



DSS Express

User's Manual

V1.0.3

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD

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 be the Device or 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.

Privacy Protection Notice

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

Revision History

Version	Software Version	Revision Content	Release Time
---------	------------------	------------------	--------------

Version	Software Version	Revision Content	Release Time
V1.0.3	1.000.0000003	- Added alarm controller, entrance, smart track, visitor management and POS. - Optimized attendance management, personnel management and access control. Optimized user's manual description and outline structure. - Deleted FTP.	2019.5
V1.0.2	1.000.0000002	Added modules of Attendance and Flow Analysis. Added generating track in the module of Face Recognition.	2018.10

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 Guide (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.

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.

Table of Contents

Foreword	II
1 Overview.....	1
1.1 Product Positioning	1
1.2 Highlights	1
2 Installation and Deployment	2
2.1 Preparations.....	2
2.1.1 Server Config Requirement.....	2
2.1.2 Configuring Server IP Address	2
2.1.3 Configuring Server System Time.....	5
2.2 Installing Program (Update)	7
2.3 Service Management	9
2.3.1 Logging in System Config Tool	9
2.3.2 Modifying Service Port.....	11
2.3.3 WAN and LAN Mapping.....	12
2.4 Installing Client.....	14
2.4.1 Installing Client	14
2.4.2 Initialization Config.....	18
2.4.3 Logging in Client.....	20
2.5 Importing License.....	23
2.5.1 License Introduction.....	23
2.5.2 Applying License.....	24
2.5.3 Loading License.....	26
3 Operation Guide	28
3.1 Installing Client.....	28
3.2 Basic Config	28
3.2.1 System Setting.....	28
3.2.2 Managing Device	35
3.2.3 Adding User	53
3.2.4 Setting Alarm Event	56
3.2.5 Setting Record Plan.....	67
3.2.6 Configuring Emap	68
3.3 Local Config	76
3.3.1 Setting Basic Parameter	77
3.3.2 Setting Real-time Video Parameter	78
3.3.3 Setting Record Playback	80
3.3.4 Setting Snapshot	80
3.3.5 Setting Recording Parameter	81
3.3.6 Setting Alarm Parameter	81
3.3.7 Setting Video Wall.....	82
3.3.8 Setting Shortcut Key	83
3.4 Live View.....	84

3.4.1 Entering Live View Interface.....	84
3.4.2 Enabling Live View	86
3.4.3 Enabling Tour View	90
3.4.4 Device Config	90
3.4.5 Setting PTZ.....	108
3.4.6 Smart Track	114
3.4.7 Smart Track	116
3.4.8 View	123
3.4.9 Favorites	125
3.4.10 Region of Interest (RoI)	127
3.5 Record.....	128
3.5.1 Record Playback.....	128
3.5.2 POS Record Playback.....	141
3.6 Event Center	141
3.6.1 Setting Alarm Parameters.....	141
3.6.2 Searching and Processing Real-Time Alarm.....	143
3.6.3 Searching and Processing History Alarm.....	145
3.7 Video Wall	146
3.7.1 Adding Encoder	147
3.7.2 Entering Video Wall Interface	147
3.7.3 Adding Video Wall.....	149
3.7.4 Adding Task.....	152
3.7.5 Setting Video Wall Plan	153
3.7.6 Applying Video Wall	160
3.8 POS.....	163
3.8.1 Adding Encoder	164
3.8.2 Modifying POS End Mark	165
3.8.3 Live View.....	166
3.8.4 Record Playback.....	168
3.9 Face Recognition	170
3.9.1 Adding Encoder	171
3.9.2 Setting Picture Storage Disk.....	171
3.9.3 Setting Record Plan.....	172
3.9.4 Managing Face Database	172
3.9.5 Setting Alarm Event	182
3.9.6 Face Recognition Application	182
3.10 ANPR.....	198
3.10.1 Adding ANPR	198
3.10.2 Setting Picture Storage Disk.....	198
3.10.3 Setting Record Plan.....	198
3.10.4 Plate Recognition Application	199
3.10.5 Vehicle Record.....	201
3.11 Flow Analysis.....	203
3.11.1 Adding Encoder.....	204
3.11.2 Flow Analysis Application.....	205
3.12 Personnel Management.....	208
3.12.1 Adding Department.....	209

3.12.2 Adding Personnel.....	210
3.12.3 Editing Personnel.....	224
3.12.4 Importing/Exporting Personnel	229
3.12.5 Batch Issue Card	232
3.12.6 Personnel Extraction	235
3.12.7 Generating Path.....	237
3.13 Access Control	238
3.13.1 Adding Access Control.....	239
3.13.2 Personnel Management	243
3.13.3 Managing Time Template	243
3.13.4 Setting Access Level	247
3.13.5 Advanced Function	249
3.13.6 Setting Record Plan.....	268
3.13.7 Configuring Super Password.....	268
3.13.8 Access Control Application	270
3.13.9 Searching Access Control Log	277
3.13.10 AC Device Maintenance	281
3.14 Visitor Management	283
3.14.1 Adding AC Device	284
3.14.2 Visitor Appointment.....	284
3.14.3 Visit Registration.....	286
3.14.4 End Visit Registration	290
3.14.5 Searching Visit Record	291
3.15 Video Intercom	293
3.15.1 Adding Video Intercom Device	293
3.15.2 Personnel Management	294
3.15.3 Configuring Building/Unit.....	294
3.15.4 Synchronizing Contacts.....	294
3.15.5 Call Management.....	296
3.15.6 Video Intercom Application	301
3.16 Attendance Management	309
3.16.1 Adding Attendance Device.....	310
3.16.2 Personnel Management	311
3.16.3 Setting Attendance Terminal.....	311
3.16.4 Setting Statistics Rule.....	312
3.16.5 Setting Attendance Period	313
3.16.6 Setting Holiday.....	318
3.16.7 Setting Attendance Shift	320
3.16.8 Shift Management.....	322
3.16.9 Viewing Attendance Report	326
3.17 Entrance	329
3.17.1 Adding Device.....	330
3.17.2 Setting Picture Storage Disk.....	337
3.17.3 Setting Alarm Event	337
3.17.4 Configuring Parking Lot.....	338
3.17.5 Vehicle Management.....	343
3.17.6 Entrance Application	346

3.18 Alarm Host.....	355
3.18.1 Adding Alarm Host	355
3.18.2 Entering Alarm Controller Interface	357
3.18.3 Updating Alarm Controller Status	359
3.18.4 Alarm Controller Application	359
4 Maintenance Guide	365
4.1 Backup and Restore	365
4.1.1 Backup	365
4.1.2 Restore	367
4.2 Update.....	369
4.3 Log	371
4.4 Password Maintenance.....	372
4.4.1 Changing Password.....	372
4.4.2 Resetting Password.....	373
Appendix 1 Service Module Introduction	376
Appendix 2 Shortcut Key List	378
Appendix 3 Deleting Videos on Central Server	379
Appendix 4 Cybersecurity Recommendