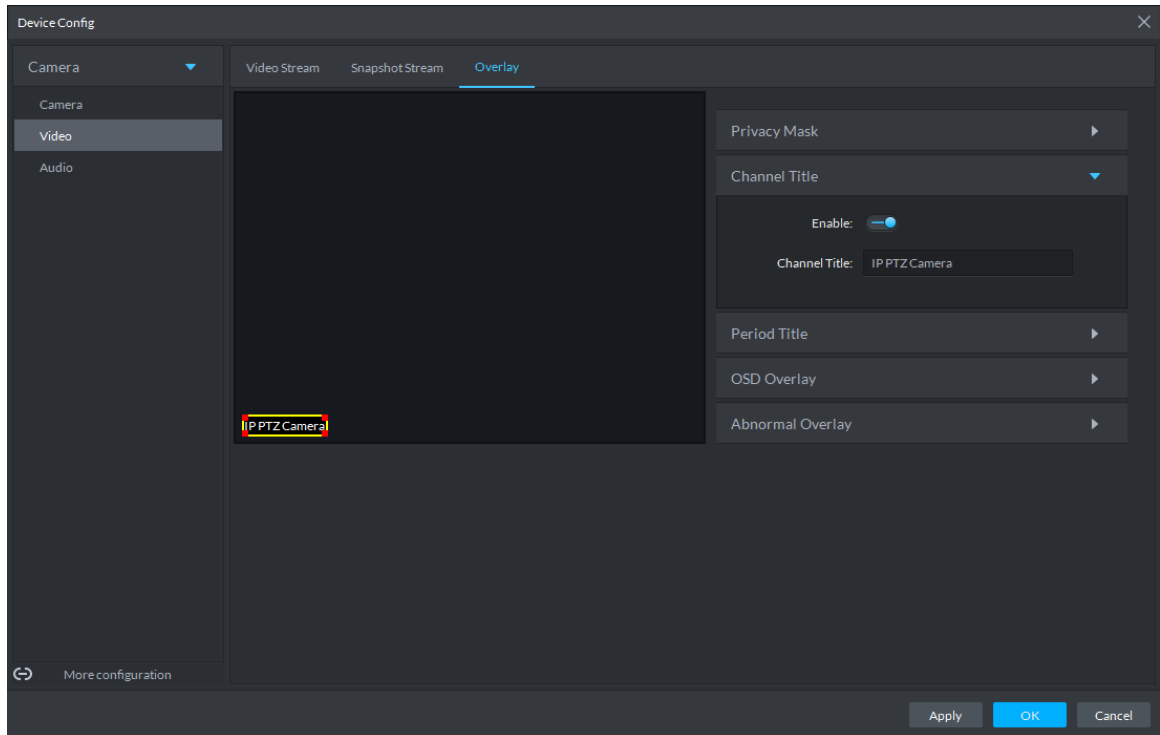
- You can draw up to four boxes.
- Click **Clear** to delete all boxes; to delete a box, select it and click **Delete**, or right-click and delete the box you want.

Step 3 (Optional) Set up Channel Title.

You can set up the Channel Title if it must be displayed in video images.

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

Figure 5-34 Set channel title



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



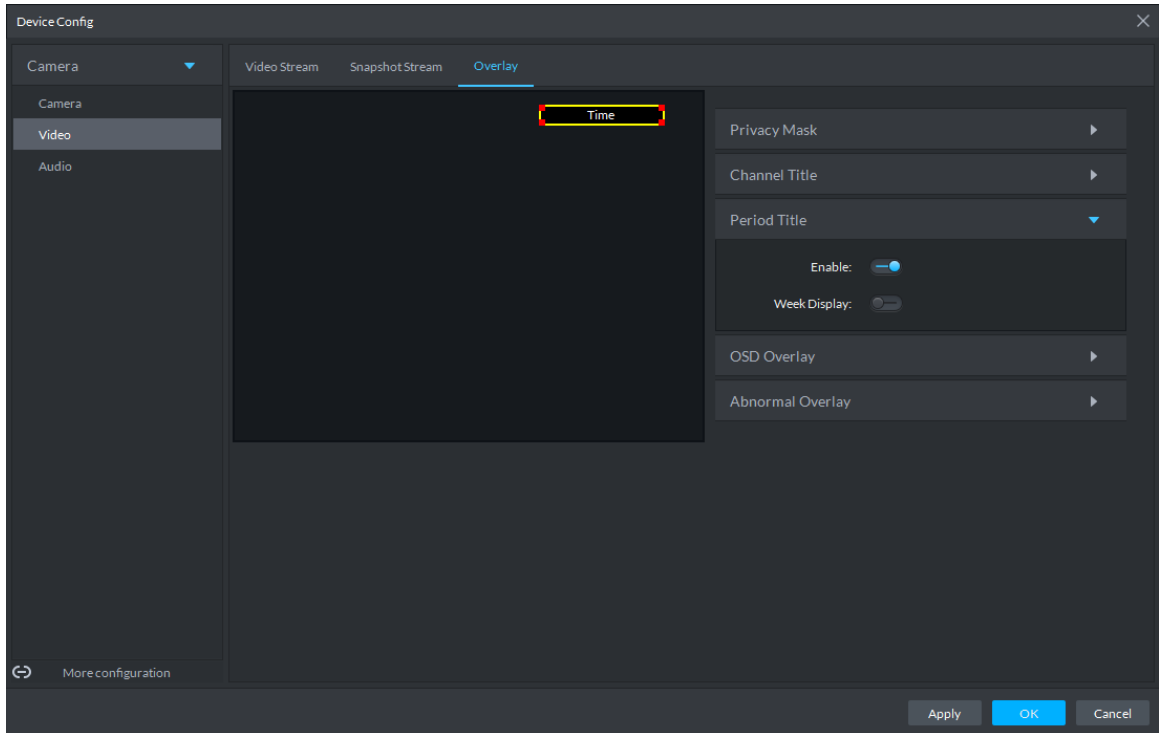
In the video image, the channel title box can be moved to a proper position.

Step 4 (Optional) Set up Period Title.

You can set up the Period Title if it must be displayed in video images.

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

Figure 5-35 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** to save the configurations.

5.3.3.3 Audio

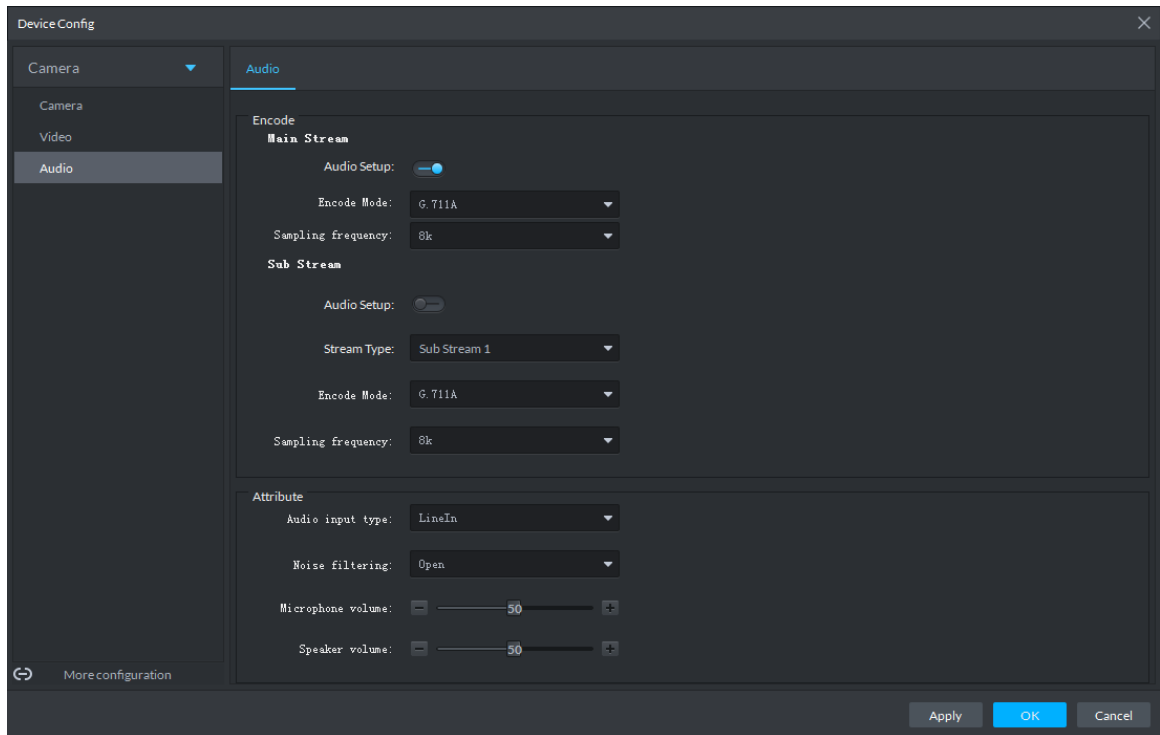
You can set some audio parameters such as Encode Mode, Sampling frequency, Audio input type, Noise filtering.



Some devices do not support audio functions.



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

Figure 5-36 Configure audio settings



Step 2 To set up audio parameters.

Table 5-23 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.
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.

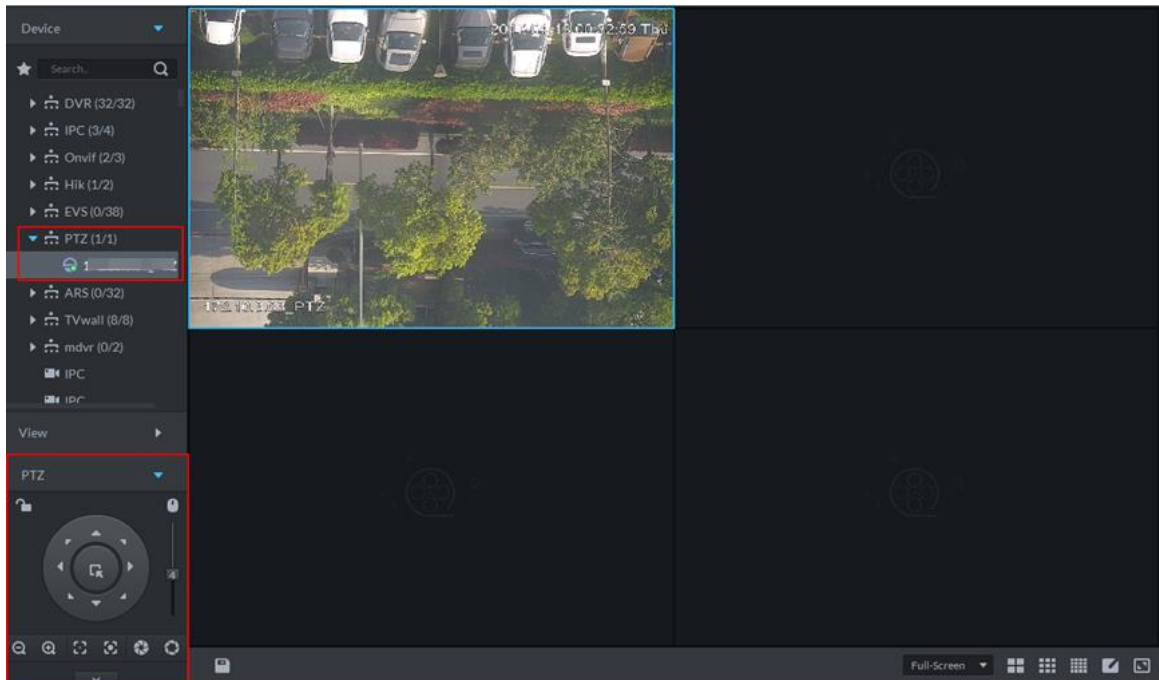
Step 3 Click **OK** to save the configurations.

5.3.4 PTZ

5.3.4.1 PTZ Operation Interface

Step 1 On **Live View** interface, open video from the PTZ camera, you can see PTZ operation interface on the left.

Figure 5-37 PTZ control panel




Step 2 Click  at the bottom of the interface to operate.

Figure 5-38 PTZ menu

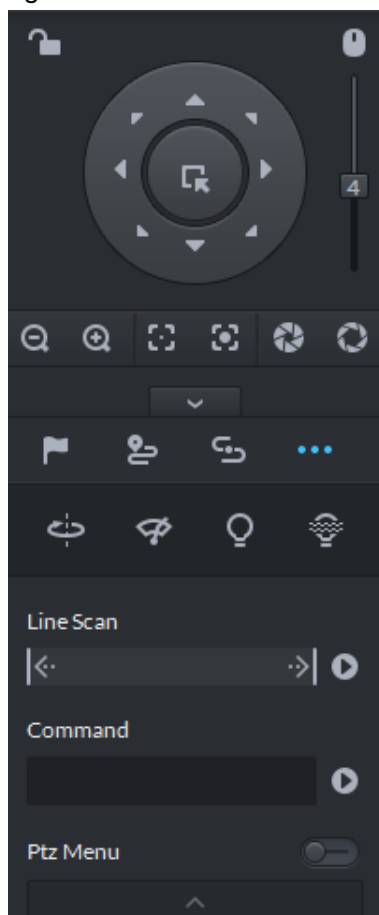















Table 5-24 Description

Parameters	Description
	<p>Click  to lock the current PTZ. Locked status shows as .</p> <p>Control over PTZ varies depending on user level.</p> <ul style="list-style-type: none"> When user of low level locks PTZ, user of high level can unlock and enable the PTZ by clicking . When user of high level locks PTZ, user of low level can't unlock the PTZ, unless PTZ automatically unlock itself. Users of the same level can unlock PTZ locked by each other. <p></p> <p>Default time for automatically unlocking PTZ is 30s.</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 Location and Partially Zoom In (for Speed Dome PTZ), to zoom in or zoom out the selected area.</p> <p></p>


Parameters	Description
	This function can be controlled with mouse only.
	From top to the bottom to adjust rotation speed of PTZ, to set the step size chosen from 1 to 8.
	Zoom, to control zoom operation of speed dome.
	Focus, to adjust focus.
	Aperture, to adjust brightness.
	Set preset, tour, pattern, scan, rotation, wiper, light, IR light function, etc. Refer to 5.3.4.2 PTZ Settings for more information.


5.3.4.2 PTZ Settings


5.3.4.2.1 Configuring Preset

By adding preset, you can rotate the camera to the specified position.



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

Step 2 Click .

Step 3 Place mouse over 1 and click .

Step 4 Input preset point No., and click .

Adding preset point completed.


To the right of , click , then camera will be rotated to the related position.


5.3.4.2.2 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.

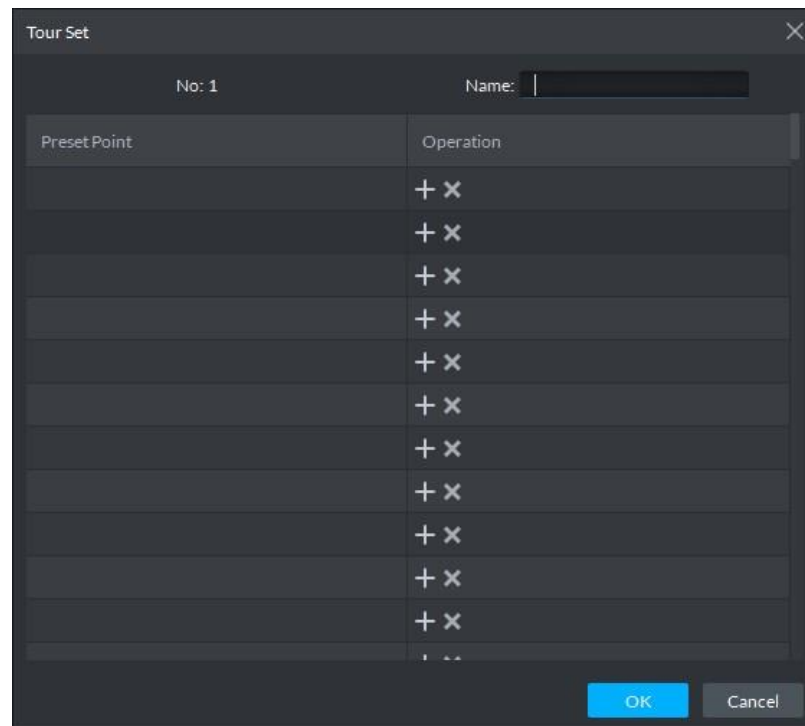
Step 1 Click .

Step 2 Place mouse over 1 and click .

Step 3 Enter name, and click operation bar .


Choose preset points from the dropdown list on the left.

Figure 5-39 Set preset points



Step 4 Click **OK**.
System prompts **Tour Saved Successfully**.

Step 5 Click **OK**.


To start tour, place mouse over 1 and click , then camera goes back and forth among the presets of Tour 1.


5.3.4.2.3 Configuring Pattern

Pattern is equivalent to a record process.

Step 1 Click .


Step 2 Place mouse over 1 and click , then operate 8 buttons of PTZ to set pattern.


Step 3 Click  to complete pattern setup.


Step 4 Click , and the camera will rotate following the pattern settings.

5.3.4.2.4 Configuring Scan




Step 1 Click .

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

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




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

5.3.4.2.5 Enable/Disable Pan

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




5.3.4.2.6 Enable/Disable Wiper

It is to use RS485 command to control the connected peripheral device wiper on/off. Make sure the connected peripheral device supports wiper function.




Click , and then click , it is to enable wiper. After enabling wiper, click  to disable.

5.3.4.2.7 Enable/Disable Light

It is to use RS485 command to control the connected peripheral device light on/off. Make sure the connected peripheral device supports light function.

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

5.3.4.2.8 Enable/Disable IR Light

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

5.3.4.2.9 Configuring Custom Commands

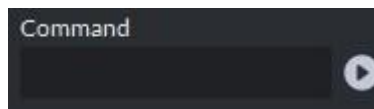


Different devices support different customized commands. Contact the manufacture for detailed information.

Step 1 Click .

Step 2 Enter command on the customized command interface.

Figure 5-40 Set custom commands



Step 3 Click  to display the function of the customized command.

5.3.4.2.10 PTZ Menu

Step 1 Click .

Figure 5-41 PTZ menu

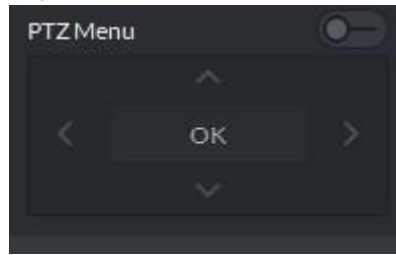








Table 5-25 Description

Parameters	Description
	Up/down button. Move the cursor to the corresponding item.
	Left/right. Move the cursor 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 cursor to Back and then click OK to go to go back to the previous menu. • Move the cursor to Exit and then click OK to exit the menu.

Step 2 Click **OK**.

Figure 5-42 PTZ main menu

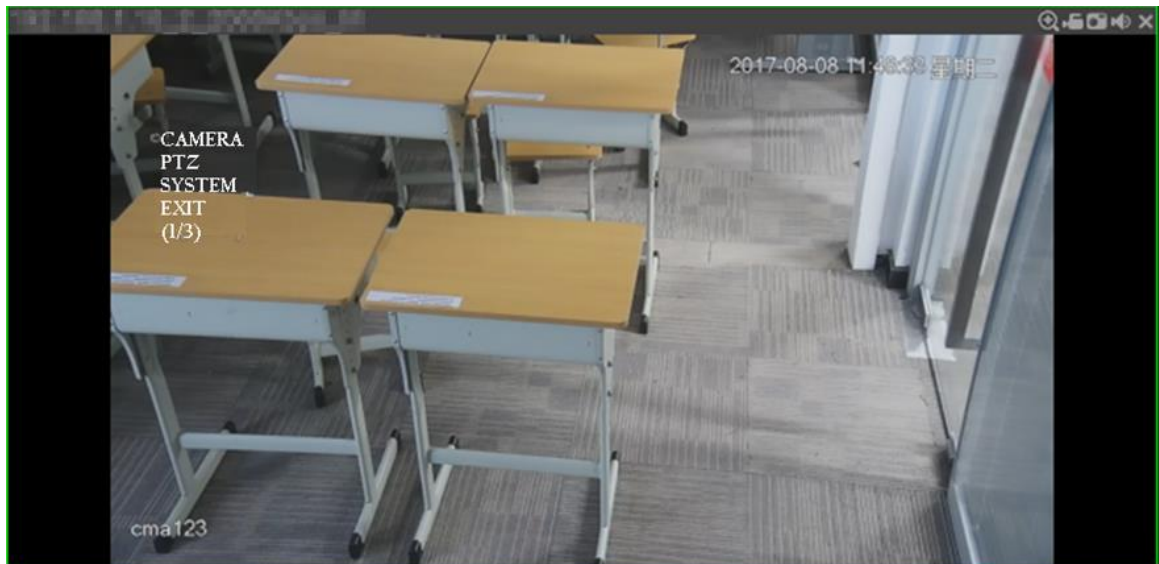


Table 5-26 Main menu description

Parameters	Description
Camera	Move the cursor to Camera and then click OK to enter camera settings sub-menu interface. It is to set camera parameters. It includes picture, exposure, backlight, day/night mode, focus and zoom, defog, default, etc.
PTZ	Move the cursor to PTZ and then click OK to enter PTZ sub-menu interface. It is to set PTZ functions. It includes preset, tour, scan, pattern, rotation, PTZ restart, etc.

Parameters	Description
System	Move the cursor to System and then click OK to enter system sub-menu interface. It is to set PTZ simulator, restore camera default settings, video camera software version and PTZ version.
Return	Move the cursor to the Return and then click OK, it is to go back to the previous menu.
Exit	Move the cursor to the Exit and then click OK, it is to exit PTZ menu.

5.3.5 Fisheye-PTZ Smart Track

DSS Client supports smart track which links fisheye speed dome to general speed dome to better control each monitoring position.

5.3.5.1 Preparations


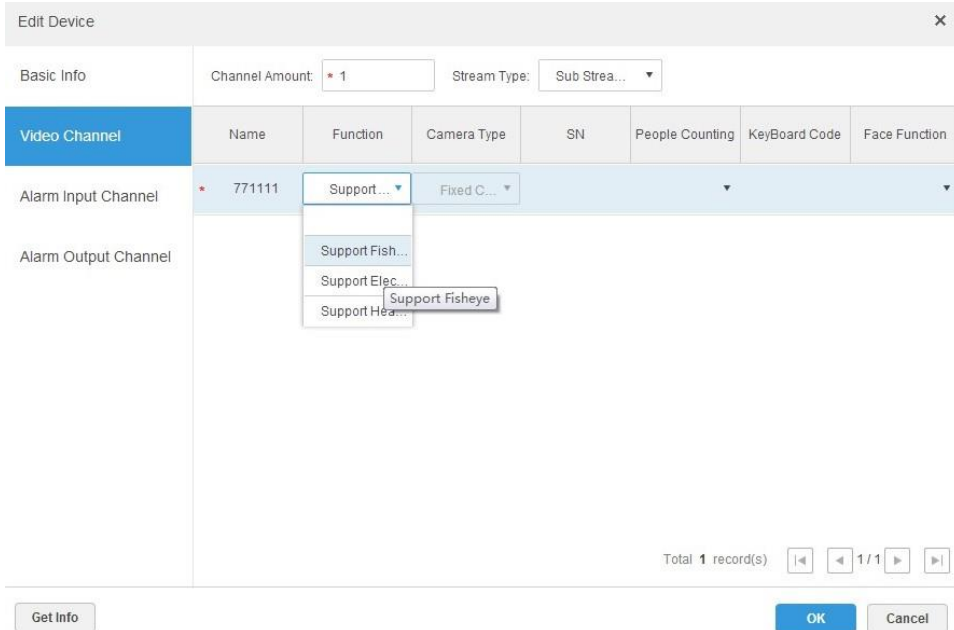
- Before operating smart track, go to Device manager to add fisheye device and PTZ camera first. Refer to "4.5 Adding Device " for detailed information.
- After device is added, click , and select fisheye and general speed dome.

Figure 5-43 Set smart track function type



The screenshot shows the 'Edit Device' window with the following details:

- Basic Info:** Channel Amount: 1, Stream Type: Sub Strea...
- Video Channel Table:**

Video Channel	Name	Function	Camera Type	SN	People Counting	KeyBoard Code	Face Function
Alarm Input Channel	771111	Support...	Fixed C...				
Alarm Output Channel							
- Function Dropdown Menu:**
 - Support Fish...
 - Support Elec...
 - Support Fisheye
 - Support Hea...
- Footer:** Total 1 record(s), navigation buttons, Get Info, OK, Cancel.

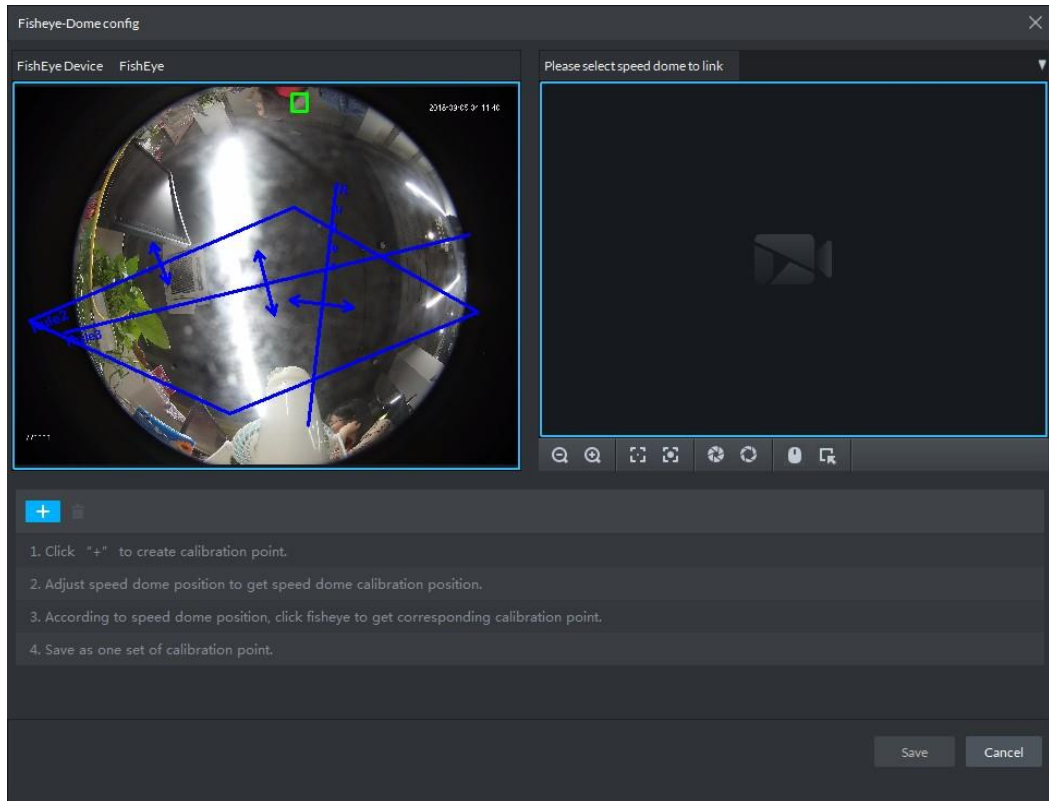
5.3.5.2 Configure Smart Track Settings

Step 1 Select the fisheye device on the device tree and then right-click to select **Smart Track**.



If it is not the first time to use smart track function, select the fisheye device and then right-click to select smart track configuration.

Figure 5-44 Set smart track rules (1)



Step 2 Click  after the Select linkage PTZ camera and then select a PTZ camera.

Step 3 Click  and then move the  of the fisheye on the right to select a position.


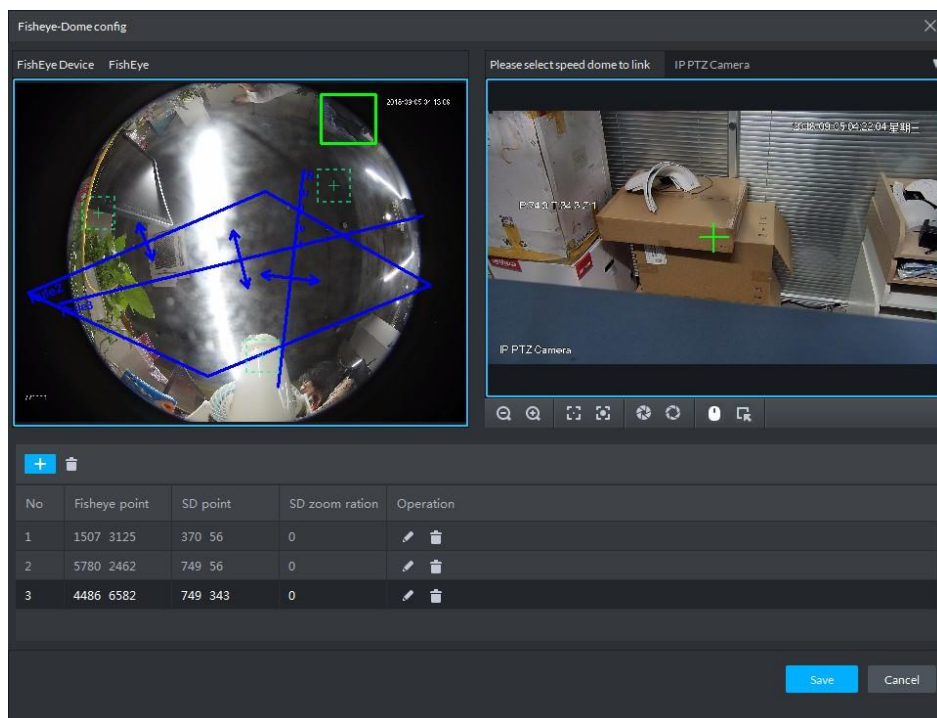


Click  on the general PTZ camera to find the position. Adjust the PTZ camera to find the position and move the PTZ to the center position (The green cross on the image).

Figure 5-45 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 4 Click  to save the calibration point.

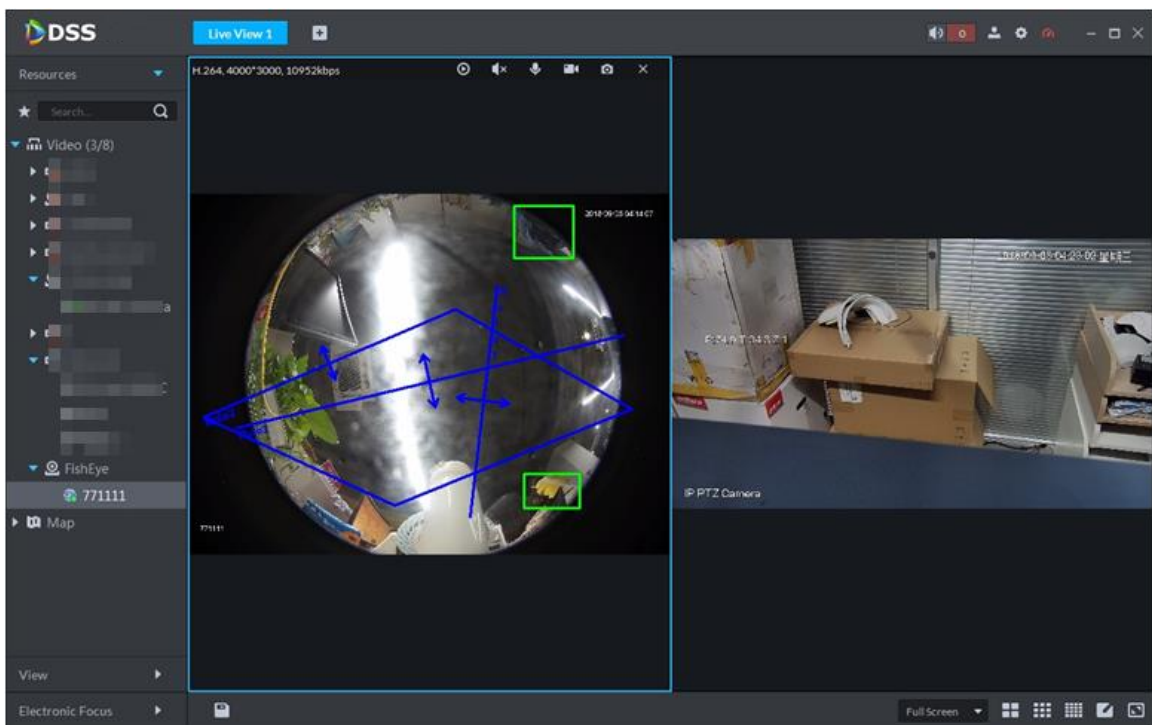
Refer to above steps to add at least three calibration points. These three points shall not be on the same straight line.

Step 5 Click Save.

5.3.5.3 Enable Smart Track Function

Step 1 Select the fisheye device on the device tree and then right-click to select **Smart Track**.

Figure 5-46 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


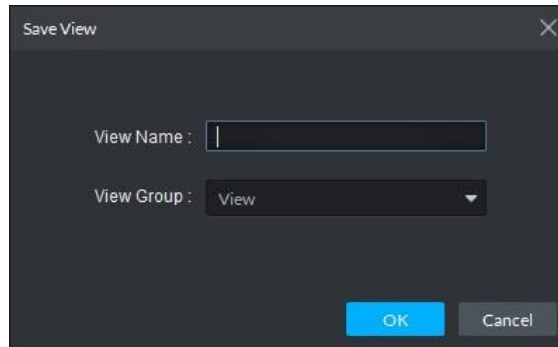
Step 3 Click , system pops up **Save View** box.

Figure 5-47 Save view



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

5.3.6 Bullet-PTZ Smart Track

Support smart track which links bullet with PTZ camera, and it is good for panoramic monitoring and details tracking. Currently smart track supports bullet PTZ all-in-one camera and panoramic + PTZ camera etc. Besides, it also supports individual bullet and PTZ camera which have been bound and calibrated.

5.3.6.1 Preparation before Operation


- Before implementing smart track (bullet + PTZ camera), it needs to add bullet and PTZ camera from **Device** on Web interface. For detailed steps, refer to "4.5 Adding Device."
- Click  after adding bullet, and select **Master Slave Track**. Tracking function can be realized after configuring master slave track.

Figure 5-48 Select master slave track

The screenshot shows the 'Edit Device' configuration window. The 'Video Channel' tab is selected. The 'Channel Amount' is set to 2. The 'Stream Type' is 'Sub Strea...'. The 'Zero Channel Code' checkbox is unchecked. The table below shows the configuration for two channels:

	Name	Camera Type	Features	SN	KeyBoard Code
Alarm Input	* IPC	Fixed Camera	Master Slave Track		
Alarm Output	* IP PTZ Camera	Speed Dome	Please click here to..		

At the bottom right of the table, it says 'Total 2 record(s)' with navigation buttons. At the bottom of the window, there are 'Get Info', 'OK', and 'Cancel' buttons.

- It needs to calibrate bullet and PTZ camera by config tool in advance if you want to add individual bullet and PTZ camera. For detailed operations, refer to config tool user manual.

5.3.6.2 Applying Smart Track

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

5.3.6.2.1 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 5-49 Manual positioning



5.3.6.2.2 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 5-50 3D positioning (1)



Figure 5-51 3D positioning (2)



5.3.6.2.3 Manual Track



- Bullet PTZ all-in-one camera, panoramic+PTZ camera and individual bullet have been configured with smart rules. For detailed operation, refer to 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 5-52 Manual track



5.3.6.2.4 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, refer to 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 5-53 Select automatic track

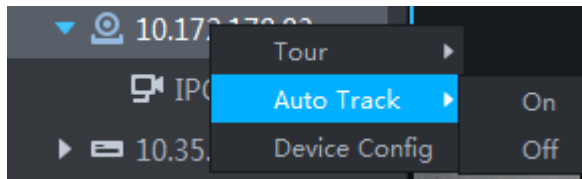


Figure 5-54 Automatic track



5.3.6.2.5 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.

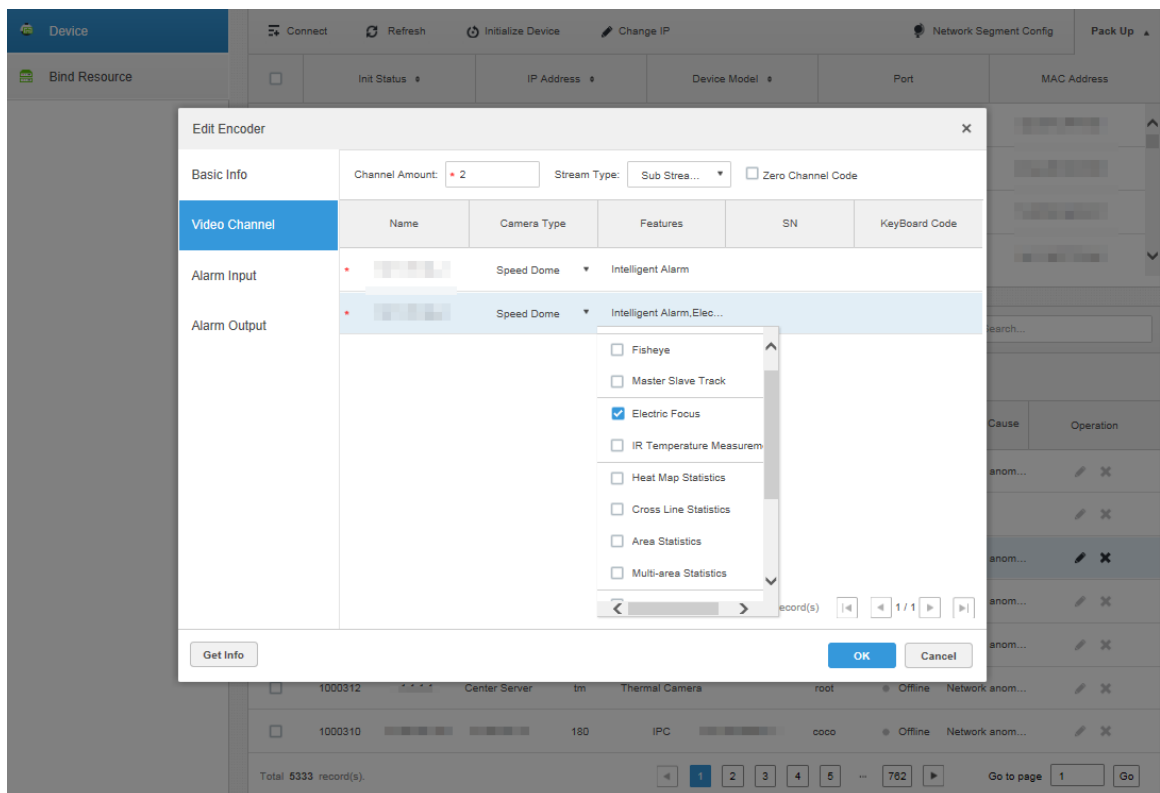
5.3.7 Electronic Focus

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 5-55.

Figure 5-55 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 5-56 Live View

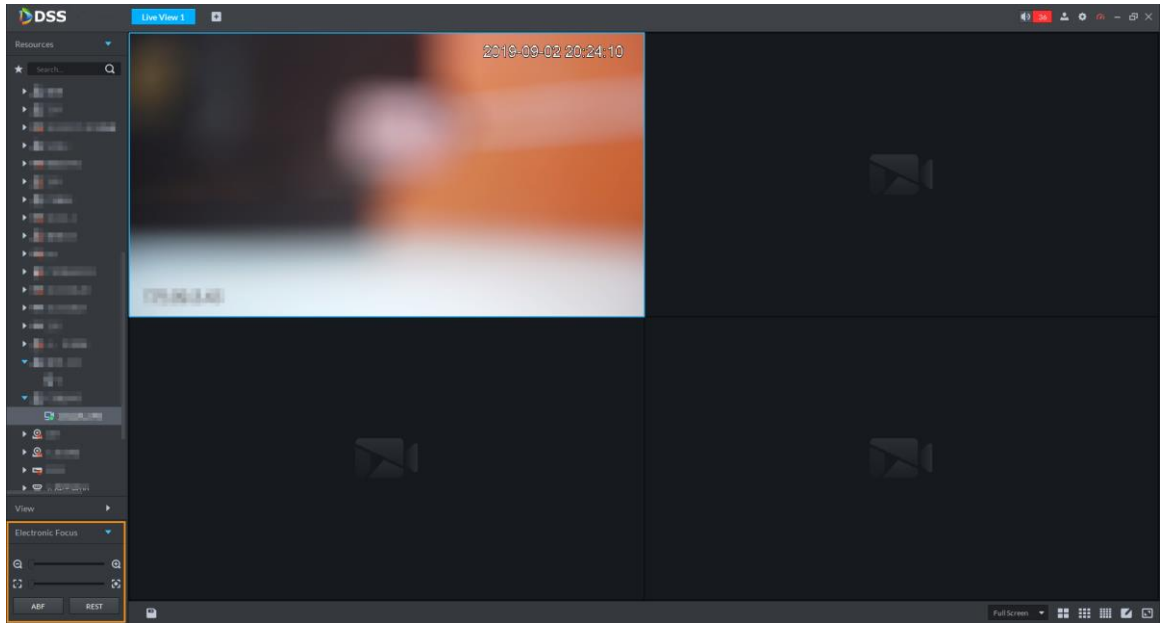









Table 5-27 Parameters description

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.

5.3.8 View Tour

Step 1 On the **Live View** interface, Double-click a channel on the left side to open the video.


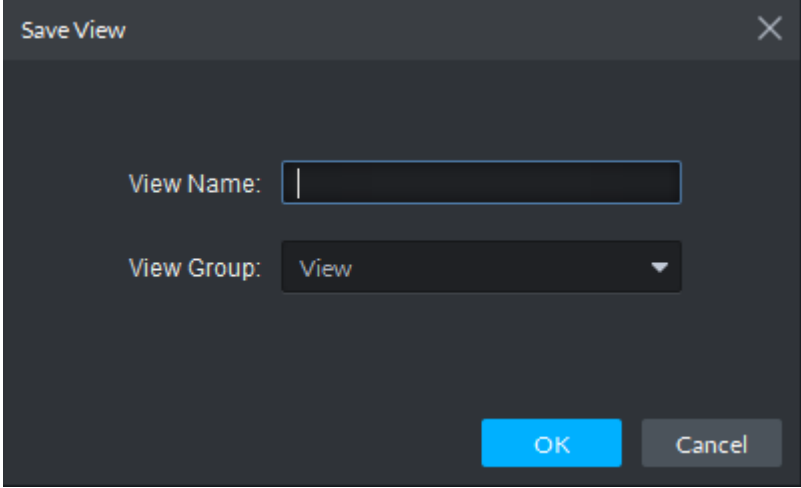
Step 2 Click  in the lower part, system pops up **Save View** dialogue box.

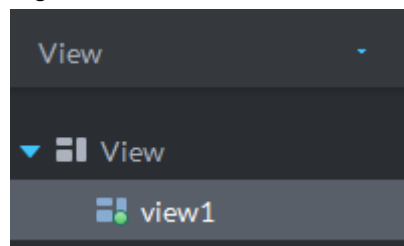
Figure 5-57 Save view



The 'Save View' dialog box is a dark-themed window with a close button (X) in the top right corner. It contains two input fields: 'View Name' with an empty text box, and 'View Group' with a dropdown menu currently showing 'View'. At the bottom right, there are two buttons: 'OK' (highlighted in blue) and 'Cancel' (greyed out).

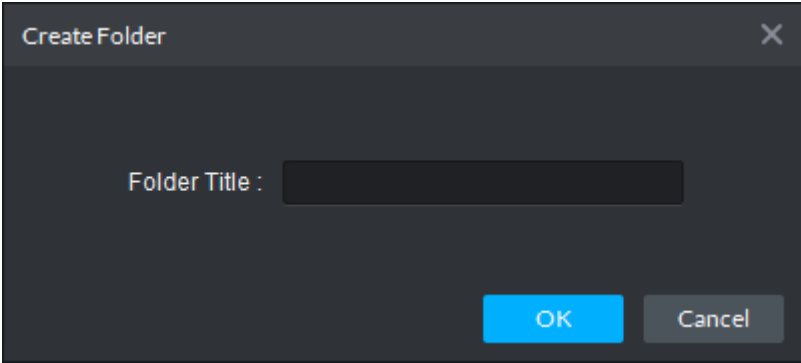
Step 3 Input **View Name**, select **View Group** and click **OK**.

Figure 5-58 Added view



Step 4 Select **View** and right-click to select **Create Folder**.

Figure 5-59 Create folder



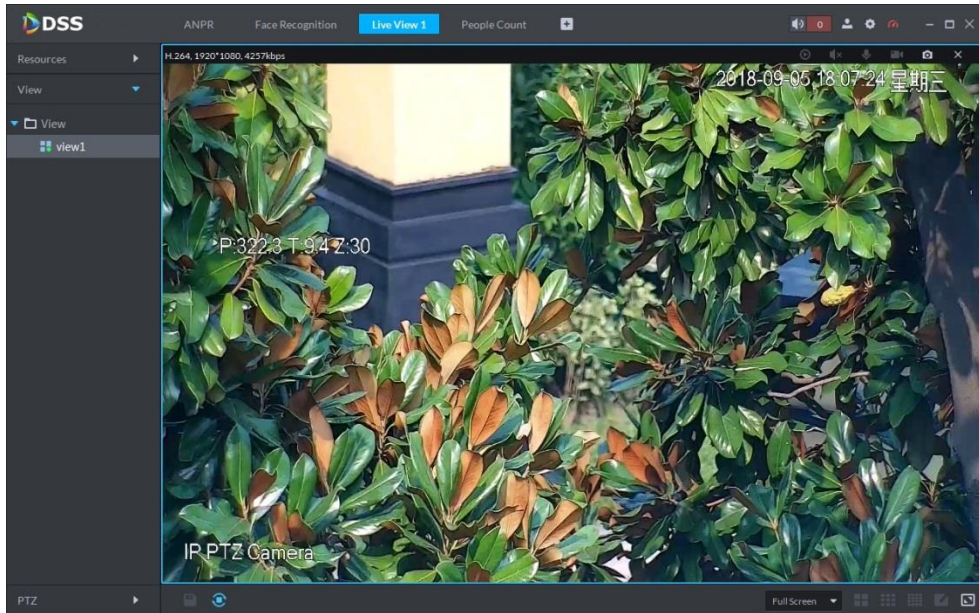
The 'Create Folder' dialog box is a dark-themed window with a close button (X) in the top right corner. It contains one input field: 'Folder Title' with an empty text box. At the bottom right, there are two buttons: 'OK' (highlighted in blue) and 'Cancel' (greyed out).

Step 5 Input **Folder Title** and click **OK**.

Step 6 Right-click **View** to select **Tour Interval**, for example, 10 s.

Click  to stop tour.

Figure 5-60 View tour

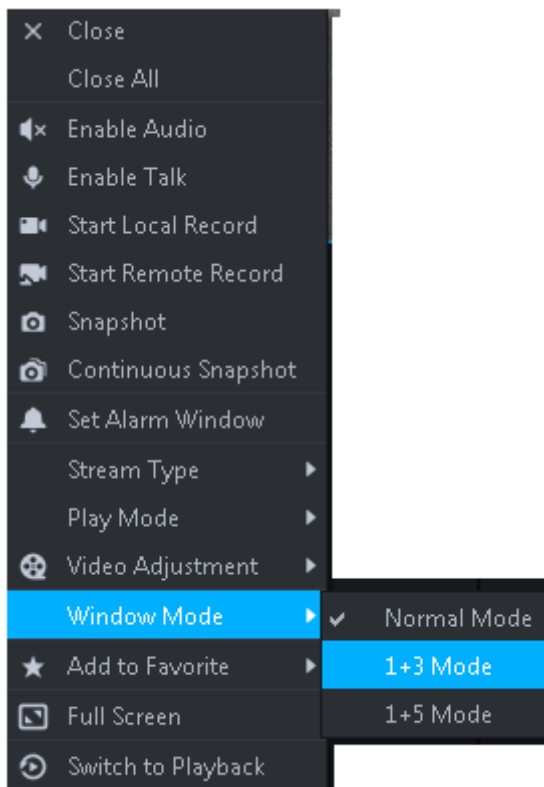


5.3.9 Region of Interest (RoI)

Client Live view window supports Normal mode, 1+3 mode and 1+5 mode.

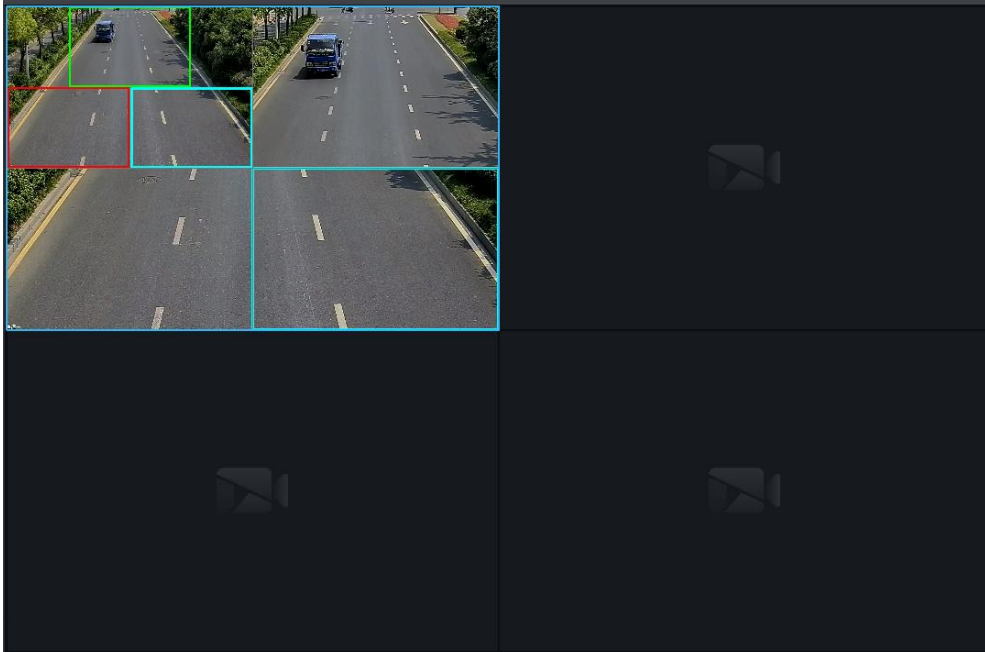
Right-click to select **Window Mode** in the live view window.

Figure 5-61 Select window mode



For example, select 1+3 mode.

Figure 5-62 1+3 mode



5.4 Configuring Intelligent Analysis

Configure intelligent analysis rules on the client to realize intelligent analysis business. Intelligent analysis types supported: IVS, people counting, face detection, and heatmap. The rule configuration interface might vary according to the function capability of different devices. The actual interface shall prevail.



The platform only supports configuring intelligent analysis rules for IPC channels.

5.4.1 Intelligent Analysis Configuration Interface

Right-click an IPC channel on the **Live View** interface, and then select **Intelligent Analyse**.

Figure 5-63 Go to intelligent analysis interface

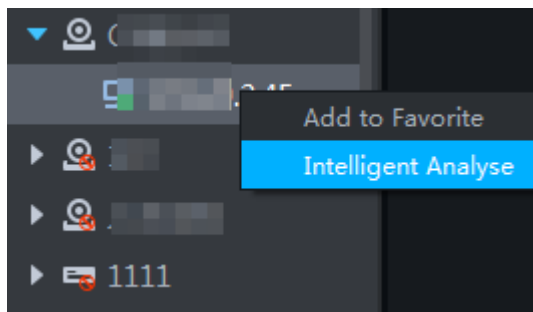
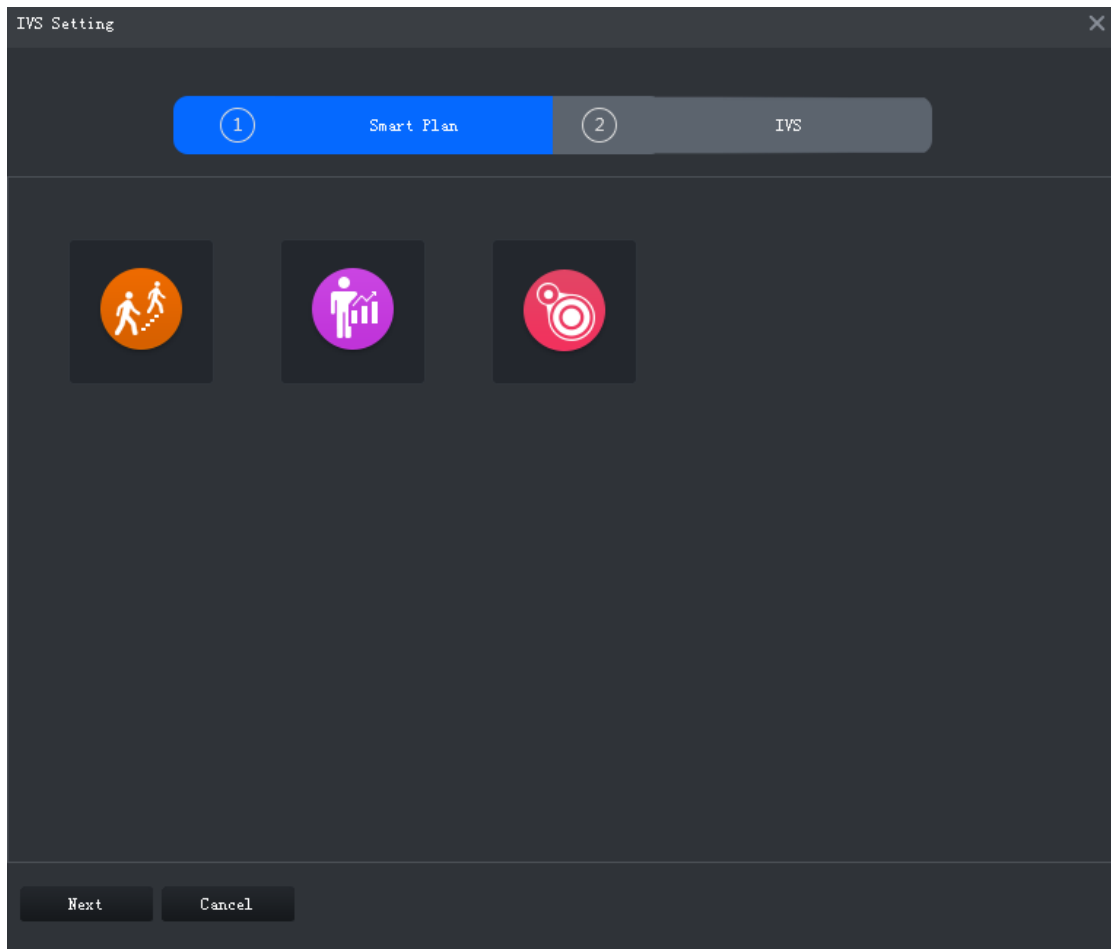


Figure 5-64 IVS setting interface



The interface might vary according to the smart function capability of the different devices. The actual interface shall prevail.

5.4.2 IVS

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.


See requirements as follows when configuring:

- 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.

5.4.2.1 Enabling IVS Smart Plan

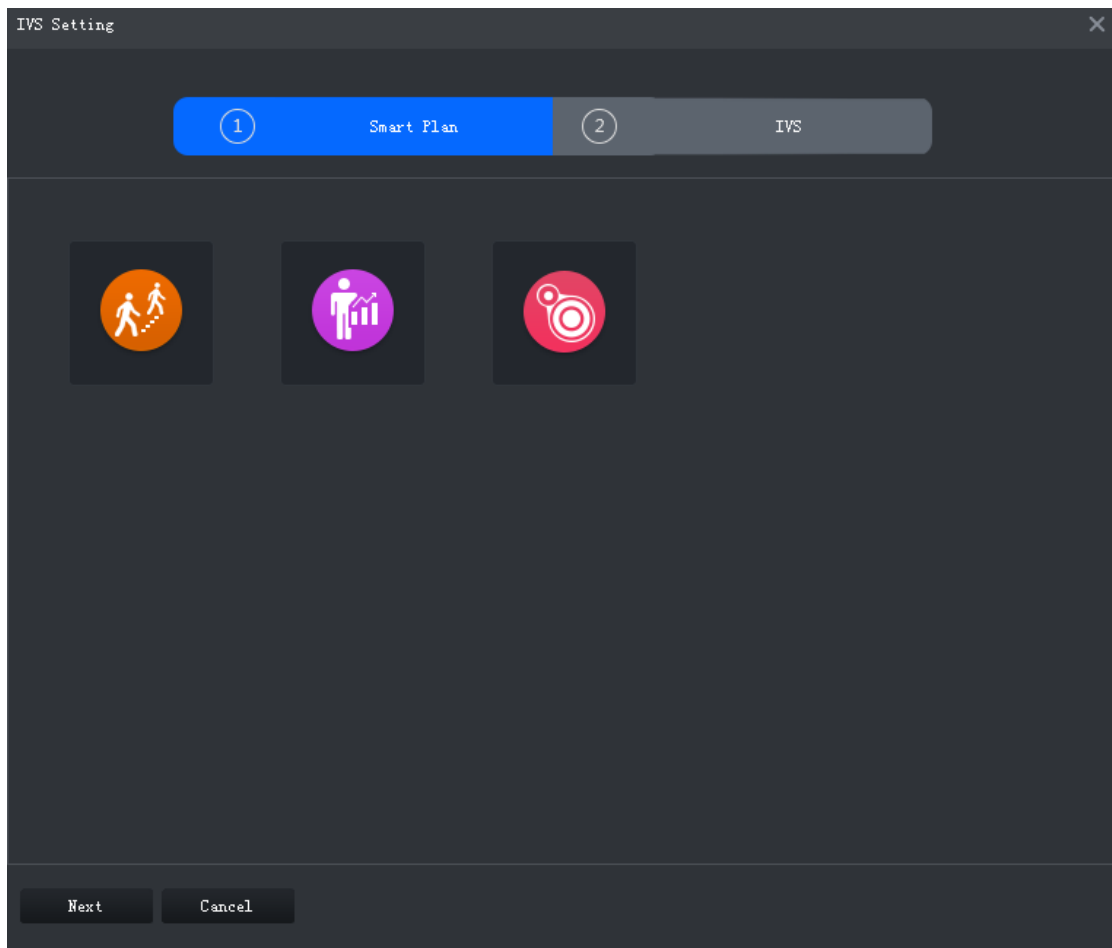
Step 1 Go to the **Intelligent Analyse** interface.

Step 2 Click  on the smart plan interface to enable IVS smart plan. See Figure 5-65.

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 5-65 Enable IVS smart plan



Step 3 Click **Next**.

The **IVS Setting** interface is displayed.

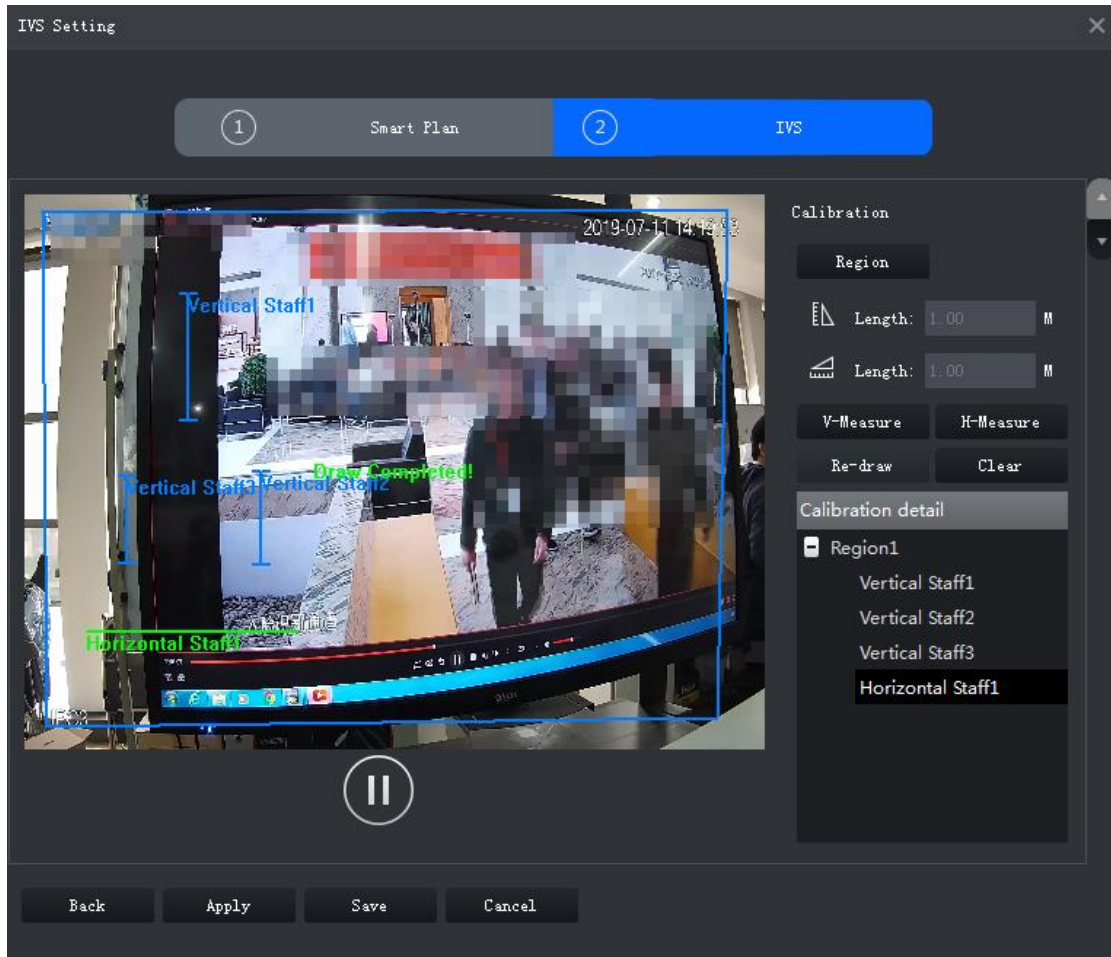
5.4.2.2 Calibrating Depth of Field

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.

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

Figure 5-66 Calibrating depth of field



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.

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 area 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.

5.4.2.3 Configuring Detection Region

Configure the detection zone of IVS.


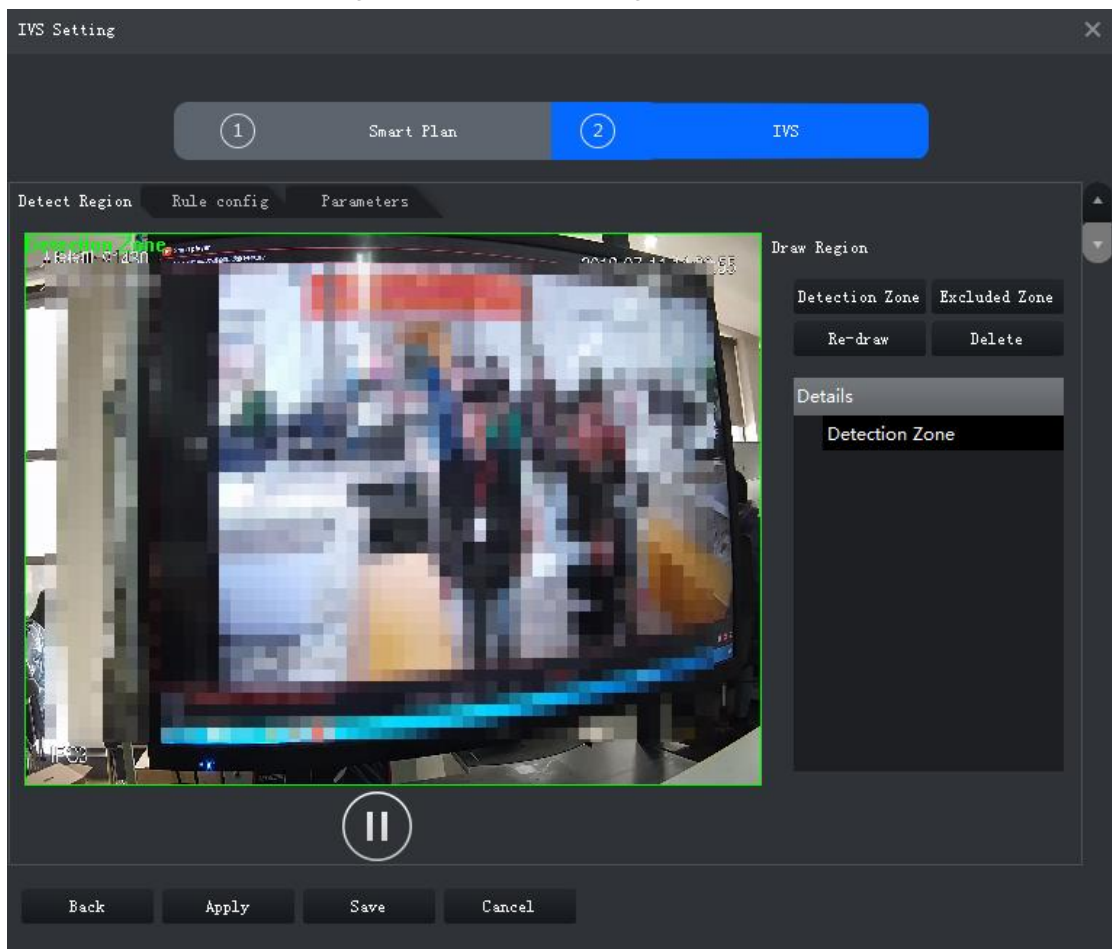
Step 1 Click .

Figure 5-67 Detection region



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.

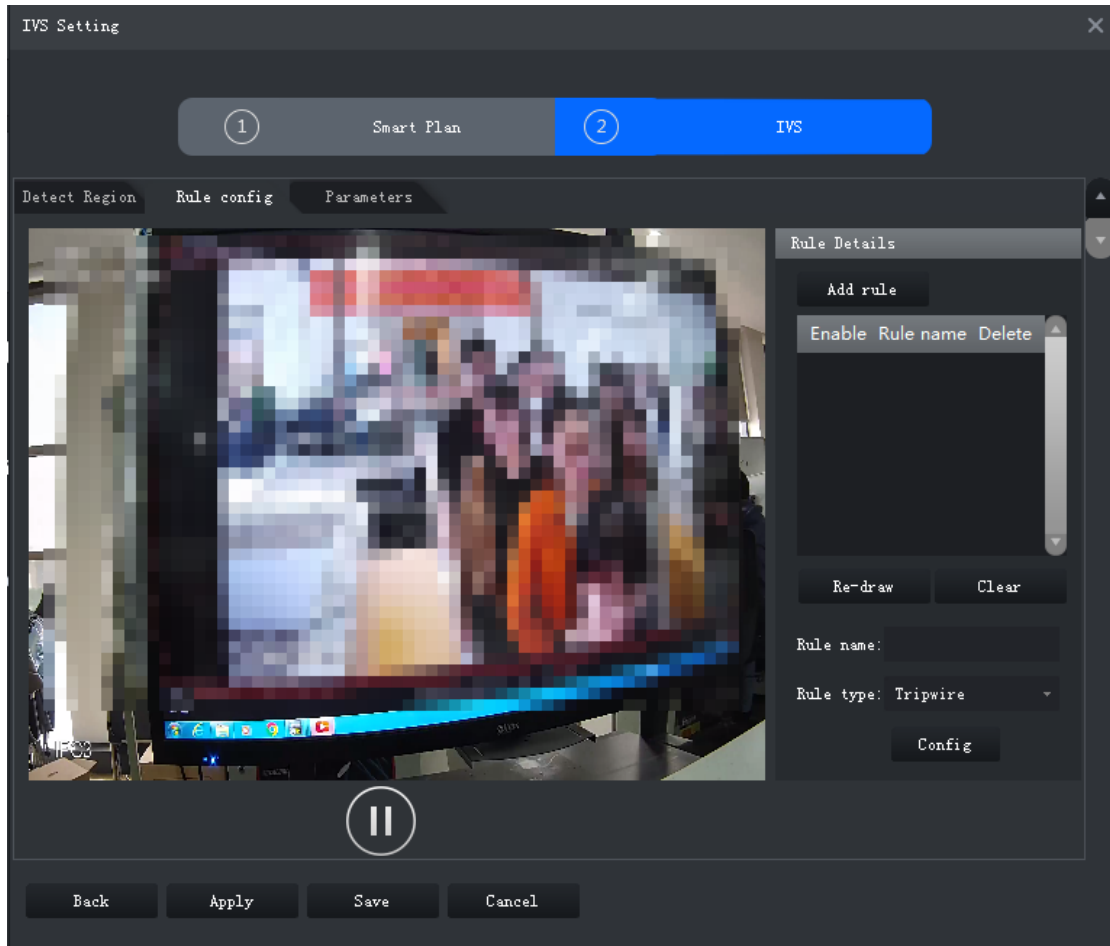


- Select the excluded zone and click **Re-draw** to draw a new excluded zone; select the detection zone and click **Re-draw** to draw a new detection zone and a new excluded zone.
- Select the excluded zone and click **Delete** to delete the excluded zone; select the detection zone and click **Delete** to delete the detection zone and excluded zone.

5.4.2.4 Configuring IVS Rule

Configure arming schedules and alarm linkages of IVS type including tripwire and intrusion. Click **Rule config**. The **Rule config** interface is displayed.

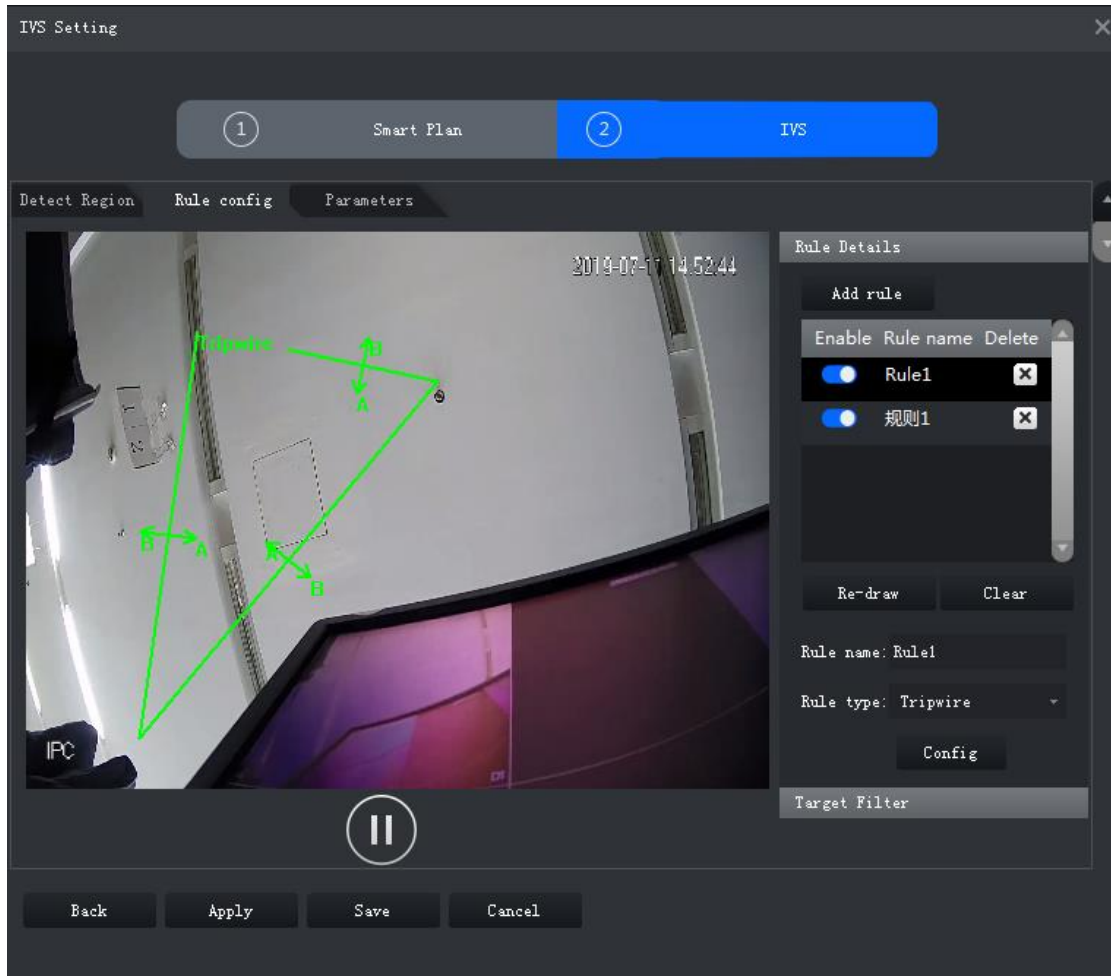
Figure 5-68 Rule configuration interface



5.4.2.4.1 Tripwire


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

Figure 5-69 Tripwire



Step 1 Click **Add rule**.

Step 2 Enable rule and modify the name and type.

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

Step 3 Draw a line on the video and right-click to finish.



Select an existing tripwire line and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage.

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

Figure 5-70 Set parameters

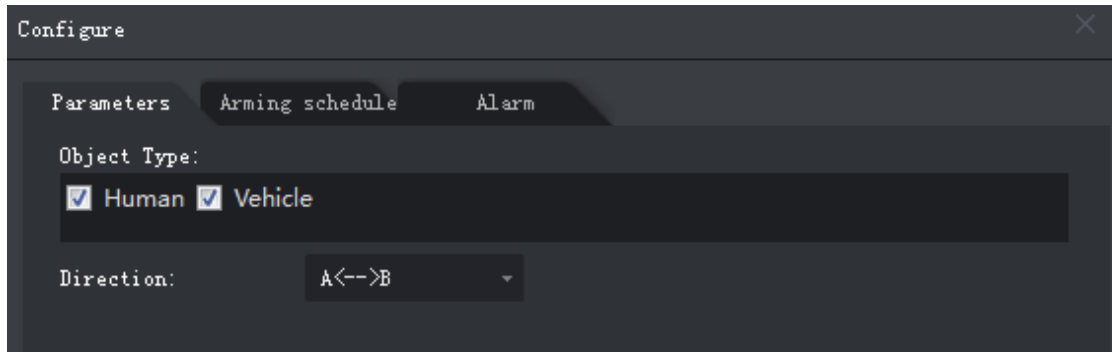


Table 5-28 Parameters

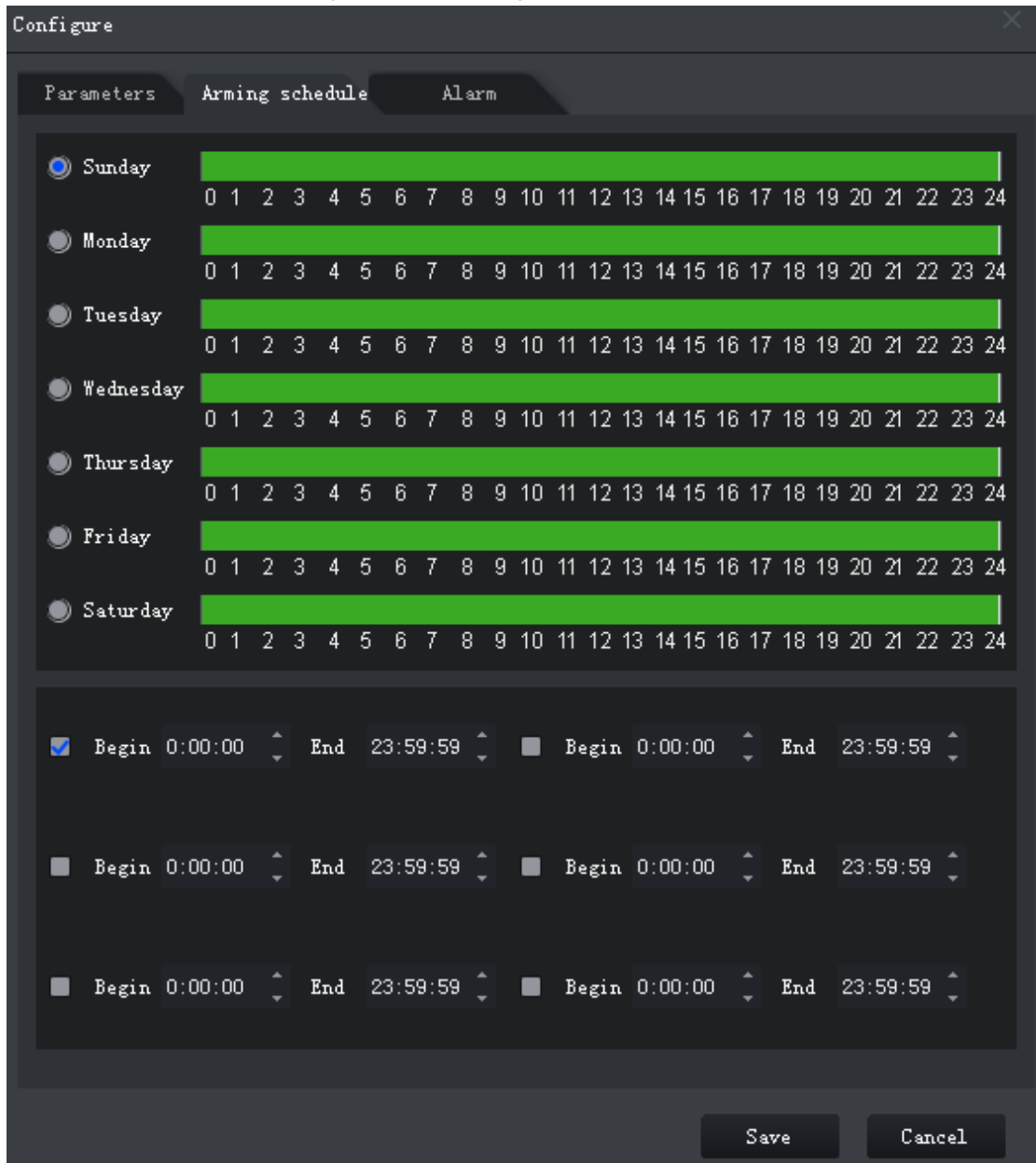
Parameter	Description
Object type	Only human or vehicle can trigger alarm.
Direction	When the target is moving in the rule direction, it is an intrusion. Directions include A→B, B→A and A↔B.

- 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 5-71 Arming schedule



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

Figure 5-72 Alarm linkage

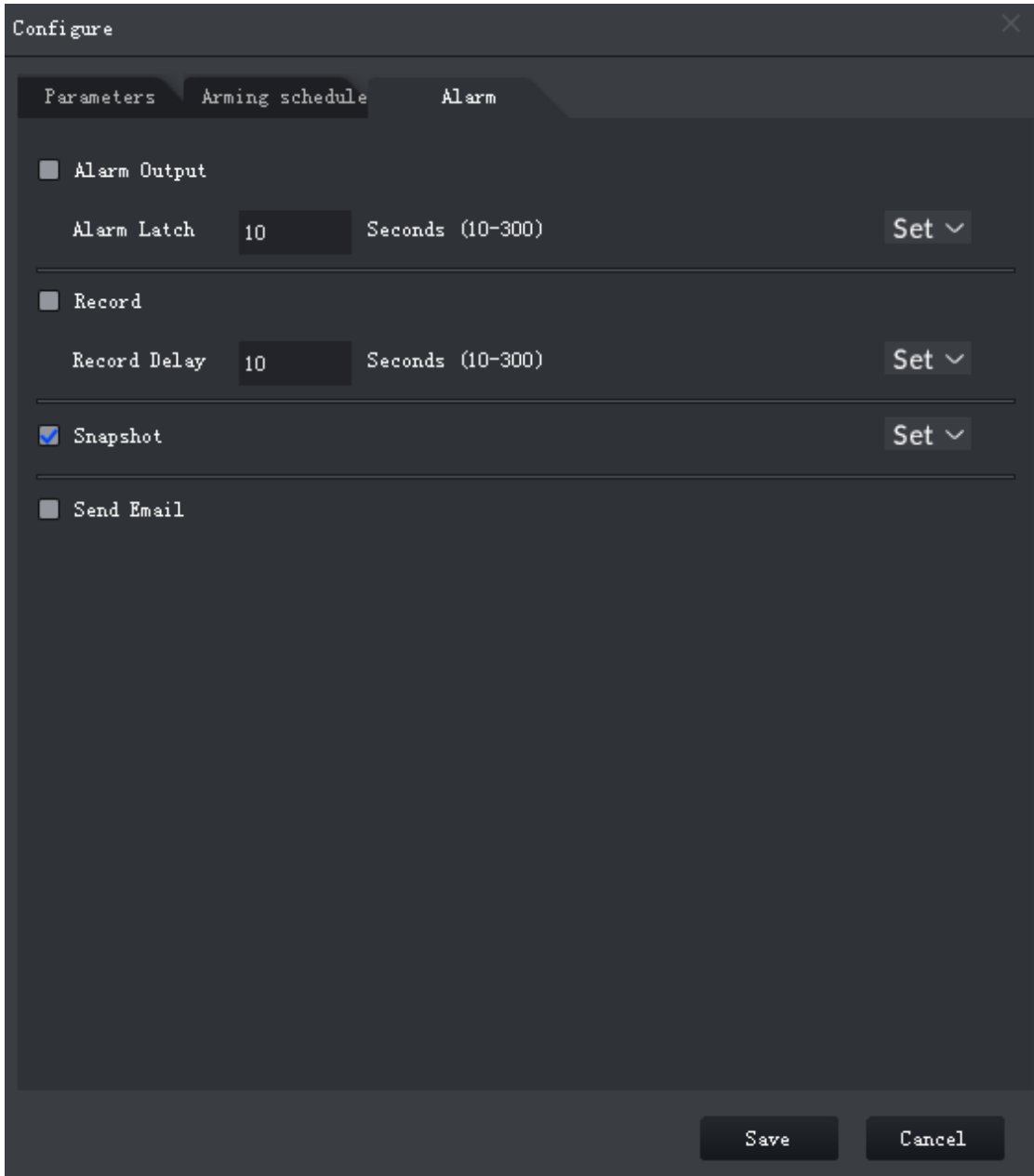





Table 5-29 Parameters

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.	Click Set next to Alarm Latch and select an alarm output channel.
Alarm latch	The alarm output action will delay stopping after the alarm event ends.	
Record	When an alarm happens, it will trigger video recording immediately.  It requires the device to have recording schedules already. See device manual	Click Set next to Record and select an alarm output channel.

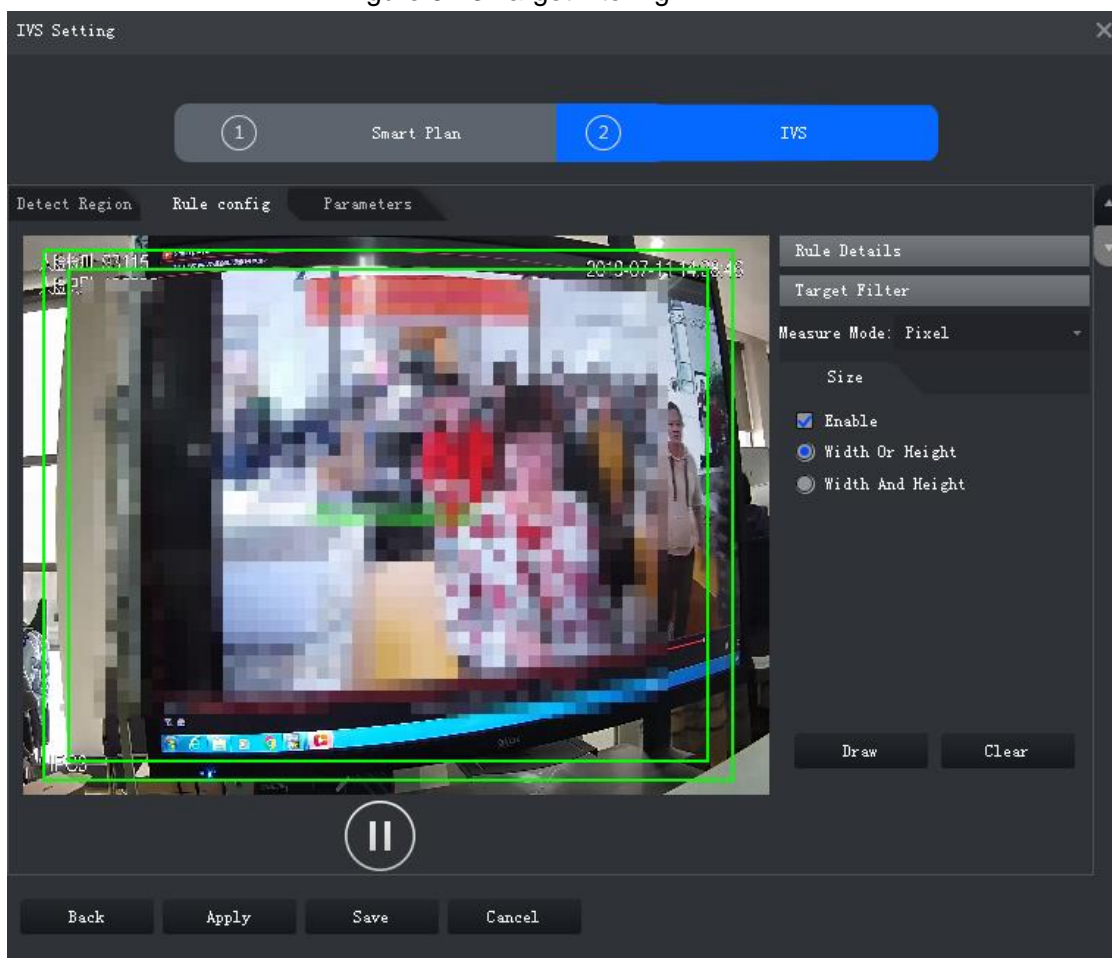
Parameter	Description	
	for detailed instruction.	
Record delay	Video recording delays stopping for a while after the alarm event ends.	
snapshot	<p>The system will take snapshots automatically when an alarm happens.</p>  <p>It requires the device to have snapshot schedules already. See device manual for detailed instruction.</p>	Click Set next to Snapshot to select the snapshot channel.
Send email	<p>The system will send an email to the related mail address when an alarm happens.</p>  <p>It requires the device to have email configured already. See device manual for detailed instruction.</p>	

4) Click **Save**.

Step 5 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 5-73 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.



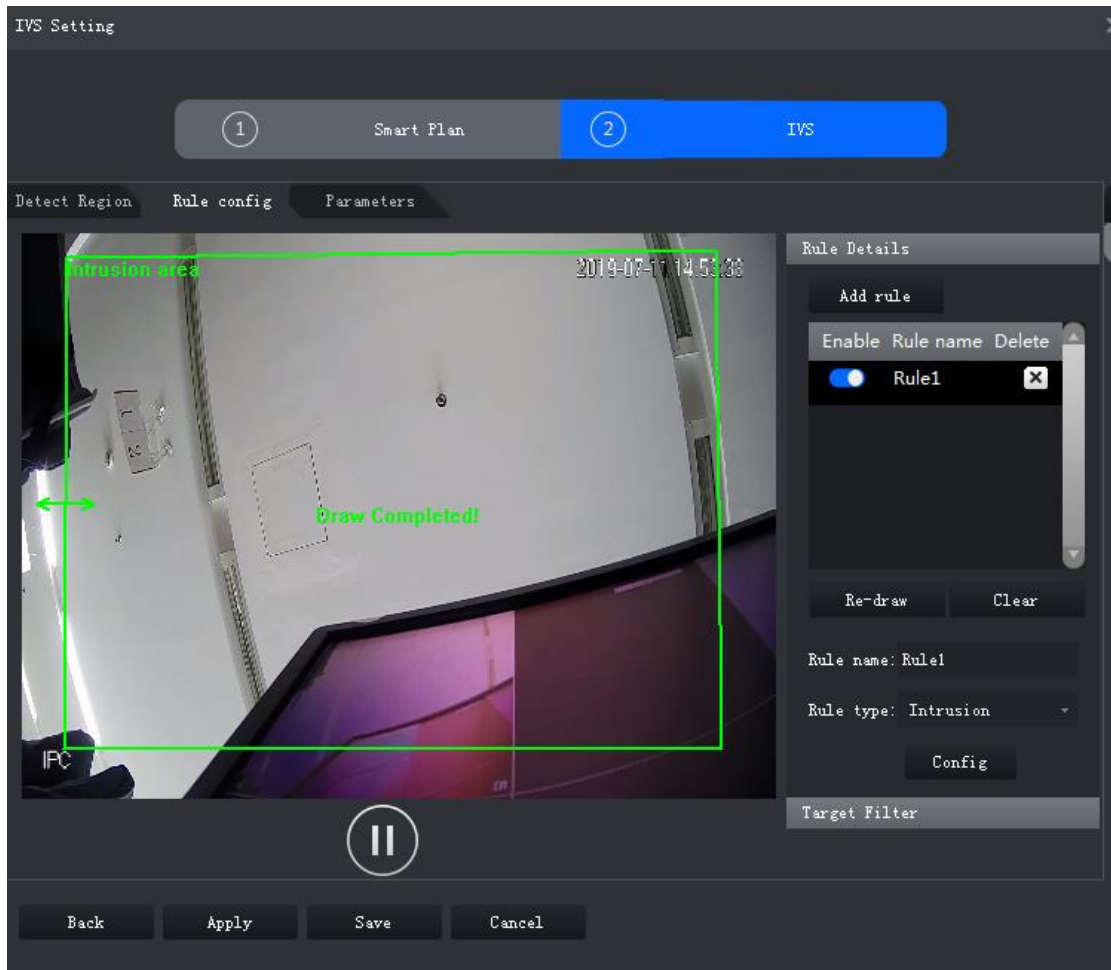
Select filtering frame, and click **Clear** to delete it.

Step 6 Click **Apply**.

5.4.2.4.2 Intrusion


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

Figure 5-74 Intrusion



Step 1 Click **Add rule**.

Step 2 Enable rule and modify the name and type.

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

Step 3 Draw a detection zone on the video and right-click to finish.



Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "5.4.2.4.1 Tripwire."

Set intrusion detection parameters.

Figure 5-75 Set parameters



Table 5-30 Parameters

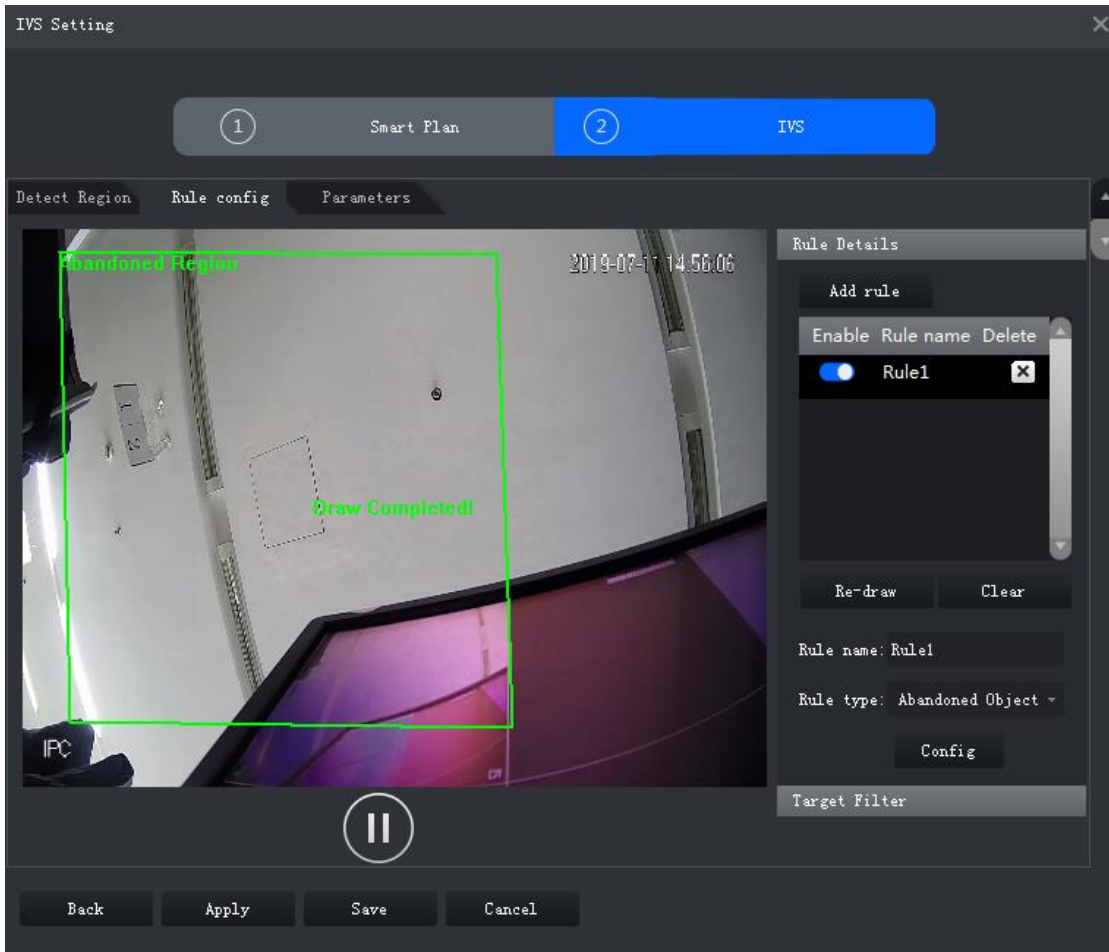
Parameter	Description
Object type	Only human or vehicle can trigger alarm.
Target actions	Appear and cross
Direction	When a crossing-zone action is selected, Direction setting will be effective. Direction includes entering zone, leaving zone and two-way.

Step 5 Click **Apply**.

5.4.2.4.3 Abandoned Object


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

Figure 5-76 Abandoned Object



Step 1 Click **Add rule**.

Step 2 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 dropdown list of **Rule type**.

Step 3 Draw a detection zone on the video and right-click to finish.



Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "5.4.2.4.1 Tripwire."

Set parameters.

Figure 5-77 Set parameters

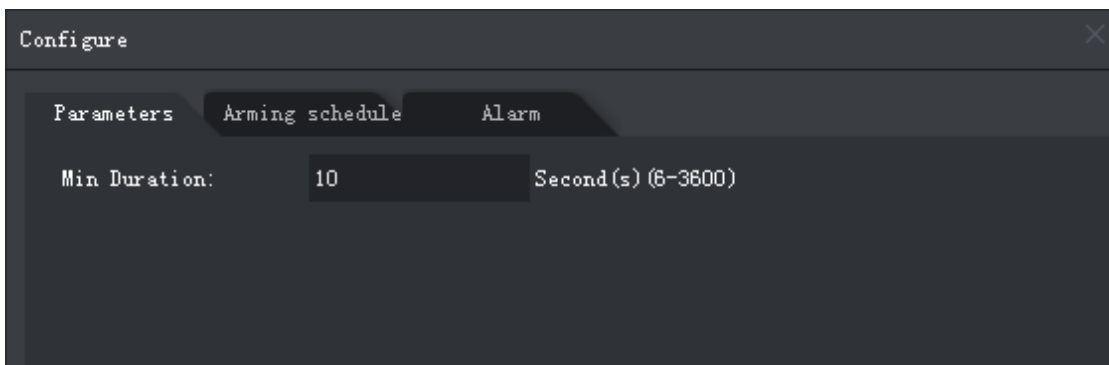


Table 5-31 Parameters

Parameter	Description
Minimum duration	The minimum time period between appearing and alarm triggering.

Step 5 Click **Apply**.

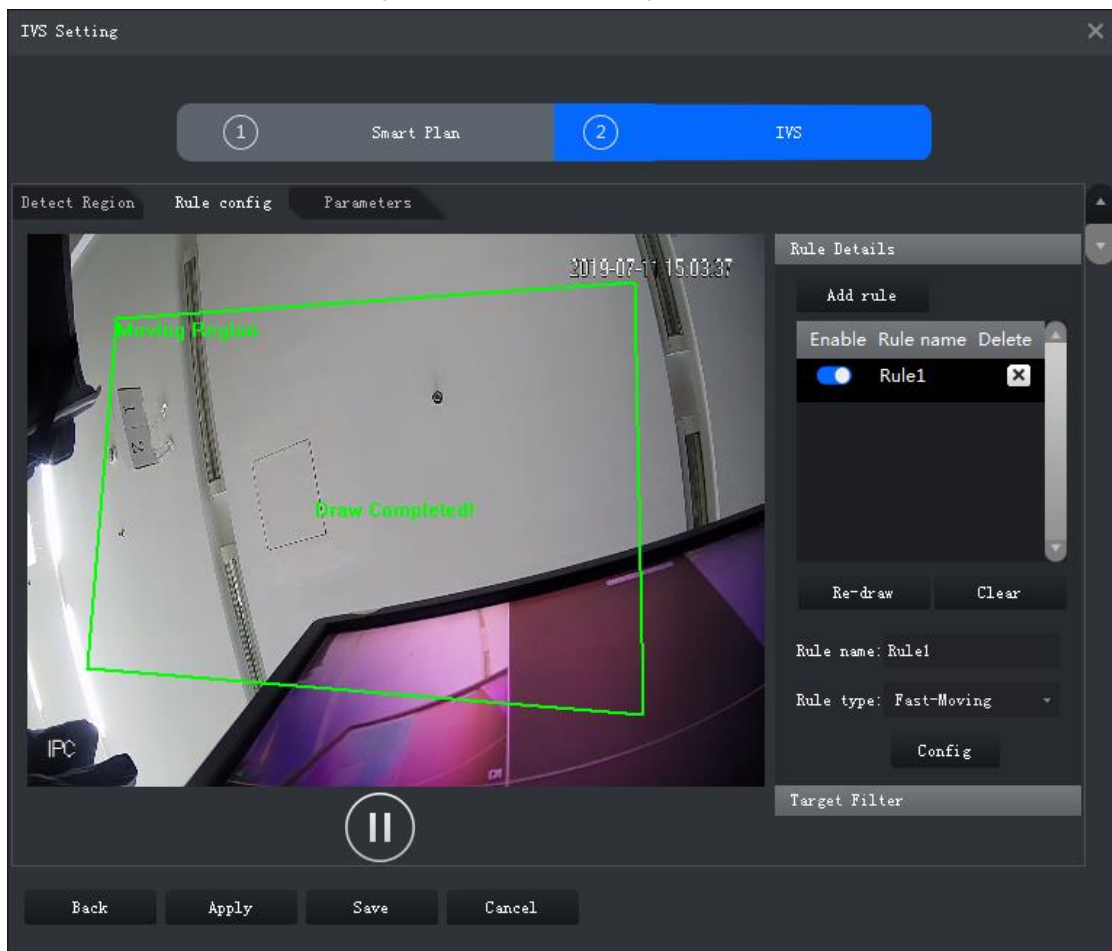
5.4.2.4.4 Fast Moving

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 you have completed the calibration configuration. See "5.4.2.2 Calibrating Depth of Field for details."

Figure 5-78 Fast moving



Step 1 Click **Add rule**.

Step 2 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 dropdown list of **Rule type**.

Step 3 Draw a detection zone on the video and right-click to finish.



Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "5.4.2.4.1 Tripwire."

Figure 5-79 Set parameters

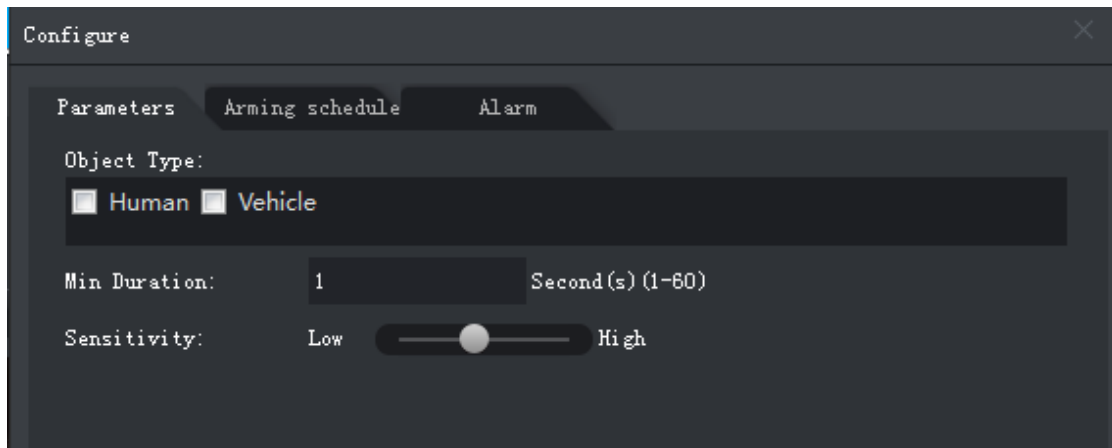


Table 5-32 Parameters

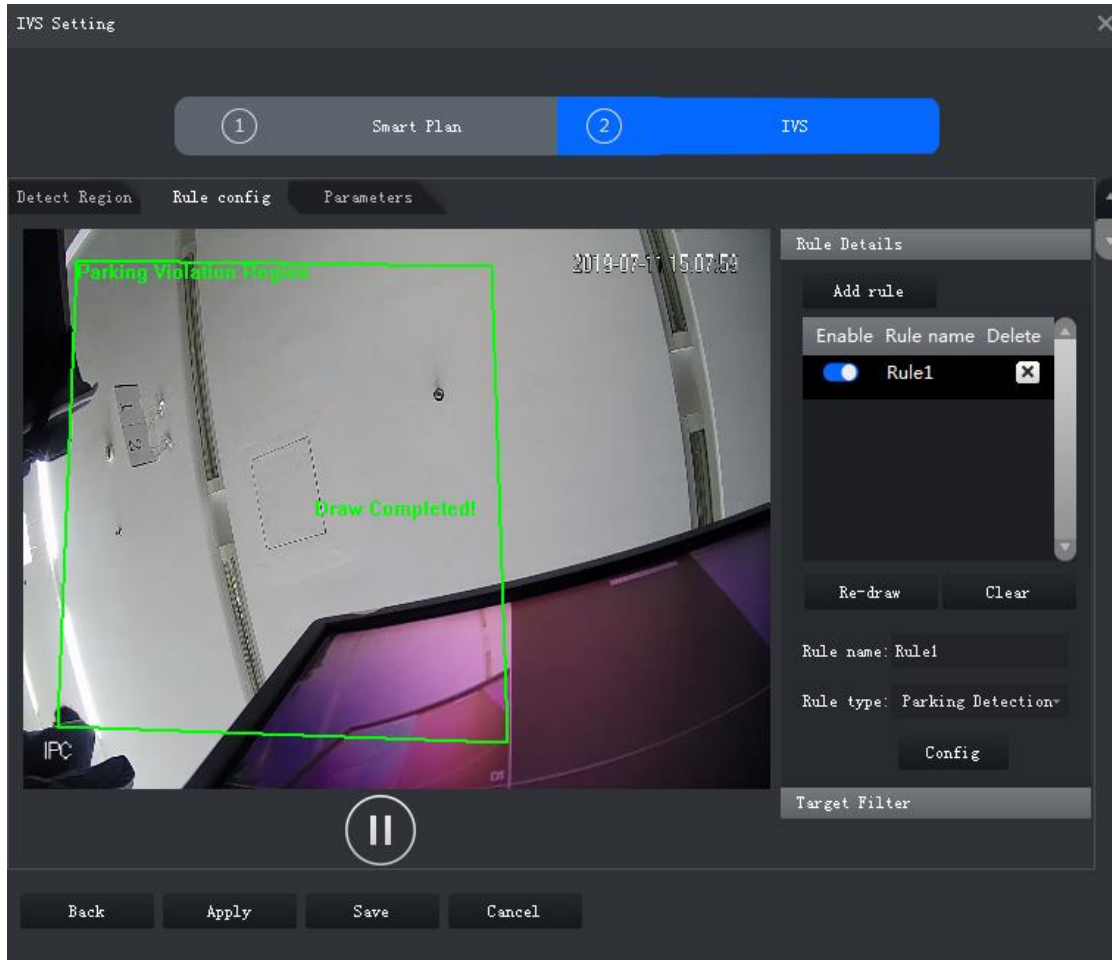
Parameter	Description
Object type	Only human or vehicle can trigger alarm.
Minimum duration	The minimum duration of fast moving in the detection zone.
Sensitivity	It is recommended to keep the default value.

Step 5 Click **Apply**.

5.4.2.4.5 Parking Detection


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

Figure 5-80 Parking detection



Step 1 Click **Add rule**.

Step 2 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 dropdown list of **Rule type**.

Step 3 Draw a detection zone on the video and right-click to finish.



Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "5.4.2.4.1 Tripwire."

Figure 5-81 Set parameters

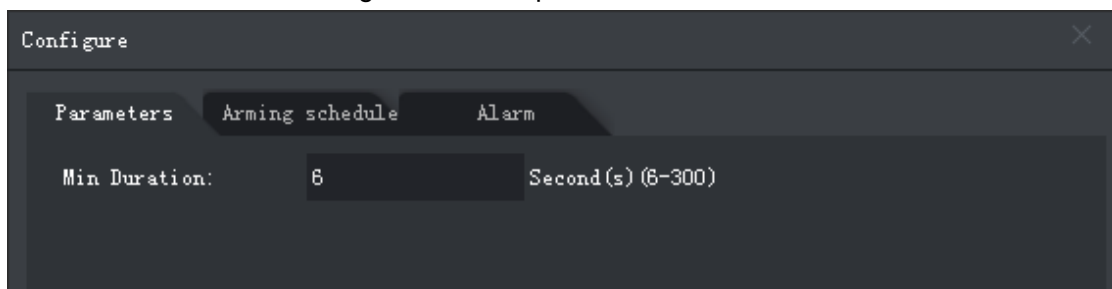


Table 5-33 Parameters

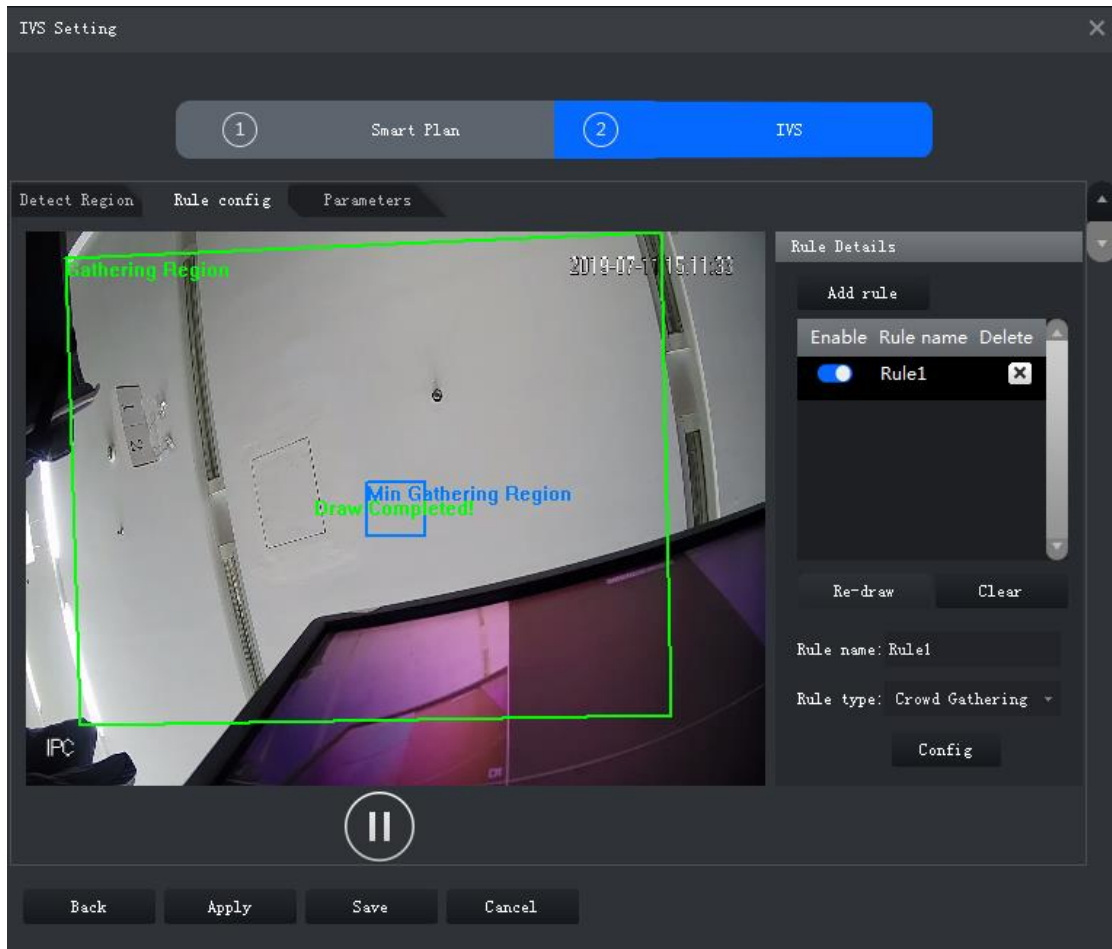
Parameter	Description
Minimum duration	The minimum time duration from parking to alarm triggering.

Step 5 Click **Apply**.

5.4.2.4.6 Crowd Gathering


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

Figure 5-82 Crowd gathering



Step 1 Click **Add rule**.

Step 2 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 dropdown list of **Rule type**.

Step 3 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.



Select an existing zone or the minimum gathering region and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "5.4.2.4.1 Tripwire."

Figure 5-83 Set parameters

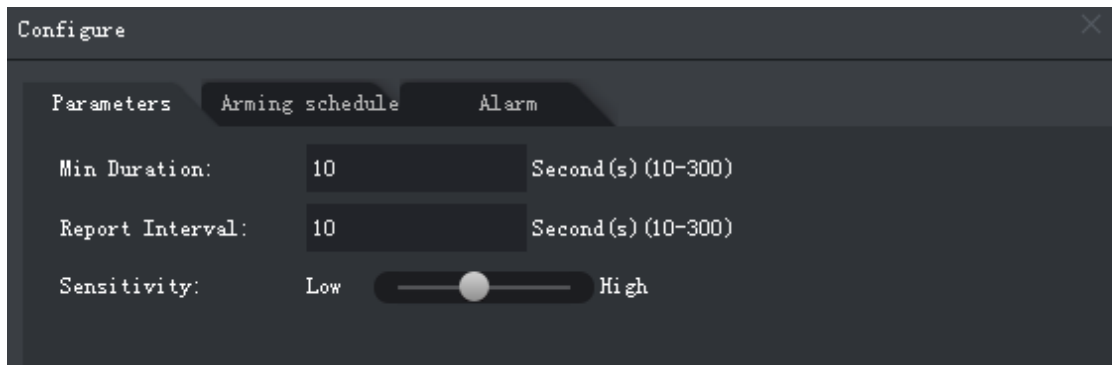


Table 5-34 Parameters

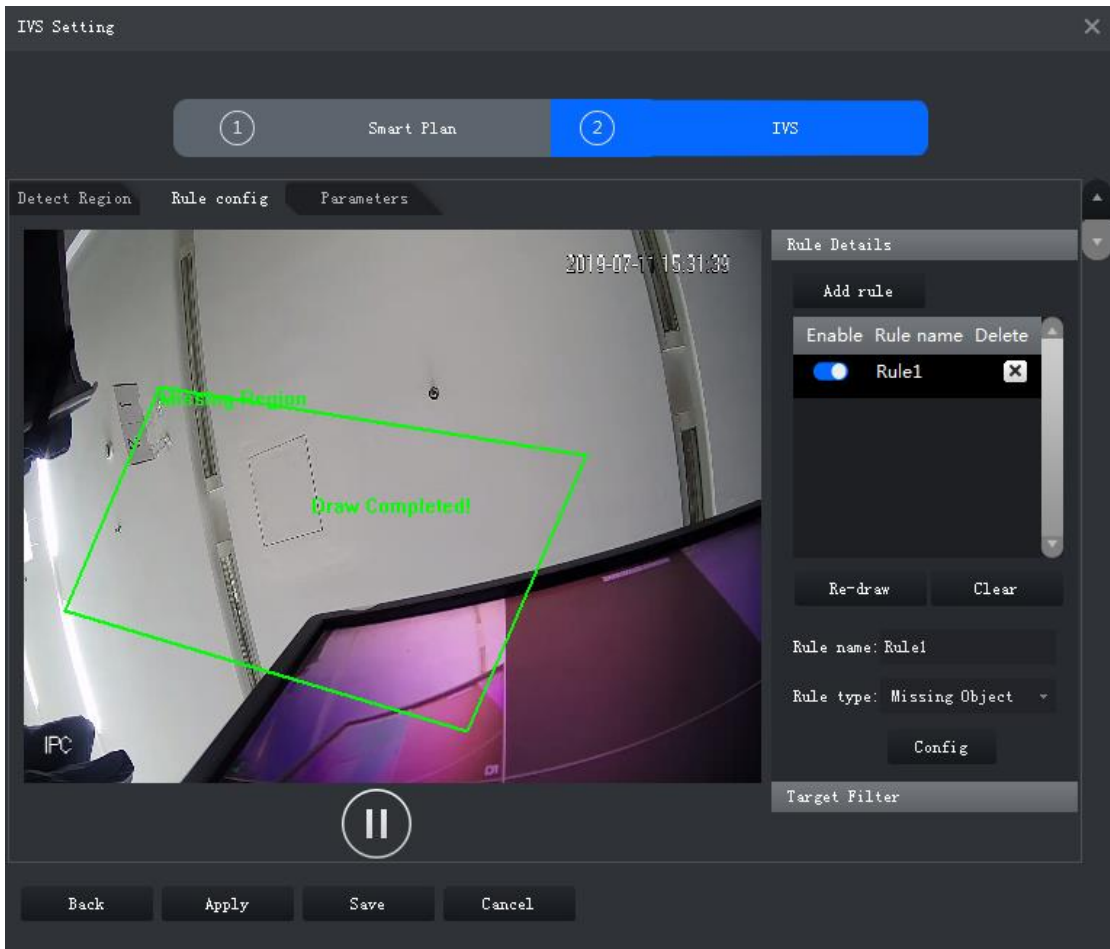
Parameter	Description
Minimum duration	The minimum duration from the time crowd gathering being detected to alarm triggering
Report interval	If the event still exists after the first alarm, system will trigger more alarms by the preset alarm interval.
Sensitivity	It is recommended to keep the default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

Step 5 Click **Apply**.

5.4.2.4.7 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.

Figure 5-84 Missing object



Step 1 Click **Add rule**.

Step 2 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 dropdown list of **Rule type**.

Step 3 Draw a detection zone on the video and right-click to finish.



Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "5.4.2.4.1 Tripwire."

Figure 5-85 Set parameters

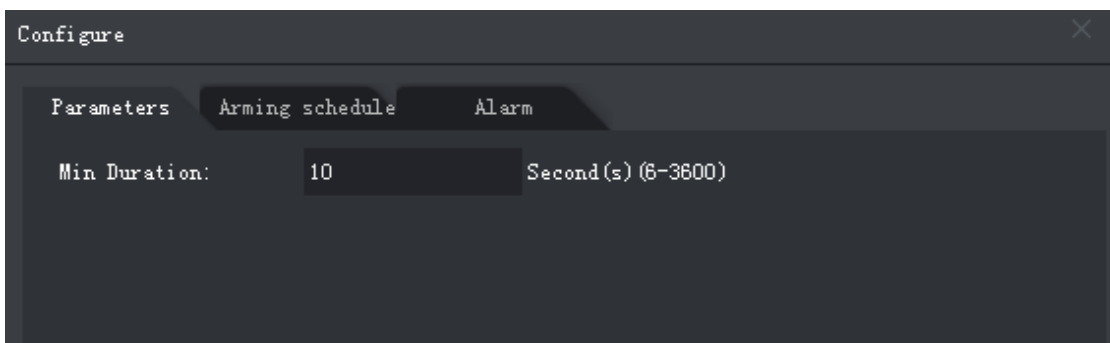


Table 5-35 Parameters

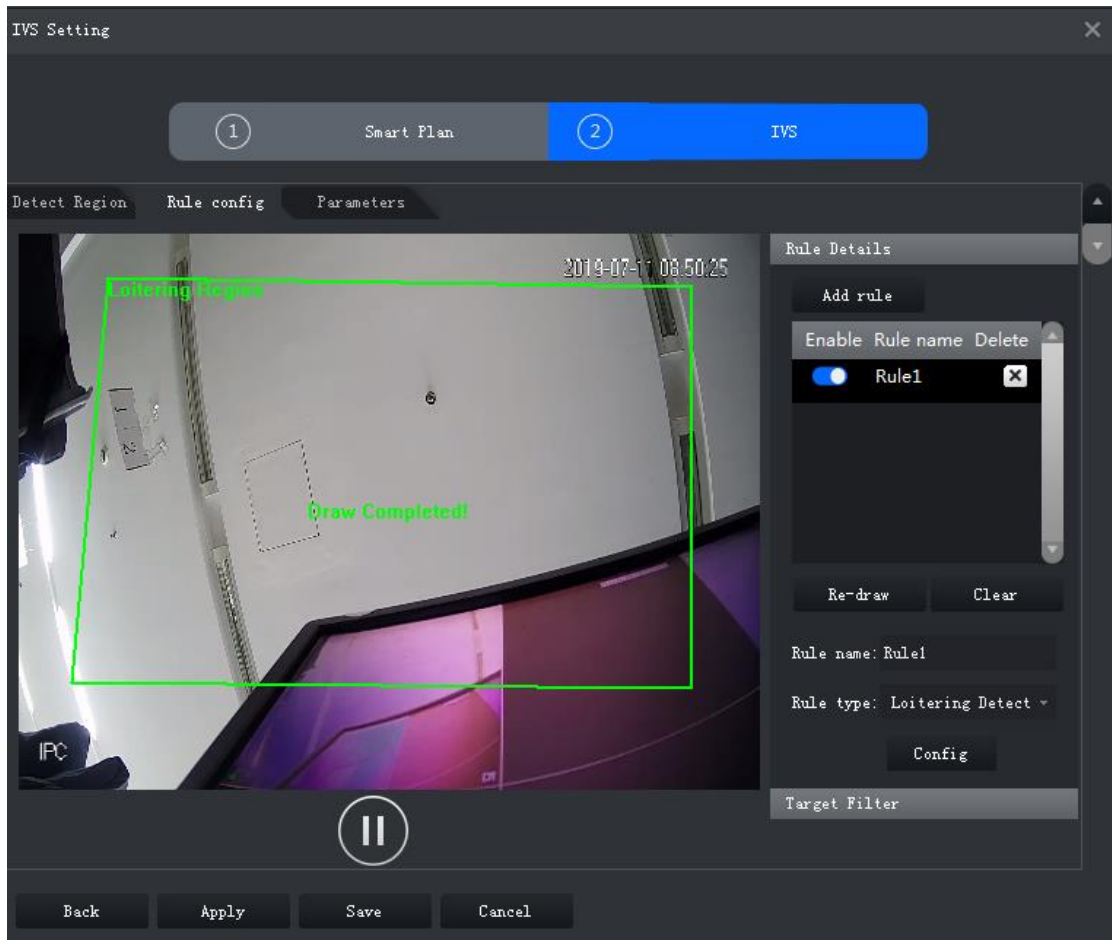
Parameter	Description
Minimum duration	The minimum time duration from object disappearing to alarm triggering.

Step 5 Click **Apply**.

5.4.2.4.8 Loitering Detection


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

Figure 5-86 Loitering detection



Step 1 Click **Add rule**.

Step 2 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 dropdown list of **Rule type**.

Step 3 Draw a detection zone on the video and right-click to finish.



Select an existing zone and click **Clear** to delete it or **Re-draw** to draw a new one.

Step 4 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame.

Figure 5-87 Set parameters

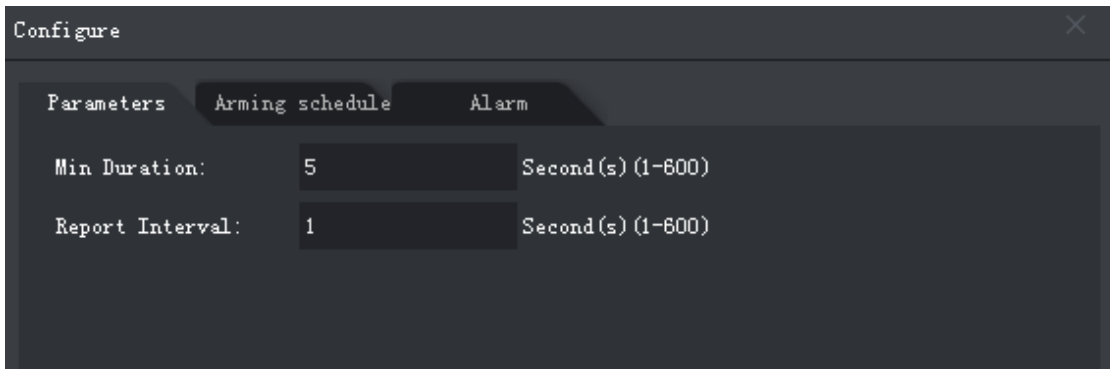


Table 5-36 Parameters

Parameter	Description
Minimum 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.

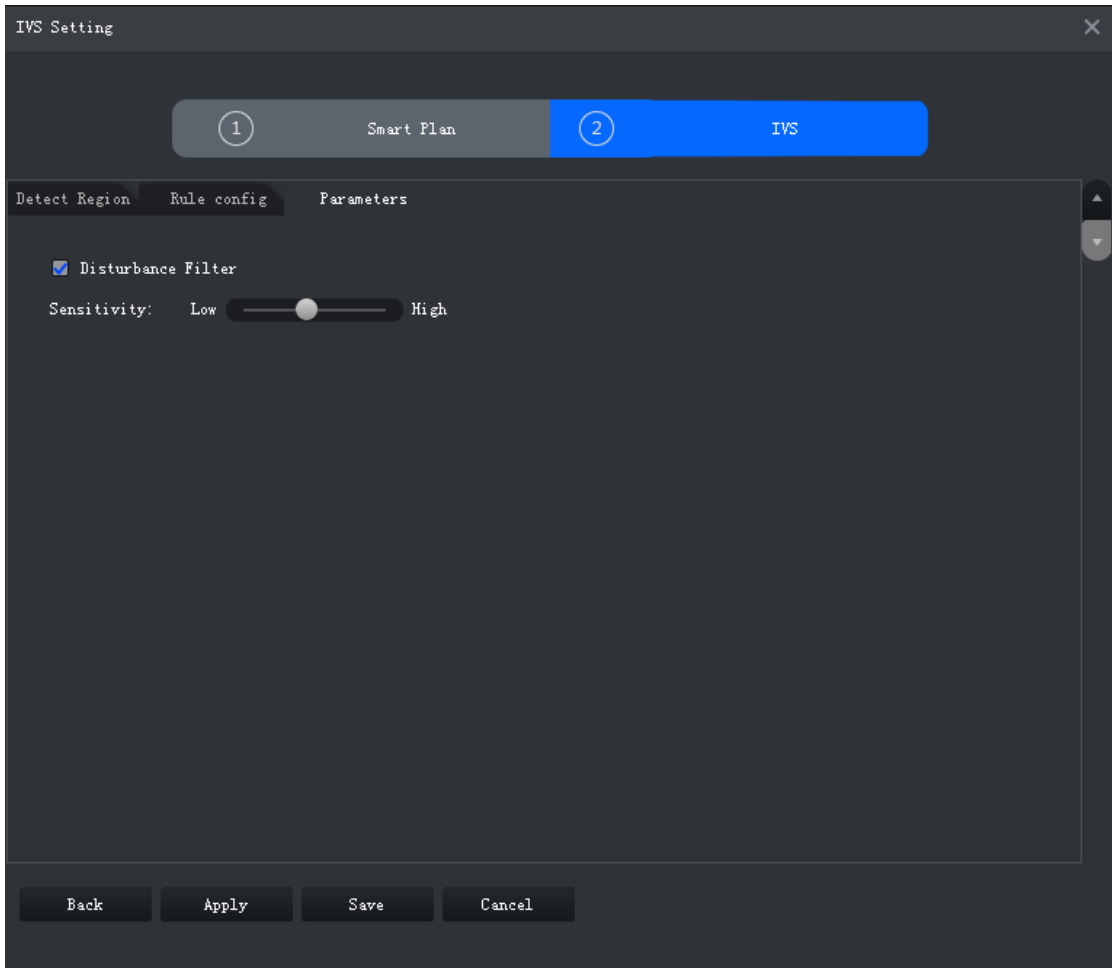
Step 5 Click **Apply**.

5.4.2.5 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.

Figure 5-88 Parameters



Step 2 Set parameters.

Table 5-37 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**.

5.4.3 Face Detection

This function supports detecting human targets in the defined zone. It supports capturing and recognizing human face, and extracting face features including gender, age, expression and glasses.

5.4.3.1 Enabling Face Detection

Step 1 Go to the **Intelligent Analyze** interface.

Step 2 Click  in the smart plan interface to select face detection.

When the icon is displayed in the white frame, it means the smart plan is selected. If another smart plan, which is conflicting with face detection, is selected already, click


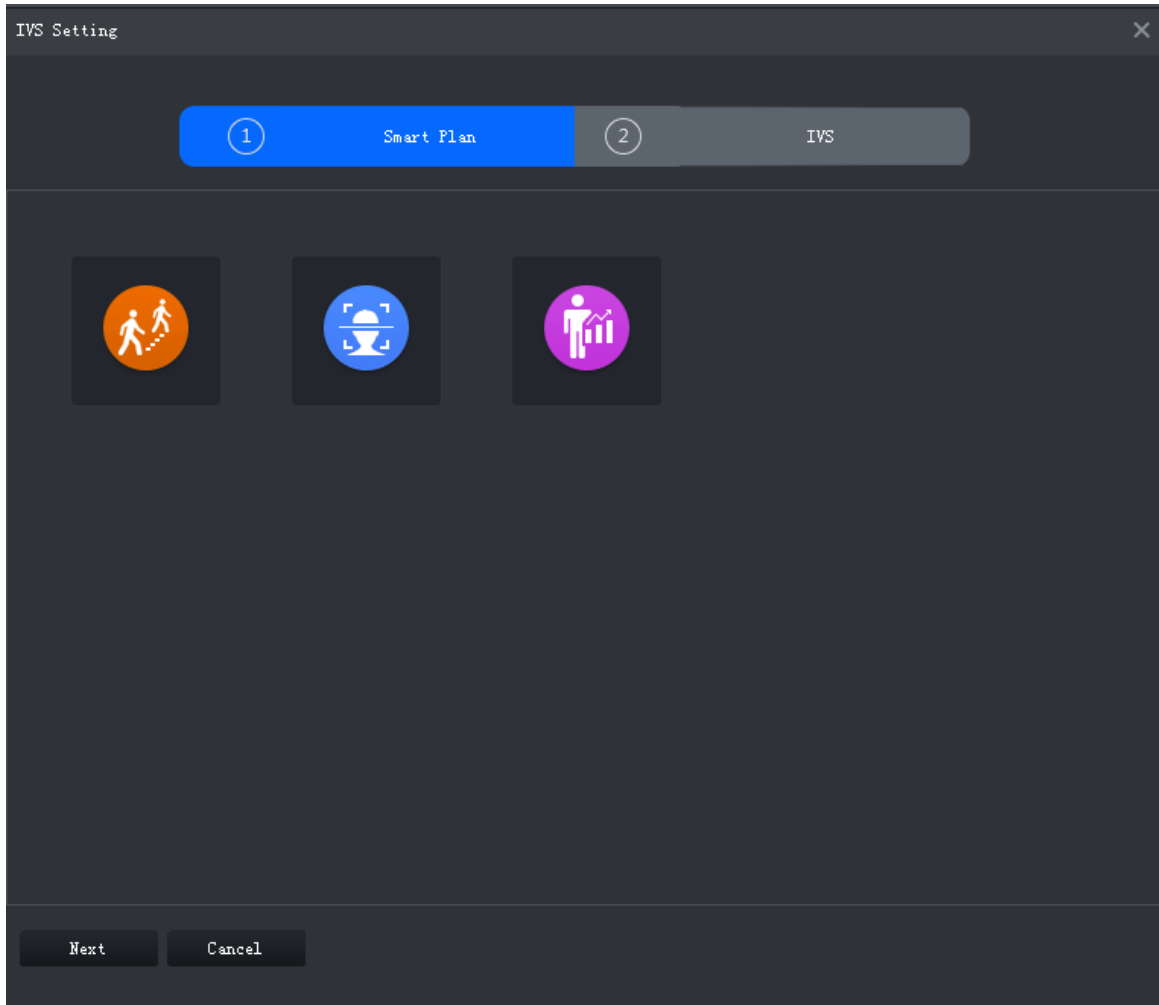
that smart plan icon to deselect it and then click  to select face detection.

Figure 5-89 Smart plan



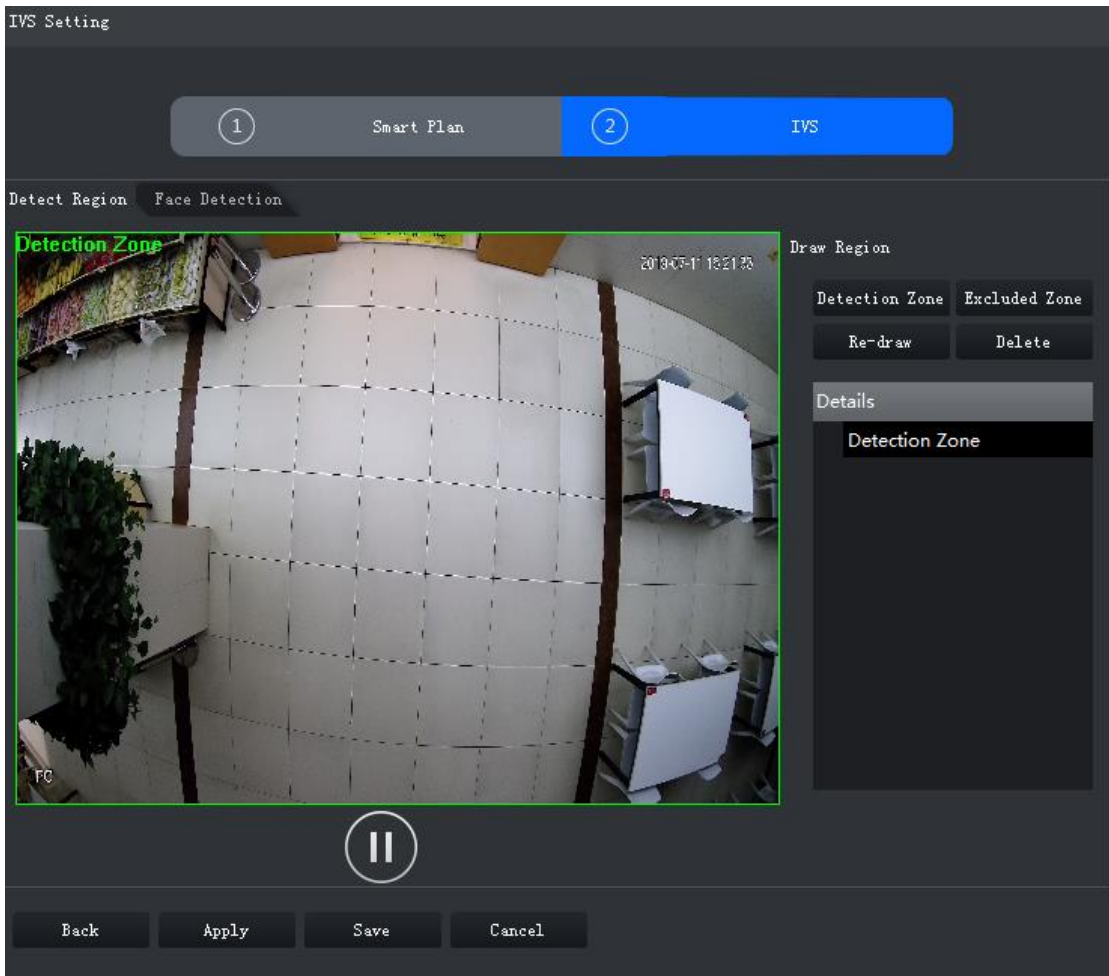
Step 3 Click **Next**.

The **IVS Setting** interface is displayed.

5.4.3.2 Configuring Detection Region

Configure the detection region.

Figure 5-90 Detection region



Step 4 Click **Detect Region** tab in the IVS interface.

Step 5 Click **Detection Zone** and then draw the frame of the detection region on the video and right-click to finish.

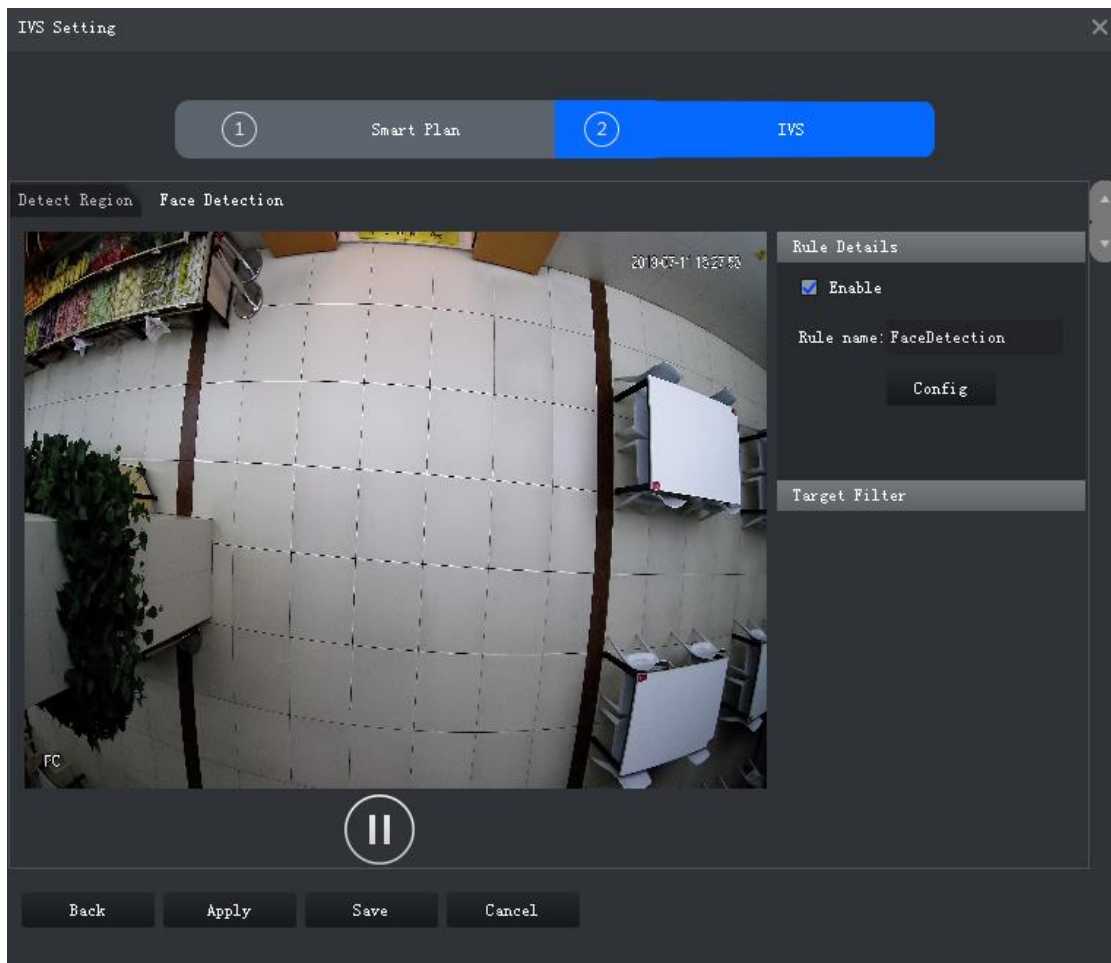
Step 6 Click **Excluded Zone** and then draw the frame of the zone on the video and right-click to finish.



- Select the excluded zone and click **Re-draw** to draw a new excluded zone; select detection region and click **Re-draw** to draw a new detection region and a new excluded zone.
- Select the excluded zone and click **Delete** to delete the excluded zone; select detection region and click **Delete** to delete the detection region and excluded zone.

5.4.3.3 Configuring Face Detection Rule

Figure 5-91 Face detection



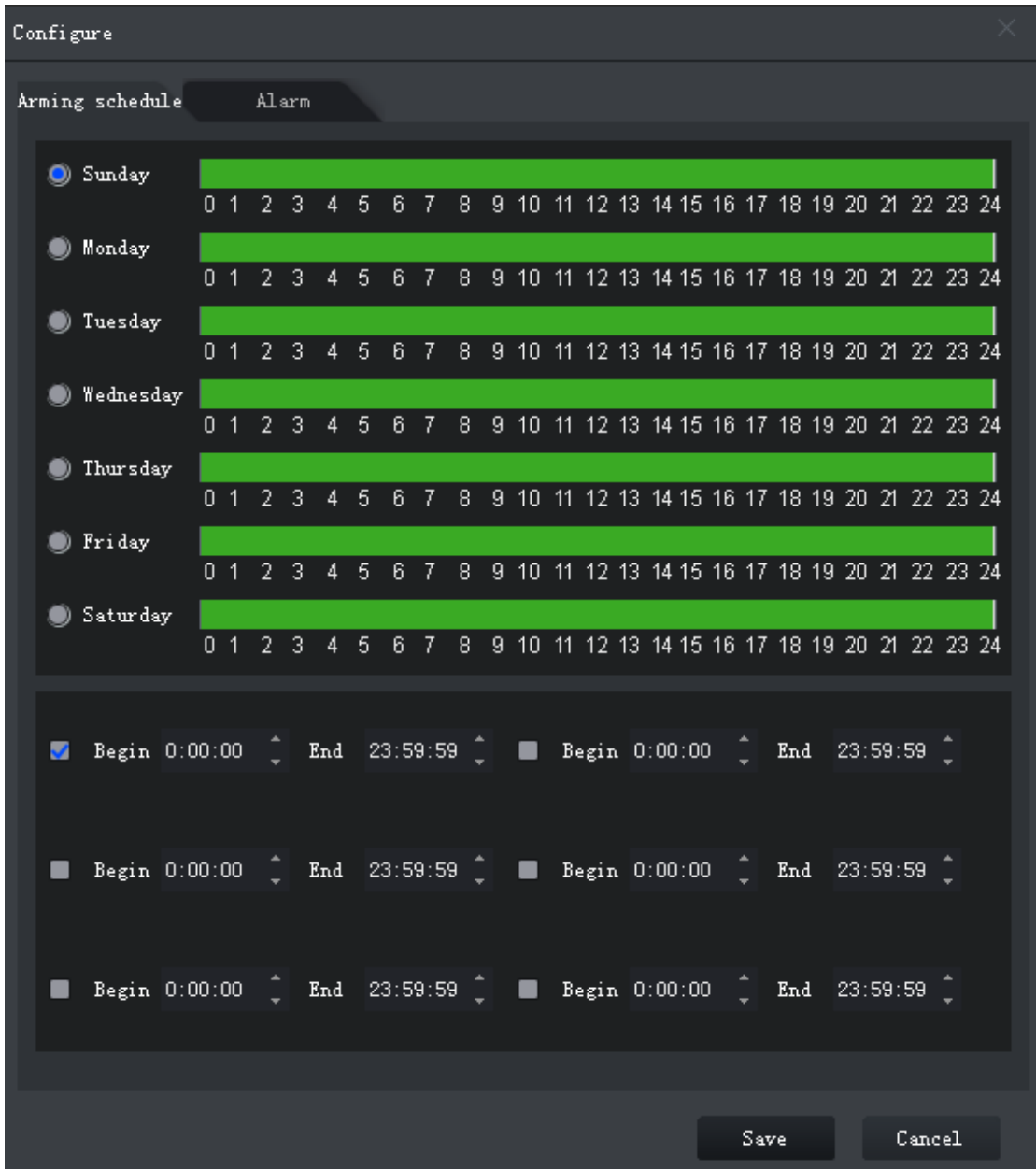
Step 1 Select the check box of **Enable** to enable face detection.

Step 2 Modify rule name.

Step 3 Configuring arming schedule and alarm linkage.

1) Click **Config**.

Figure 5-92 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 5-93 Alarm

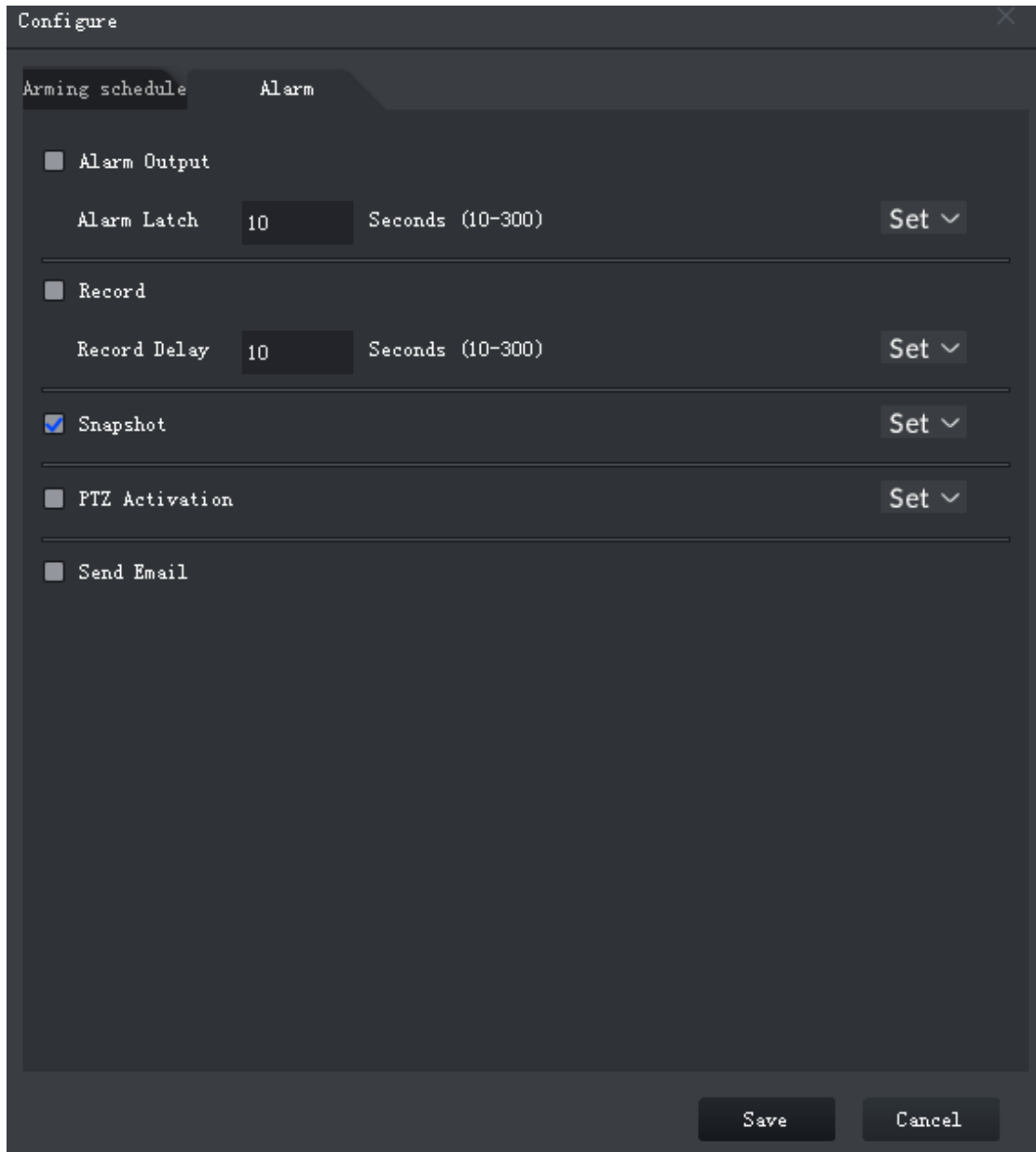





Table 5-38 Parameters

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.	Click Set next to Alarm Latch and select an alarm output channel.
Alarm latch	The alarm output action will delay stopping after the the alarm event ends.	
Record	When an alarm happens, it will trigger auto video recording immediately.  To get video records, set the recording schedule in advance. See device manual for detailed instruction.	Click Set next to Record to select the recording channel.

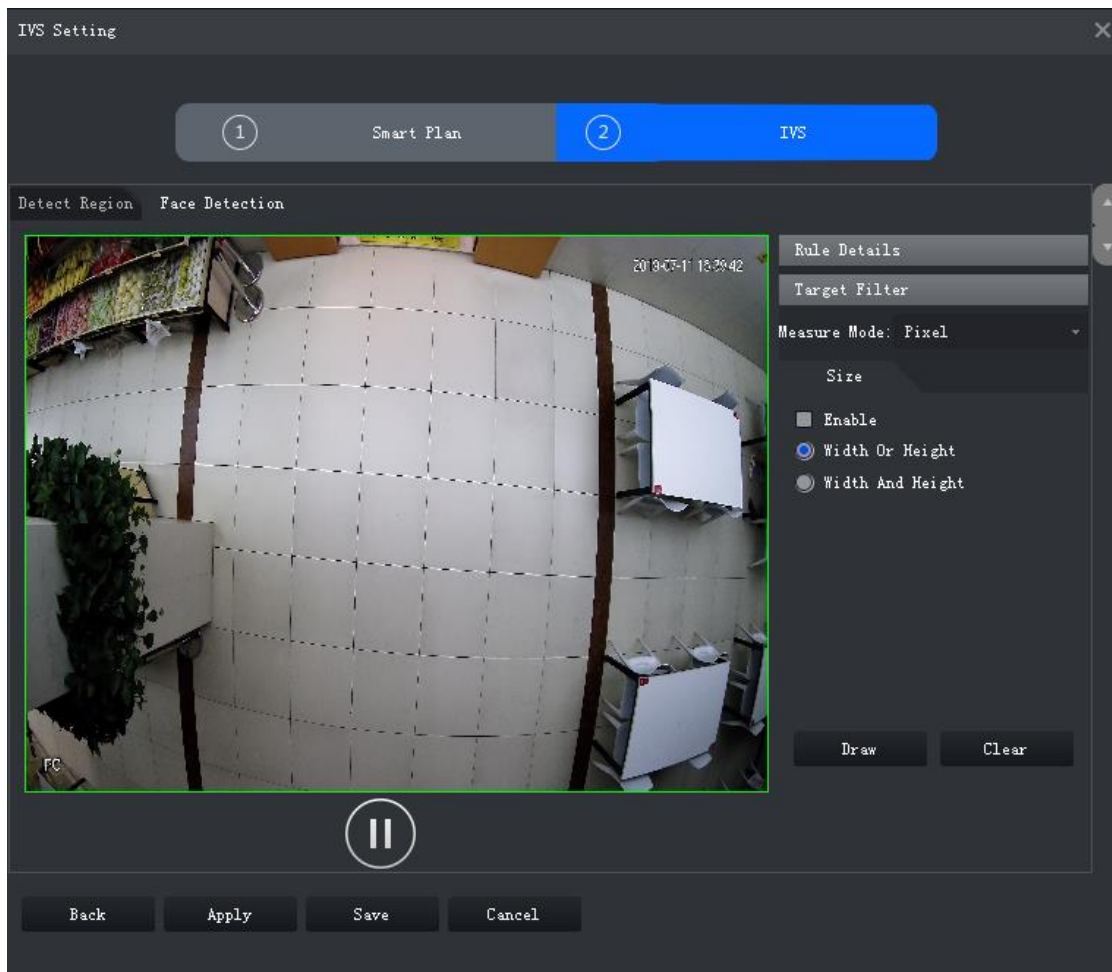
Parameter	Description	
Record delay	Video recording delays stopping for a while after the alarm event ends.	
Snapshot	<p>The system will take snapshots automatically when an alarm happens.</p>  <p>It requires the device to have snapshot schedules already. See device manual for detailed instruction.</p>	Click Set next to Snapshot to select the snapshot channel.
Send email	<p>The system will send an email to the related mail address when an alarm happens.</p>  <p>It requires the device to have email configured already. See device manual for detailed instruction.</p>	None

4) Click **Save**.

Step 4 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 setting value, it can trigger alarms.

Figure 5-94 Target filtering



1) Select **Enable**.

- 2) Select a filtering method.
Two filtering methods:
 - ◇ **Width or Height** means the target will be kept when either width or height meets the requirement.
 - ◇ **Width and Height** means the target will be kept only when both width and height meet the requirement.
- 3) Click **Draw** and draw a filtering frame on the video.
Select filtering frame and drag the four angles adjust the size.



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


Step 5 Click **Save**.

5.4.4 People Counting

Count the number of people entry and exit.

5.4.4.1 Enabling People Counting

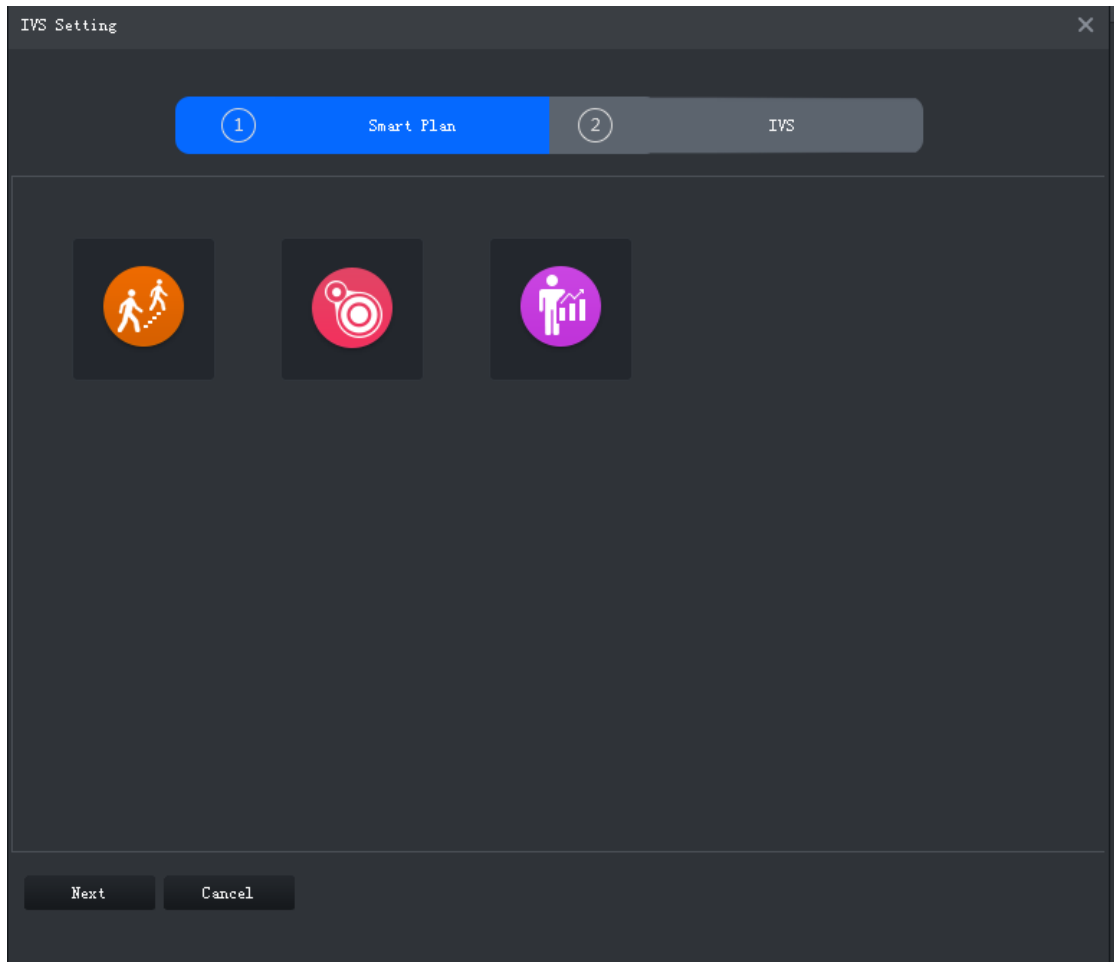
Step 1 Go into the **Intelligent Analyse** interface.

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.

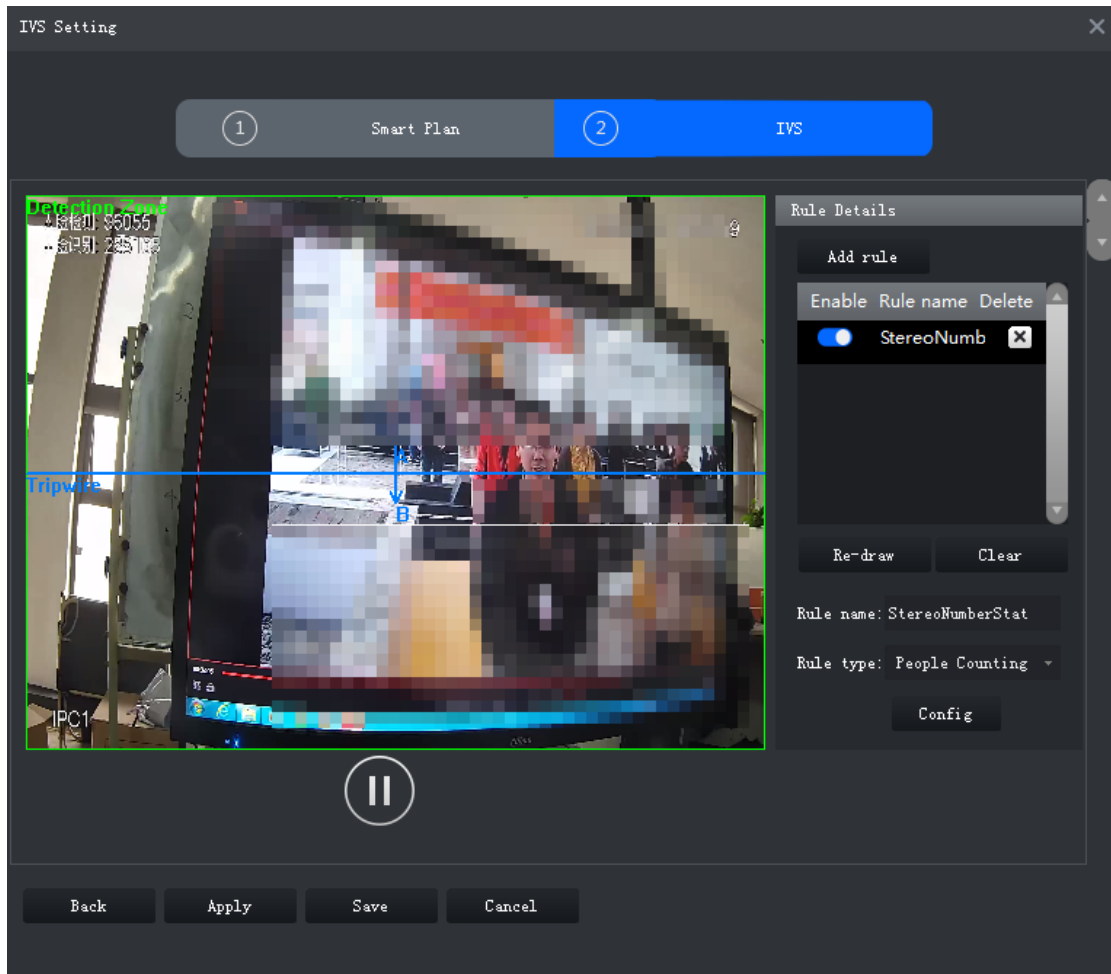
Figure 5-95 Smart plan



- Step 3** Click **Next**.
The **IVS Setting** interface is displayed.

5.4.4.2 Configuring People Counting Rule

Figure 5-96 People counting



Step 1 Click **Add rule**.

Step 2 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 dropdown 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 3 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 4 Set parameters, arming schedule and alarm linkage.

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

Figure 5-97 Set parameters (People counting)

The screenshot shows a 'Configure' dialog box with three tabs: 'Parameters', 'Arming schedule', and 'Alarm'. The 'Parameters' tab is active. It contains the following fields and controls:

Field	Value	Unit / Range
Min Height:	50	cm (0-200)
Max Height:	220	cm (0-300)
Enter No. :	0	
Exit No. :	0	
Remaining No. :	0	
Sensitivity:	Low	Slider (Low to High)

At the bottom of the dialog box, there are two buttons: 'Save' and 'Cancel'.

Figure 5-98 Set parameters (ManNumDetection)

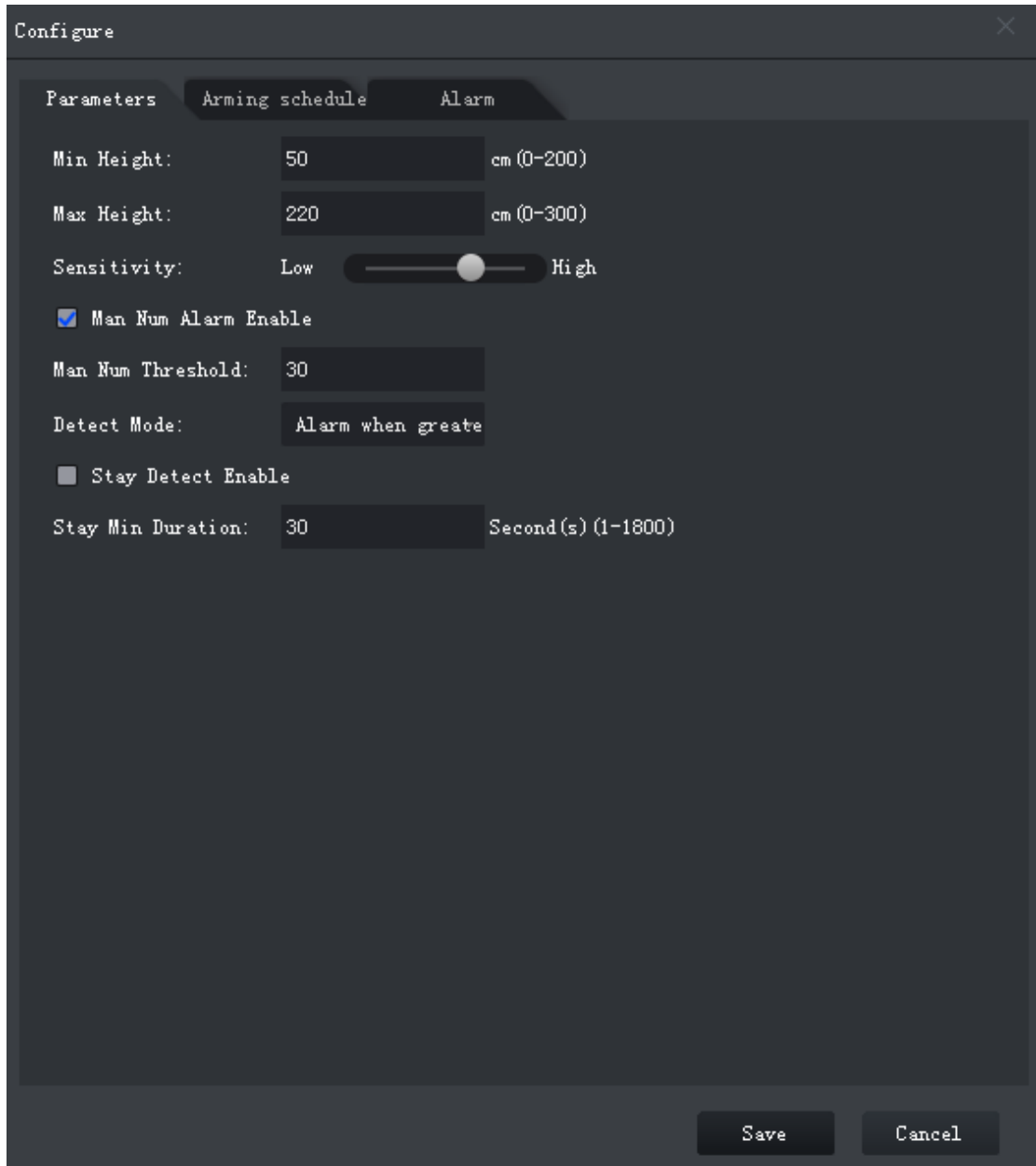


Table 5-39 Parameters

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.
Stay Min Duration	
Enter No.	When the entry number exceeds the preset value, system will trigger an

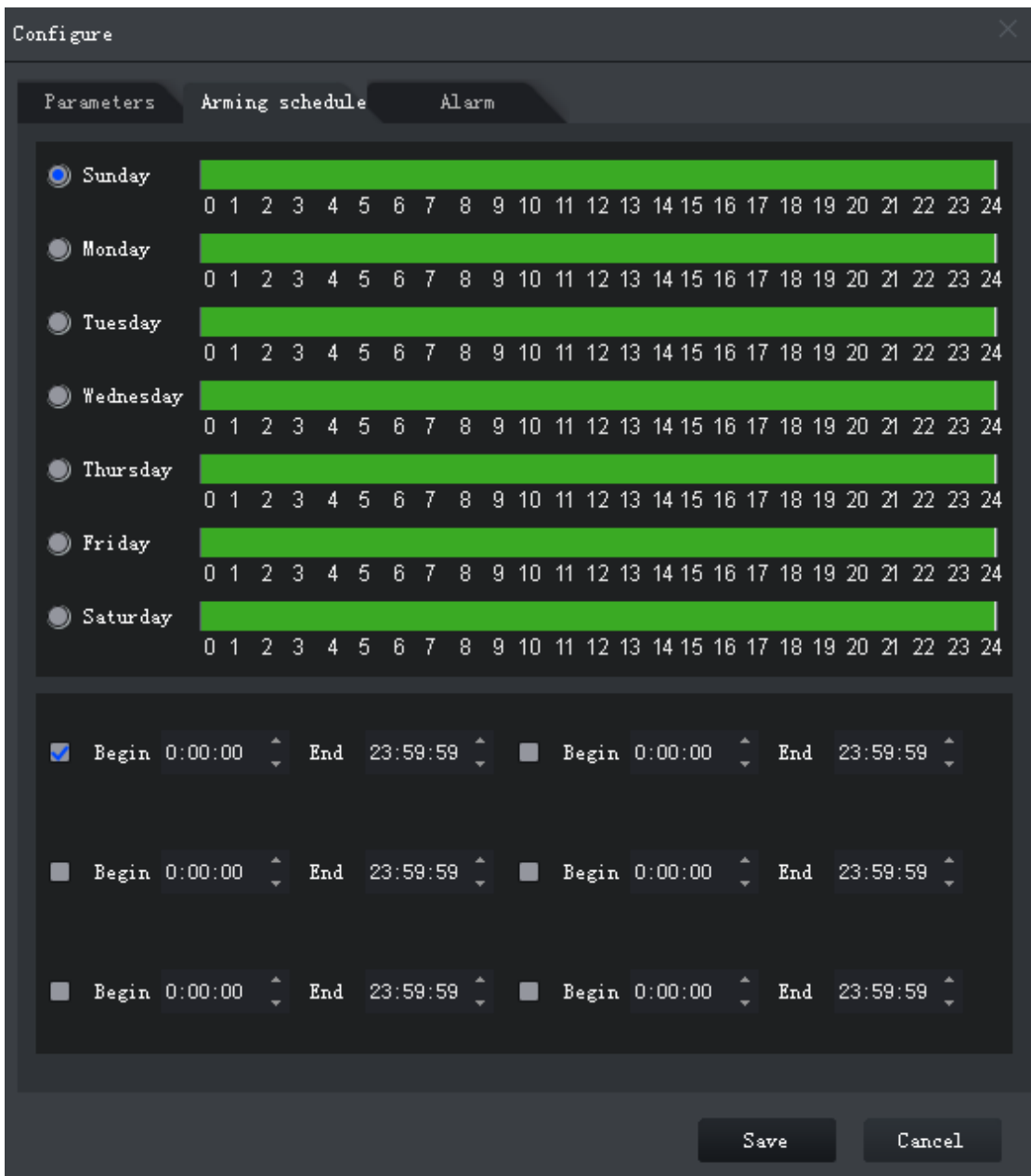
Parameter	Description
	alarm.
Exit No.	When the exit number exceeds the preset value, system will trigger an alarm.
Remaining No.	When the remaining people number exceeds the preset value, system will trigger an alarm.
Sensitivity	It is recommended to keep the default value.

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 5-99 Arming schedule



3) Click **Alarm** to set linkage actions.

Figure 5-100 Alarm

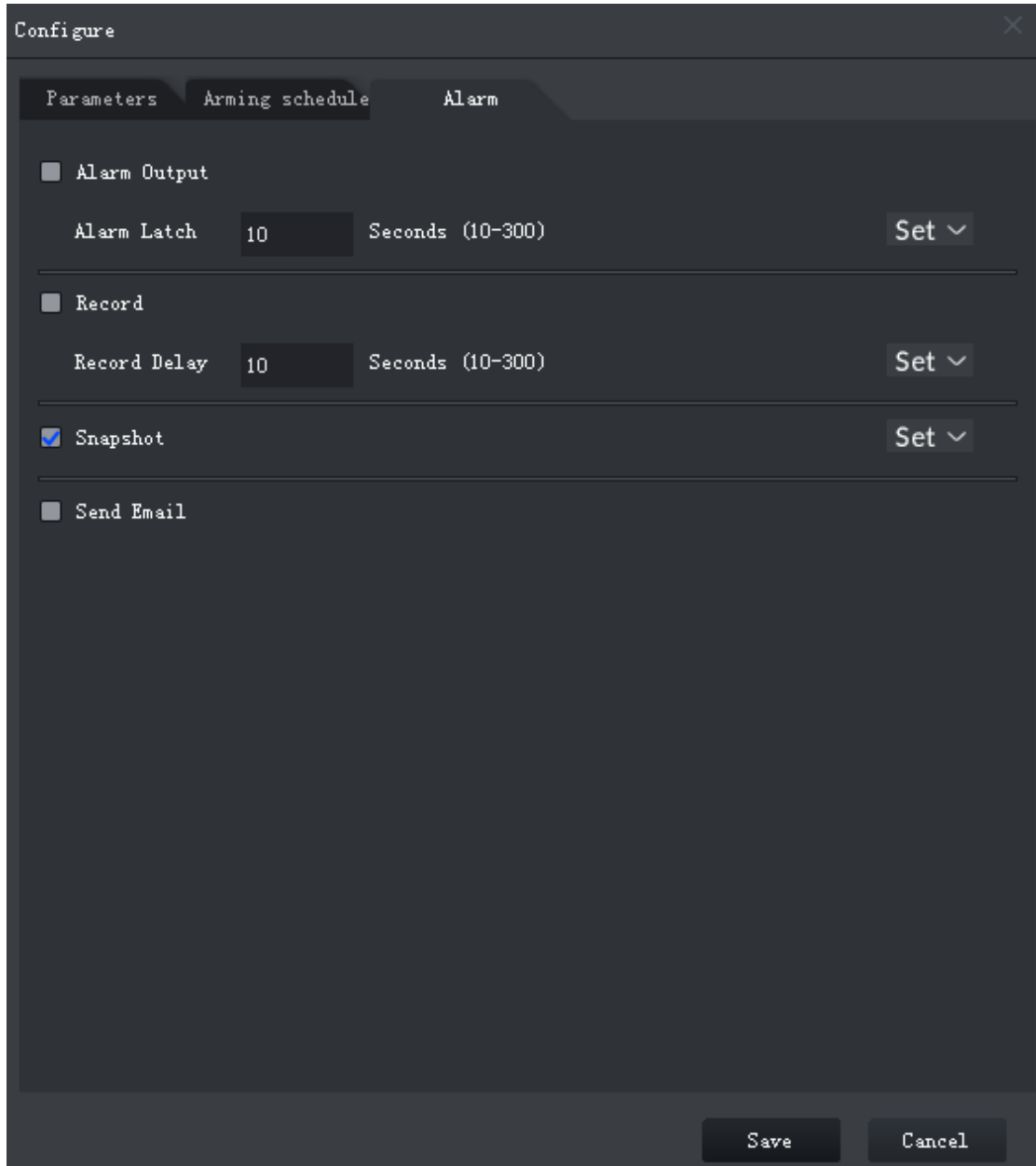





Table 5-40 Parameters

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.	Click Set next to Alarm Latch and select an alarm output channel.
Alarm latch	The alarm output action will delay stopping after the alarm event ends.	
Record	When an alarm happens, it will trigger auto video recording immediately.  It requires the device to have recording schedules already. See device manual	Click Set next to Record to select the recording channel.

Parameter	Description	
	for detailed instruction.	
Record delay	Video recording delays stopping for a while after the alarm event ends.	
Snapshot	<p>The system will take snapshots automatically when an alarm happens.</p>  <p>It requires the device to have snapshot schedules already. See device manual for detailed instruction.</p>	Click Set next to Snapshot to select the snapshot channel.
Send email	<p>The system will send an email to the related mail address when an alarm happens.</p>  <p>It requires the device to have email configured already. See device manual for detailed instruction.</p>	—

4) Click **Save**.

Step 5 Click **Save**.

5.4.5 Heatmap

Detect the accumulated people density in a specific zone and display the result in different colors which range from blue to red. Blue indicates low density and red means high density.

5.4.5.1 Enabling Heatmap

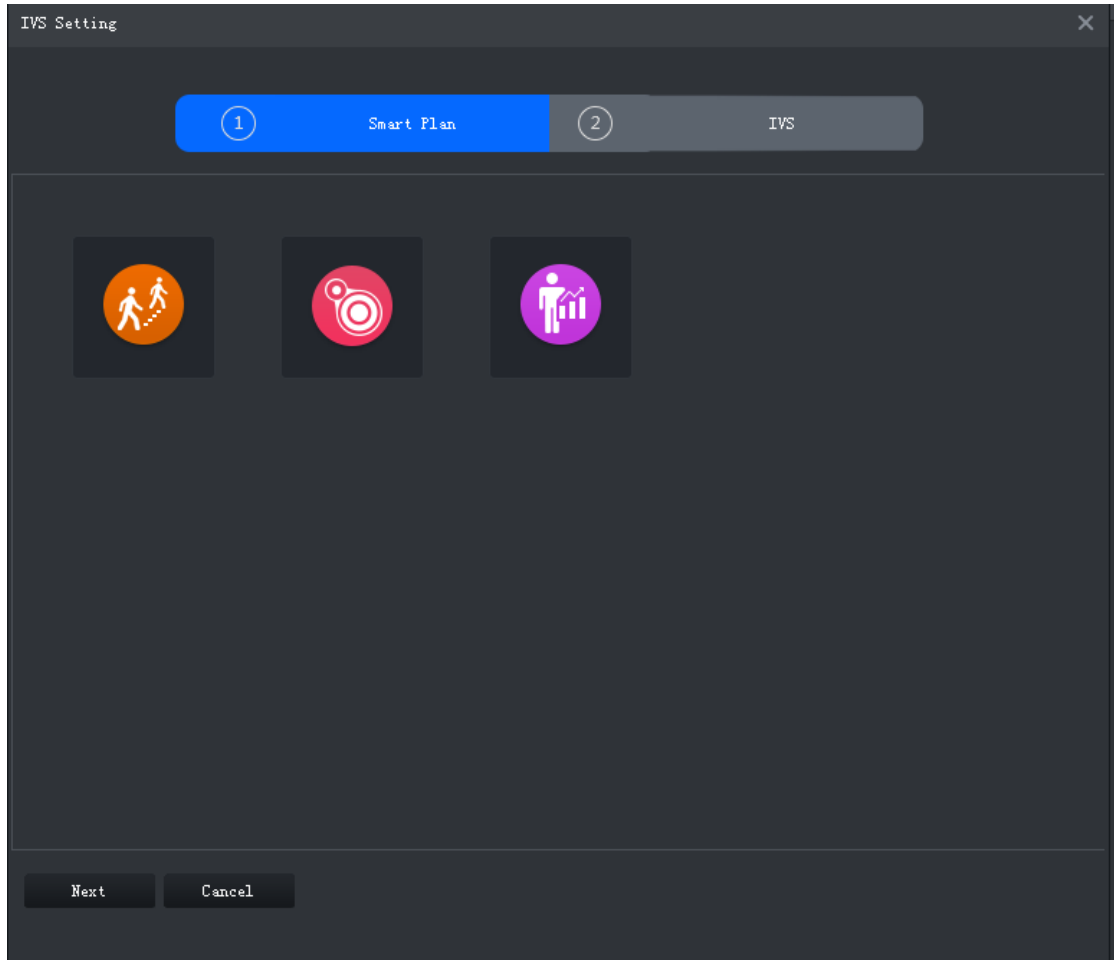
Step 1 Go to the **Intelligent Analyse** interface.

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

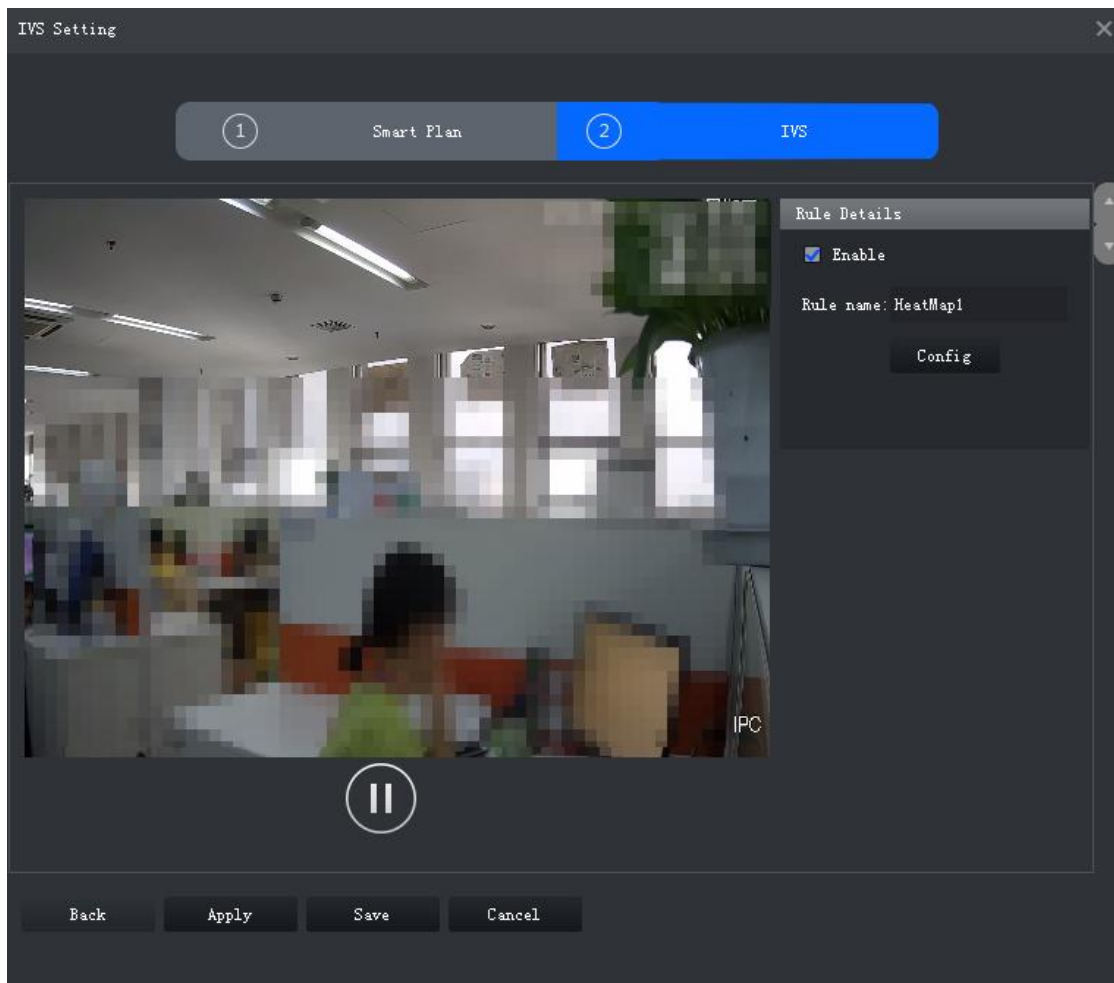
deselect it and then click  to select heatmap.

Figure 5-101 Smart plan



5.4.5.2 Configuring Heatmap Rule

Figure 5-102 Heatmap



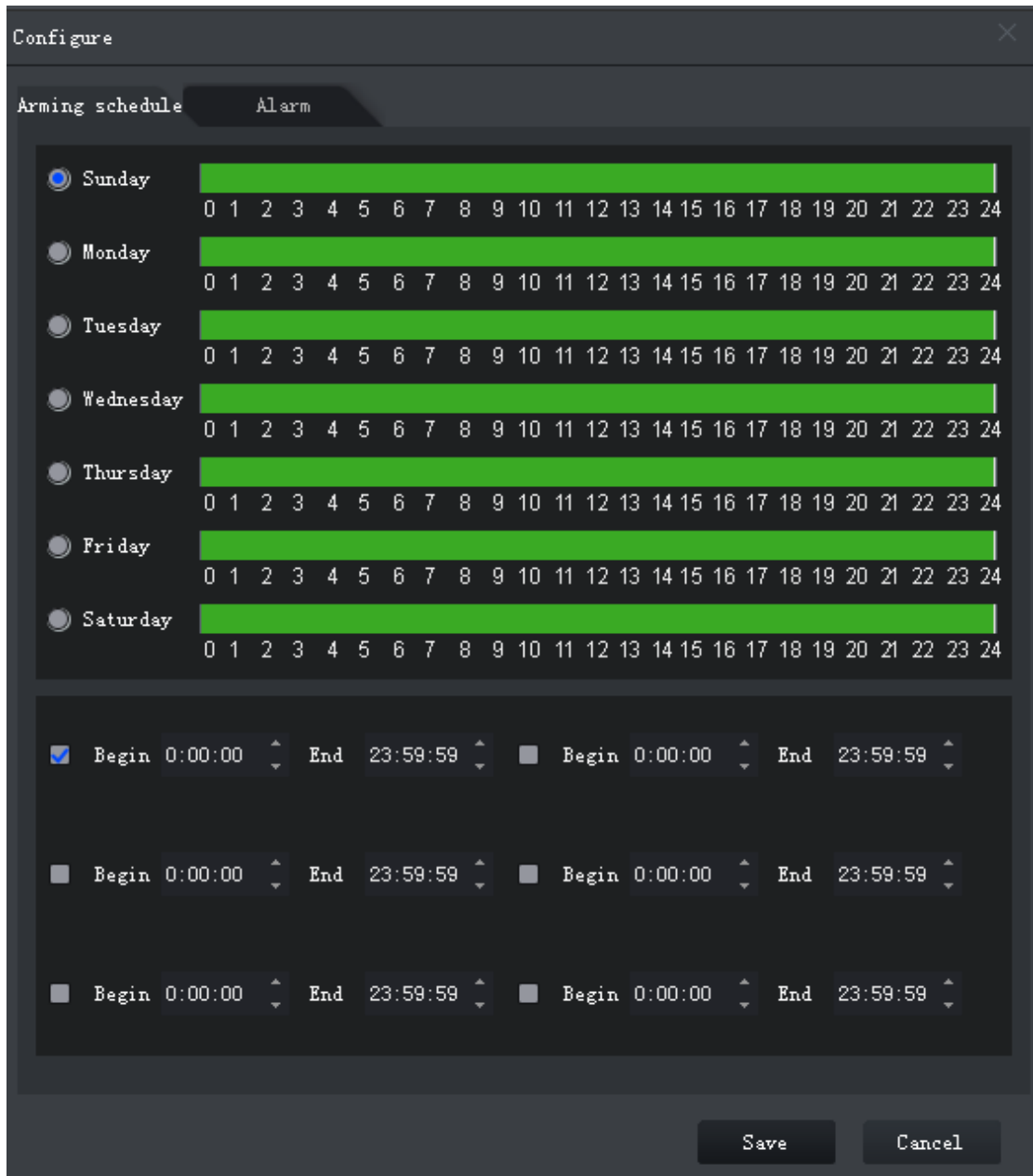
Step 1 Select the check box of **Enable** to enable heatmap.

Step 2 Modify rule name.

Step 3 Configuring arming schedule and alarm linkage.

1) Click **Config**.

Figure 5-103 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 5-104 Alarm

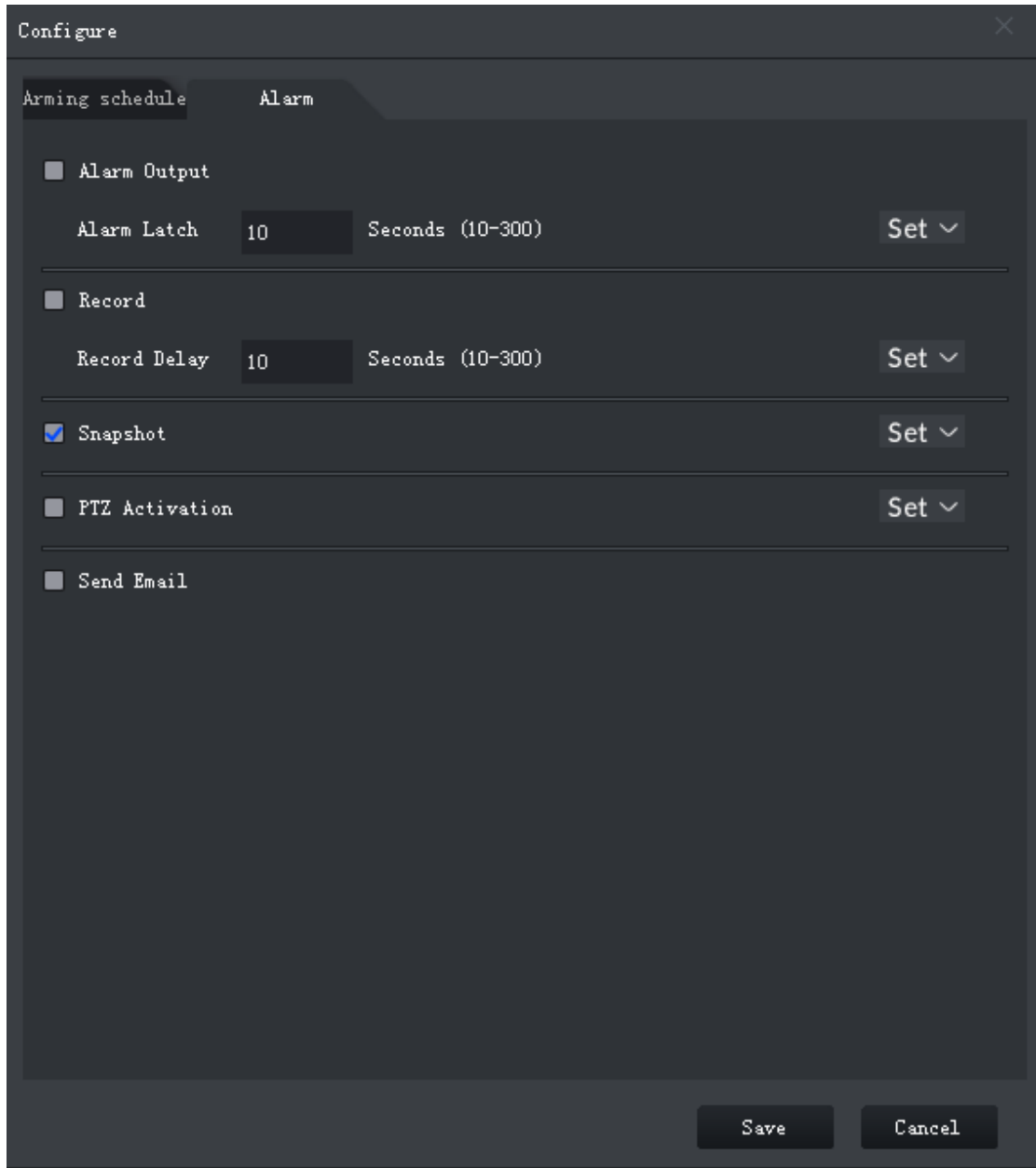





Table 5-41 Parameters

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.	Click Set next to Alarm Latch and select an alarm output channel.
Alarm latch	The alarm output action will delay stopping after the the alarm event ends.	
Record	When an alarm happens, it will trigger auto video recording immediately.  It requires the device to have recording schedules already. See device manual	Click Set next to Record to select the recording channel.

Parameter	Description	
	for detailed instruction.	
Record delay	Video recording delays stopping for a while after the alarm event ends.	
Snapshot	<p>The system will take snapshots automatically when an alarm happens.</p>  <p>It requires the device to have snapshot schedules already. See device manual for detailed instruction.</p>	Click Set next to Snapshot to select the snapshot channel.
Send email	<p>The system will send an email to the related mail address when an alarm happens.</p>  <p>It requires the device to have email configured already. See device manual for detailed instruction.</p>	None

4) Click **Save**.

Step 4 Click **Save**.

5.5 Record

System can search and playback records from the device or center storage media, which enables you to search, playback and download records of different channels, different times and different types from the Client. If there are records, system displays different colors in date selection region.

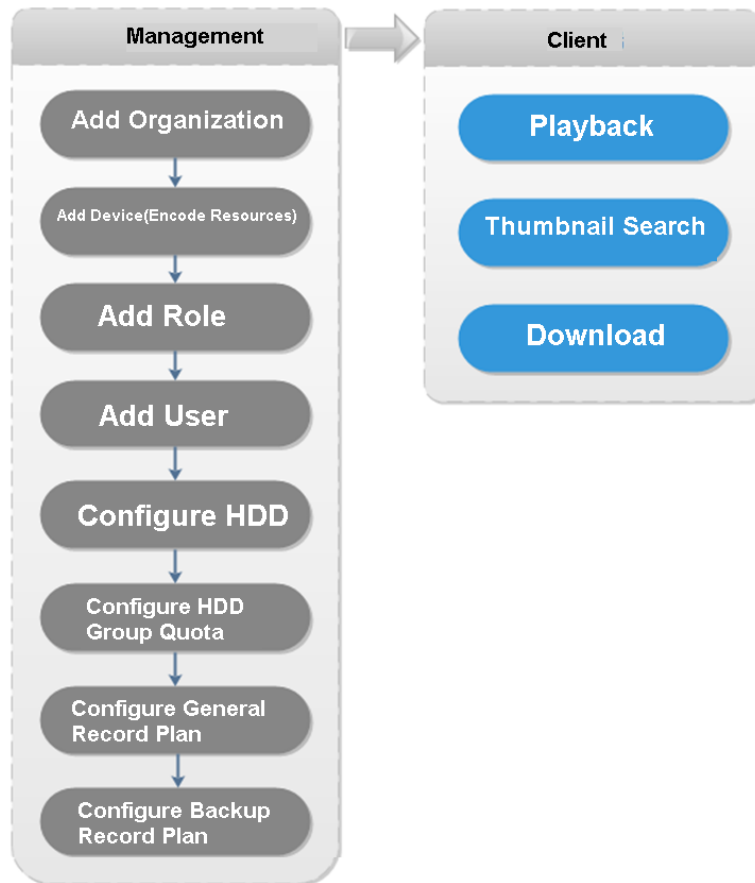
- Device Storage: Record to be stored in front-end SD card, or disks like DVR or NVR. Storage plan is configured on the device.
- Center Storage: Record to be stored in network storage server or DSS disks. To play back the record, you need to configure the record plan first, and then system will store the record of the specified period in network storage server.

5.5.1 Preparations

Make sure you have set record schedule on the manager. Contact the admin or refer to 4.6 Configuring Record Schedule for detailed information.

Refer to Figure 5-105 for Playback flows information.

Figure 5-105 Playback business flow



5.5.2 Record Playback

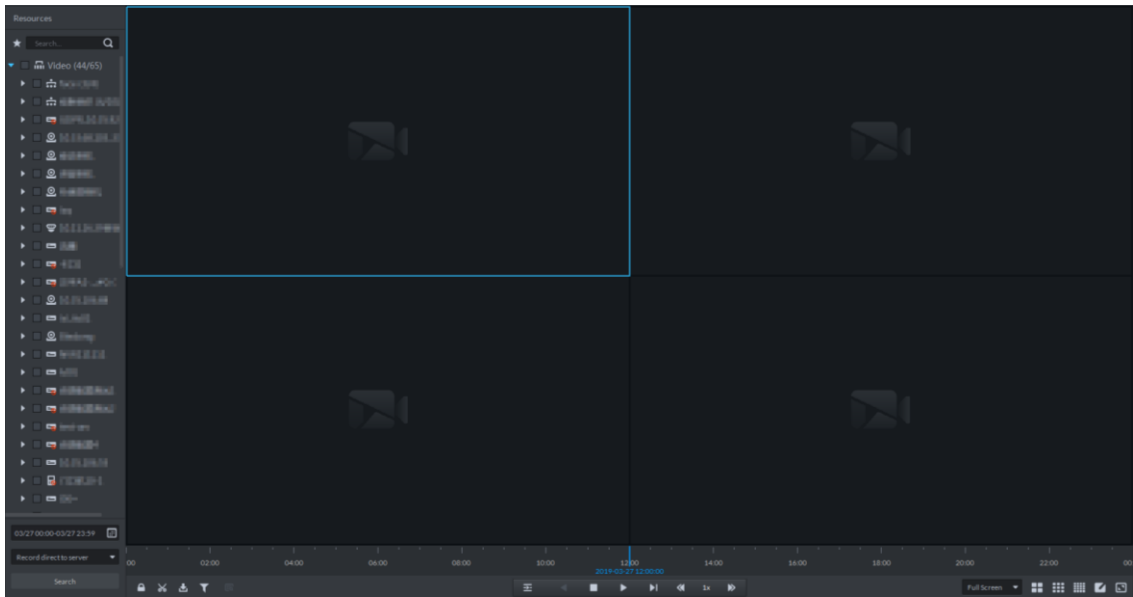
5.5.2.1 Search Record

Search record of today, specified date or specified period.

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


Step 2 Click .

Figure 5-106 Playback interface



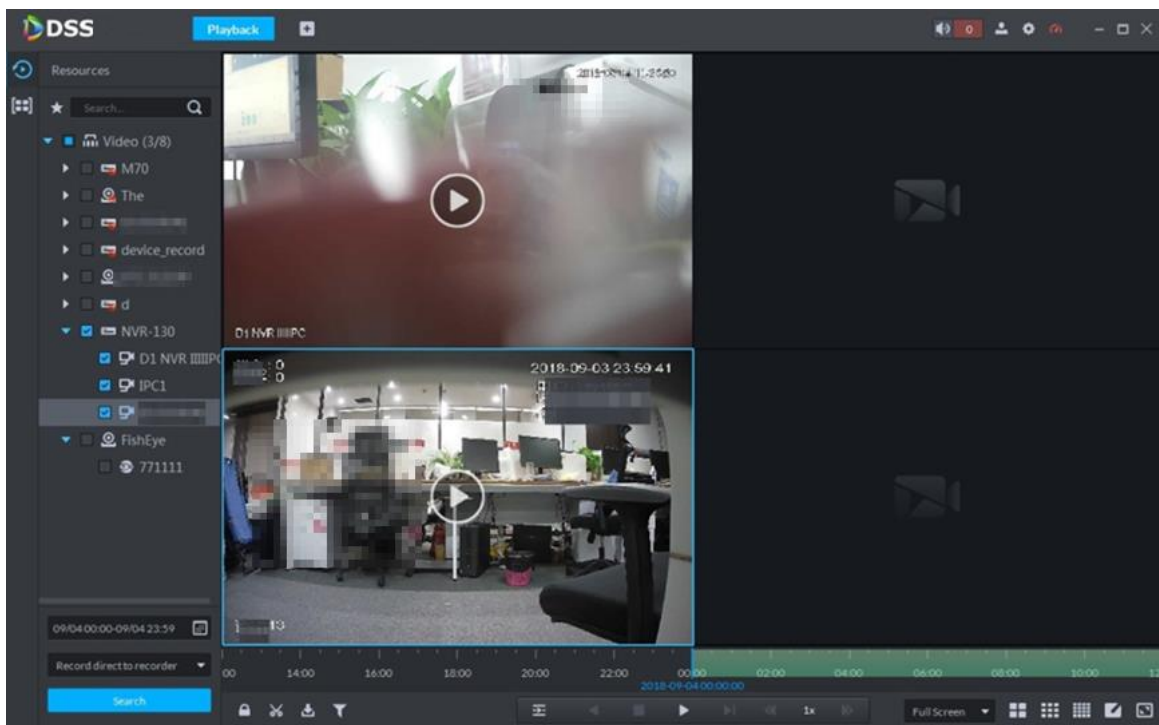
Step 3 Select a channel on the device tree.

Step 4 Select date and record storage position. Click **Search**.

Step 5 Select a video window that has the record and then click .

Corresponding window begins playback the record of current channel.










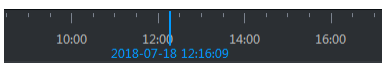
Figure 5-107 Playback



5.5.2.2 Record Control

Refer to Table 5-42 for buttons at the bottom of record playback interface and the description.

Table 5-42 Icons 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.
	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.

5.5.2.3 Record Type Filter

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

Step 1 On **Record Playback** interface, click .

Figure 5-108 Record playback interface

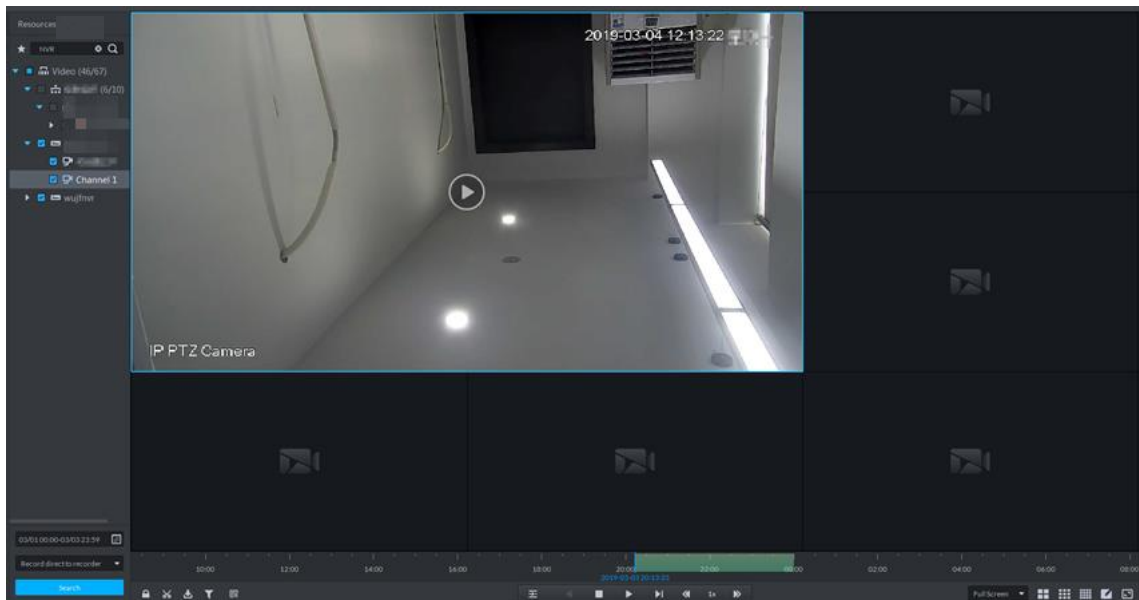
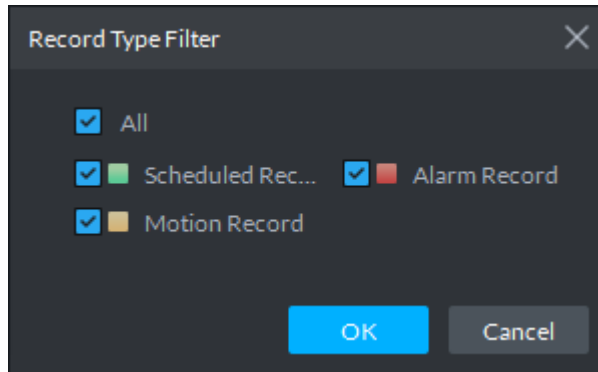


Figure 5-109 Record type filter



Step 2 Select a record type (or types) and then click **OK**.
The system only displays the video of selected type.

5.5.2.4 Smart Search

It makes dynamic detection analysis over some area and only replays the video with dynamic image within the detection area. The added device is required to support smart search, otherwise the search result will be null.

Step 1 Click  on the interface of **Record Playback**, and then select a type.

Figure 5-110 Enable smart search

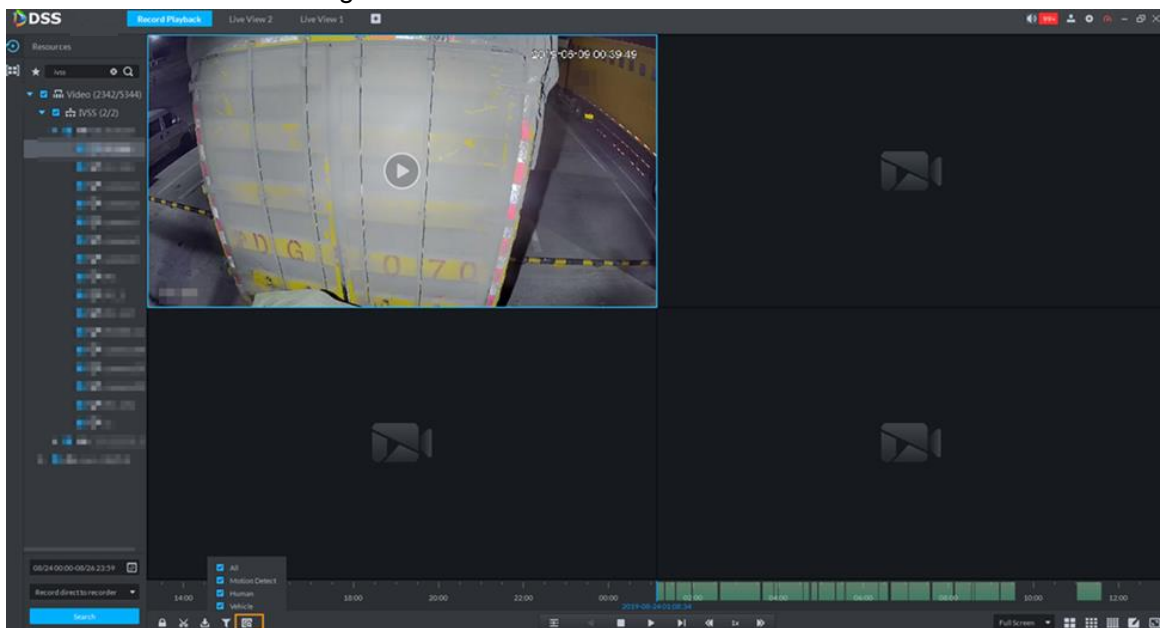
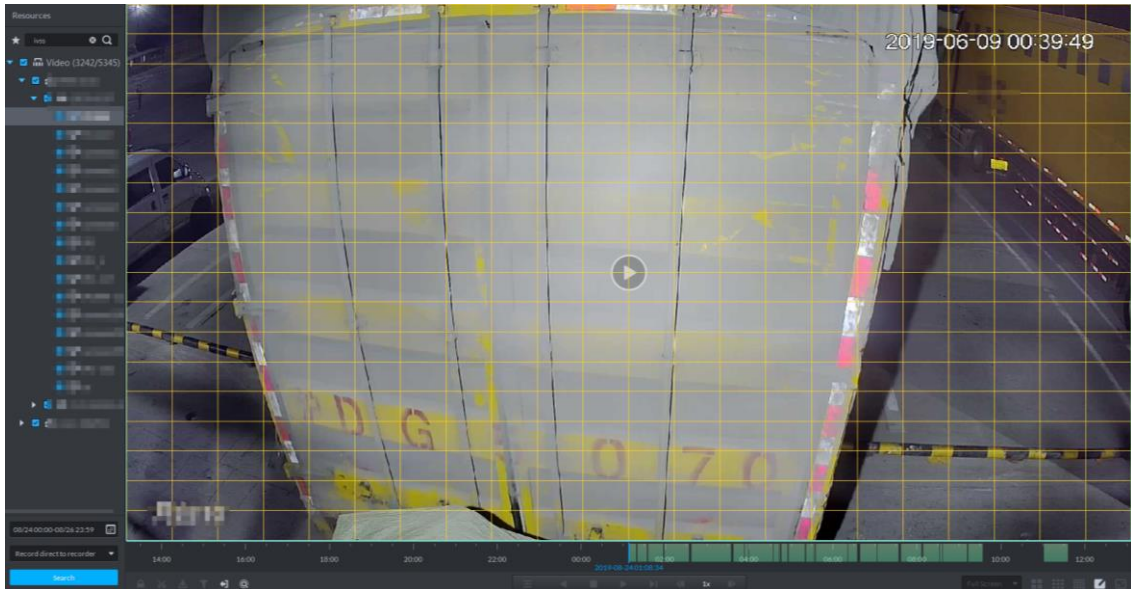


Figure 5-111 Smart search



Step 2 Click the square and select detection area, you can select several areas.




- Select detection area; move the mouse 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 3 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 4 Click the play button on the image or control bar.

The system only replays search result, which is the purple display frame on the time progress bar.

Step 5 Click  and exit smart search.

5.5.2.5 Lock Record

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

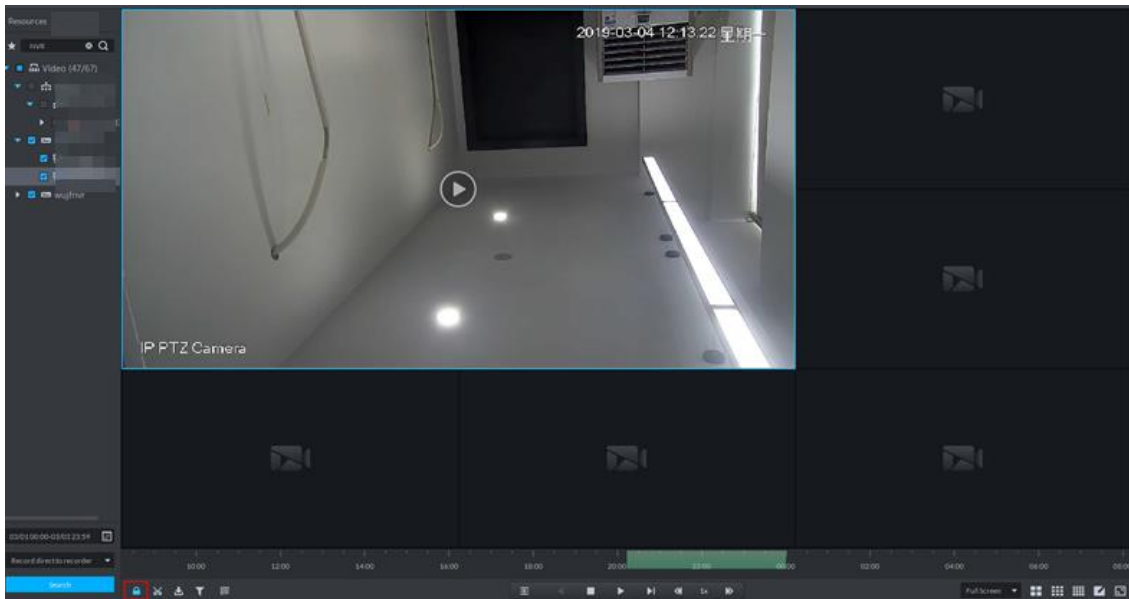


You can only lock the central video stored on the server.

Step 1 Click  at the bottom of the **Record Playback** interface (make sure the window has the record).

Place the mouse to the time progress bar.

Figure 5-112 Select lock time



- Step 2** Click the time progress bar to select lock start time, then drag mouse, and then click to select end time.
System pops up **Save Lock** dialogue box.
- Step 3** Click **OK**.

5.5.2.6 Add Mark

You can mark records that interest you by Add Mark for a subsequent search and location.


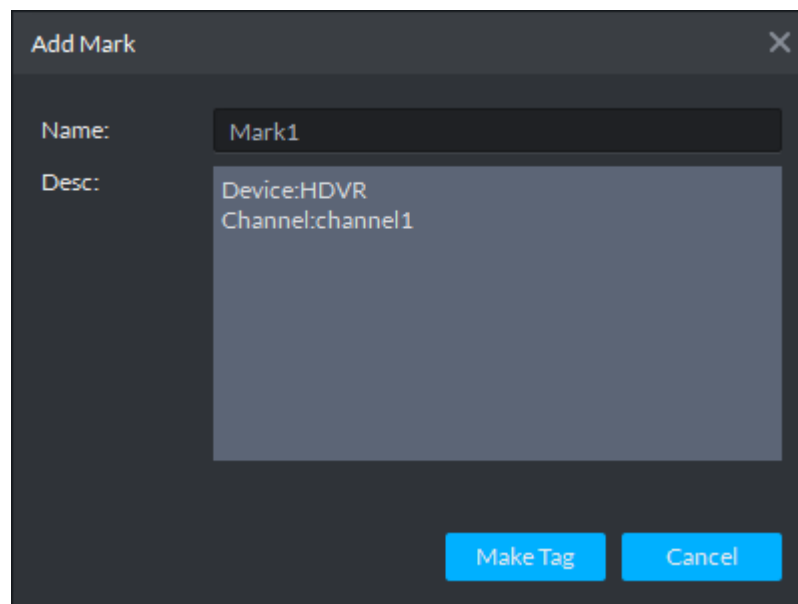
- Step 1** On **Record Playback** interface, move mouse to the window that is playing record. Click  at the upper-left corner.

Figure 5-113 Add mark



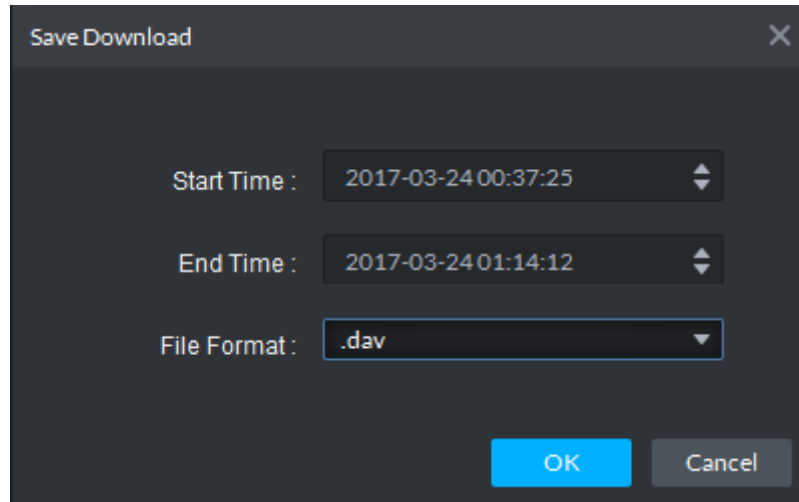
- Step 2** Input **Name** and **Description**, and then click **Make Tag**.
System prompts **Tag Creation Successful**. You can search record via mark in the **Download Center**.

5.5.2.7 Clip Record

Step 1 Click  at the bottom of the **Record Playback** interface (make sure there is record in the window).

Step 2 During the timeline, click to start clip and then drag the mouse, click to stop clip.

Figure 5-114 Save download



Step 3 Set file format and then click **OK**.

5.5.2.8 Downloading Recording


The system supports downloading the record in the server or the device to the client.

Click  at the bottom side of the **Record Playback** interface, and the **Download Center** interface is displayed. For details, see "5.6 Record Download."

5.5.3 Search 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 On **Record Playback** interface, click .

Step 2 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.

Figure 5-115 Select time

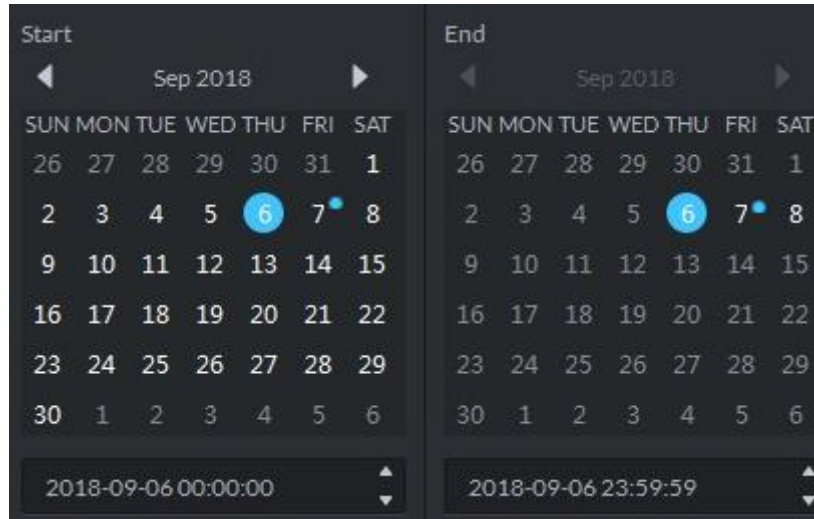
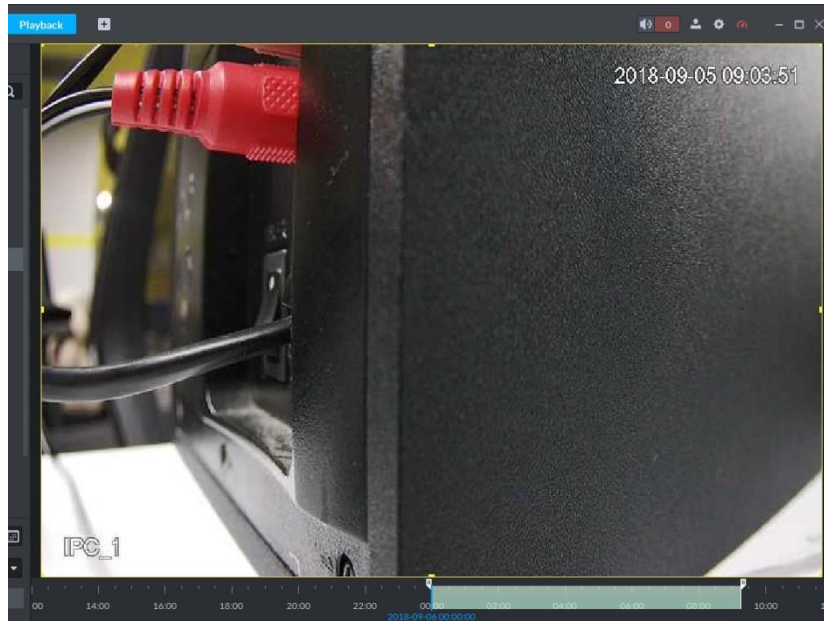


Figure 5-116 Search result




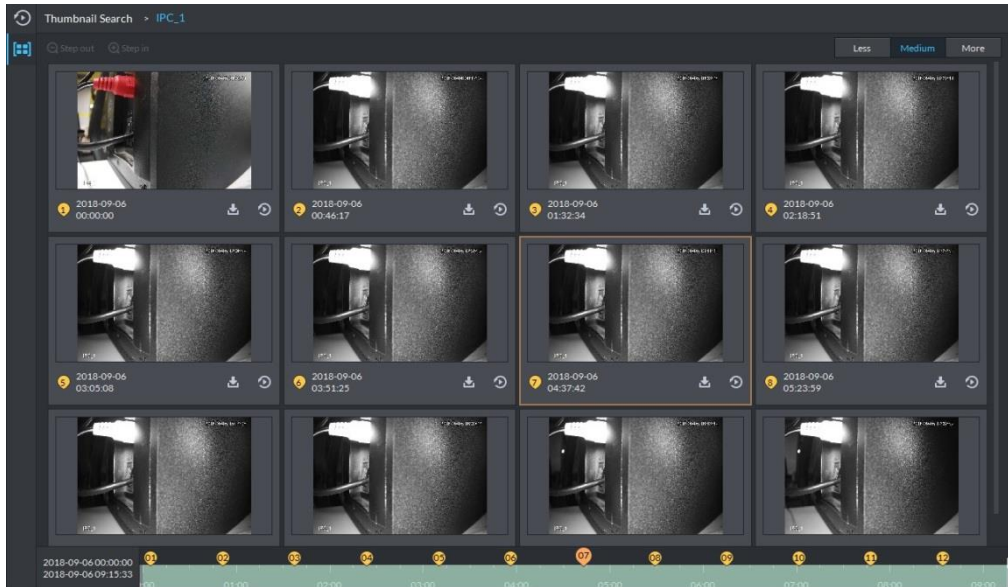
Step 3 Drag the yellow frame on the right to set thumbnail range. Click . System displays the video of current range.

Figure 5-117 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.


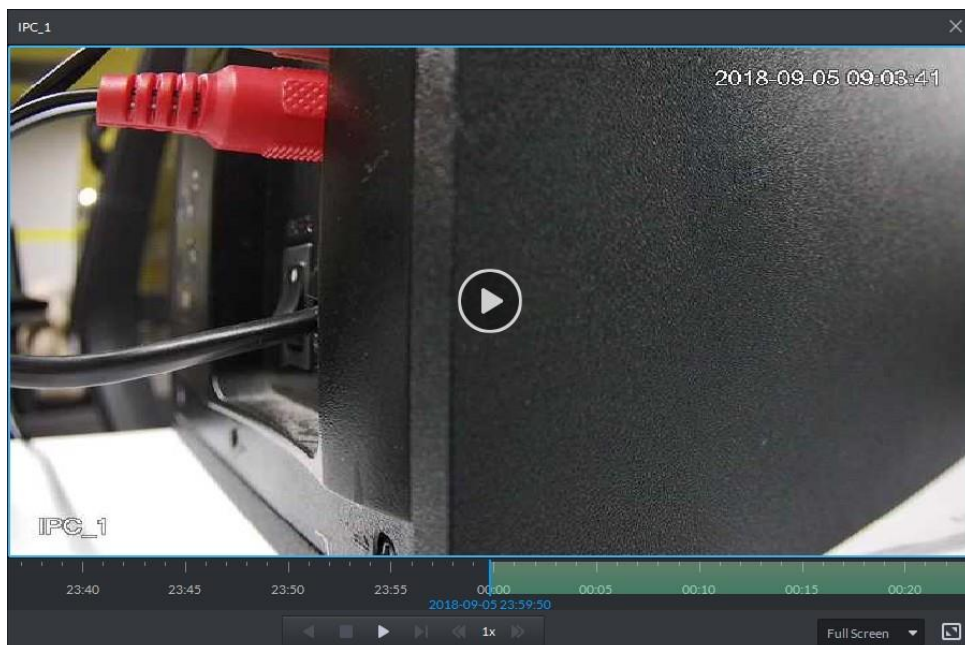
Step 4 Click the  at the bottom right corner of the thumbnail, you can view the corresponding video related to the thumbnail.

Figure 5-118 Video playback



Step 5 Download Record



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


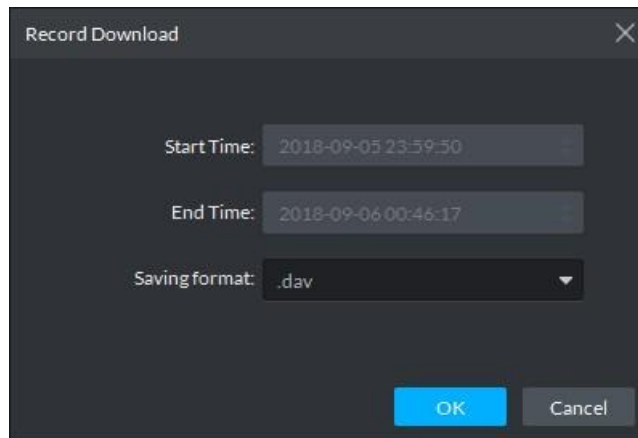
- 1) Click  at the right corner of the thumbnail, system downloads the record between current image and the next image. See Figure 5-119.

Figure 5-119 Download video



- 2) Select file format and then click **OK**.
Go to the Download center to view download detailed information. Refer to "5.6 Record Download" for detailed information.

5.6 Record Download

The system supports three download methods: Timeline, File List and Label.

5.6.1 Preparation

Make sure the record has been saved in the server, or SD card or HDD of device.

5.6.2 Timeline

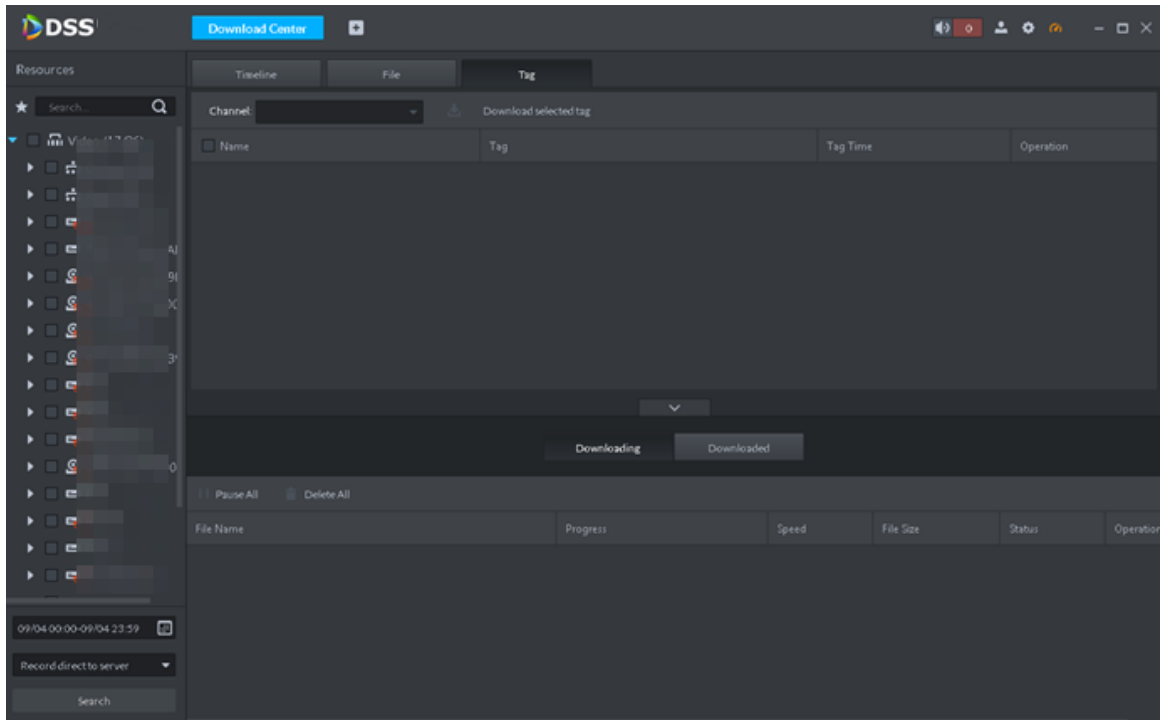
Download video within some period.



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

Step 1 Click , on the **New Tab** interface, select **Download center**.

Figure 5-120 Download center

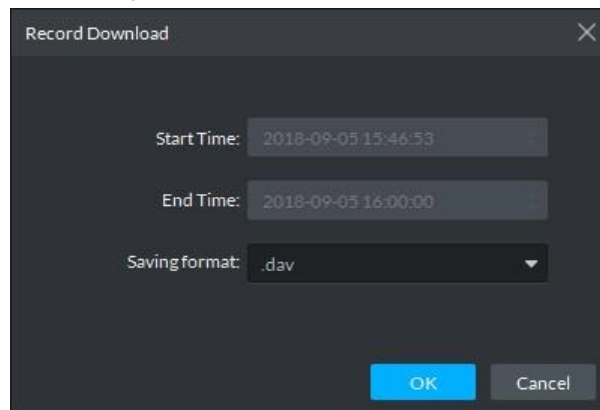


Step 2 Click **Timeline**.

Step 3 Select device channel, set search period and record storage position. Click **Search**.

Step 4 Select the period on the timeline, system pops up download dialogue box.

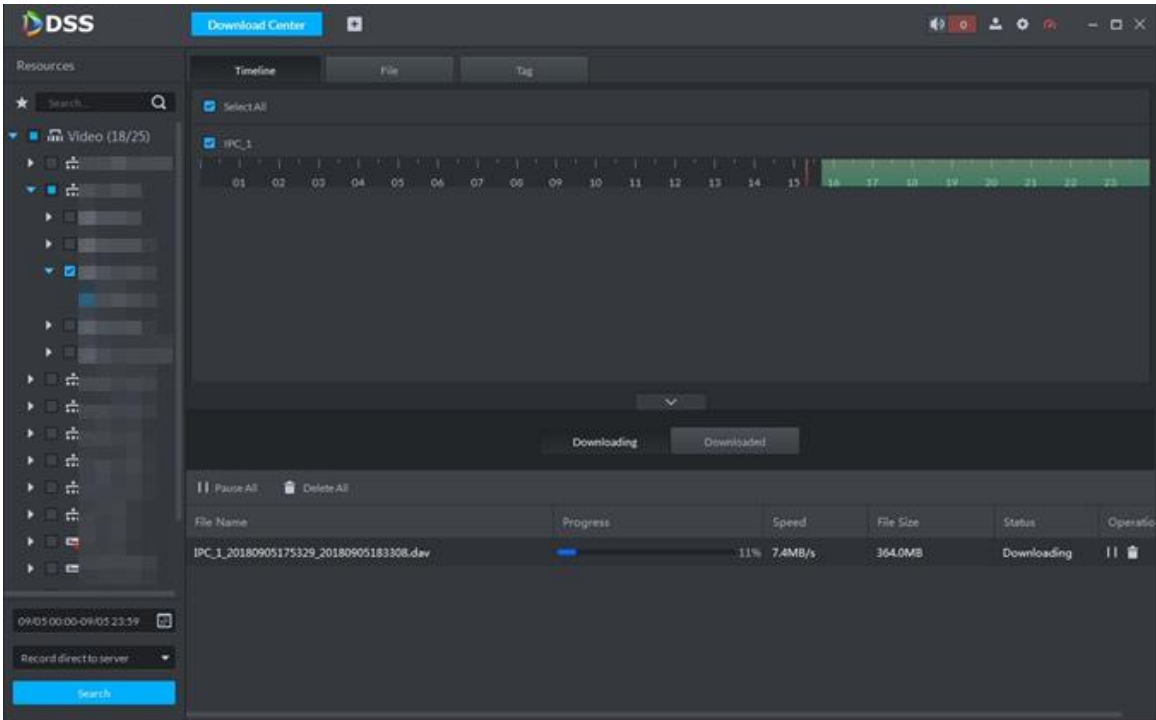
Figure 5-121 Select time



Step 5 Set file format and then click **OK**.

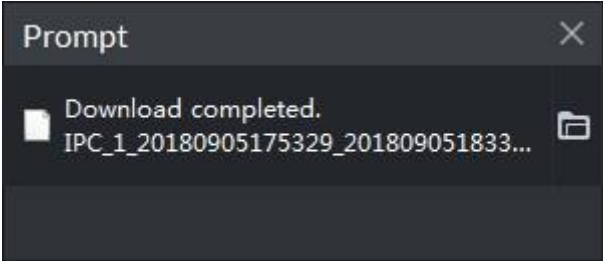
You can view the download process at the bottom of the interface.

Figure 5-122 Download process



System pops up the following dialogue box once the download is complete.

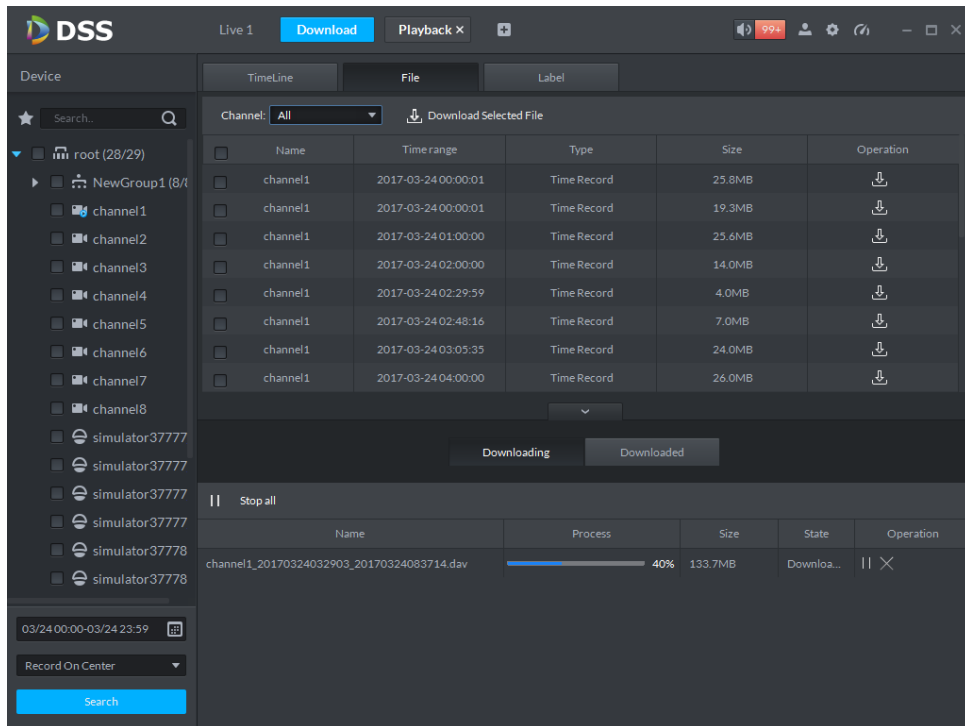
Figure 5-123 Download completed




5.6.3 File List

Step 1 In the **Download** interface, click the **File** tab.

Figure 5-124 Record files



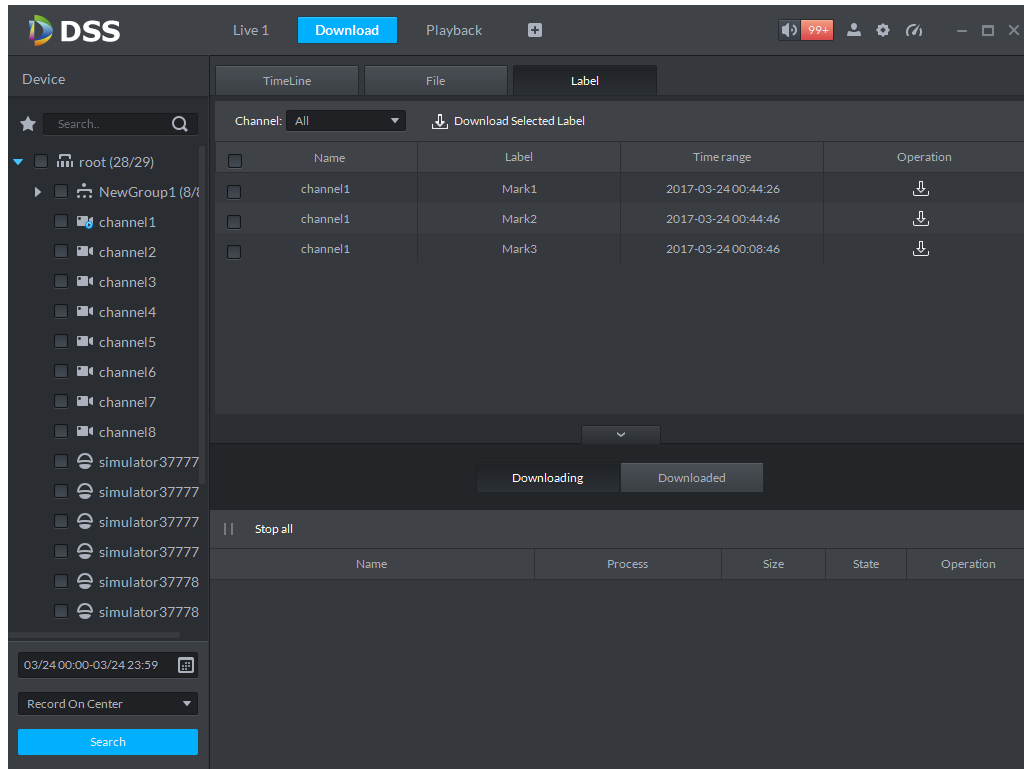
Step 2 Directly click  in the record file list, or check multiple files and click **Download Selected Files**.


System displays download process at the bottom of the interface. System pops up dialogue box once the download is complete.

5.6.4 Label

Step 1 On the **Download** interface, click the **Label** tab. System displays marked record files.

Figure 5-125 Marked video files



Step 2 Directly click  in the record file list, or check multiple files and click **Download Selected Files**.

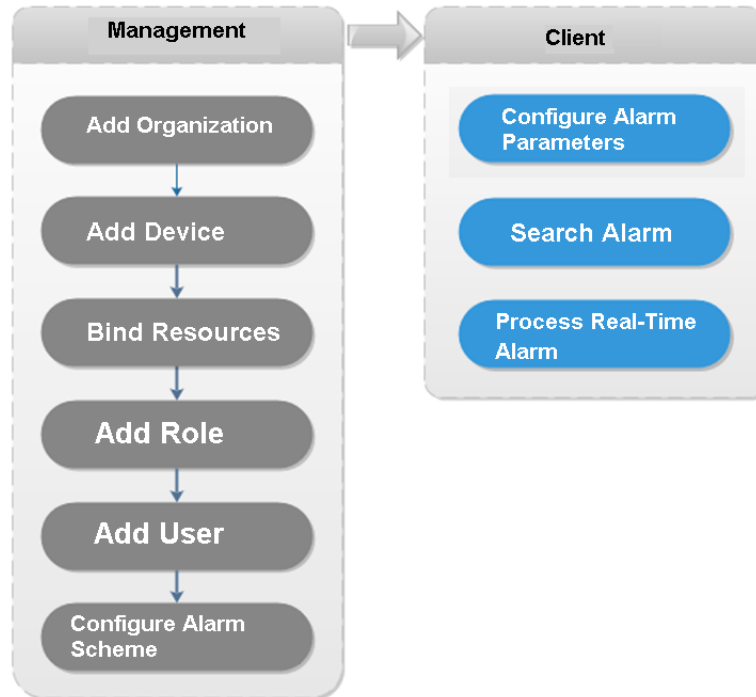
System displays download process at the bottom of the interface. System pops up dialogue box once the download is complete.

5.7 Event Center

5.7.1 Preparations

- Make sure you have added corresponding devices on the manager. Refer to "4.5 Adding Device for detailed information."
- You have completed event management settings on the manager. Refer to "4.7 Configuring Event for detailed information."

Figure 5-126 Event management flow



5.7.2 Configuring Alarm Parameters

It is to set alarm mode on the client. It includes alarm audio, alarm flashing on the map or not, etc.



Step 1 Click  at the upper-right corner, from **General > Alarm**.

Figure 5-127 Set alarm parameters

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

Table 5-43 Parameters

Parameters	Description
Play alarm sound	Check the box, system generates a sound when an alarm occurs.
Loop	Check the box; system plays alarm sound repeatedly when an

Parameters	Description
	alarm occurs.  This item is only valid when Play alarm sound function is enabled.
Alarm type	It is to set alarm type. System can play sound when corresponding alarm occurs.  This item is only valid when Play alarm sound function is enabled.
Sound path	It is to select alarm audio file path.
Map flashes when alarm occurred	Check the box and then select alarm type. When the corresponding alarm occurs, the device on the emap can flash.
Display alarm link video when alarm occurred	Check the box, system automatically opens linkage video when an alarm occurs.
Display type	System automatically opens linkage video when an alarm occurs. You can view on the pop-up window or on the preview interface.

5.7.3 Searching and Processing Real-Time Alarm



The customized alarm supports modification and deletion.

- If the alarm scheme has used the customized alarm type, you can only modify the alarm. You cannot delete it.
- If the alarm scheme has not used the customized alarm type, the alarm input channel and alarm type restores default value if you delete the alarm type.
- Once you modified the customized alarm type, the previous data still uses the original name; the new data uses the modified name.

5.7.3.1 Processing Real-Time Alarm

Step 1 Click  on the **New Tab** interface select **Event Center**.


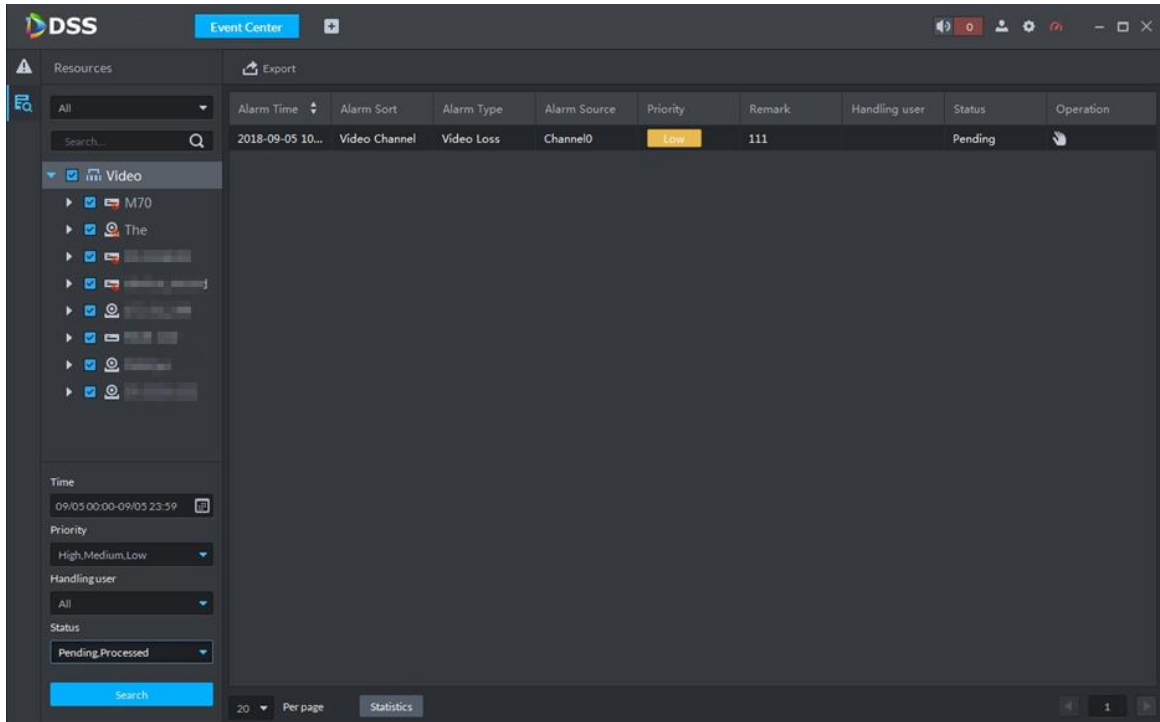
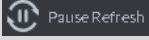
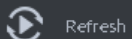
Step 2 Click  on the left navigation bar.

Figure 5-128 Alarm processing interface



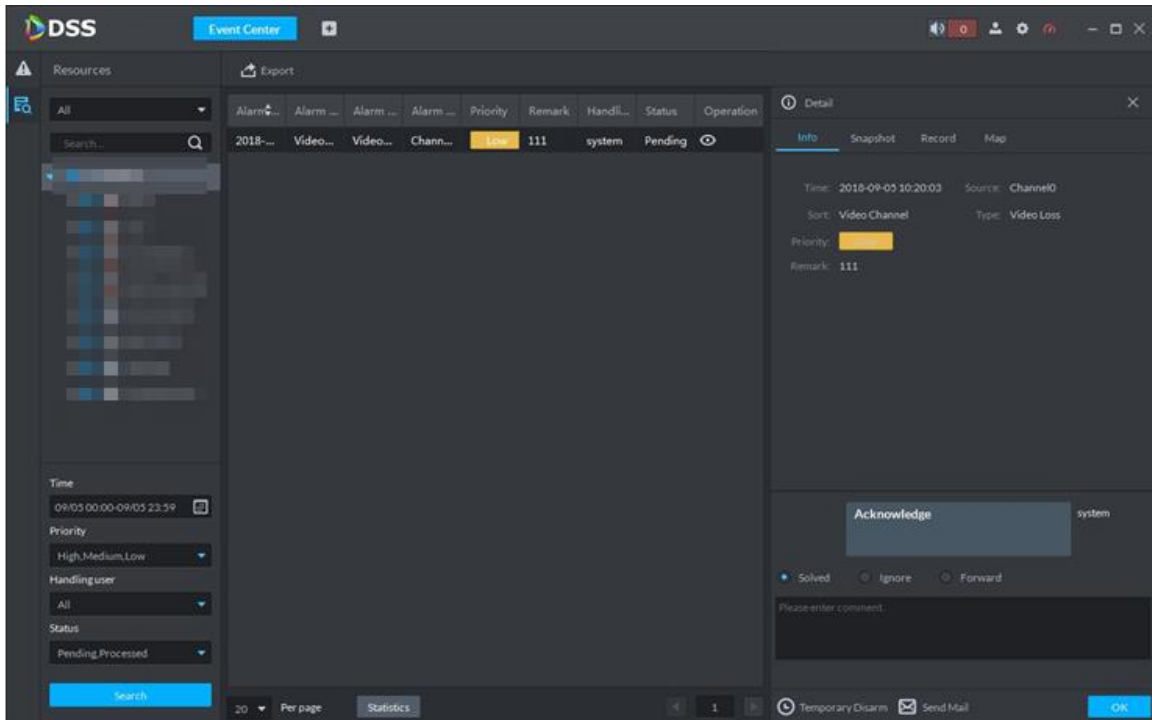
System refreshes to display real-time alarm by default. Click  to pause refresh, click  to continue refresh.

Step 3 Click  of an alarm item.

The logged in user can claim the alarm. After claimed, the system displays user name on the user column.

Step 4 Click  to view details and process the alarm.

Figure 5-129 Process alarms



Step 5 Click **Message**, **Snapshot**, **Record**, and **Map** tabs to view corresponding alarm information.

Step 6 Select processing results such as processed, ignored, transferred and then input comments.



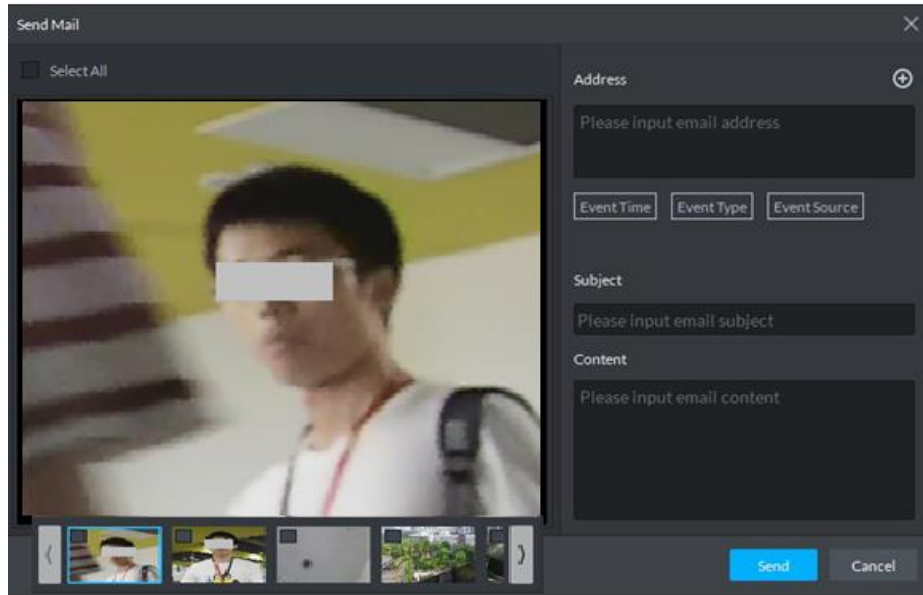
When selecting **Forward**, you can select other users on the dialog box. It is to send current event to specified user to process.

Step 7 Click **OK**.

Operations

- Disarm temporarily: Click **disarm temporarily**, and then set disarm time on the pop-up window. Click **OK**.
- Send mail: Click **Send Mail**, and then set email information on the pop-up window. Click **Send**.

Figure 5-130 Set mail parameters



5.7.3.2 Searching Alarm Record

Step 1 Click  on the **New Tab** interface select **Event Center**.


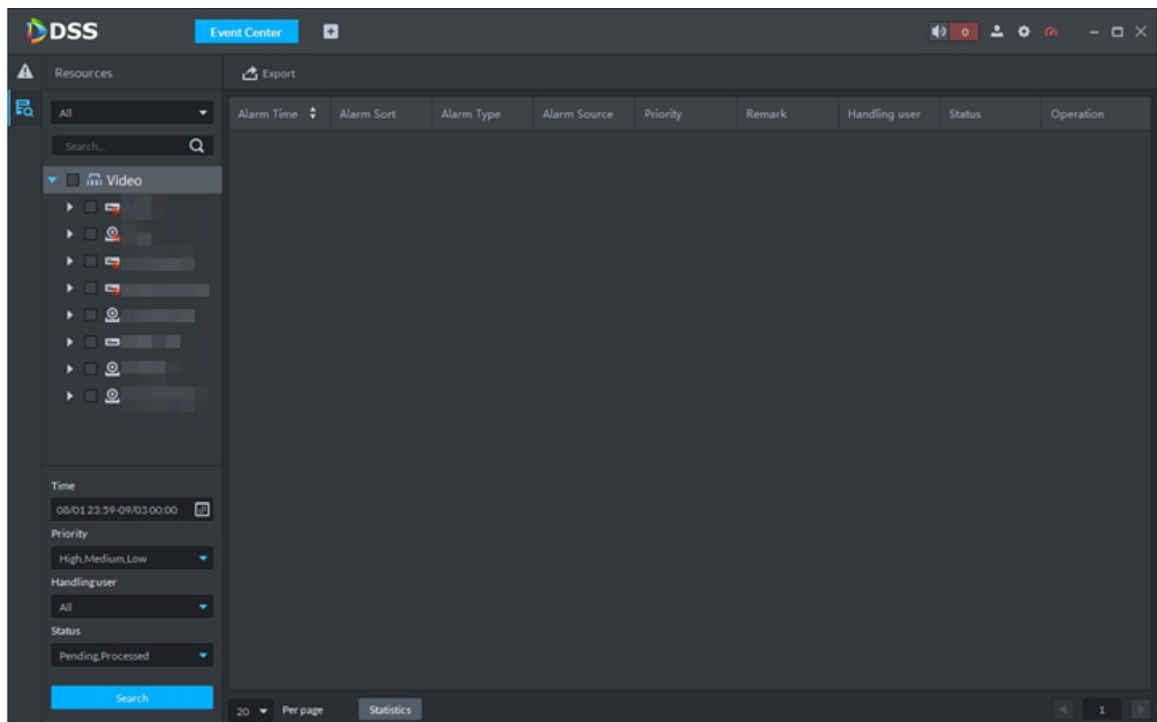
Step 2 Click  on the left navigation bar.

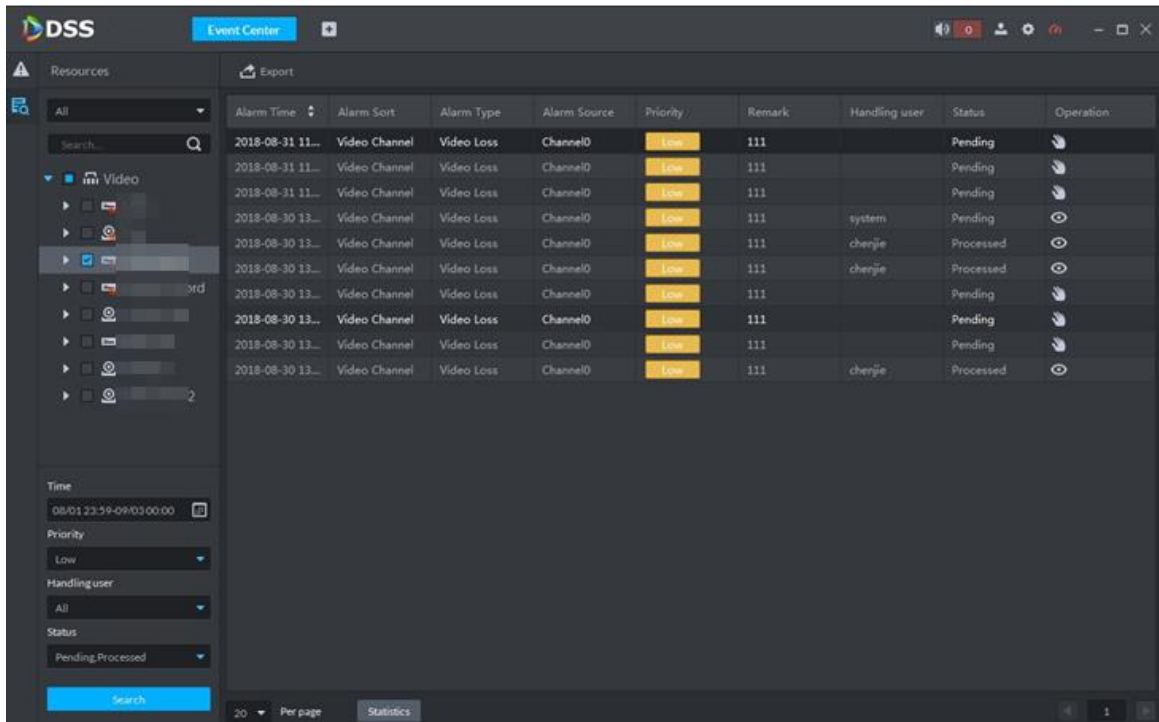
Figure 5-131 Alarm search



Step 3 Select device channel, search time, alarm level, user or alarm status.

Step 4 Click **Search**.

Figure 5-132 Alarms



Operations

- Select amount on Per page, it is to set displayed alarm message amount each time.
- Click Statistics, it is to display the total alarm message amount of corresponding device.
- Click Export, it is to export device alarm message.
- Click to claim alarm, click to process alarm. Refer to "5.7.3.1 Processing Real-Time Alarm" for detailed information.

5.8 Video Wall

5.8.1 Preparations

To achieve video display on video, you need to complete the following settings.

- Adding devices. Pay attention to select **Video Wall Control** in the **Device Category** dropdown list. For details, see "4.5 Adding Device."

Figure 5-133 Add a decoder

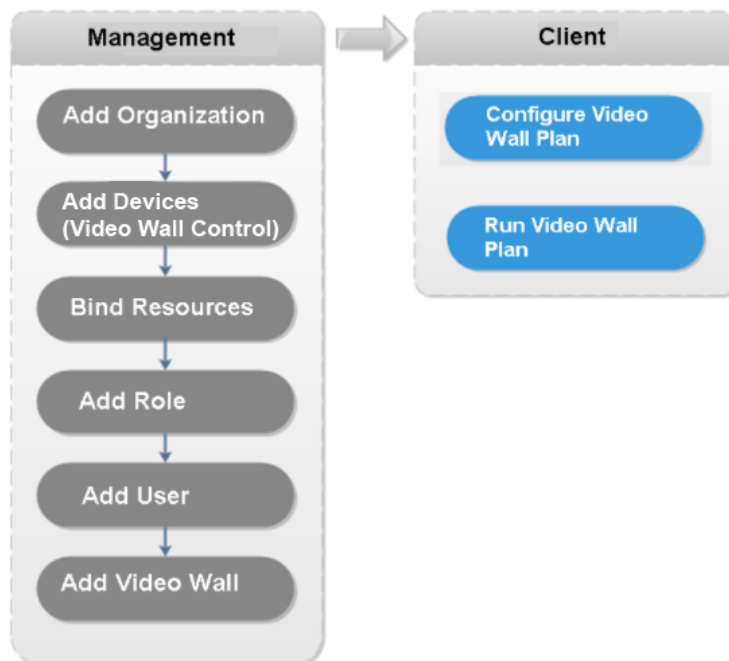
The screenshot shows a dialog box titled "Add All" with a close button (X) in the top right corner. It features two tabs: "1. Login Information" (which is selected and highlighted in green) and "2. Device Information". Below the tabs are several input fields:

- Protocol: [Dropdown menu]
- Manufacturer: [Dropdown menu]
- Add Type: IP Address [Dropdown menu]
- Device Category: Video Wall Control [Dropdown menu, highlighted with an orange border]
- IP Address: * [Text input field]
- Device Port: * 37777 [Text input field]
- User: * 1 [Text input field]
- Password: [Text input field]
- Org: root [Dropdown menu]
- Home Server: Center Server [Dropdown menu]

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

- Add a video wall. For details, see "4.8 Adding Video Wall".

Figure 5-134 Video wall configuration flow



5.8.2 Video Wall Display

Step 1 Click **+**, on the **New Tab** interface select **Video wall**, system displays video wall interface.

Figure 5-135 Video wall interface

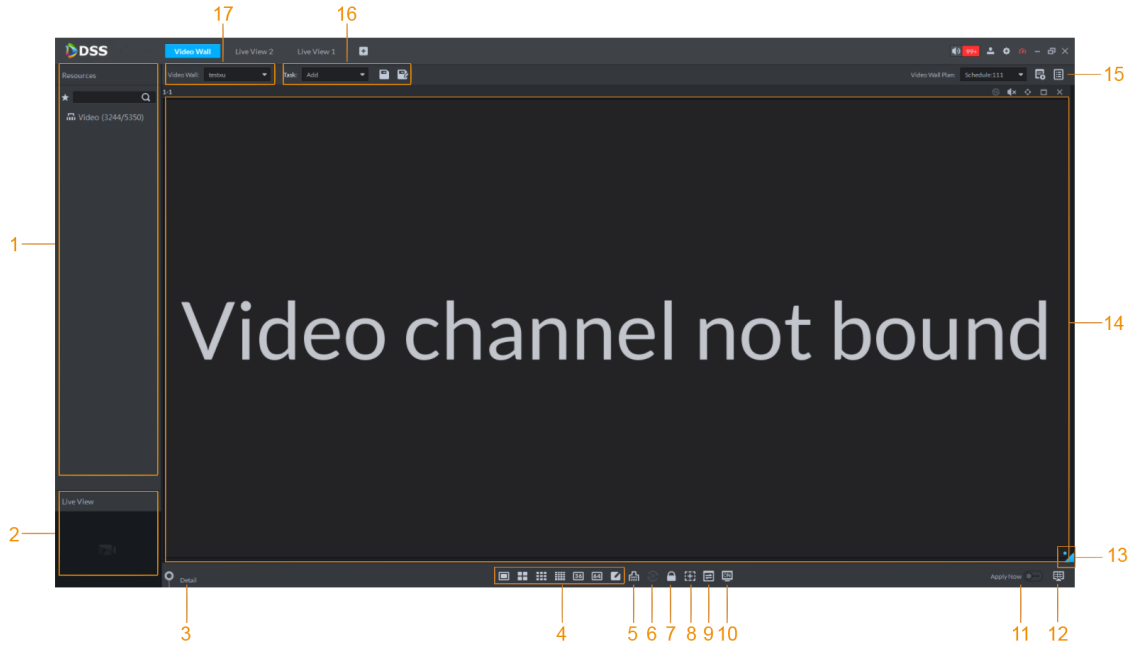









Table 5-44 Description

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.
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. Refer to "5.8.3 Video Wall Plan" for details.
16	Task management pane	Add, save or delete a task.

No.	Name	Function
17	Video wall selection	Select a video wall.

Step 2 Select a video wall and then select a window.

Step 3 Double-click the video channel or drag the video channel to the window.


The window displays **1 video source has been bound**.



- Enter device name or channel name to search.
- One window can bind several video channels at the same time.
- Video source binding mode is set in **Local Config > Video Wall**. For details, see "5.2 Local Configuration."

Step 4 Click  to output the video to the wall.

Once one window has bound several video channels at the same time, the window automatically begins tour operation after you output the video to the wall.

- Right-click mouse or on the Detail pane, you can modify channel stay time and bit stream.
- Click  to change tour sequence.

To stop all tours, click .




Stream type on video wall changes automatically according to window split number. For details, see "5.2 Local Configuration."

5.8.3 Video Wall Plan

5.8.3.1 Configuring Scheduled Plan

After setting a schedule plan, you can play videos on the video wall as scheduled.

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


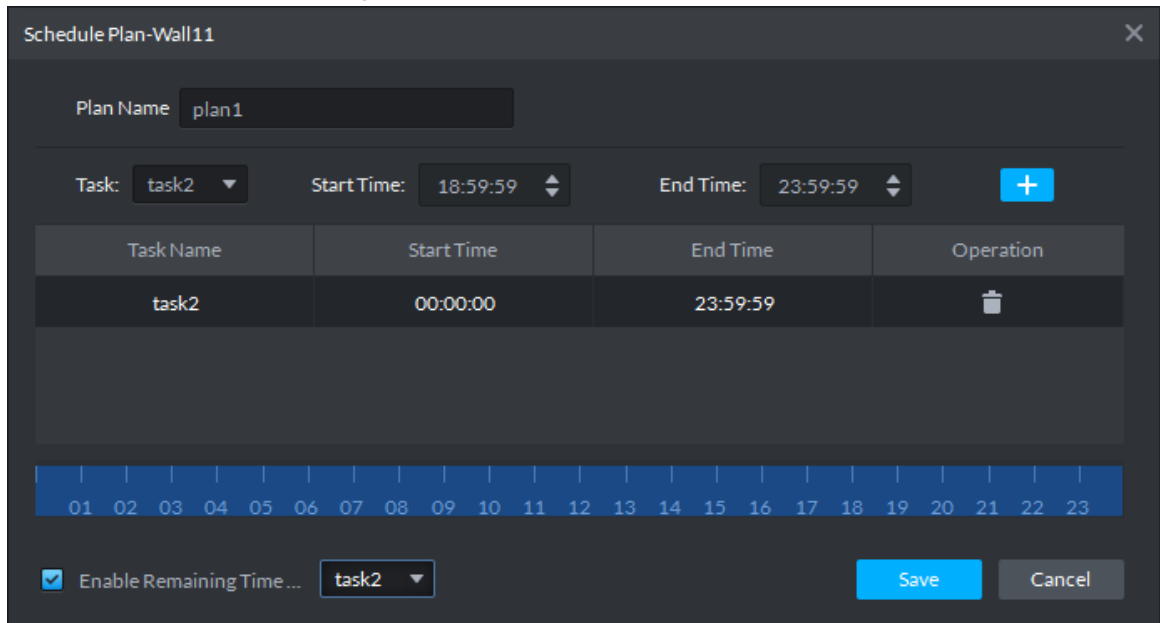

Step 2 Select .

Figure 5-136 Set schedule plan



Step 3 Enter the plan name.



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

The list displays detailed plan information. The specified period on the timeline is highlighted as blue.



Select the **Enable remaining time schedule** check box, and then set the task. The video wall displays corresponding video if it is not in the scheduled plan period.

Figure 5-137 Task time



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

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

Step 5 Click **Save**.


Step 6 Click  to start the 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.

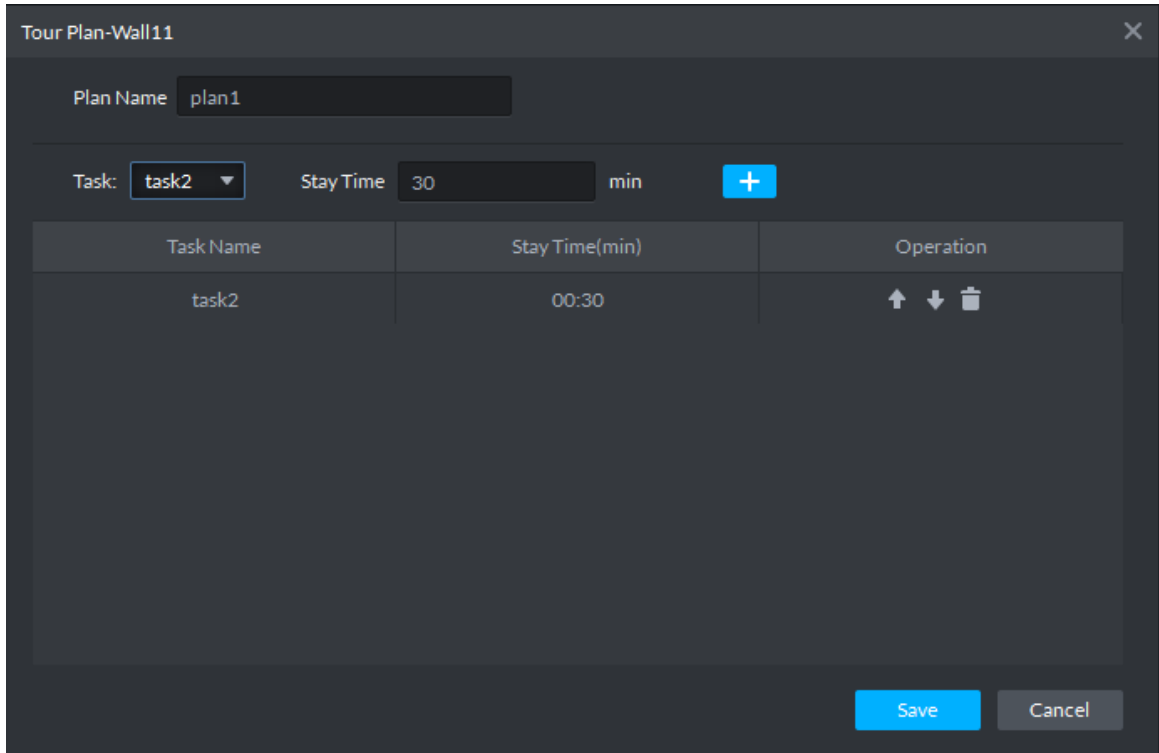
5.8.3.2 Configuring Tour Plan

After setting tour plan, you can output several plans to the TV wall.



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

Step 2 Click .

Figure 5-138 Tour plan



Step 3 Input task name.

Step 4 Select a video task and then set stay time. Click  .



Click  to adjust task sequence; click  to delete task.

Figure 5-139 Tour information



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

Step 5 Click Save.

Enter Video wall plan interface.

Step 6 Click  to start the 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.

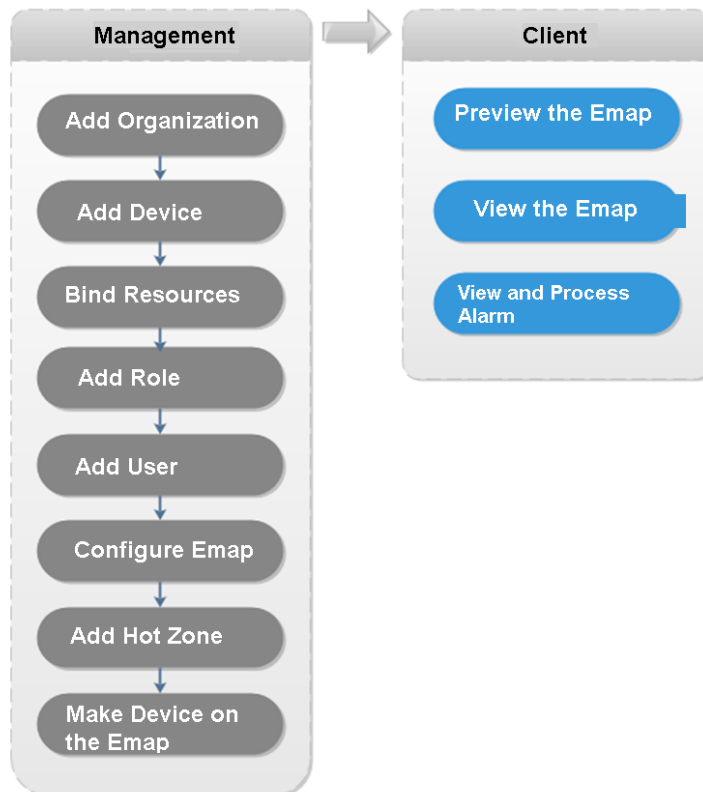
5.9 Emap

On the DSS client, you can view the configured e-map and corresponding device information.

5.9.1 Preparations

Refer to "4.8 Configuring Map" to add emap and hot zone on the platform manager and mark the device on the map.

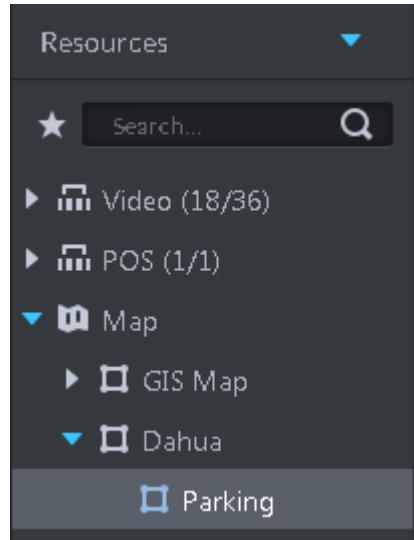
Figure 5-140 Emap business flow



5.9.2 Opening Emap in Live View

Step 1 On the **Live View** interface, click **Map** at the bottom of the device tree on the left.

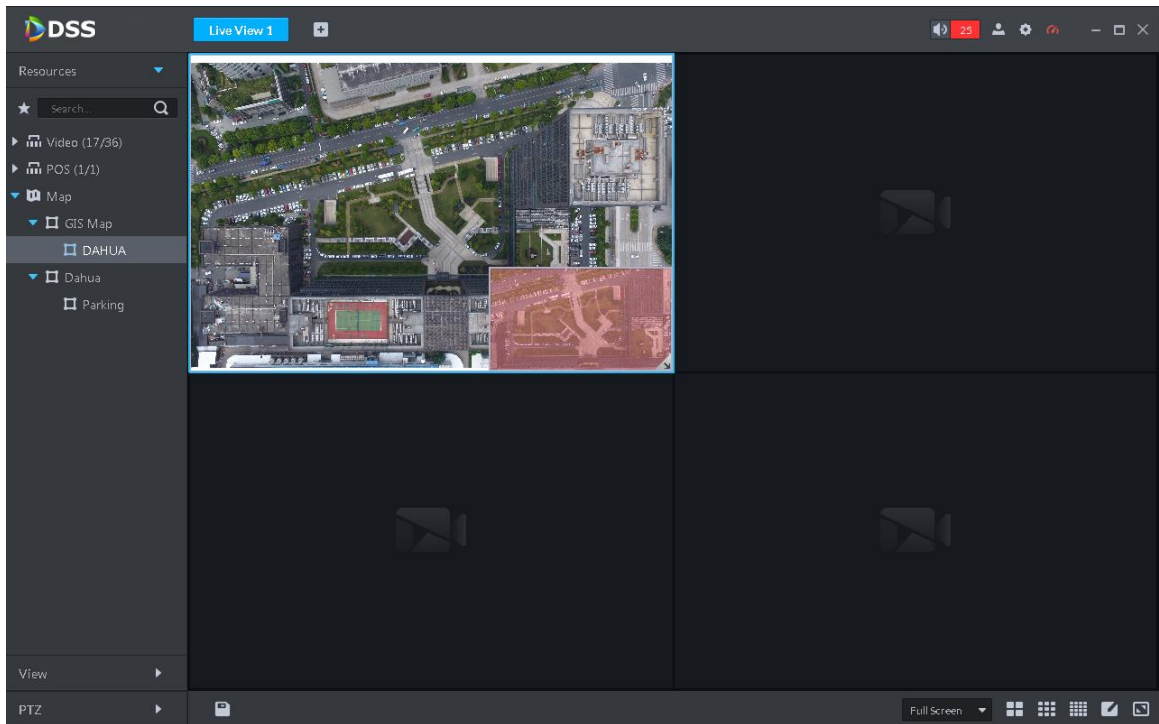
Figure 5-141



Step 2 Double-click a map, you can view the map and the added devices.

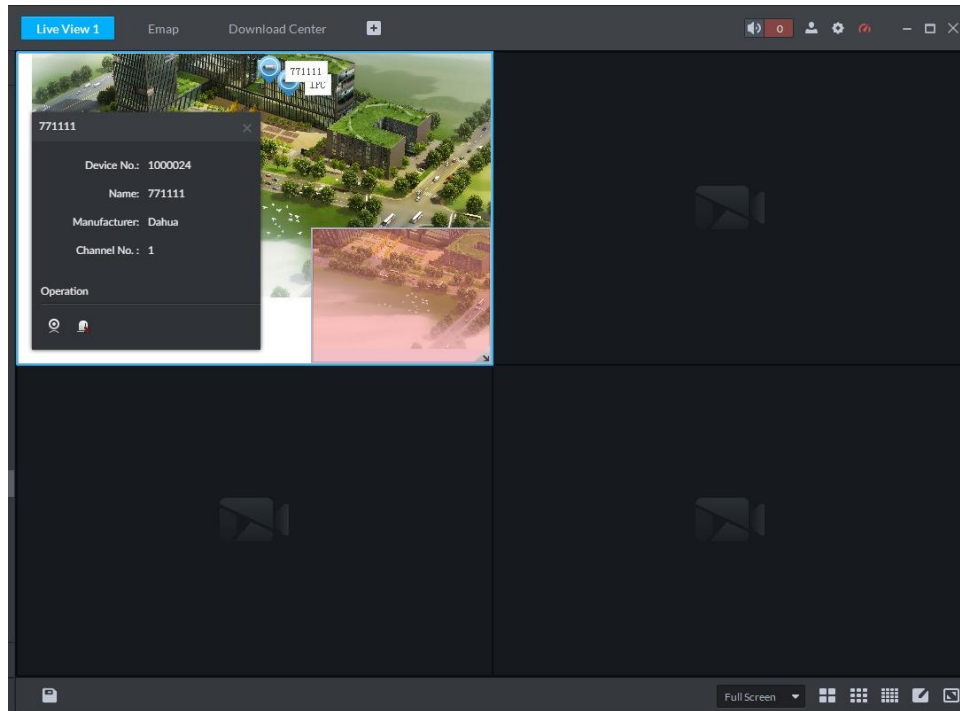
On the map, you can record real-time video, playback record file, cancel alarm, etc.

Figure 5-142 Map



Step 3 Click the marked channel.

Figure 5-143 Channel details




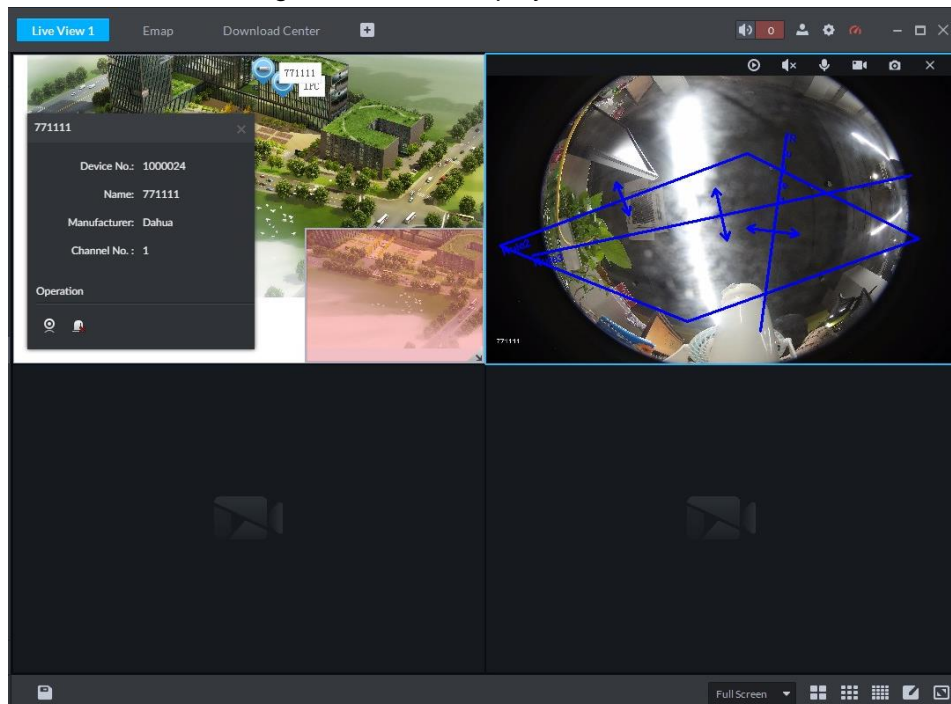
Step 4 Click  to playback real-time video on the window..

Figure 5-144 Video playback



5.9.3 Viewing Map

Here we use Google map to continue.

Step 1 Click , on the **New Tab** interface select Emap.

Step 2 Select Google map or raster map.

Figure 5-145 Emap

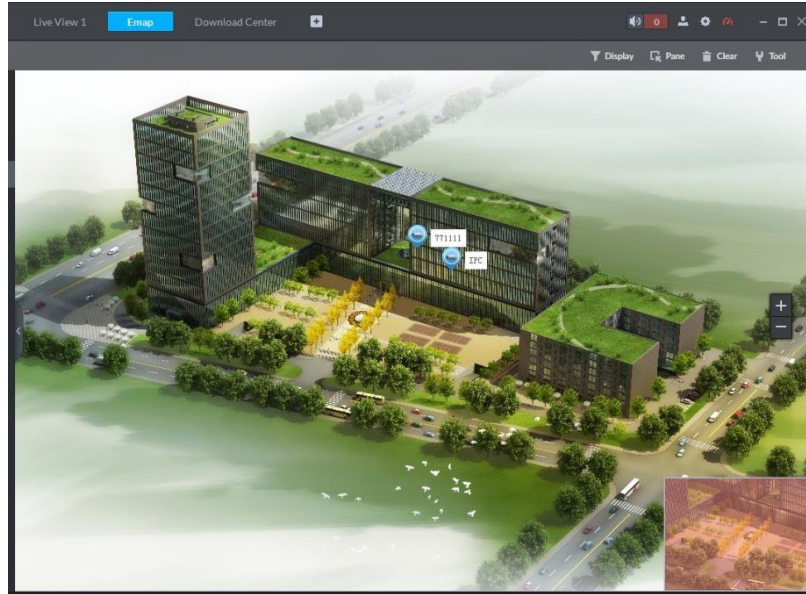


Table 5-45 Description

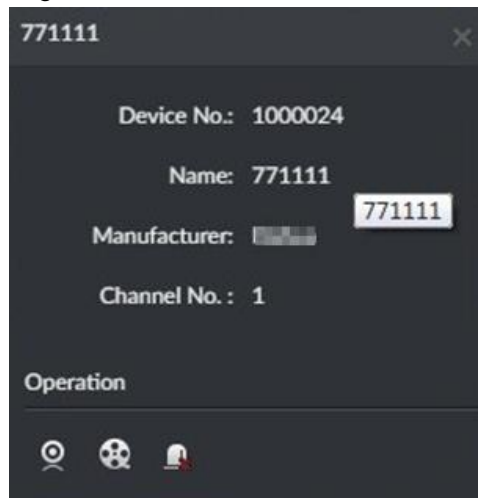
No.	Name	Description
1	Display	It is filter to display video device, alarm input channel.
2	Pane	Use frame to select a device.
3	Clear	Clear selection track on the screen.
4	Tool	It includes mark, reset, and video relay. <ul style="list-style-type: none"> ● Mark: It is to give a mark on the map. ● Reset: The map restores default position. ● Video relay: This function is null right now.



Step 3 Double-click the channel on the device tree on the left, you can view the channel position on the map.

Step 4 Click the channel on the map.

System displays device No., channel name, manufacture, channel information, etc.

Figure 5-146 Channel details




- Click  to playback video of current channel.
- Click  to playback record.

- Click  to cancel alarm.

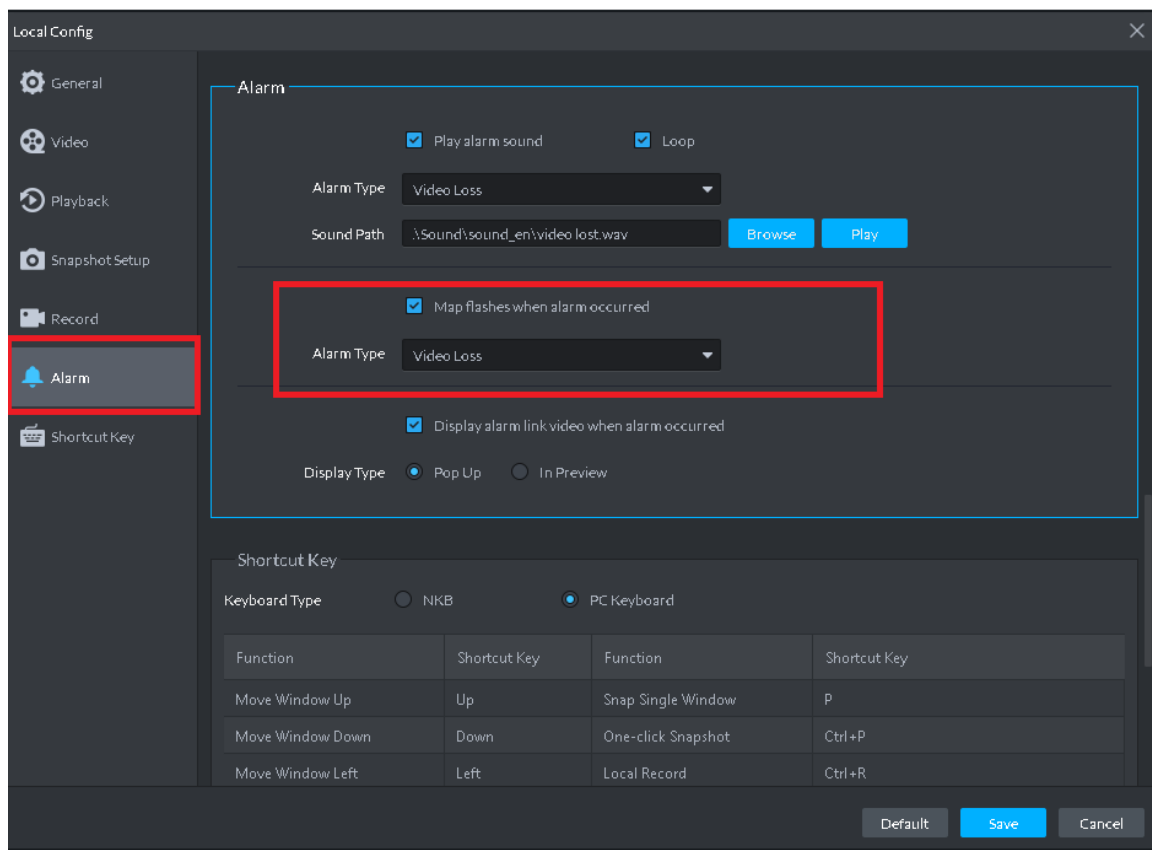
5.9.4 Alarm Flashing on the Map

5.9.4.1 Configuring Alarm Flashing on the Client

Step 1 Click  at the upper-right corner, it is to open General interface.

Step 2 Click the **Alarm** tab, select Map flashes when an alarm occurs and then set alarm type from the dropdown list.

Figure 5-147 Set alarm type



Step 3 Click Save.

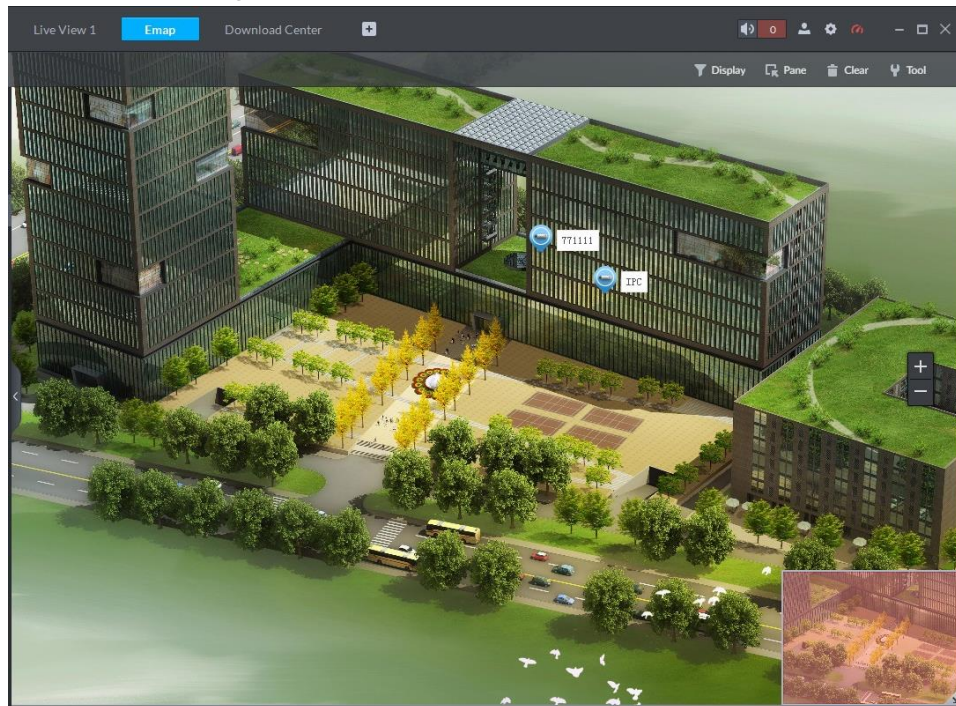
5.9.4.2 Client Triggering Alarm

Step 1 Click , on the **New Tab** interface select Emap.

Step 2 Click to go to Google map or Raster map.
Here we use raster map to continue.

Step 3 The channel is flashing when an alarm occurs.

Figure 5-148 Alarm channel flashes



5.10 Flow Analysis

The system supports flow analysis functions including people counting and heatmap.

5.10.1 Preparations


- IPC with people counting or area statistics function is added to the client. Refer to 4.5 Adding Device.
- After adding the IPC, click , and then select the **Cross Line Statistics** or **Area Statistics** from the drop-down list according to the requirement. See Figure 5-150.

Figure 5-149 Select camera features

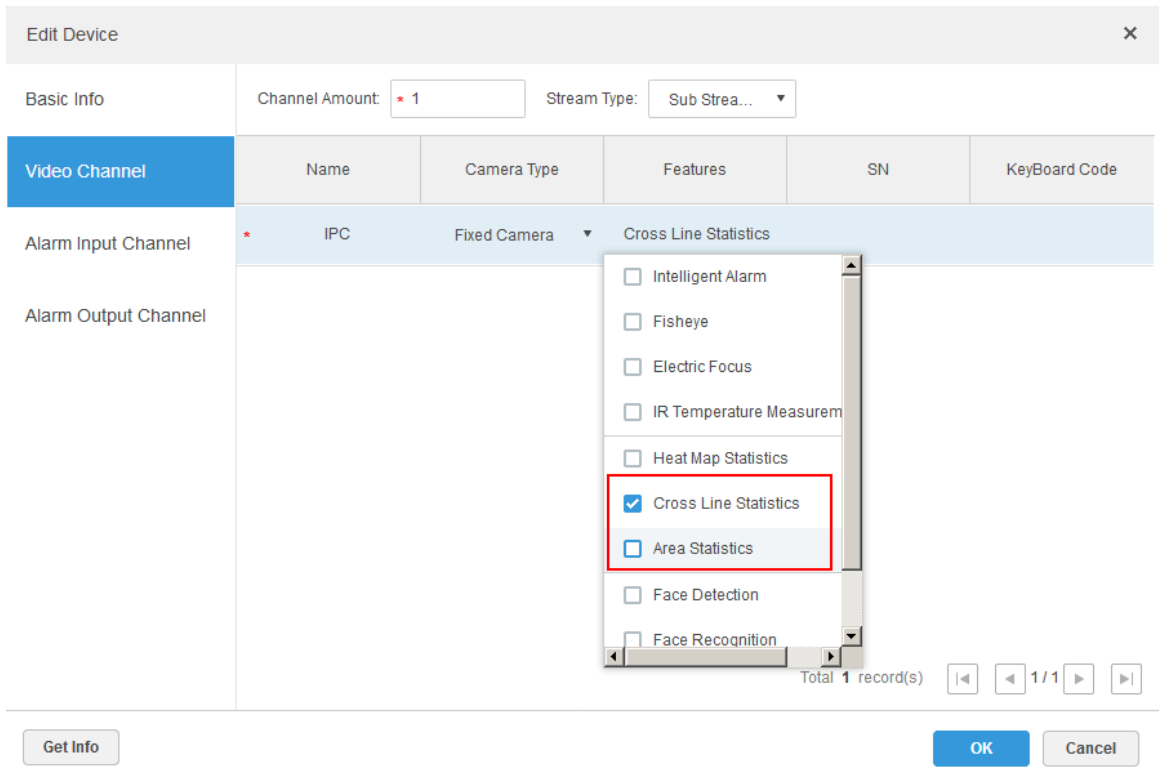
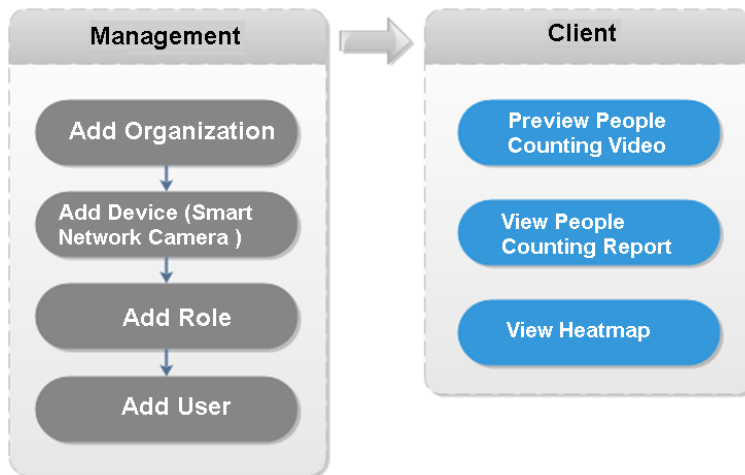


Figure 5-150 People counting business flow

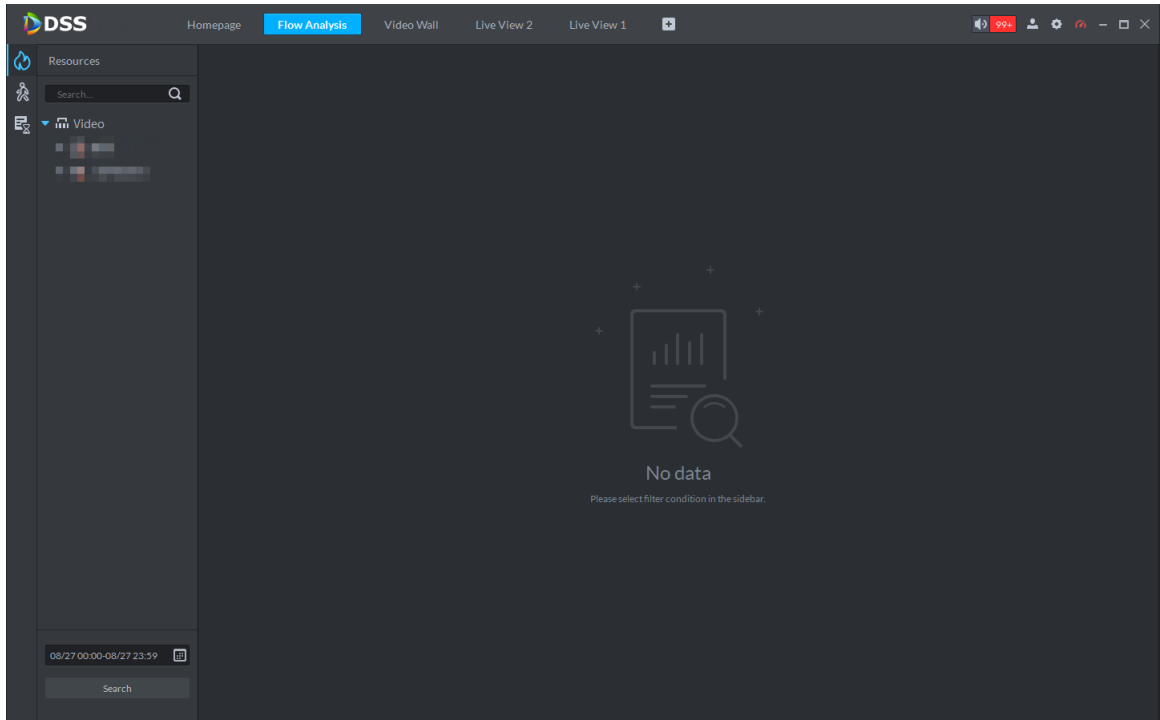



5.10.2 Heatmap

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 5-151 Heatmap



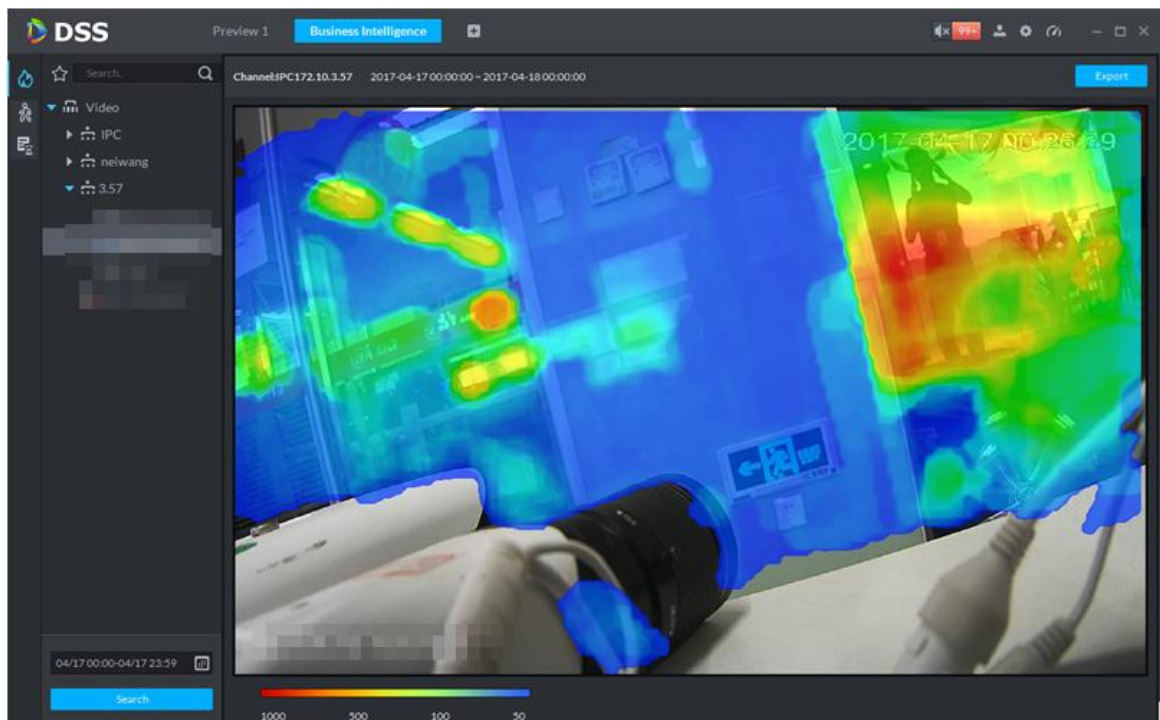
Step 2 Click the  tab on the flow analysis interface.

Step 3 Select a channel, set time, and then click **Search**.



The device sends heat map 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 5-152 Heatmap interface



Step 4 Click **Export** at the upper-right corner to export heat map in .bmp format.

5.10.3 People Counting Report

View reports 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.


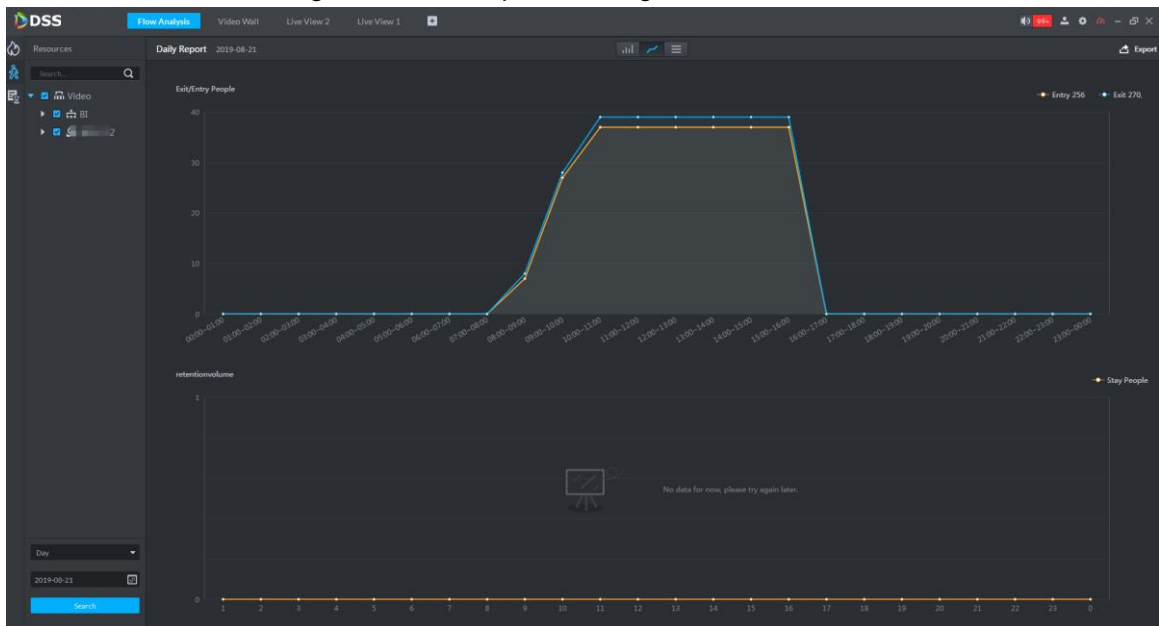
Step 1 Click  on the **Flow Analysis** interface.

Figure 5-153 People counting interface



Step 2 Select a people-counting channel, set report type and search time, and then click **Search**. The report is displayed. See Figure 5-154.

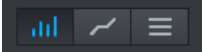
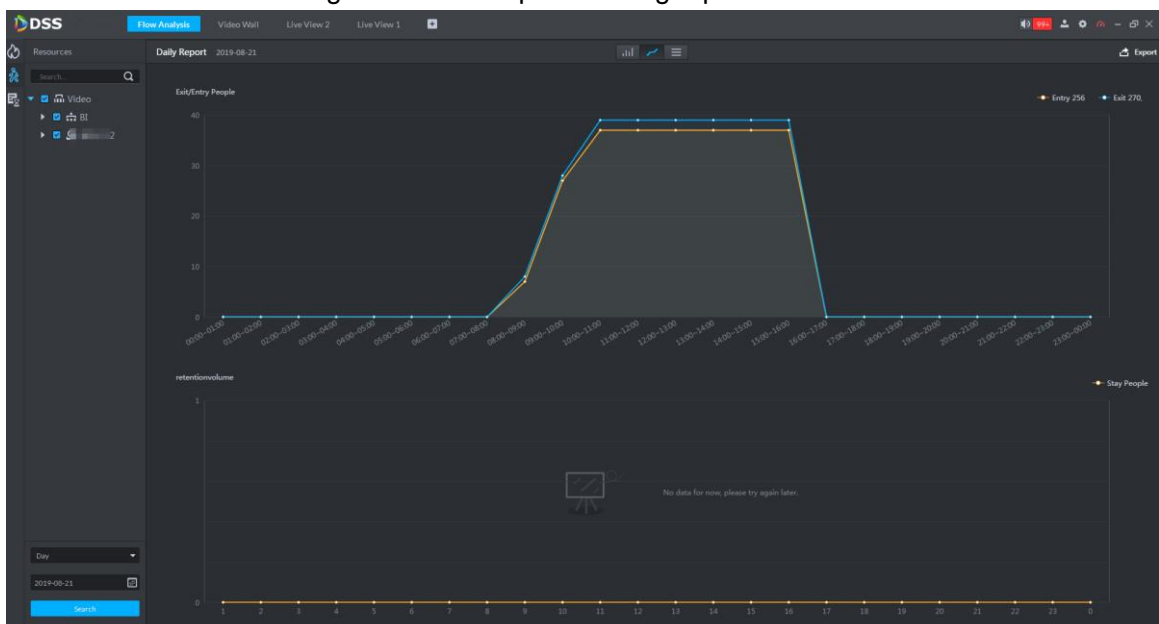
To switch to bar chart or list, click the corresponding tabs on the  section.

Figure 5-154 People counting report



To save the report, you can click **Export** at the top-right corner. The report is exported in the .pdf format.

5.11 Human Face Recognition

5.11.1 Preparations

- Refer to "4.10.1 Creating Face Database" to create human face database on the manager.
- Refer to "4.10.2 Arm Config" to arm human face database on the platform manager.

Figure 5-155 Face recognition business flow



5.11.2 Real-Time Human Face Video

Human face recognition function is applied to real-time video and snapshot human face image.

Step 1 Click , on the **New Tab** interface select Face recognition.

Step 2 Click .

Figure 5-156 Live video

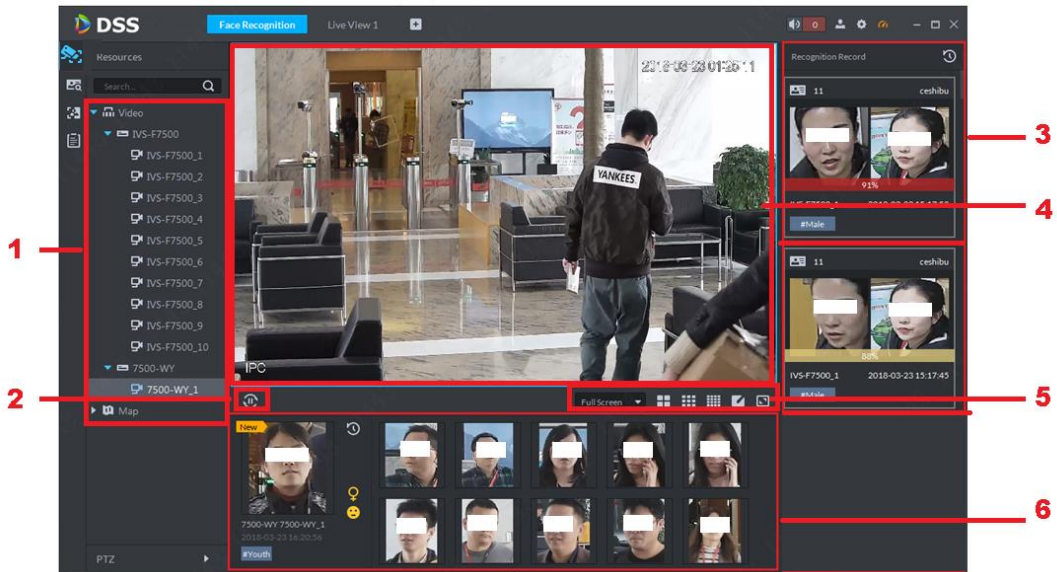







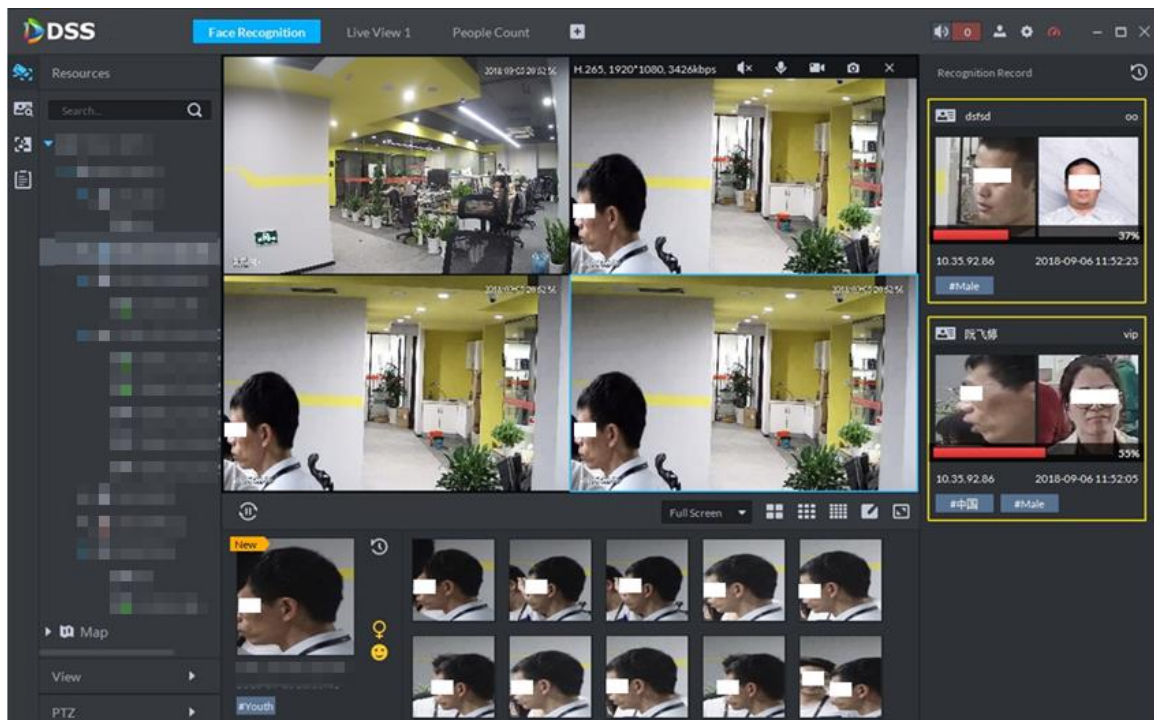
Table 5-46 Description

No.	Name	Description
1	Device tree	It is to display device information.
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	Recognition history record	It is to display the snapshot human face image of the video.
4	Monitor window	It is to 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	 Image display rate	<ul style="list-style-type: none"> There are two modes: full screen, and original scale. The full screen refers to one window at the full screen.
	 Window split switch	It is to display switched window amount. System supports customized settings.
	 Full screen display	The system displays window at full screen.
6	Snapshot human face image display pane	It is to display snapshot human face image.

Step 3 Enable live view.

- Select a monitor window (white frame means it is the checked window). Double-click a channel or record file to enable real-time surveillance.
- Drag the channel or the video file to the monitor window.

Figure 5-157 Enable live view



Step 4 Double-click snapshot human image.

System displays human detailed information interface.

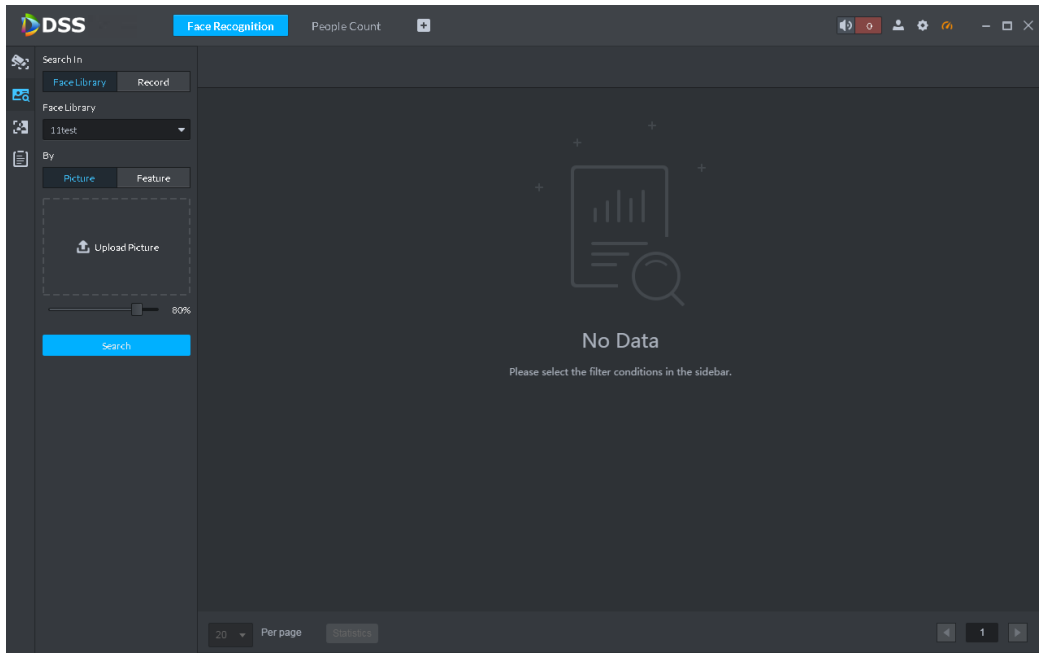
5.11.3 Face Search

With the human face recognition function, you can search for face pictures you are interested in by setting person features including age and gender or uploading a face picture. Support searching the face database or snapshot records.

Step 1 On the **Face Recognition** interface, click



Figure 5-158 Face search

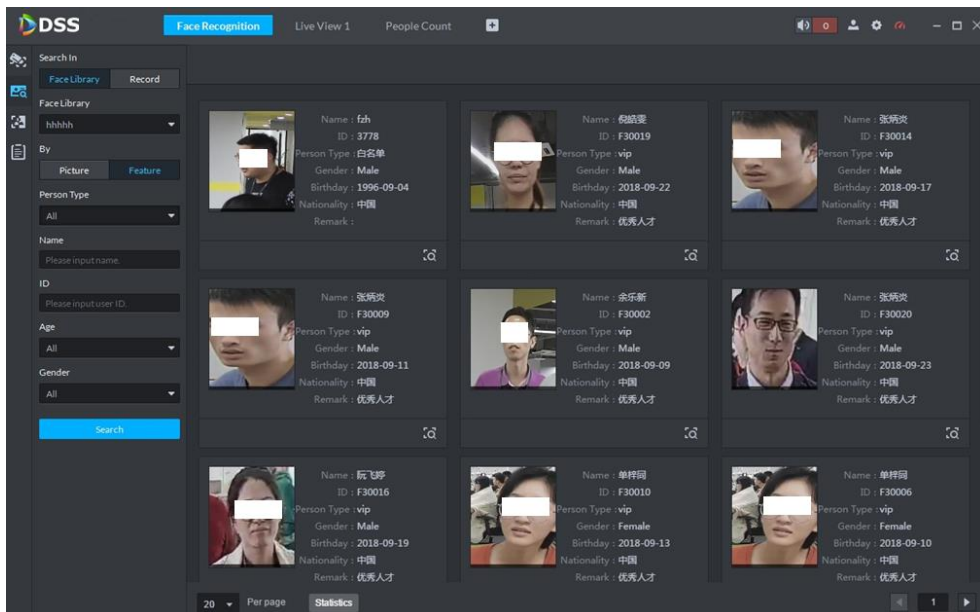


Step 2 Set search conditions.

- You can search the face database (by selecting the **Face Library** 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.
- In the **Sequence** dropdown list, you can select **Start from Earliest Time** or **Start from Current Time** to set time sequence for the results.

Step 3 Click **Search**.

Figure 5-159 Search result



Up to 1000 earliest or latest results can be displayed at once.

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. See Figure 5-160.

Figure 5-160 Search results in list

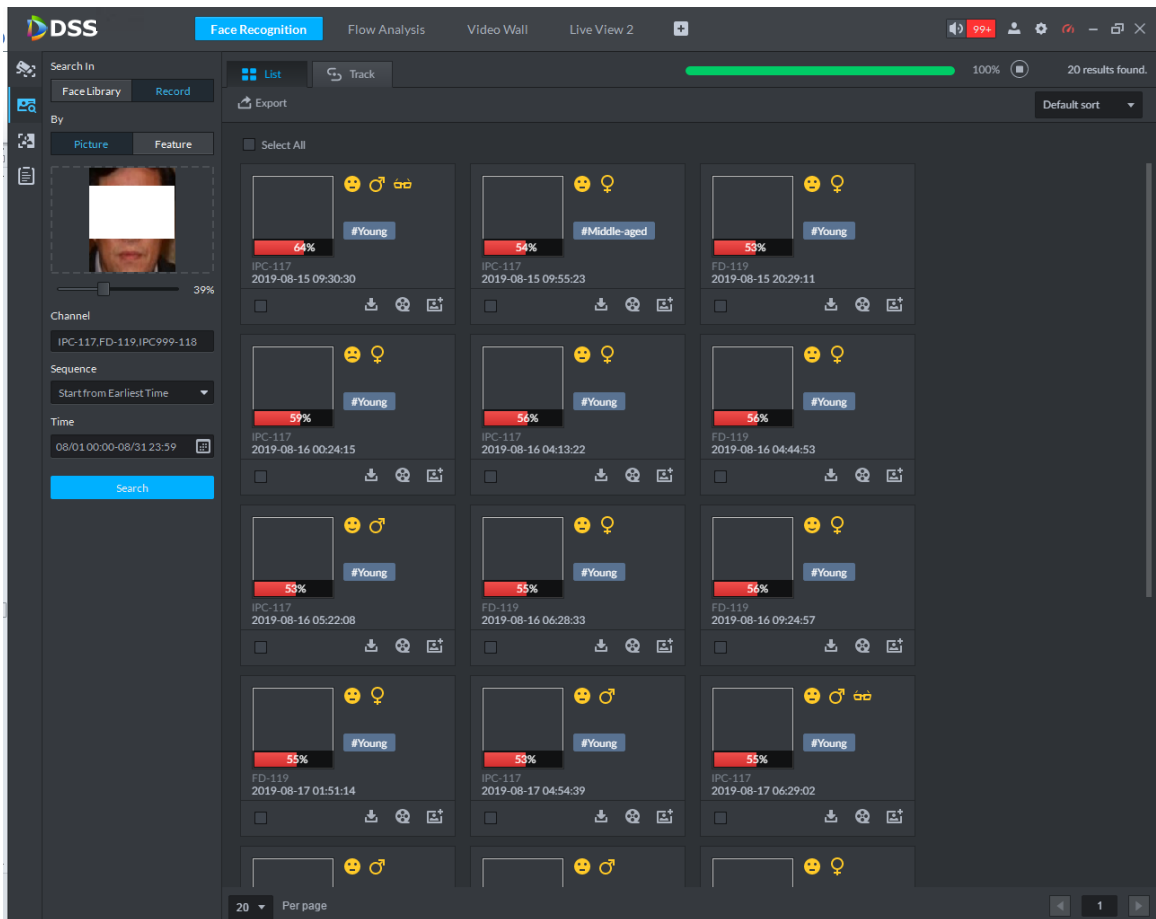




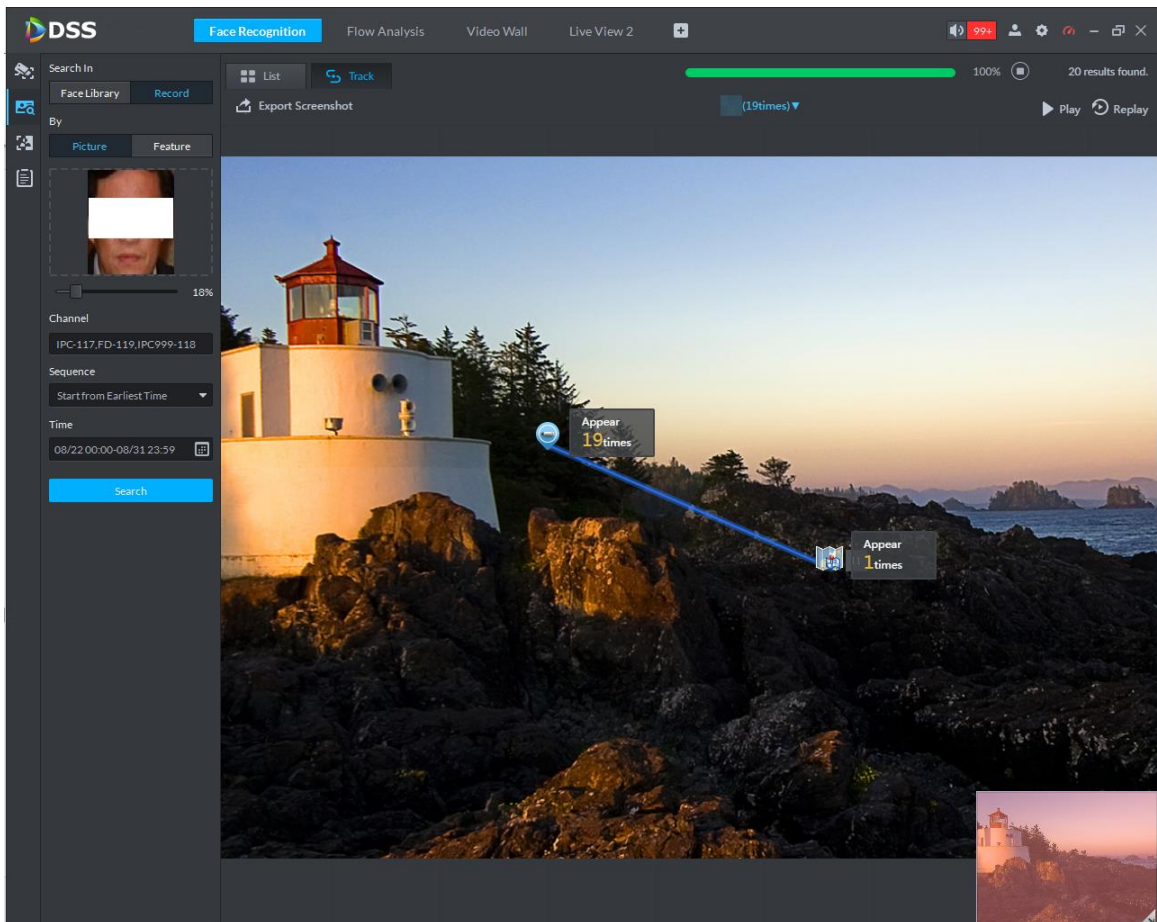
Table 5-47 Functions description

Operation	Description
Download Record	Click to save rar file to the specified path. The .rar file contains the human face snapshot images and snapshot panoramic images.
Playback record	Click to playback the 15-seconds video record before and after the snapshot.

Operation	Description
Add person	<p>Add the snapshot person to the database.</p> <ol style="list-style-type: none"> 1. Click . 2. Set person information and then click OK.
Search record	<p>You can upload a face image to search for the target face record.</p> <ol style="list-style-type: none"> 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.

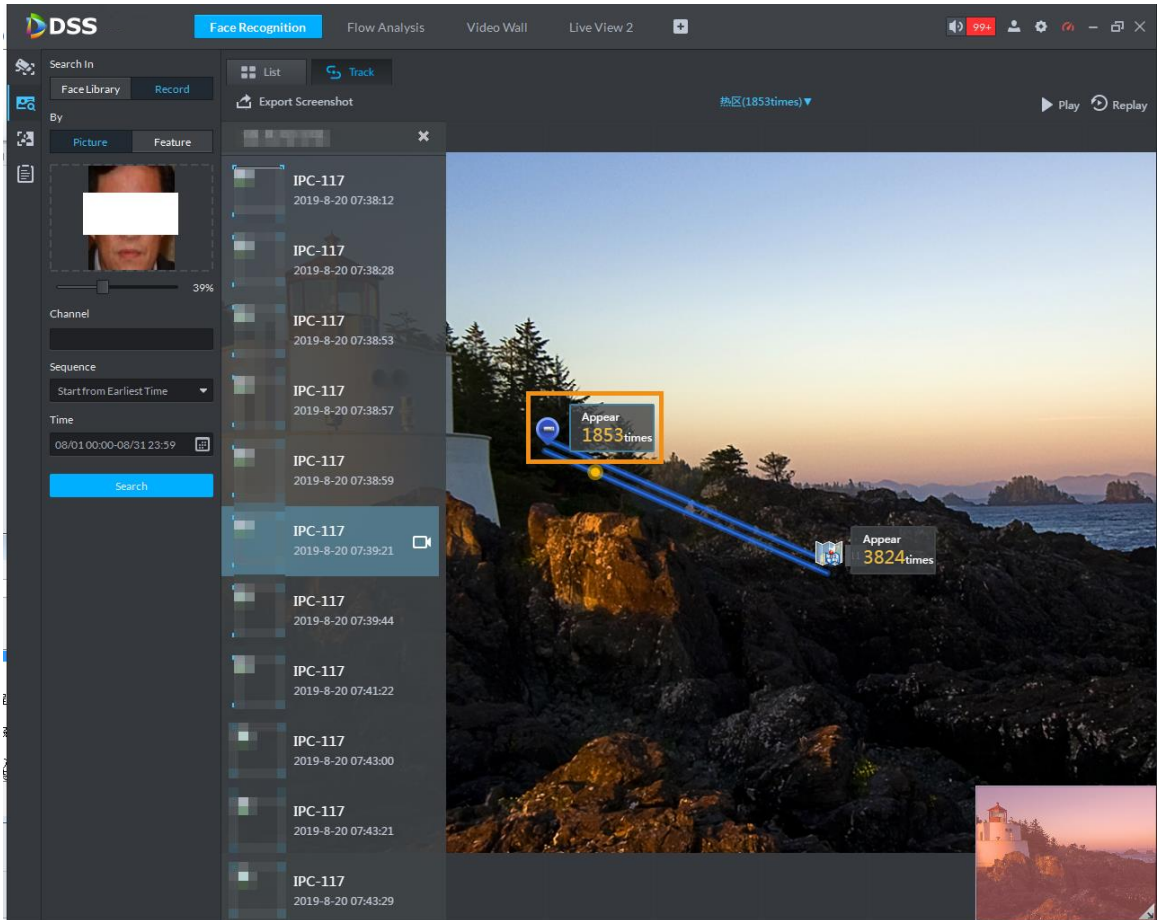
Figure 5-161 Face track on map



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 5-162 View detailed snapshot records



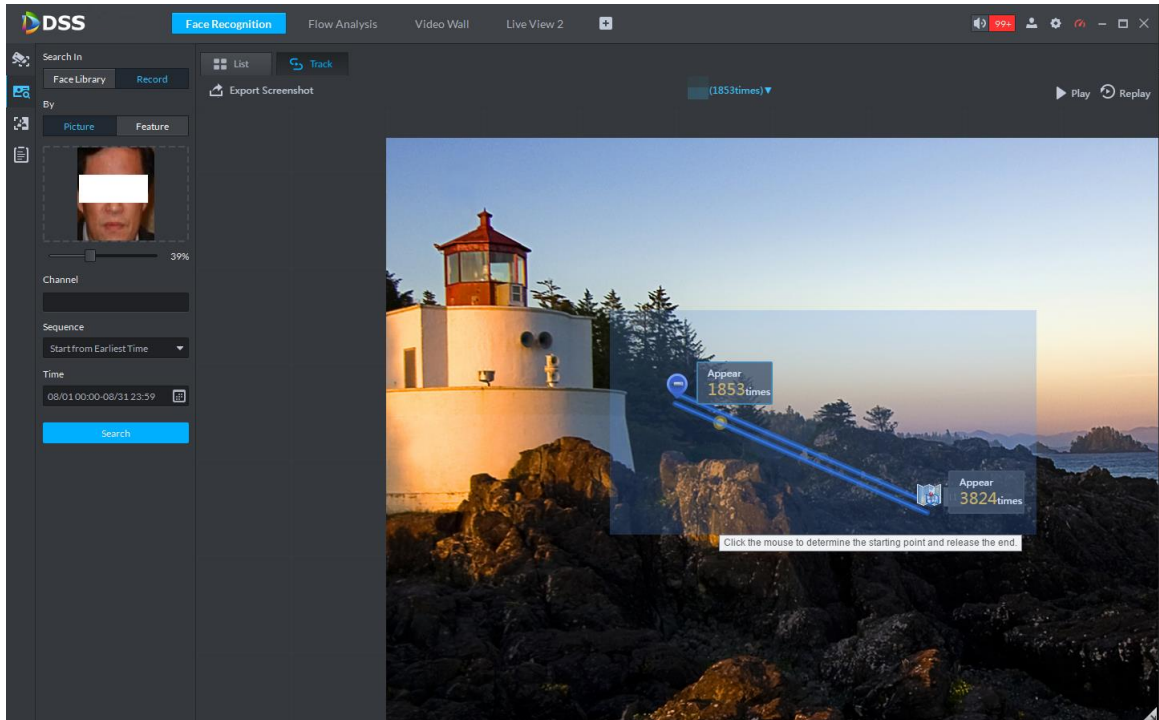
- Click  to play the moving track. Click  to stop. Click  to play again.

- 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**, select a desired area by drawing a frame on the map, and then follow the onscreen instruction to save the picture locally.

Figure 5-163 Export face track

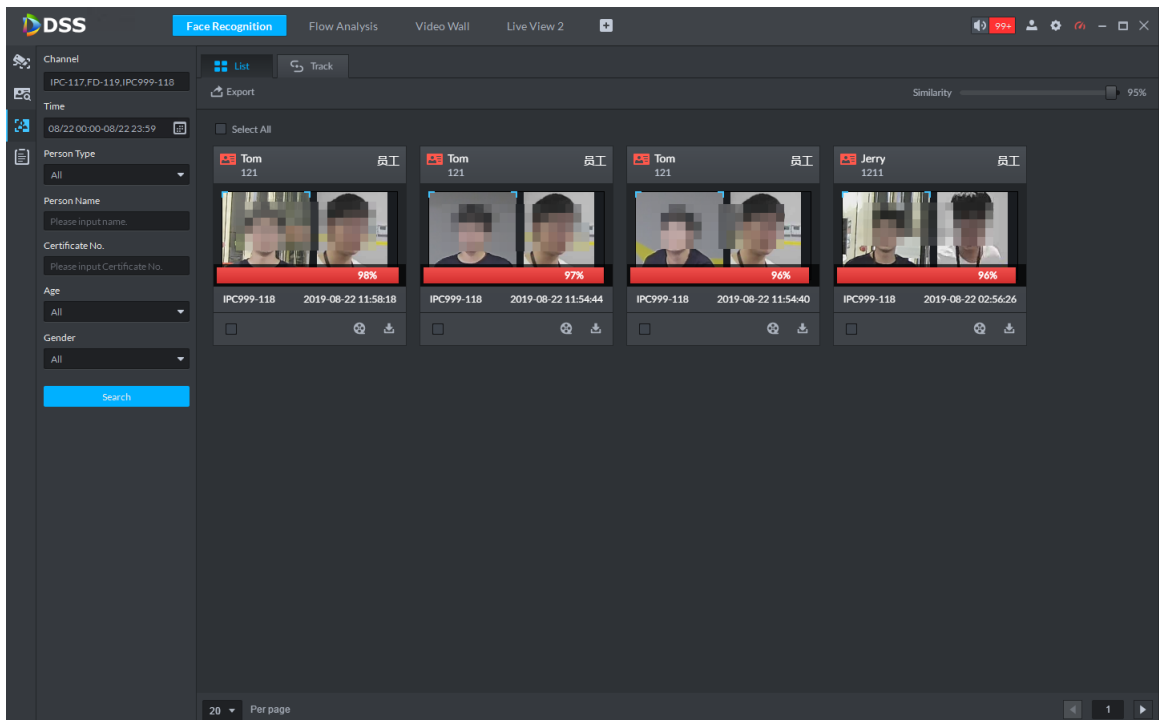


5.11.4 Face Recognition Record Search

Search the recognition records for specific 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 5-164 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**.

Up to 1000 pieces of records can be displayed. 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. See Figure 5-166. There is no image on the left if you do not upload image when setting search criteria

Figure 5-165 Records in list

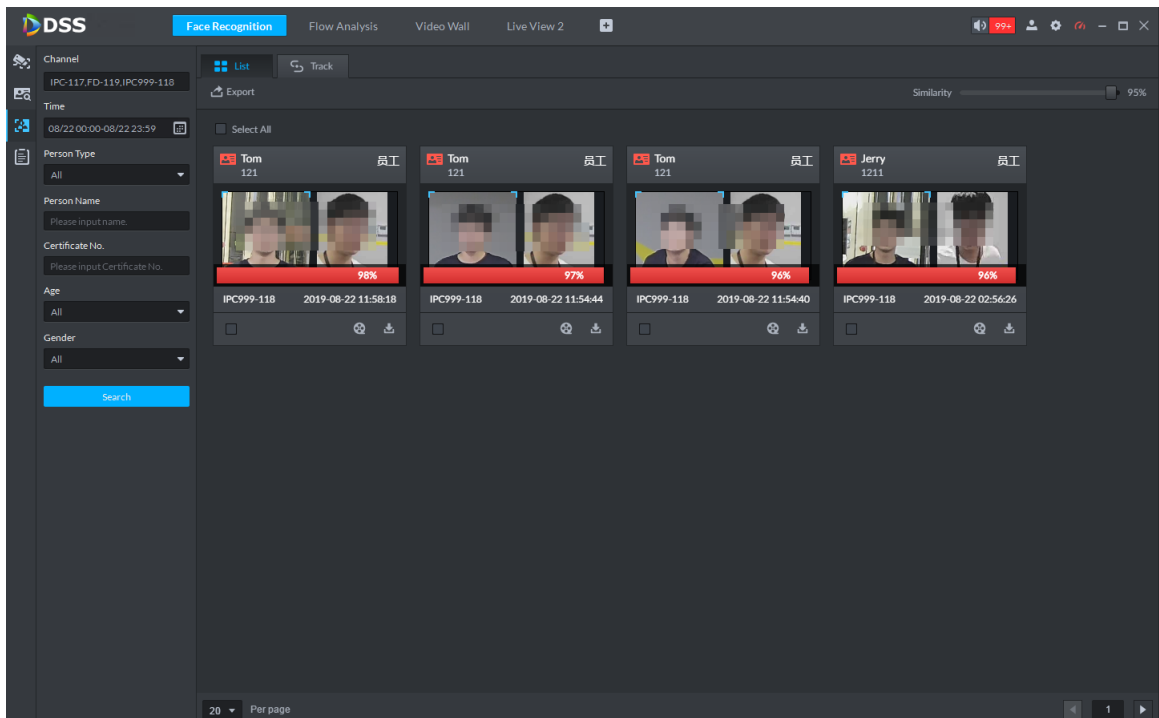


Figure 5-166 Record details

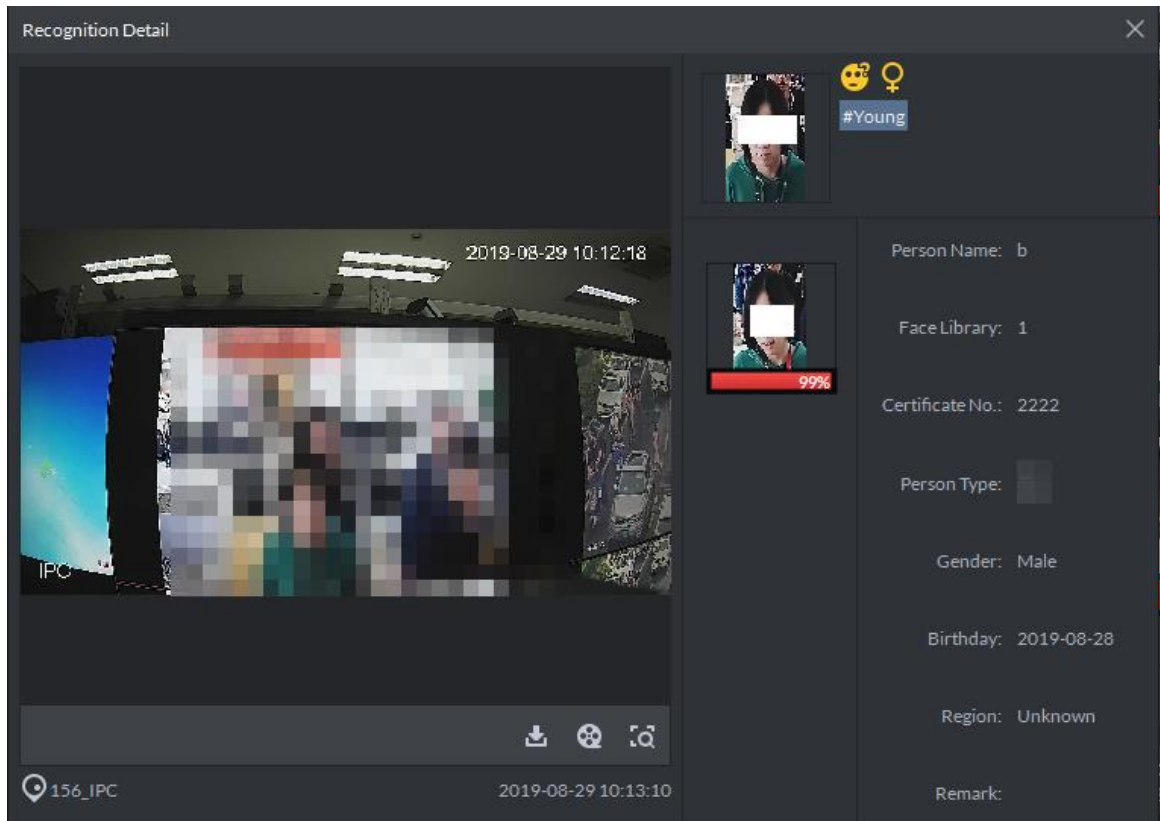



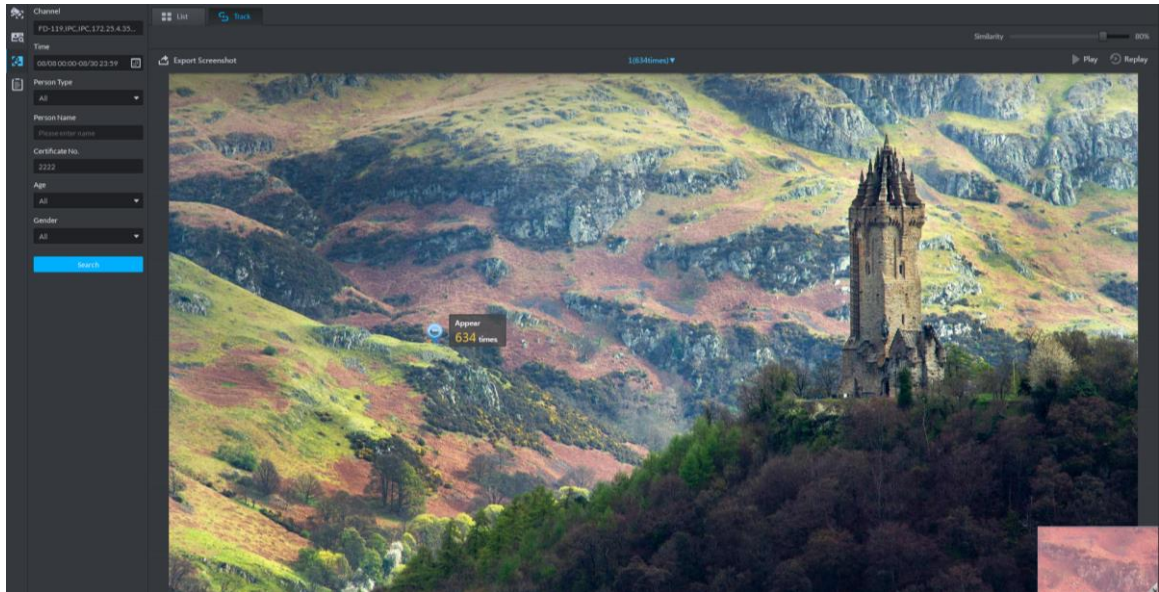


Table 5-48 Functions description

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.
Search record	Click  , and then system goes to human recognition search interface with the snapshot image.

- Click **Track**. The face track is displayed on the map. For more instruction about face track operation, see "5.11.3 Face Search."

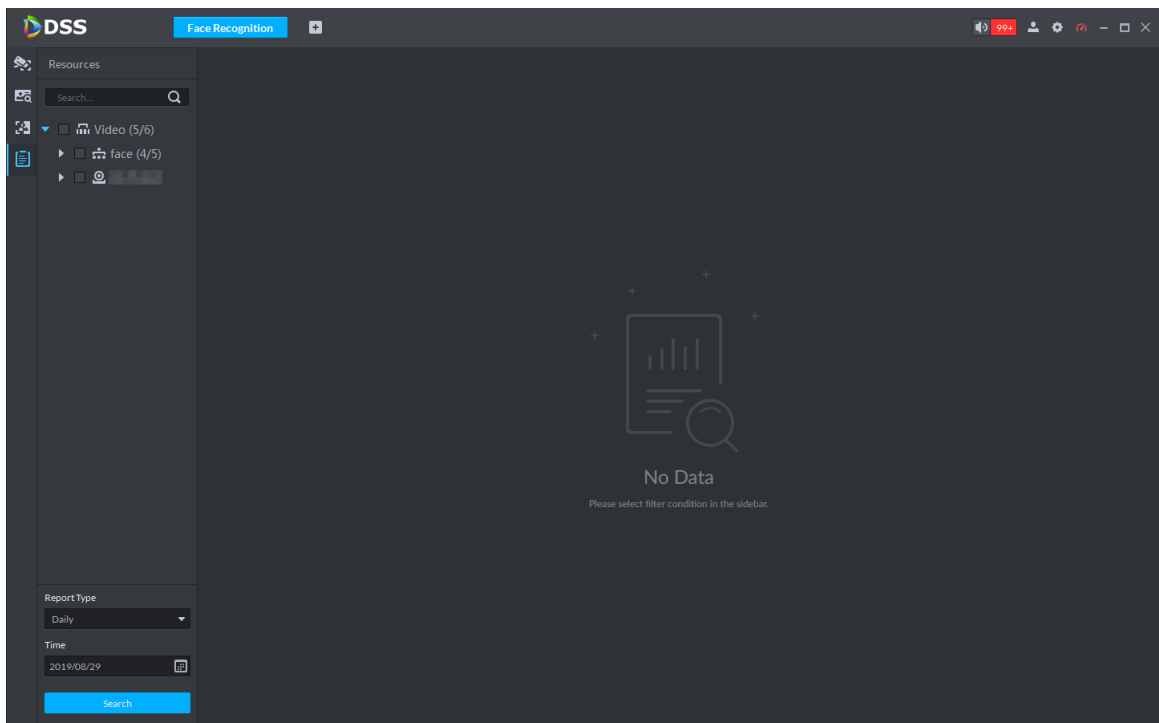
Figure 5-167 View face track



5.11.5 Statistics Report

Step 1 On the **Face Recognition** interface, click .

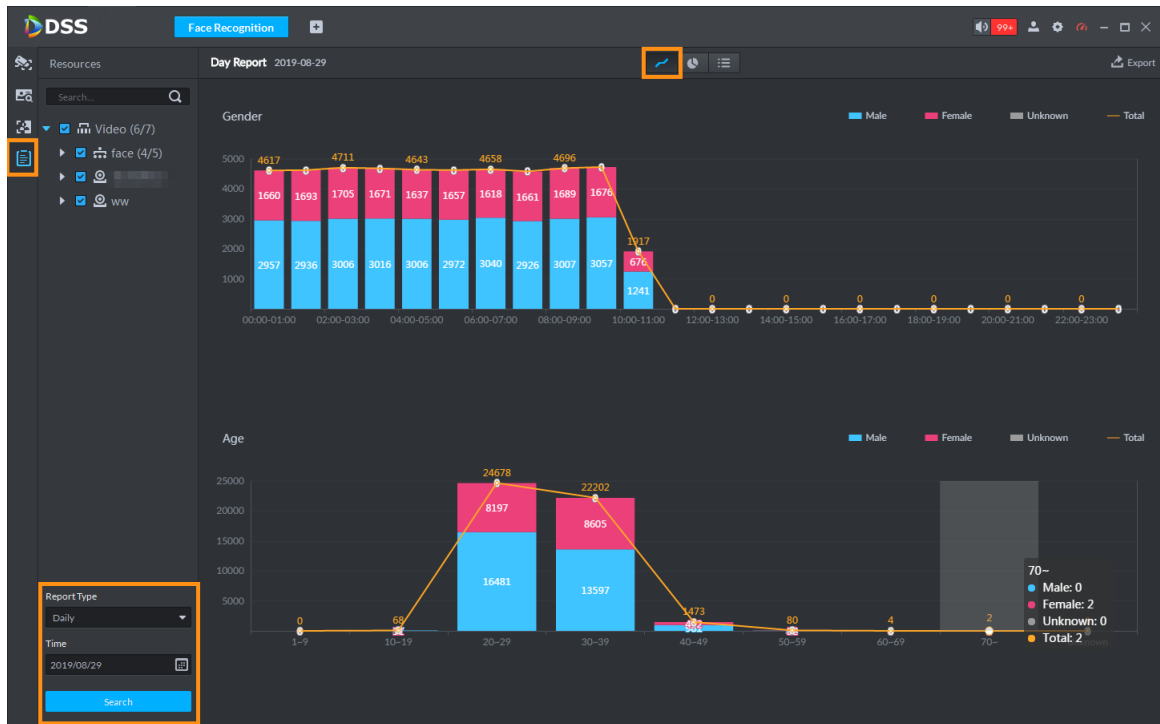
Figure 5-168 Statistics report search





Step 2 Set search criteria.
Set video channel, report type and time.

Step 3 Click **Search**.

Figure 5-169 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 the .pdf format.

5.12 Number Plate Recognition Applications

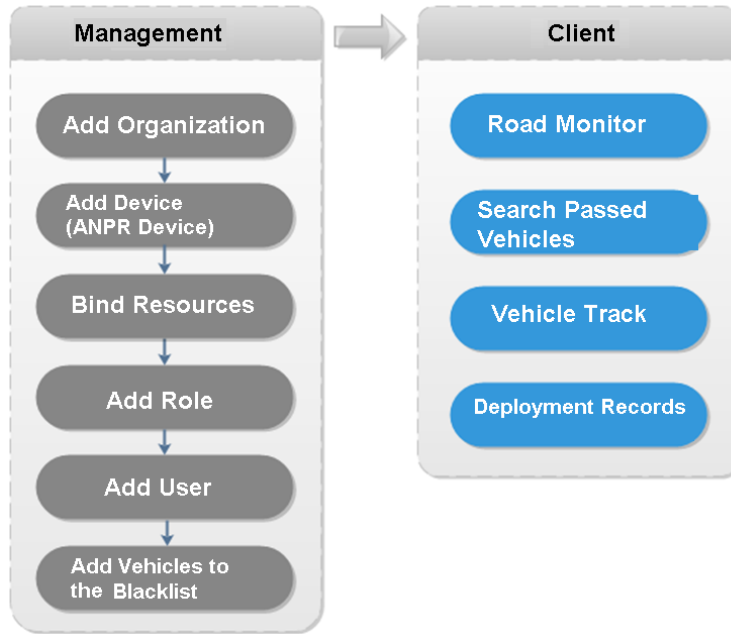
The platform can display automatic number plate recognition video and records. You can search for vehicle records and related alarms.

5.12.1 Preparations

- Refer to "4.5 Adding Device" to add ANPR device on the platform manager.
- Refer to "4.11 Adding Vehicle Blacklist" to add vehicle blacklist on the platform manager.

Refer to Figure 5-170 for road monitor flows.

Figure 5-170 ANPR business flow



5.12.2 Number Plate Recognition

Step 1 Click , on the **New Tab** interface select ANPR.


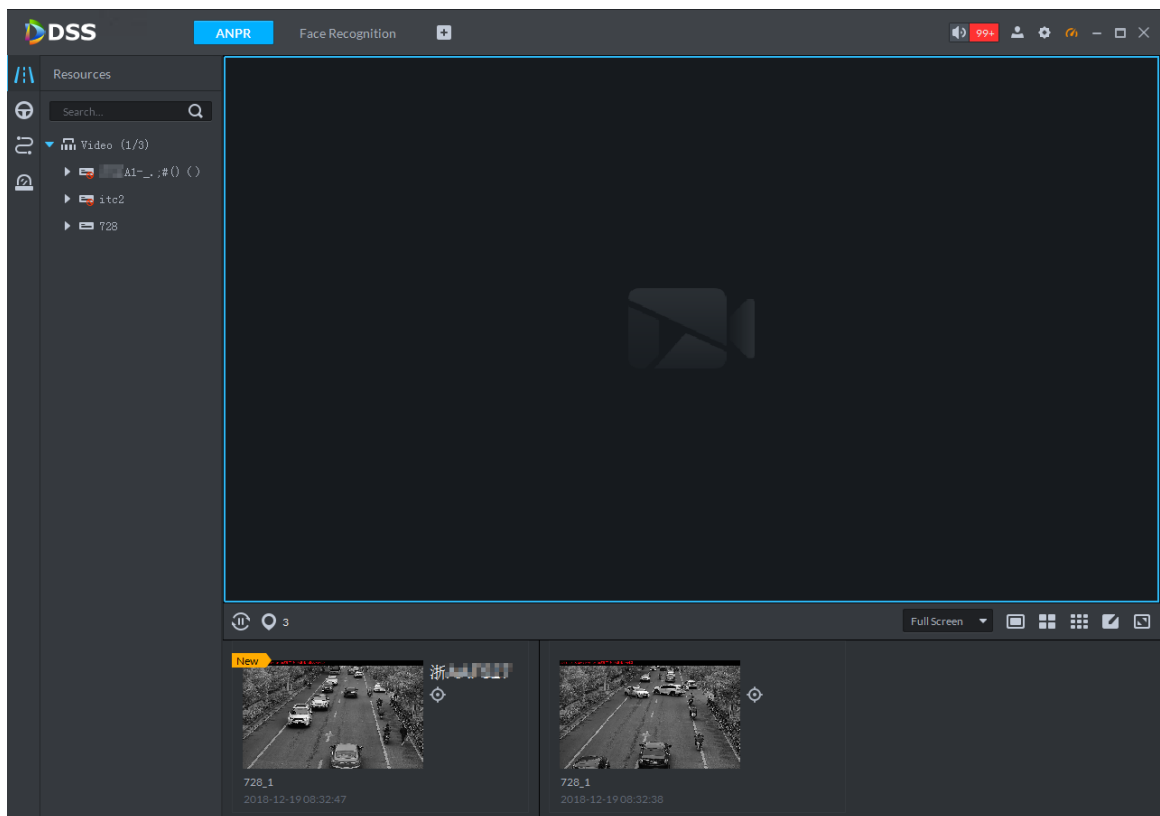
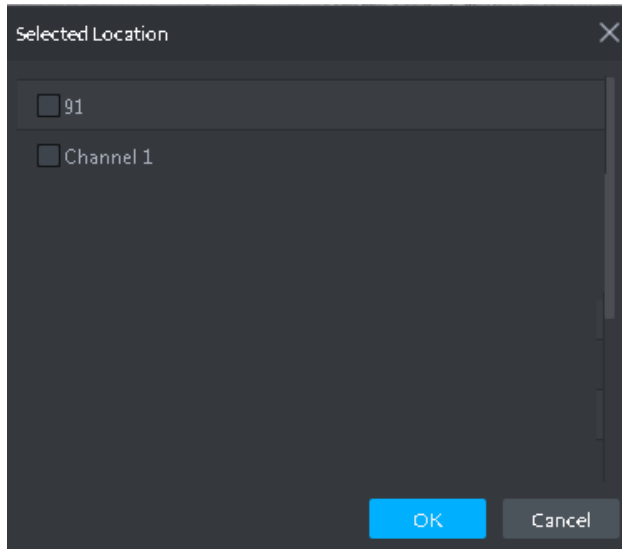
Step 2 Click , system displays ANPR interface.

Figure 5-171 ANPR interface



Step 3 Click  to select the ANPR channel..

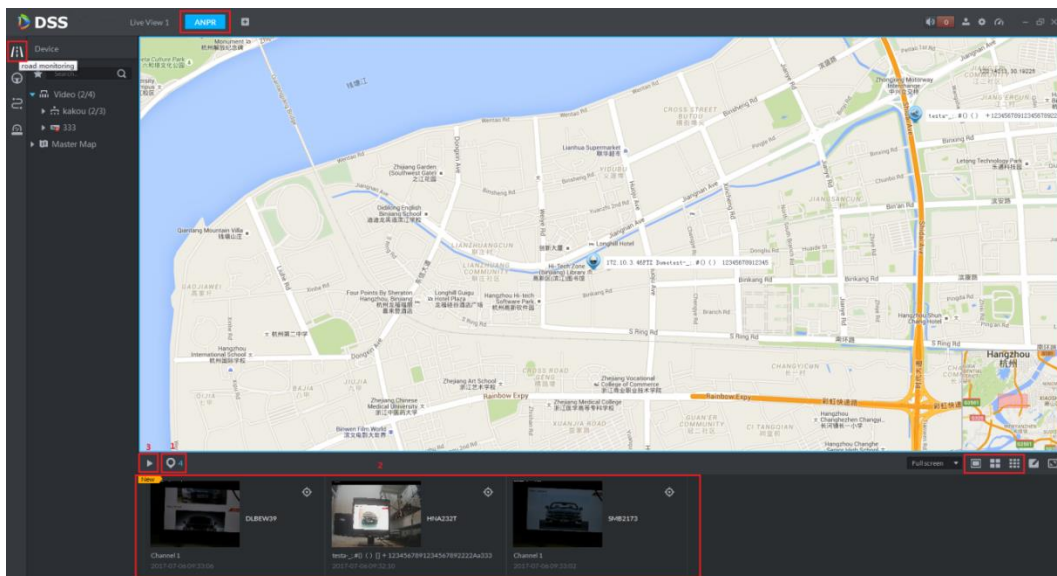
Figure 5-172 Select an ANPR channel



Step 4 Select ANPR device and then click **OK**.

System displays the selected channel amount and the latest passing vehicle image on the rolling pane. See Figure 5-173.

Figure 5-173 ANPR view

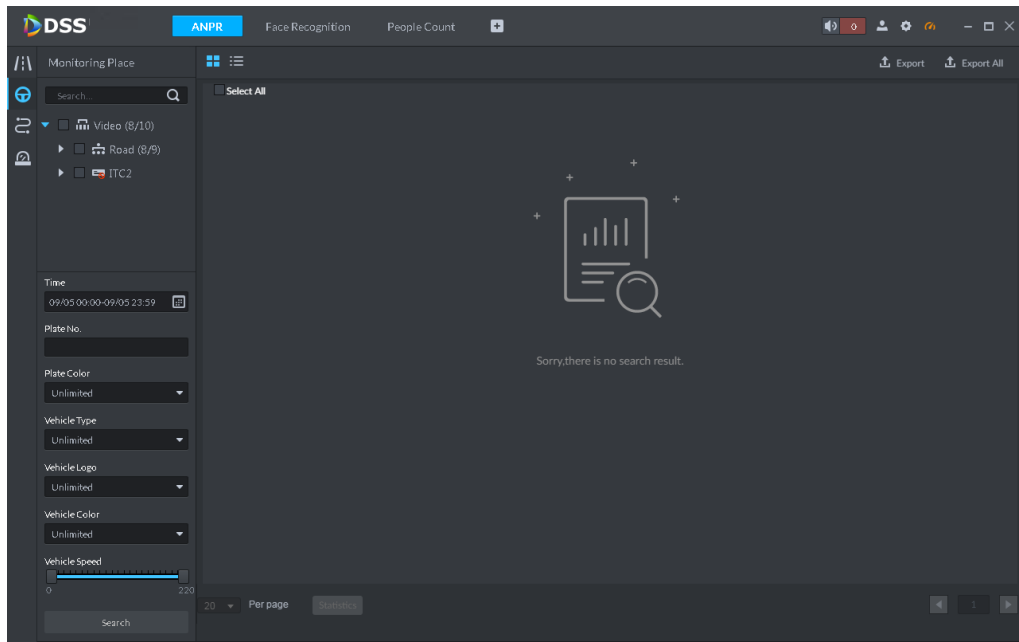


Step 5 Double-click the image to view image details. It includes plate number, snapshot time, ANPR channel name, vehicle logo, vehicle color.

5.12.3 Searching Passed Vehicle

Step 1 Click .

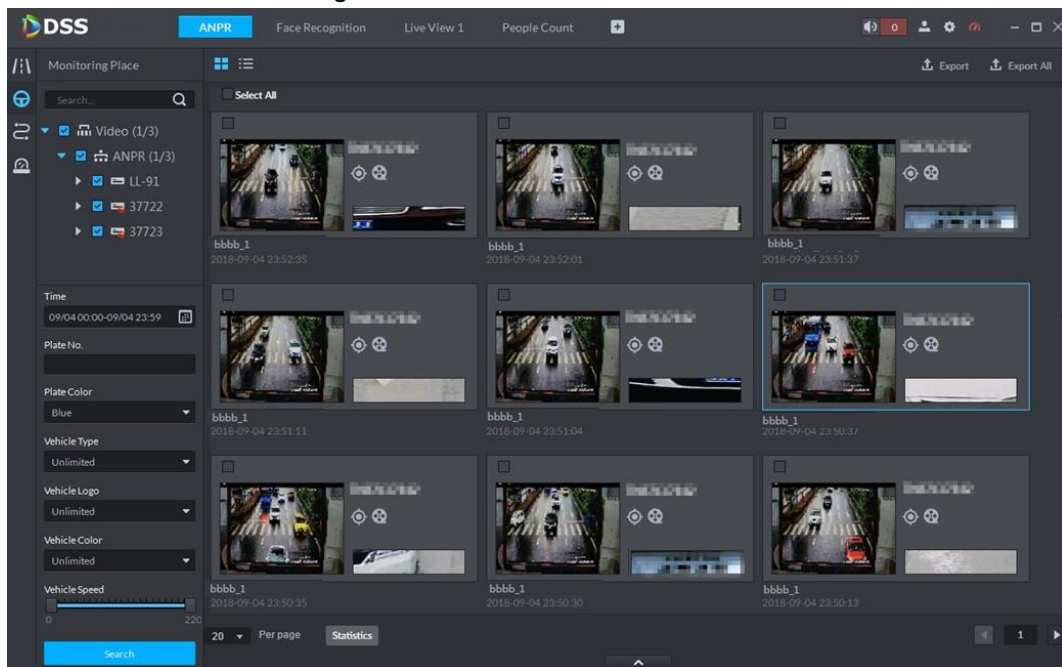
Figure 5-174 Vehicle record search



Step 2 Select video channel and search criteria. It includes time, plate number, plate color, plate type, vehicle logo, vehicle body color and lane.

Step 3 Click **Search**.

Figure 5-175 Search results



For the passed vehicle, you can view its detailed information, record and running track. Refer to the operations listed below.




- Click view mode () or list mode () to select different display mode.
- Select a snapshot image and then click  or double-click the image, system displays detailed information. Move the cursor to the middle to select the specified zone, you can zoom in it.

Figure 5-176 Vehicle record

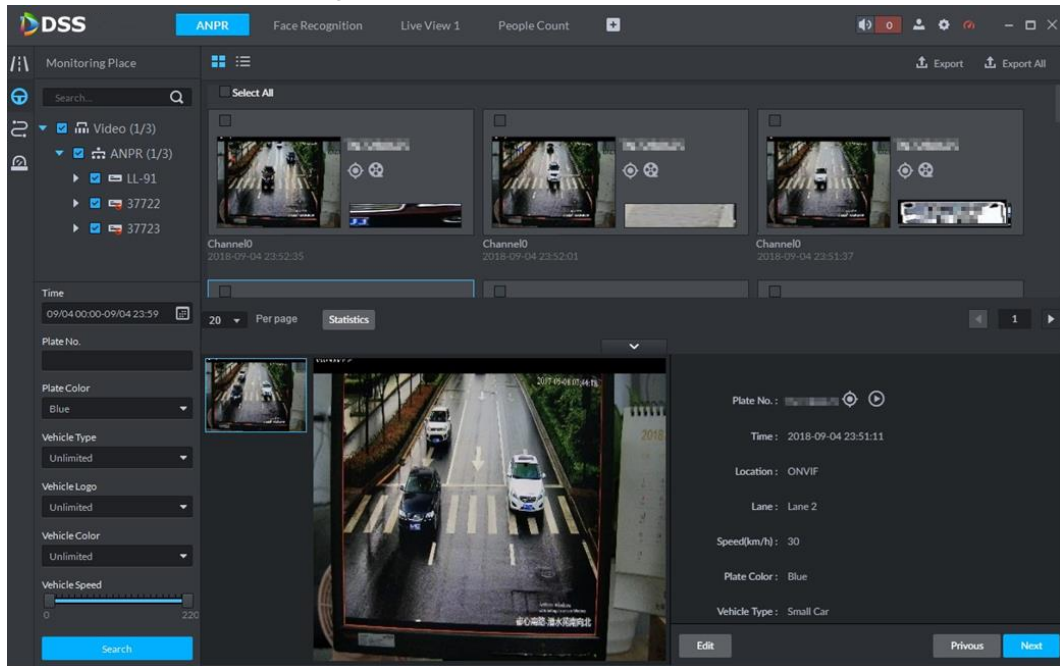
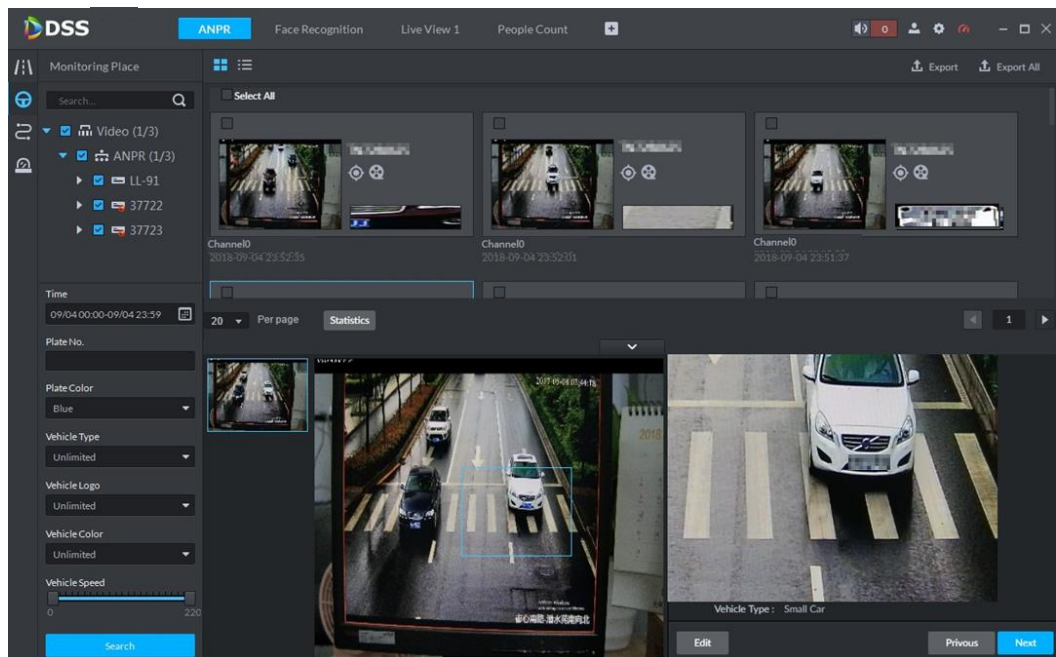


Figure 5-177 Zoom in image




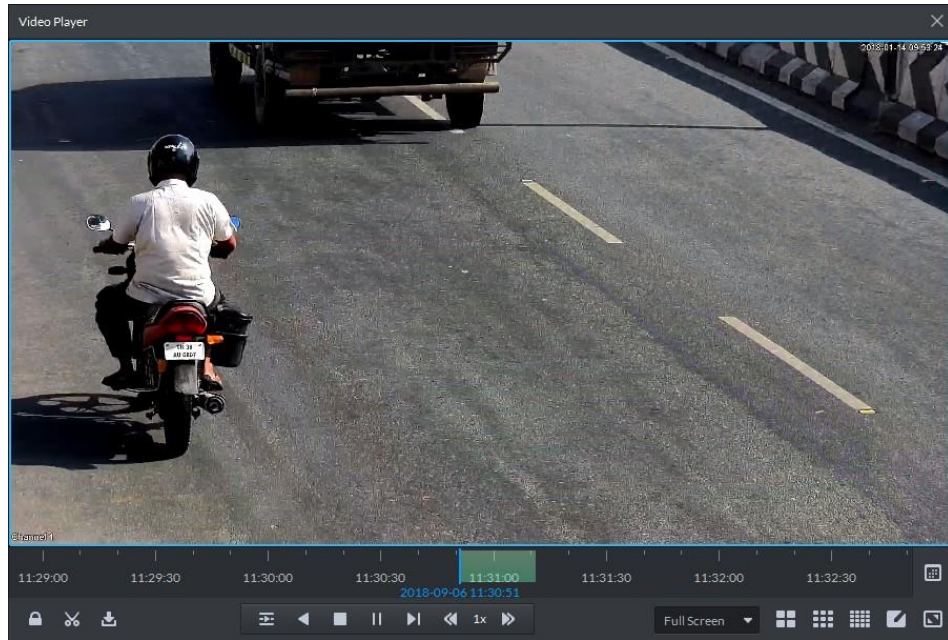

- Click  to playback the 15-second video before and after the vehicle passed time. See Figure 5-178. The video file is total 30 seconds. It is to display the 15-second video before and after the vehicle passed.

Figure 5-178 Vehicle video playback



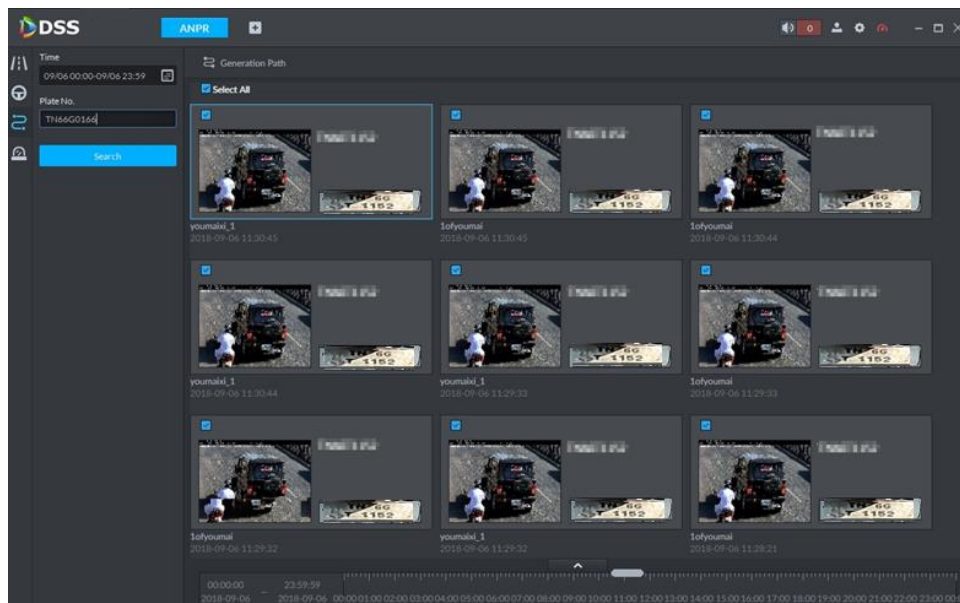
- Click  to view the vehicle running track. Refer to "5.12.4 Vehicle Track for detailed information."
- Export: Select the passed vehicle information and then click **Export**. It is to export selected passed vehicle. Click **Export all**, it is to export all searched passed vehicle information.

5.12.4 Vehicle Track

Step 1 Click .

Step 2 Select time and then enter a plate number. Click **Search**.

Figure 5-179 Vehicle track records



Refer to the operations listed below.


- Select the snapshot image and then click  or double-click the image, you can view snapshot vehicle detailed information. Move the cursor to the middle to select the specified zone, you can zoom in it.

Figure 5-180 Vehicle record

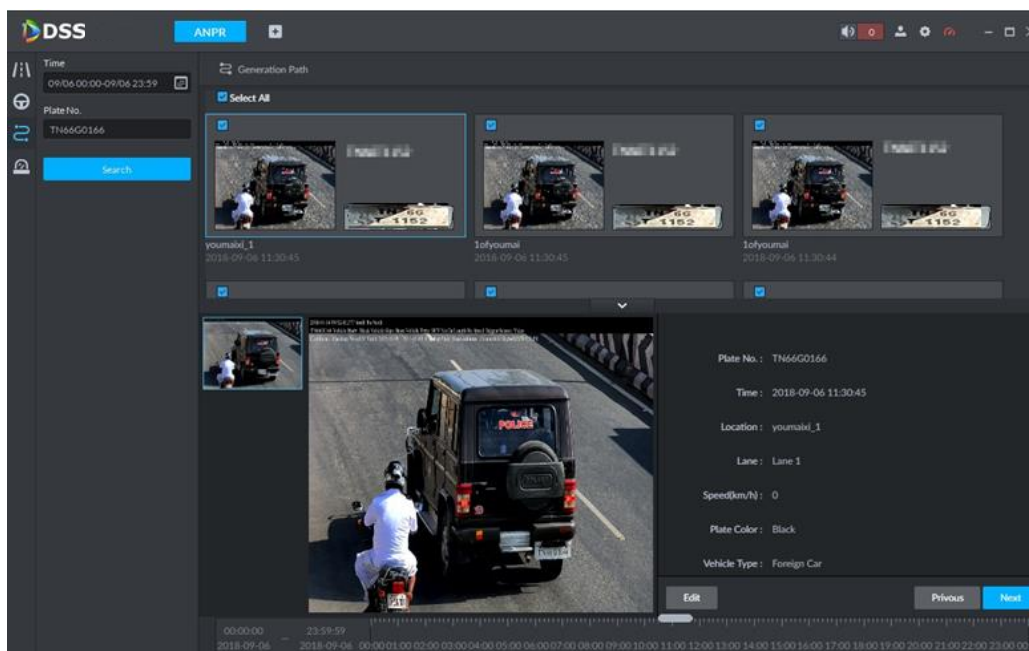
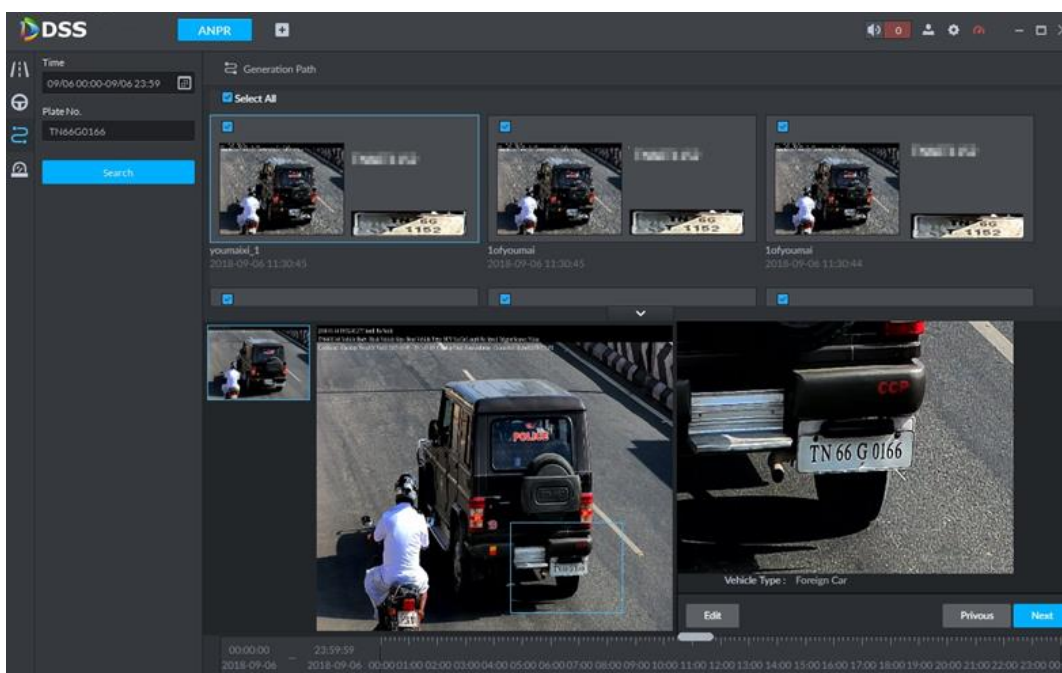
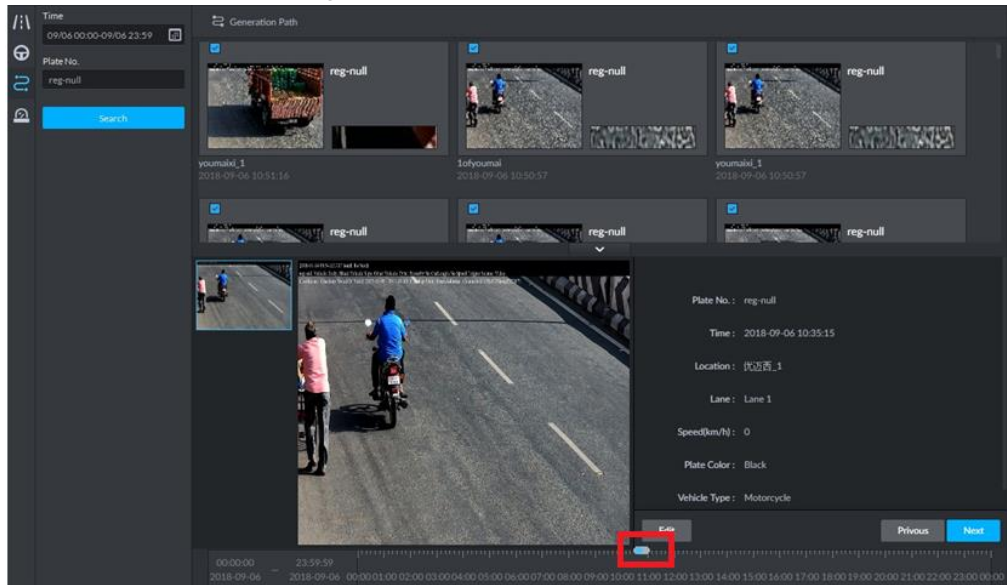


Figure 5-181 Zoom in image for details



- Click **Edit**, it is to edit vehicle basic information.
- Click **Previous** or **Next** to view the previous or the next search item.
- Click the timeline that has the records, you can view the vehicle information of the specified time.

Figure 5-182 Select time



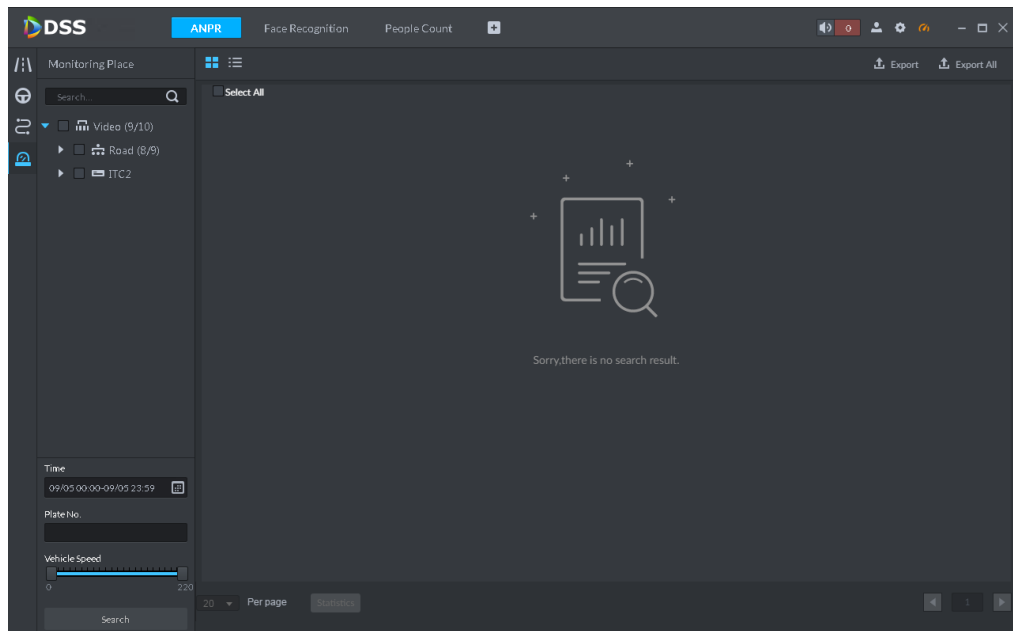
- Select the snapshot image and then click the **Generation Path** (track), you can view the vehicle track on the map.

5.12.5 Vehicle Alarms

View and confirm the alarm information.

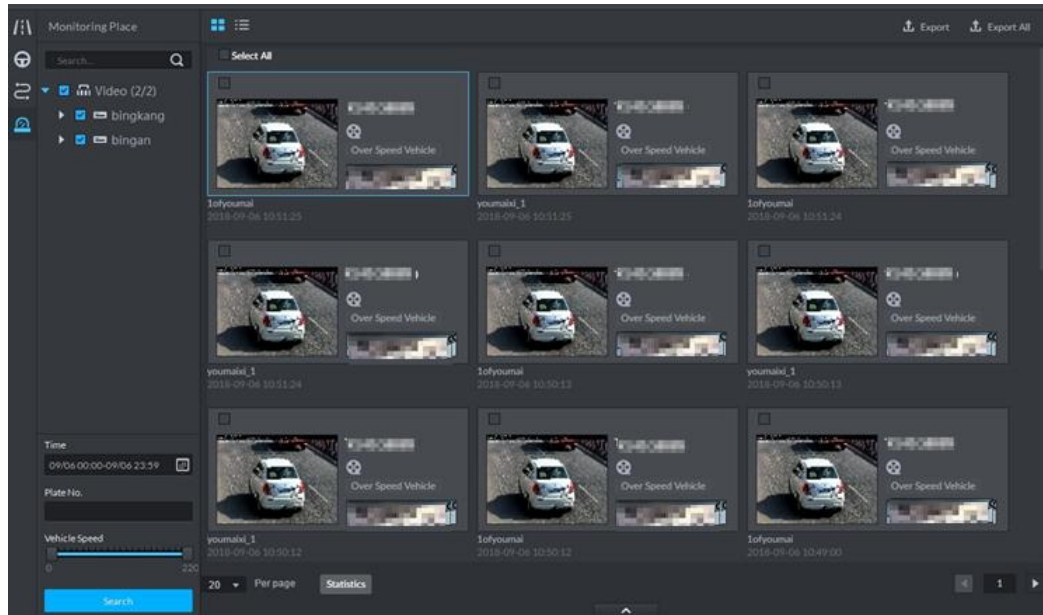
Step 1 Click .

Figure 5-183 Monitoring place interface



Step 2 Select device channel, and then set time, plate number, speed. Click **Search**.

Figure 5-184 Search results



For the monitor record, you can view vehicle detailed information, corresponding video, edit vehicle information. Refer to the operations listed below.




- Click view mode () or List mode (), it is to select different display mode.
- Select the snapshot image and then click  or double-click the image, you can view snapshot vehicle detailed information. Move the cursor to the middle to select the specified zone, you can zoom in it.

Figure 5-185 Vehicle records

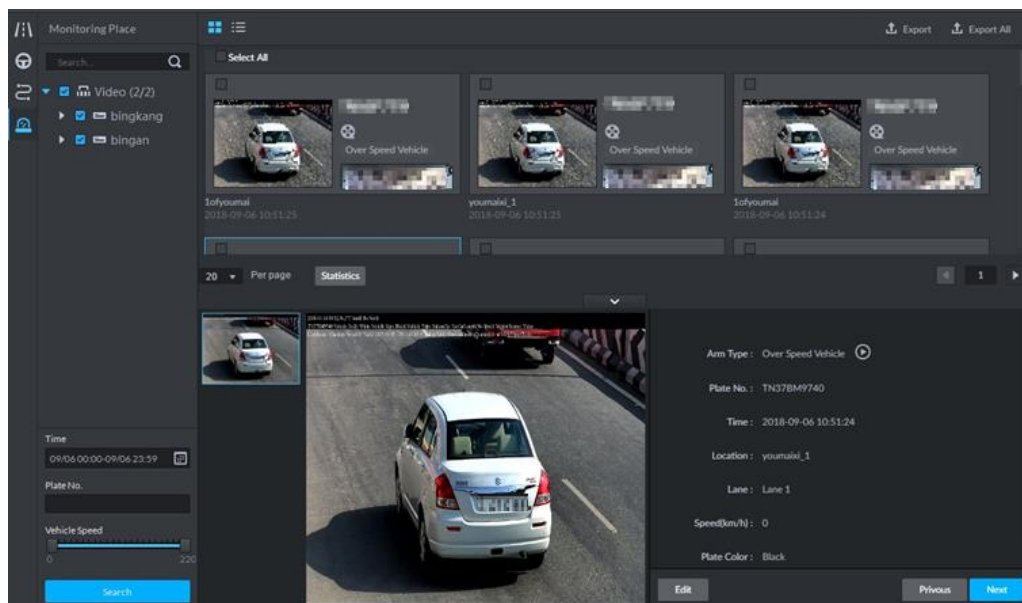
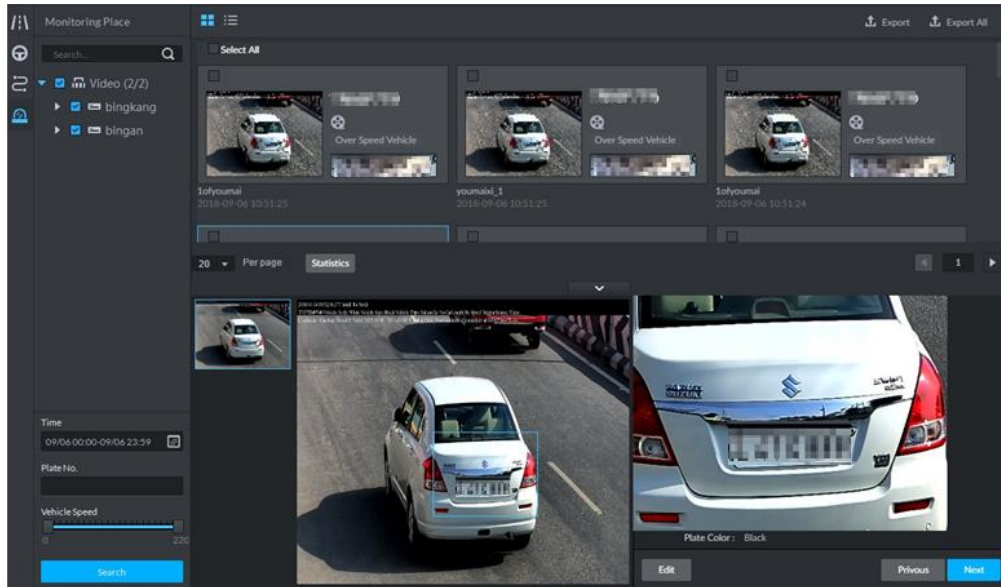


Figure 5-186 Zoom in image for details




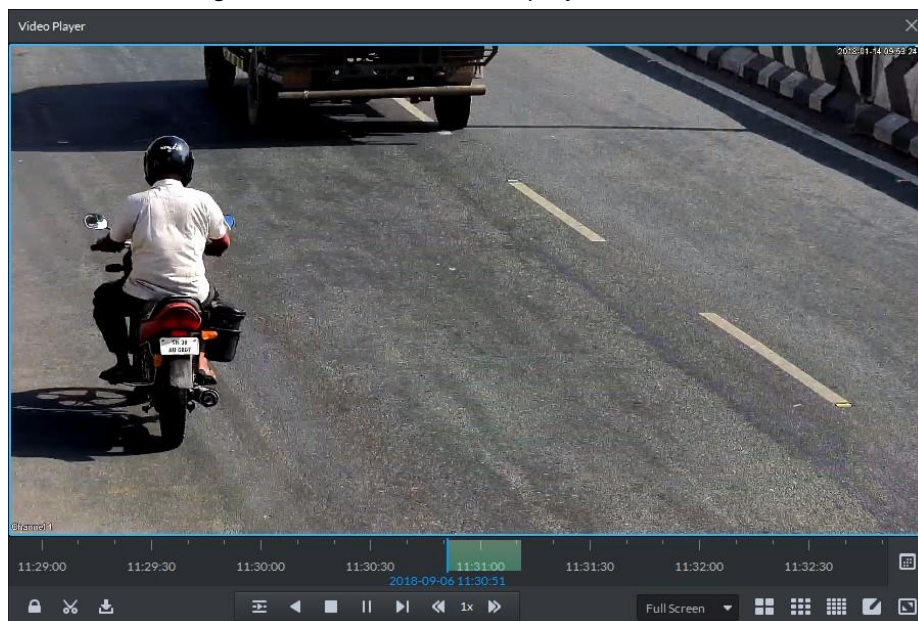

- Click  to playback the 15-second video before and after the vehicle passed time. See Figure 5-187. The video file is total 30 seconds.

Figure 5-187 Vehicle video playback



- Click  to view the vehicle running track. Refer to 5.12.4 Vehicle Track for detailed information.
- Export: Select the passed vehicle information and then click Export. It is to export selected monitor position information. Click Export all, it is to export all monitor position information.

5.13 Target Detection

5.13.1 Preparations


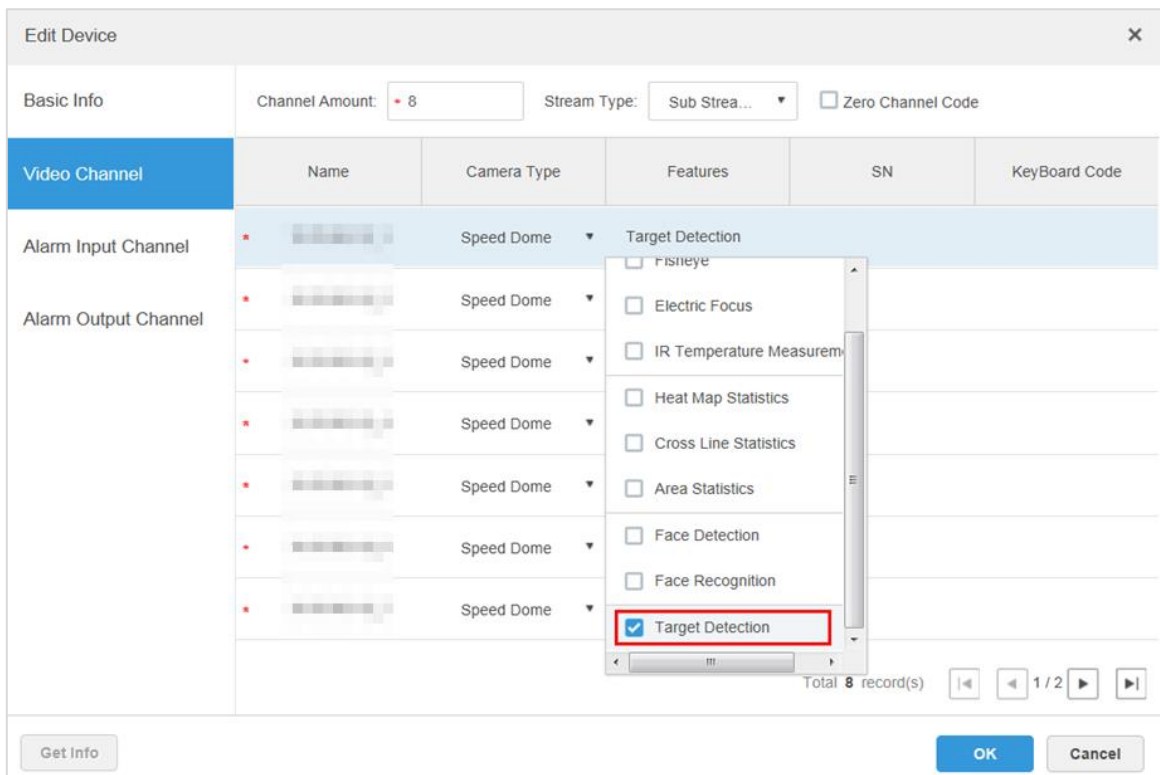
- Cameras with video metadata functions have been added to the web manager. See "4.5 for specific steps."
- After devices are added, click , and select **Target Detection** from the **Features** dropdown box. See Figure 5-188.

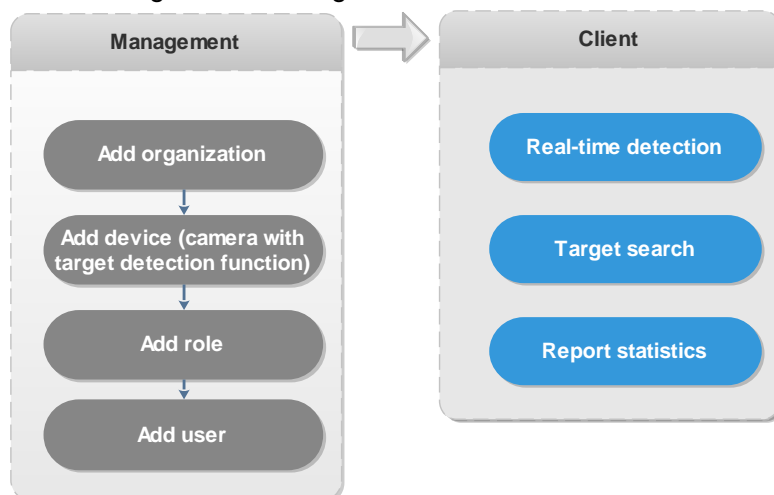
Figure 5-188 Set device features



- The video metadata IVS rules of the camera have been enabled. See the user manuals of cameras for detailed steps.

Target detection procedures are shown in Figure 5-189.

Figure 5-189 Target detection business flow



5.13.2 View Real-time Detection

To view the real-time snapshots captured by the cameras, including information about human, motorized vehicles, and non-motor vehicles:

Step 1 Click . On the **Homepage** interface, select **Target Detection**.


Step 2 Click .

Figure 5-190 Real-time detection interface

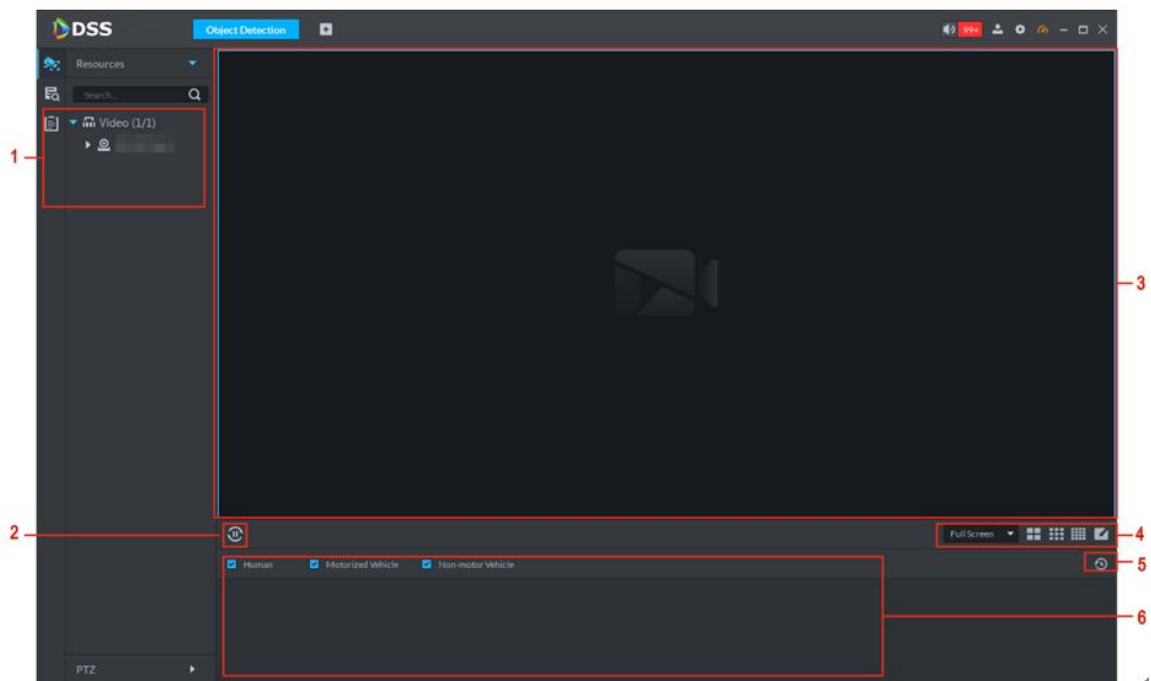


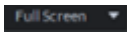



Table 5-49 Description

No.	Name	Description
1	Device Tree	Displays device information.
2	Pause Refresh/Start Refresh	<ul style="list-style-type: none"> If the interface displays this icon , the snapshot display area does not refresh snapshots. Click this icon to refresh face snapshots in real time. If the interface displays this icon , the snapshot display area refreshes face snapshots. Click this icon to stop refreshing snapshots.
3	Monitoring window	Displays the channel preview video. In the multi-window display mode, double-clicking a window switches to single window display. Another double-clicking returns to the original multi-window display mode.
4	 Picture display ratio	Supports Full Screen and Original Scale modes. The Full Screen mode refers to the single window display

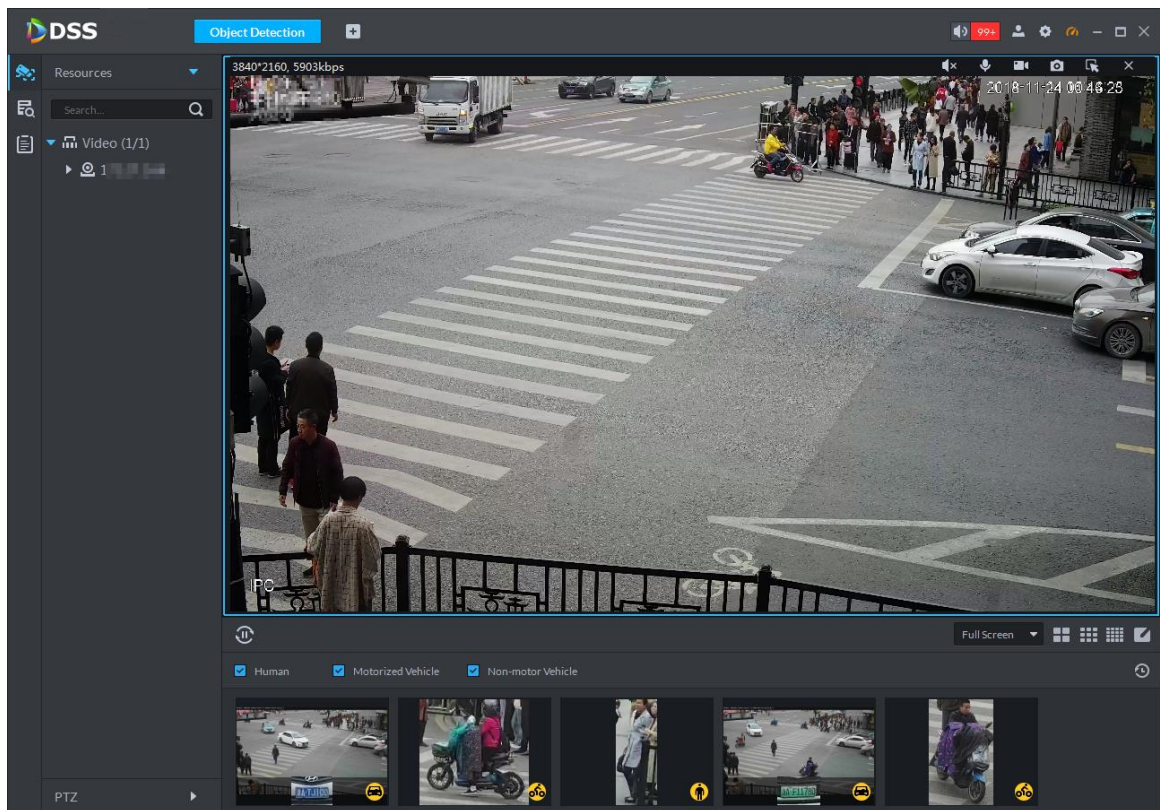
No.	Name	Description
		in full screen.
	 Number of windows	Supports switching the number of display windows, and you can customize the numbers.
5	The button that allows for jumping to the Report Statistics interface.	Click this icon to jump to the Report Statistics interface.
6	Snapshot display area	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 snapshot display area displays snapshots in real time.

Figure 5-191 Live view display



Step 5 Double-click the snapshot.

- 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, jump to the search interface, and view the recordings. You can quickly jump to search by image for human faces.
- Motorized 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.

- Non-motor vehicle snapshots display the panoramic view, vehicle type, vehicle color, and the number of people involved.

Figure 5-192 Snapshot details

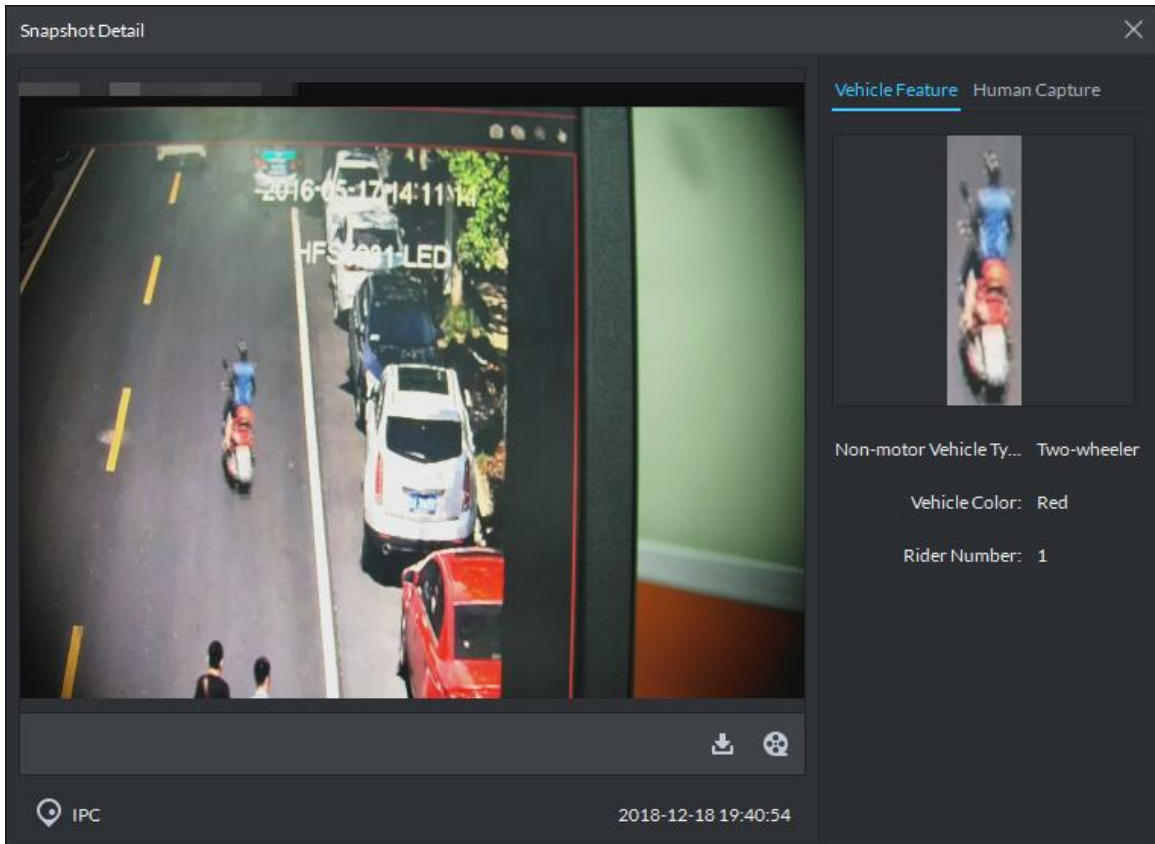




Table 5-50 Description

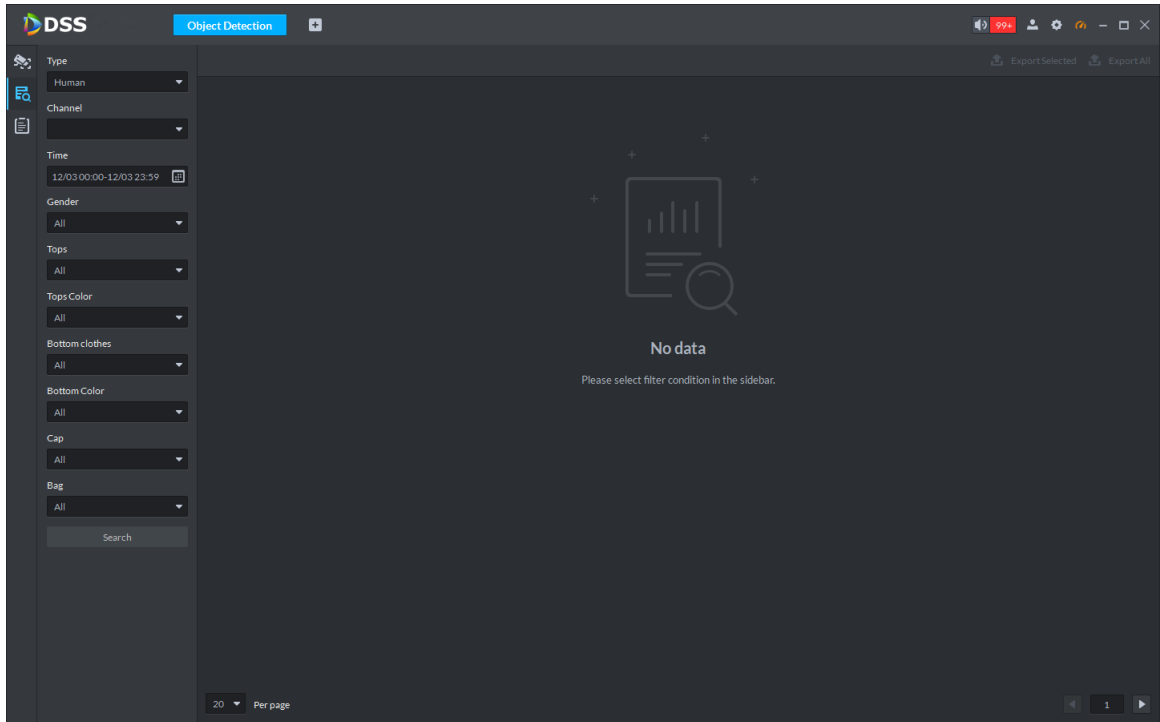
Operation	Description
Download	Click  and save .rar files in the specified path.
Playback	Click  to play back the video recordings timed before and after the snapshot.

5.13.3 Searching for Snapshot Targets

Identify the targets in the snapshot database quickly by setting up criteria.

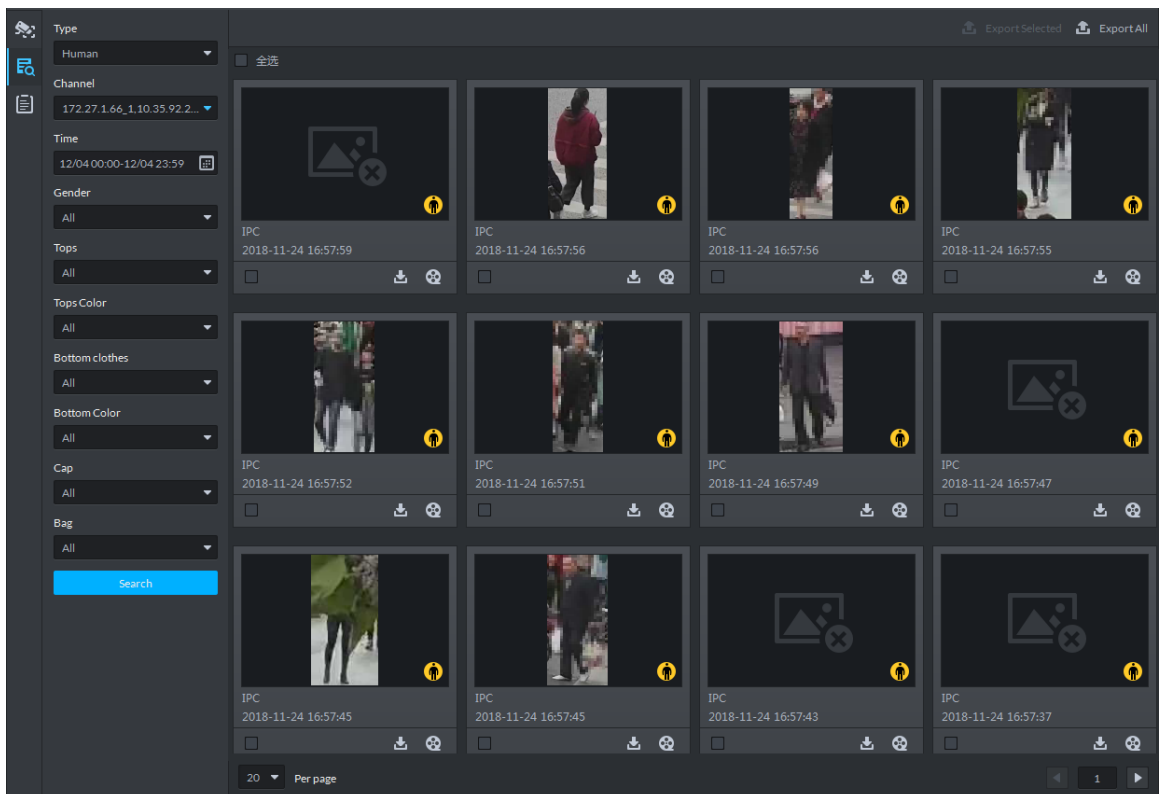
Step 1 On the **Object Detection** interface, click .

Figure 5-193 Object search



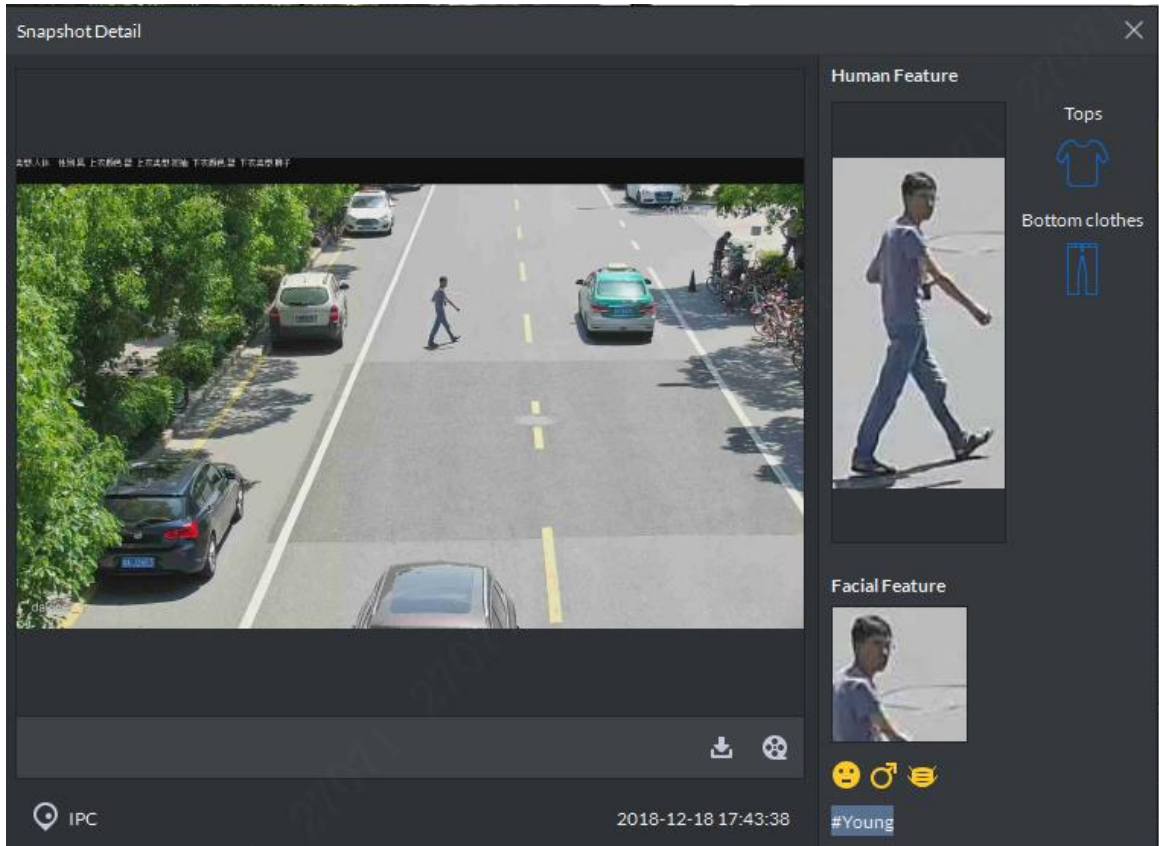
Step 2 Set up search criteria and click **Search**.

Figure 5-194 Search results



Step 3 Double-click the snapshot.

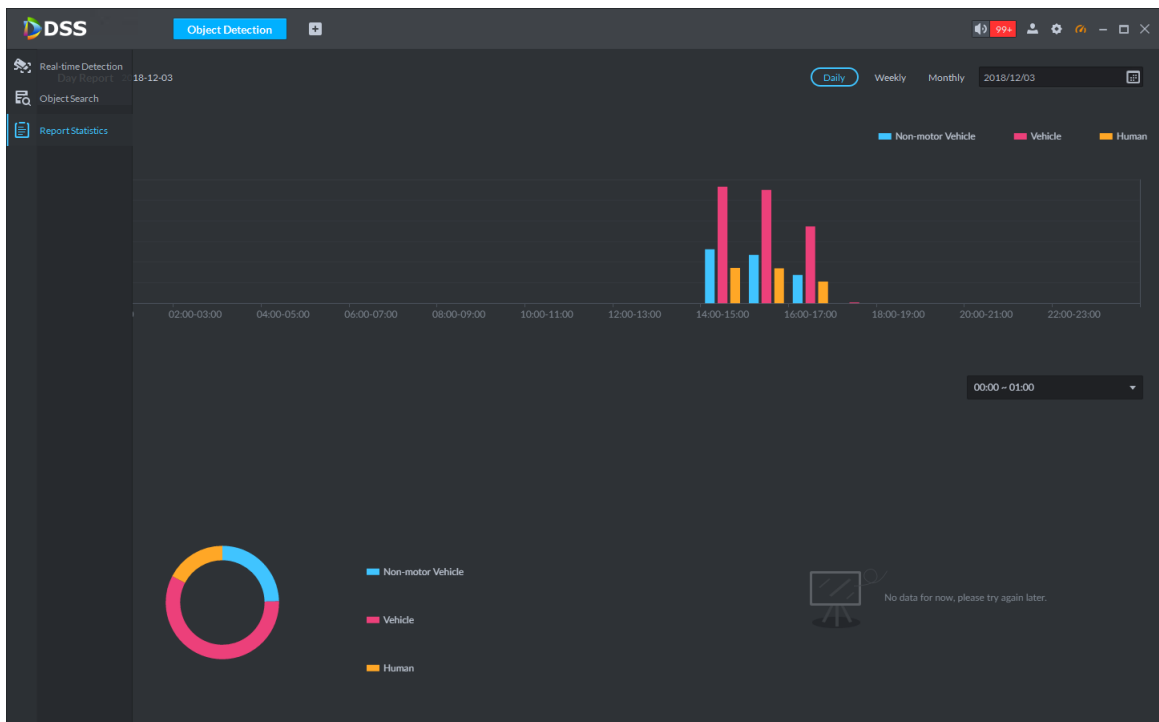
Figure 5-195 Snapshot details



5.13.4 Statistical Report

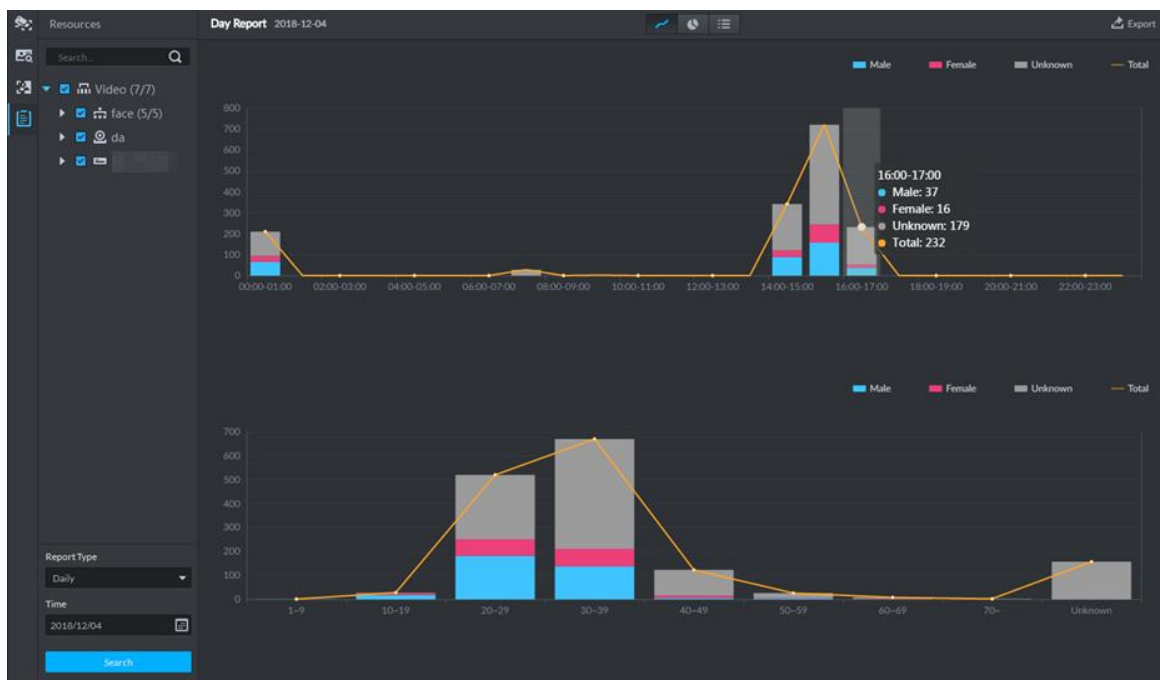
Step 1 On the **Object Detection** interface, click .

Figure 5-196 Report interface



Step 2 Set the criteria for the statistics.

Figure 5-197 Report



5.14 Personnel Management

Configure personnel information for access control.

5.14.1 Configuring Personnel Information

Personnel refer to the target people of access control. They have different permissions to get through doors with password, fingerprint, card, or face recognition.

Figure 5-198 Personnel management flow



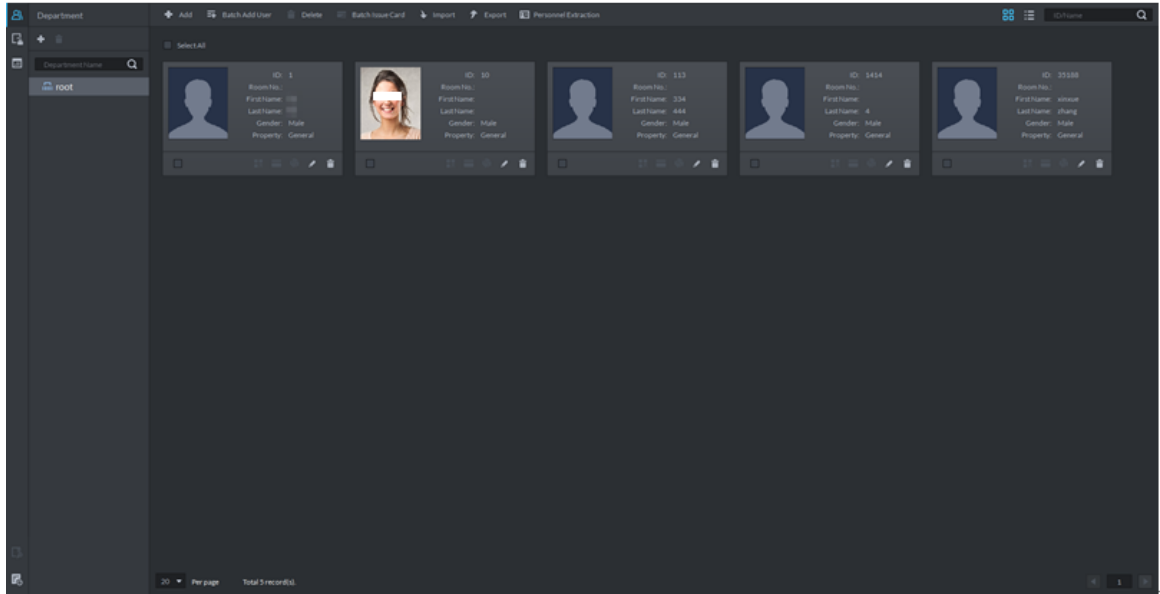
5.14.1.2 Adding Department

Adding department is to manage personnel by departments.

Step 1 On the **Homepage** interface, select **Personnel Management**.

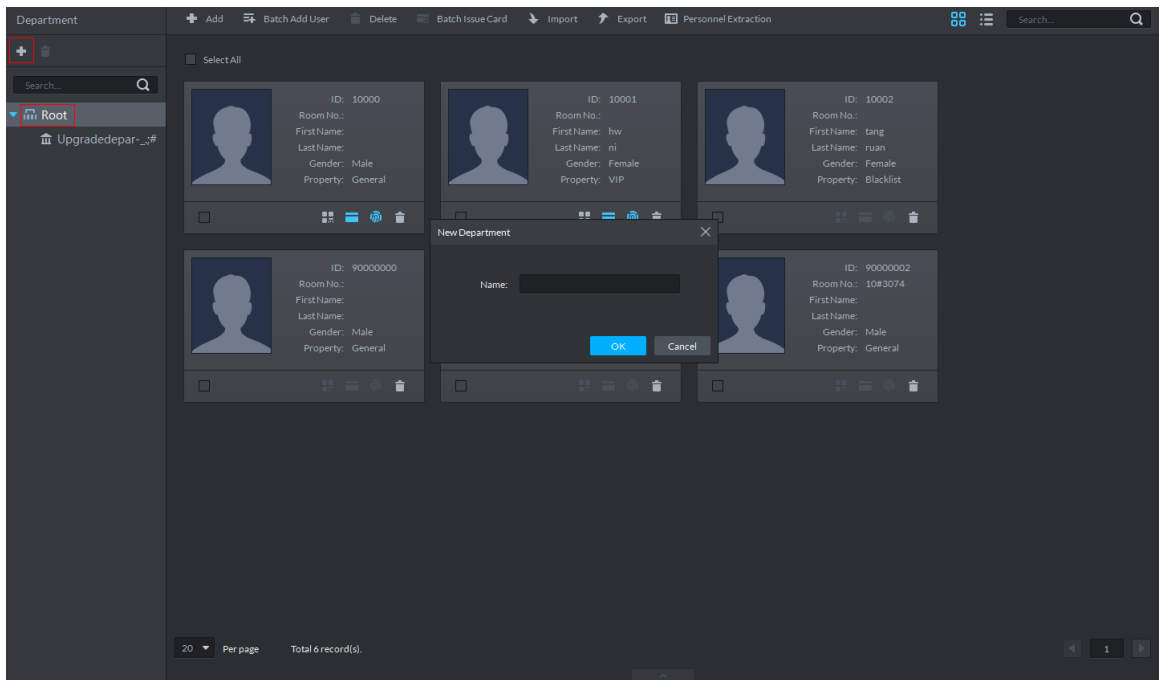
Step 2 Click .

Figure 5-199 Personnel management interface



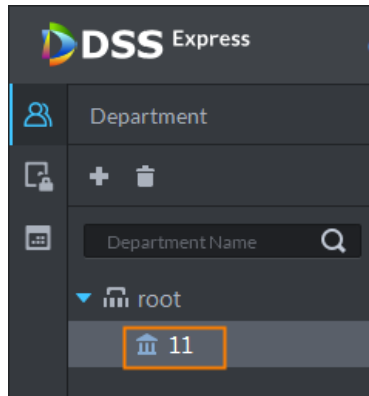
Step 3 Select a node from the department list on the left side, and click **Add**.
The new department is directly under the selected node.

Figure 5-200 New department





Step 4 Enter the department name, and then click **OK**.

Figure 5-201



You can delete or rename a newly added department.

- To delete a department, select it, click , and follow the instructions on the interface. You cannot delete a department with personnel.
- To rename a department, select the department and click the corresponding  to modify the name.

5.14.1.3 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.

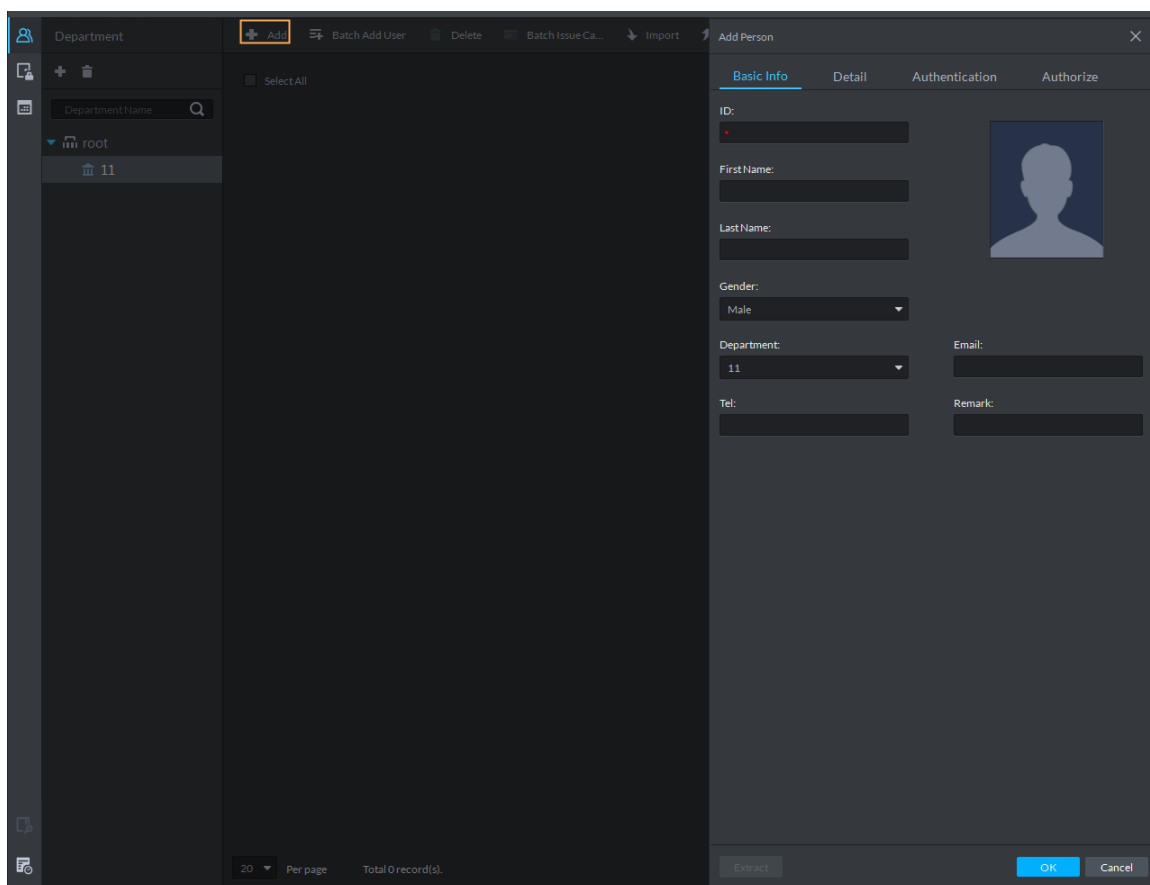


- Person ID shall be the same on the platform and access control devices; otherwise person data could be wrong.
- To collect fingerprints or card No., connect a fingerprint collector or card reader first.

5.14.1.3.1 Adding a Person

Step 1 On the **Personnel Management** interface, click **Add**.

Figure 5-202 Add a person



Step 2 Click the **Basic Info** tab to configure person information.

- 1) Move the mouse cursor to the picture section, and then click **Upload**. Follow the instructions on the interface to upload a picture. If the PC comes with a camera, click **Snapshot** to take a face snapshot and upload it.
- 2) Fill in personnel information as necessary. ID is required, and others are optional.

Step 3 Click the **Detail** tab, and then set person details as required.

Step 4 Click the **Authentication** tab, and then set access control information.

Figure 5-203 Authentication

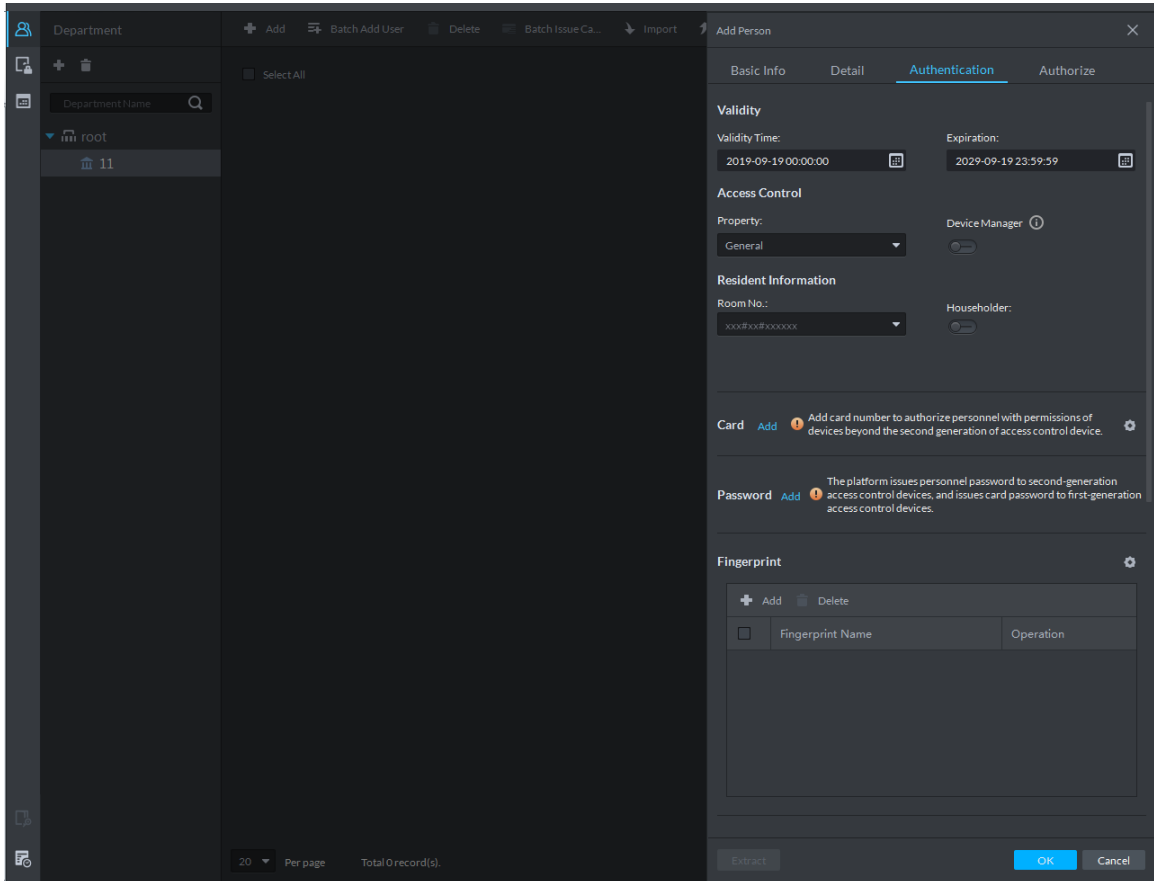



Table 5-51 Authentication parameters

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 dropdown 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.
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.

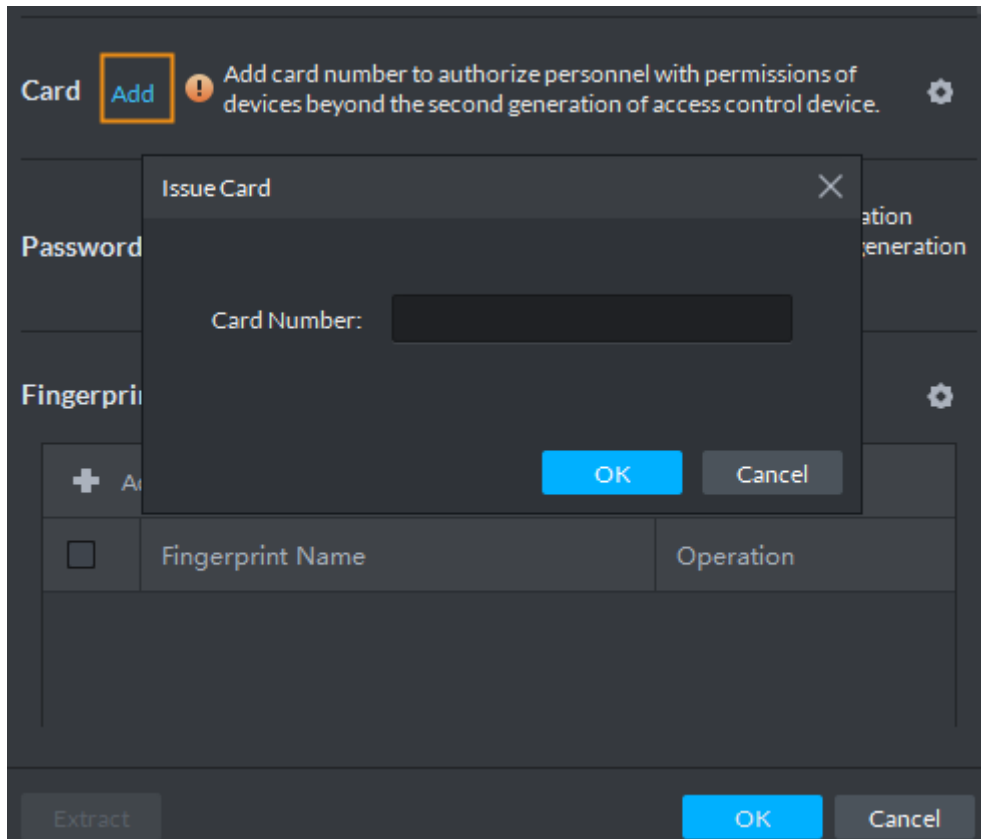
Step 5 Issue cards to personnel.

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 5-204 Issue card by entering card No.



2) Enter card number and click **OK**.
The card is added.

Figure 5-205 Added card

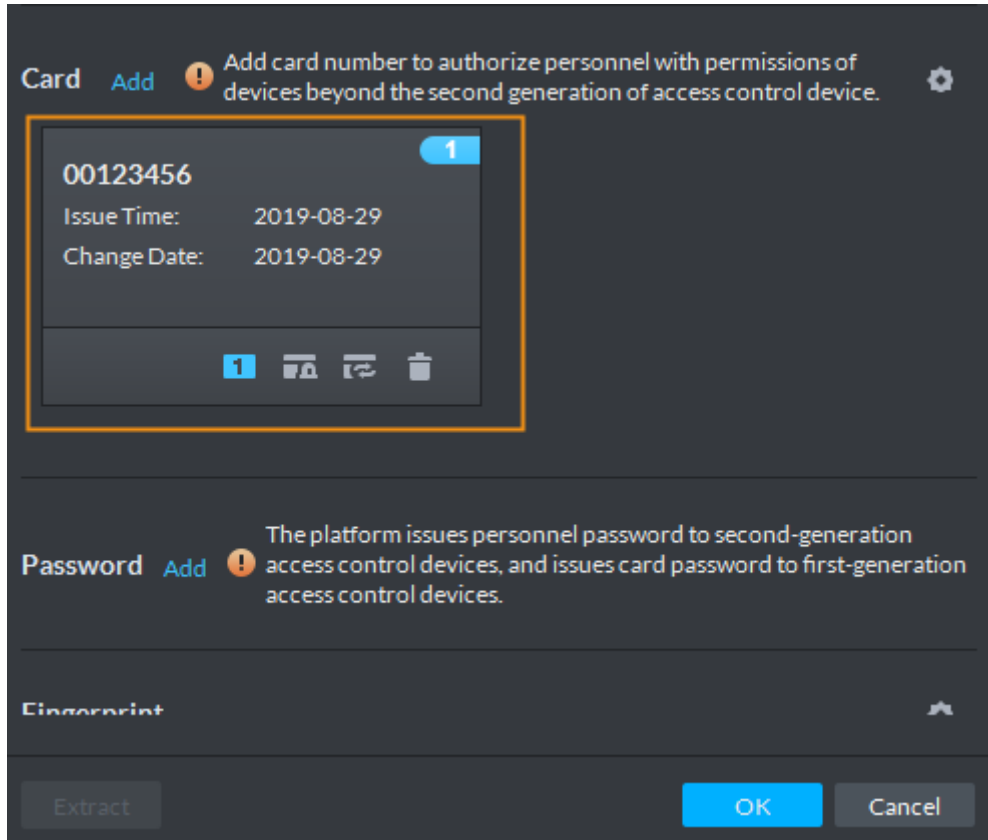


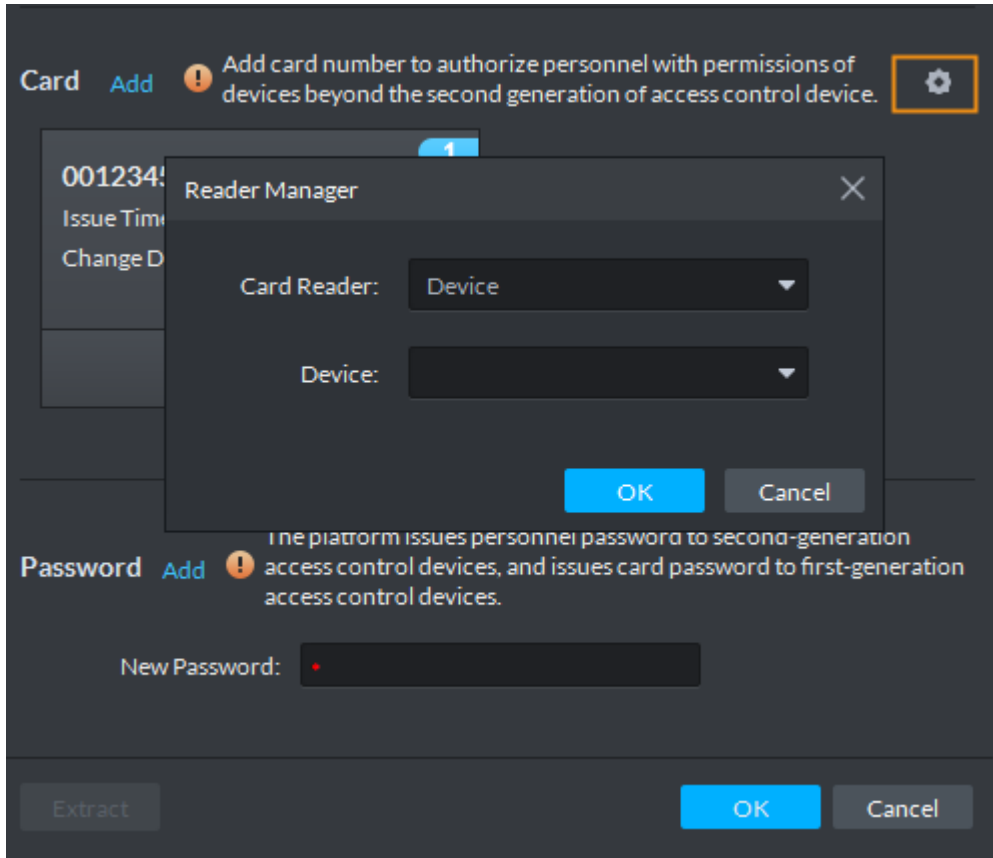
Table 5-52 Card operations

Icon	Description
	<p>If a person has more than one card, only the main card can be issued to the first-generation access control devices. 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 5-206 Issue card by card reader



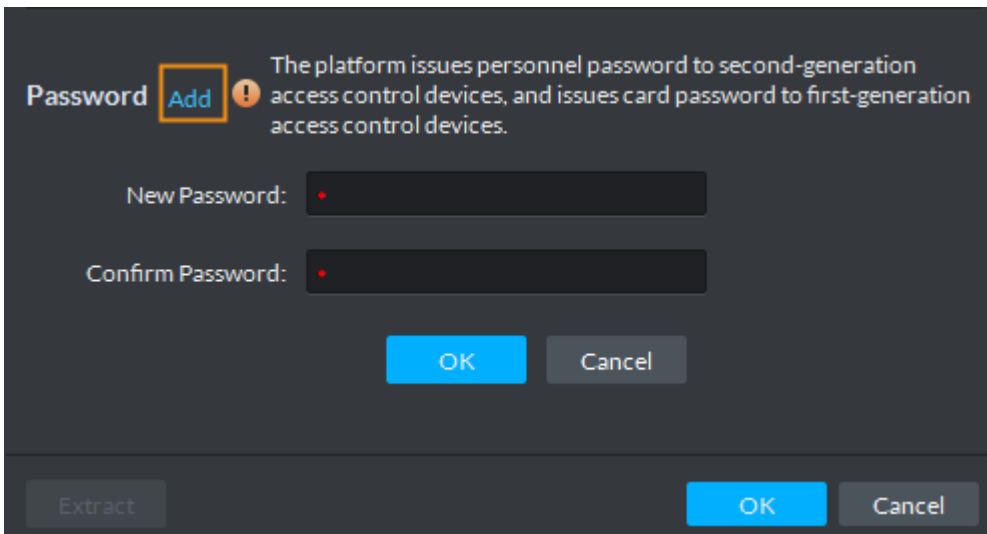
- 2) Select from **Card Reader** or **Device**, and then click **OK**.
- 3) Swipe card on the card reader or device.
The card is added.

Step 6 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 5-207 Set a password



- 2) Enter the password, and then click **OK**.

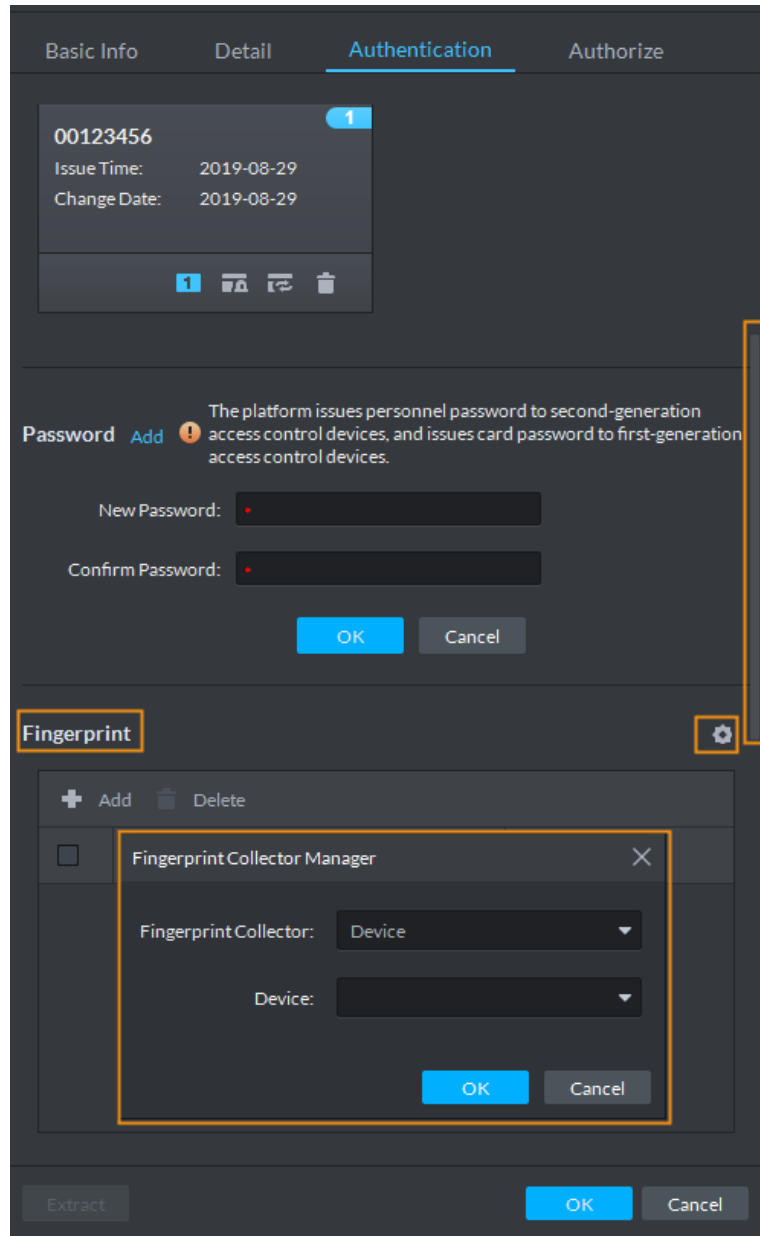
Step 7 Collect fingerprint.

To open door with fingerprint, you need to collect personnel fingerprints. A person can have up to 10 fingerprints.

1) Scroll down the **Authentication** page, and then in the Fingerprint section, click



Figure 5-208 Fingerprint collector manager



Basic Info Detail **Authentication** Authorize

00123456 1
Issue Time: 2019-08-29
Change Date: 2019-08-29

Password **Add** ! The platform issues personnel password to second-generation access control devices, and issues card password to first-generation access control devices.

New Password:

Confirm Password:

OK Cancel

Fingerprint ⚙️

+ Add - Delete

Fingerprint Collector Manager ×

Fingerprint Collector: Device

Device:

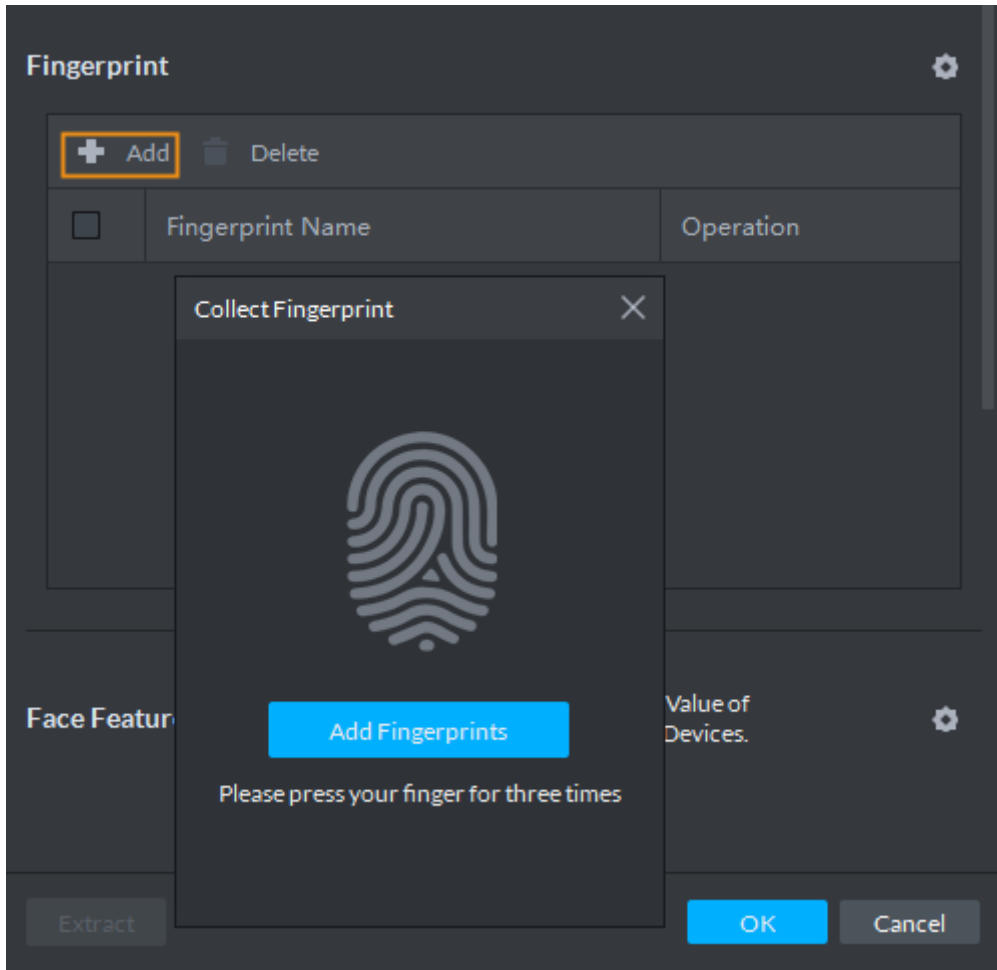
OK Cancel

Extract OK Cancel

2) Select a fingerprint collector, and then click **OK**.

3) Click **Add**.

Figure 5-209 Collect fingerprint



- 4) Click Add Fingerprints.

Figure 5-210 Collect fingerprint



- 5) Record fingerprint on the reader by raising and then pressing the finger after hearing the beep sound. Repeat this for three times to finish fingerprint collection.

Figure 5-211 Collecting fingerprint



Figure 5-212 A collected fingerprint

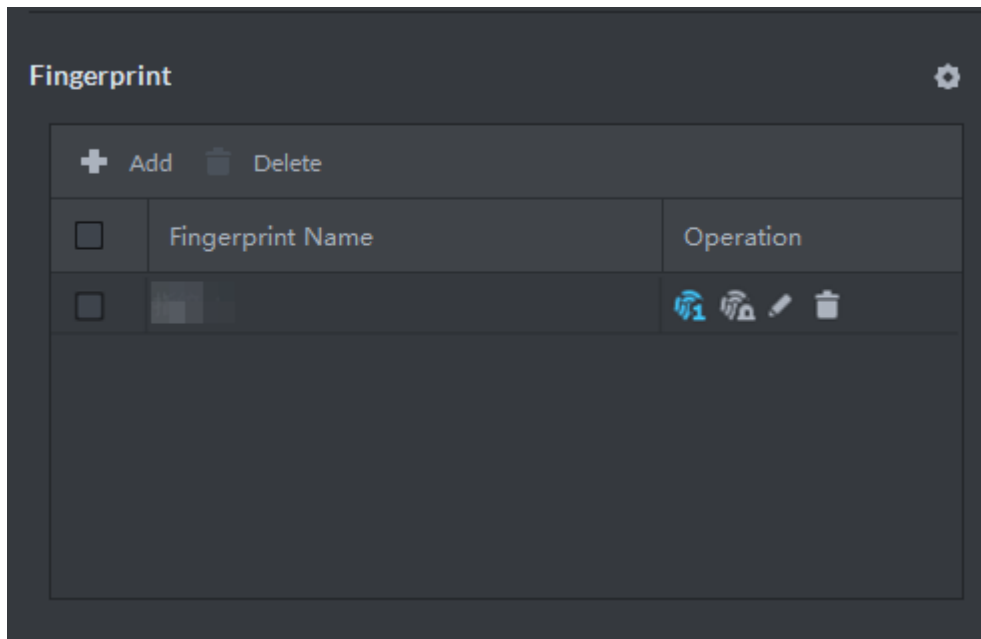


Table 5-53 Fingerprint operations

Icon	Description
	When more than 3 fingerprints are collected, only the main fingerprints can be issued to devices. The first 3 fingerprints are main ones by default. One person can have up to 3 main fingerprints. 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 8 Add vehicle information.

Add vehicle information to a person, so as to enable vehicle access permission for this person.

Click **Add** to assign parking space number to the person and collect vehicle plate numbers. If the person has more than one vehicle, you need to add them one by one.



If the added number of vehicles is larger than the given number of parking spaces, only the given number of them can get in.

Figure 5-213 Add vehicle information

The screenshot shows a 'Vehicle' configuration window. At the top, there is a 'Spots Available' dropdown menu set to '8'. Below this, there are '+ Add' and '- Delete' buttons. A table is displayed with two columns: 'Plate No.' and 'Operation'. The 'Plate No.' column has a text input field, and the 'Operation' column has a trash can icon. At the bottom of the window, there are three buttons: 'Extract', 'OK', and 'Cancel'.

Step 9 Collect face feature code.

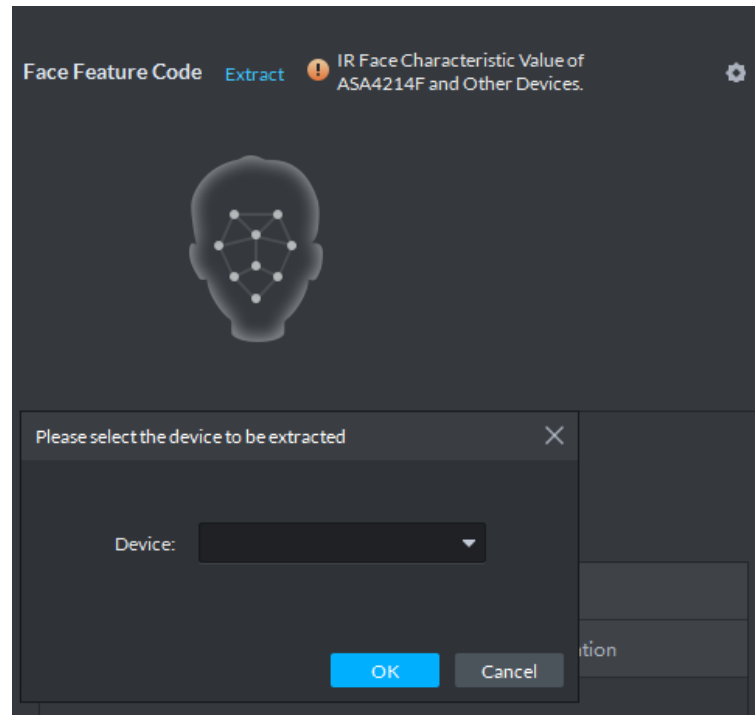
When the IR face device is used, you can collect IR face feature codes through the device for face recognition and access control.



It is required that face feature code exists on the IR face device.

- 1) Click  in the **Face Feature Code** section.

Figure 5-214 Select a device



- 2) Select an IR face device, and then click **OK**.
- 3) Click **Extract**.

The extraction starts.

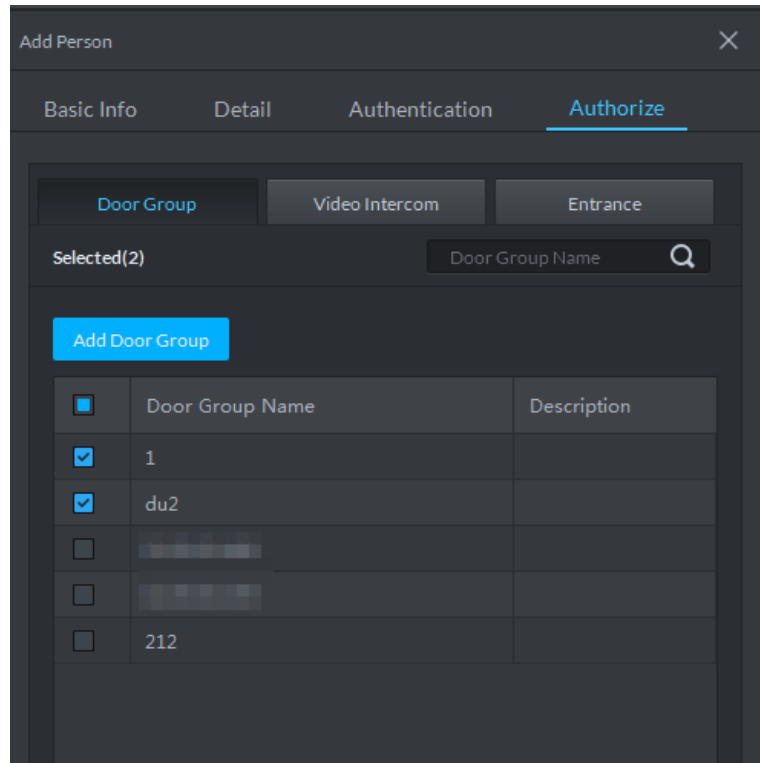
Step 10 Click the **Authorize** tab.

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 5-215 Authorize



Step 11 Click **OK**.




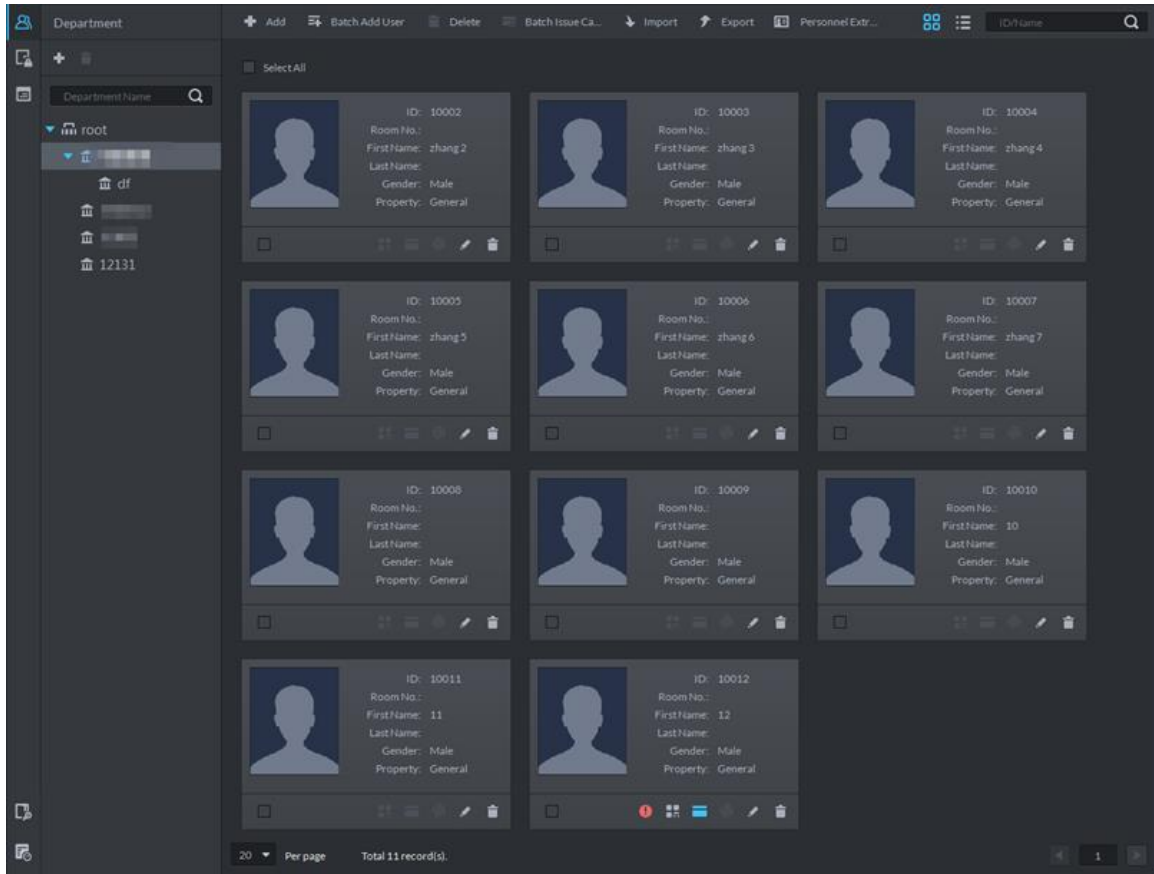
- To edit person information such as basic details, passwords, fingerprints, IR face feature codes and face pictures, see "5.14.1.4 Editing Personnel Information."
- To delete a person, you can select the person, and then click ; to delete all people on this page, select the **Select All** check box, and then click **Delete**.

Figure 5-216 Added people



5.14.1.3.2 Adding Personnel in Batches

If multiple people are added at one time, you can issue cards to them. When you need to issue passwords and fingerprints to them, you can edit personnel authorization separately.

Step 1 On the **Personnel Management** interface, click **Batch Add User**.

Figure 5-217 Add personnel in batch (1)

Department

+ Add Batch Add User Delete Batch Issue Ca... Import

Select All

Department Name

root

11

ID: *

Quantity: *

Department: 11

Validity Time: 2019-09-19 00:00:00

Expiration: 2029-09-19 23:59:59

Issue Card

ID	Card No.	Operation
----	----------	-----------

20 Per page Total 0 record(s)

OK Cancel

Step 2 Enter the starting ID number in the **ID** box, enter the number of people you need in the **Quantity** box, select a department, and then set the term of validity.

Figure 5-218 Add personnel in batch

Batch Add User ✕

ID: Quantity:

Department:

Validity Time: Expiration:

Issue Card ⚙️

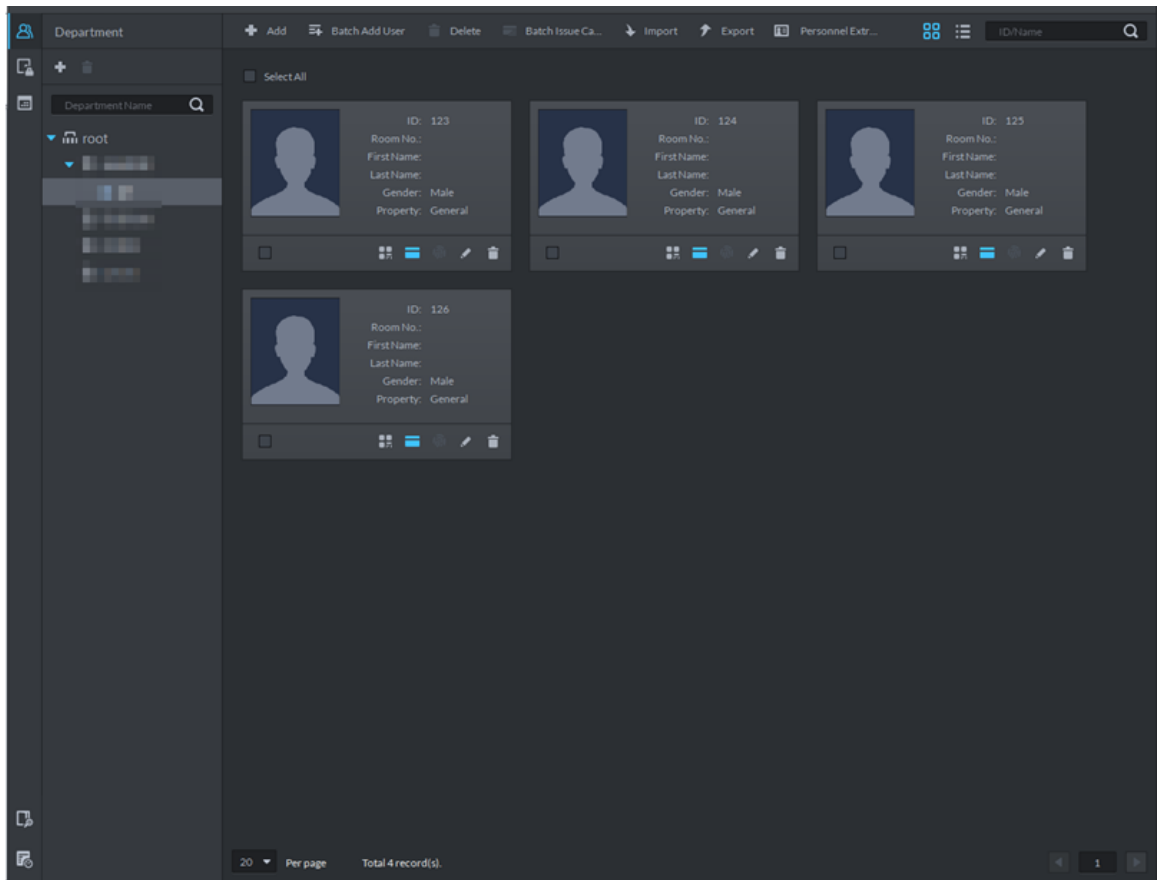
ID	Card No.	Operation
123		
124		
125		
126		
127		
128		
129		
130		
131		

Step 3 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 5-219 Newly added people




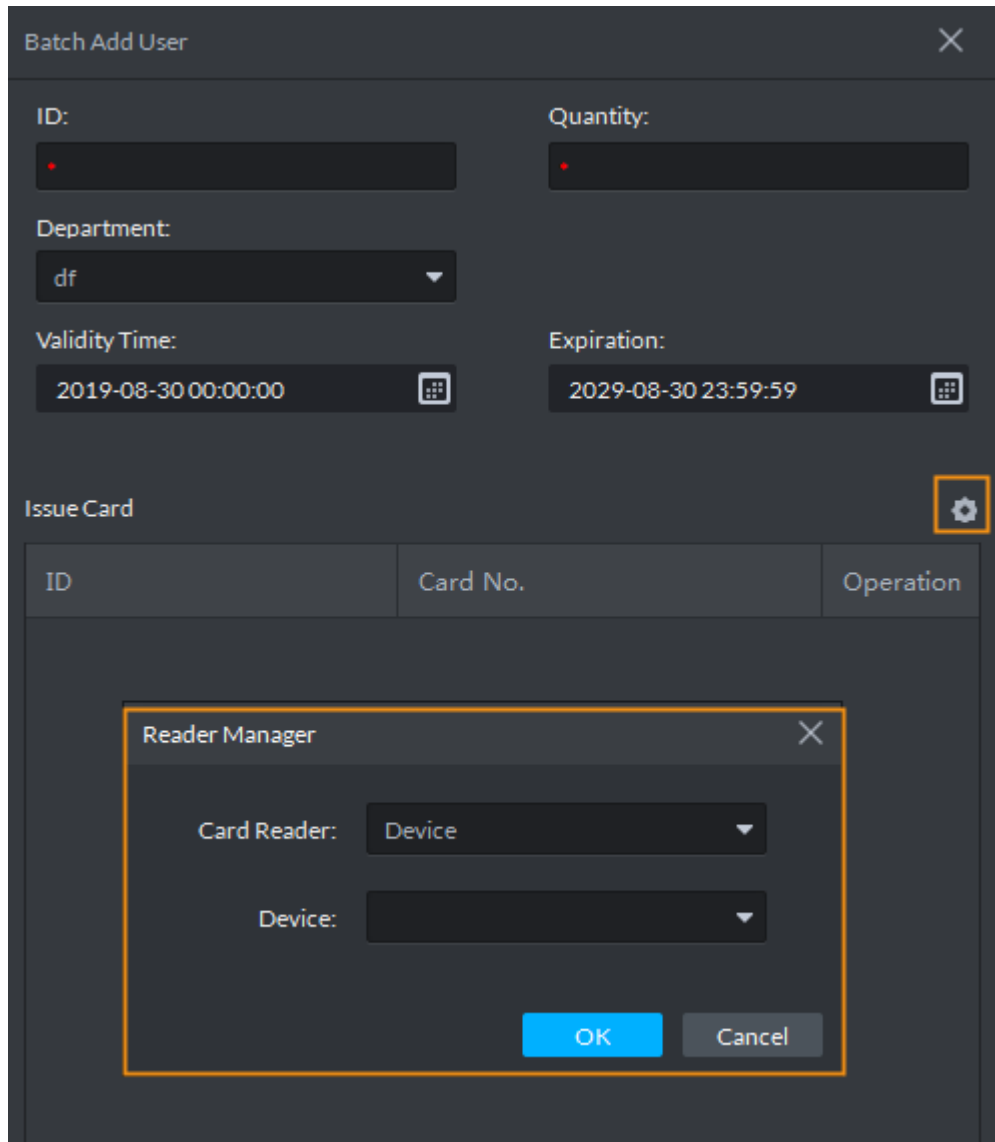
- By using card reader.
- 1) On the **Batch Add User** interface, click .

Figure 5-220 Reader manager



- 2) Select a card reader or a device, and then click **OK**.
- 3) Select people, and then swipe cards on the card reader or device.
- 4) Click **OK**.


To edit personnel information such as password and fingerprint, see "5.14.1.4 Editing Personnel Information."

5.14.1.4 Editing Personnel Information

Modify personnel information including basic information, authentication details, and authorization. Person ID cannot be modified.



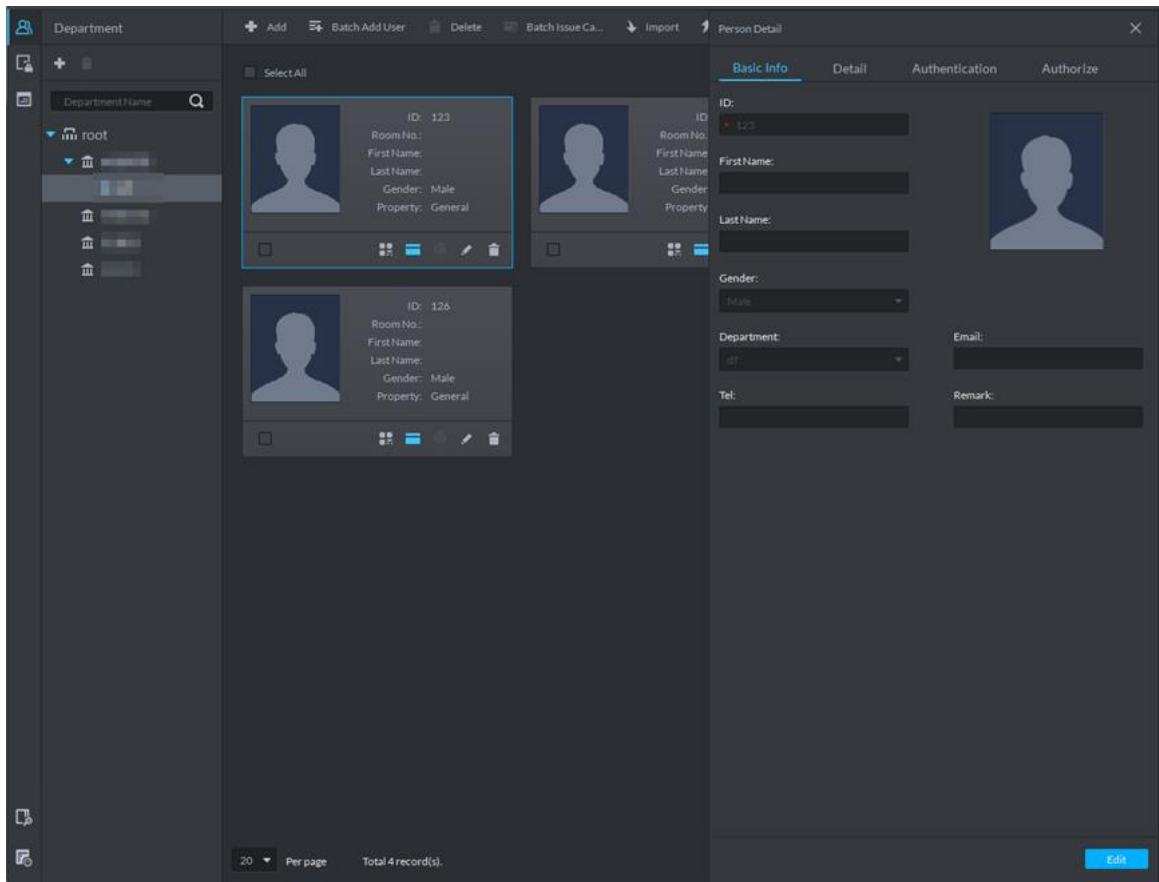
Make sure the corresponding devices are well-connected before collecting fingerprints, card numbers or face pictures from fingerprint collectors, card readers, or IR face devices.

Step 1 On the **Personnel Management** interface, double-click a person or click .



If the person information has been set on the access control device, you can synchronize from the device by clicking **Extract**.

Figure 5-221 Edit personnel information

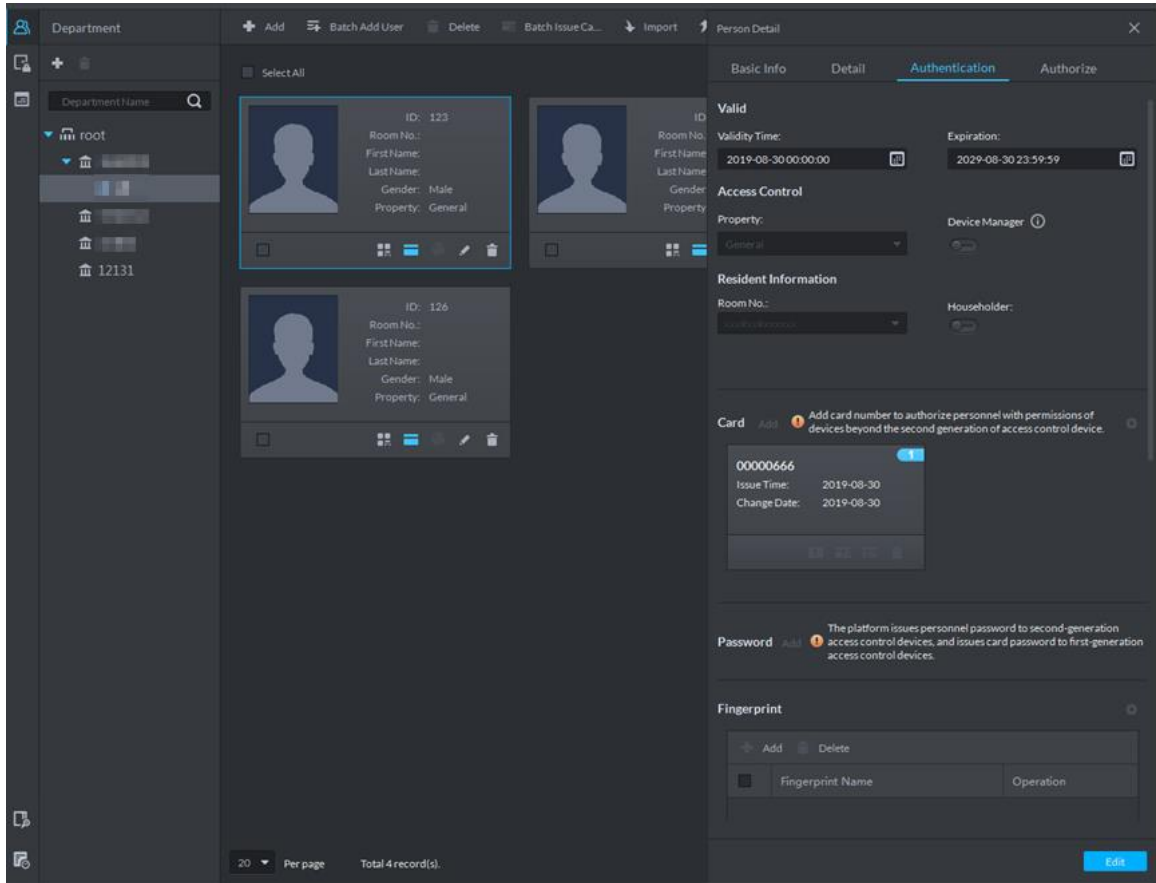


Step 2 Modify person information except ID.

Step 3 Click the **Authentication** tab.

To start modifying authentication details, click **Edit**.

Figure 5-222 Authentication information



Step 4 Manage a card.

To modify card status, click **Edit**.

Figure 5-223 Card

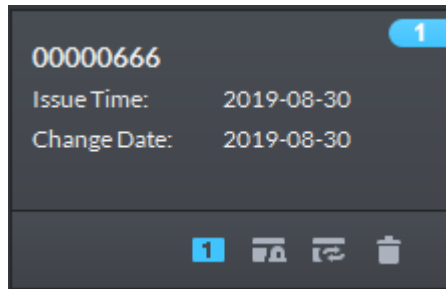








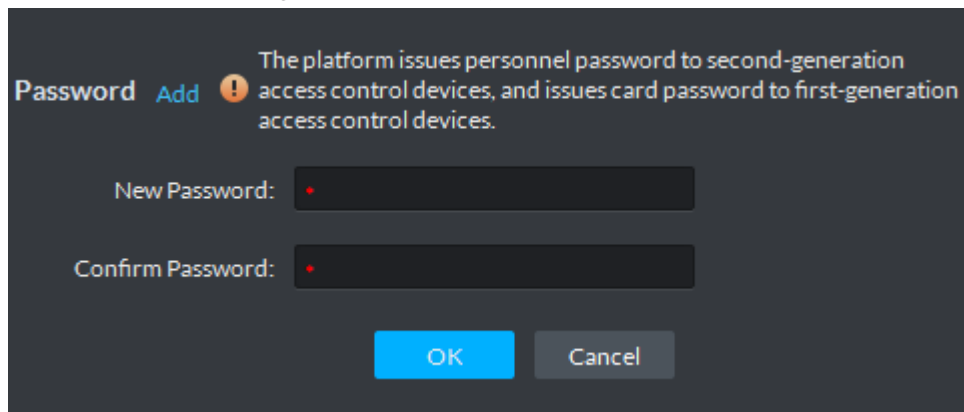
Table 5-54 Card operations

Icon	Description
	<p>If a person has more than one card, only the main card can be issued to the first-generation access control devices. 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>

Icon	Description
	Set a card as duress card. When opening door with a duress, there will be a duress alarm. 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  .
	Change card for the person when the current card does not work.
	Remove the card , and then it has no access permission.

Step 5 To modify a password, click **Edit**, click **Add** next to **Password**, and then set a new password.

Figure 5-224 Modify password



Step 6 To edit fingerprint name and status, click **Edit**. For details, see Table 5-55.

Figure 5-225 A collected fingerprint

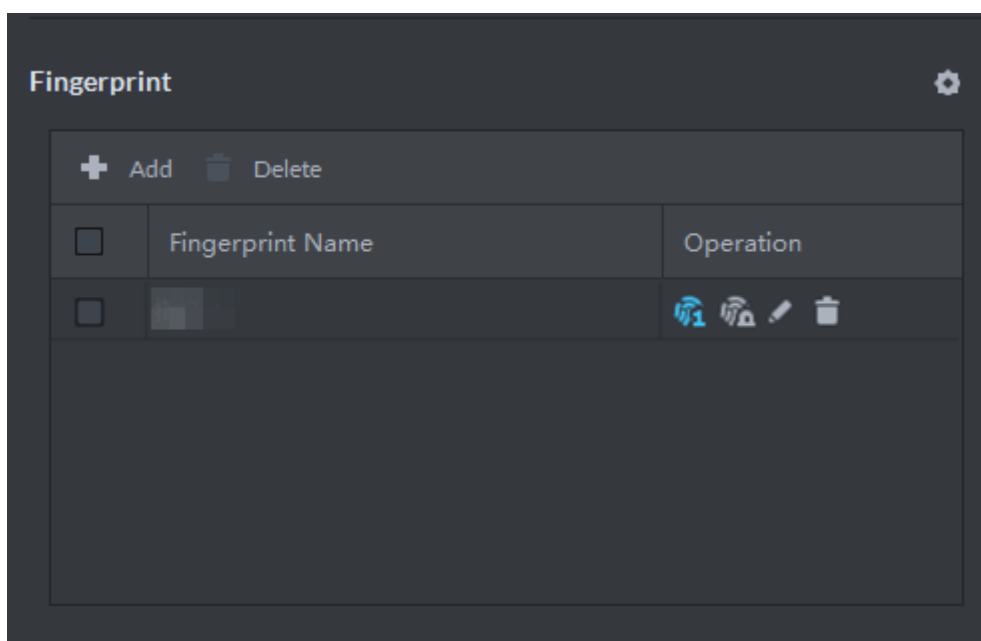










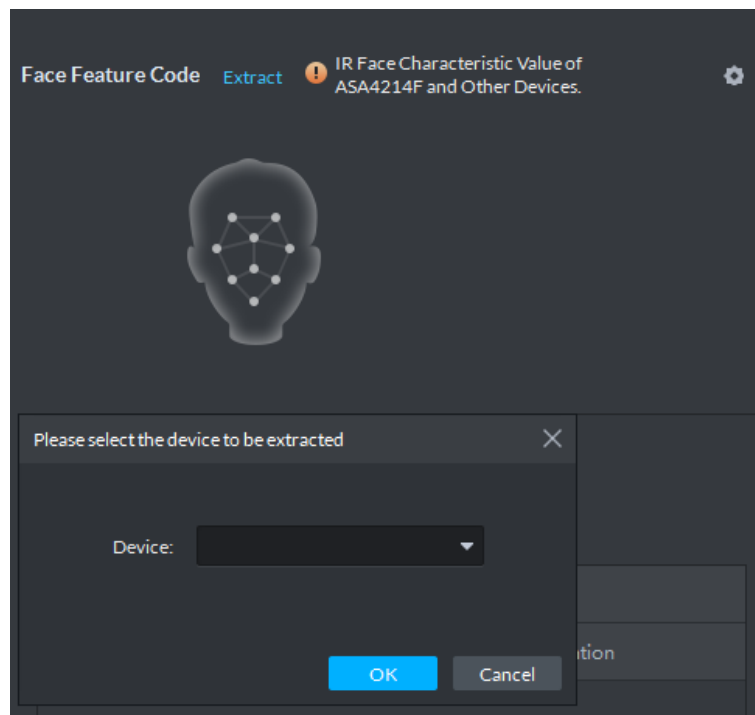
Table 5-55 Fingerprint operations

Icon	Description
	<p>When more than 3 fingerprints are collected, only the main fingerprints can be issued to devices. The first 3 fingerprints are main ones by default. One person can have up to 3 main fingerprints.</p> <p>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 .</p>
	<p>Set a fingerprint as duress fingerprint. When opening door with a duress, there will be a duress alarm.</p> <p>Click this icon, it turns into , which indicates that the fingerprint has been set as a duress fingerprint. To cancel the duress setting, click .</p>
	<p>Modify fingerprint name.</p>
	<p>Remove the fingerprint , and then it has no access permission.</p>

Step 7 Extract IR face feature code.

- 1) Click  in the **Face Feature Code** section.

Figure 5-226 Select a device



- 2) Select a device, and then click **OK**.
- 3) Click **Extract**.

The system starts extracting the IR face features code of people with the same ID number.



Face feature code can be modified.

Step 8 To modify parking space number and license plate number, enter the number in the **Spots Available** box.

To modify license plate number, click the **Plate No.** column.




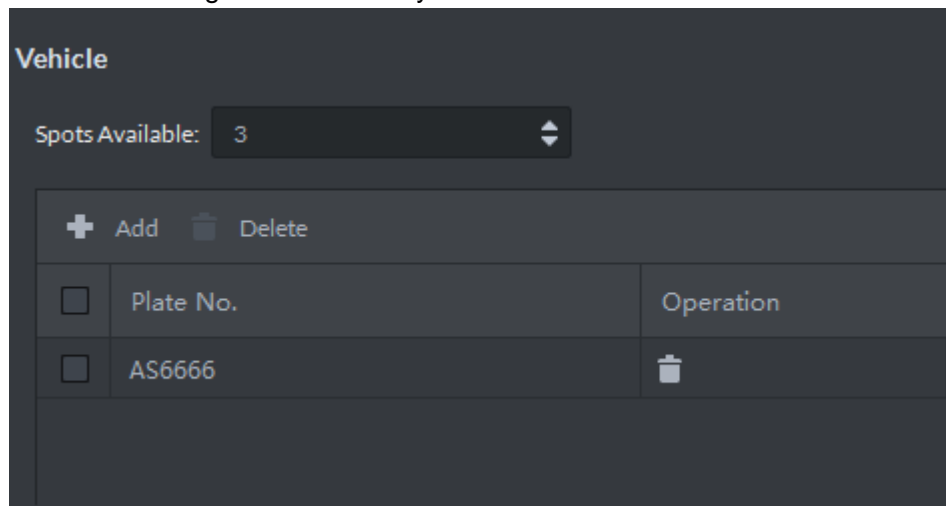
To remove a plate number, click .

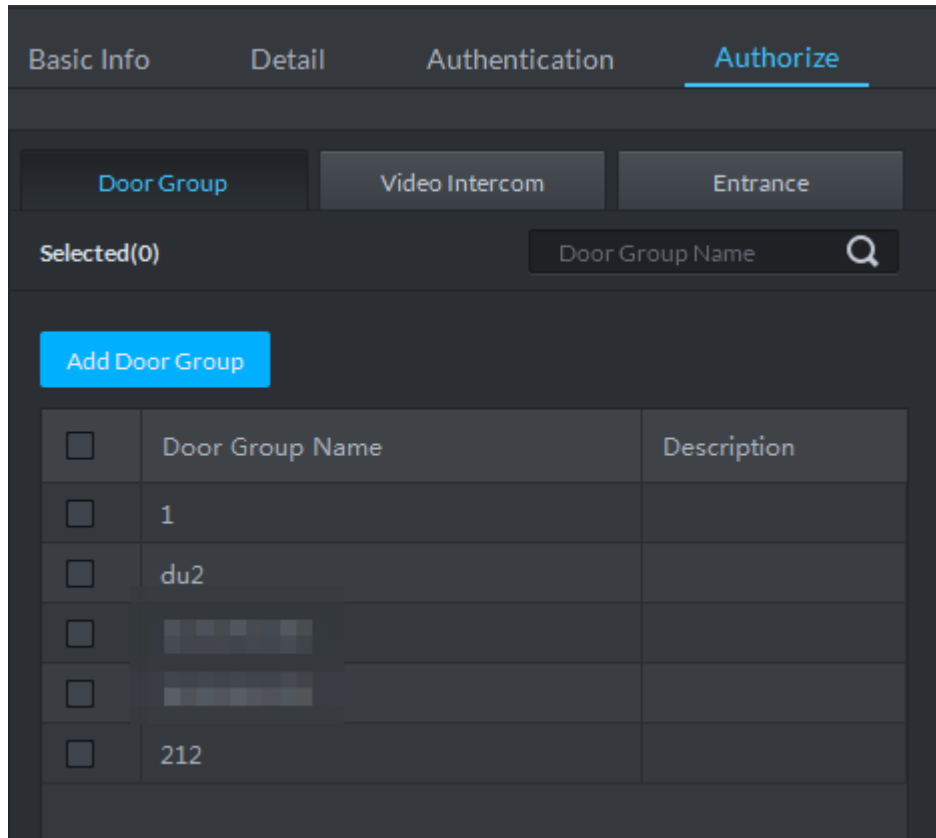
Figure 5-227 Modify vehicle information



Vehicle	
Spots Available:	3
+ Add - Delete	
Plate No.	Operation
<input type="checkbox"/> AS6666	

Step 9 To modify access control permissions such as door group, video intercom and vehicle entry & exit, click the **Authorize** tab.

Figure 5-228 Access control authorization



Step 10 Click **OK** to save configuration.

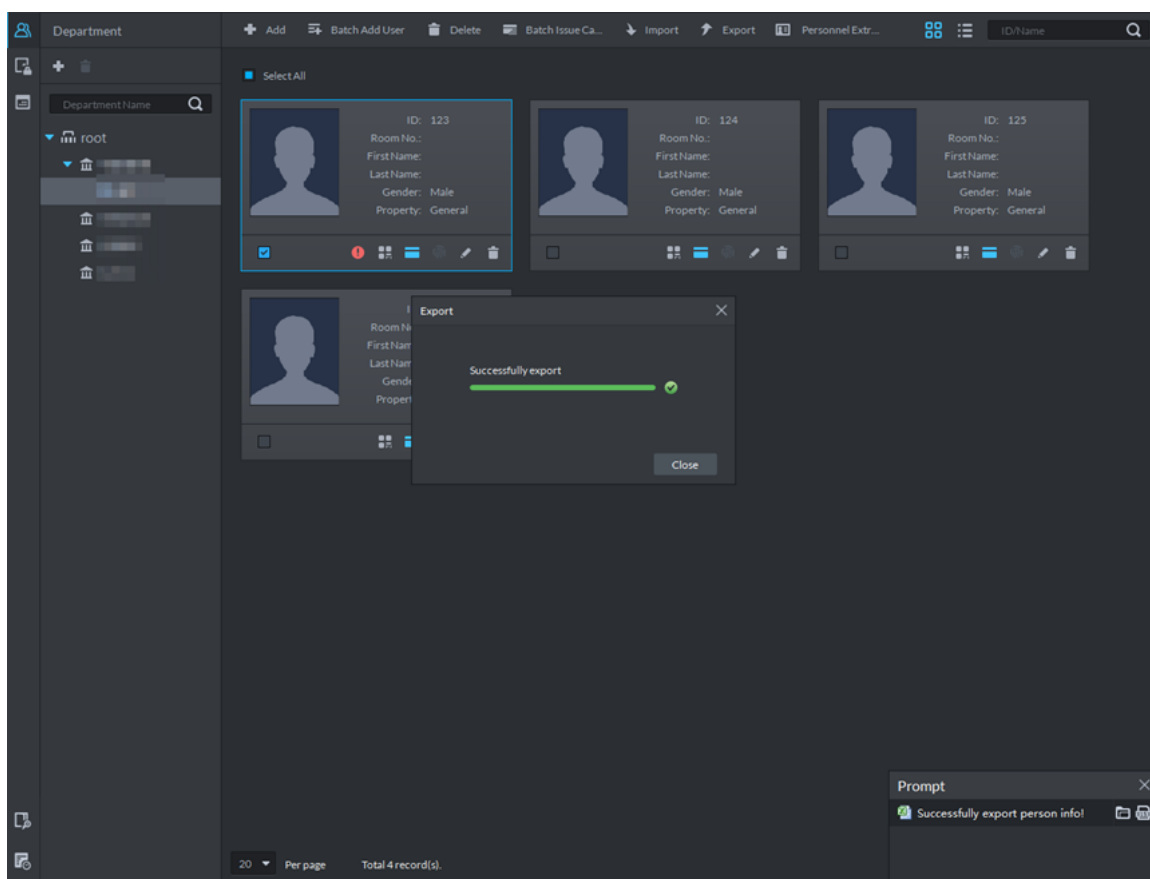
5.14.1.5 Importing/Exporting Personnel

5.14.1.5.1 Exporting Personnel

You can export personnel information if necessary.

Step 1 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 5-229 Export progress



Step 2 Click **Close**.

5.14.1.5.2 Importing Personnel

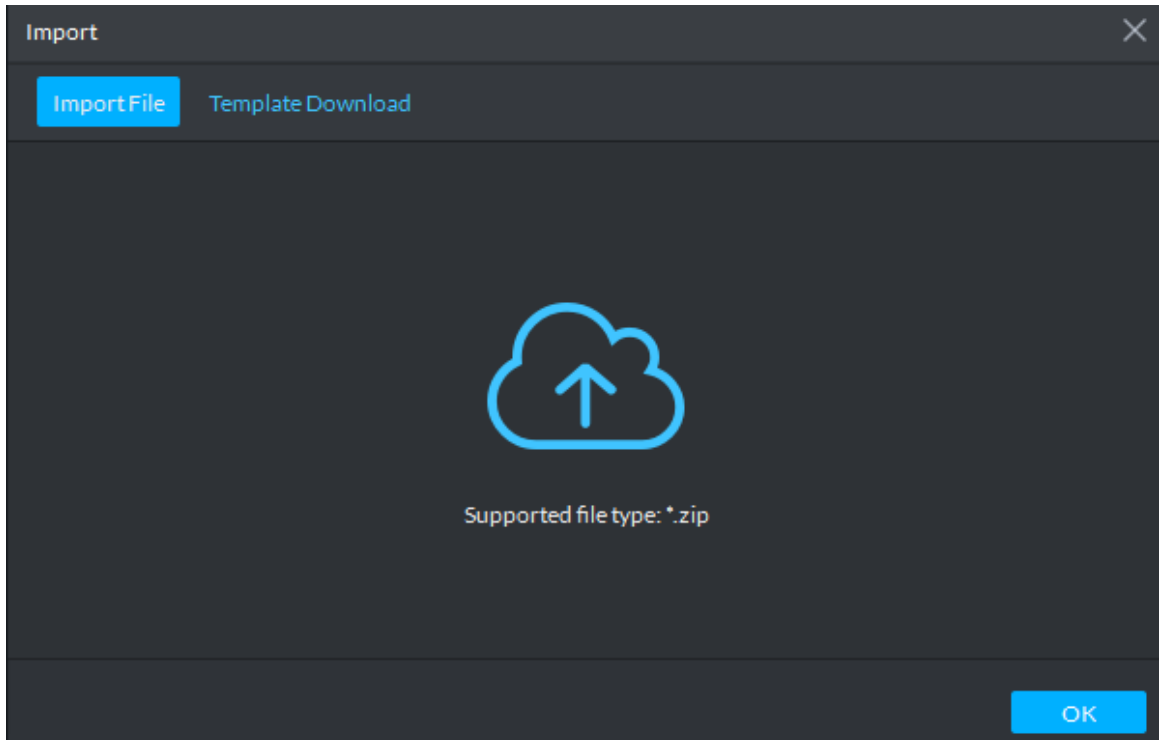
To quickly add a number of personnel, you can download a personnel template, fill in it and then import it to the platform. You can also import an existing personnel file.



- 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 On the **Personnel Management** interface, click **Import**.

Figure 5-230 Import personnel information



Step 2 Import personnel information files.

- 1) Click **Import**, and then select files.



If there is no personnel information file, click **Template Download** and follow the instructions on the interface to create personnel information.

- 2) Click **OK**.

The following cases might occur during an import:

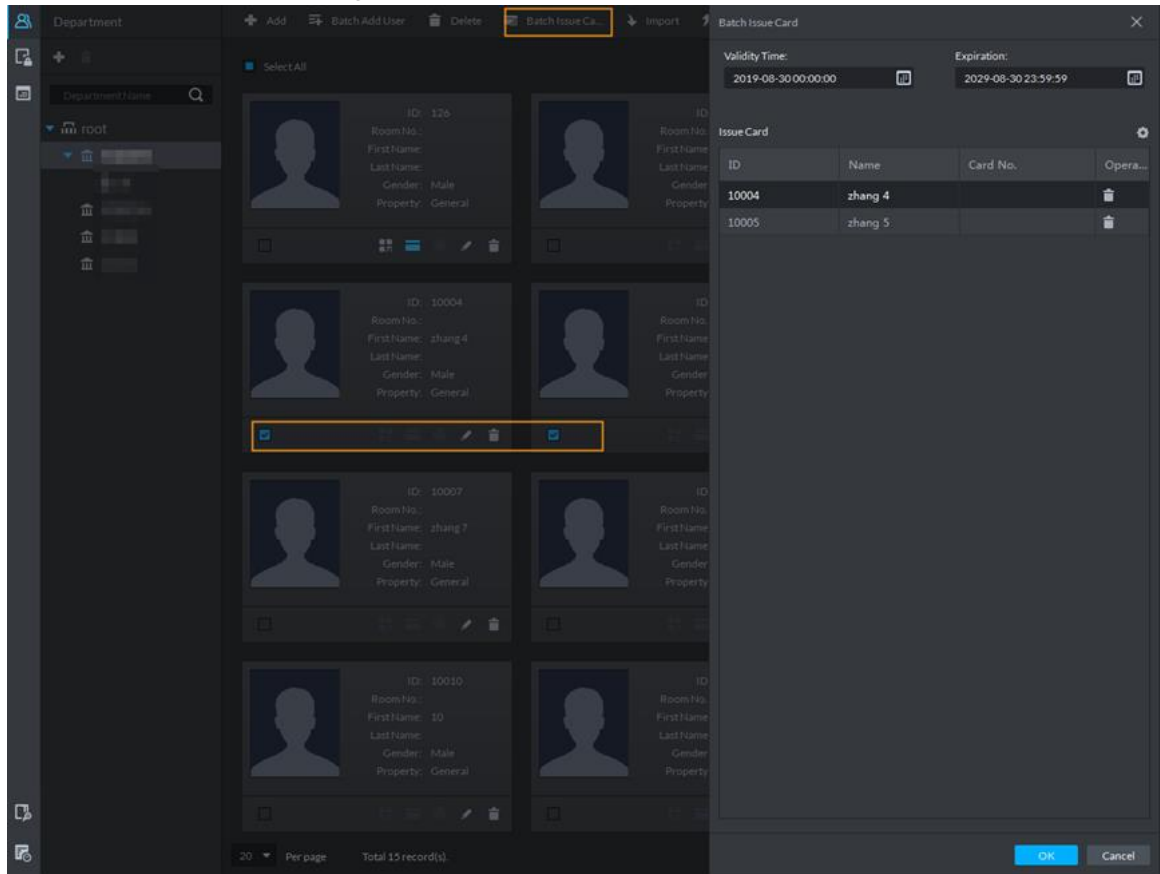
- If there are failures, you can download the failures list to view details.
- A person does not exist and the department does not exist, either. A new department will be created under the root node; if the department exists, the person is created under the department; department information matches by name.
- Cannot read the contents with a parsing error reported directly.

5.14.1.6 Issuing Cards in Batch

Support issuing cards in batch.

Step 1 On the **Personnel Management** interface, select the people to issue card to, and click **Batch Issue Card**.

Figure 5-231 Issue card in batch



Step 2 Set term of validity.

Step 3 Issue cards to personnel.

Support issuing cards by entering card number or by using a card reader.

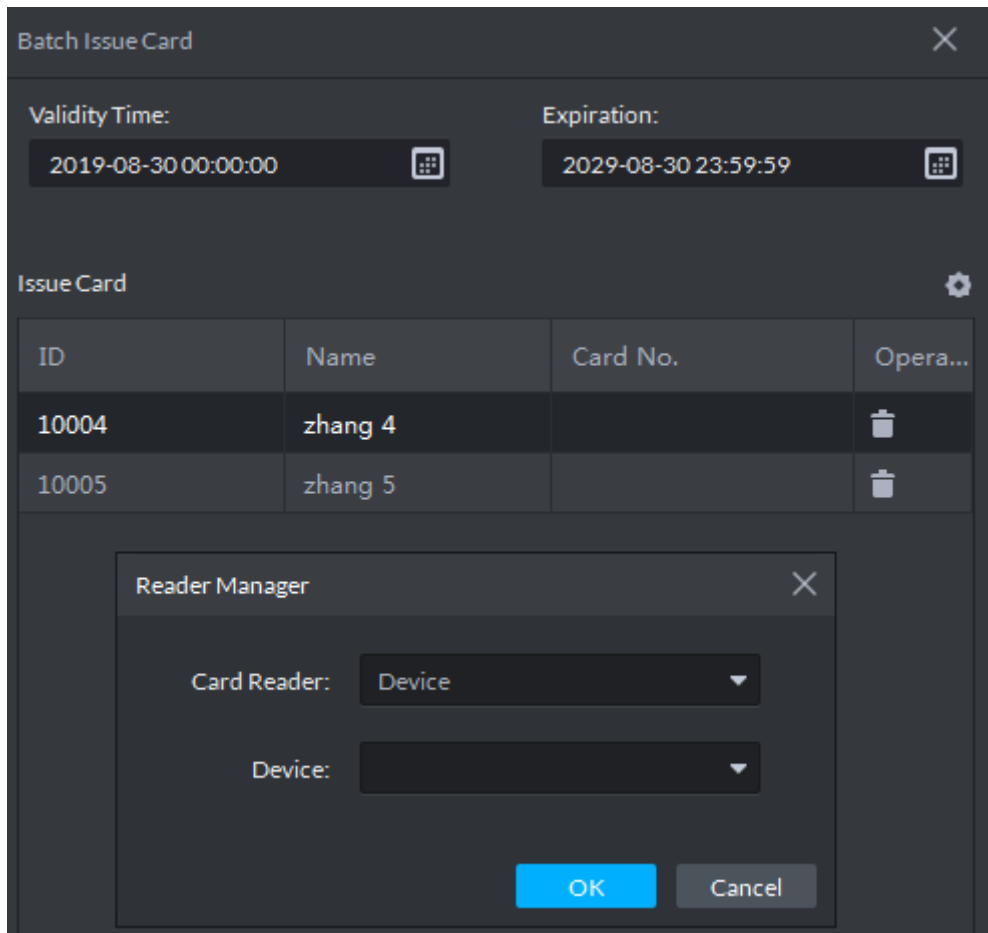
- By entering card number

- 1) Click the Card No. cells to enter card numbers one by one.
- 2) Click **OK**.

- By using a card reader

- 1) Click .

Figure 5-232 Reader manager



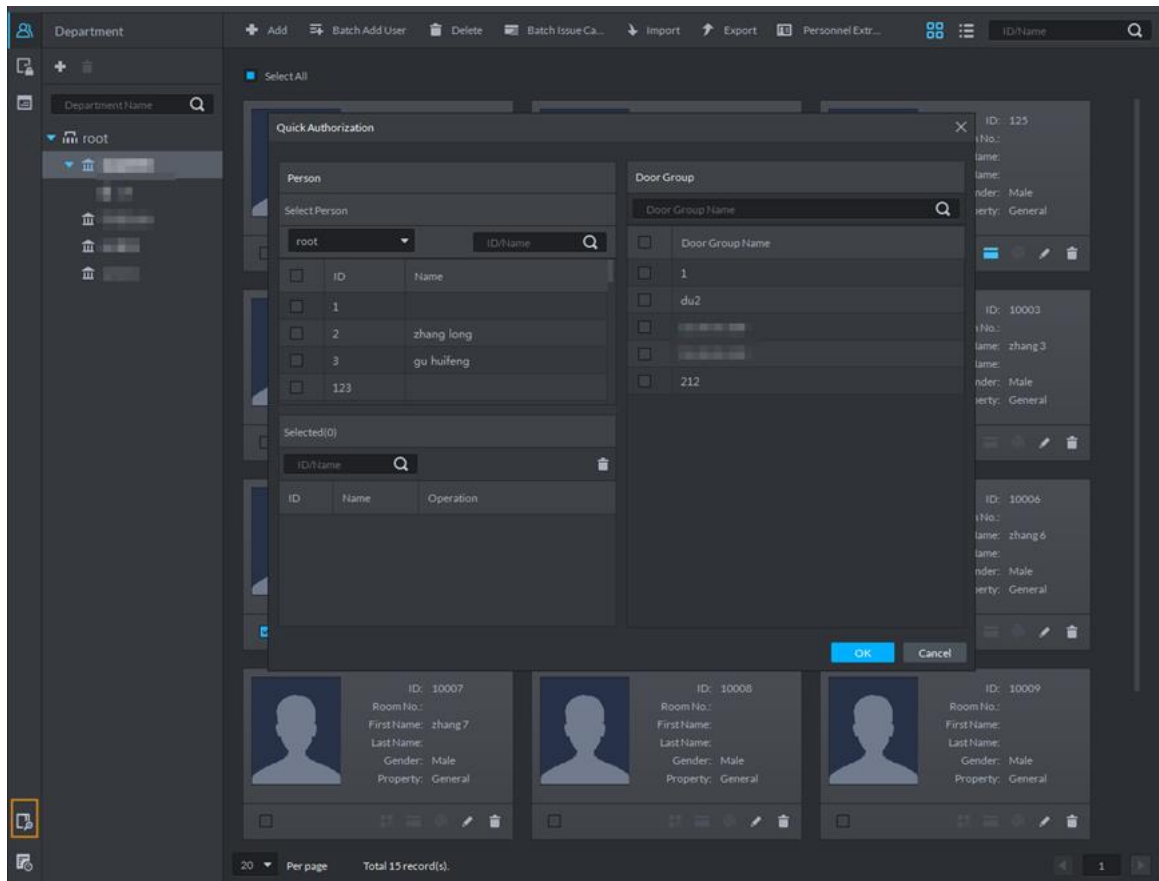
- 2) Select a card reader or device, and then click **OK**.
- 3) Select people one by one and swipe cards respectively until everyone has a card number.
- 4) Click **OK**.

5.14.1.7 Quick Authorization

Configure access permissions in a fast way.

Step 1 On the **Personnel Management** interface, click .

Figure 5-233 Quick authorization




Step 2 Select personnel in the personnel list.

Step 3 Select door groups in the door group list.

Step 4 Click **OK**.



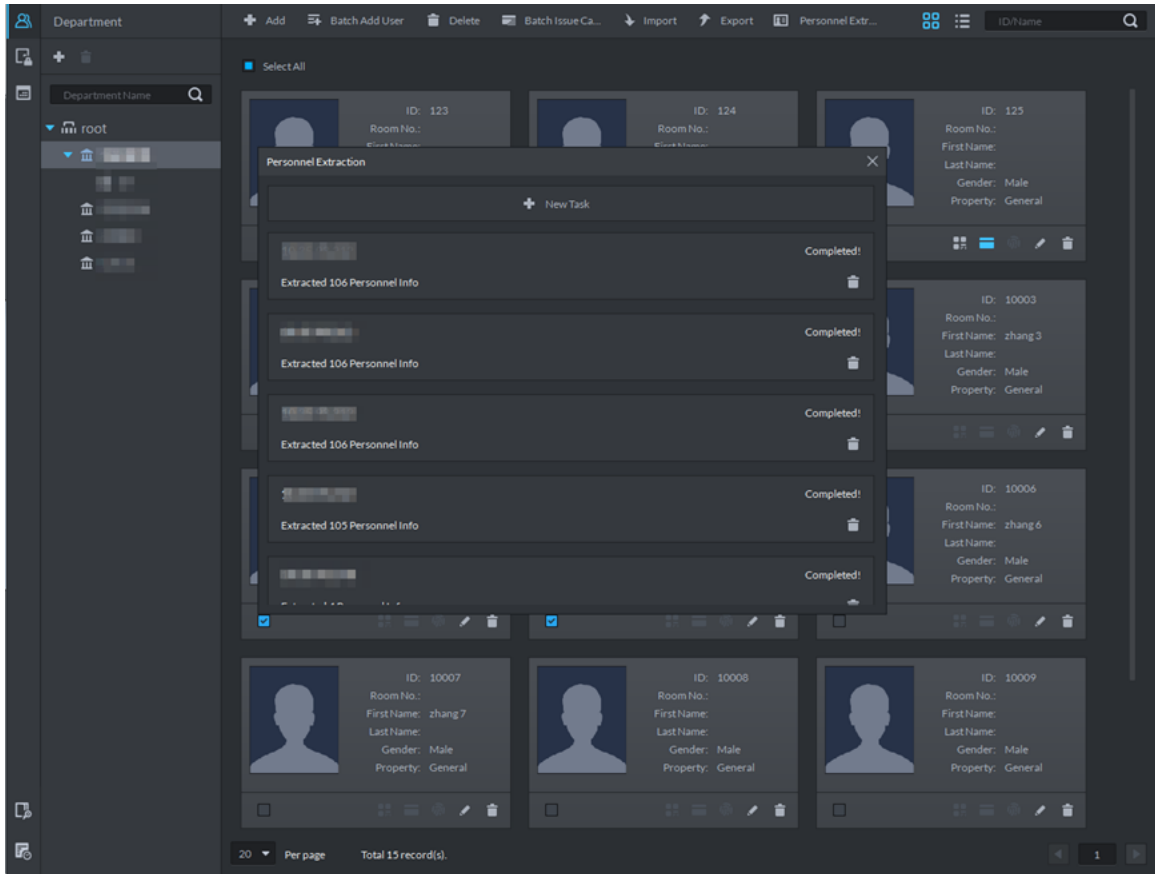
Click  to view authorization progress.

5.14.1.8 Extracting Personnel Information

When personnel information has been configured on the devices, you can directly synchronize personnel information from the devices.

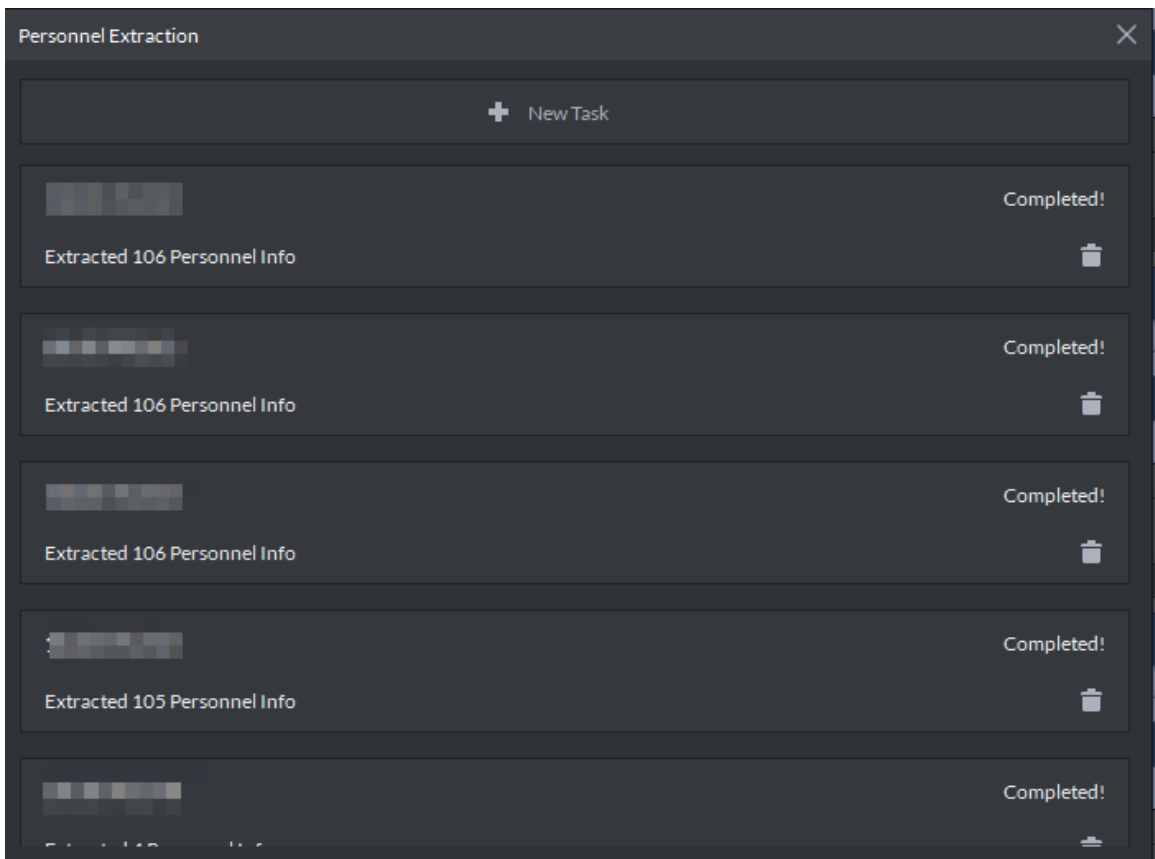
Step 1 On the Personnel Management interface, click **Personnel Extraction**.

Figure 5-234 Personnel extraction



Step 2 Click **New Task**, select a device, and then click **OK**.

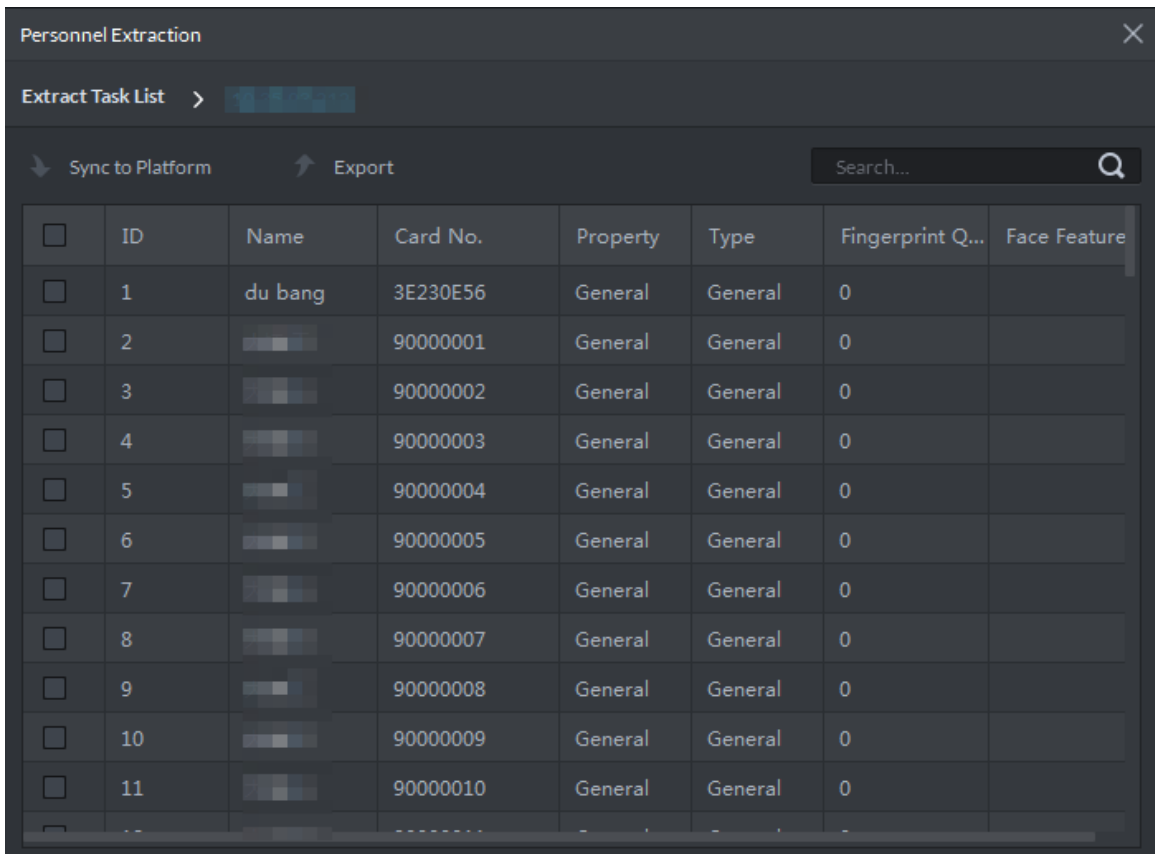
Figure 5-235 Personnel extraction results



Step 3 Double-click a piece of result.

The personnel details are displayed.

Figure 5-236 Personnel details



The screenshot shows a window titled "Personnel Extraction" with a close button in the top right. Below the title bar is a header area with "Extract Task List" and a right-pointing arrow. Below that are two buttons: "Sync to Platform" with a left-pointing arrow and "Export" with a right-pointing arrow. To the right of these buttons is a search bar labeled "Search..." with a magnifying glass icon. Below the header is a table with the following columns: ID, Name, Card No., Property, Type, Fingerprint Q..., and Face Feature. The table contains 11 rows of data, with the first row having the name "du bang".

<input type="checkbox"/>	ID	Name	Card No.	Property	Type	Fingerprint Q...	Face Feature
<input type="checkbox"/>	1	du bang	3E230E56	General	General	0	
<input type="checkbox"/>	2		90000001	General	General	0	
<input type="checkbox"/>	3		90000002	General	General	0	
<input type="checkbox"/>	4		90000003	General	General	0	
<input type="checkbox"/>	5		90000004	General	General	0	
<input type="checkbox"/>	6		90000005	General	General	0	
<input type="checkbox"/>	7		90000006	General	General	0	
<input type="checkbox"/>	8		90000007	General	General	0	
<input type="checkbox"/>	9		90000008	General	General	0	
<input type="checkbox"/>	10		90000009	General	General	0	
<input type="checkbox"/>	11		90000010	General	General	0	

Step 4 Select personnel, and then click **Sync to Platform**.

The selected personnel are added to the platform.



Click **Export**, and then you can export the personnel list.

5.14.1.9 Viewing 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.

See "错误!未找到引用源。 错误!未找到引用源。" for detailed steps.


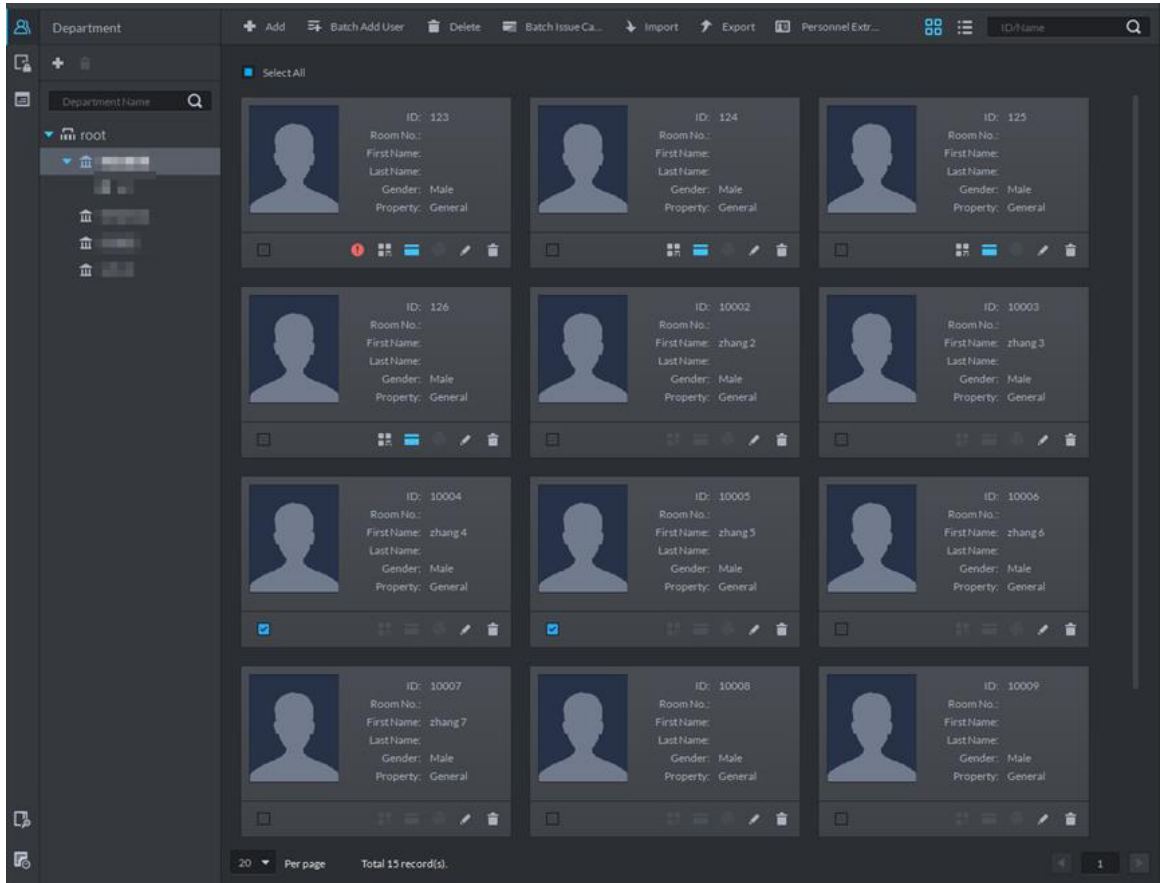
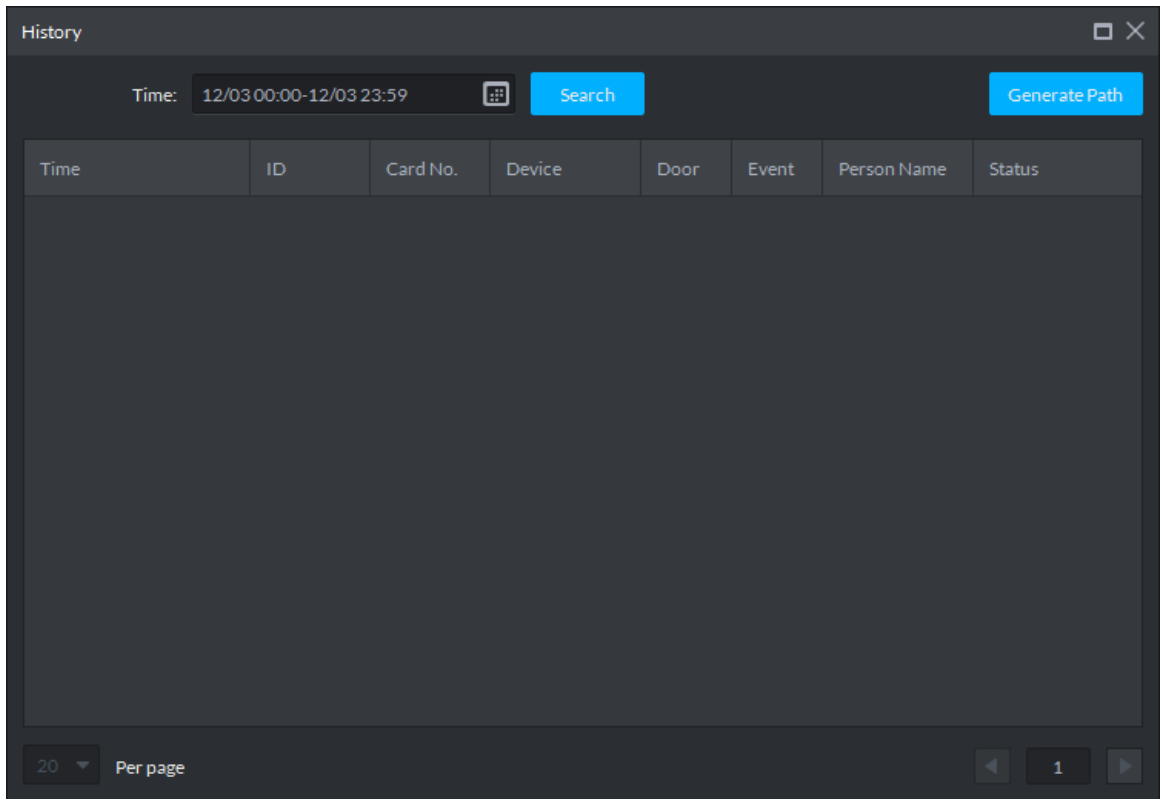
Step 1 Click . On the **Homepage** interface, select **Personnel Management**.

Figure 5-237 Personnel management interface



Step 2 Click  or .

Figure 5-238 History



Step 3 Set search time, and then click **Search**.

The search results are displayed.

Step 4 Click **Generate Path**.

The map interface which shows the corresponding path is displayed.

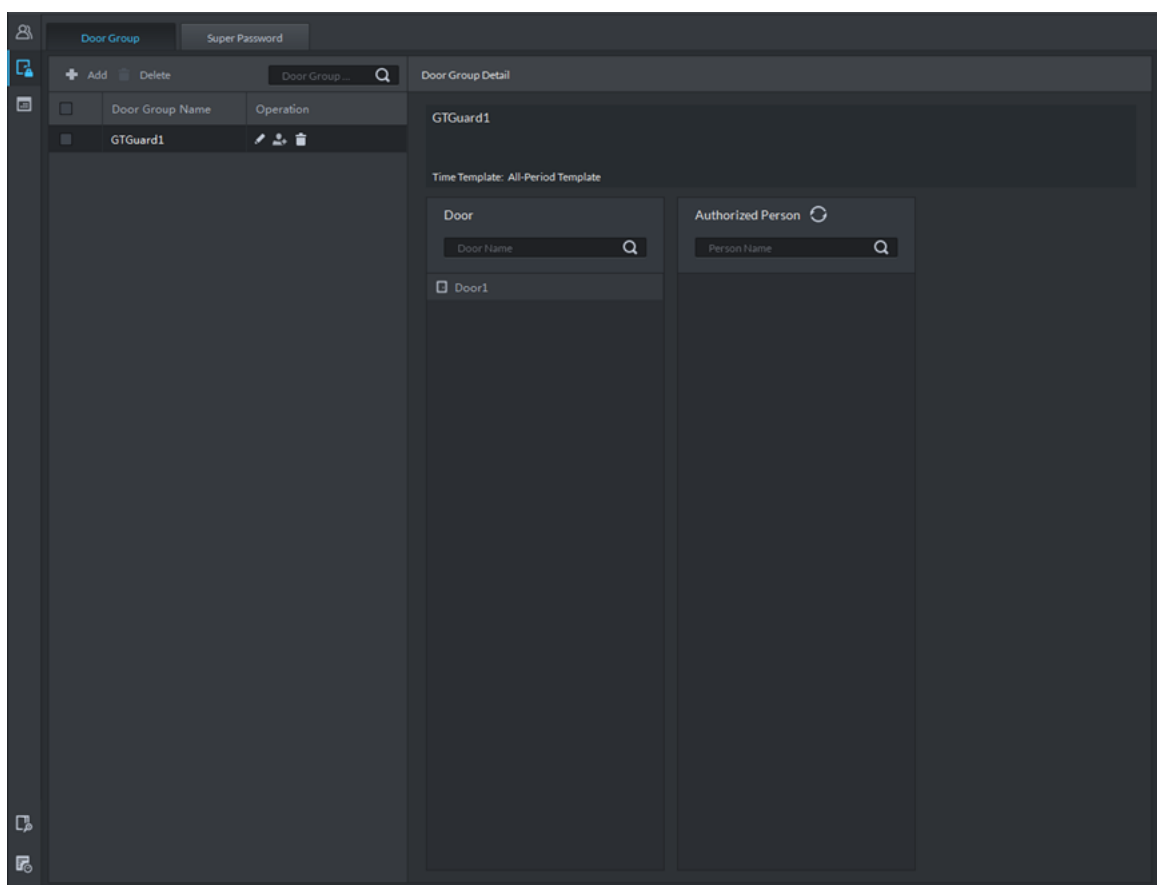
Step 5 Click **Export**, and then drag to select a region to save the path as a picture to the local disk.

5.14.2 Configuring Door Groups

Configure door groups so that you can quickly assign permissions by door groups.

Step 1 On the **Personnel Management** interface, click .

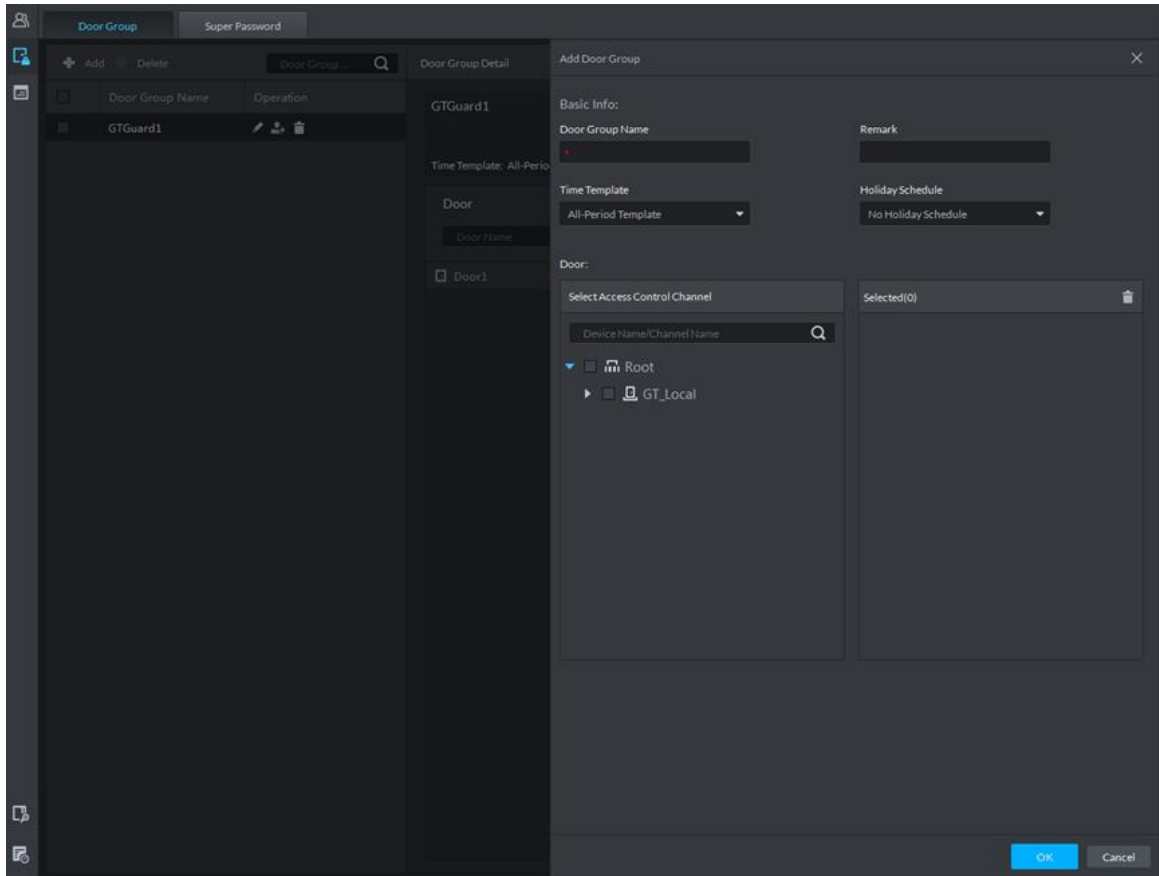
Figure 5-239 Access control permission interface



Step 2 Create a door group.

- 1) Click the **Door Group** tab.
- 2) Click **Add**.

Figure 5-240 Add a door group



- 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, when assigning permissions to personnel, it is valid only to select a time period within the template and select a channel as selected here.

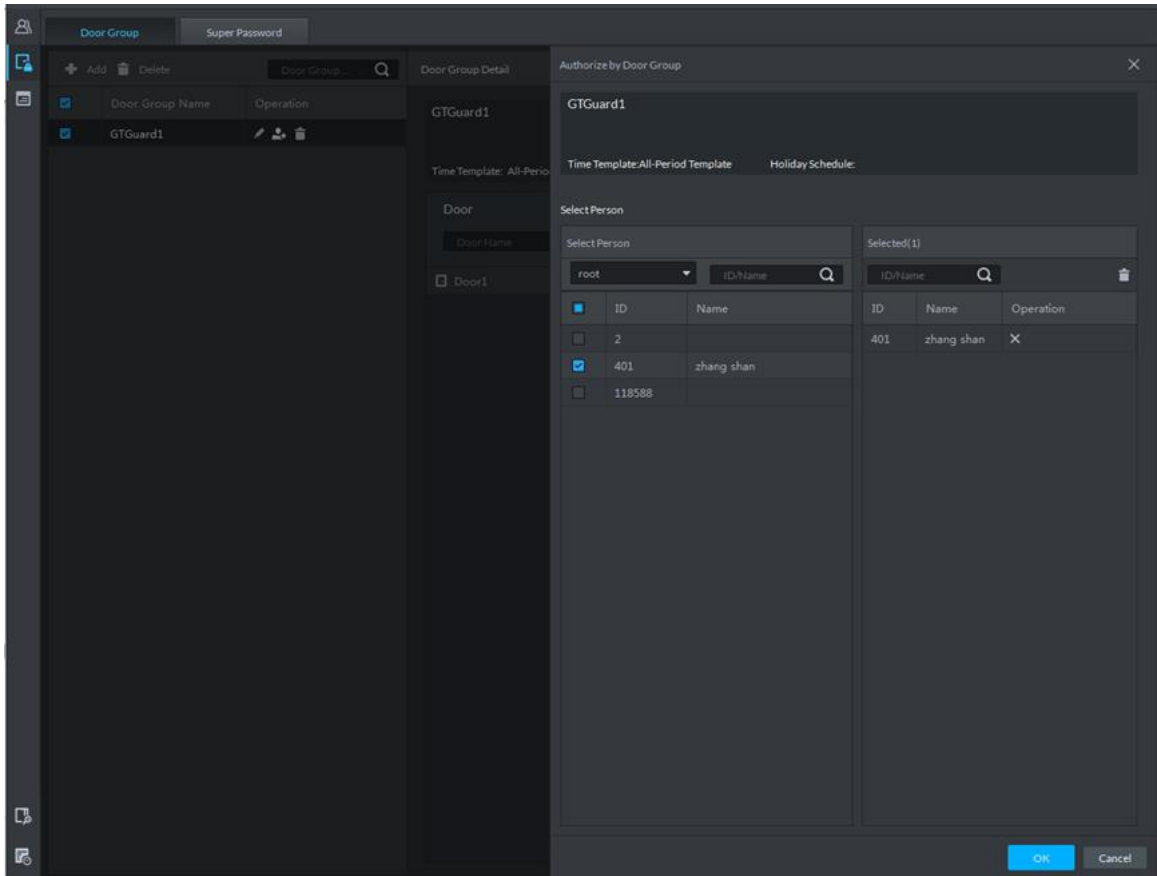


- To create a new time template, select **Manage time template** in the **Time Template** dropdown list. For details, see "5.14.4 Configuring Time Templates."
- To create a new holiday schedule, select **Add Holiday Schedule** in the **Holiday Schedule** dropdown list. For details, see "5.14.5 Configuring Holiday Schedules."

Step 3 Authorize.


- 1) On the **Door Group** interface, select a door group, and then click the corresponding  icon.

Figure 5-241 Authorize by door group



- 2) Select personnel, and then click **OK**.



Click  to update authorized personnel.

5.14.3 Configuring Super Passwords

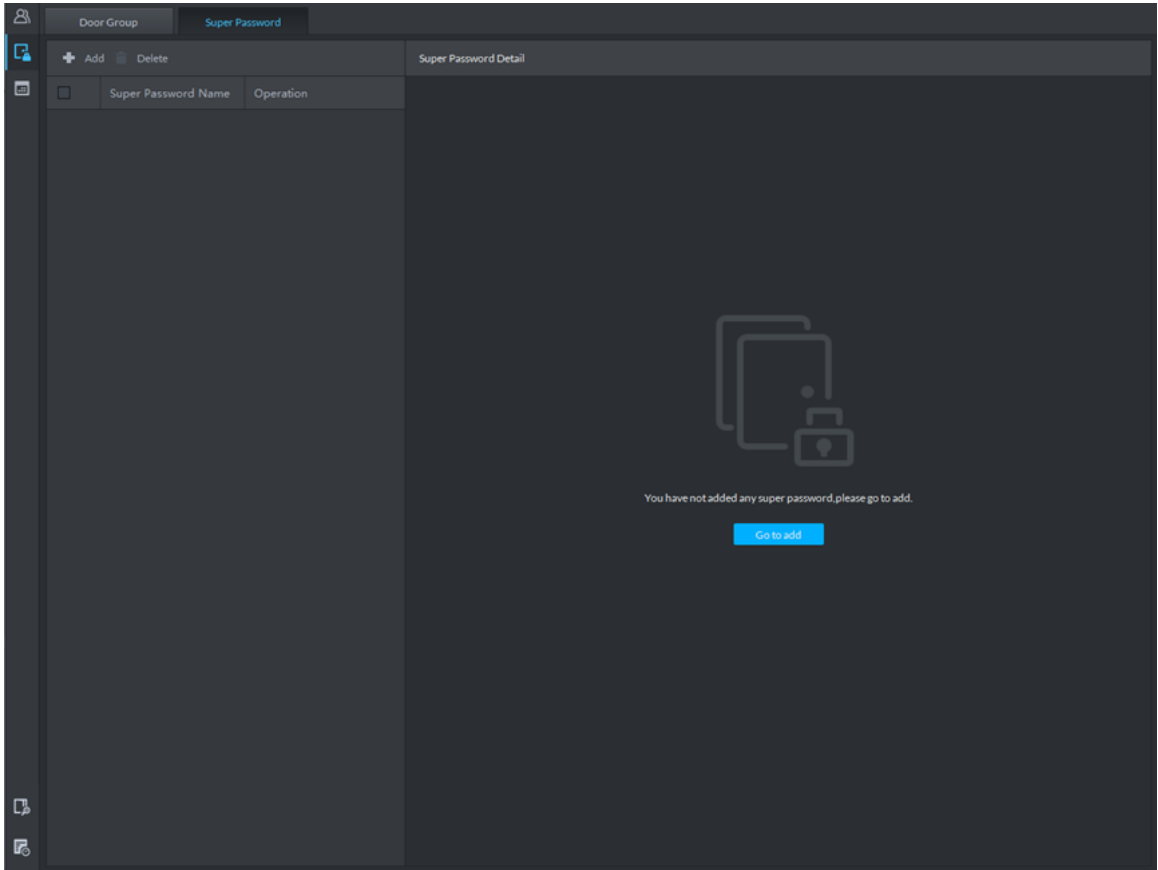
The second-generation access control devices support opening door with super passwords.



After super password is configured, you can use super password to open door. For details about how to configure super password, see "5.15.2 Adding Access Control."

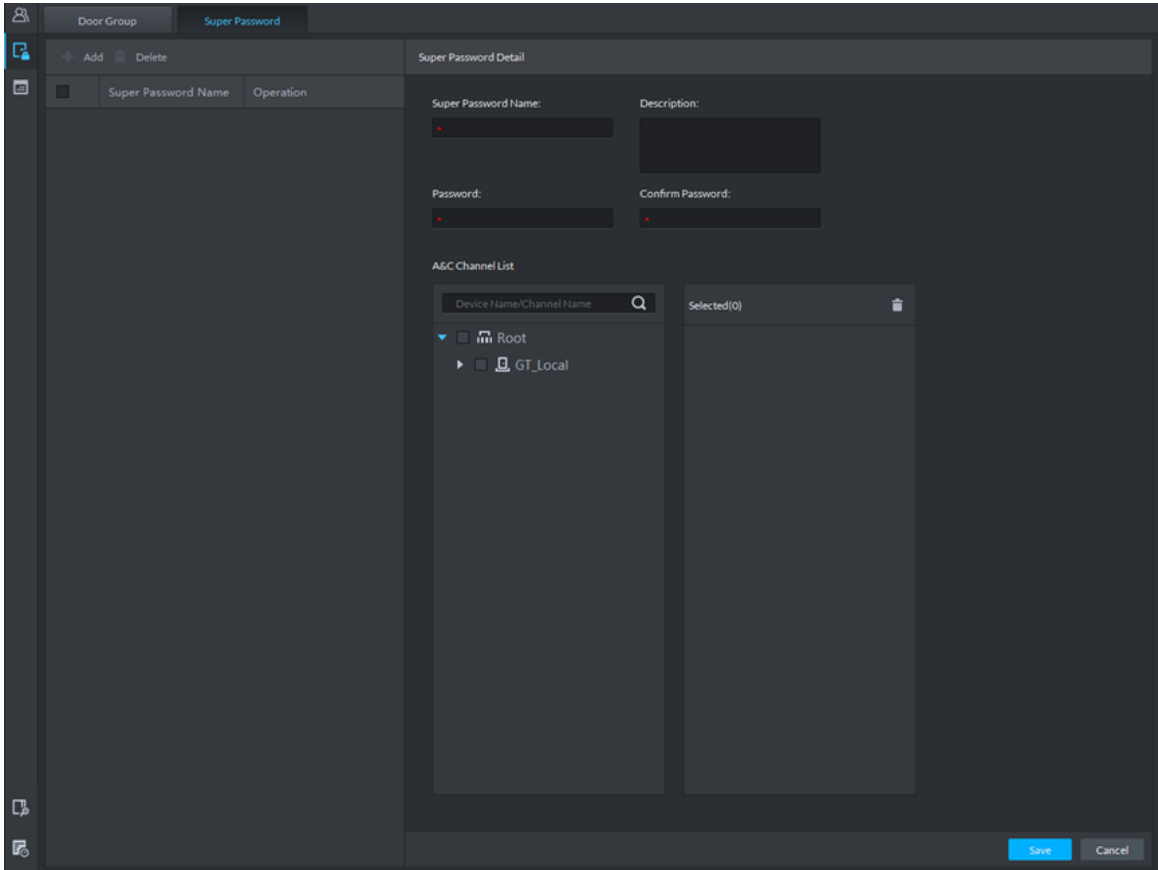
Step 1 On the **Access Control Permission** interface, click the **Super Password** tab.

Figure 5-242 Super password



Step 2 Click **Add**.

Figure 5-243 Add a super password



Step 3 Set parameters, and then select device channels (second-generation access control devices).

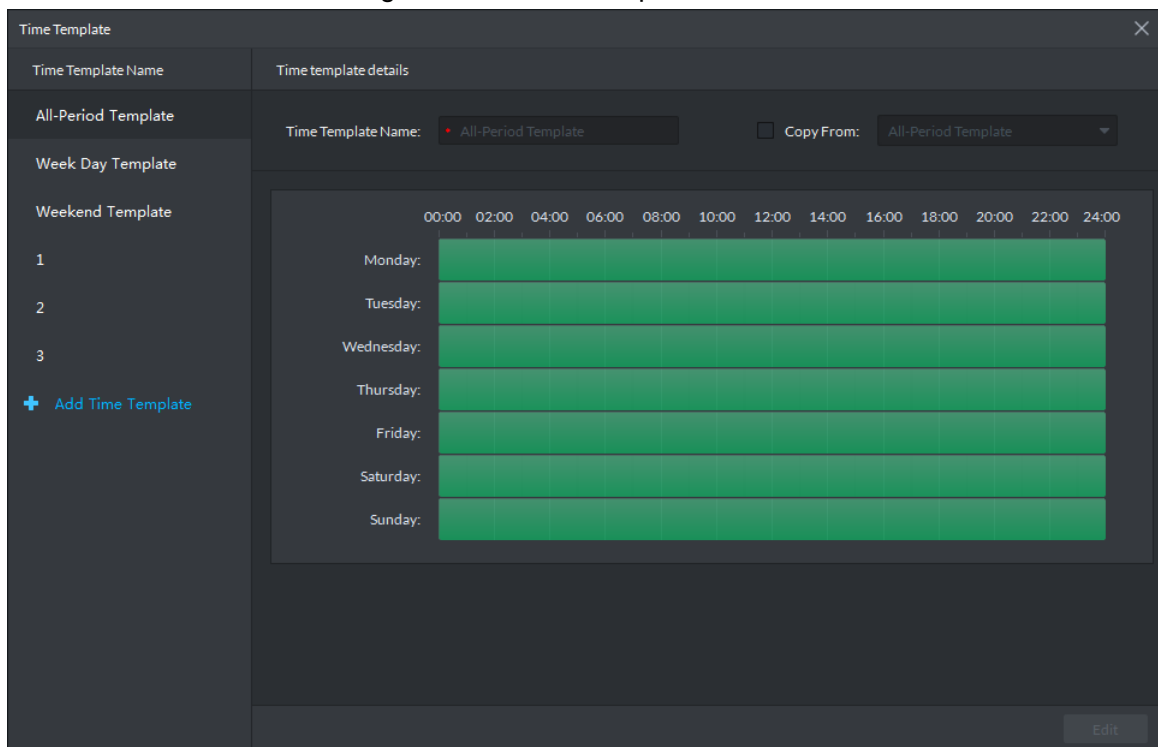
Step 4 Click **Save**.

5.14.4 Configuring Time Templates

Configure time templates for access control. A permission is only valid within the selected time period.

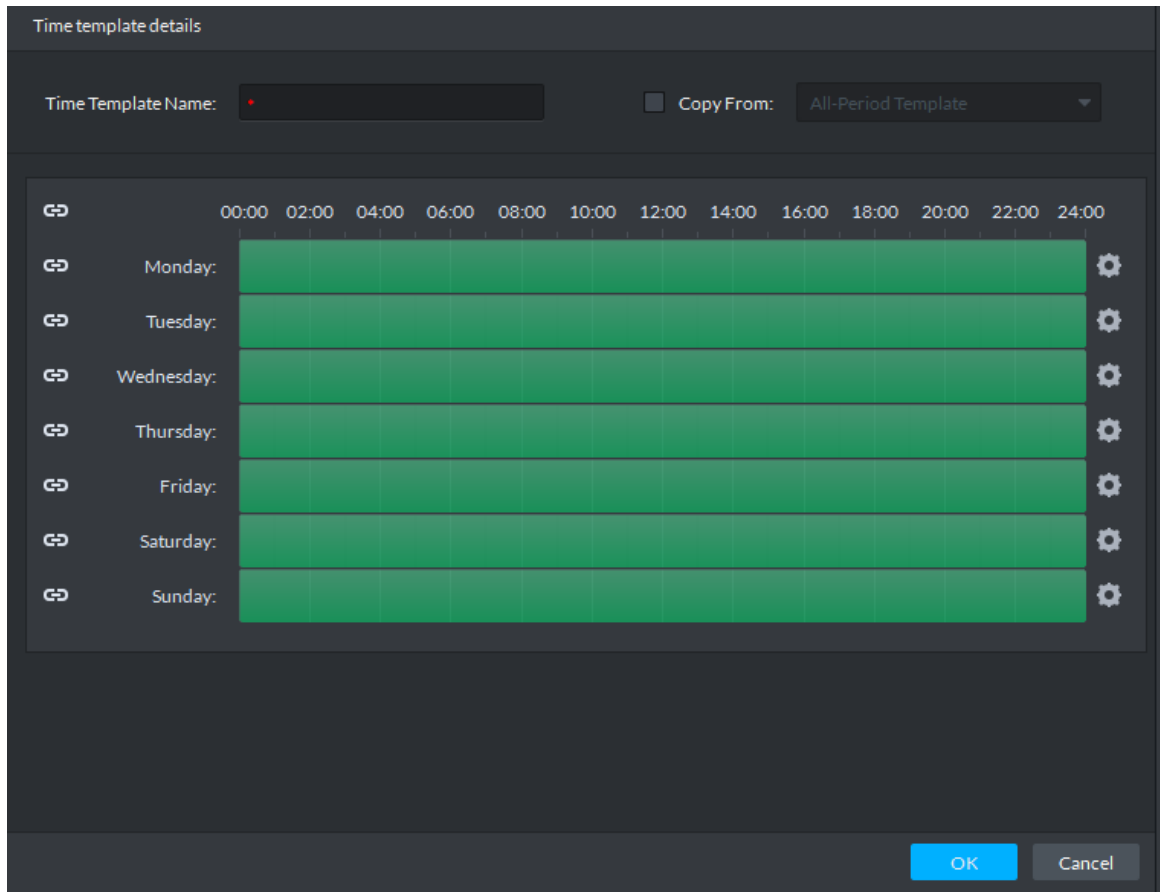
Step 1 When adding or editing a door group, select **Manage time template** in the **Time Template** dropdown list.

Figure 5-244 Time template



Step 2 Click **Add Time Template**.

Figure 5-245 Add a time template



Step 3 Enter the template name, set time periods, and then click **OK**.







To use an existing template, select the **Copy From** check box and then select a template in the dropdown list.

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.

5.14.5 Configuring Holiday Schedules

Configure holiday schedules.

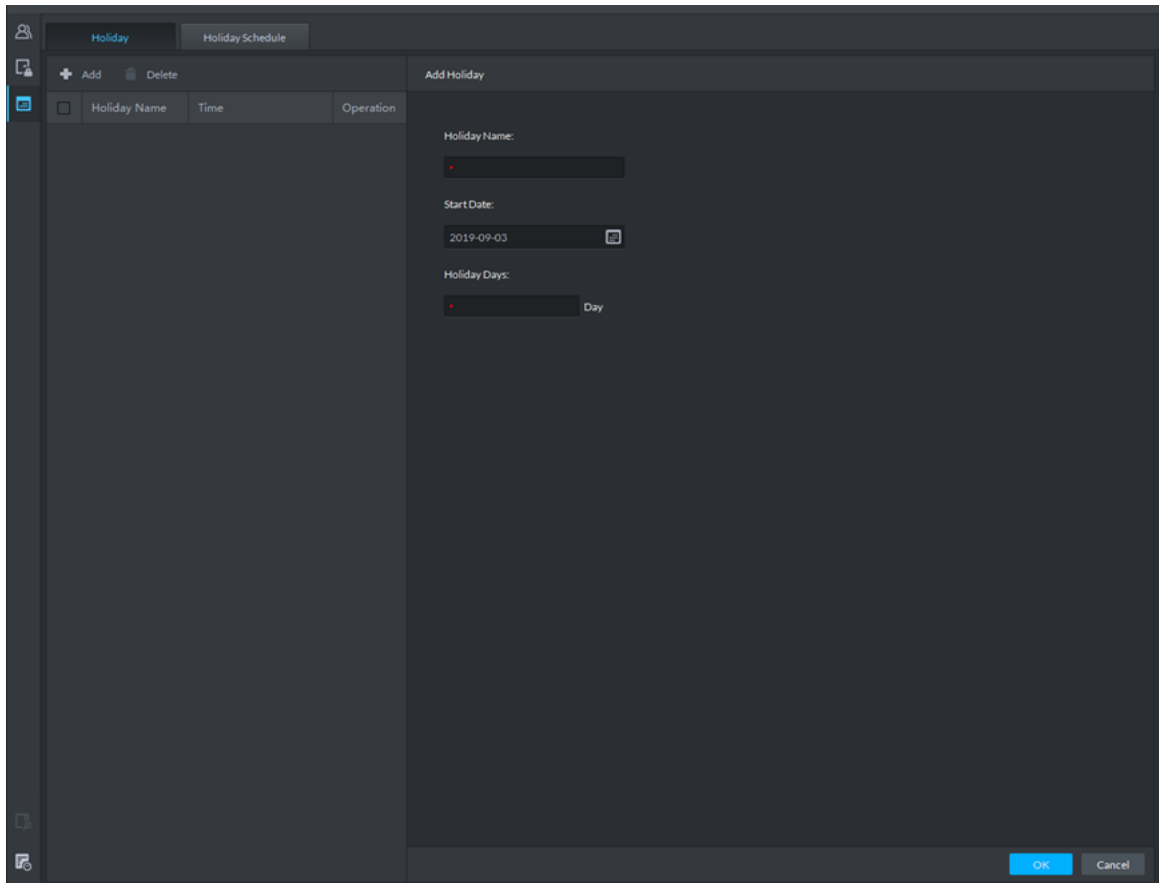
5.14.5.1 Setting Holidays

Set holidays before configuring holiday schedules. Support up to 16 holidays.

Step 1 On the **Personnel Management** interface, click .

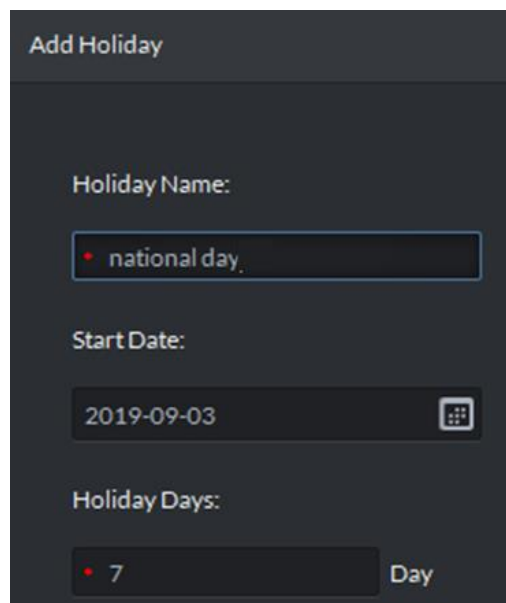
Step 2 Click the **Holiday** tab.

Figure 5-246 Holiday



Step 3 Click **Add**, and then set a holiday.

Figure 5-247 Add a holiday



Step 4 Click **OK**.

5.14.5.2 Configuring Holiday Permissions

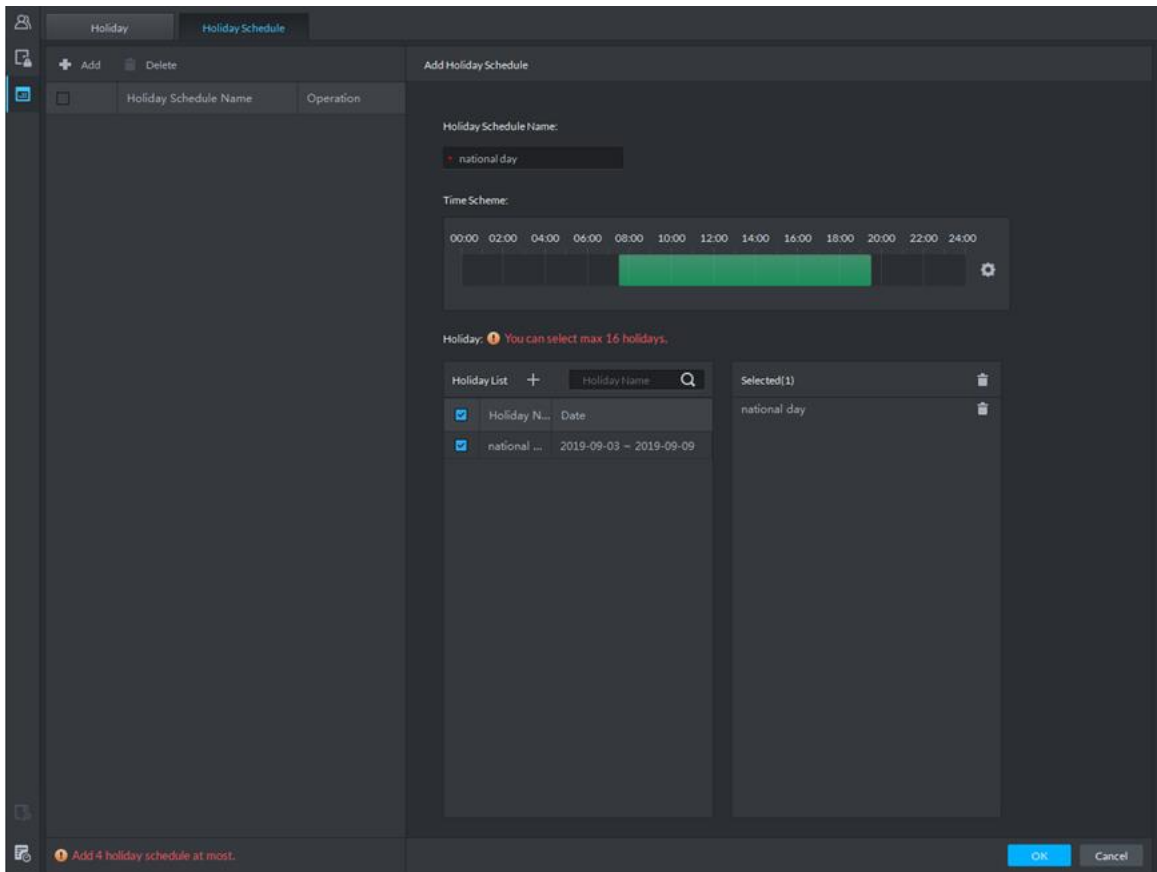
Set access control schedules for the holidays. Up to 4 schedules can be added.

Step 1 On the **Personnel Management** interface, click .

Step 2 Click the **Holiday Schedule** tab.

Step 3 Click **Add**.

Figure 5-248 Add a holiday schedule

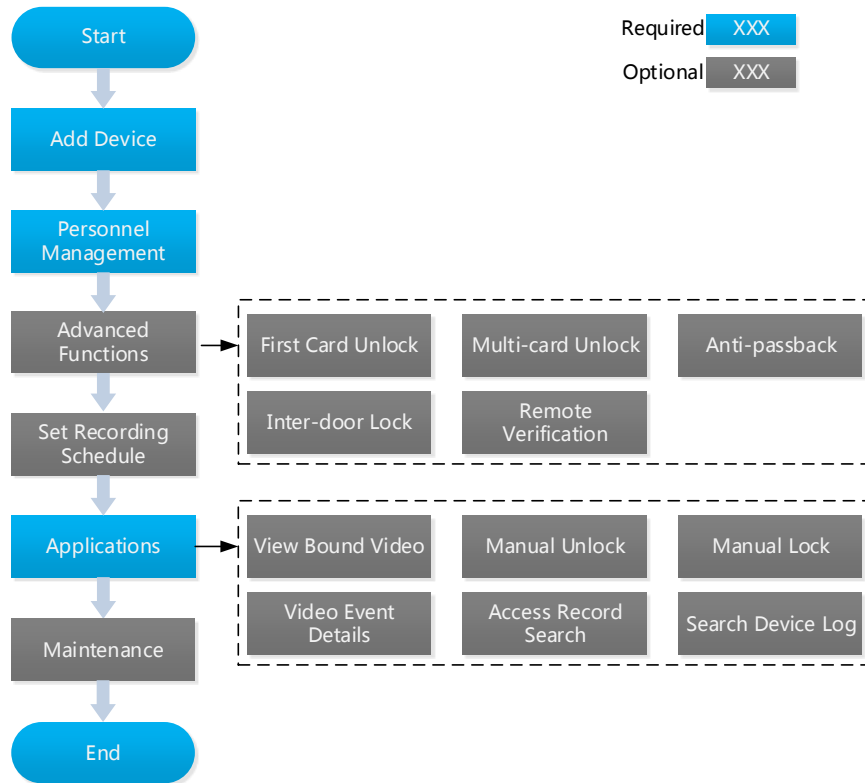


Step 4 Set the parameters as required, and then click **OK**.

5.15 Access Control

After adding access control devices on Pro, you can control the door locking/unlocking on platform, view videos and events related to the access control channel, and configure advanced access control functions, such as First Card Unlock and Multi-card Unlock.

Figure 5-249 Access control business flow



5.15.2 Adding Access Control

Step 1 Add access control device. For more details, see "错误!未找到引用源。 错误!未找到引用源。."

Support access control devices including general access control device, integrated access controller, second-generation access control device, face access control device and IR face access control device. Set **Device Category** as **Access Control** when adding.

Step 2 Bind resources.

If panoramic camera is installed in the scene, it supports binding AC channel and panoramic camera. You can view real-time video image of panoramic camera on console. When alarm is triggered, you can view video of bound panoramic camera.



The panoramic camera is required to be added to platform before binding resources.

- 1) On client homepage, click **Config**.
The system displays **Config** interface.
- 2) In the left device tree, select AC channel, and then click **Resource Bind**.

Figure 5-250 Enter resource bind interface

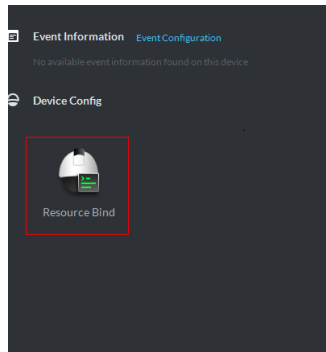
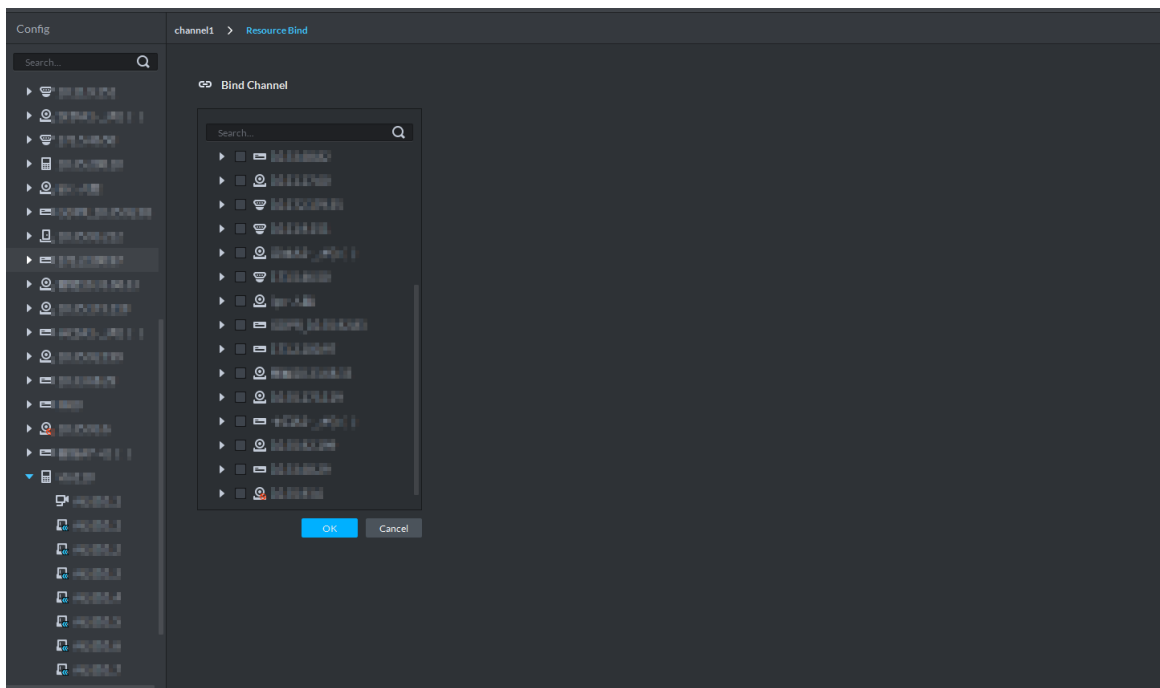


Figure 5-251 Resource bind



- 3) Select bound video channel, click **OK**.

Step 3 Configure door info.

You can configure door status, NC and NO period, alarm enable and unlock length.

- 1) On client homepage, click **Config**.
- 2) In left device tree, select AC channel, and then click **Door Configuration**.



For the console on access control interface, right-click **AC Channel**, select **AC Channel Config** and enter **Door Config** interface.

Figure 5-252 Enter config interface

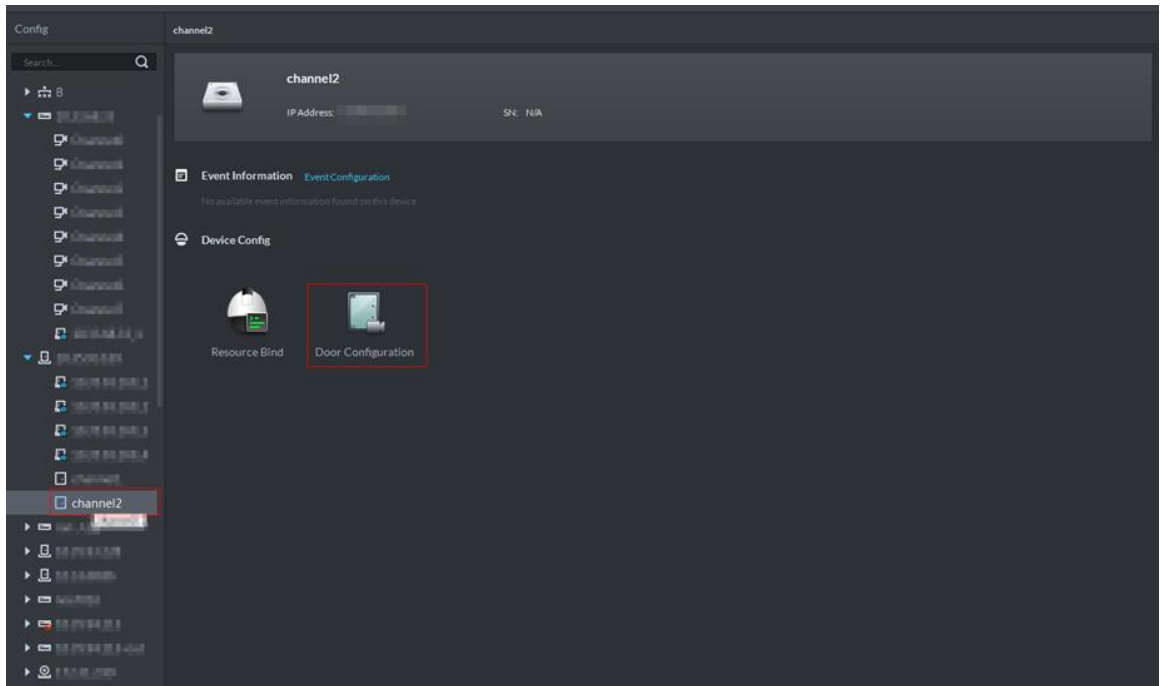
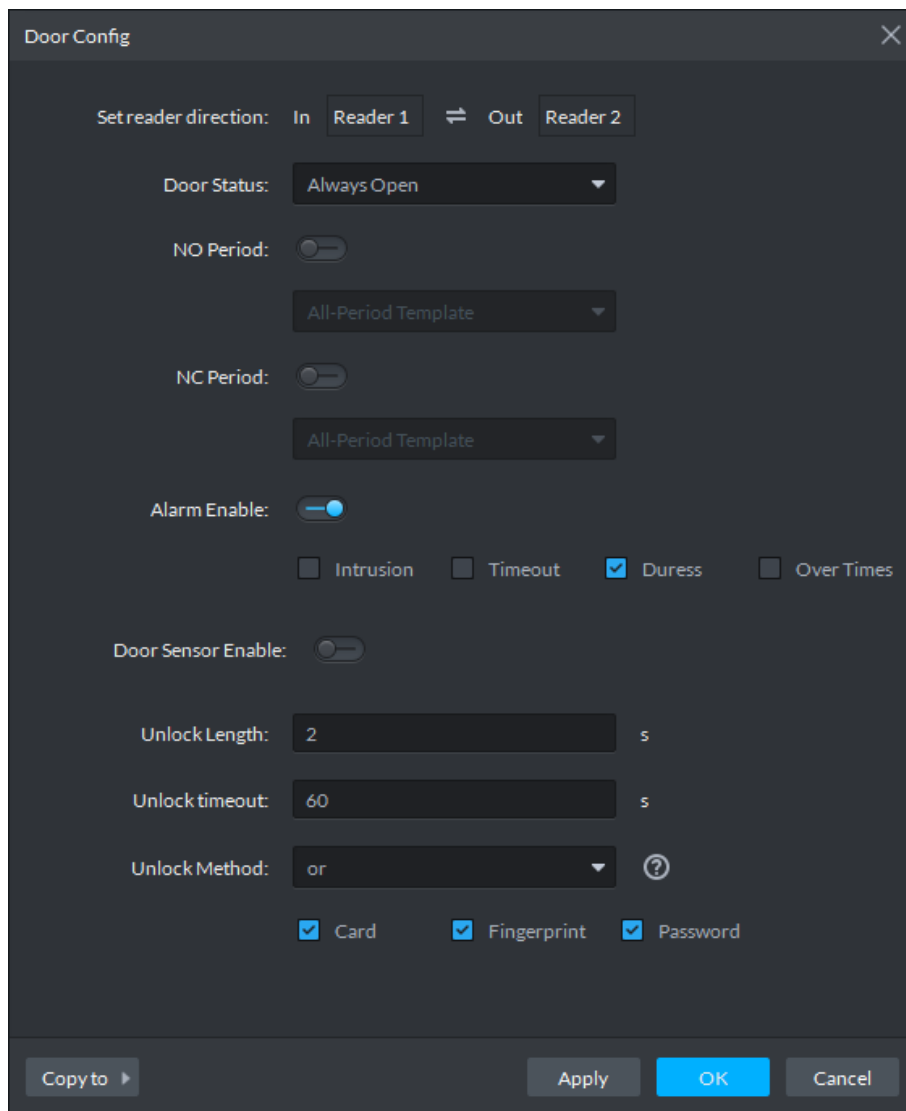


Figure 5-253 Door config



3) Configure door information and click **OK**.



The interface might be different for different access control devices connected. The actual interfaces shall prevail.

Table 5-56 Door configuration description

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 opened not as intended, the door sensor is enabled and triggers an intrusion alarm. • Entry with the duress card, duress password, or duress fingerprint triggers a duress alarm. • Unlock duration exceeding the Unlock timeout triggers a timeout alarm. • Swiping an illegal card for more than five times triggers a malicious alarm.
Super Password	Super passwords take effect after being enabled.
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	There can only be one door open in a door group at the same time. When one door is open, the others will keep locked until that door closes. See "3.13.5.4 Inter-door Lock" for details.
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.

5.15.3 Personnel Management

If you want to add personnel, see "5.14 Personnel Management." When adding personnel, you need to add information such as card, fingerprint and face comparison according to requirement, and enable access control permission.

5.15.4 Advanced Function

5.15.4.1 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** dropdown list when adding this person. For details, see "5.14 Personnel Management."


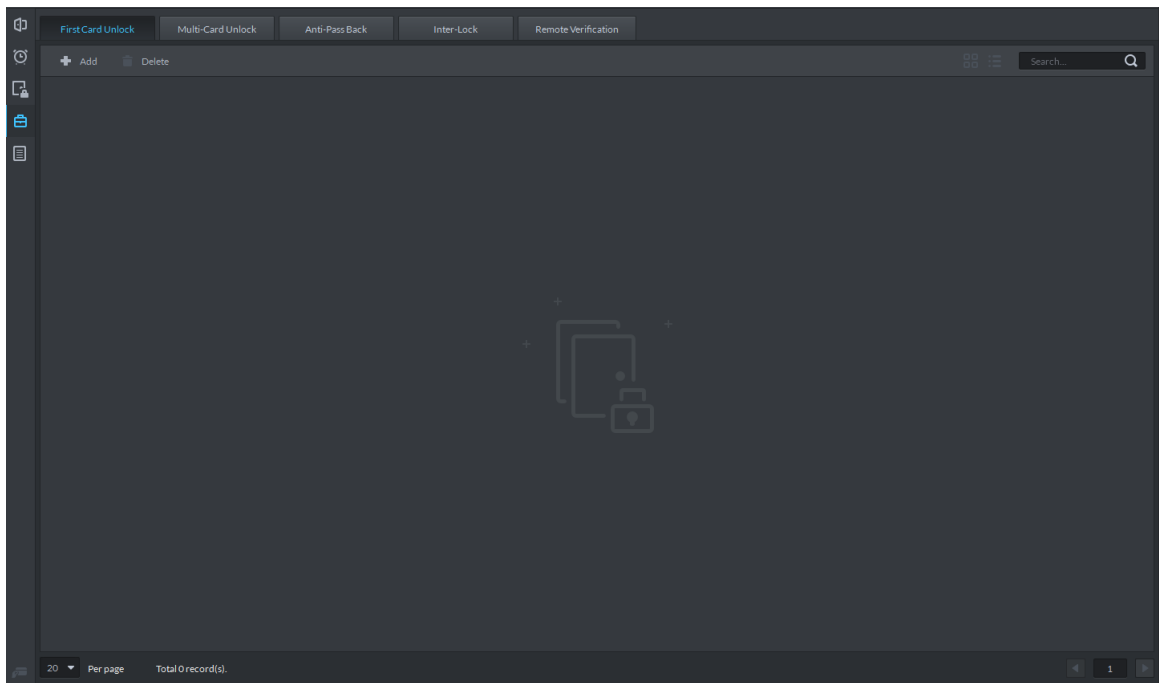
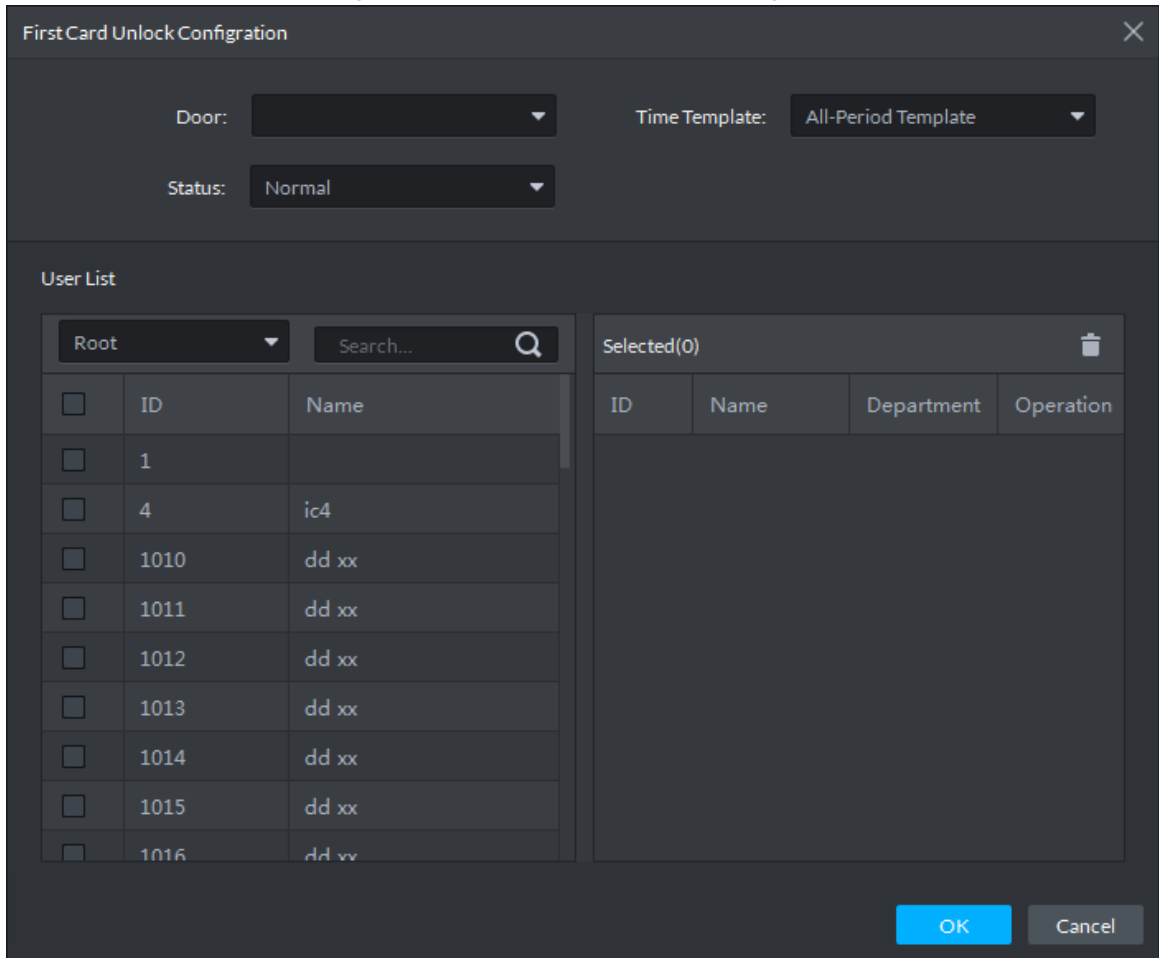
Step 1 On the **Access Control** interface, click  and select **First Card Unlock**

Figure 5-254 First card unlock



Step 2 Click **Add**.

Figure 5-255 First card unlock config



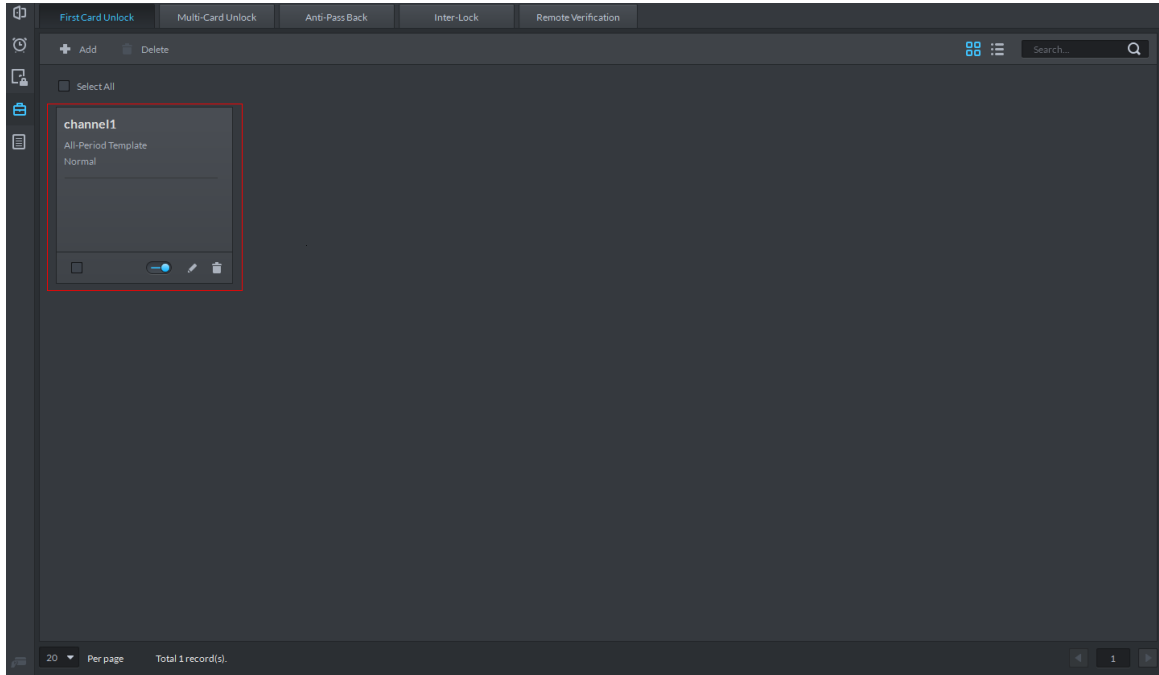
Step 3 Configure the **First Card Unlock** parameters and click **OK**.

First Card Unlock is enabled by default.

Table 5-57 First card unlock parameter description

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 5-256 First card info list



Step 4 Click .
The icon changing into  indicates **First Card Unlock** is enabled.

5.15.4.2 Multi-Card Unlock

In this mode, 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 64 users.
- One person can only belong to one group.
- With Multi-Card Unlock enabled for an access control channel, it supports up to four groups of users being on site at the same time for verification. The total number of users can be 64 at most, with up to five valid users.


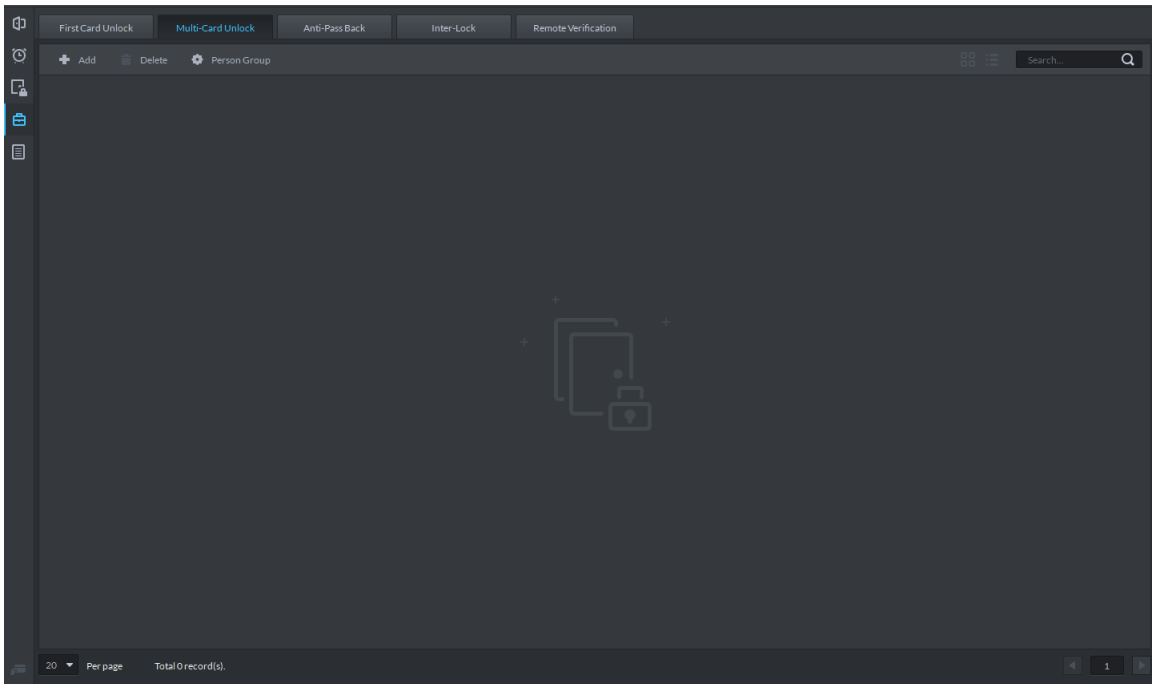
Step 1 On the **Access Control** interface, click  and select **Multi-card Unlock**.

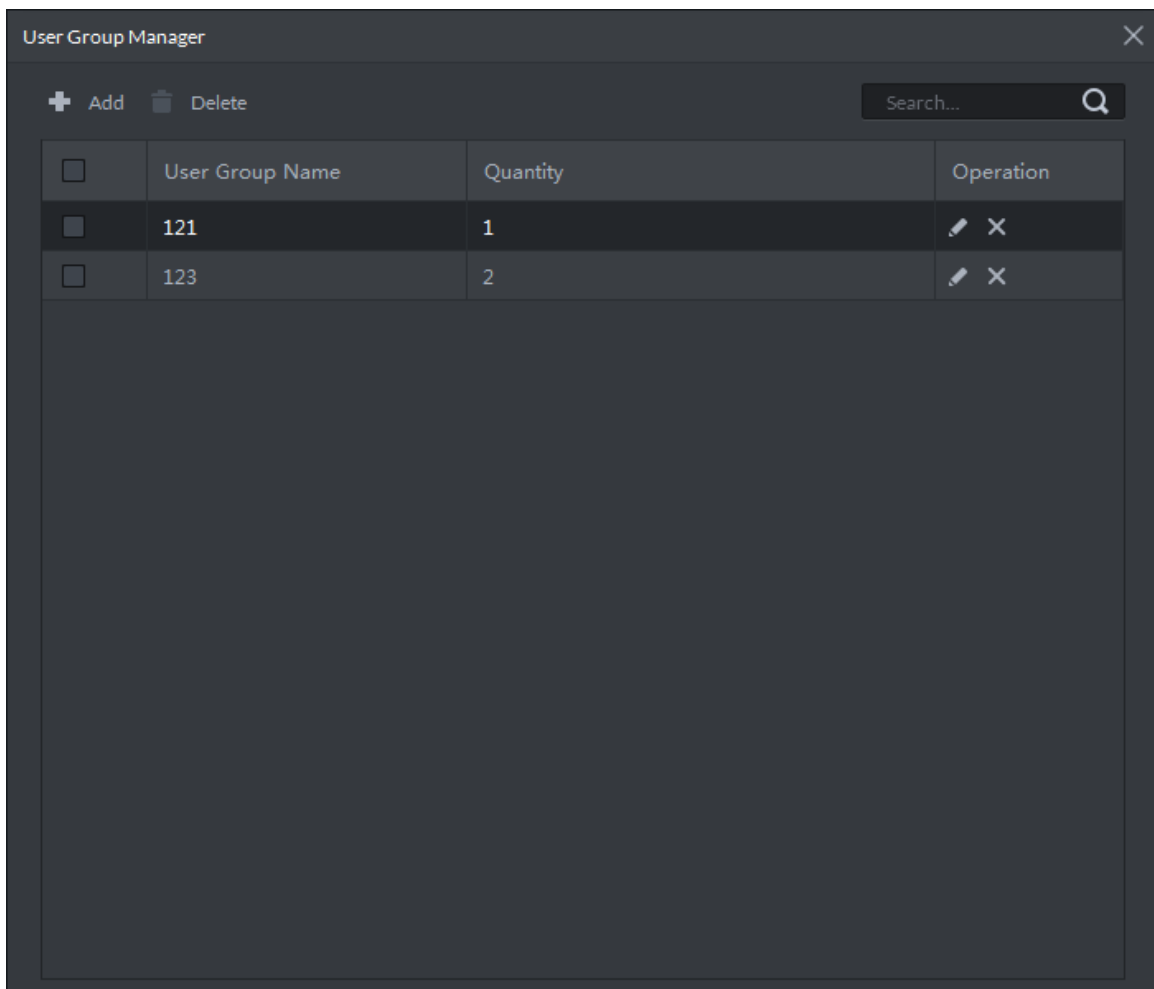
Figure 5-257 Multi-card unlock



Step 2 Add user group.

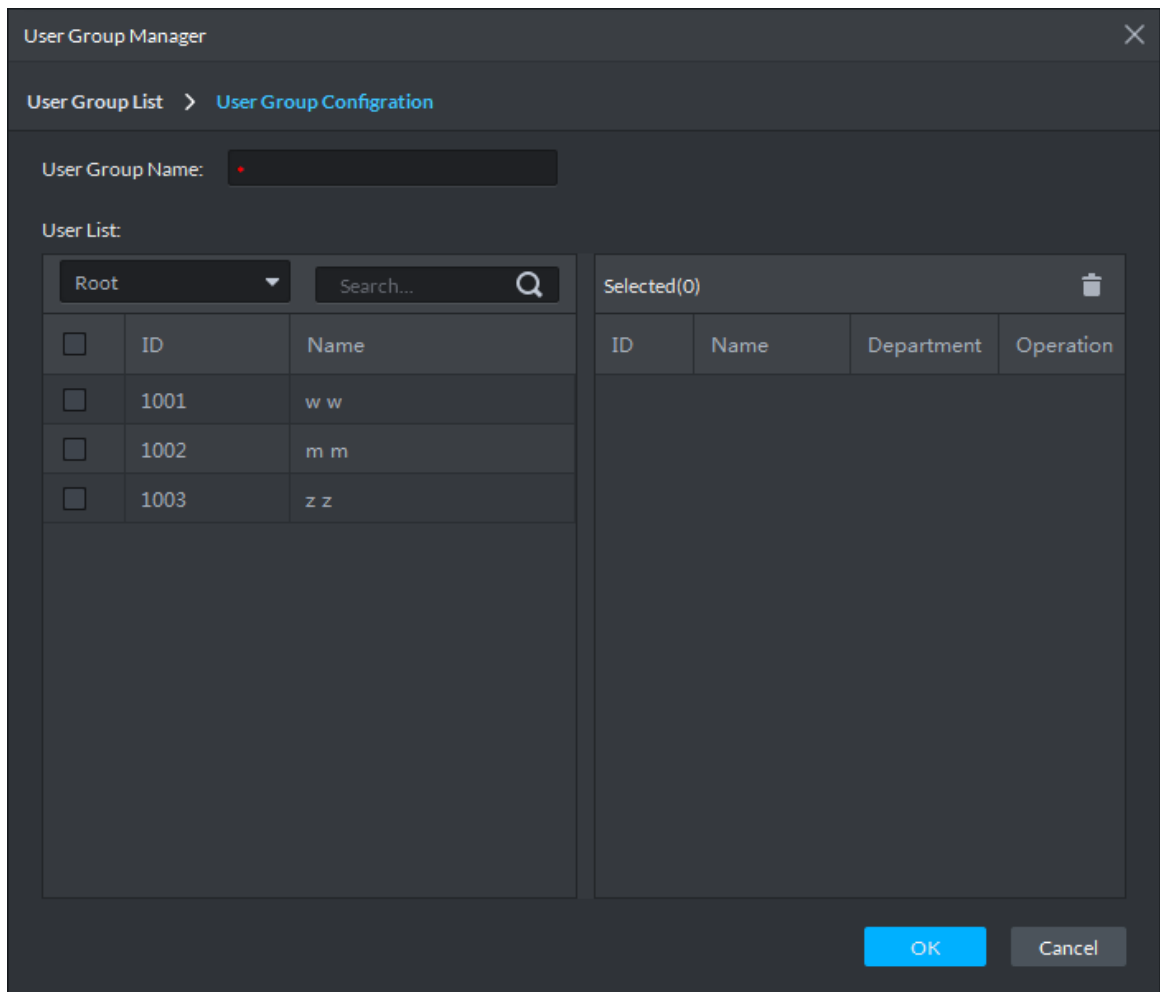
- 1) Click Person Group.

Figure 5-258 User group manager




- 2) Click **Add**.

Figure 5-259 User group config



- 3) Set up **User Group Name**. Select users from **User List** and click **OK**. You can select up to 64 users.

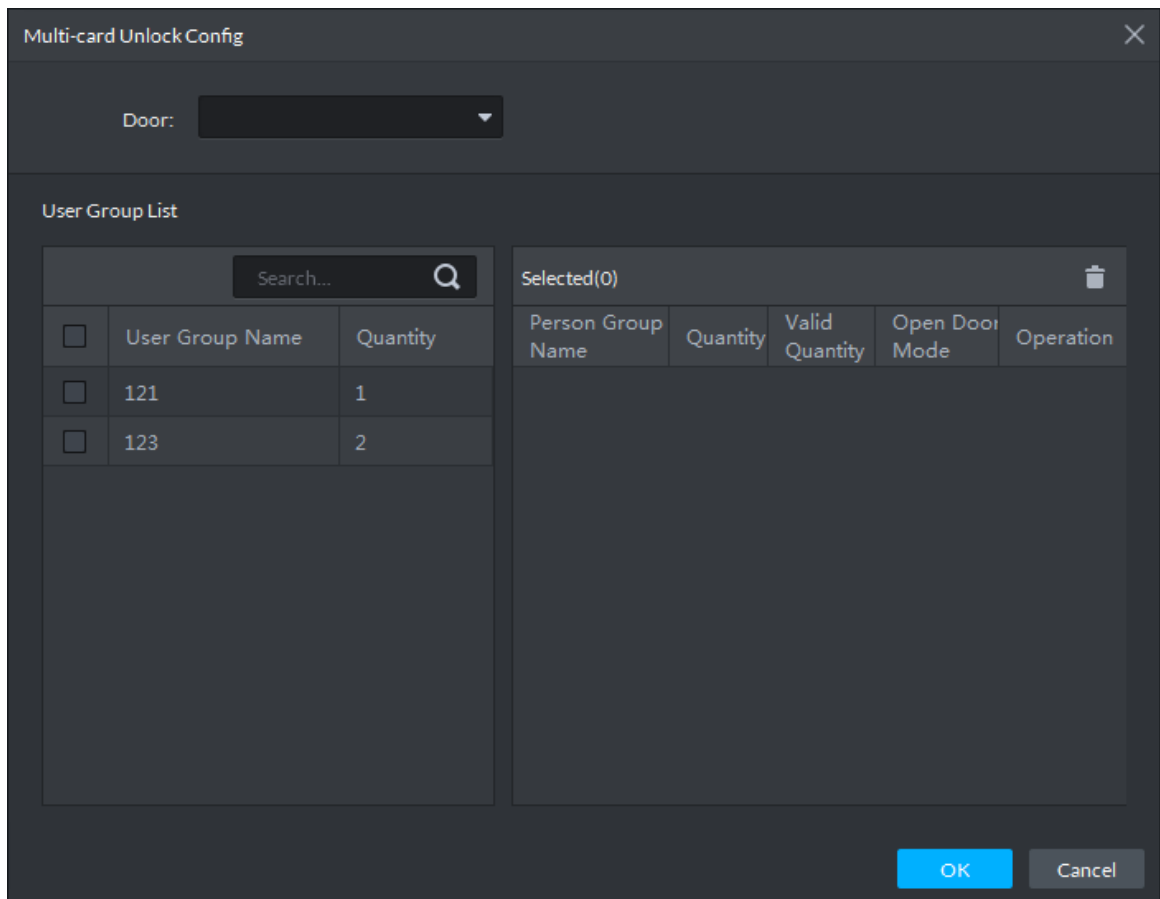
The system displays the user group information.

- 4) Click  in the upper-right corner of the **User Group Manager** interface.

Step 3 Configure Multi-Card Unlock.

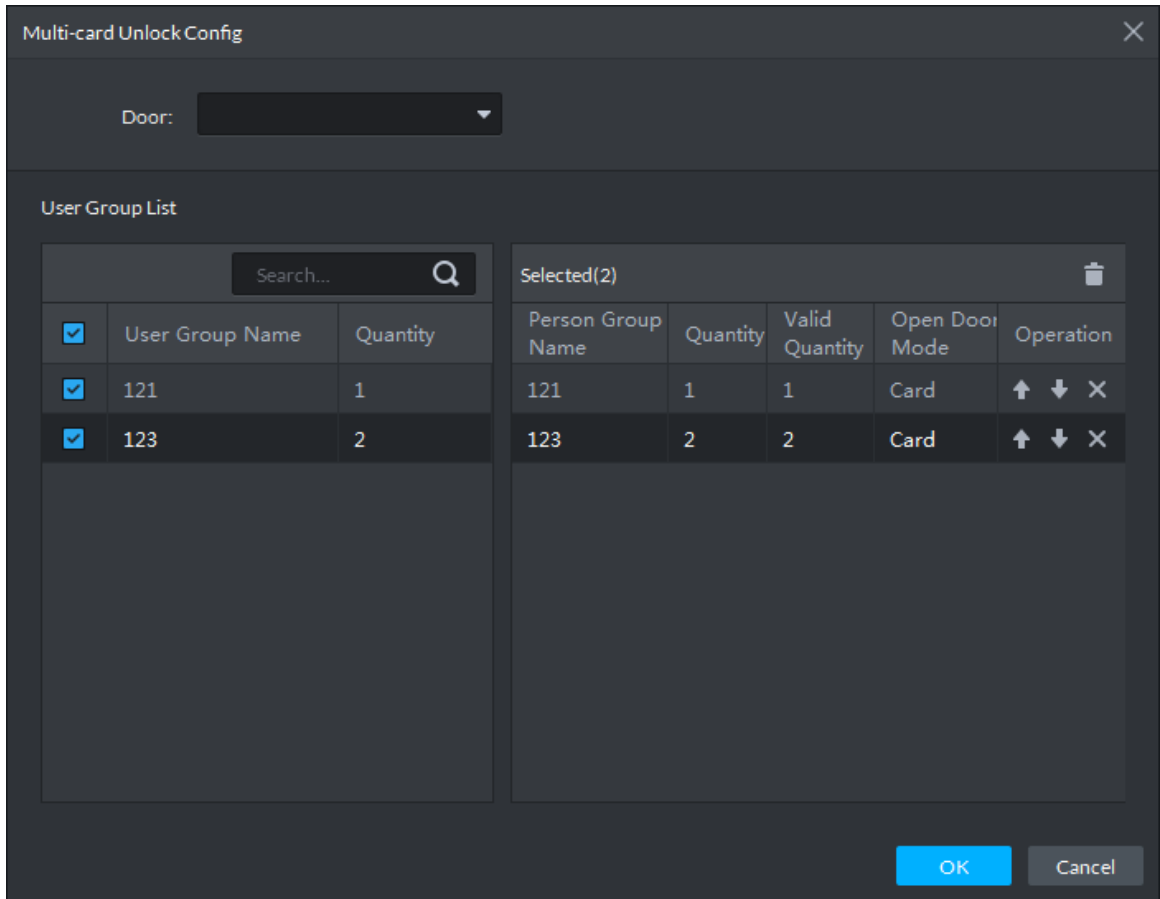
- 1) Click **Add**.

Figure 5-260 Configure user group



- 2) Select the door to set up Multi-Card Unlock.
- 3) Select the user group. You can select up to four groups.

Figure 5-261 Select user group



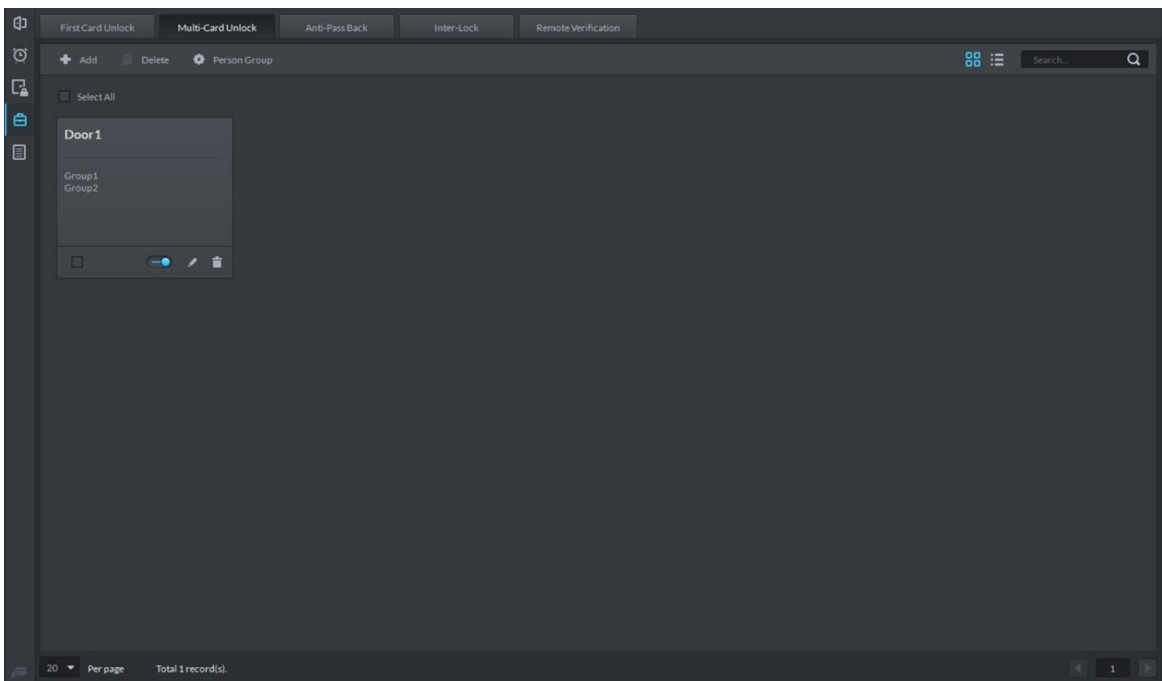
4) Fill in the **Valid Quantity** for each group to be on site and the **Open Door Mode**.

Click  or  to adjust the user sequence for each group 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.

5) Click **OK**.

Figure 5-262 Multi-card unlock



Step 4 Click .

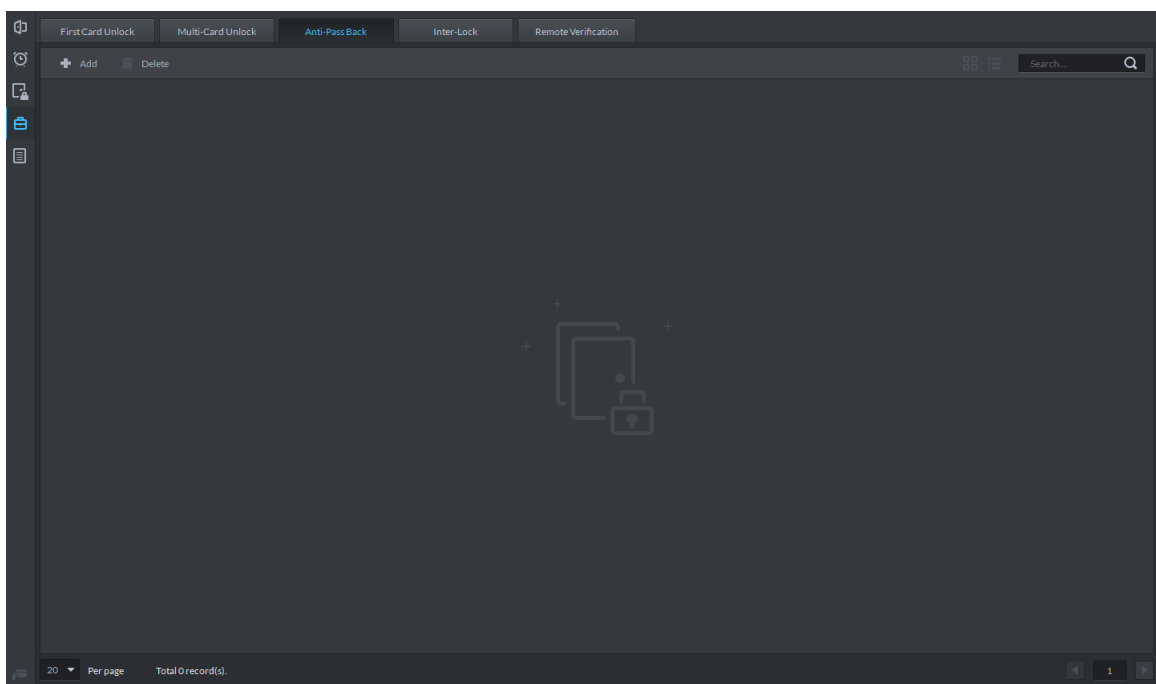
The icon changing into  indicates Multi-Card Unlock is enabled.

5.15.4.3 Anti-Pass Back

The Anti-Pass Back feature refers to that a user entering through a door group by verification must exit from the same door group by verification. One entry swipe must have a matching exit swipe. A non-verified user following a verified one to enter cannot pass the verification when taking exit; a non-verified user following a verified one to exit cannot pass verification when taking entry again. The door cannot be unlocked by swiping cards until the reset period on the A&C Central Controller expires.

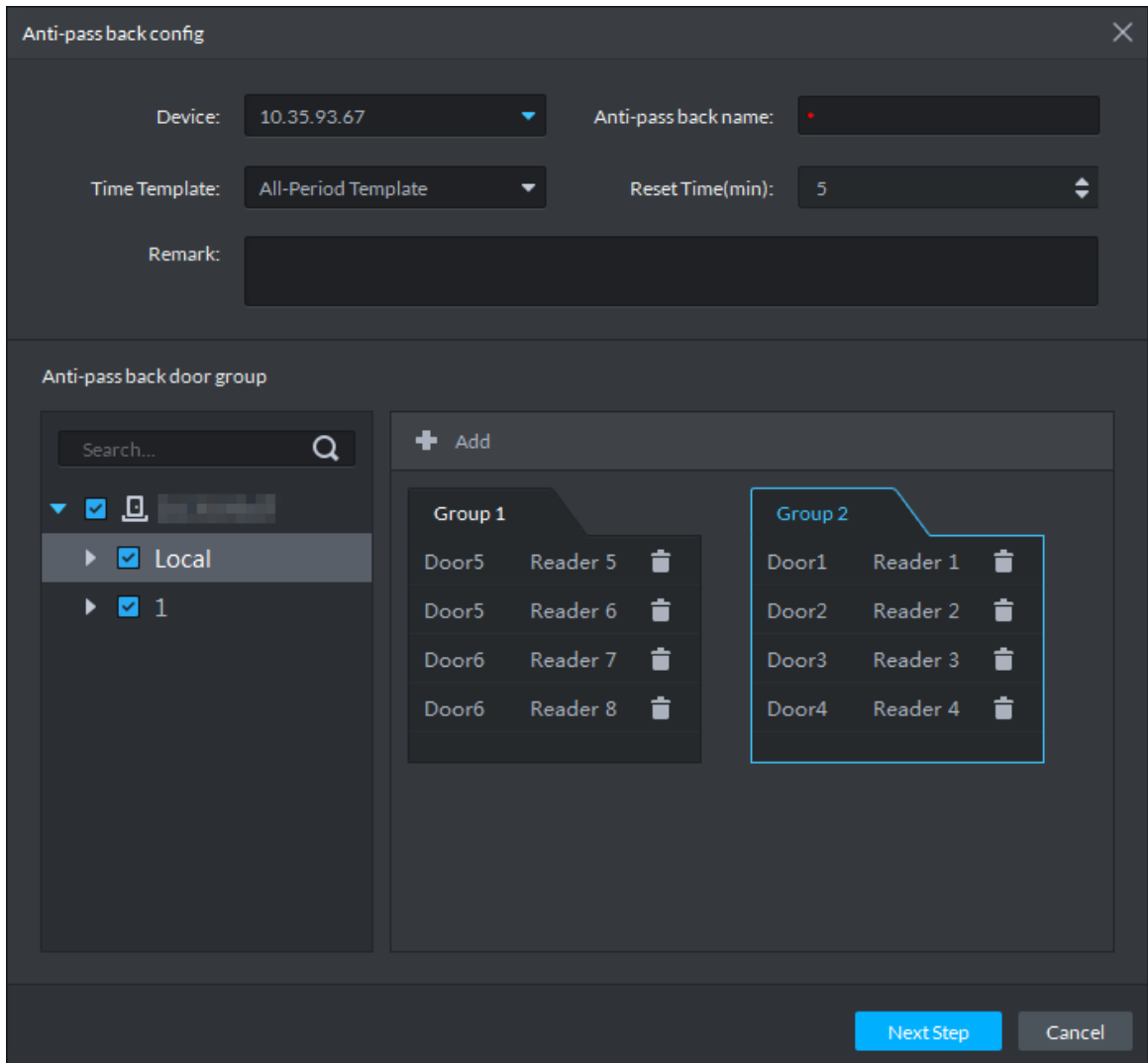
Step 1 On the **Access Control** interface, click  and select **Anti-pass Back**

Figure 5-263 Anti-pass back



Step 2 Click **Add**.

Figure 5-264 Anti-pass back config



Step 3 Configure the anti-pass back parameters and click **Next Step**.

Table 5-58 Parameters



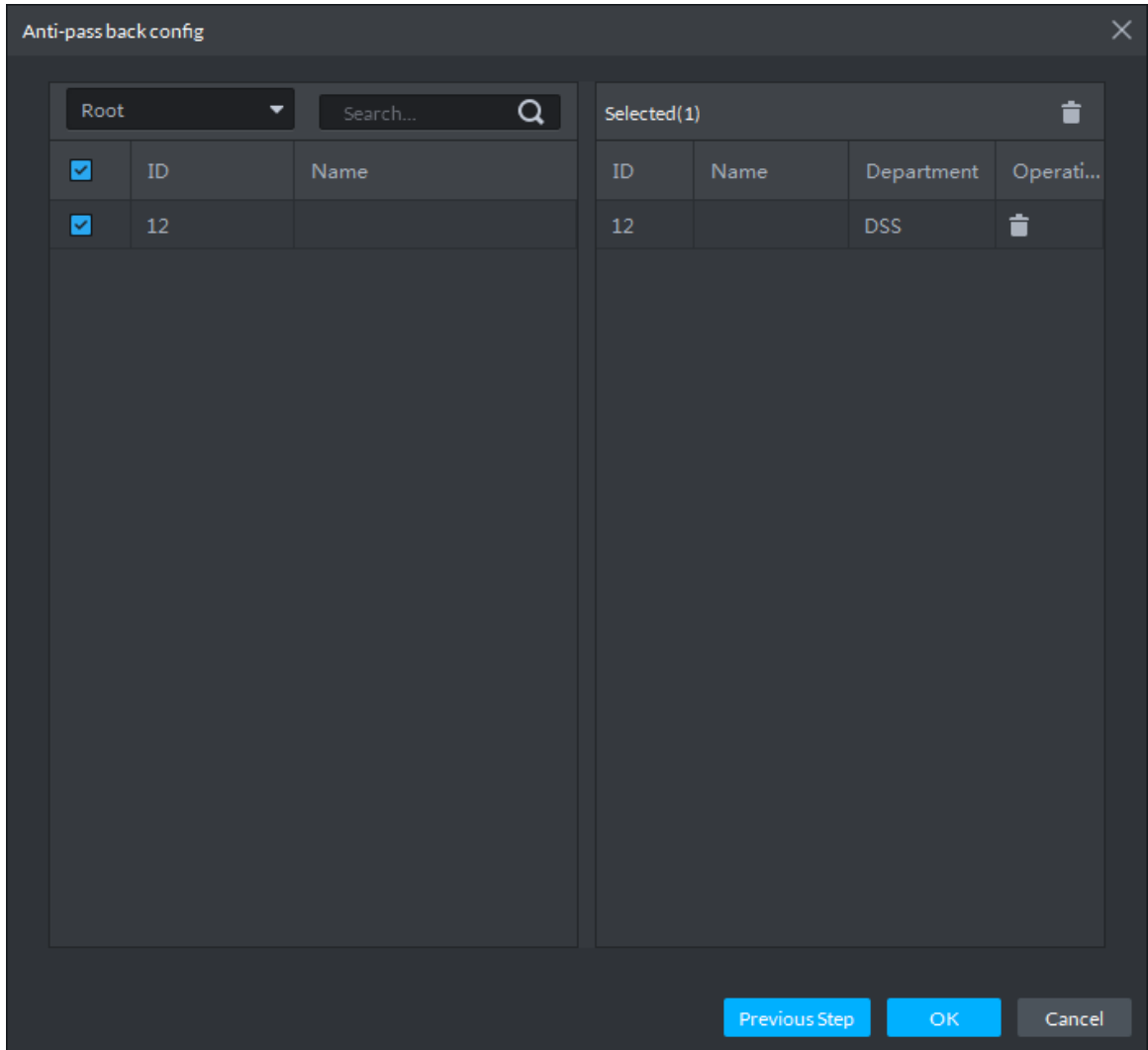
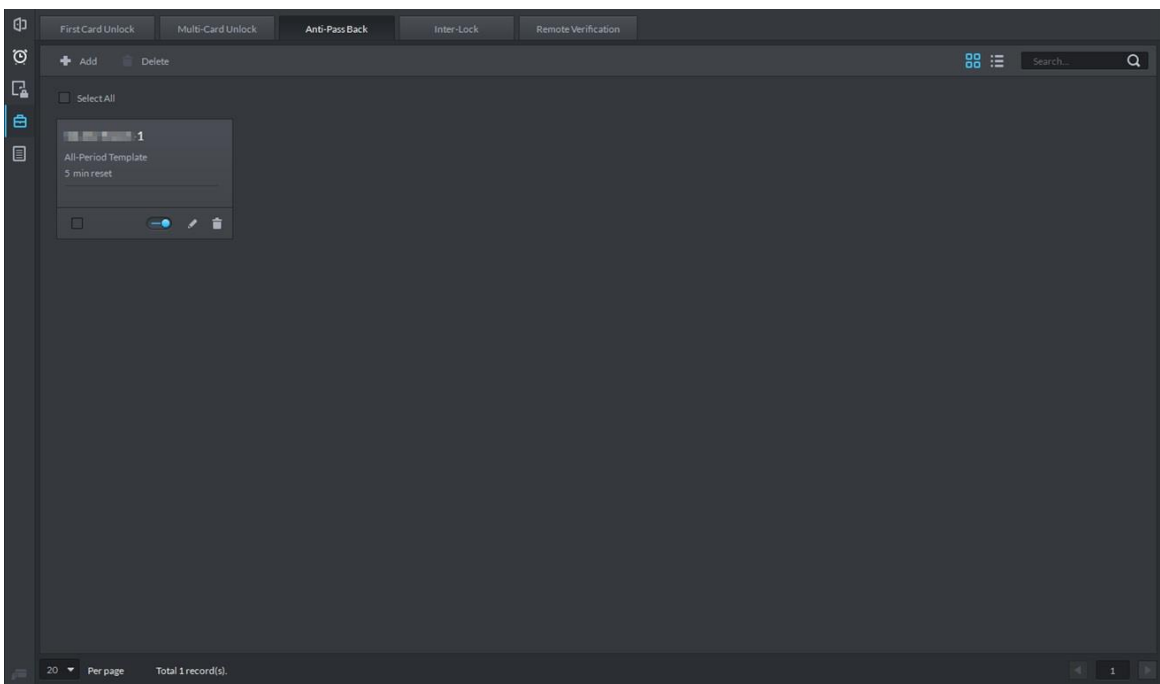
Parameter	Description	
Device	You can select the device to configure the anti-pass back rules.	
Anti-pass back name	You can customize the name of an anti-pass back rule.	
Reset Time(min)	The access card becomes invalid if an anti-pass back rule is violated. The reset time is the invalidity duration.	 When the selected device is a multi-door controller, you must set up these parameters.
Time Template	You can select the time periods to implement the anti-pass back rules.	
Remark	Note info.	
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.	

Figure 5-265 Select user




Step 4 Select users and click **OK**.

Figure 5-266 Anti-pass back



Step 5 Click .

The icon changing into  indicates Anti-Pass Back is enabled.

5.15.4.4 Inter-door Lock

The inter-door lock function varies depending on the controller types.

- Regular access controller

A regular access controller employs inter-lock within the group. When one of the access control channels is opened, other corresponding channels are closed. To open one of the access control channels (under normal access control), other corresponding access control channels must be closed; otherwise the door cannot be unlocked.

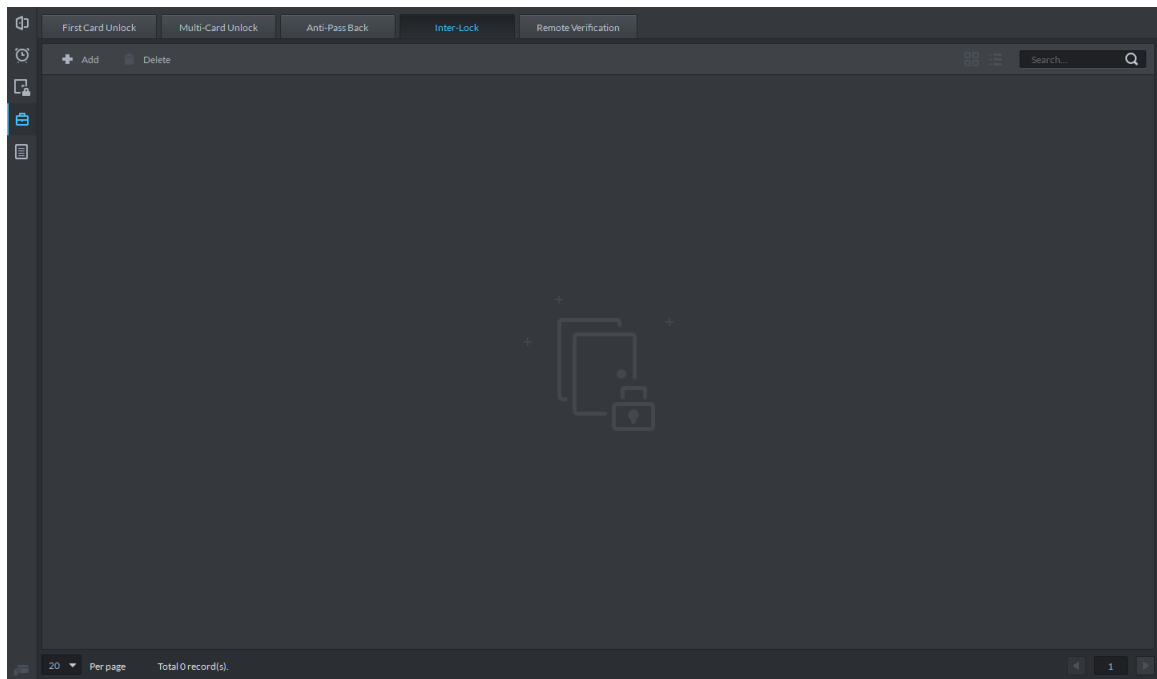
- Central controller

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.

In this section, we take A&C Central Controller as an example to illustrate the configuration procedure.

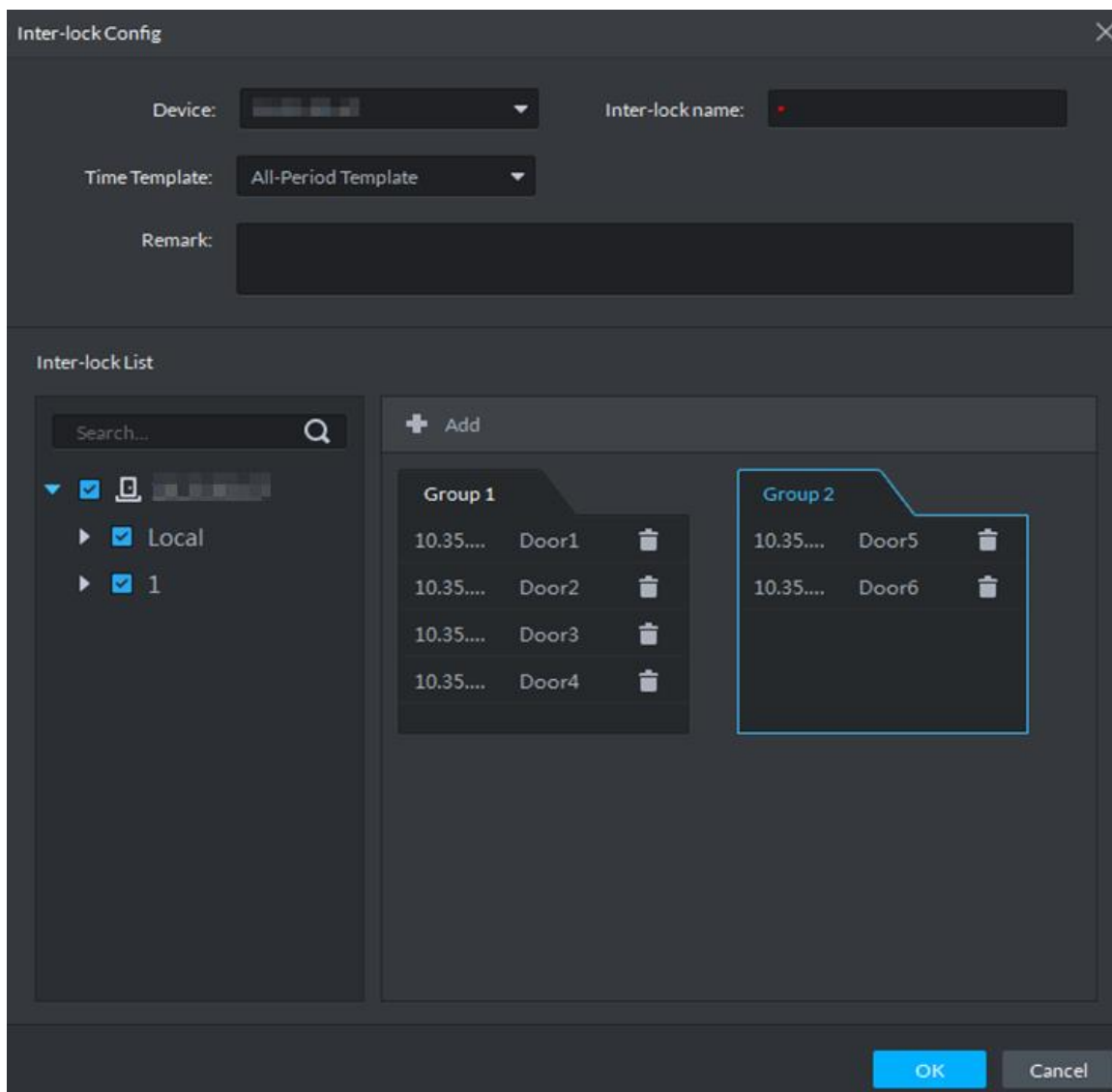
Step 1 On the **Access Control** interface, click  and select **Inter-lock**.

Figure 5-267 Inter-lock



Step 2 Click **Add**.

Figure 5-268 Inter-lock config



Step 3 Configure inter-lock parameters and click **OK**.

Table 5-59 Inter-lock config



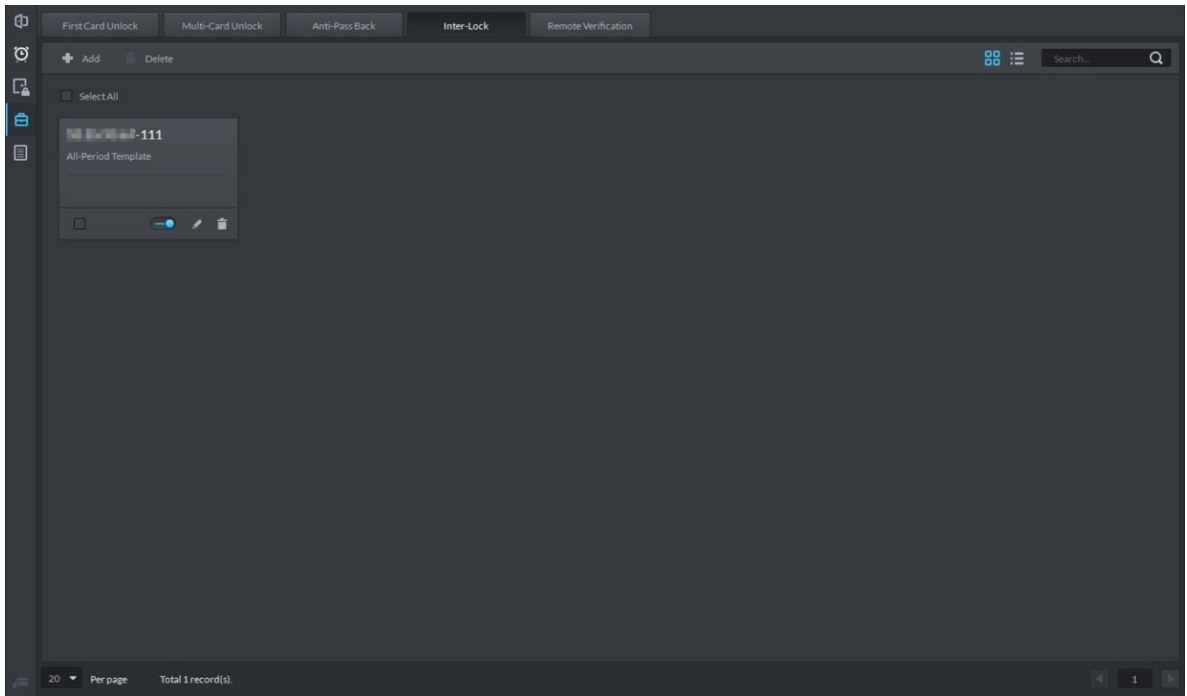

Parameter	Description	
Device	You can select the device to set up inter-lock.	
Inter-lock name	You can customize the name of the inter-lock rule.	
Time Template	You can select the time period to implement inter-lock.	 When the selected device is a multi-door controller, you must set up these parameters.
Remark	Note info.	
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 5-269 Inter-lock list



Step 4 Click .

The icon changing into  indicates Inter-Lock is enabled.

5.15.4.5 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.


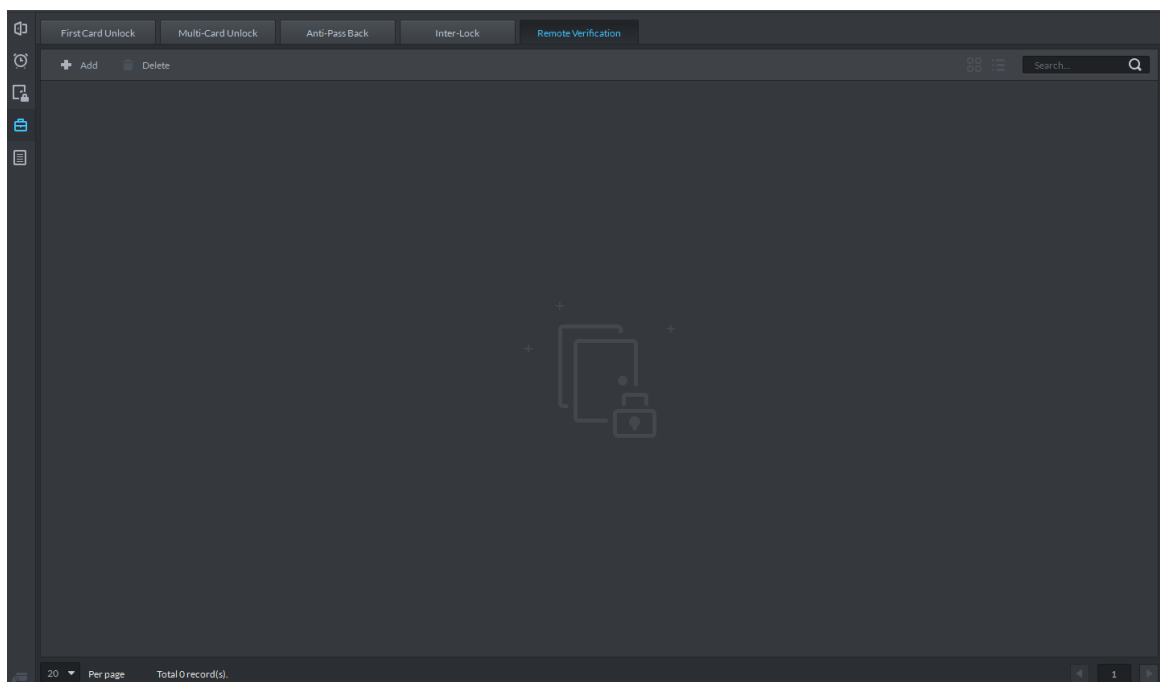
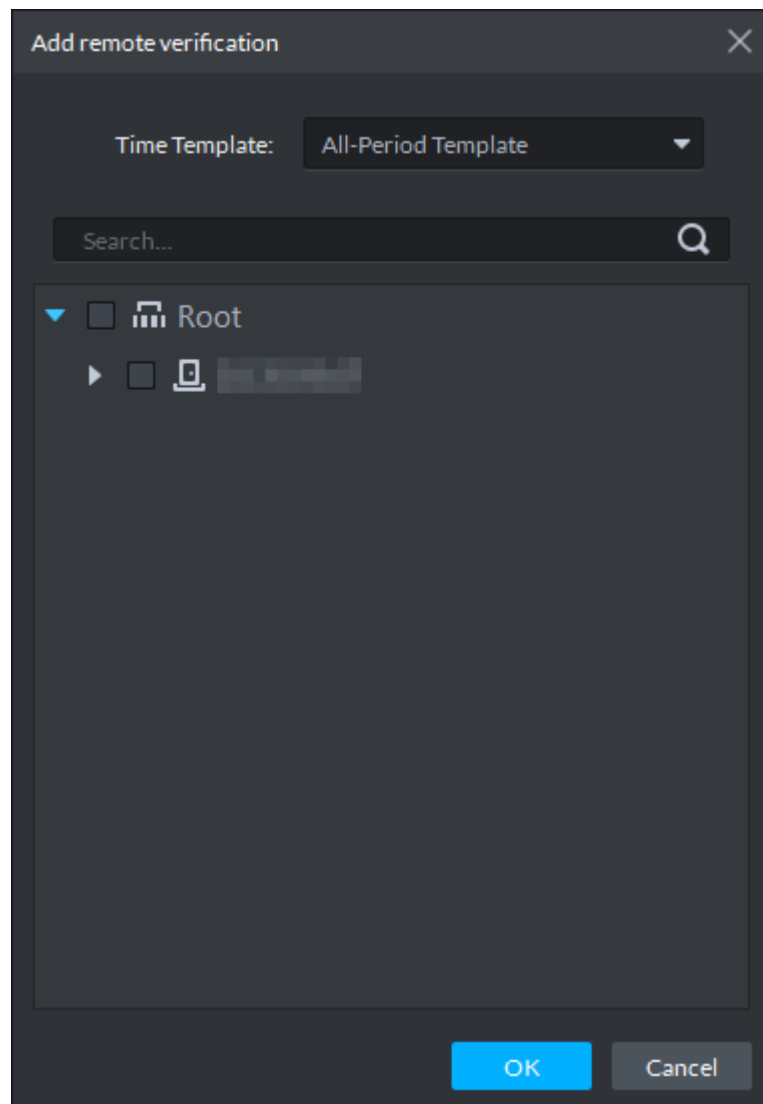
Step 1 On the **Access Control** interface, click  and select **Remote Verification**.

Figure 5-270 Remote verification



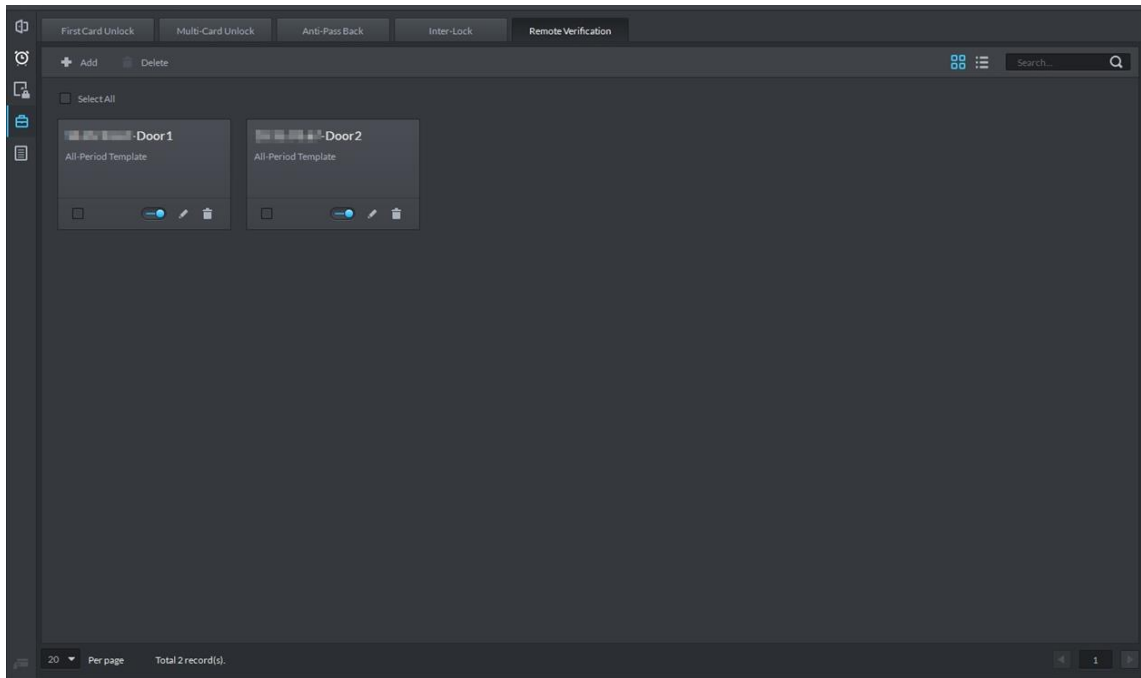
Step 2 Click **Add**.

Figure 5-271 Add remote verification



Step 3 Select **Time Template** and access control channel, and click **OK**.

Figure 5-272 Remote verification list



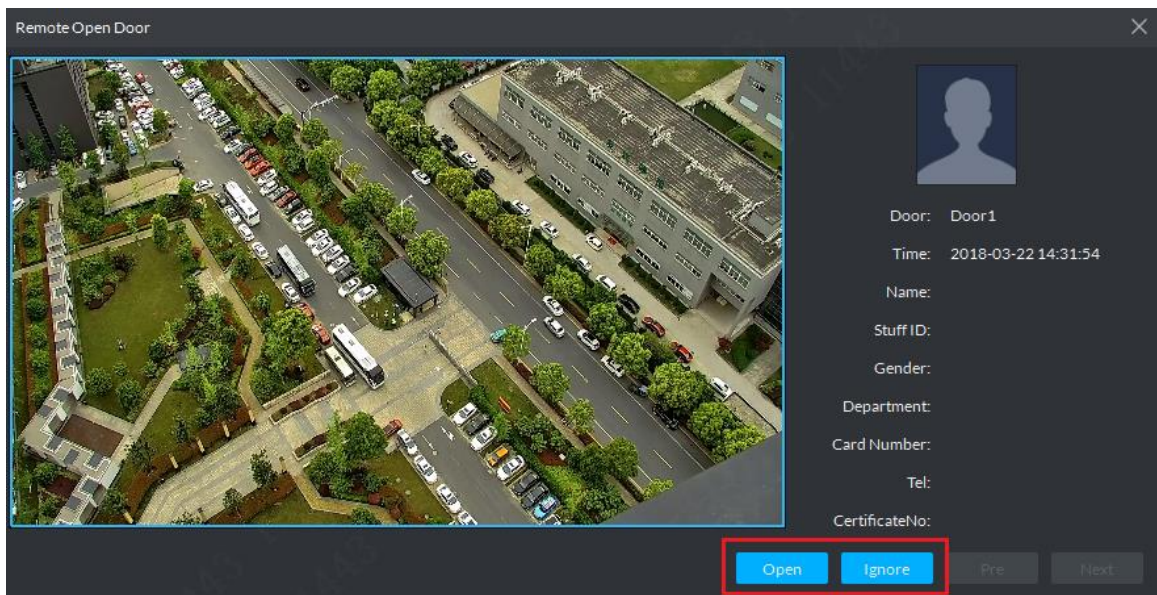
Step 4 Click .

The icon changing into  indicates First Card Unlock is enabled.

Step 5 After the setup, door unlocking by card, fingerprint, or password that takes place in the corresponding access control channel triggers a popup on the client.

Step 6 You can choose to unlock the door or ignore it by clicking the corresponding button, and the popup automatically disappears.

Figure 5-273 Remote open door



5.15.5 Setting Record Plan

Video before and after alarm can be stored only when record storage plan is configured, and the platform can play video 10 seconds before and after event alarm. If you want to set record storage plan, see "错误!未找到引用源。 错误!未找到引用源。."

5.15.6 Access Control Application

You can control lock, unlock and view related video and event info on console, and enter door config interface.

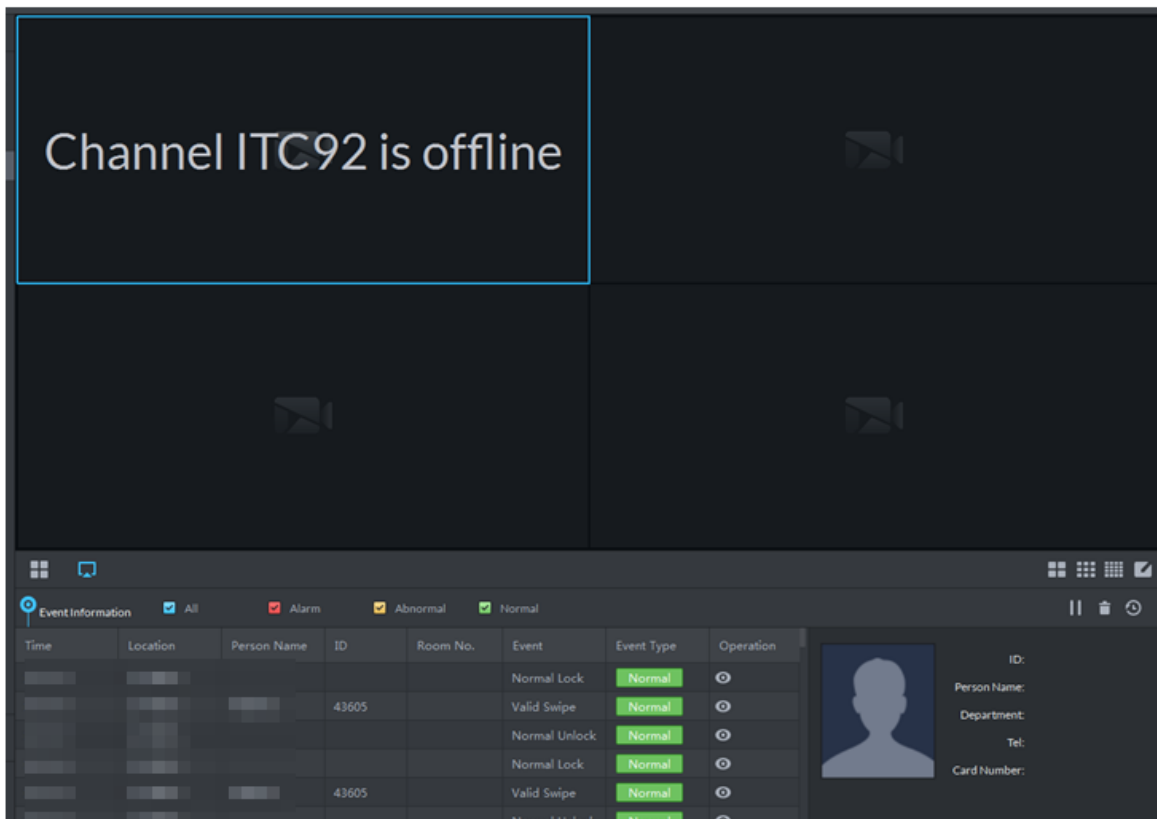
5.15.6.1 Viewing Video of Bound Channel

When adding access control devices, if you have already bound a video channel to the channel, you can view the real-time videos of the bound video channels on the console. To bind video channels, see "5.15.2 Adding Access Control."

Step 1 On client homepage, click **Access Control**.

Step 2 Click .

Figure 5-274 Console



Step 3 View related video of AC channel.



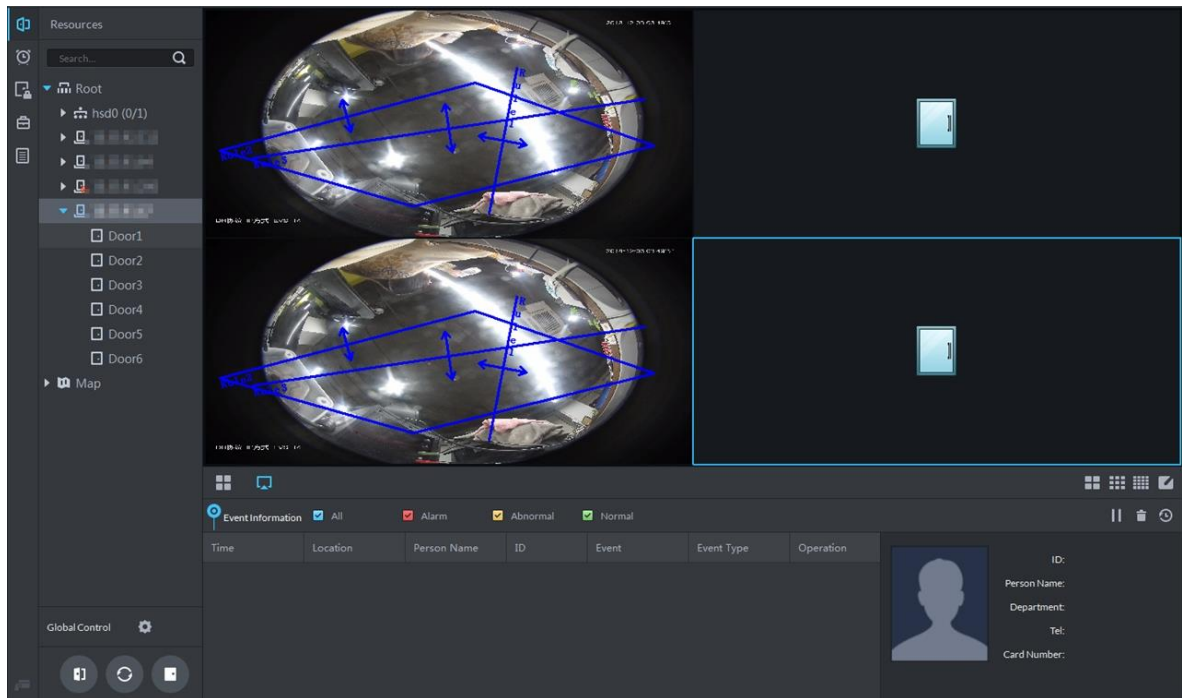
- On the right side of the console interface, click  in the access control channel list. The system displays videos in real time.
- Click  on the console interface. The system displays the video interface. Drag the access control channel on the left side of the screen to the live view interface on the right side.

Figure 5-275 Linked channel video



5.15.6.2 Manual Unlock

In addition to the open-door methods of Always Open and linked unlock, the console also supports manually opening door by operating the access control channel. After being unlocked, the door automatically locks up after a specified time period (5s by default, and 10s in this example) as preset.

Step 1 On the **Homepage** interface, click **Access Control**.


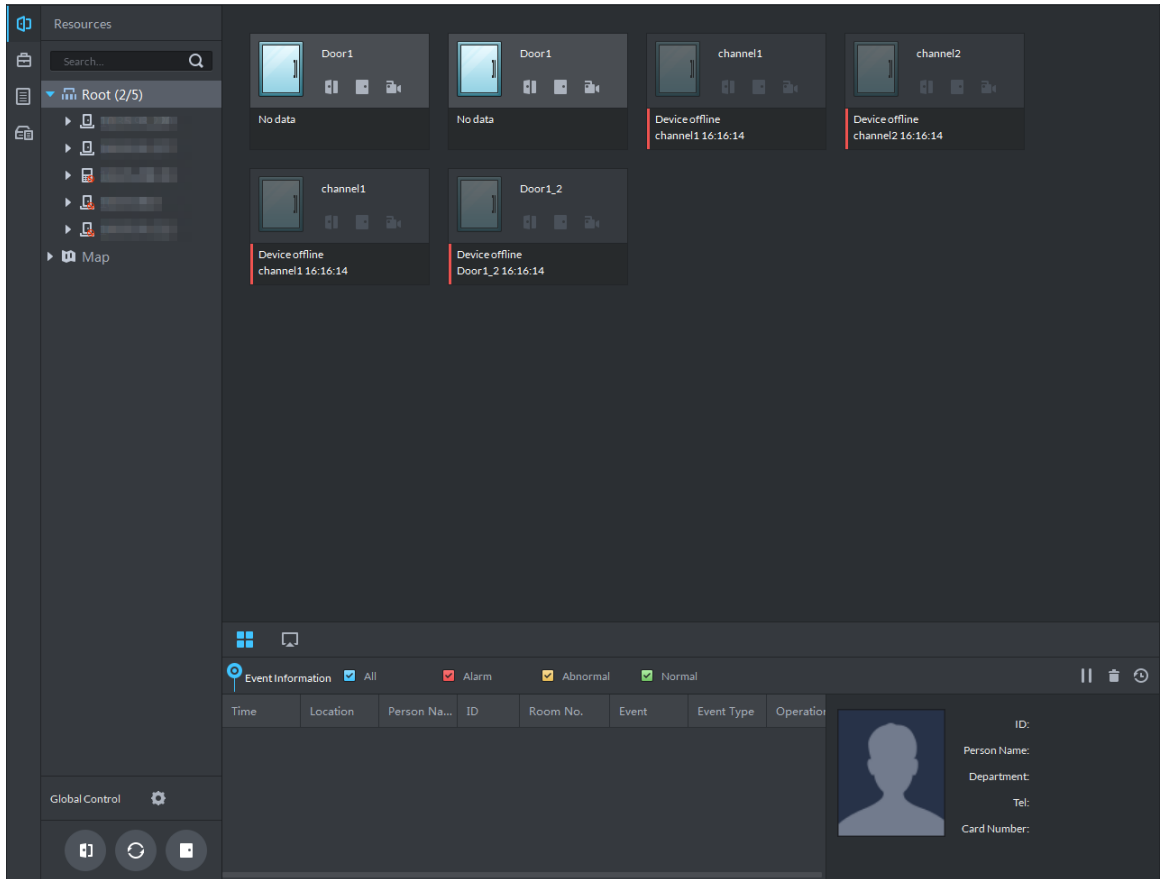
Step 2 Click .

Figure 5-276 Console



Step 3 Manual unlock.

- 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


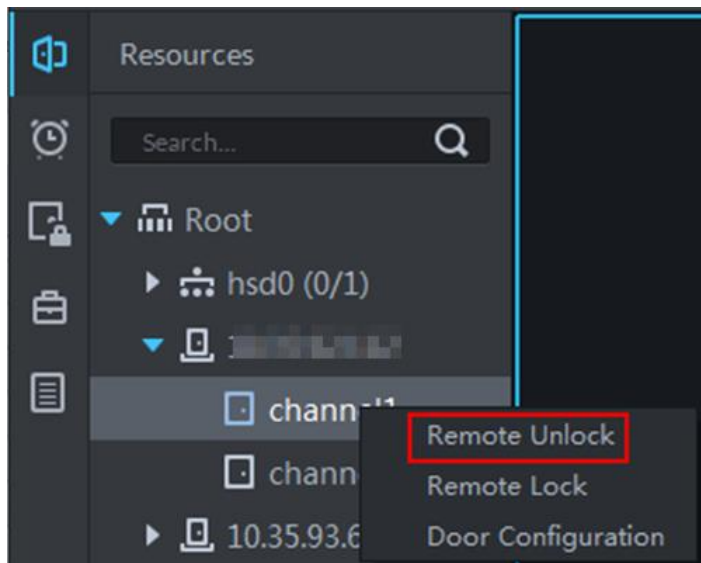
to open, as .

Figure 5-277 Remote unlock (1)





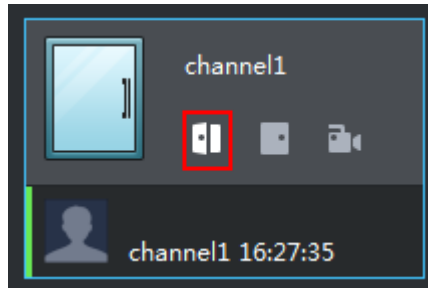
- Click  on the door channel interface to unlock the door. After unlocking, the door status in the access control channel list on the right side of the interface changes to open, as .

Figure 5-278 Unlock (2)




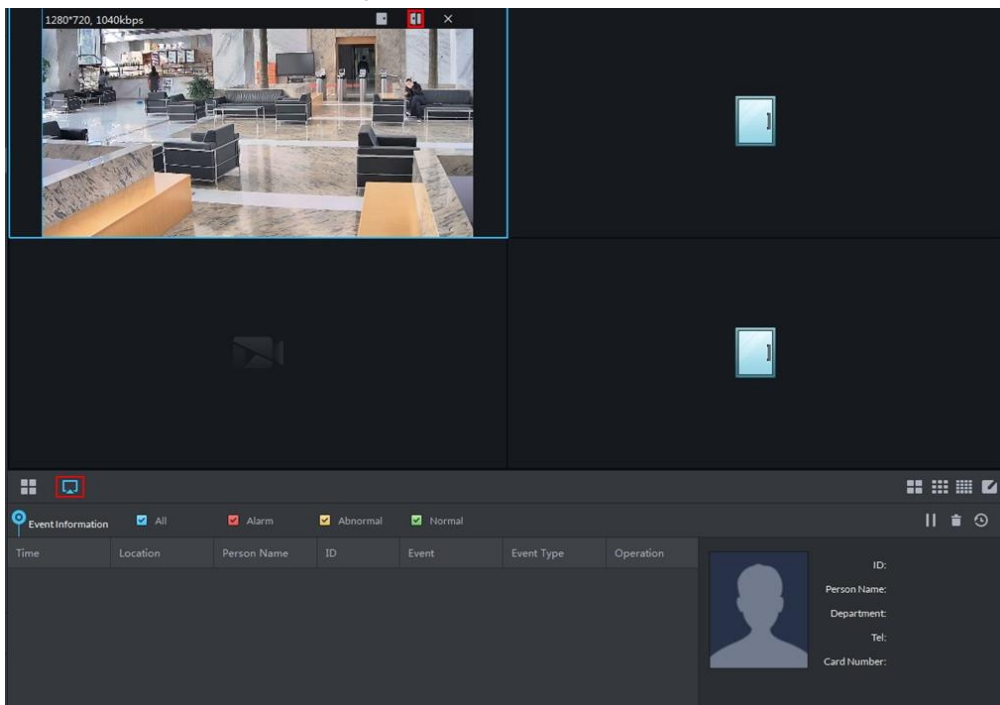
- When viewing videos bound to the channel, click  on the video interface to unlock the door.

Figure 5-279 Unlock(3)




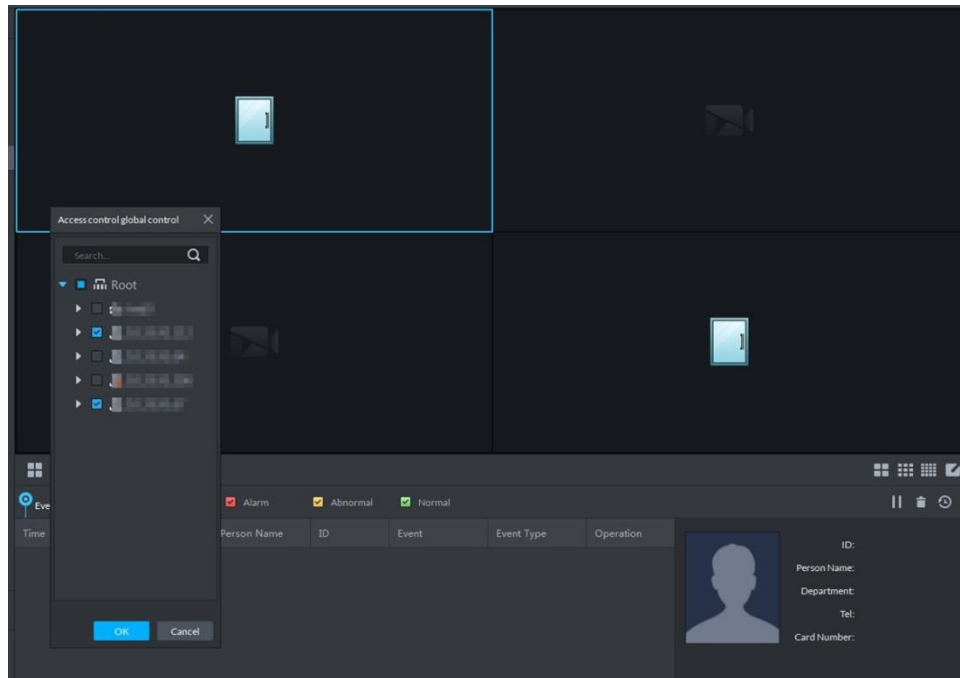

- Temporary Always Open of multiple doors
Select a door channel through global control and you can set the door to be Always Open. Recovery to normal status after unlocking requires manual operations.
- Click  on the bottom left of the console interface of the Access Control module.

Figure 5-280 Global control



- 2) Select an access control channel to be set to Always Open via global control, and click **OK**.
- 3) Click **Always Open** on the bottom left of the interface.
- 4) Enter current user's password, and click **OK**.

All the doors of the selected access control channels are set to Always Open. The status of all the doors in the access control channel list on the right side of the

interface changes to open, as . The interface control changes from **Always Open** to **Recover**.



Click **Recover** and the doors return to normal status.

5.15.6.3 Manual Lock

In addition to the close-door methods of Always Close or linked lock, the console also supports locking by manually controlling the access control channel.

Step 1 On the **Homepage** interface, click **Access Control**.

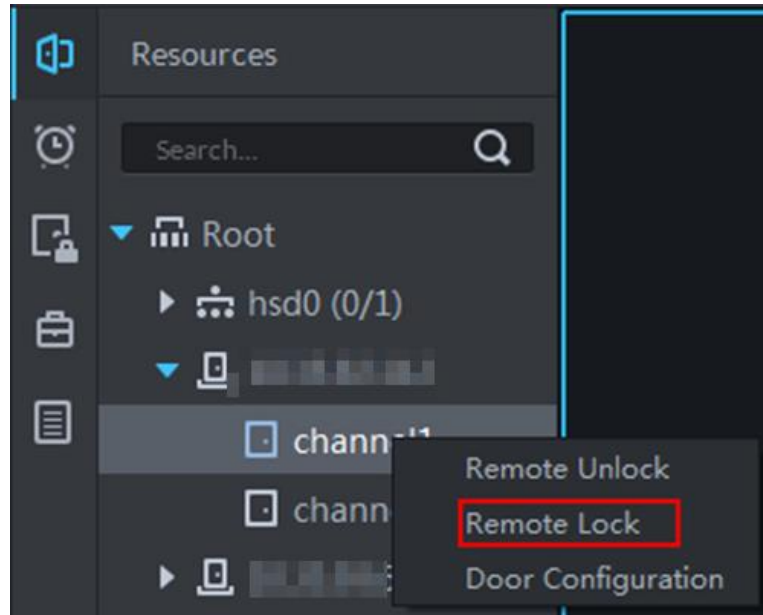
Step 2 Click .

Step 3 Manually lock door

- 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 5-281 Lock (1)





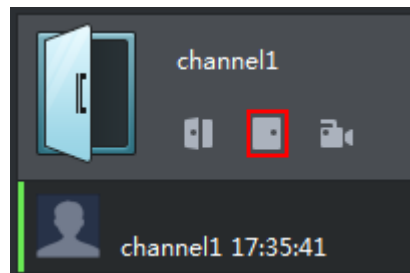
- Click  on the door channel interface to lock the door. After locking, the door status in the access control channel list on the right side of the interface changes to closed, as .

Figure 5-282 Lock (2)




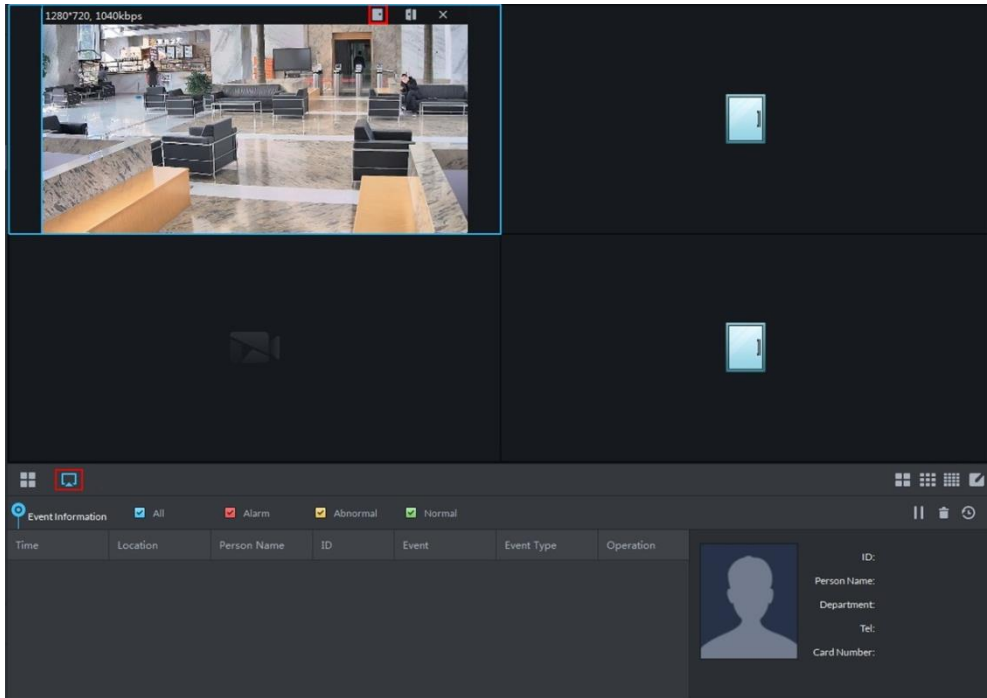
- When viewing videos bound to the channel, click  on the video screen to lock the door.

Figure 5-283 Lock (3)




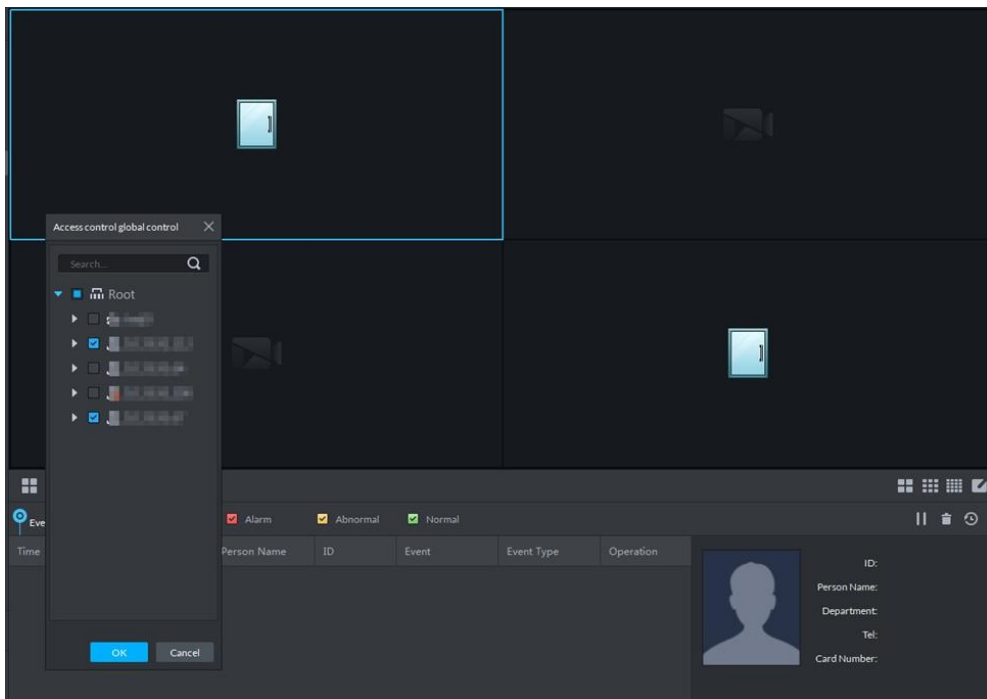
- Temporary Always Open of multiple doors
Select a door channel through global control and you can set the door to be Always Close. Recovery to normal status after locking requires manual operations.
- 1) Click  on the bottom left of the console interface of the Access Control module.

Figure 5-284 Global control



- 2) Select an access control channel to be set to Always Close via global control, and click **OK**.
- 3) Click **Always Close** on the bottom left of the interface.
- 4) Enter current user's password, and click **OK**.

All the doors of the selected access control channels are set to **Always Close**. The status of all the doors in the access control channel list on the right side of the

interface changes to closed, as . The interface control changes from **Always Close** to **Recover**.



Click **Recover** and the doors return to normal status.

5.15.6.4 Viewing Event Details

Supports viewing 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 Bind Resources.
- When snapshot and video recording require configuring event management, access control-related alarm devices are linked with the camera.
- The console displays all event information except for locking related info, including unlock, duress unlock, and invalid swipe.

Step 1 On the **Homepage** interface, click **Access Control**.

Step 2 Click .


Step 3 In the event list below the console interface, click  next to the event records.

Figure 5-285 Event details

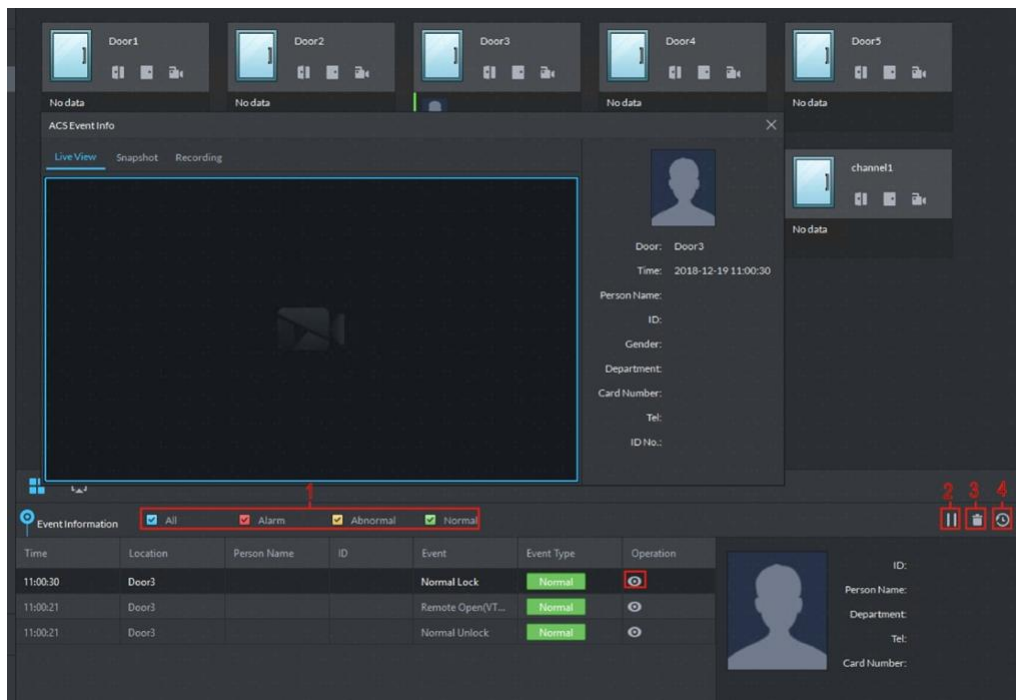






Table 5-60 Operation description

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.

No.	Description
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	Clearing the events from the current event list, does not delete them from the log.
4	Click to jump to the A&C Log interface.

Step 4 Click the corresponding tab to view the live view, snapshots, and video recordings of the linked video channel.

5.15.6.5 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 had not been added to the platform or were disconnected from the platform. After the device is added to the platform or gets reconnected to the platform, the platform will read the records generated when the device was offline.

5.15.6.5.1 Online Records

Step 1 Go to the records interface.

Two ways to go to the records interface.




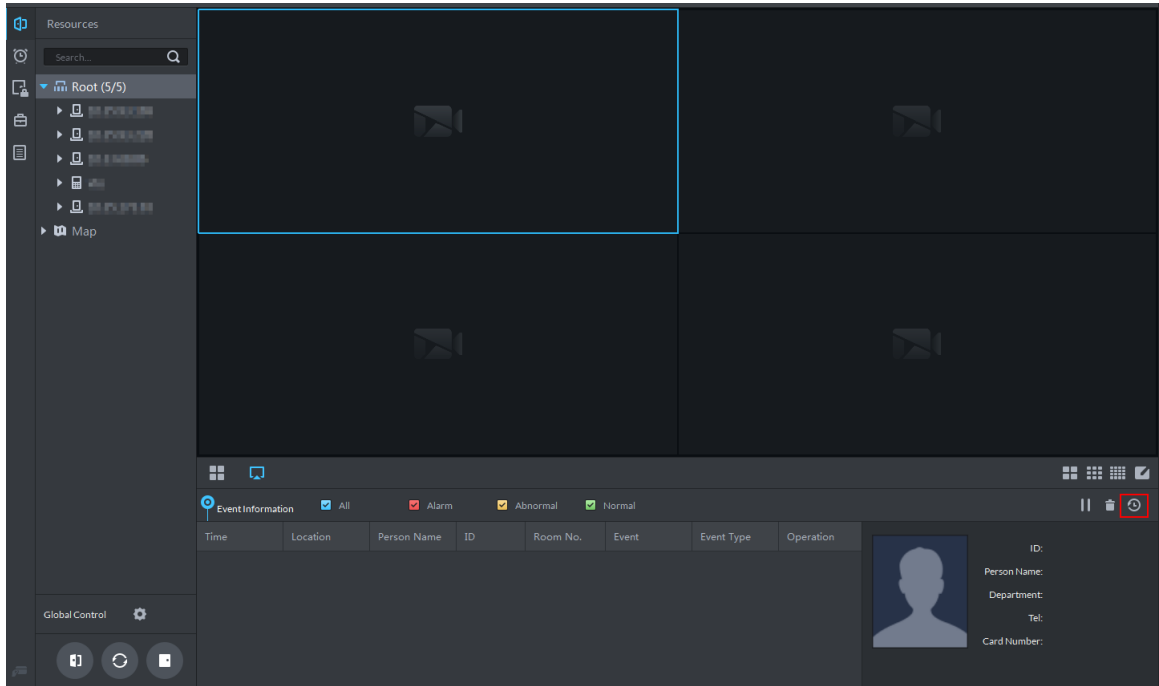
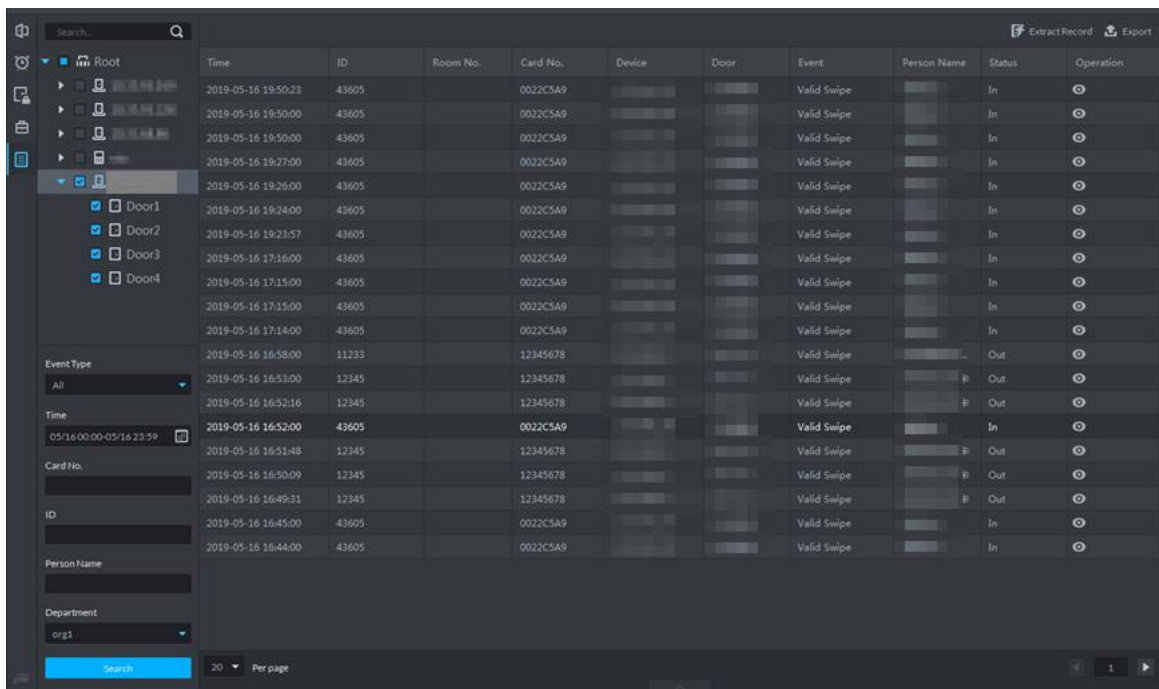
- On **Access Control** interface, click .
- On **Access Control** interface, click , and then click .

Figure 5-286 Go to the records interface



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

Figure 5-287 Search AC log



5.15.6.5.2 Offline Records

Step 1 On **Access Control** interface, click .

The **Access Control Records** interface is displayed.

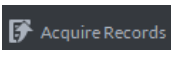
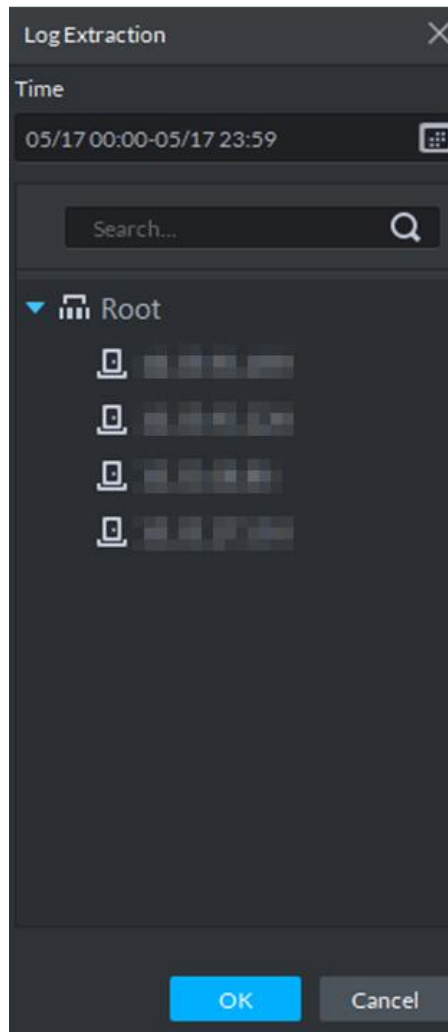
Step 2 Click  **Acquire Records** at the upper-right corner.

Figure 5-288 Extract logs during device offline



Step 3 Click  and set period.

Step 4 Click  to display devices, and then select a channel.

Step 5 Click **OK**.

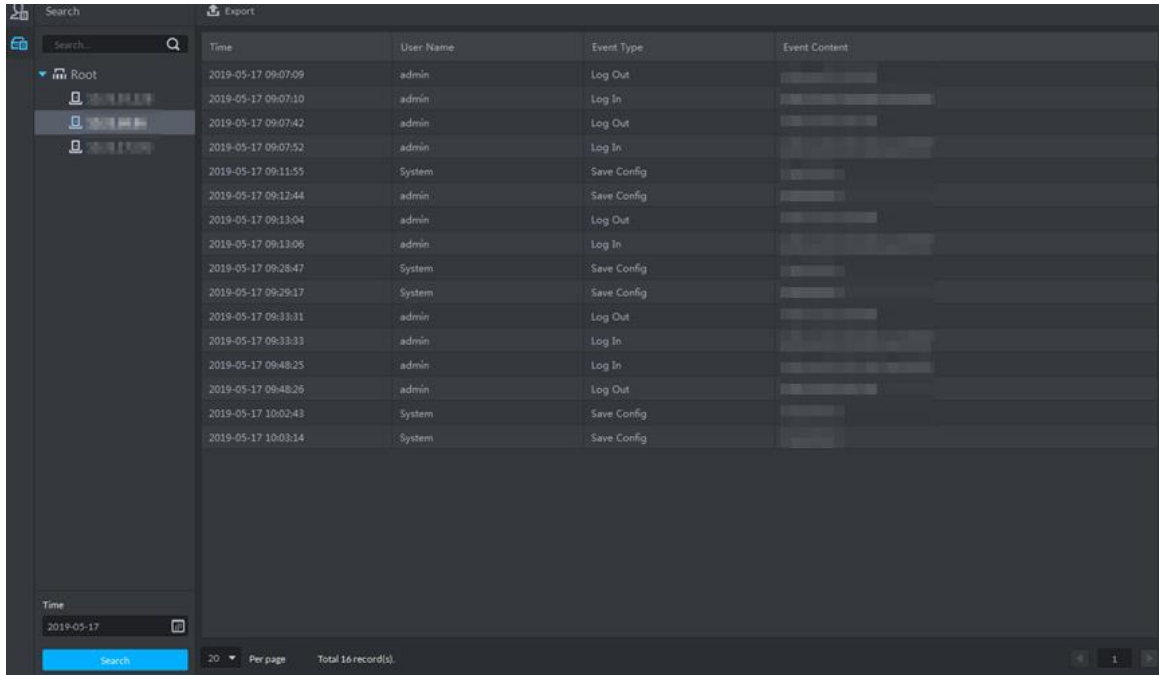
The records are displayed.

5.15.6.6 Viewing Device Logs

View logs of access control devices, such as login and logout logs.

Step 1 On the **Access Control** interface, click .

Figure 5-289 Device log



Time	User Name	Event Type	Event Content
2019-05-17 09:07:09	admin	Log Out	
2019-05-17 09:07:10	admin	Log In	
2019-05-17 09:07:42	admin	Log Out	
2019-05-17 09:07:52	admin	Log In	
2019-05-17 09:11:55	System	Save Config	
2019-05-17 09:12:44	admin	Save Config	
2019-05-17 09:13:04	admin	Log Out	
2019-05-17 09:13:06	admin	Log In	
2019-05-17 09:28:47	System	Save Config	
2019-05-17 09:29:17	System	Save Config	
2019-05-17 09:33:31	admin	Log Out	
2019-05-17 09:33:33	admin	Log In	
2019-05-17 09:48:25	admin	Log In	
2019-05-17 09:48:26	admin	Log Out	
2019-05-17 10:02:43	System	Save Config	
2019-05-17 10:03:14	System	Save Config	

Step 2 Select a device and time, and then click **Search**.
The search results are displayed.

5.15.7 Device Maintenance

Support updating or restarting access control devices by platform. Skip this section if you do not need to update or restart devices.

5.15.7.1 Updating Devices

You can update AC device remotely by platform. Before update, please make sure you have acquired AC device program, otherwise, please contact technical support for the program.

Step 1 On client homepage, click **Config**.

Step 2 In left device tree, select AC device, and then click **Device Update**.

The system displays **Device Update** interface, and version info of AC device.

Figure 5-290 Enter device update interface

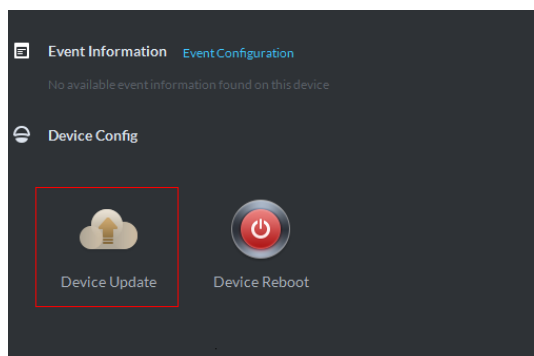
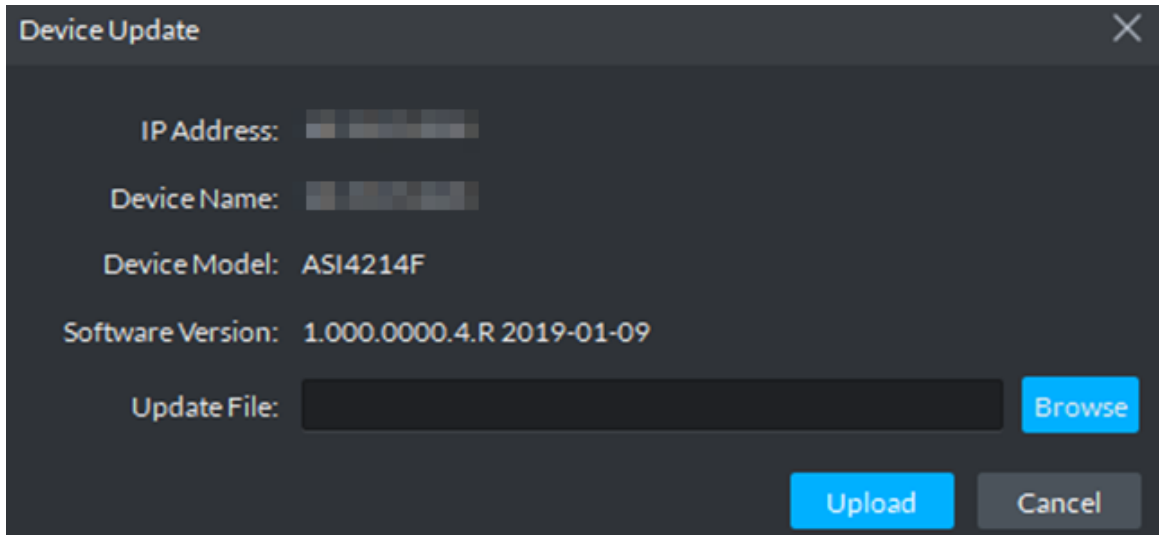


Figure 5-291 Device update



Step 3 Click **Browse** and select update file.

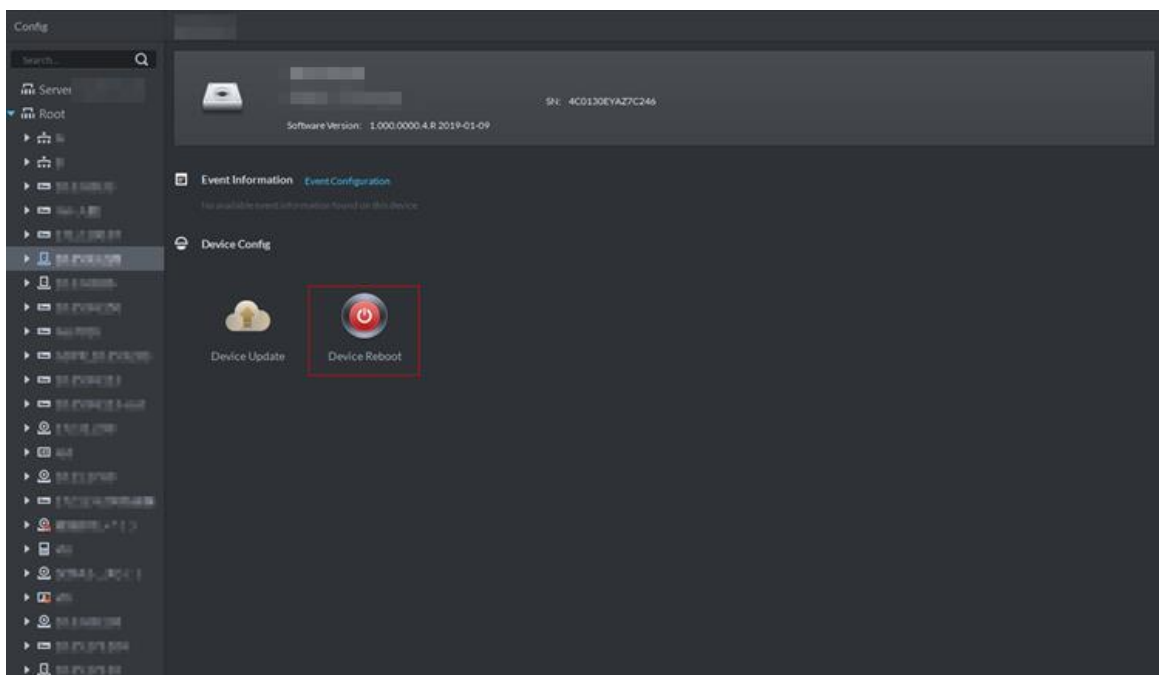
Step 4 Click **Upload** and update device.

5.15.7.2 Restarting Devices

Step 1 On client homepage, click **Config**.

Step 2 In left device tree, select a device, and then click **Device Reboot**.

Figure 5-292 Enter device reboot



Step 3 Click **Yes** and restart device.

5.15.7.3 Synchronizing Device Time

Synchronize device time to make it consistent with the platform time.

Step 1 On the **Homepage** interface, click **Config**.

Step 2 In the device tree, select an access control device, and then click **Time Setting**.

Figure 5-293 Go to the time setting interface

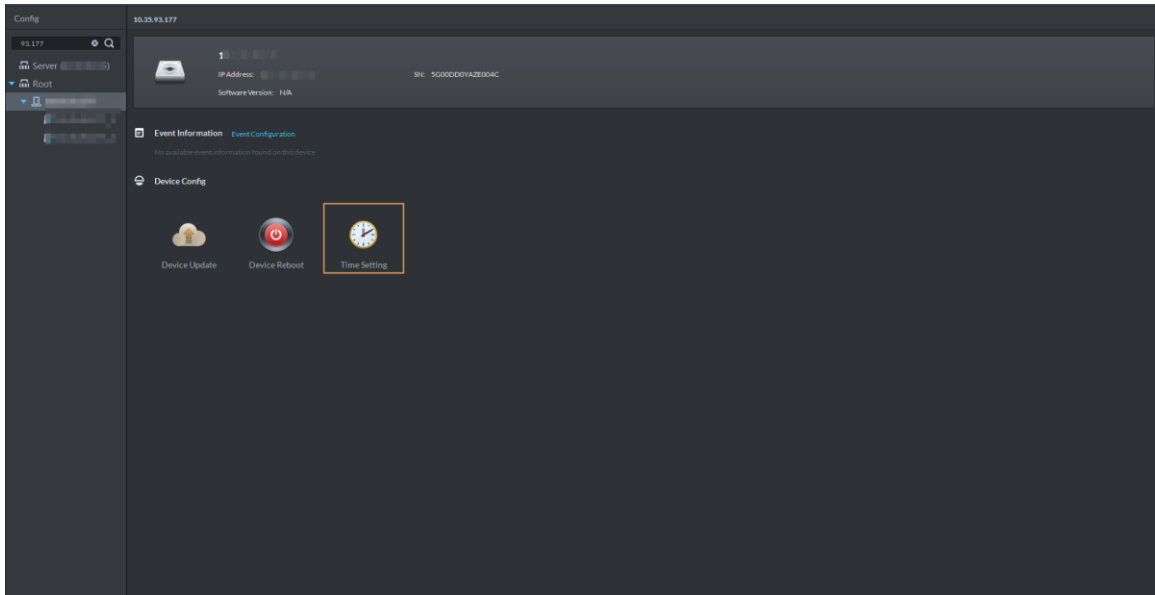
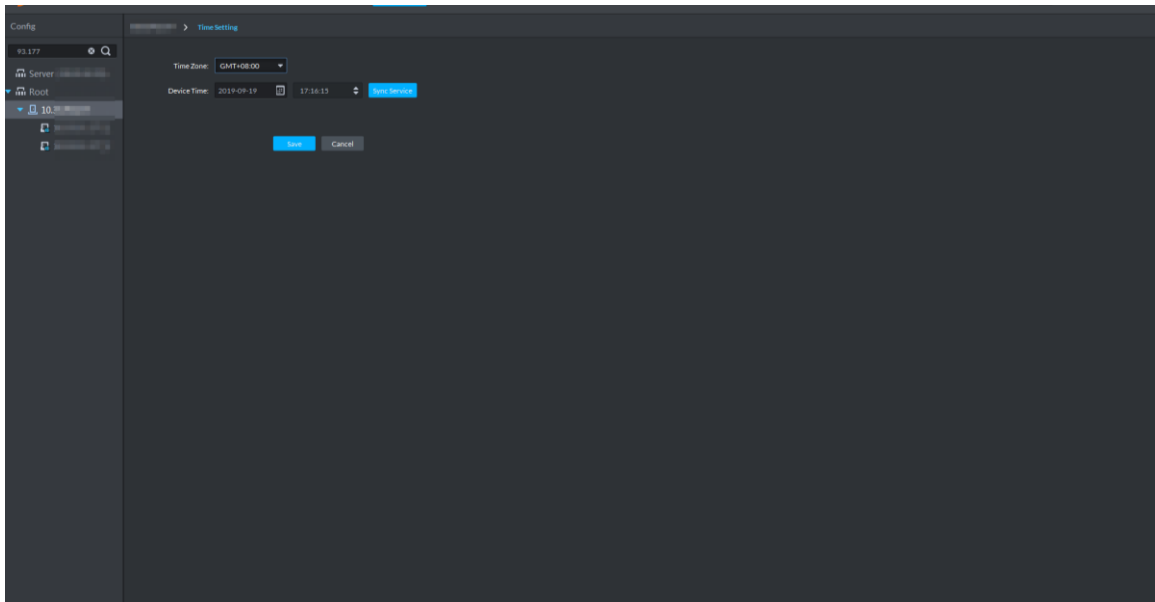


Figure 5-294 Time setting



Step 3 Click **Sync Service**.

Step 4 Click **Save**.

The platform starts synchronizing device time.

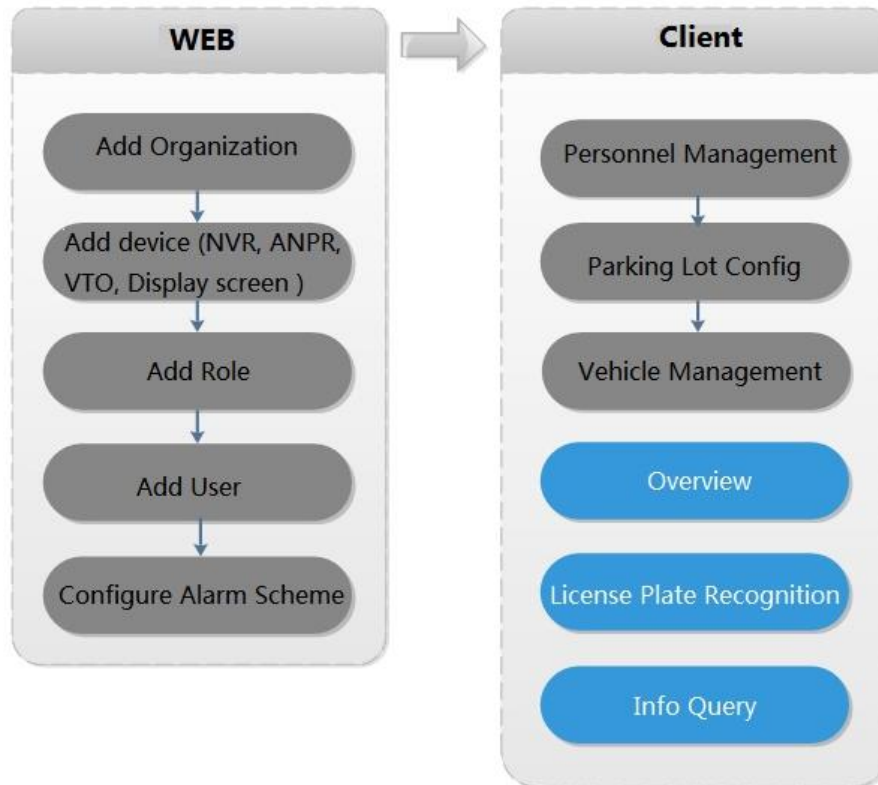
Step 5 Click **Cancel** to exit the time setting interface.

5.16 Entrance

Integrate entrance module, realize entrance and exit recognition barrier unlock, remaining parking space information display, blacklist vehicle alarm, message search and other functions. When it fails to recognize vehicle by entrance, then it can unlock by VTO password, swipe card to unlock, fingerprint unlock and unlock by face recognition to open barrier. The supported VTO unlock mode is based on the performance of accessed VTO.

5.16.1 Preparations

Figure 5-295 ANPR business flow



5.16.2 Adding Device



If users want to use the new device, it needs to select **User Management > User** on WEB, enter **User** interface, and edit user to make him or her have access to device, otherwise the device cannot be used.

5.16.2.1 Adding ANPR Camera

ANPR device is used to recognize license plate and vehicle information.



- Please make sure ANPR device is fully configured before adding, for example, complete initialization config, and modify IP etc.
- The device category is **ANPR Device**.

Step 1 Add encoder ANPR. For more details, refer to "4.5 Adding Device."
Modify device type.

- 1) On the **Device** interface, click  of added ANPR device.

Figure 5-296 Device interface

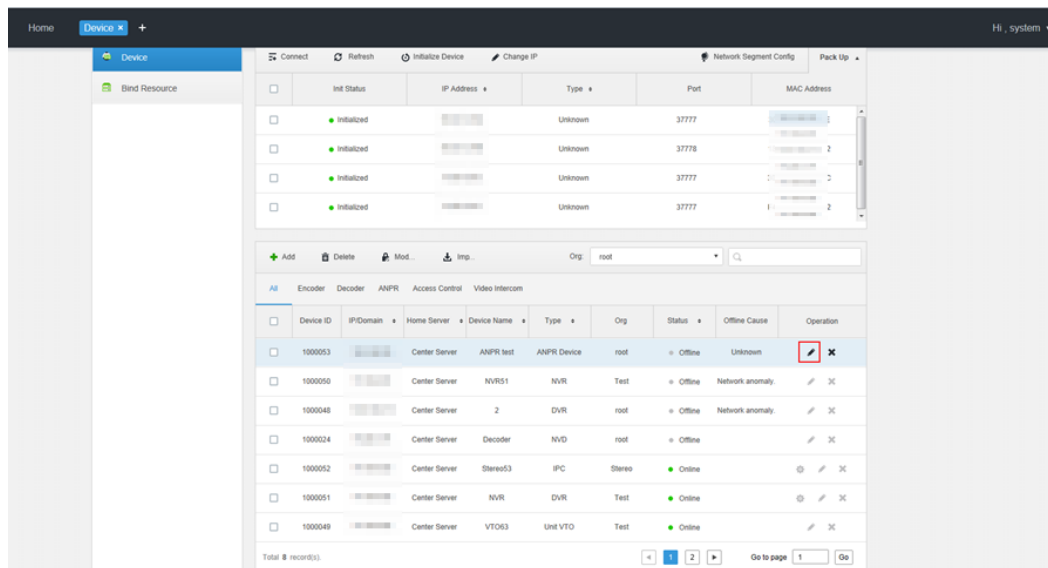
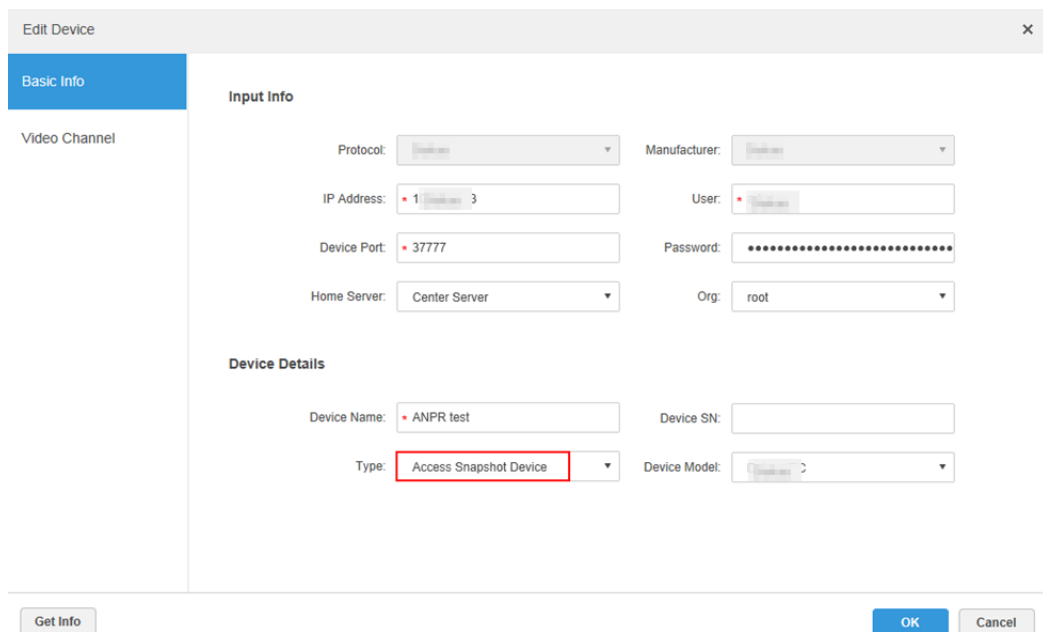


Figure 5-297 Edit device



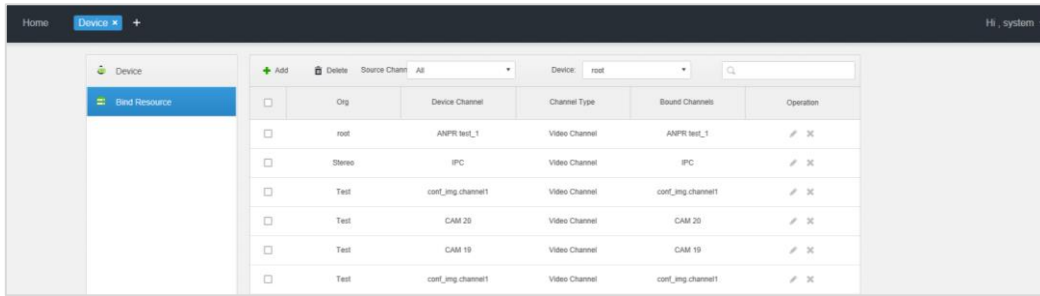
- 2) Set type as Access Snapshot Device.
- 3) Click **OK** and complete configuration.

Step 2 Bind Resource

If there is camera installed at the entrance to view entrance panoramic picture, support binding ANPR and video camera. License plate recognition can view realtime video image. You can view video of bound camera.

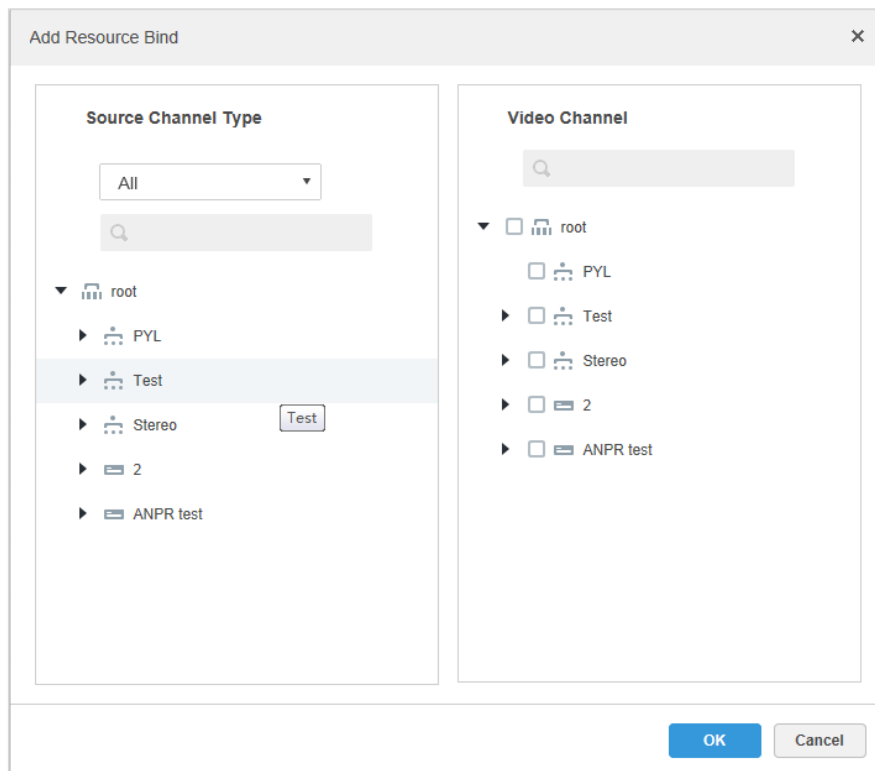
- 1) Click **Bind Resource** tab on the interface of **Device**.

Figure 5-298 Bind resource



2) Click **Add**.

Figure 5-299 Add resource bind



- 3) Select ANPR from the list of **Source Channel Type**, and select video camera from the list of **Video Channel**.
- 4) Click **OK** and complete configuration.

5.16.2.2 Adding NVR

NVR is used to connect ANPR and DSS platform, and realize data transmission.



- Please make sure NVR is fully configured before adding. For example, modify IP address, add remote device.
- NVR device category is Encoder.

Step 1 Add encoder **NVR**. For detailed operation, refer to "4.5 Adding Device."

Step 2 Modify device capacity set.


- 1) Click  of added NVR on the **Device** interface on Web.

Figure 5-300 Device interface

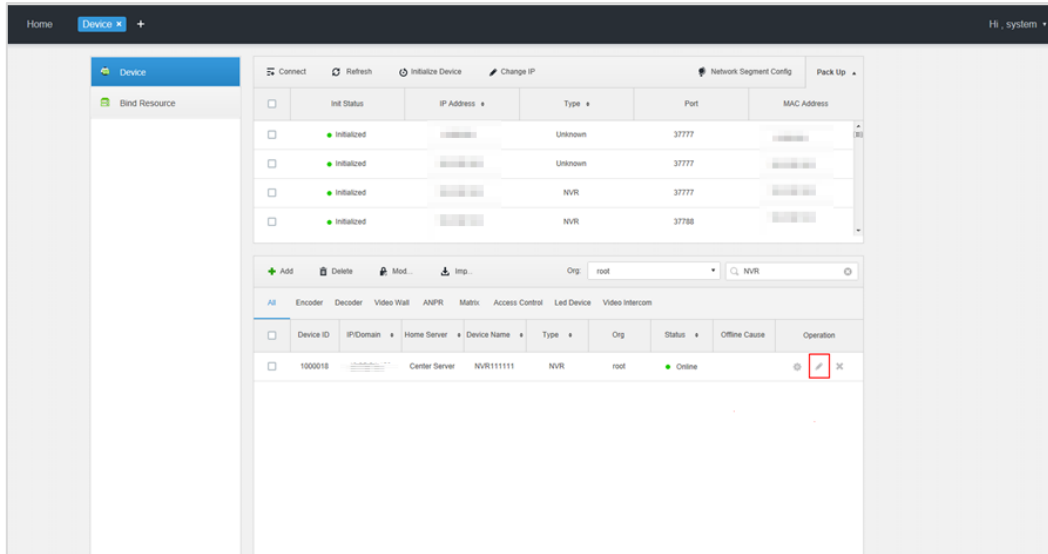
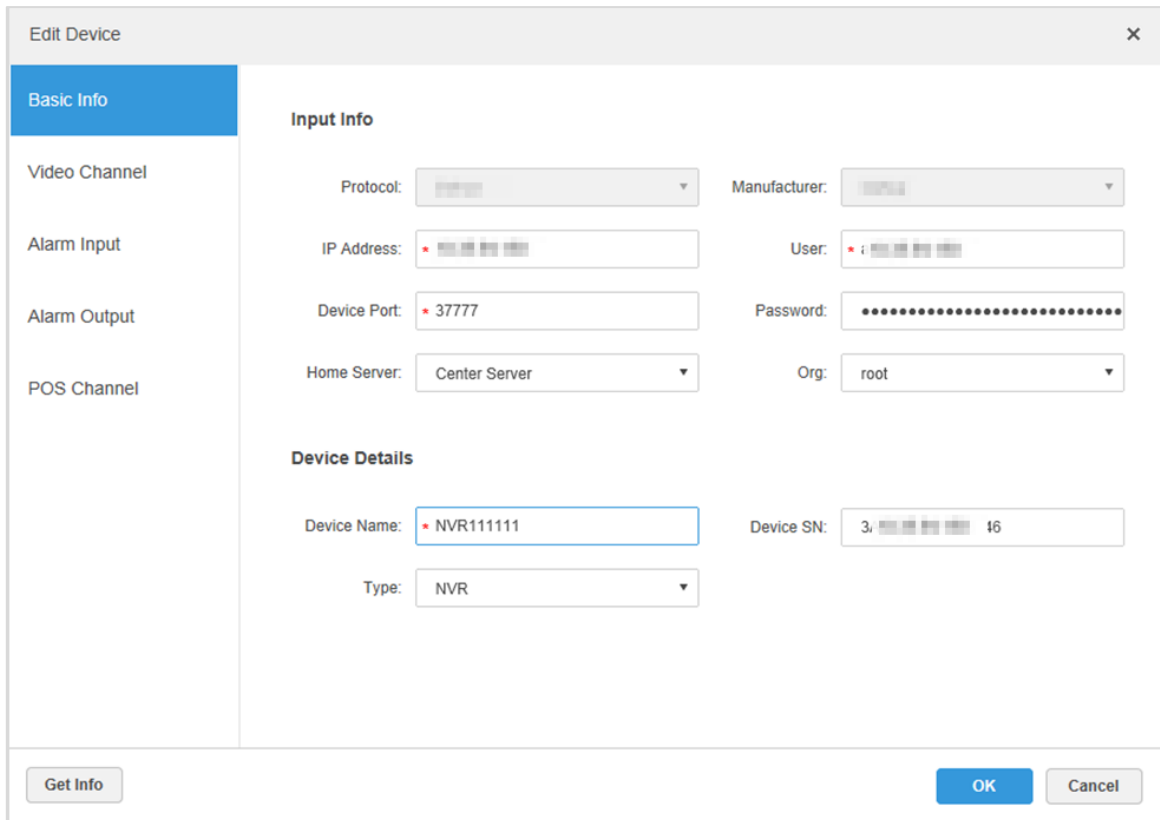


Figure 5-301 Edit device



- 2) Click the tab of Video Channel, set features as **Access Snapshot**.
The feature of all the bound ANPR device channel is set as **Access Snapshot**.

Figure 5-302 Set device features

3) Click **OK** and complete configuration.

5.16.2.3 Adding VTO

When ANPR fails to recognize vehicle, you can use VTO to recognize people and unlock barrier or call administrator by VTO to unlock barrier remotely.



- Please make sure VTO is completely configured before adding. For example, modify IP address, configure SIP server information, unit enable, building enable etc.
- Unit enable and building enable of VTO are required to be in accordance with the platform; otherwise it will fail to add VTO.
- For more details of adding VTO, refer to "4.5 Adding Device."

5.16.2.4 Adding Remaining Parking Screen

Collect the data of vehicle entrance and exit from ANPR camera; make statistics of parking space quantity, then parking space quantity will be displayed on the screen.



- Please make sure remaining parking space is completely configured before adding. For example, modify IP address.
- The device category of remaining parking screen is **LED Device**.

Step 1 Add remaining parking screen, for detailed operation, refer to "4.5 Adding Device."

Step 2 Modify the information of remaining parking screen.

- 1) Click  of added remaining parking screen on the **Device** interface..

Figure 5-303 Device interface

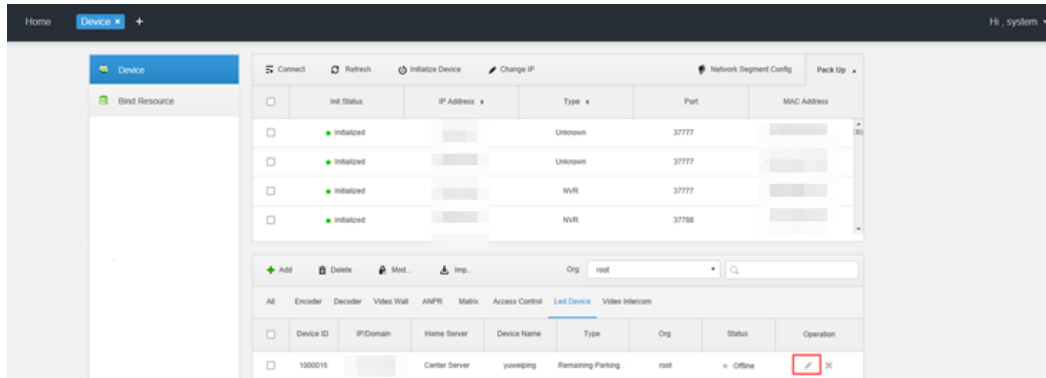
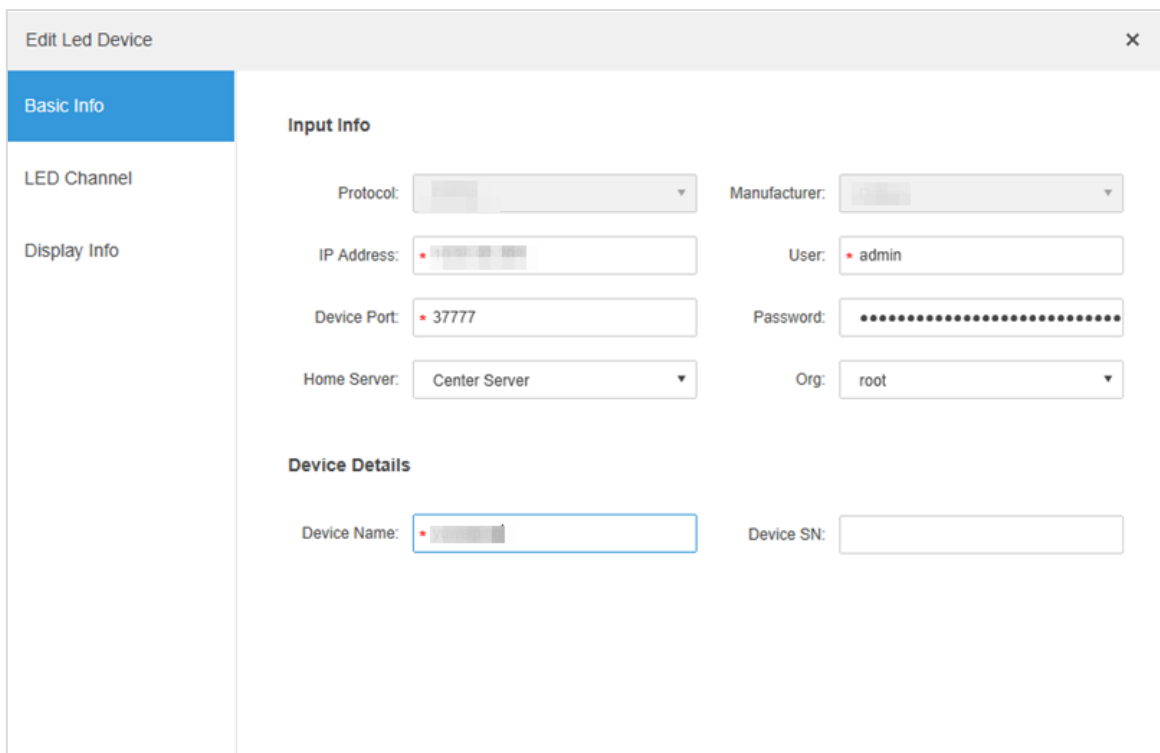
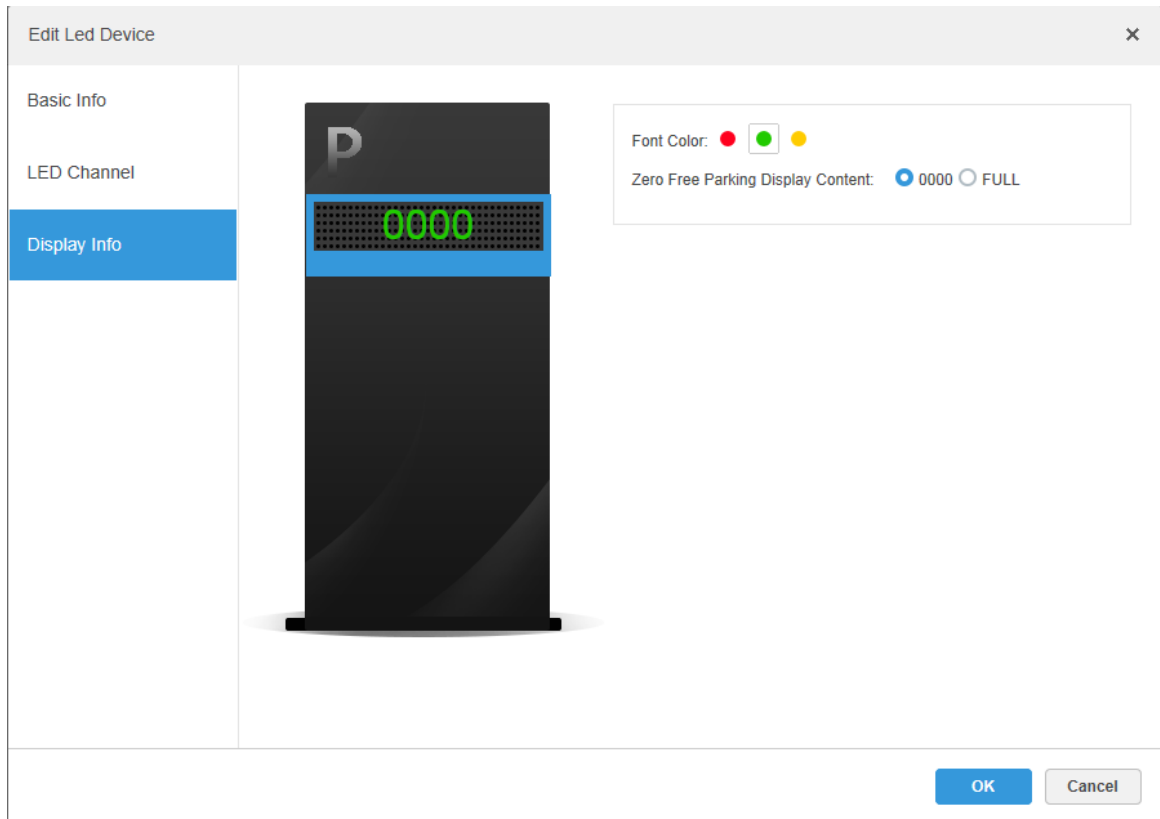


Figure 5-304 Edit LED device



- 2) Click the tab of Display Information, select Font Color and Zero Free Parking Display Content.
Font color is the color of the words displayed on the screen; Zero free parking display content is the information displayed on the screen when there is no parking space available.
- 3) Click **OK** to complete configuration.

Figure 5-305 Set display information



5.16.3 Personnel Management

It needs to add personnel and authorize them if you want to realize face recognition unlock by VTO. For detailed operation, refer to "5.14 Personnel Management."

5.16.4 Configuring Alarm Scheme

Related alarm schemes of entrance include:

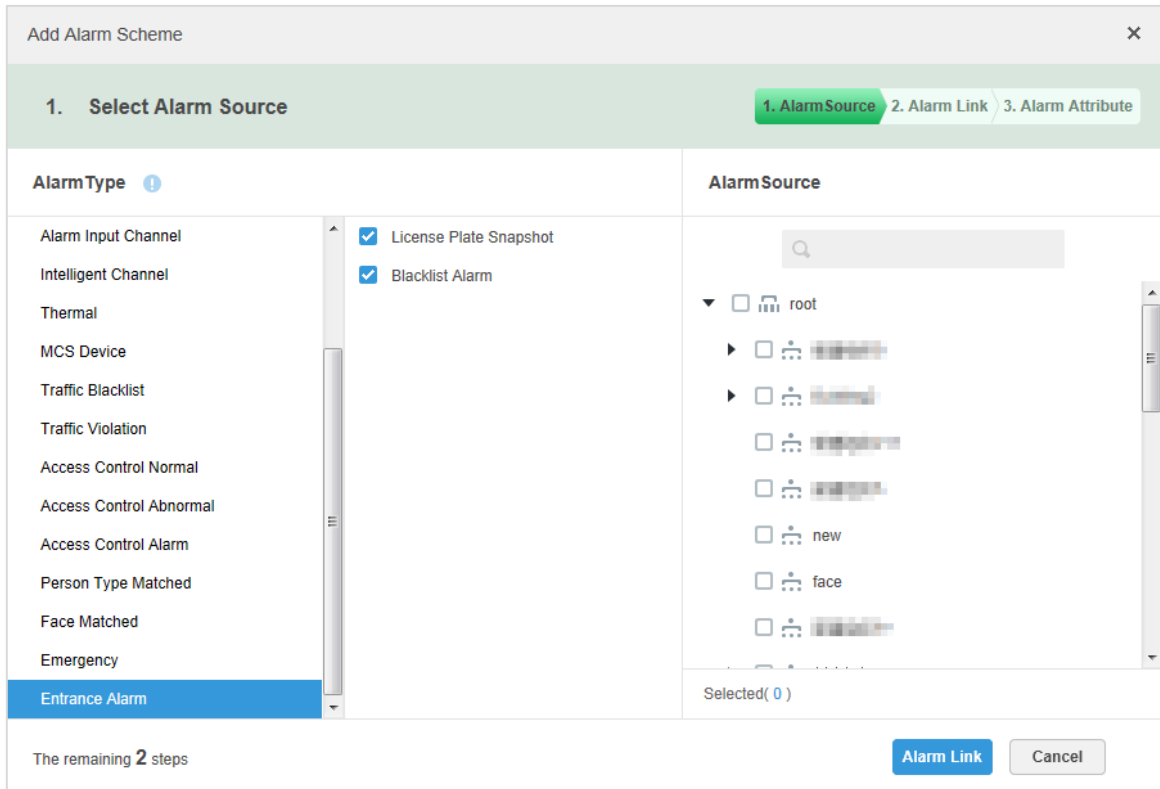
- License plate recognition
When ANPR device recognizes license plate, it will be reported to DSS platform by NVR, alarm is triggered on DSS platform, and extract video before and after license plate recognition happens from NVR, save it on the server installed on DSS platform. Default record time is 20s, 10s before and 10s after alarm is triggered.
- Blacklist Alarm
Mark some plate number as blacklist vehicle, compare the plate number reported by ANPR device with the plate number of blacklist vehicle. It will trigger alarm if it is the plate number of blacklist vehicle.



Refer to "5.16.6 Vehicle Management" for more details.

Add entrance alarm scheme on the **Event** interface of Web.

Figure 5-306 Add entrance alarm scheme



5.16.5 Configuring Parking Lot

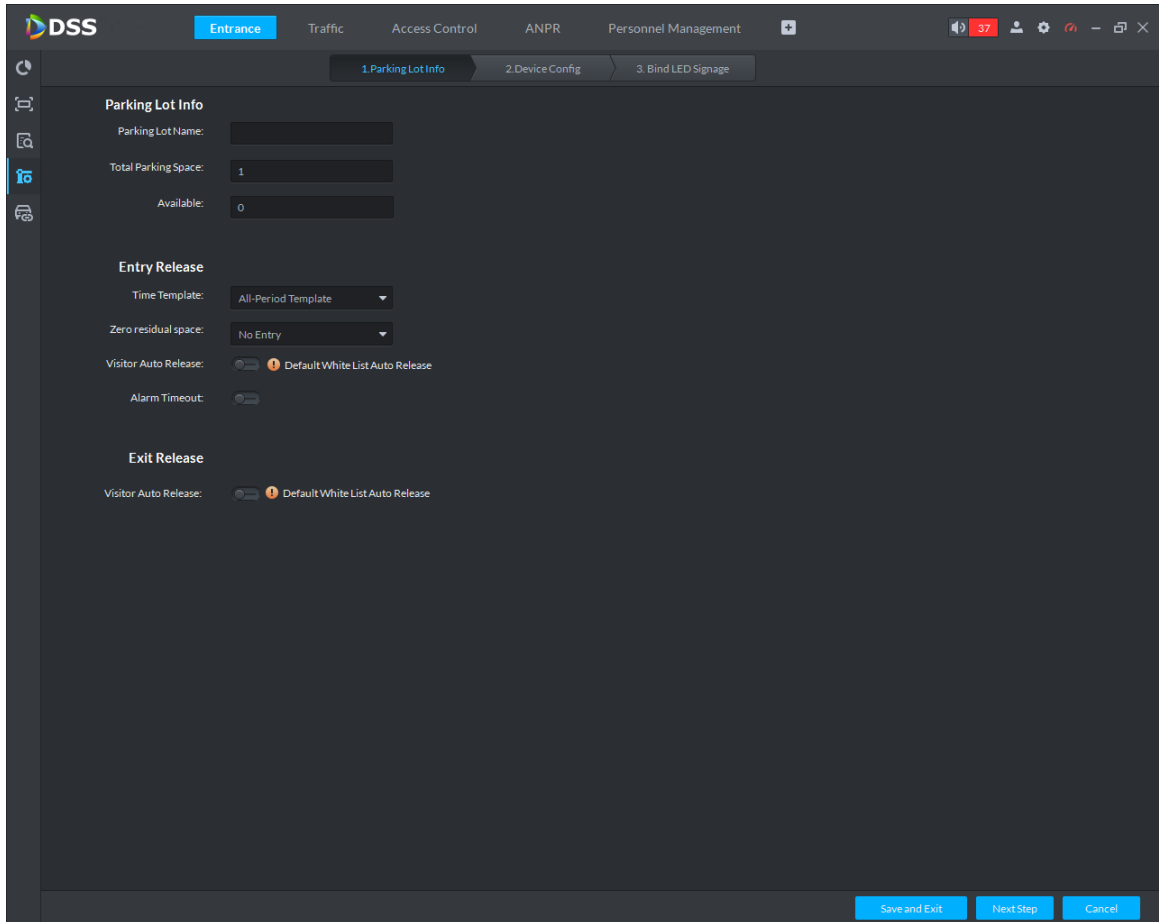
Generally one parking lot is considered as an area. Parking lot configuration includes setting parking space quantity, release situation and other information. Bind ANPR device channel and use it to recognize vehicles, bound VTO is used to recognize people.

Step 1 Click  and select **Entrance** on the **Homepage** interface.

Step 2 Click .

Step 3 Click **New Parking Lot**.








Figure 5-307 Add a parking lot



Step 4 Configure parking lot information.

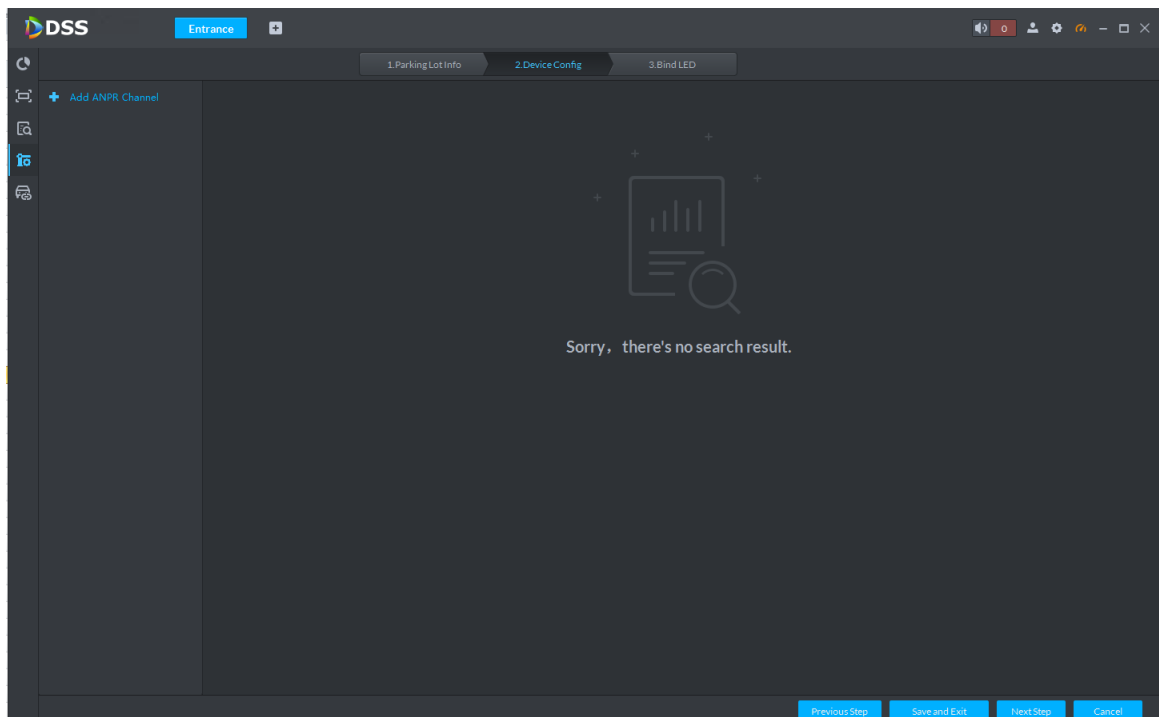
Table 5-61 Parameters

Parameter		Description
Parking lot info	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.
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: 1. All-period template: 00:00 to 24:00 daily. 2. Weekday template: 00:00 to 24:00 Mon to Fri. 3. Weekend template: 00:00 to 24:00 Sat and Sun.
	Zero residual space	Release option when remaining space is zero. 1. No entry. Any vehicle is not allowed to enter. 2. All Any vehicle is allowed to enter. 3. Whitelist Whitelist vehicles include several vehicle types, such as

Parameter		Description
		<p>no group, general and VIP. Only three types of vehicle above are allowed to enter when remaining space is zero.</p> <p>4. VIP Only VIP vehicle is allowed to enter when remaining space is zero.</p> <p></p> <p>Vehicle type should be set during vehicle management.</p>
	Visitor auto release	<p>Those which are not registered on DSS platform are considered as visitor vehicles. Confirm if it unlocks barrier automatically when visitor vehicle enters according scenario design. If it is required to release, and then click , the icon displays as . Otherwise, it remains as , and it will not unlock barrier to release when visitor wants to enter parking lot.</p>
	Alarm Timeout	An alarm will occur when a vehicle has not left the parking lot after the timeout threshold.
Exit Release	Visitor auto release	<p>Those which are not registered on DSS platform are considered as visitor vehicles. Confirm if it unlocks barrier automatically when visitor vehicle exits according scenario design. If it is required to release, and then click , the icon displays as . Otherwise, it remains as , and it will not unlock barrier to release when visitor wants to exit parking lot.</p>

Step 5 Click **Next Step**.

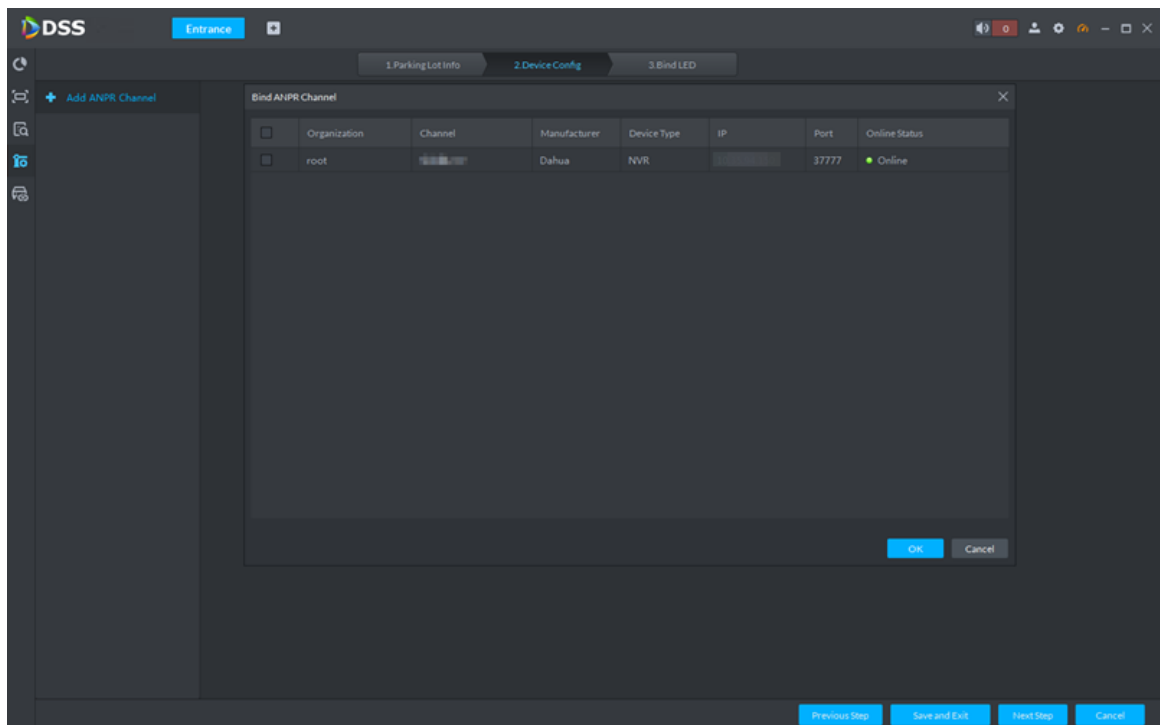
Figure 5-308 Device configuration interface



Step 6 Add an ANPR device.

- 1) Click **Add ANPR Channel** and you can select all the ANPR devices deployed at entrance and exit of the parking lot on the interface.

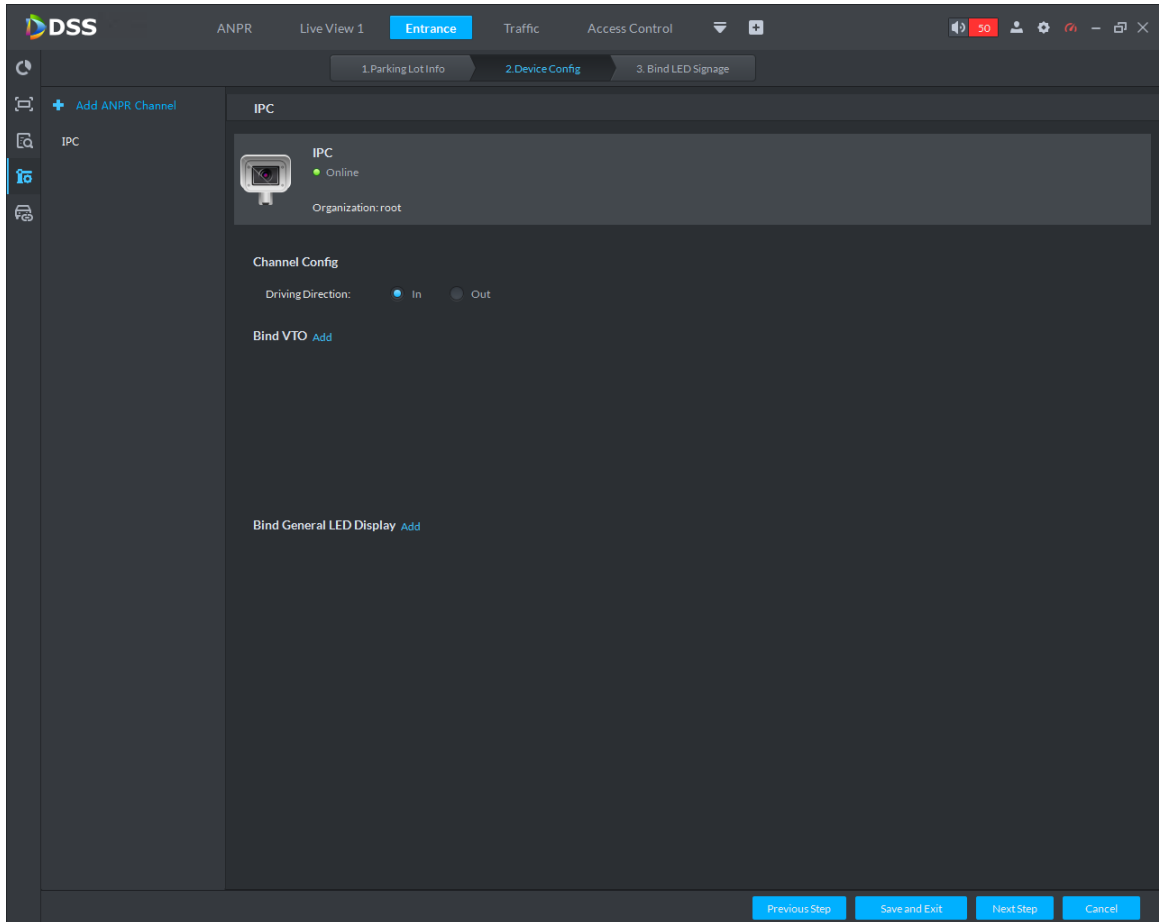
Figure 5-309 Add ANPR channel



- 2) Click **OK**.

The information of added ANPR device is displayed.

Figure 5-310 ANPR device information



- 3) Select ANPR device from device list in sequence, and set corresponding driving direction.

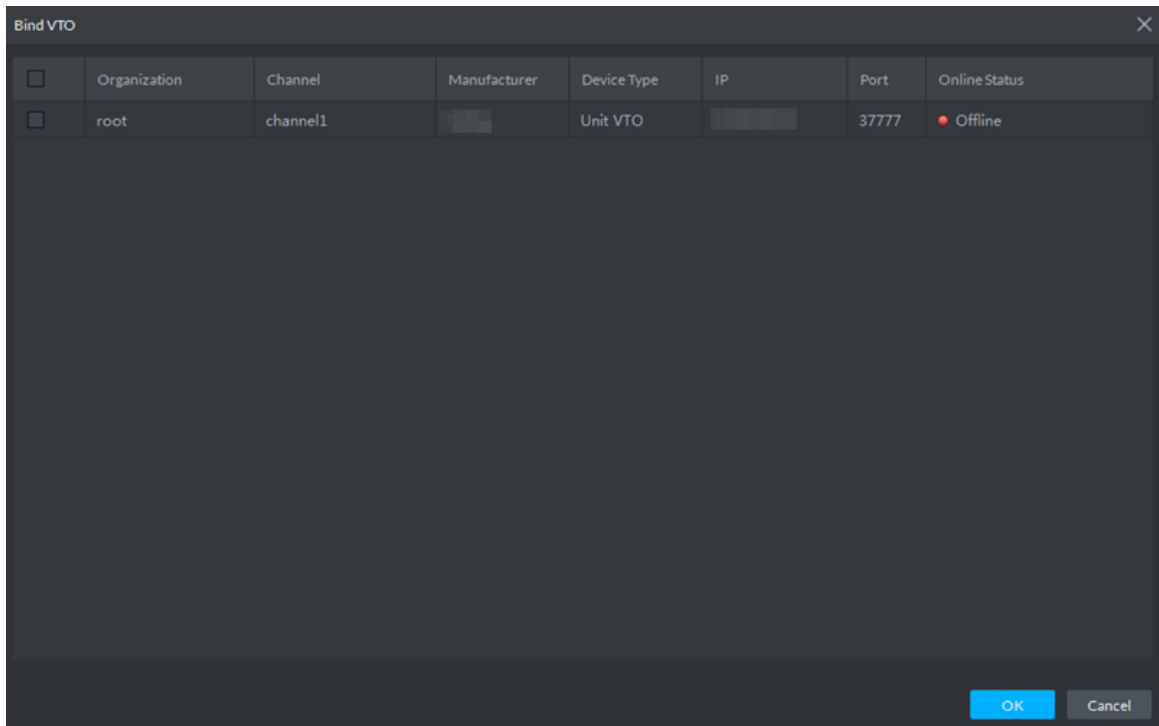
The default driving direction is **In**.

Step 7 Bind VTO device.

VTO device is used to recognize people, and unlock barrier. Please skip this step if there is no VTO in the networking.

- 1) Click **Add** next to **Bind VTO**.

Figure 5-311 Bind VTO

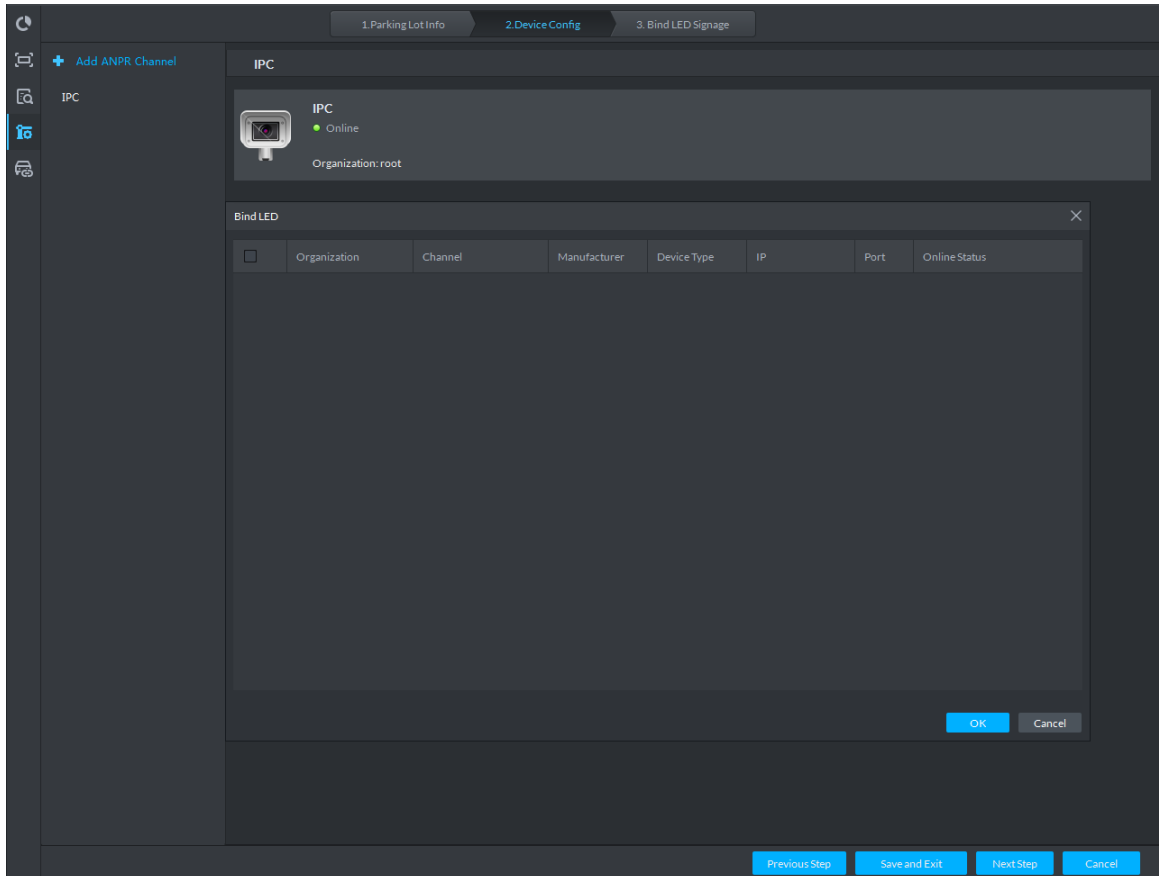


2) Select the VTO that is deployed next to barrier, and then click **OK**.

Step 8 Bind an LED display.

1) Click Add next to Bind General LED Display.

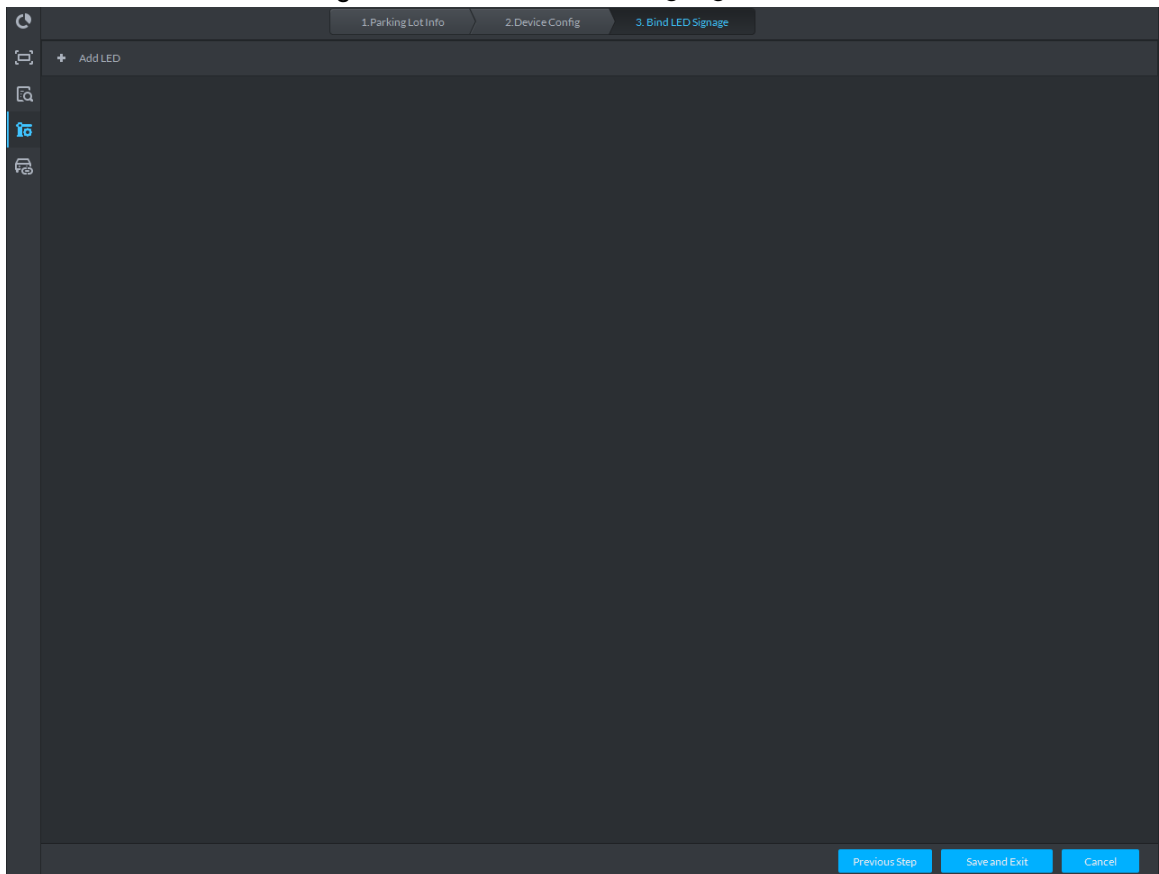
Figure 5-312 Bind an LED display



2) Select an LED display, and then click **OK**.

Step 9 Click **Next Step**.

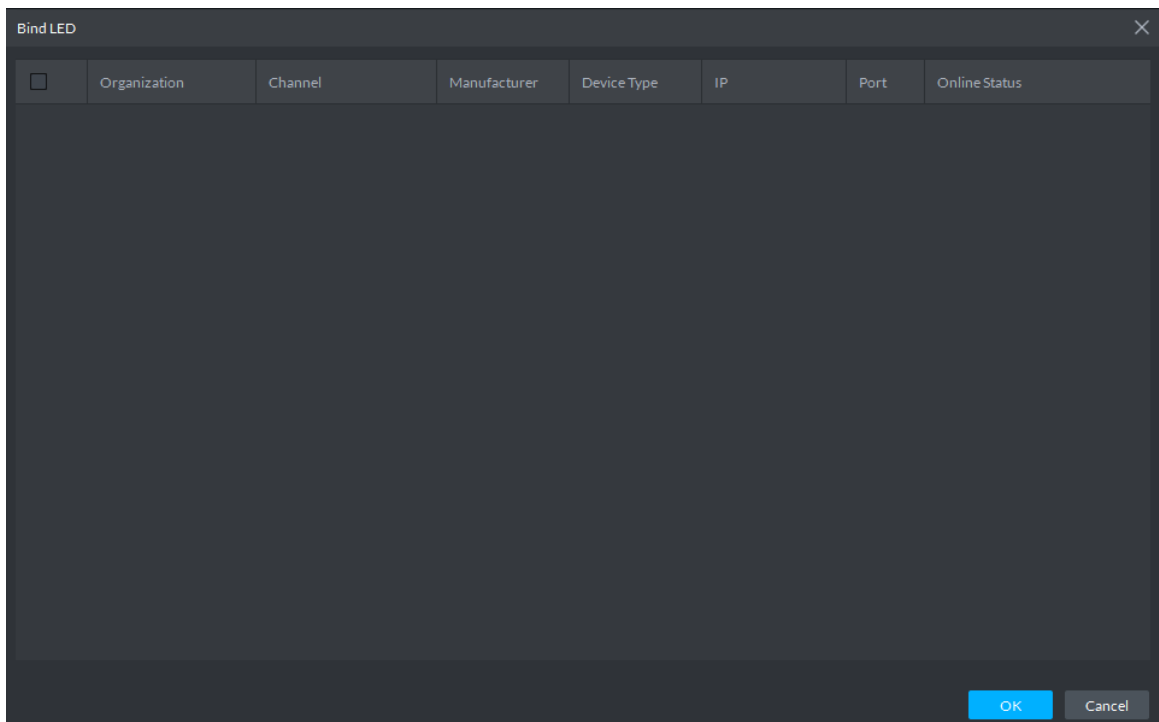
Figure 5-313 Bind an LED signage



Step 10 Add an LED signage.

1) Click **Add LED**.


Figure 5-314 Bind LED



2) Select all the LED of the parking lot and click **OK**.

5.16.6 Vehicle Management

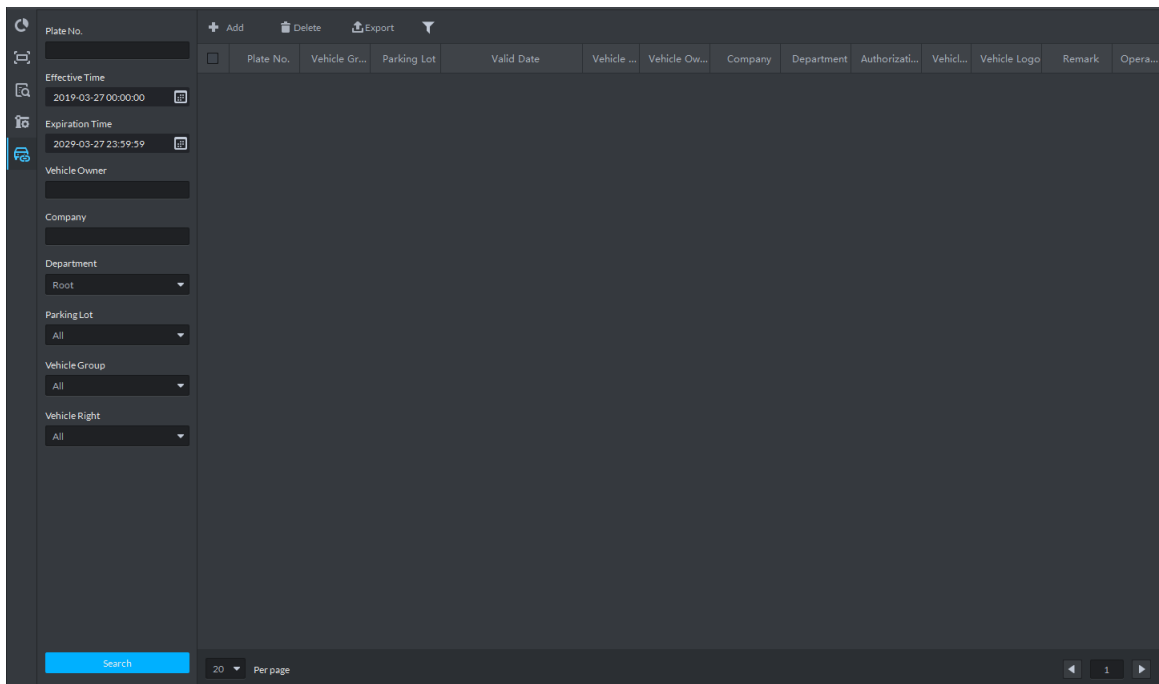
Vehicle information management includes vehicle type, department, related personnel and release ANPR, which are used as judgment basis to confirm if the vehicle can enter some area. Vehicle management can synchronize added vehicle information from personnel management module.

Step 1 Click  on the interface of **Entrance**.



You can set search condition, click **Search** and the system displays vehicle information. Including vehicle information added on personnel management module.

Figure 5-315 Vehicle management



Step 2 Click **Add**.

Figure 5-316 Add vehicle information

Step 3 Click the tab of **Vehicle information** and add vehicle information, click **Next** and the **Personnel information** interface is displayed.

Figure 5-317 Add personnel information

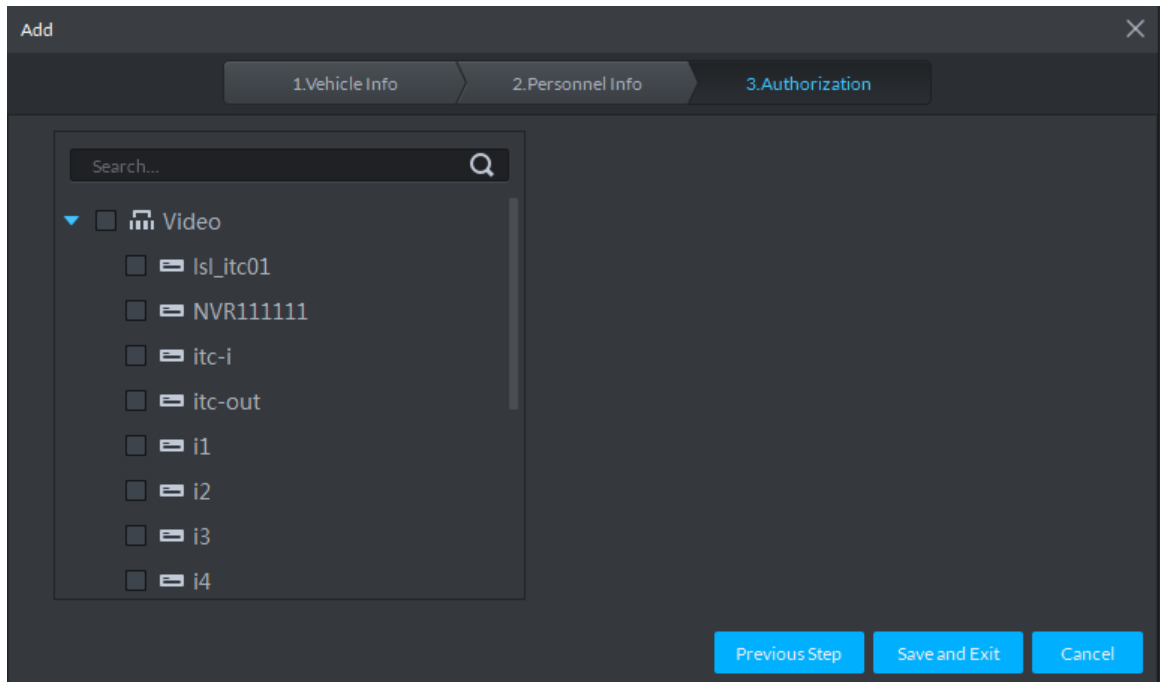
Table 5-62 Parameters

Parameter	Description
Plate No.	The plate number of added vehicle.
Vehicle Type	Include no group, general, VIP and blacklist. The first three types make up whitelist. If blacklist alarm scheme is set, then set vehicle type as blacklist, it will trigger alarm when vehicle is recognized.
Vehicle Color	Vehicle color of added vehicle. You can set Not Recognized if vehicle color cannot be recognized. If the color is beyond the selected range, then you

Parameter	Description
	can set is as Other .
Vehicle Logo	Main vehicle logos on the market.
Parking Lot	Area where vehicle belongs (required).
Validity Time	Validity period of added vehicle.
Expiration	
New Vehicle	If there are several vehicles, then click the button to add continuously. One person can add up to 5 vehicles.

Step 4 Set vehicle related personnel information, click **Next**.

Figure 5-318 Authorization



Step 5 Select all the ANPR devices that allow entrance and exit of the parking lot, click **Save and Exit**. Synchronize vehicle information to corresponding ANPR device; make sure the ANPR device can make judgment if it has to release the vehicle even if ANPR device is disconnected to DSS platform.

5.16.7 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.


Click  on the **Entrance** interface. The **Overview** interface is displayed.

Figure 5-319 Overview

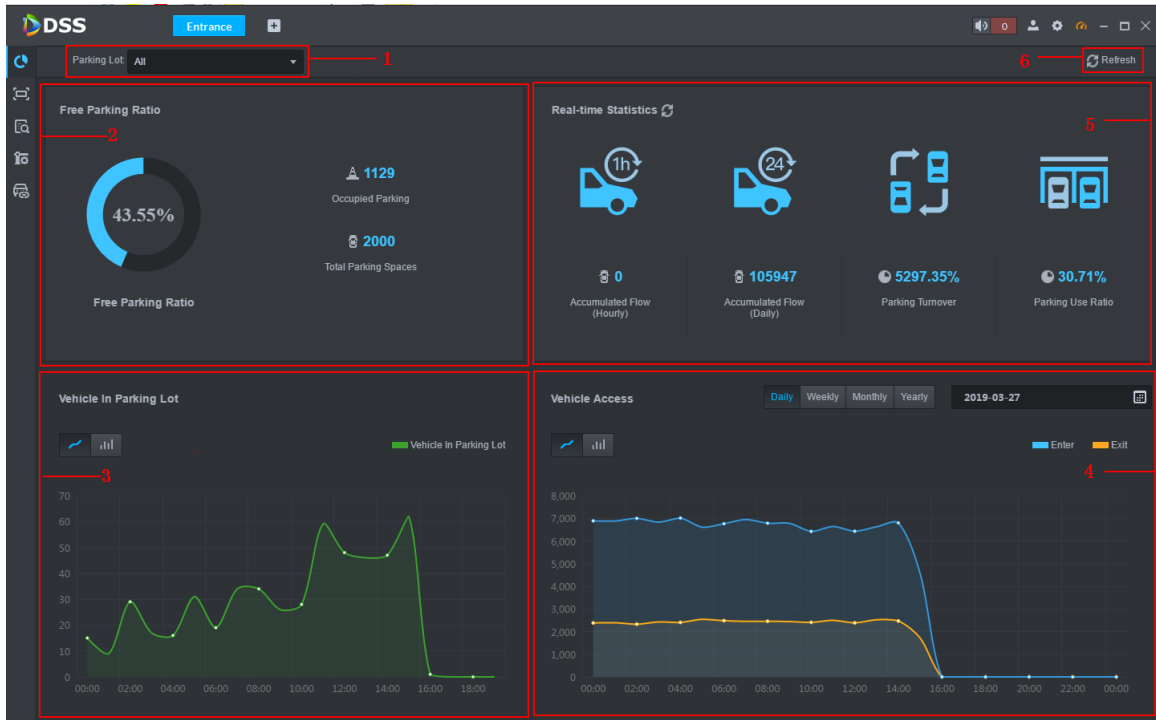


Table 5-63 Parameters

No.	Description
1	Interface displays the information of selected area; refer to 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. Move mouse on the image and displays 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 displays by line chart or bar chart. Move the mouse on the image and display corresponding time and occupied parking space quantity.
5	<p>Display following data.</p> <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). Accumulated vehicle flow (Daily) Vehicle flow of the day (Start statistics from 00:00) 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. Parking Use Ratio The bigger the parking use ratio is, the average time of vehicle parking is longer.

No.	Description
6	Automatically refresh overview information every 5 minutes. Click Refresh to sync realtime data.

5.16.8 License Plate Recognition

Click  on the **Entrance** interface. The **License Plate Recognition** interface is displayed.

Figure 5-320 License plate recognition

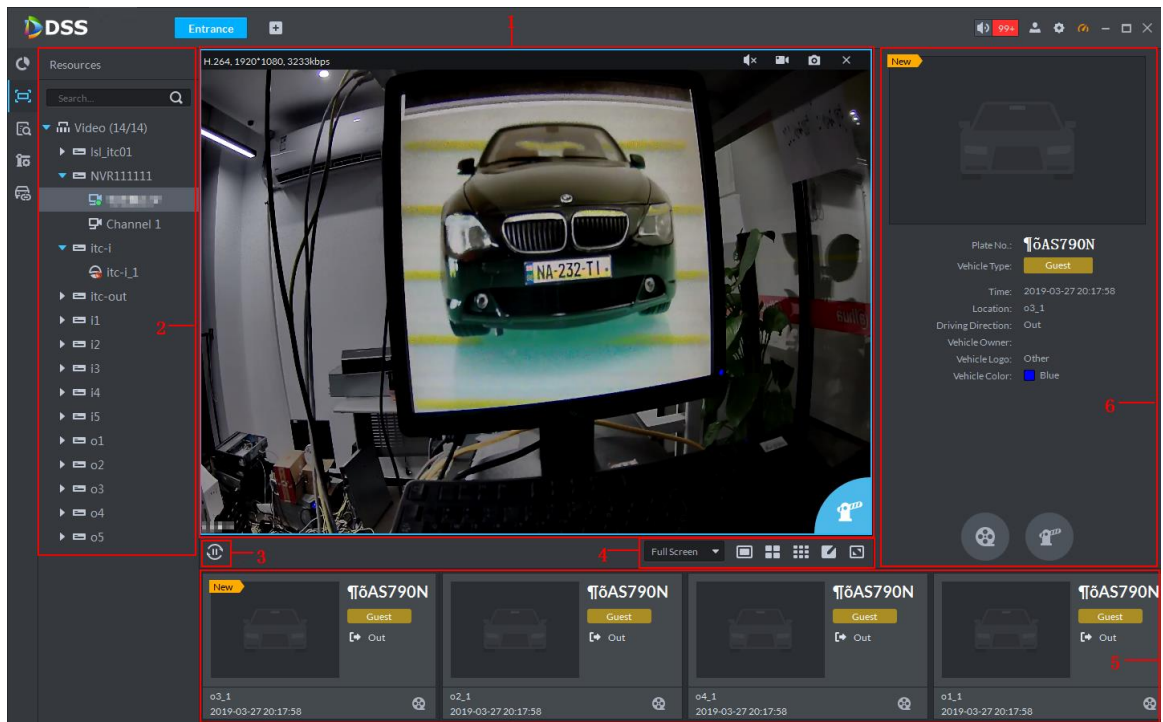




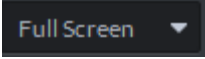









Table 5-64 Description

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.
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

No.	Description
	<p>splits, or click  and customize split mode.</p> <ul style="list-style-type: none"> Click , 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	<p>Display latest 4 snapshots of LPR. More details as follows.</p> <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	<p>Display license plate snapshot and vehicle which need to be released manually. More operation as follows.</p> <ul style="list-style-type: none"> Click  and unlock barrier to release vehicle. Click  and view video of linked channel.

5.16.9 Info Query

Search accessed vehicle, on-site vehicle and snapshot record.

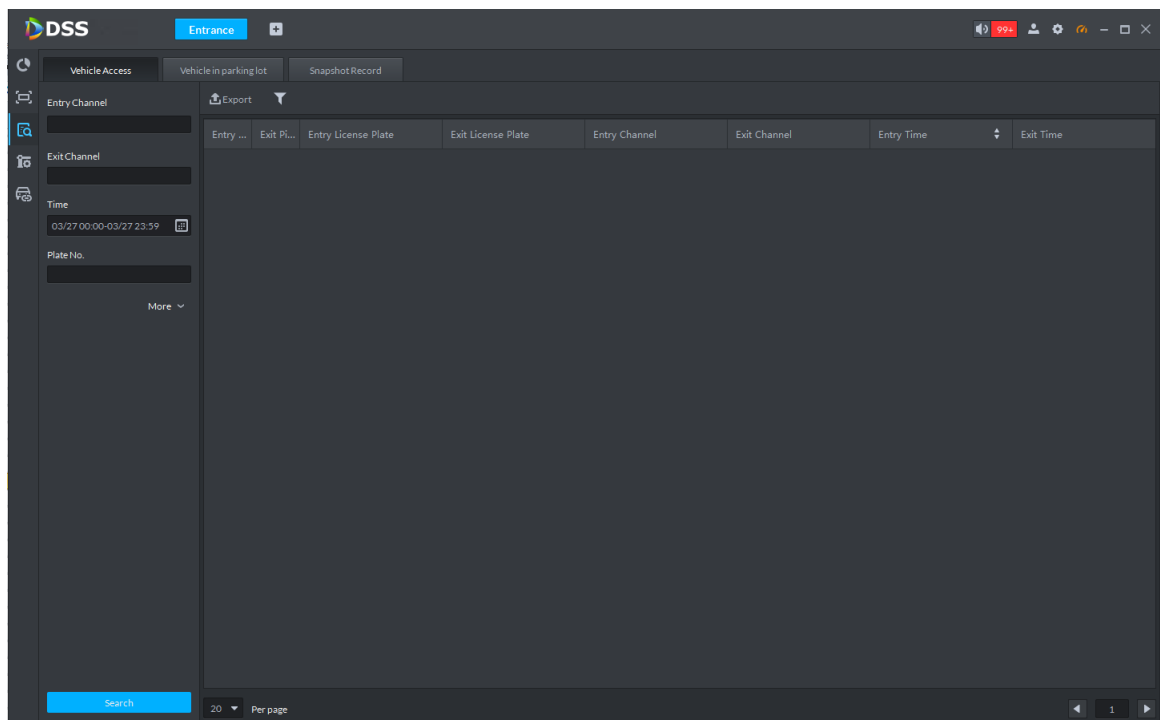
Step 1 Click  on the **Entrance** interface.

The system displays the interface of information **Query**.

Step 2 Search vehicle in and out information.

Step 3 Click the tab of **Vehicle Access**.

Figure 5-321 Vehicle access

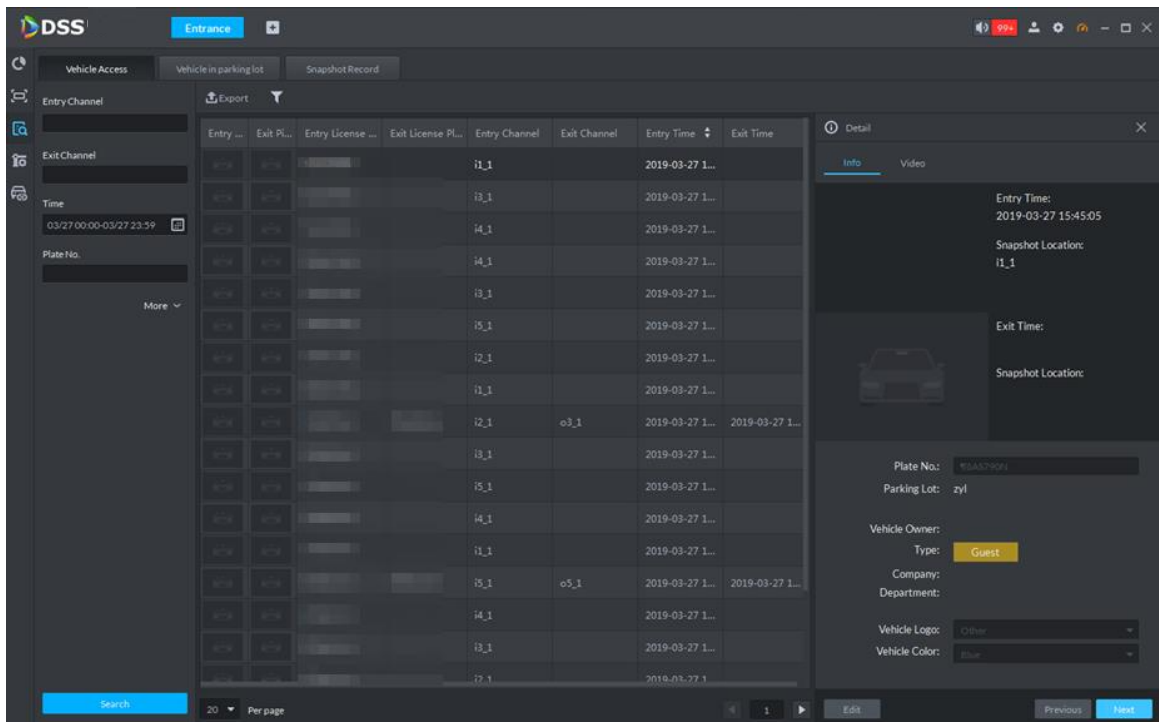


1) Set search condition, and then click **Search**.



Click **More** and you can search by vehicle owner, department and vehicle type etc.

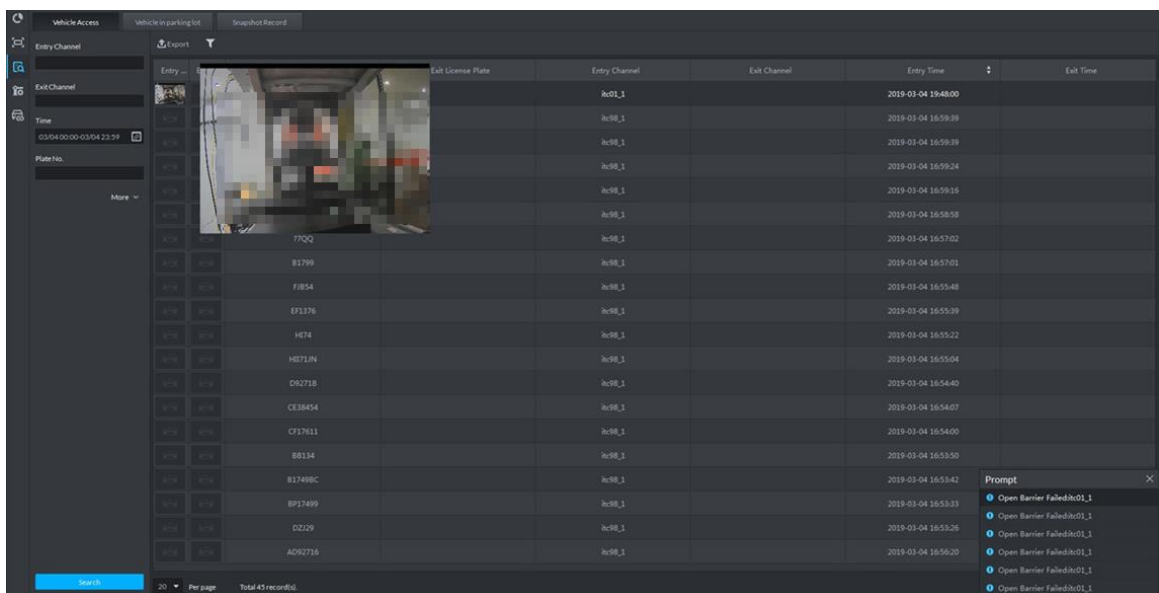
Figure 5-322 Search results



2) The related operations of vehicle access are as follows.

- ◇ Move the mouse to the recorded entry picture or exit picture, and the system will display a bigger picture.

Figure 5-323 View bigger picture



- ◇ Double-click the record, and detailed information is displayed on the right of interface. Double-click the picture in the Information, display big picture, drag green box and the big picture will be displayed in the lower right corner. Click **Edit** to modify vehicle information, click **OK** to save configuration. Click **Video** to view linked video.

Figure 5-324 Details

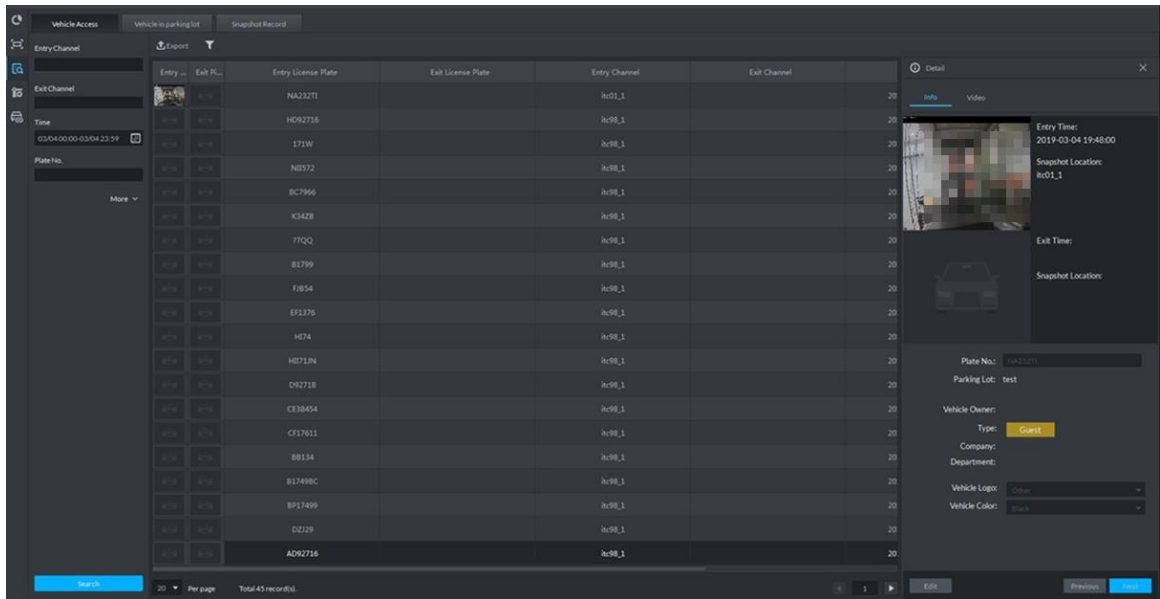
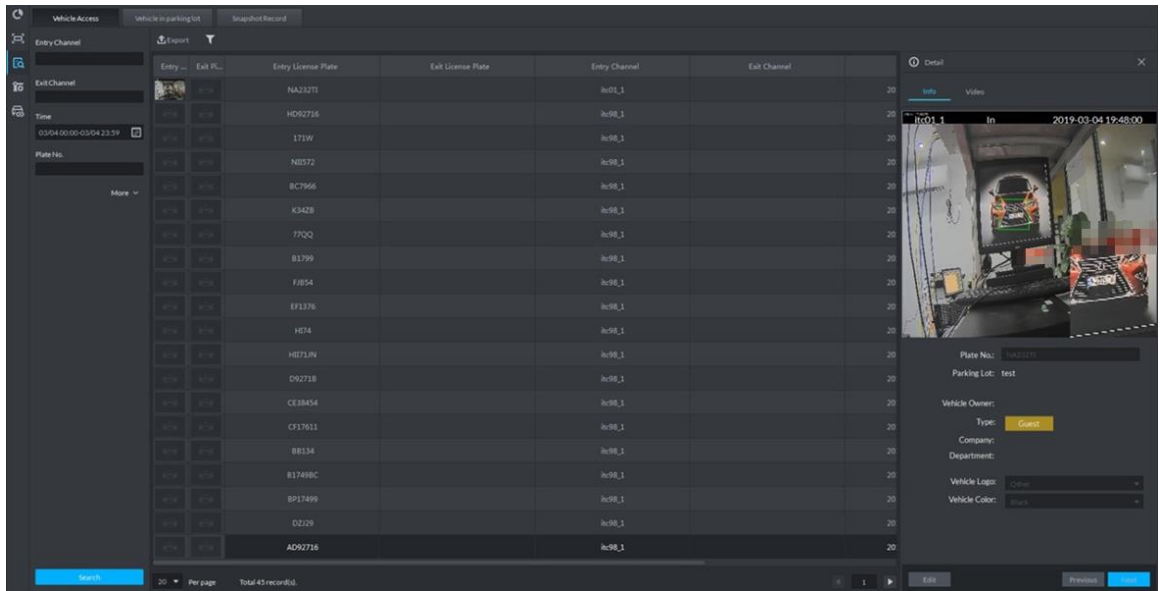



Figure 5-325 Big picture

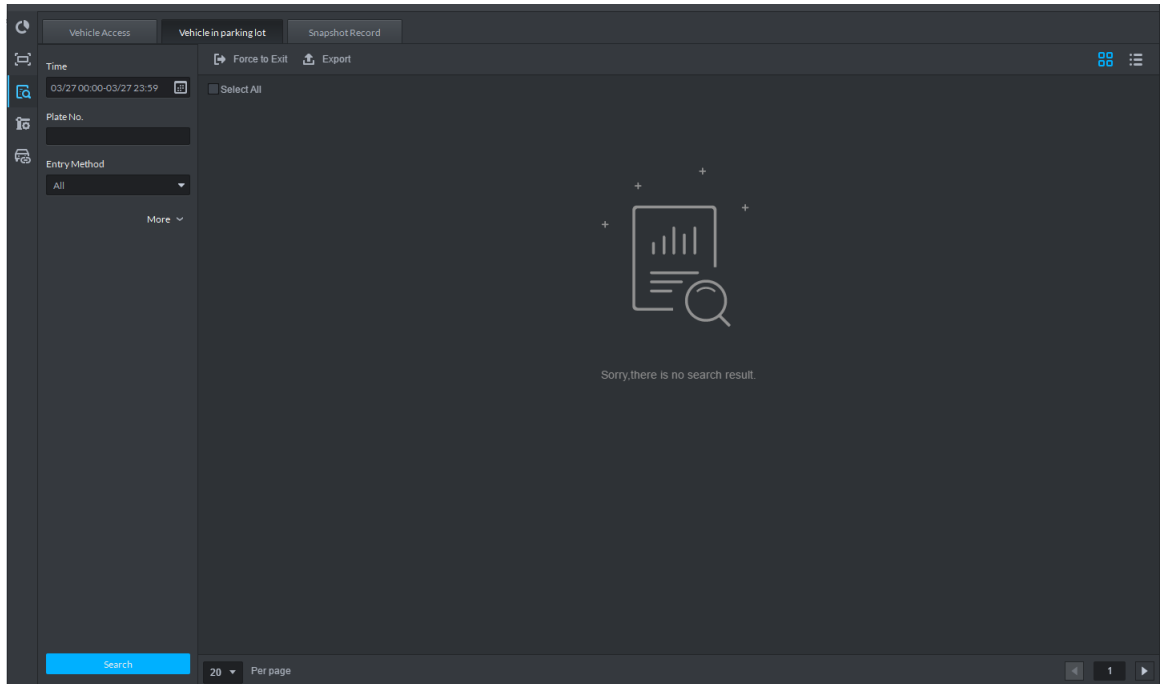


- ◇ Export information. Click **Export** to export all the searched vehicle access information.
- ◇ Set information display item. Click  and select display item.
- ◇ Click **Next** and display next information detail. Click **Previous** and display previous information detail.

Step 4 Search on-site vehicle.

- 1) Click the tab of Vehicle in parking lot.

Figure 5-326 Vehicle in parking lot

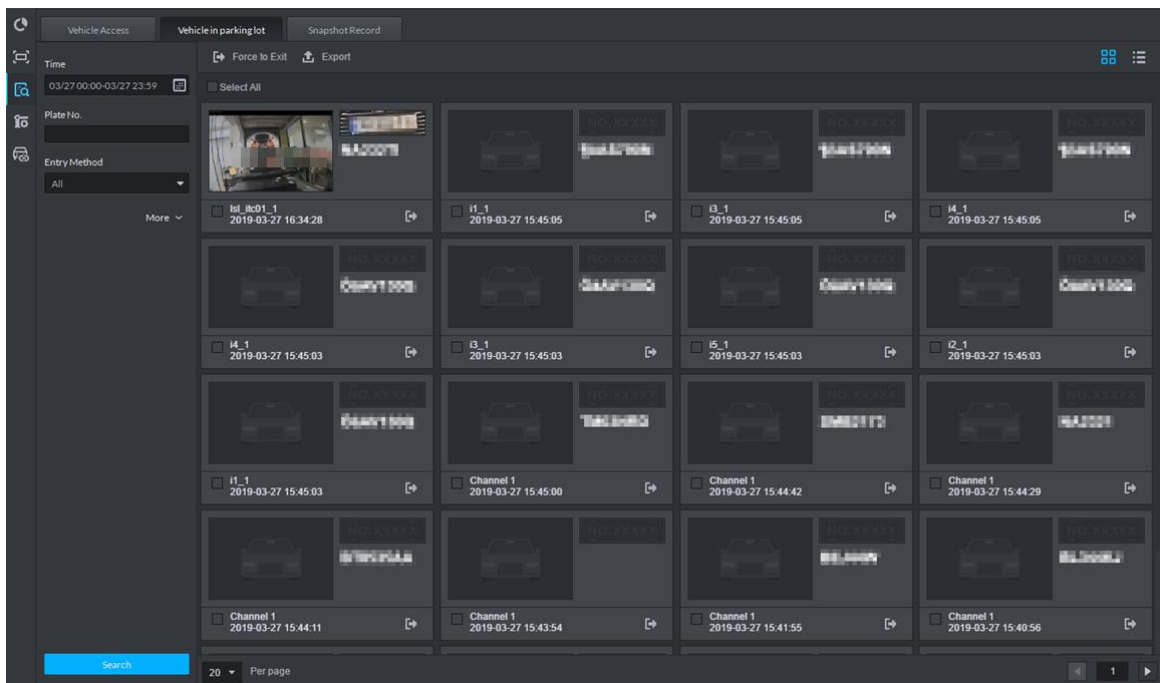


2) Set search condition, and then click **Search**.







Click **More** and you can search information via vehicle owner, department and vehicle type etc.

Figure 5-327 Search results



3) Related operations of vehicle in and out are as follows.

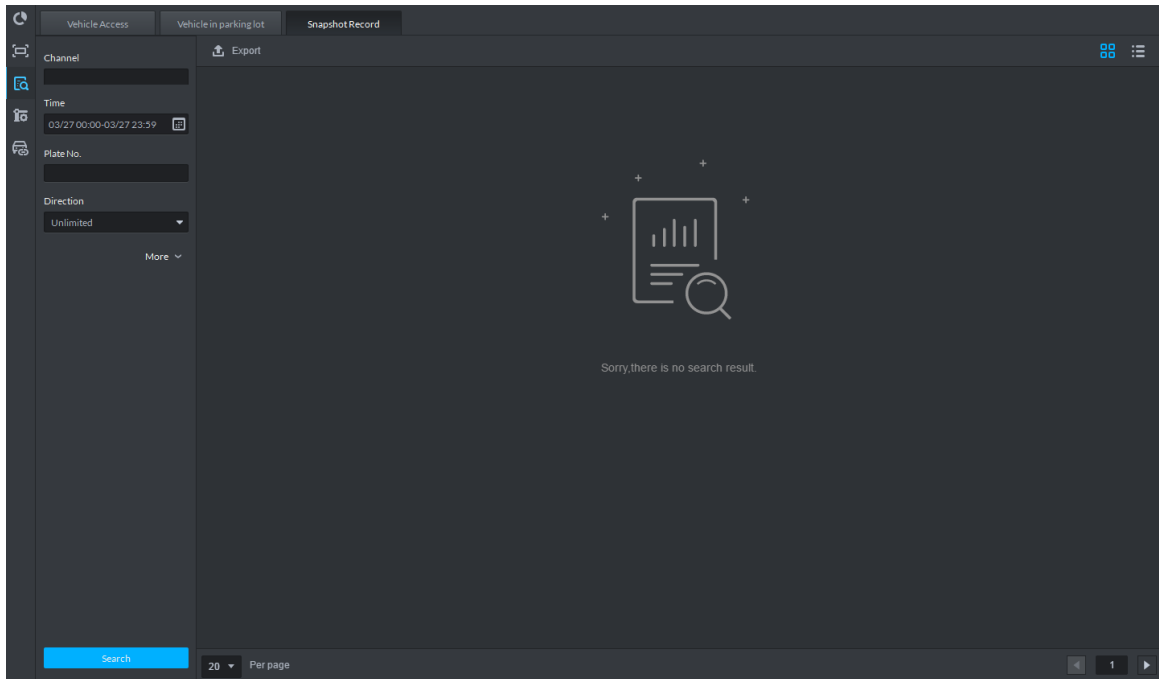
- ◇ If the vehicle is confirmed not to be in the area, then click to select information (several items supported), click **Force to Exit** or , make sure the vehicle exits by Pro.

- ◇ Export information. Click **Export** and export all the information of on-site vehicles that can be searched.
- ◇ Set information display item. Click  and select display item.
- ◇ Click view mode () or list mode () to select different display mode.

Step 5 Search Snapshot Record

- 1) Click the tab of **Snapshot Record**.

Figure 5-328 Snapshot record

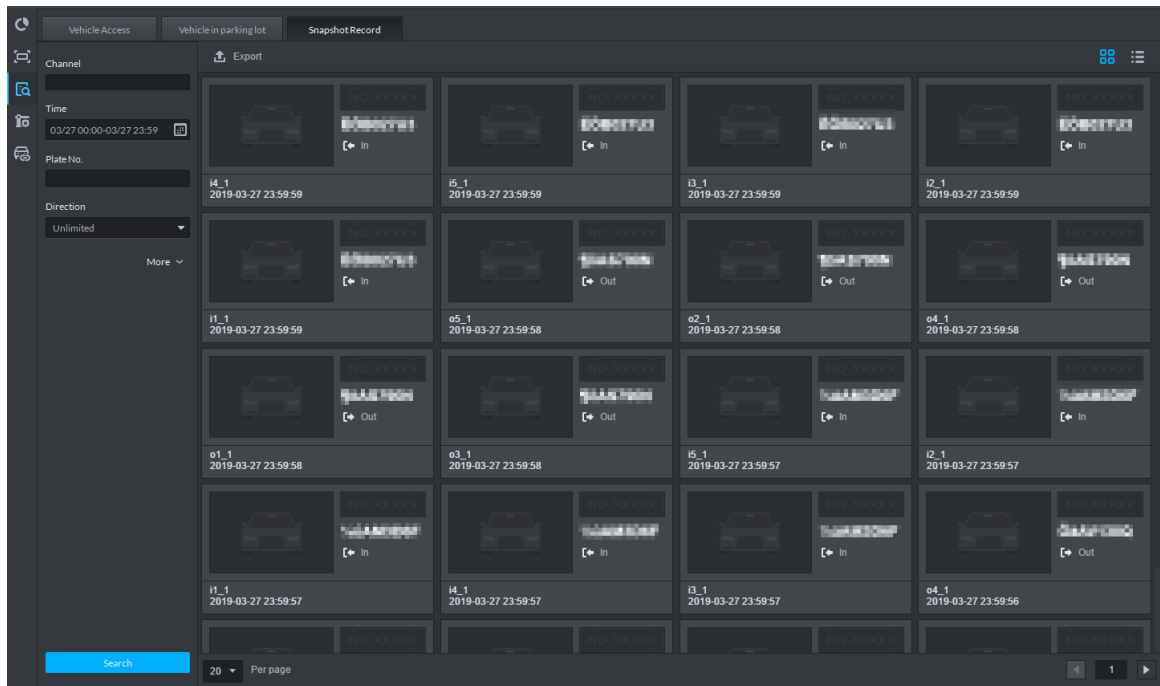




- 2) Set search condition, click **Search**.



Click **More** and you can search information via vehicle owner, department and vehicle type etc.

Figure 5-329 Search results



- 3) Related operations of vehicle snapshot are as follows.
- ◇ Export information. Click **Export** to export all the information of on-site vehicles that can be searched.
 - ◇ Click view mode () or list mode () and select different display modes.

5.17 Video Intercom

After integrating video talk module and adding video intercom device, you can realize device talk, real-time monitoring and issuing information.

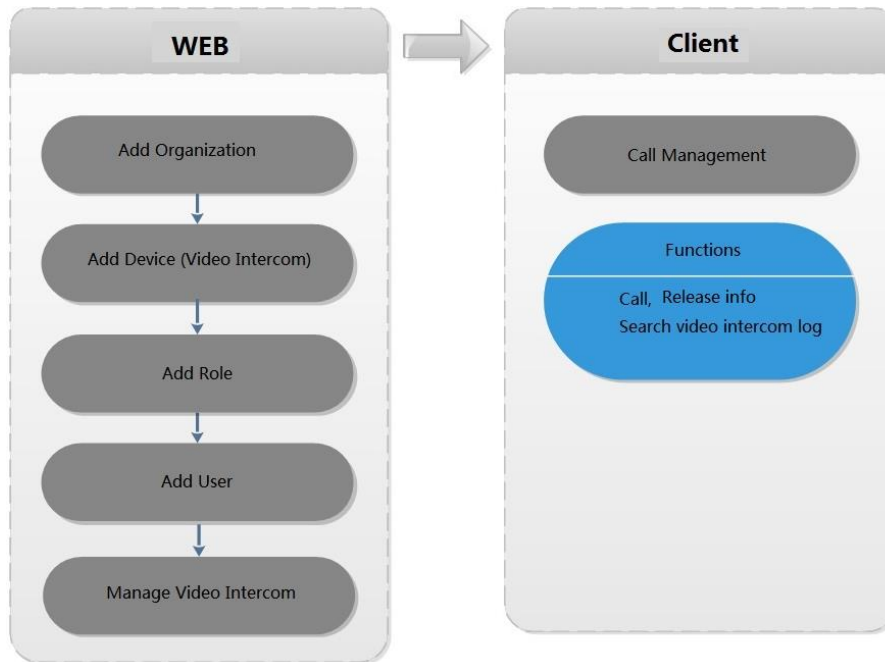
5.17.1 Preparations

- The video intercom device is already configured before configuring video talk function in Pro. For details, refer to user manual.
- Complete video intercom management on Web; refer to "4.12 Video Intercom Management" for more details.
- Add video talk devices such as unit VTO, VTH and fence VTO etc. Set Device Category as Video Intercom. Refer to "4.5 Adding Device" for more details.



Device will not actively push information to DSS if device configuration is modified during operation. It needs to enter the device modification interface and manually acquire device information.


Figure 5-330 Video intercom business flow



5.17.2 Call Management

Create device group, management group and relation group respectively; realize mutual call in the specific group. Only default system account supports the function.



Click  on the interface of device group, management group or relation group, the system will restore management group and relation group to original status.

5.17.2.1 Device Group Config

You can realize mutual call only when VTO and VTH are added into the same device group. DSS 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.

5.17.2.2 Adding Management Group

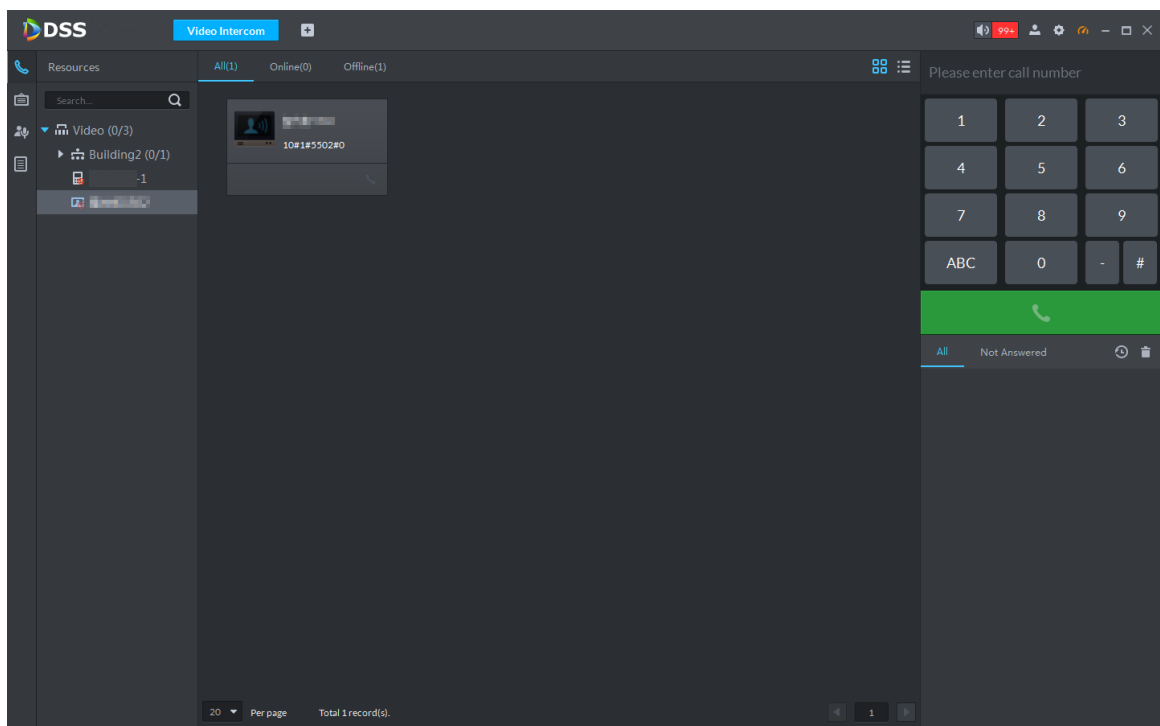
Management group is to make groups for administrators, and realize relation binding of one to one, one to many or many to many. Administrators include DSS administrator and VTS. If there is default management group, VTS will be automatically added to management group when it is added.



- 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  and select **Video Intercom** on the interface of **Homepage**.

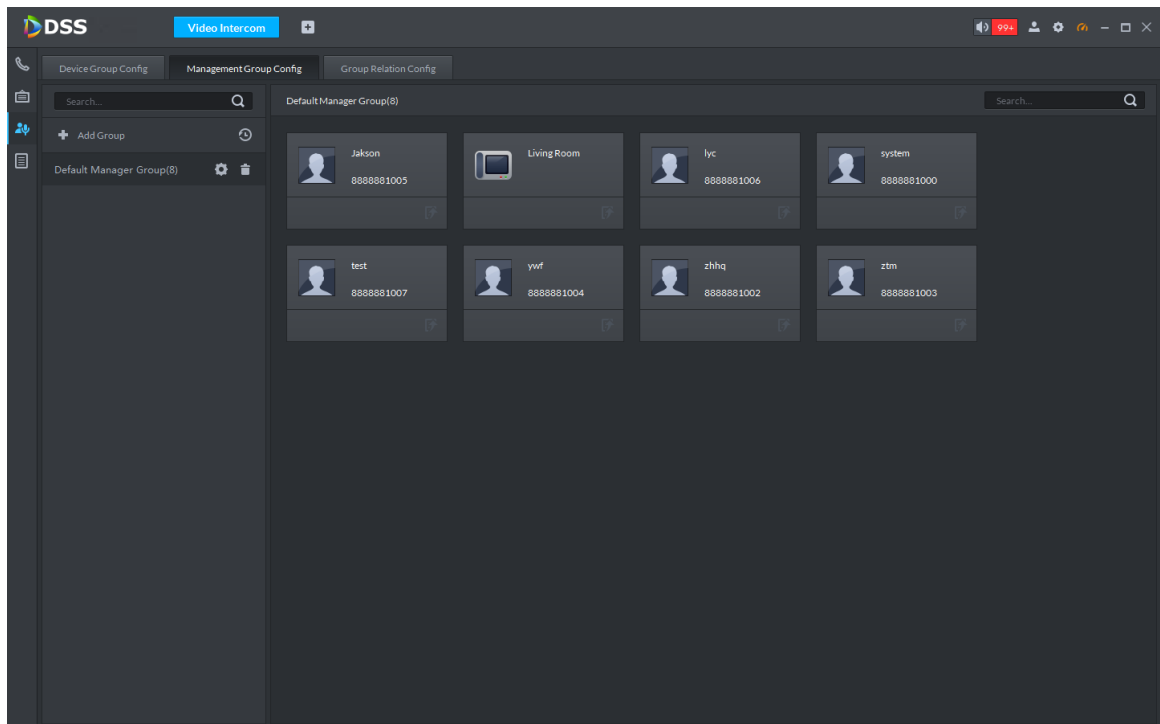
Figure 5-331 Video intercom



Step 2 Click .

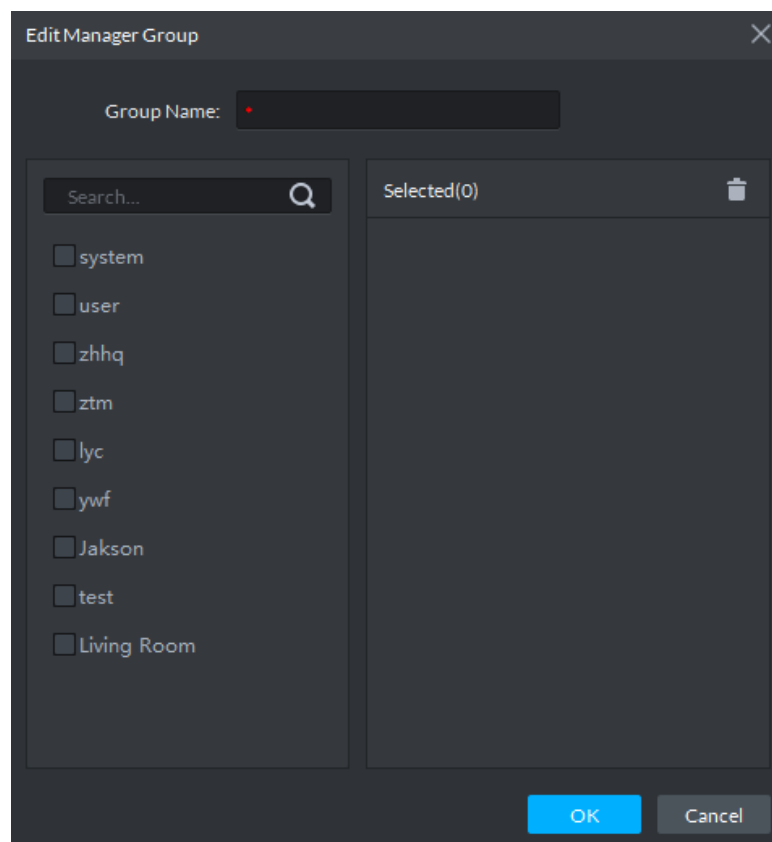
Step 3 Click Management Group Config.

Figure 5-332 Management group configuration



Step 4 Click **Add Group**.

Figure 5-333 Edit manager group



Step 5 Enter group name, select administrator account or VTS, and click **OK**.

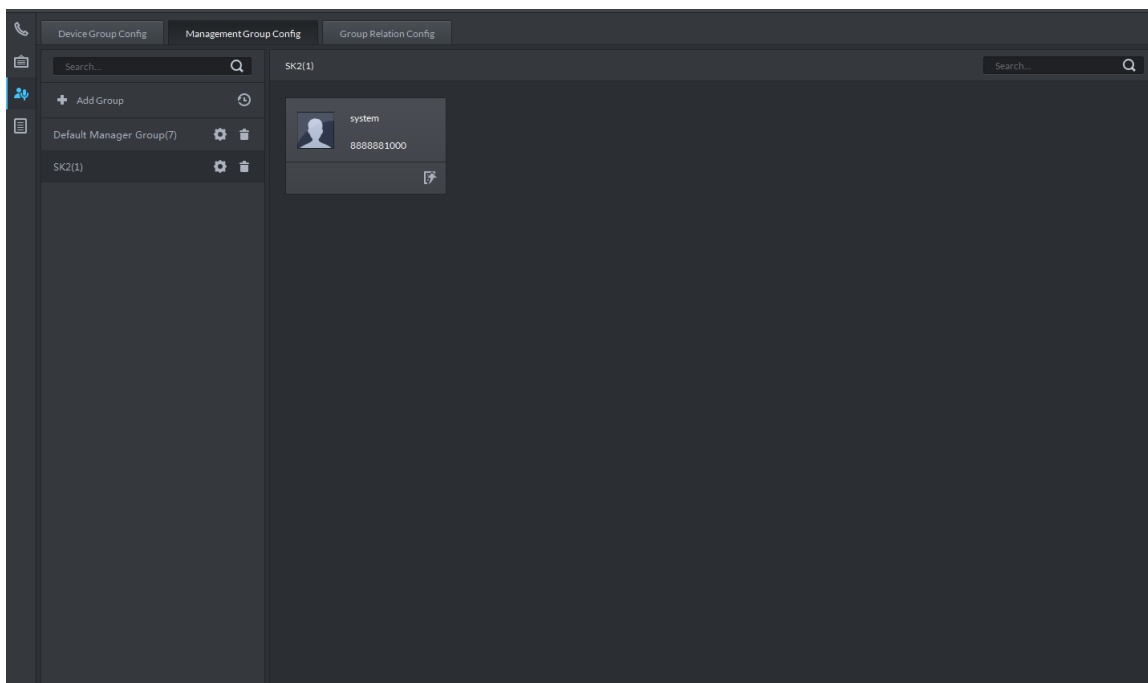


The members in management group support following operation.

- Transfer members, click  and move the member to the group.

- Manage group members, click  to add or delete group member.

Figure 5-334 Added management group




5.17.2.3 Group Relation Config

Relation group configuration means adding both device group and management group to the same relation group, making them related. Realize VTO or VTH only calling administration or VTS within the relation group.

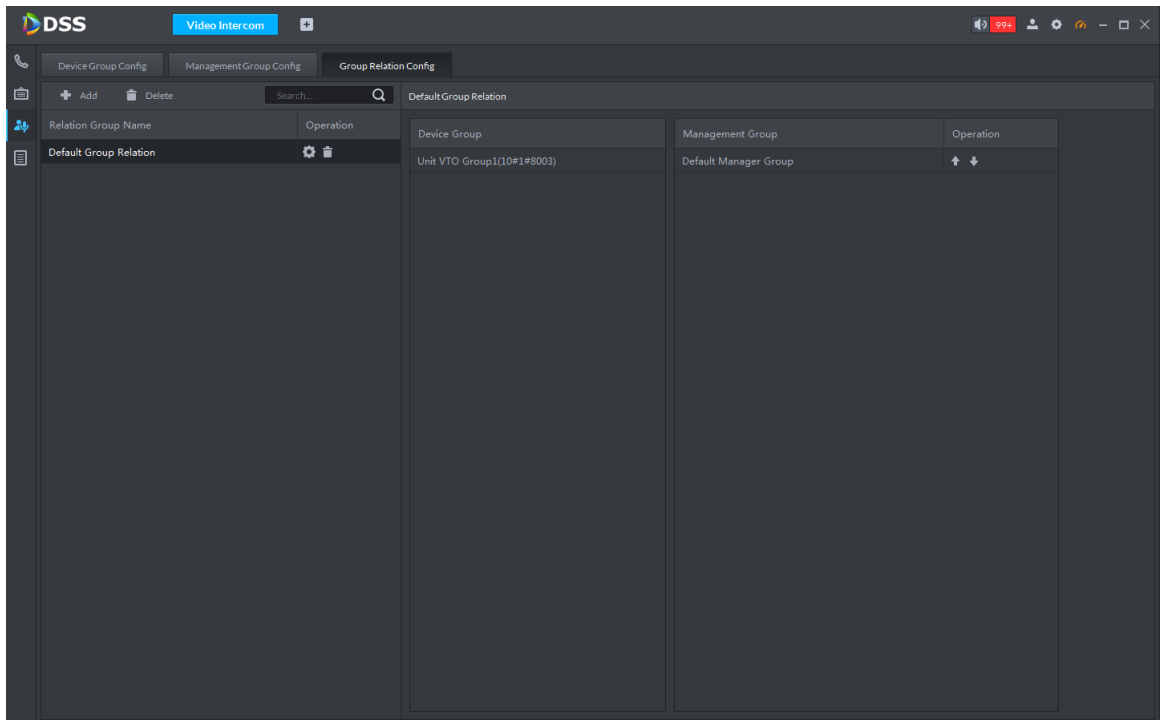
There are two situations for relation binding.

- 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 one 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 interface of **Video Intercom**.

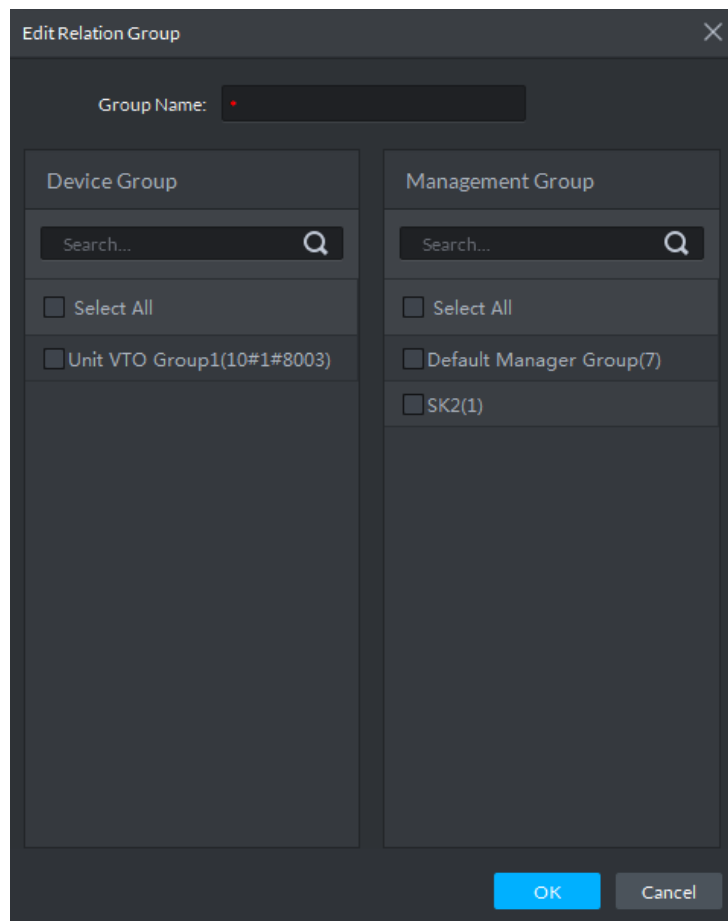
Step 2 Click the tab of **Relation Group Config**.

Figure 5-335 Relation group configuration



Step 3 Click **Add**.

Figure 5-336



Step 4 Enter name, select device group and management group, and then click **OK**.



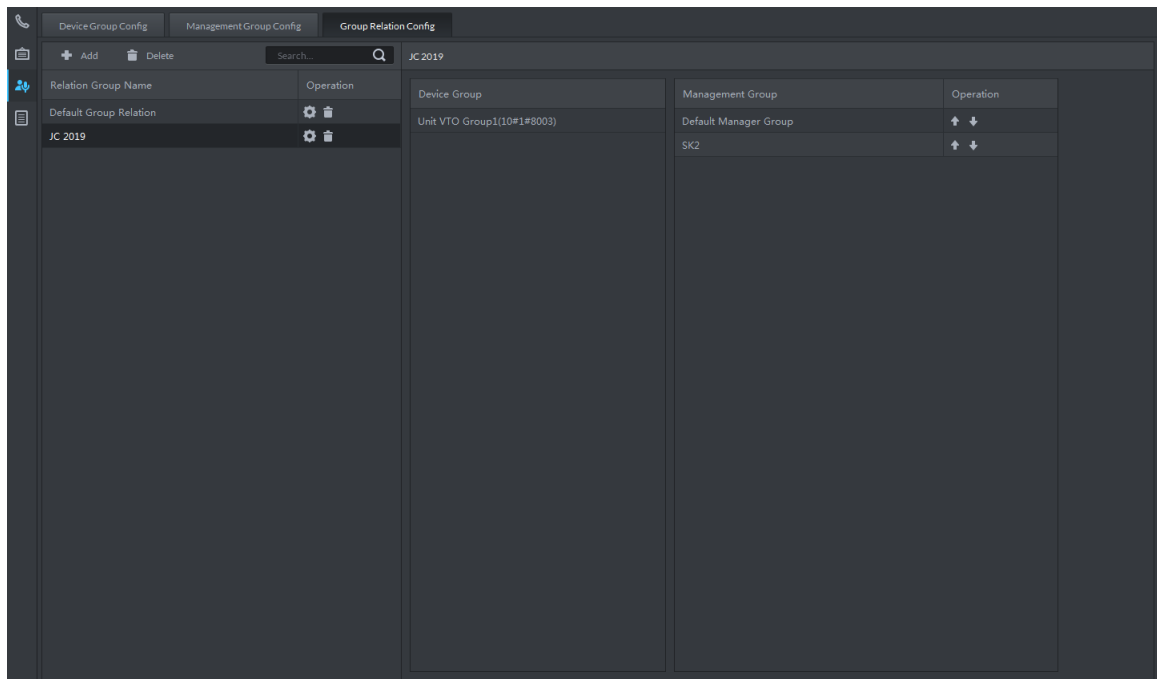
Added relation group is displayed in the list. If there are several relation groups, you can click  or  to adjust priority level. When there is call, the online administrators with high priority will generate ring bell first.

Figure 5-337 Added relation group



5.17.3 Video Intercom Application

5.17.3.1 Call Center

Realize call among the platform, VTO and VTH.


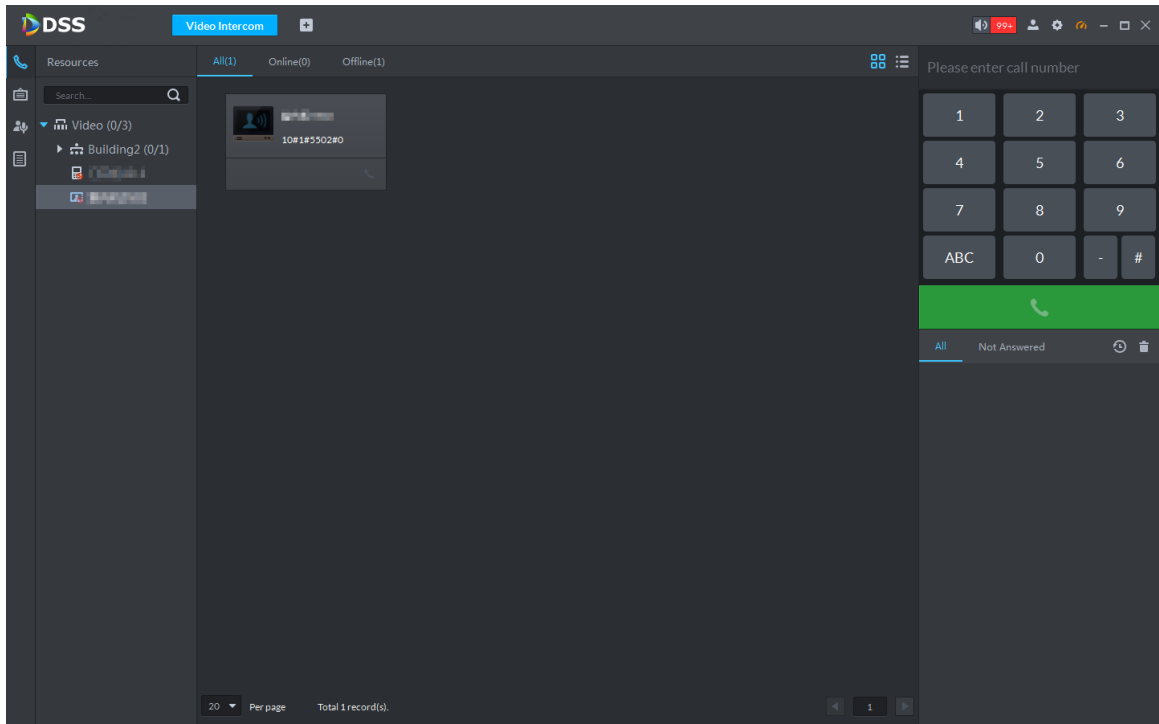

Step 1 Click  on the interface of **Video Intercom**.

Figure 5-338 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 and realize video talk. See Figure 5-339. Following operations are support during call.





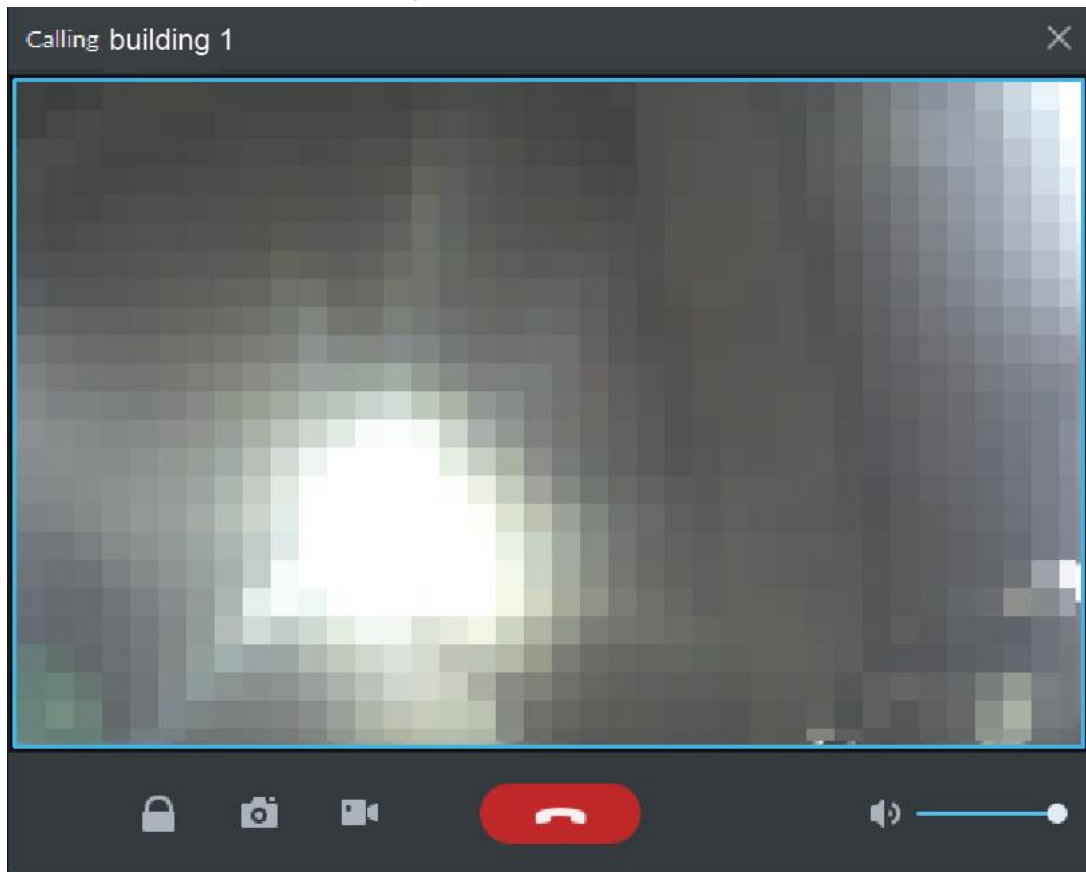

- ◇ , if VTO is connected to lock, click the icon to unlock.
- ◇ , click the icon to capture picture, the snapshot is saved into the default directory installed by client. If you need to modify the save path of snapshot, refer to "5.2 Local Configuration" for more details.
- ◇ , click the icon to start record, click again to stop record. The video is saved in default path installed by client. If you need to modify the save path, refer to "5.2 Local Configuration" for more details.
- ◇ , click the icon to hang up.

Figure 5-339 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 ...**, see Figure 5-340. There are two modes for answering the call.


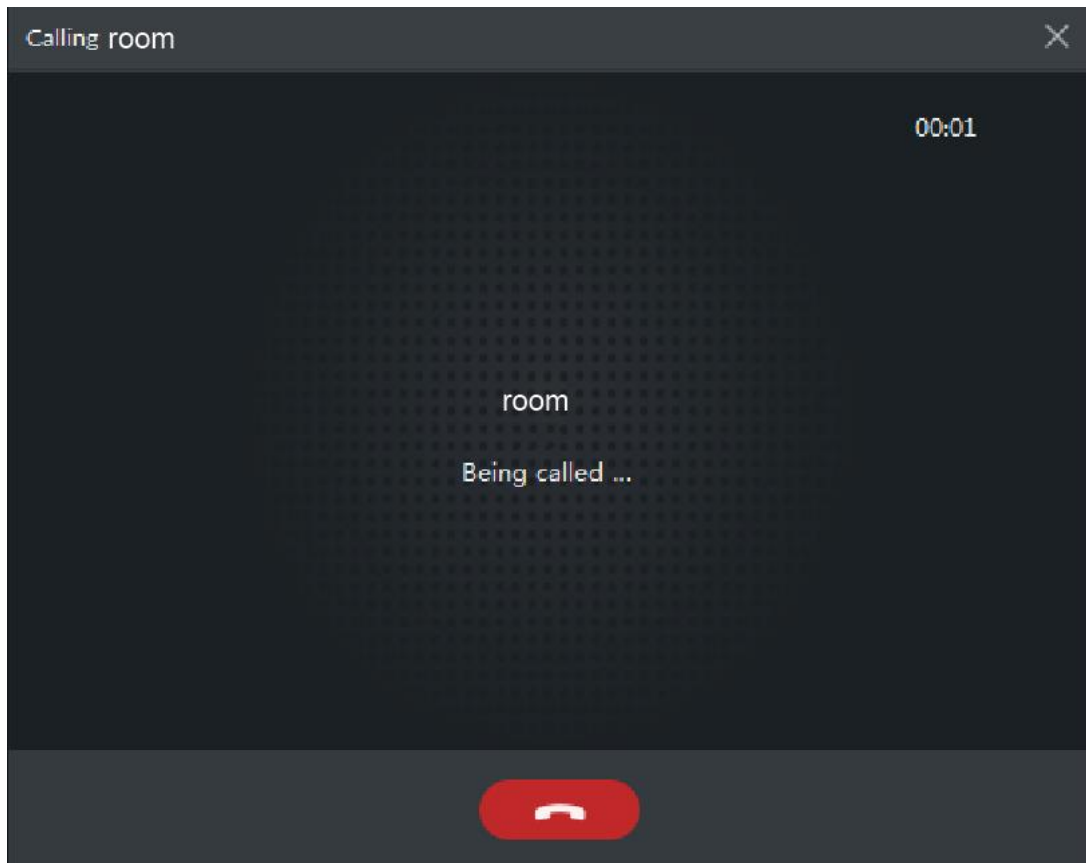
- ◇ Answer by VTH, bidirectional talk between client and VTH. Press  to hang up when you answer the call.
- ◇ If VTH fails to answer over 30s, busy or hang up directly, then it means the call is busy.

Figure 5-340 Calling






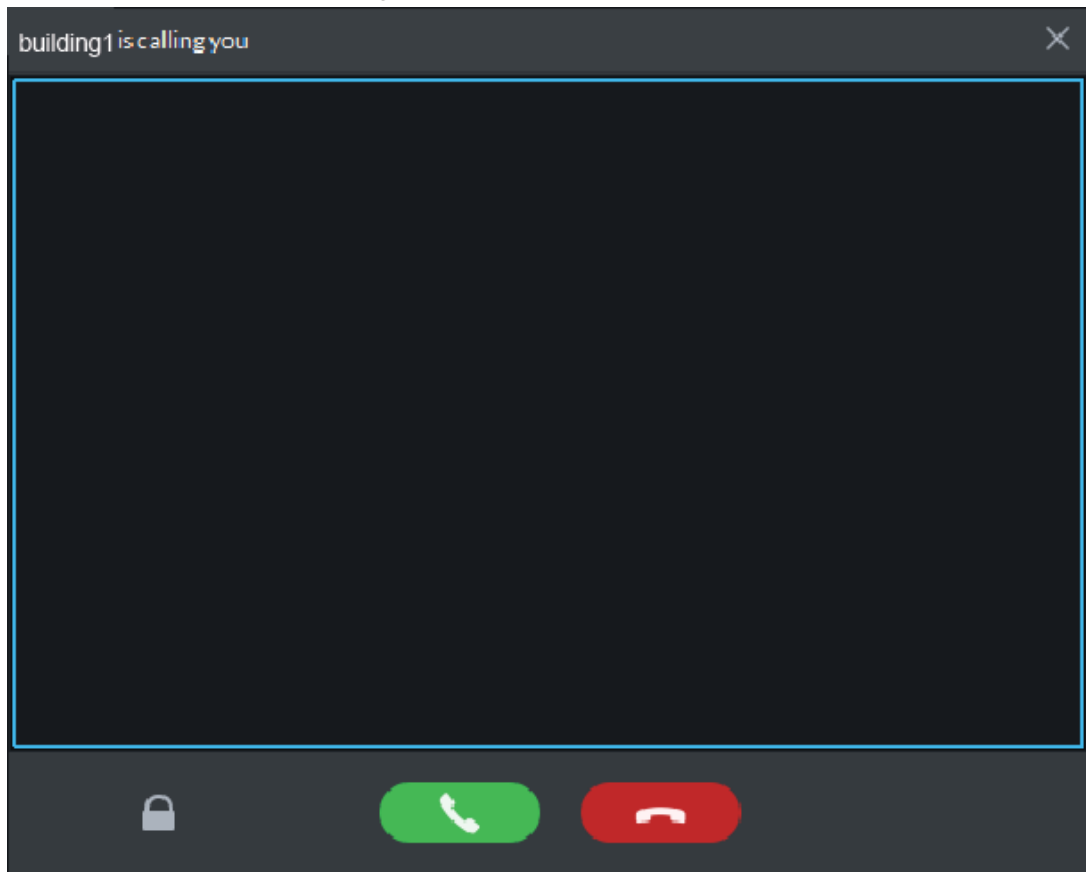

- Call from VTO to the platform
VTO calls the platform, client pops up the dialog box of VTO calling. See Figure 5-341.
 - ◇  , if VTO is connected to lock, click the icon to unlock.
 - ◇  , click the icon, answer VTO, realize mutual call after connected.
 - ◇  , click the icon to hang up.

Figure 5-341 VTO Call



- When VTH is calling the platform

The client pops out the dialog box of VTH calling. See Figure 5-342. Click  and realize talk with VTH.



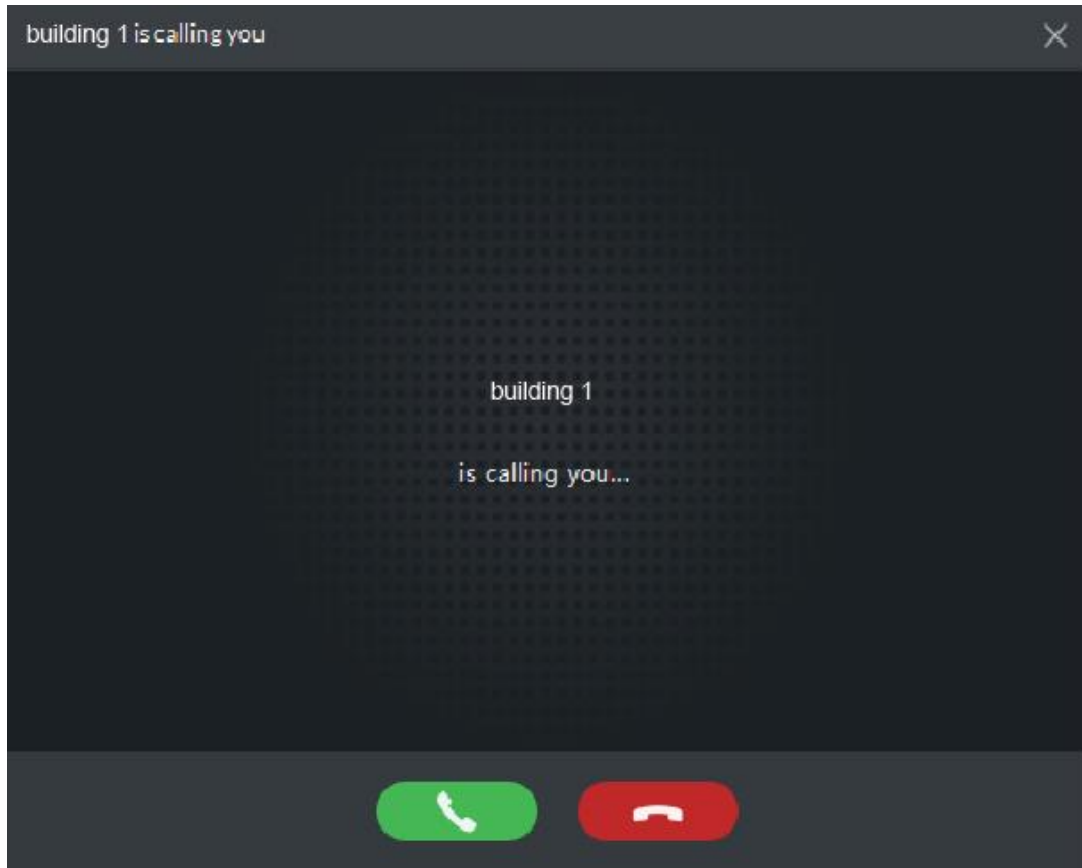
- ◇ , click the icon and answer VTO, realize mutual talk after connected.
- ◇ , click the icon and hang up.

Figure 5-342 VTH call




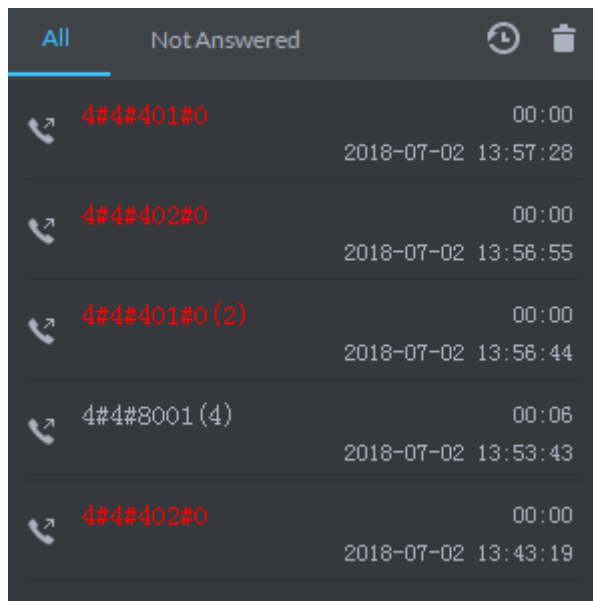
- Call through call records
All the call records are displayed in the **Call Record** at the lower right corner of the interface of **Video Intercom**. Move the mouse to the record, click  and call back.

Figure 5-343 Call records



5.17.3.2 Release Info

Send message to designated VTH.


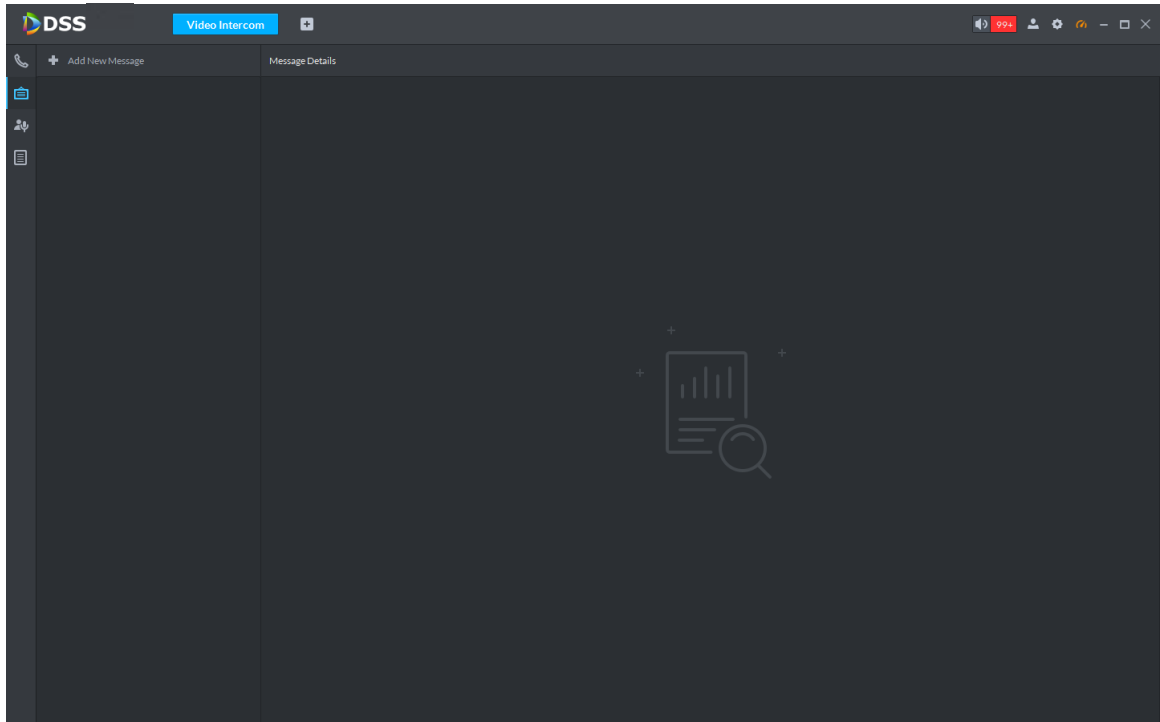
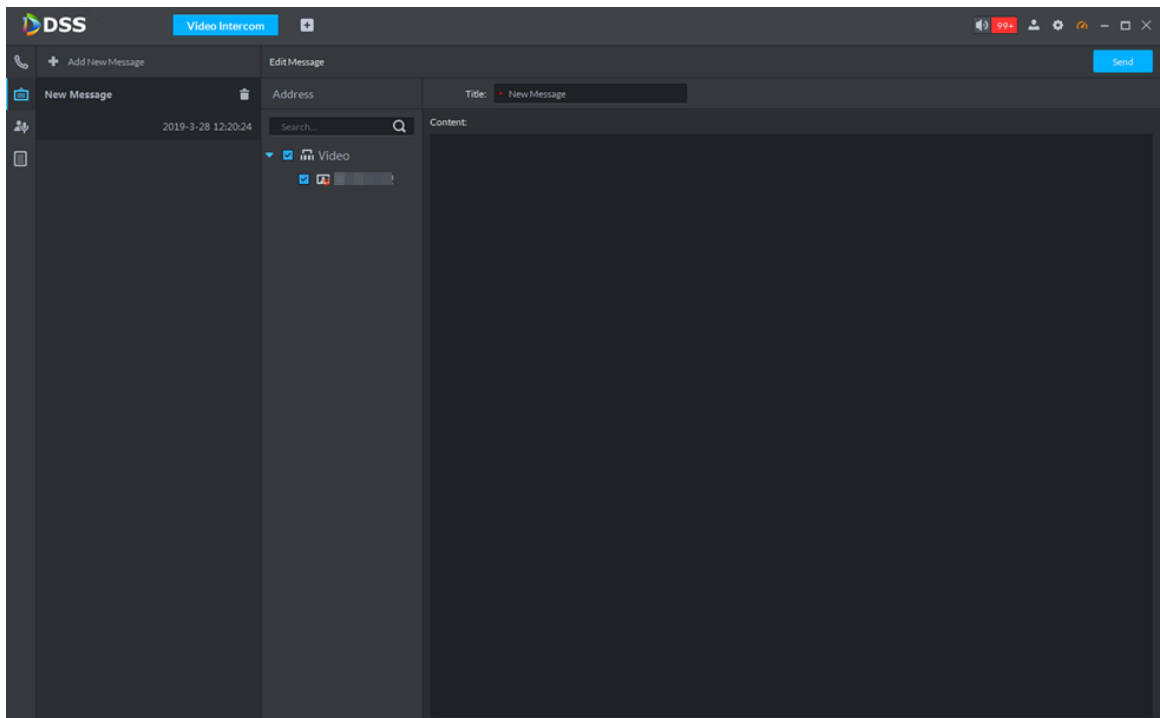
Step 1 Click  on the interface of **Video Intercom**.

Figure 5-344 Release interface



Step 2 Click **Add New Message**, select VTH and add release information.

Figure 5-345 Add new message



Step 3 Click **Send**.


The VTH will receive the message after it is sent successfully.

5.17.3.3 Search Video Intercom Log

View log records and you can trace recorded calls.

Step 1 Enter the interface of video intercom log.

The system supports following two ways to enter.

Step 2 Click  on the interface of **Video Intercom**.


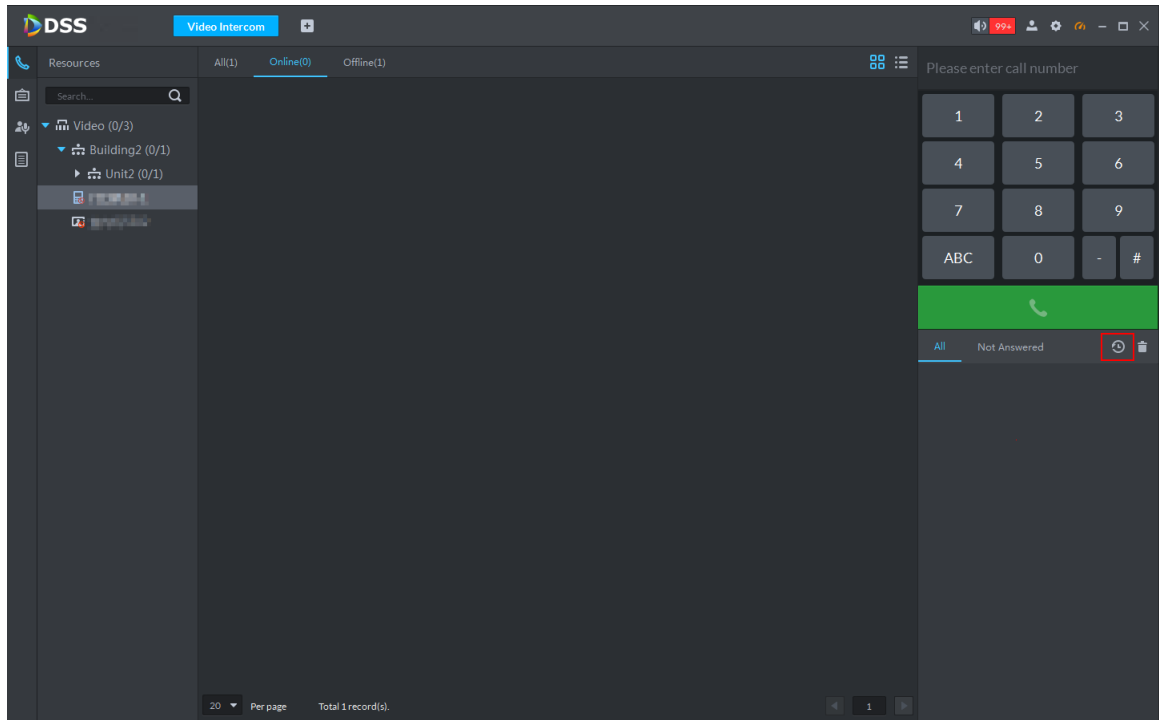
Step 3 Click  and enter console on the interface of **Video Intercom**.

Figure 5-346 Enter console



Step 4 Set conditions, and then click **Search**.

Figure 5-347 Logs

Device Name	Call Type	Room No.	Start Time	Talk Time	End Status
	Incoming	10#1#5502#0	2019-03-25 20:34:05	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:30:57	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:30:46	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:30:00	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:28:22	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:28:05	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:25:42	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:24:50	00:00	Missed
	Incoming	10#1#8003	2019-03-25 20:24:38	00:09	Received
	Incoming	10#1#5502#0	2019-03-25 20:20:50	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:19:55	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:18:34	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 20:18:18	00:00	Missed
	Outgoing	10#1#5502#0	2019-03-25 20:02:49	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 19:55:12	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 19:55:02	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 19:54:41	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 19:48:18	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 19:48:06	00:00	Missed
	Incoming	10#1#5502#0	2019-03-25 19:47:59	00:00	Missed

Step 5 Click **Export** and the logs will be saved locally according to system prompt.

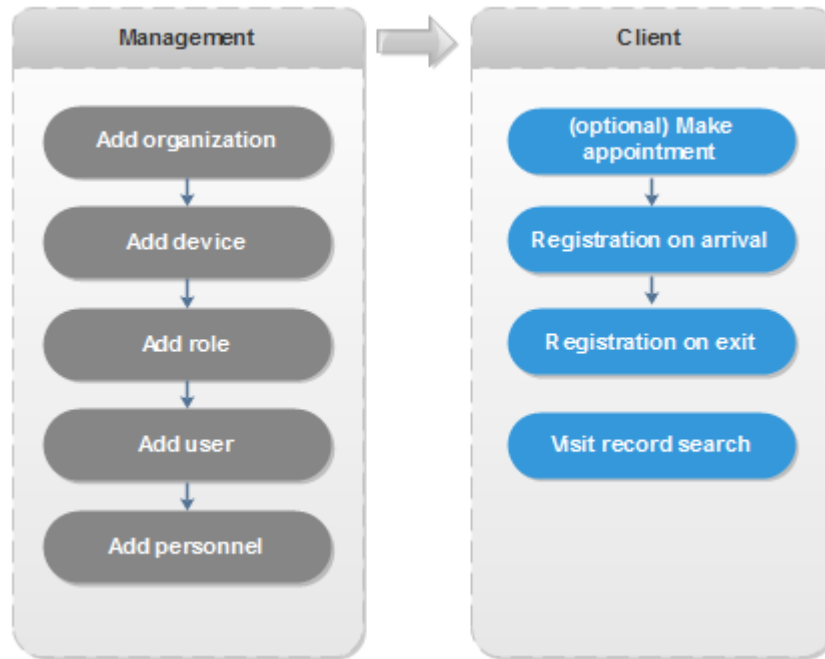
5.18 Visitor Management

After appointment is made on platform, and visitor is registered in the company, then you can have access permission. Access permission is disabled when leaving the company.

5.18.1 Preparations

- Access control devices have been added into the system. For details, see "4.5 Adding Device."
- Personnel list have been added into the system. For details, see "5.14 Personnel Management."

Figure 5-348 Visitor management business flow



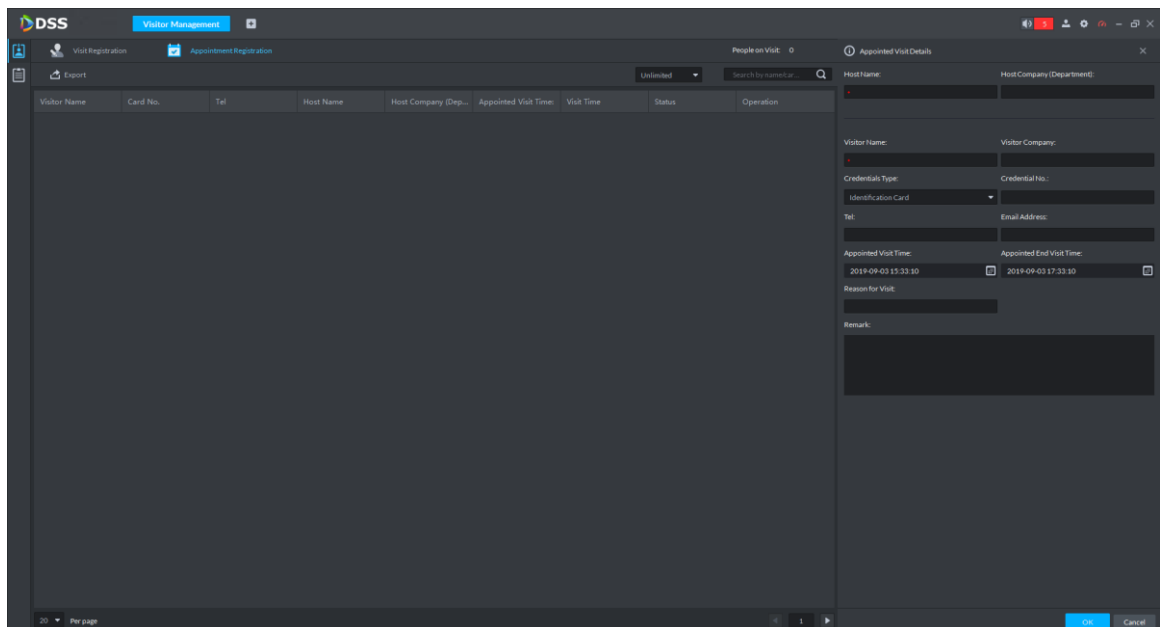
5.18.2 Visitor Appointment

Record visitor information on the platform.

Step 1 On client homepage, click **Visitor Management**.

Step 2 Click **Appointment Registration**.

Figure 5-349 Appointment registration

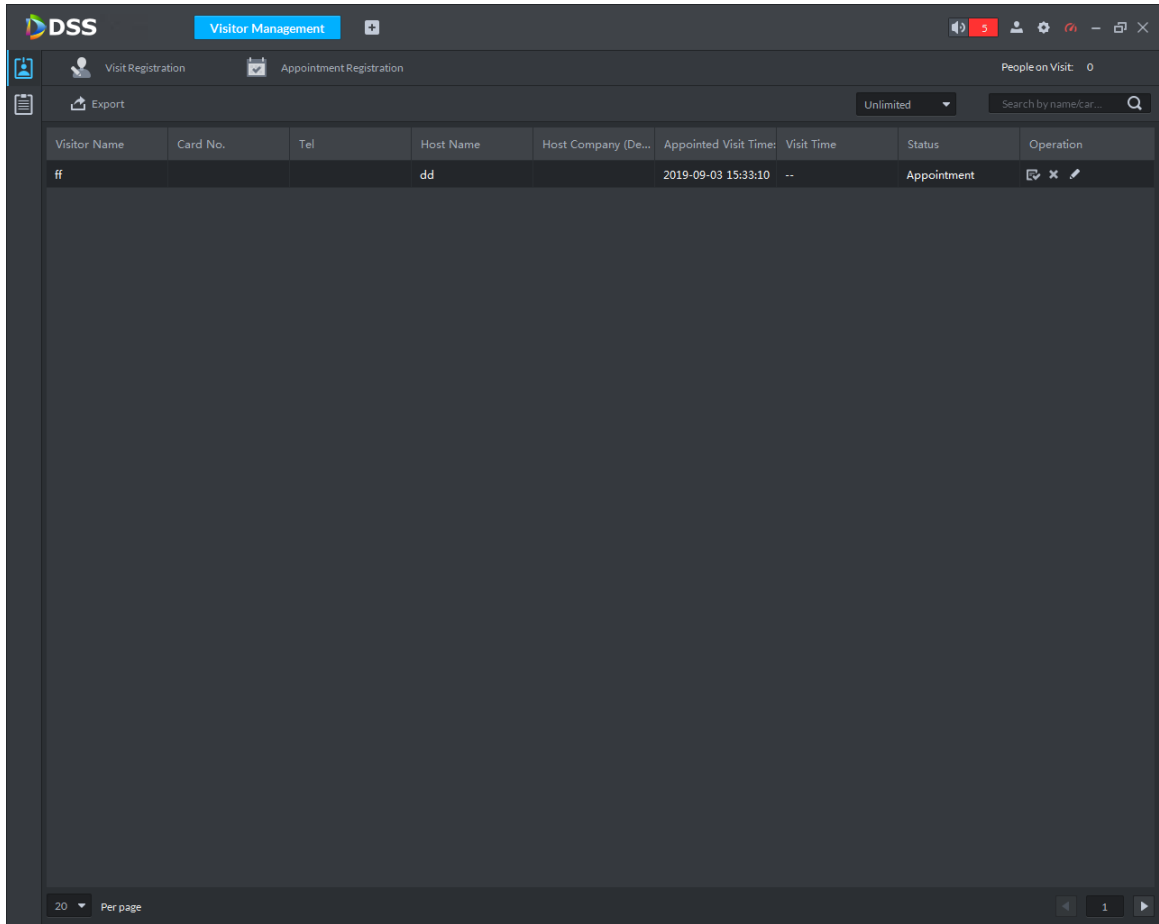


Step 3 Enter visitor and some other information, and then click **OK**.



Click  and skip to visit registration interface.

Figure 5-350 Appointed visitor info



The screenshot shows the DSS Visitor Management interface. At the top, there is a navigation bar with 'DSS' and 'Visitor Management'. Below this, there are tabs for 'Visit Registration' and 'Appointment Registration'. The main area displays a table with the following columns: Visitor Name, Card No., Tel, Host Name, Host Company (De...), Appointed Visit Time, Visit Time, Status, and Operation. The table contains one row with the following data: Visitor Name: ff, Card No.: , Tel: , Host Name: dd, Host Company (De...): , Appointed Visit Time: 2019-09-03 15:33:10, Visit Time: --, Status: Appointment, and Operation: [edit, delete, refresh icons]. The interface also includes an 'Export' button, a search bar, and a 'People on Visit: 0' indicator.

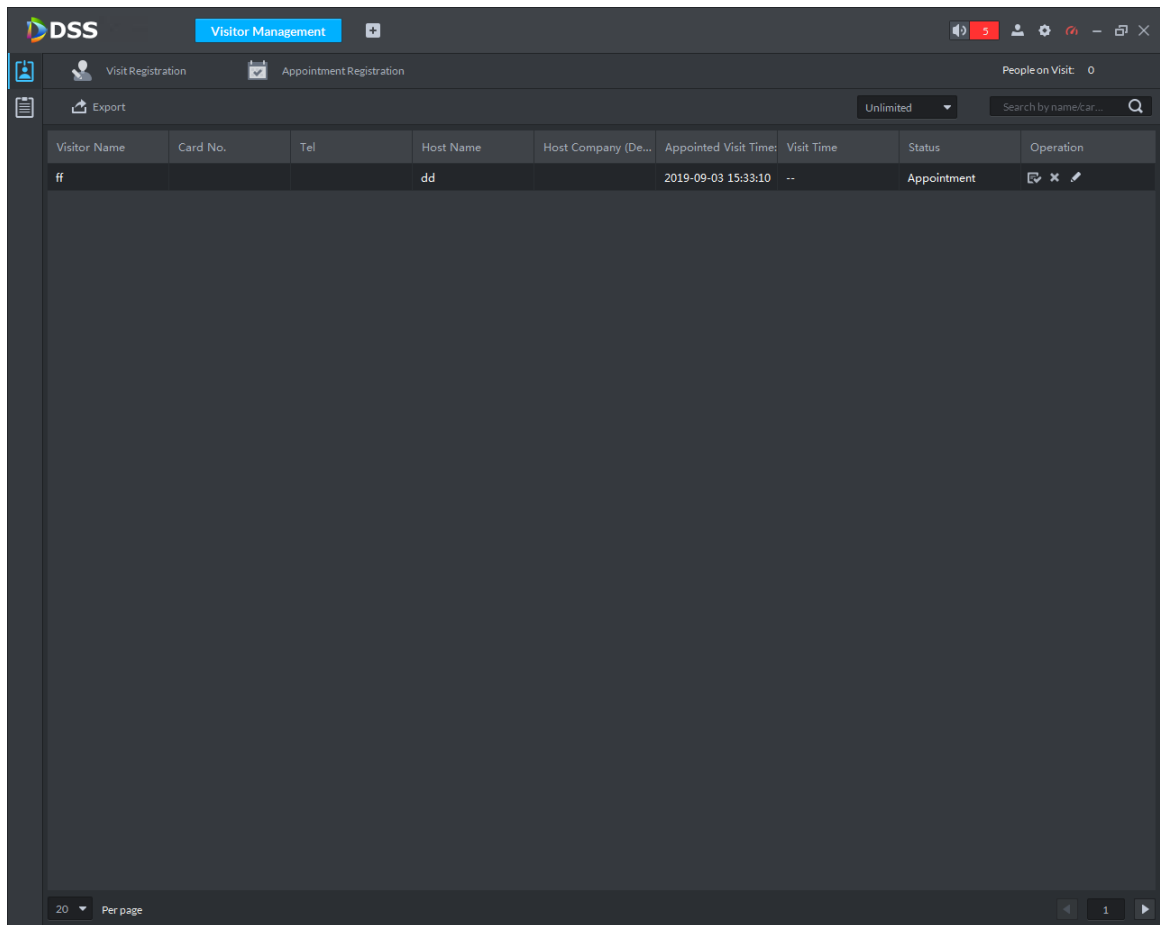
Visitor Name	Card No.	Tel	Host Name	Host Company (De...	Appointed Visit Time	Visit Time	Status	Operation
ff			dd		2019-09-03 15:33:10	--	Appointment	[edit] [delete] [refresh]

5.18.3 Visit Registration

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 temporary visitor. Visitors can get access by swiping card or face recognition.


Step 1 On **Visitor Management** interface, click .

Figure 5-351 Visitor management



Step 2 Get into the visit registration information interface.

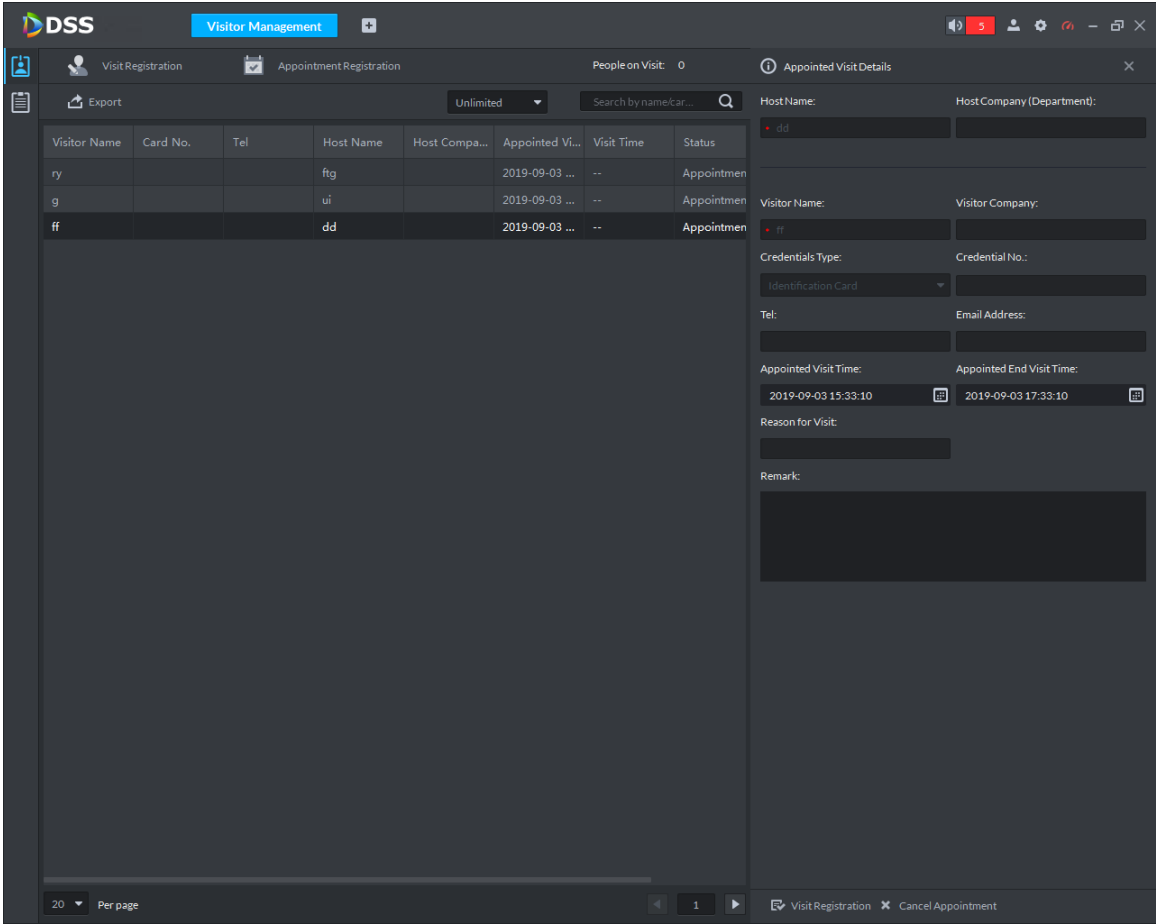
- If a visitor is appointed

Find the visitor information, and then double-click . The visitor registration details are displayed. See Figure 5-352.

- If a visitor is not appointed

Click **Visit Registration**, the visitor registration details interface is displayed. You need to enter the appointment information manually.

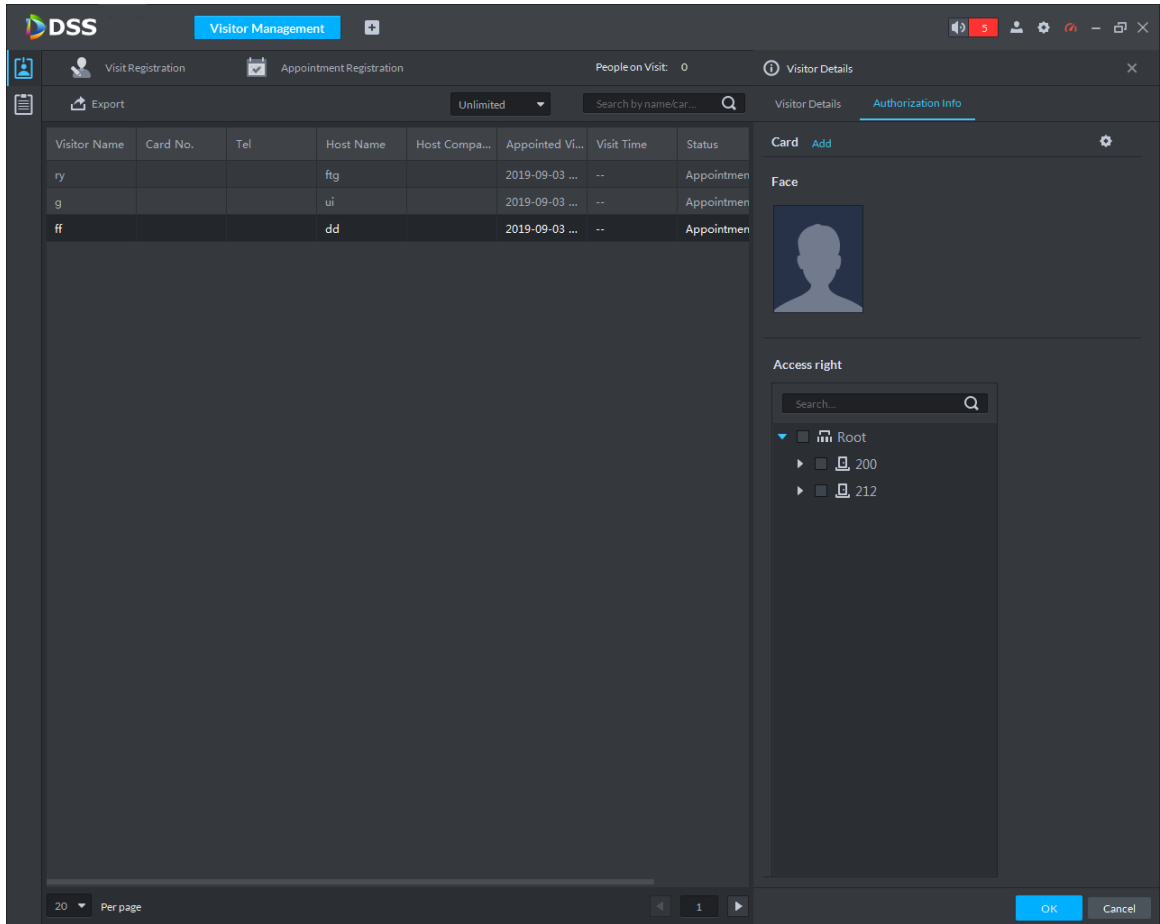
Figure 5-352 Visit information



Step 3 Double-click , and then click  at the bottom.

Step 4 Click the **Authorization information** tab.

Figure 5-353 Visitor authorization

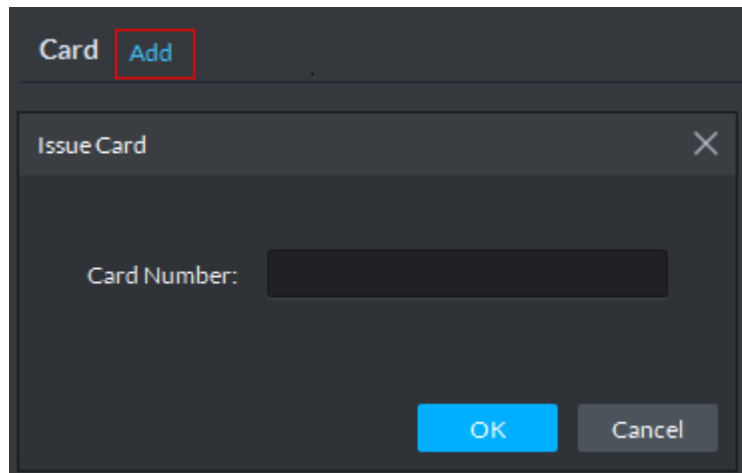


Step 5 Issue cards.

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
- 1) Click **Add** next to **Card**.

Figure 5-354 Add a card

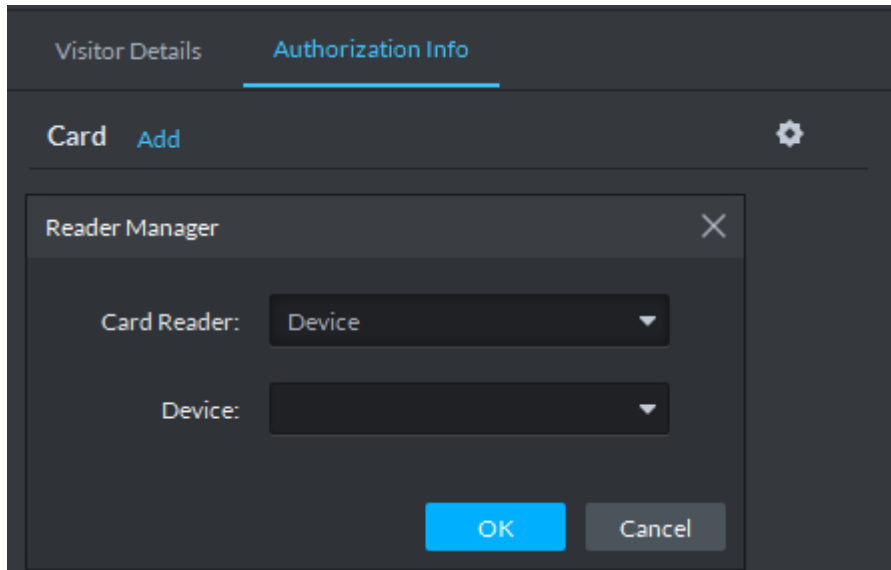


- 2) Enter a card number, click **OK**, and the card is issued.

- Issue card by using a card reader

1) Click .

Figure 5-355 Reader manager

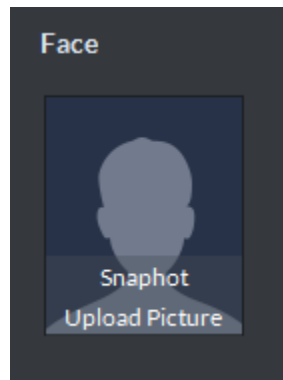


- 2) Select a card reader or device, and then click **OK**.
- 3) Swipe card on reader or device, and card is issued.

Step 6 Move your mouse cursor over the face snapshot area, click **Snapshot**, and then you can take a face snapshot.

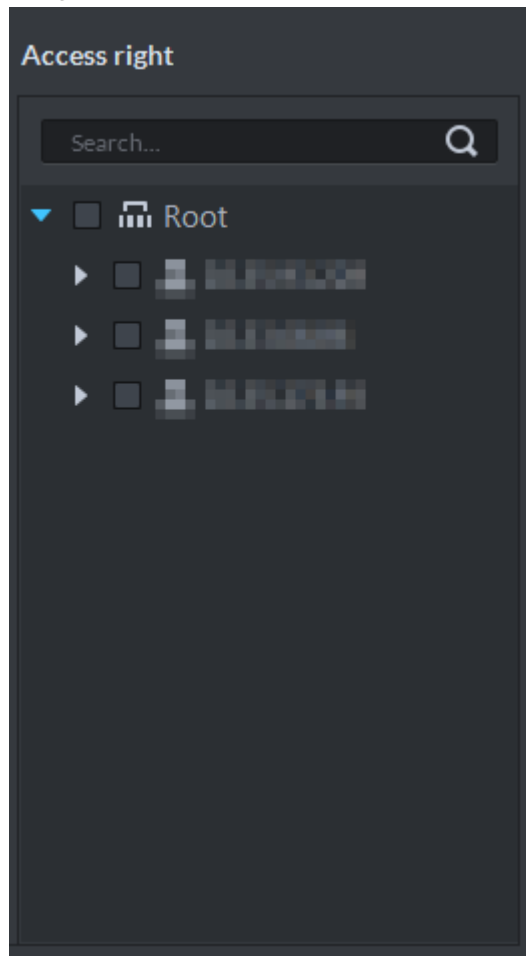
The face snapshot is used for face recognition and door control.

Figure 5-356 Take a face snapshot



Step 7 In **Access Right** area, select a channel that the visitor can pass.

Figure 5-357 Select a channel



Step 8 Click **OK** to complete visitor registration.





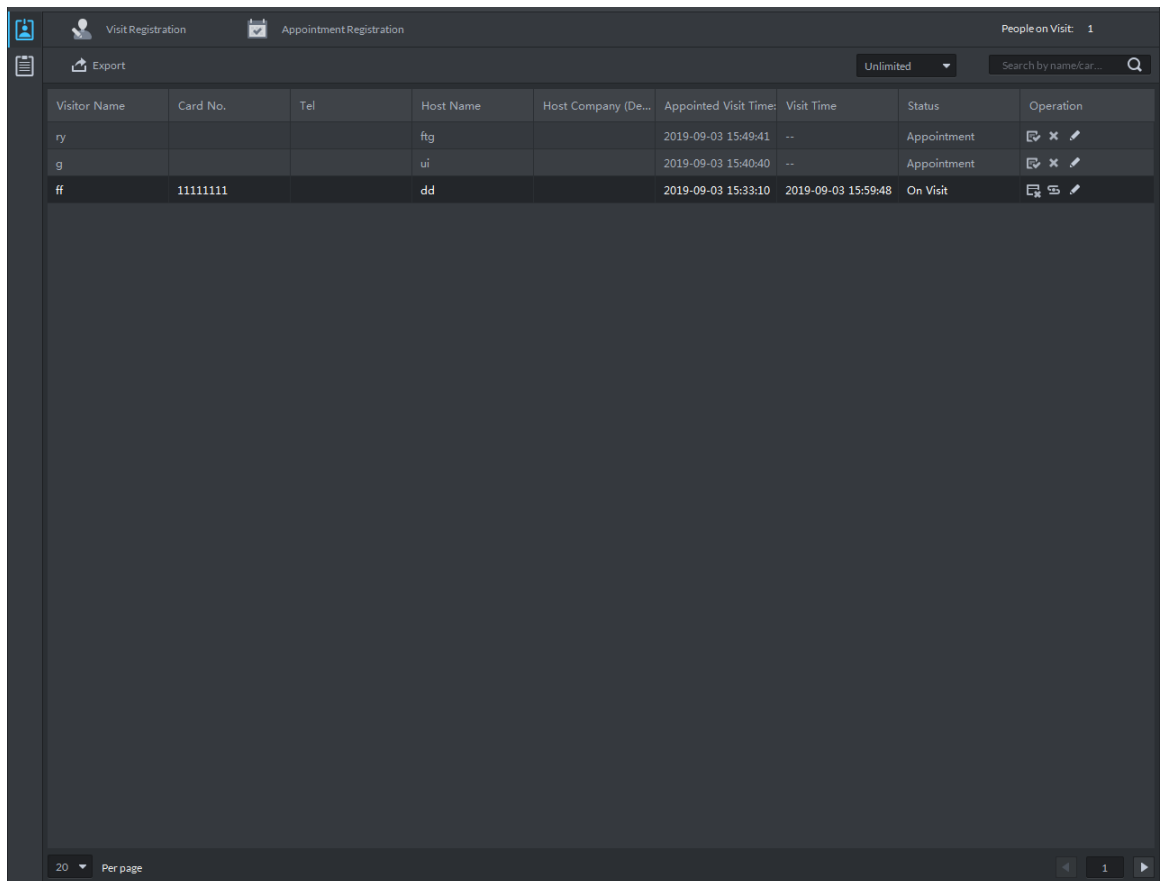









- Click  and skip to the **End Visit** interface.
- Click  and view visitor card swiping records.

Figure 5-358 Visit registration



The screenshot shows a software interface for visit registration. At the top, there are tabs for 'Visit Registration' and 'Appointment Registration'. The 'Visit Registration' tab is active. In the top right corner, it says 'People on Visit: 1'. Below the tabs, there is an 'Export' button and a search bar with the text 'Search by name/Card No...'. The main area contains a table with the following data:

Visitor Name	Card No.	Tel	Host Name	Host Company (De...	Appointed Visit Time	Visit Time	Status	Operation
ry			ftg		2019-09-03 15:49:41	--	Appointment	  
g			ui		2019-09-03 15:40:40	--	Appointment	  
ff	11111111		dd		2019-09-03 15:33:10	2019-09-03 15:59:48	On Visit	  

At the bottom left, there is a dropdown menu set to '20' and the text 'Per page'. At the bottom right, there are navigation arrows and the page number '1'.

5.18.4 End Visit Registration

When visitors are leaving, close their access permissions.

Step 1 On the **Visitor Management** interface, click .


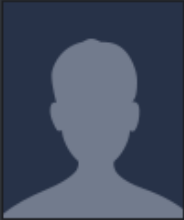
Step 2 Find the appointment record of the visitor, and then click .

Figure 5-359 End visit

Host Name:	Host Company (Department):	
dd	--	
	Visitor Name:	Reason for Visit:
	ff	--
	Tel:	Visitor Company:
	--	--
	Visit Time:	Email Address:
	2019-09-03 15:59:48	--
	Credentials Type:	Remark:
	Identification Card	--
	Credential No.:	
	--	

Step 3 Click **OK** to close the access permission.

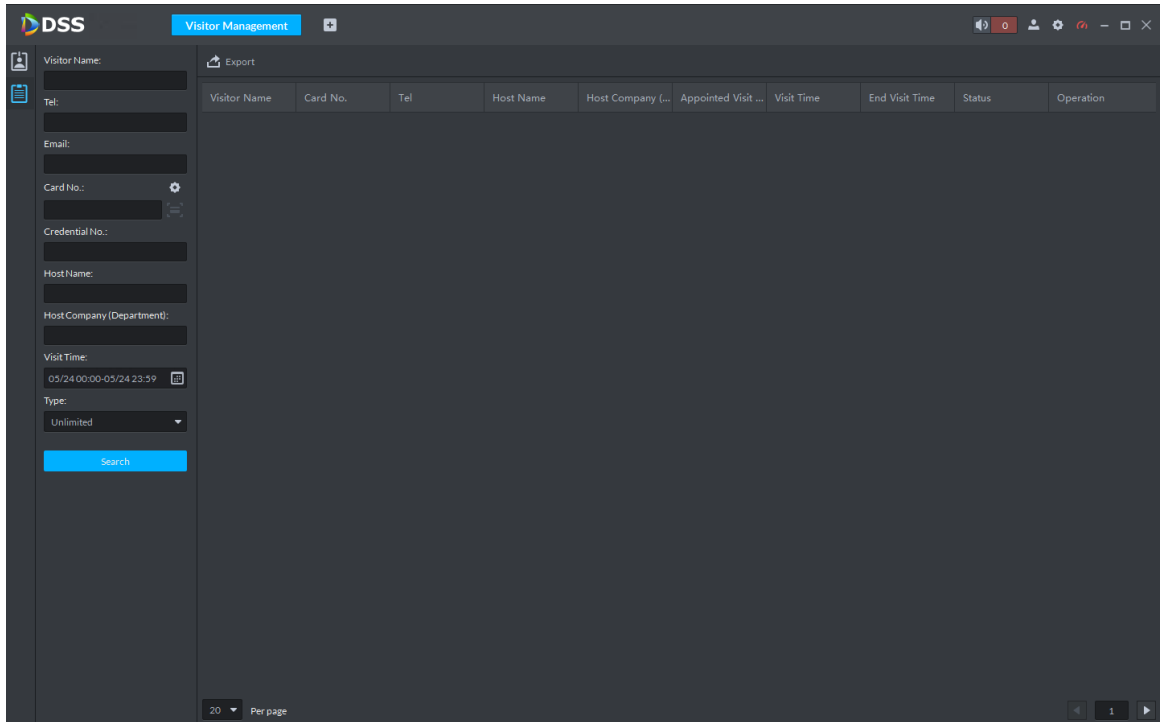
If you have issued a card to visitor, make sure the card is returned when the visitor leaves.

5.18.5 Searching for Visit Records

Search for visit records, and view visitor details and the card swiping records.

Step 1 On **Visitor Management** interface, click .

Figure 5-360 Visit record



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




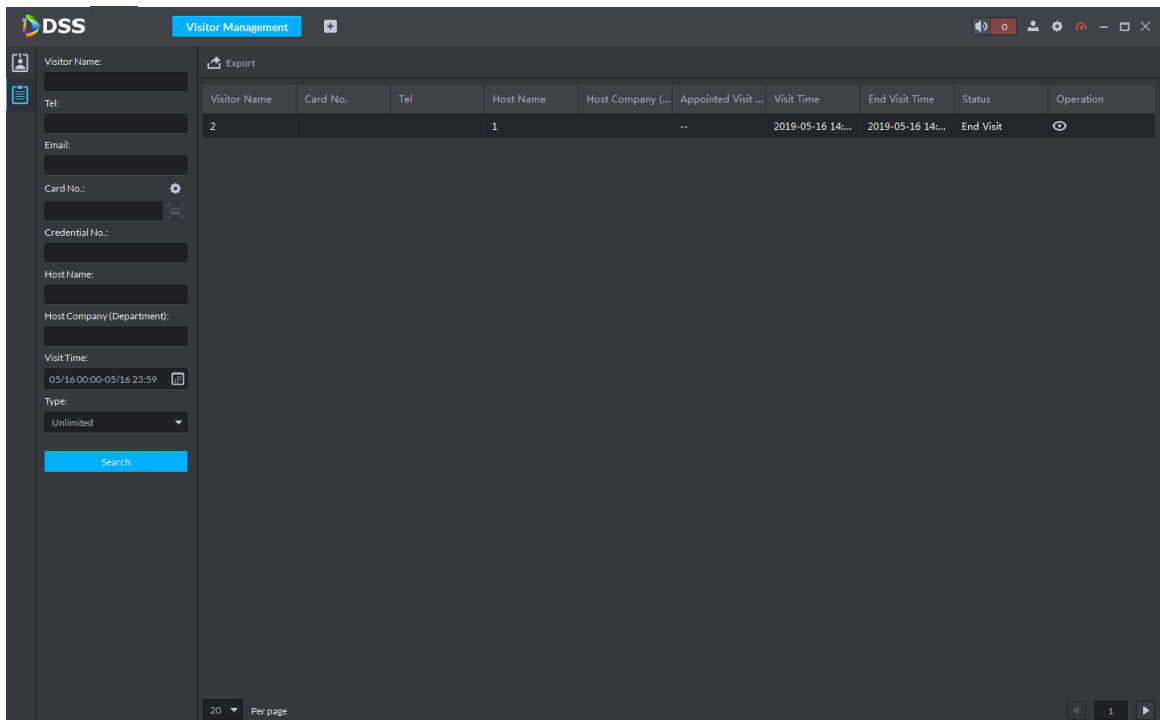

In addition to entering card number manually, you can also click , select a card reader and then get the card number by swiping card.

Figure 5-361 Search visit result



Step 3 Click  to view visitor details and card swiping records.

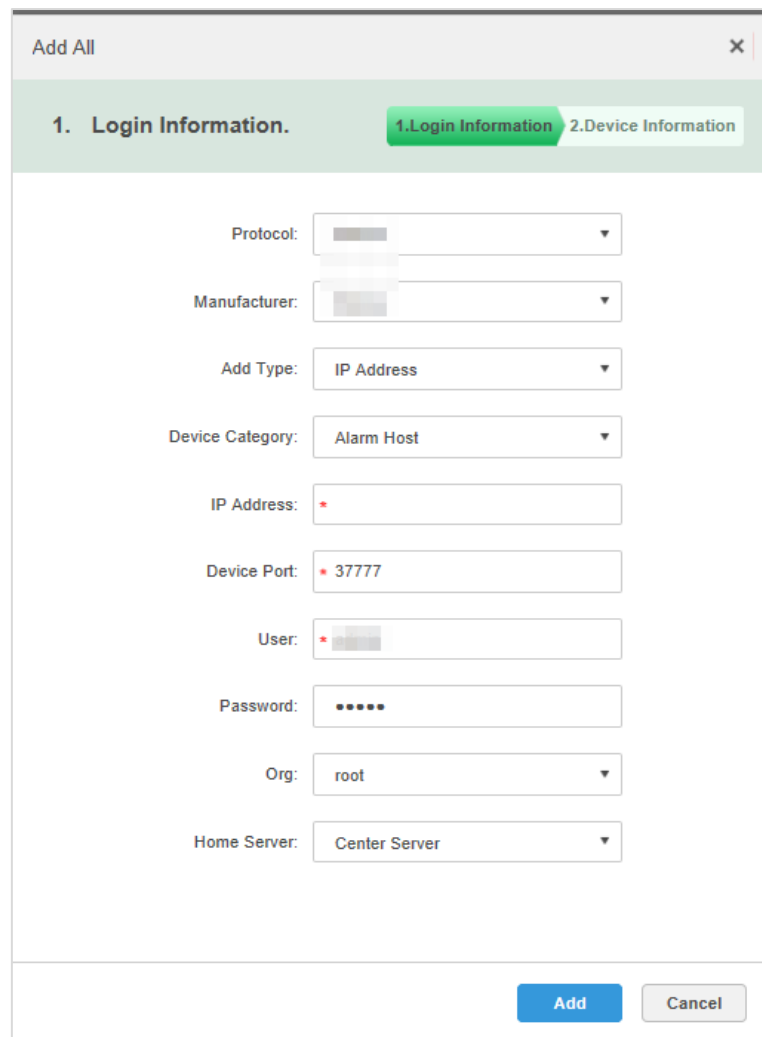
5.19 Alarm Controller

After adding alarm controllers to platform, you can manage and configure alarm zones and sub systems centrally.

5.19.1 Preparations

- Alarm controllers have been added into the system. See Figure 5-362. For details, see "4.5 Adding Device."

Figure 5-362 Add an alarm controller



The screenshot shows a web-based configuration window titled "Add All" with a close button in the top right corner. The window is divided into two tabs: "1. Login Information." (which is the active tab) and "2. Device Information". Under the "1. Login Information." tab, there are several form fields:

- Protocol:** A dropdown menu.
- Manufacturer:** A dropdown menu.
- Add Type:** A dropdown menu with "IP Address" selected.
- Device Category:** A dropdown menu with "Alarm Host" selected.
- IP Address:** A text input field with a red asterisk indicating a required field.
- Device Port:** A text input field containing "37777" and a red asterisk.
- User:** A text input field with a red asterisk.
- Password:** A password input field with dots.
- Org:** A dropdown menu with "root" selected.
- Home Server:** A dropdown menu with "Center Server" selected.

At the bottom right of the window, there are two buttons: a blue "Add" button and a grey "Cancel" button.

- Modify zone types. For example, if a zone is a smoke sensor, select **Smoke Sensor** as the alarm type. See Figure 5-363. The alarm types can be customized. Select **Customized Alarm Type** in the **Alarm Type** dropdown list and then set the type details as needed. After alarm type configuration, you can configure the corresponding event types for the zones.

Figure 5-363 Set zone type

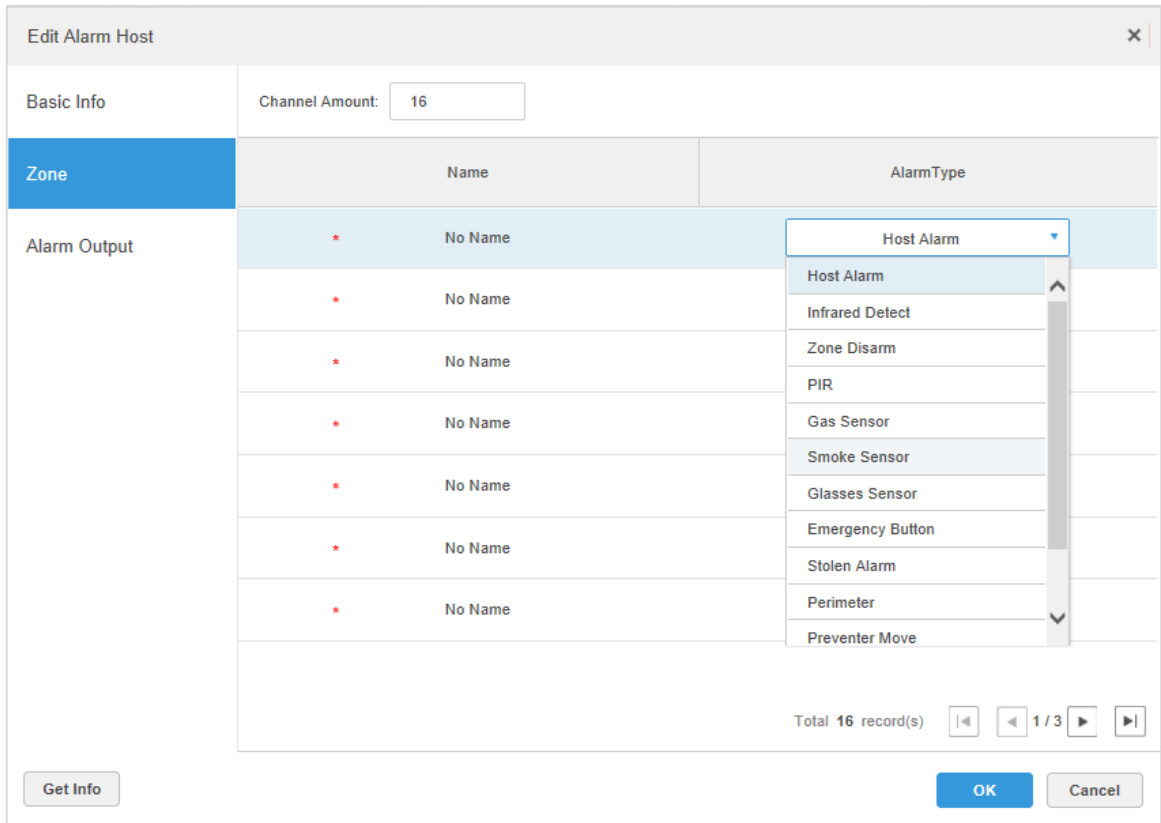
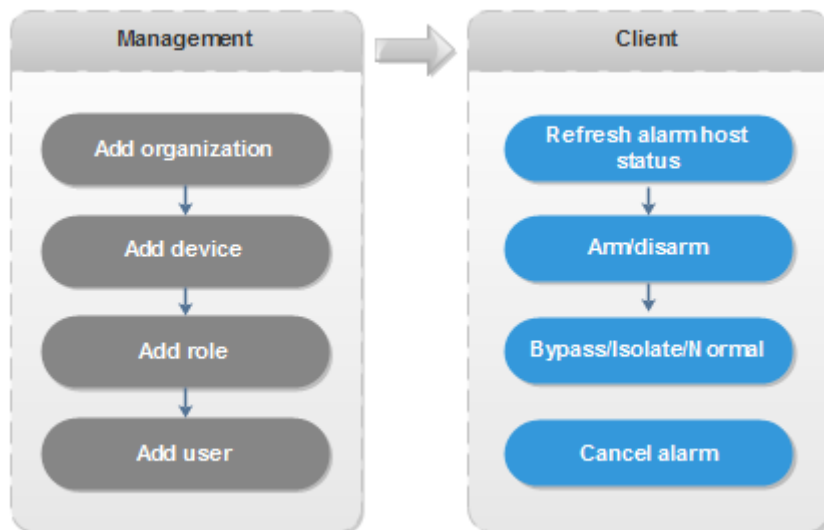


Figure 5-364 Alarm controller management flow



5.19.2 Alarm Controller Interface

Click , and then select **Alarm Controller** on the client homepage.

Figure 5-365 Alarm controller interface

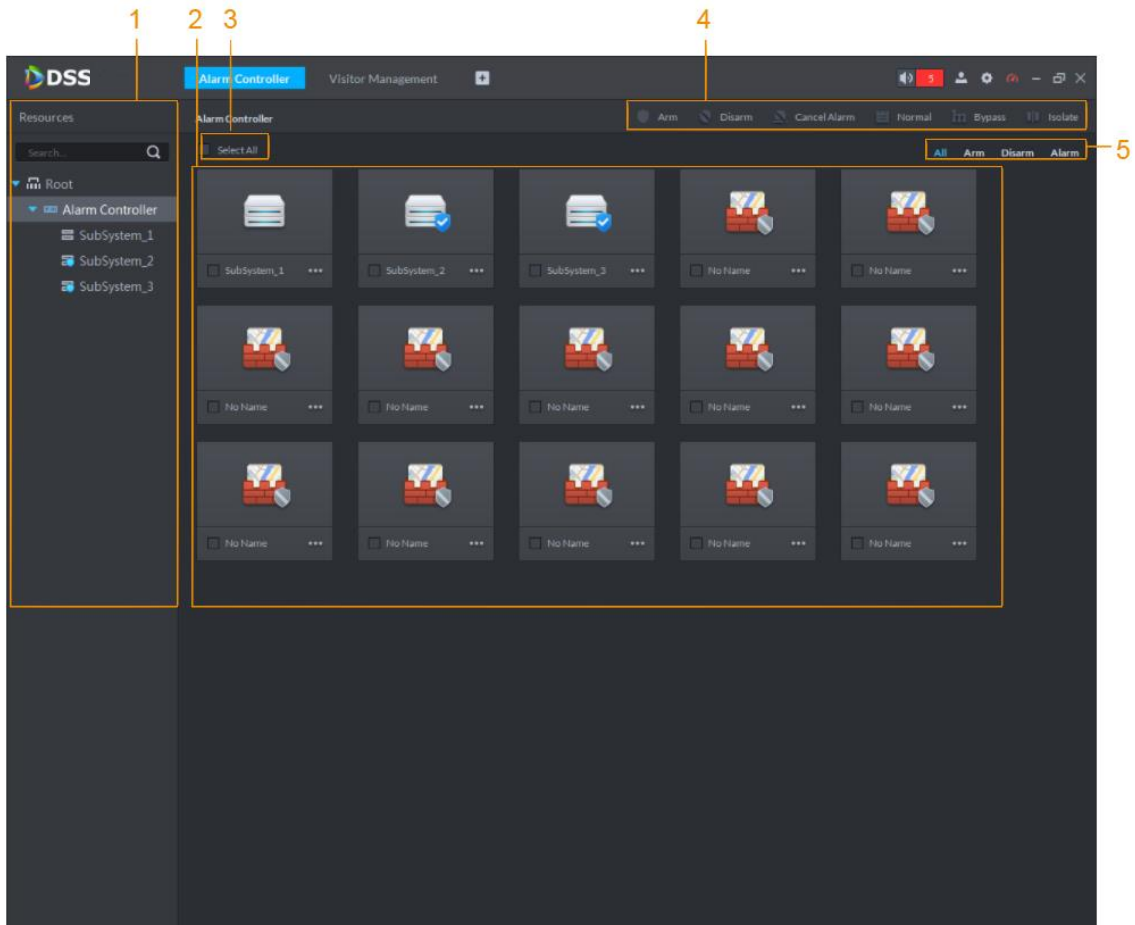













Table 5-65 Alarm controller interface description

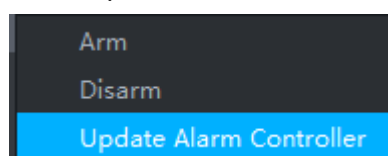
No.	Name	Description
1	Device list	<p>Display all alarm controller devices and subsystems under device. Icon status of subsystem</p> <ul style="list-style-type: none"> , no zone under subsystem. , zone exists under subsystem <p></p> <p>The subsystem and zone information displayed on platform can be acquired 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.

5.19.3 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 5-366 Update alarm controller



5.19.4 Alarm Controller Operation

5.19.4.1 Arming/Disarming

A zone detects and reports alarms only when it is armed. After being disarmed, a zone will not upload alarms any more.

5.19.4.1.1 Global Arming/Disarming

Globally arm or disarm all zones under an alarm controller.

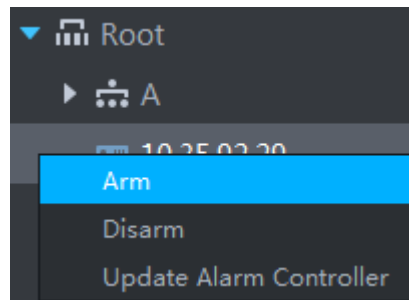
Arming

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.

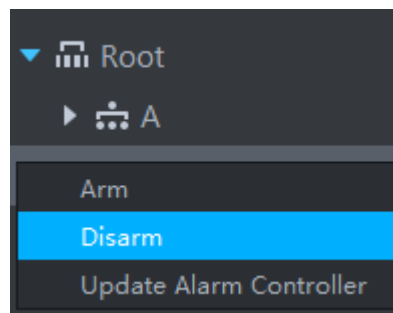
Figure 5-367 Global arm



Disarming

In device tree area, right-click the alarm controller that needs to be disarmed globally, and then select **Disarm**.

Figure 5-368 Global disarm



5.19.4.1.2 Arming/Disarming a Zone/Subsystem

Arm or disarm a single zone or subsystem.

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, 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 5-369 Arm a zone

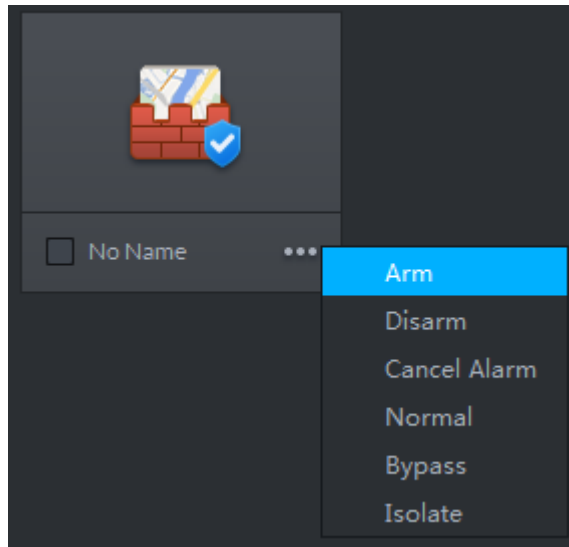
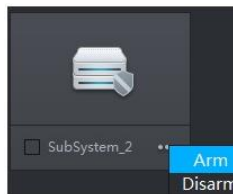
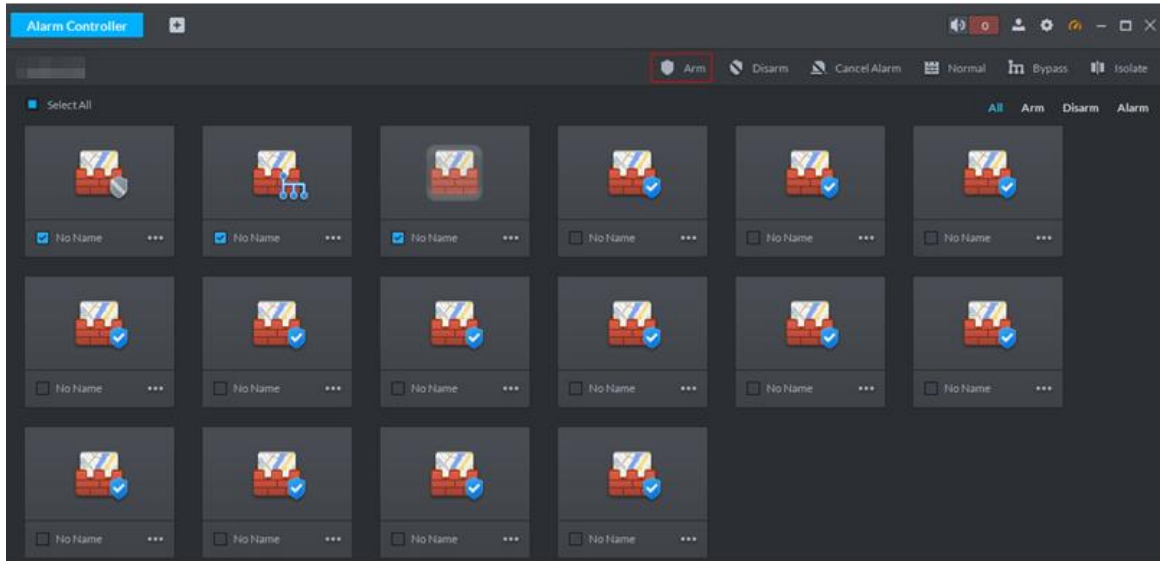


Figure 5-370 Arm a subsystem



- Select the zone or subsystem you want to arm (multiple choice supported), and then click **Arm** on the top of the interface.

Figure 5-371 Arm



Disarming

Supports disarming by the following two methods.


- Click the zone you want to disarm or  of the corresponding subsystem, and then select **Disarm**.

Figure 5-372 Disarm a zone

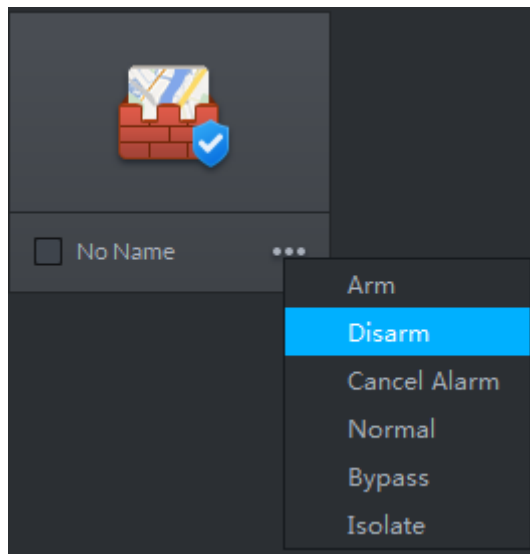
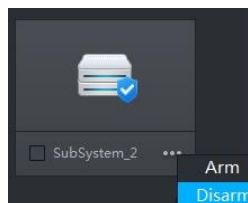
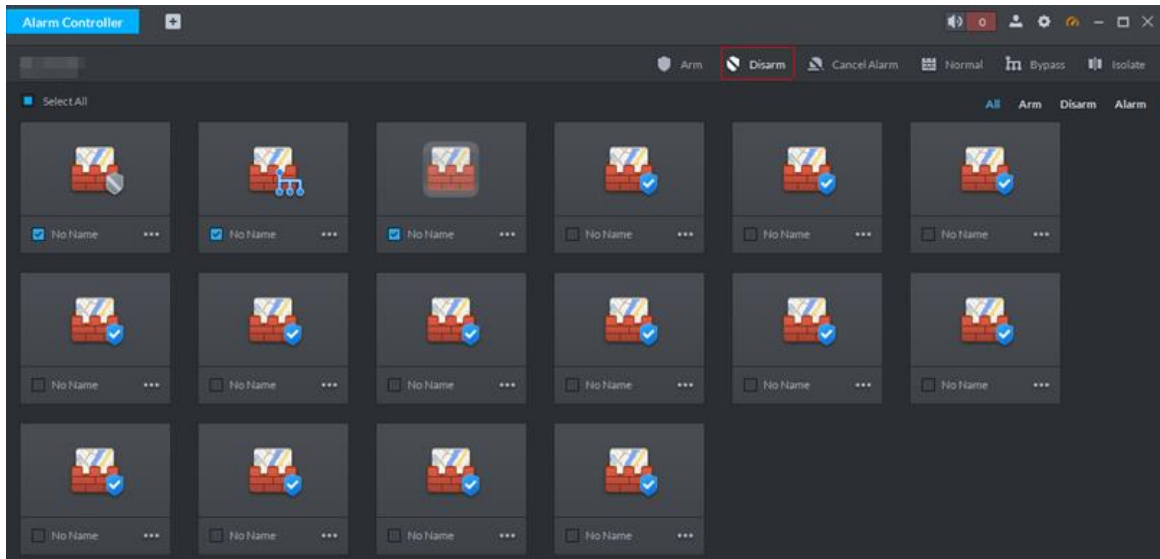


Figure 5-373 Disarm a subsystem



- Select the zone or subsystem you want to disarm (multiple choice supported), and then click **Disarm** on the top of the interface.

Figure 5-374 Disarm



5.19.4.2 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:


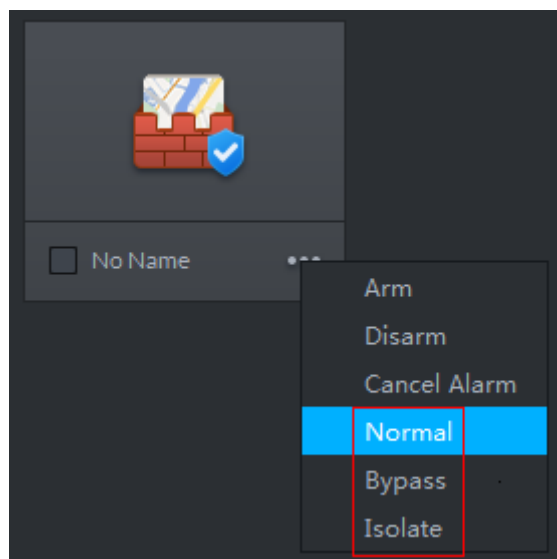
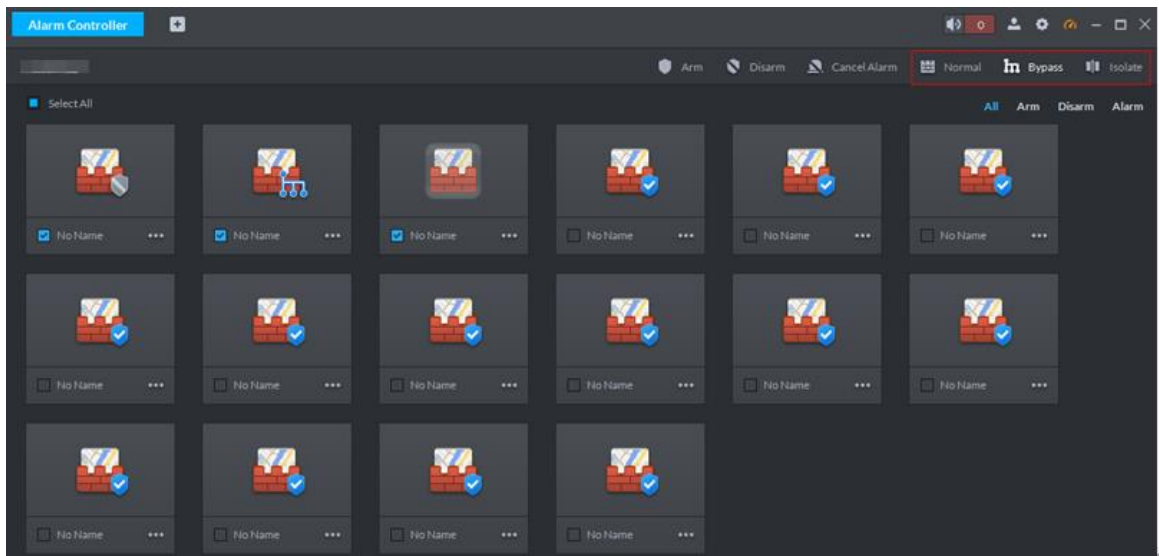
- Click  of the zone that needs to be bypassed, isolated or recovered to normal, and then select operation.

Figure 5-375 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 5-376 Bypass/isolate zone (2)

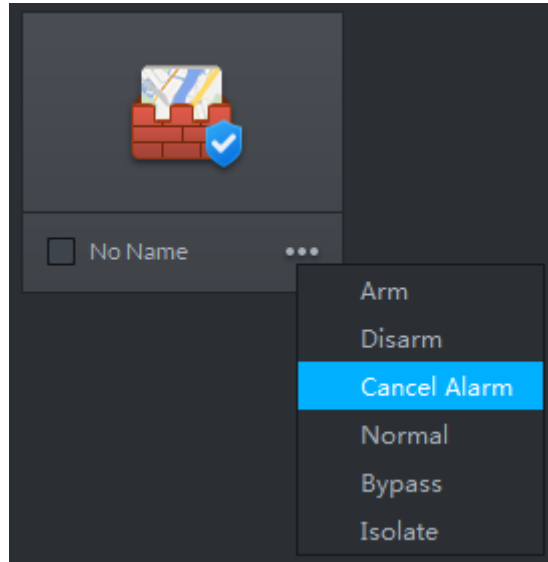


5.19.4.3 Cancel Alarms

You can remove an alarm by **Cancel Alarm** when the alarm is triggered.

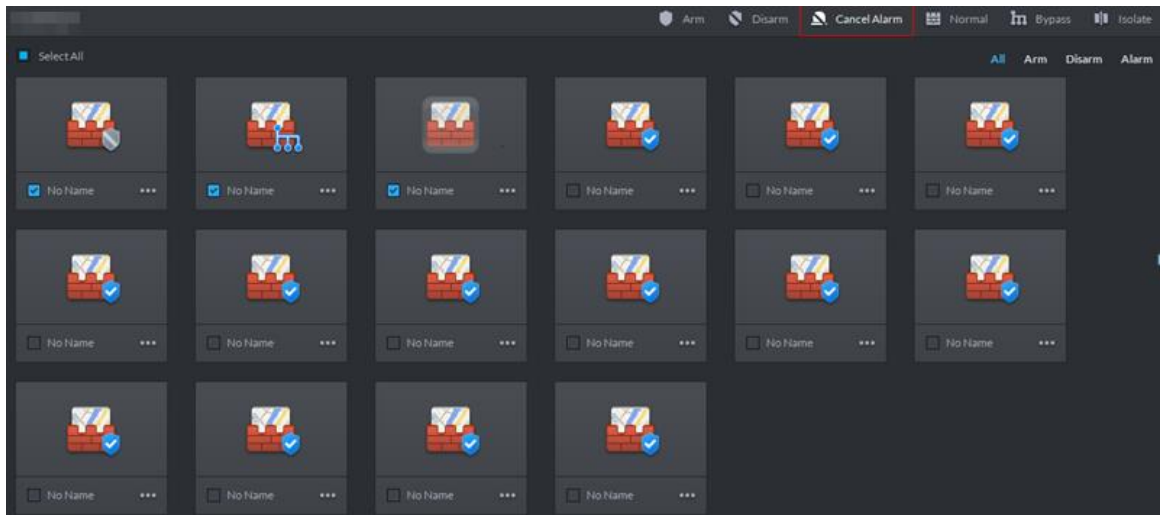
- Click the zone you want to cancel alarm, and then select **Cancel Alarm**.

Figure 5-377 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 5-378 Cancel alarms (2)



5.20 Time Synchronization

5.20.1 Device Time Synchronization

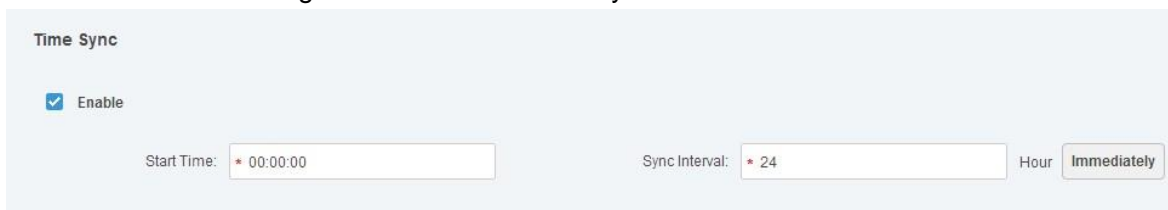
Automatically or manually synchronize front-end device time with platform server. The automatic method synchronizes device time with the server at the pre-defined interval and time. When necessary, you can also manually synchronize system time.

5.20.1.1 Automatic Synchronization

Step 1 Click **+** and then on the **New Tab** interface select System settings.

Step 2 Click **Time Sync** and then check the box to enable the function. Set time synchronization parameters.

Figure 5-379 Enable time synchronization



The screenshot shows the 'Time Sync' configuration panel. At the top, there is a section titled 'Time Sync' with a checked checkbox labeled 'Enable'. Below this, there are three input fields: 'Start Time' with the value '00:00:00', 'Sync Interval' with the value '24', and a 'Hour' dropdown menu currently set to 'Immediately'.

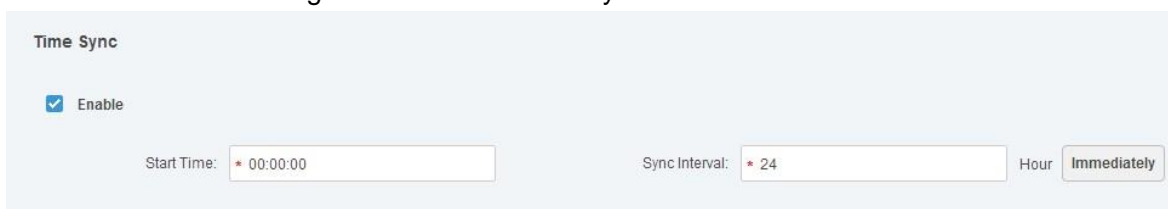
Step 3 Click **Save** to save configuration information.

5.20.1.2 Manual Synchronization

Step 1 Click **+** and then on the **New Tab** interface select **System settings**.

Step 2 Click **Immediately**.

Figure 5-380 Immediate synchronization



This screenshot is identical to Figure 5-379, showing the 'Time Sync' configuration panel with 'Enable' checked, 'Start Time' at '00:00:00', 'Sync Interval' at '24', and the 'Hour' dropdown set to 'Immediately'.

5.20.2 Time Synchronization on the Client

Manually or automatically synchronize client PC time with platform server. The automatic method synchronizes device time with the server at the pre-defined interval and time. When necessary, you can also manually synchronize client PC time.

5.20.2.1 Automatic Synchronization

Step 1 Log in to DSS client.

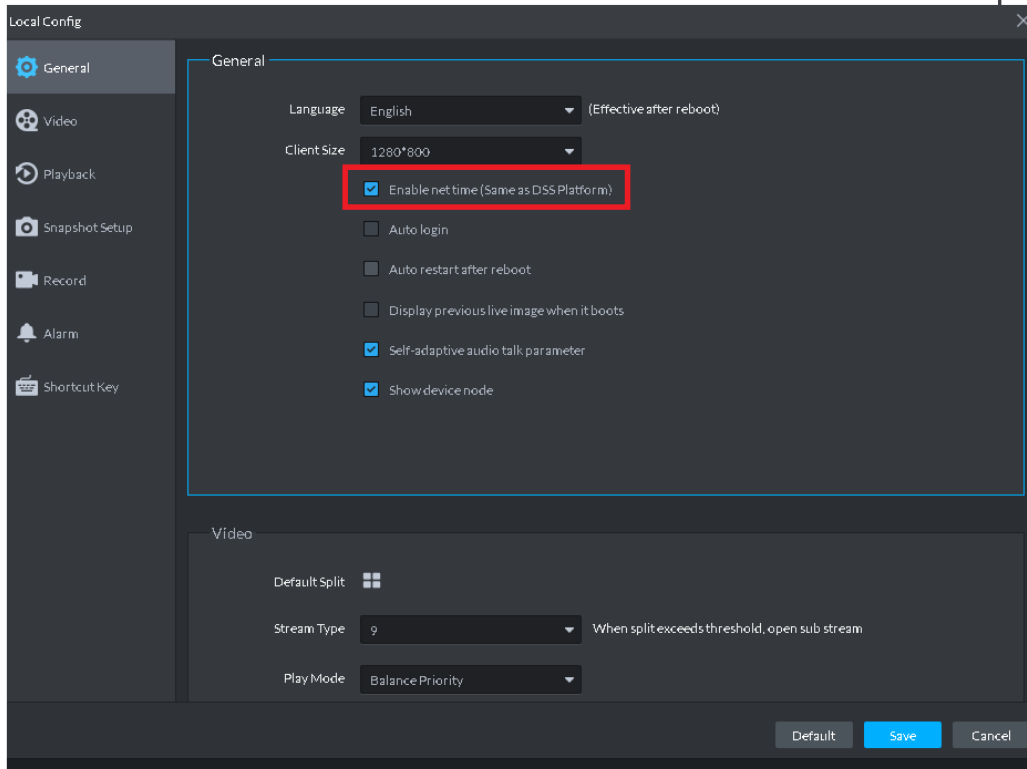
Step 2 Click **⚙** at the upper-right corner. Enter **Local Config** interface.

Step 3 Click the **General** tab and then enable client time sync function. Click **Save**.



After you enabled time sync function on the **General** interface, client begins the request to the server immediately. It is to complete the time synchronization.

Figure 5-381 Enable client time synchronization

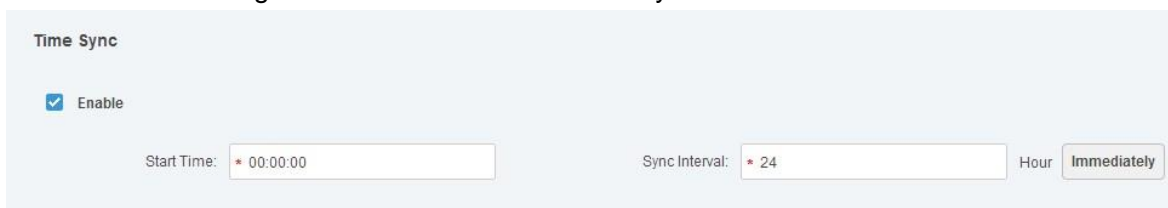


Step 4 Click **Save**.

Step 5 Login DSS manager, and then on the **New Tab** interface select System settings.

Step 6 Click **Time sync** and then check the box to enable the function. See time sync parameters.


Figure 5-382 Enable device time synchronization



Step 7 Click **Save** to save configuration information.

5.20.2.2 Manual Synchronization

Step 1 Log in to DSS client.

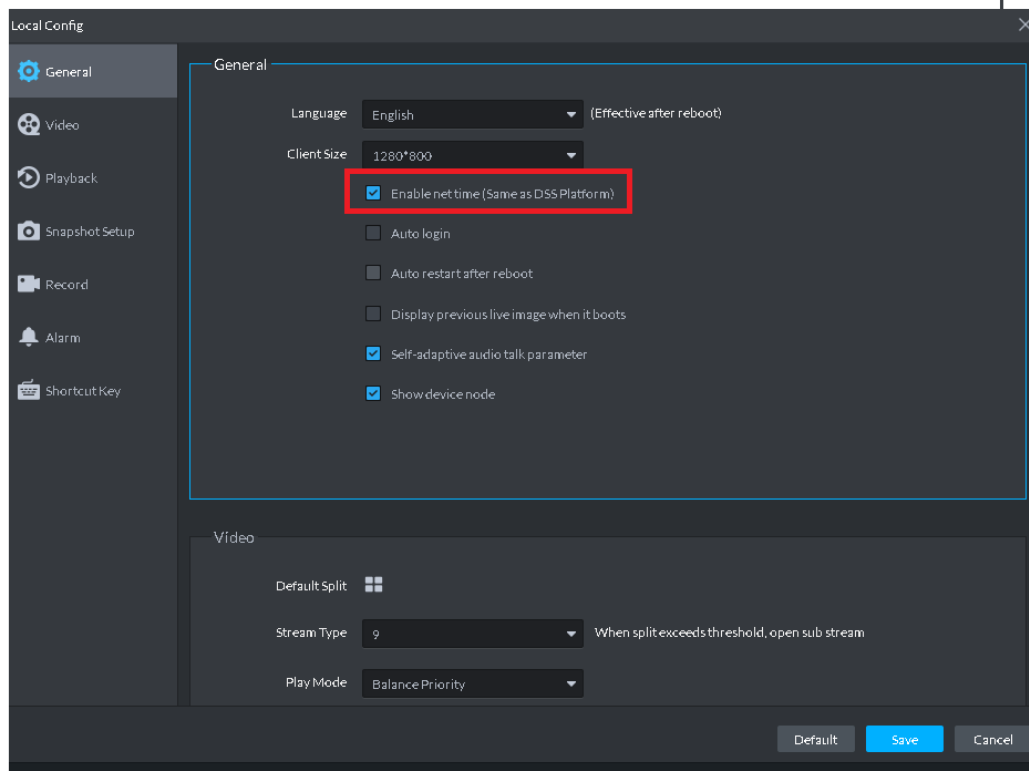
Step 2 Click  at the upper-right corner. Enter **Local Config** interface.

Step 3 Click the **General** tab and then enable client time sync function. Click **Save**..



After you enabled time sync function on the General interface, client begins the request to the server immediately. It is to complete the time synchronization.

Figure 5-383 Enable client time synchronization

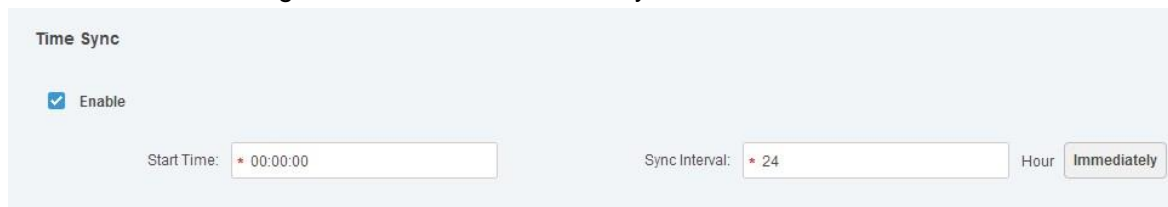


Step 4 Click **Save**.

Step 5 Log in to Web Manager, and then on the **New Tab** interface select **System settings**.

Step 6 Click the **immediately** button.

Figure 5-384 Immediate time synchronization



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.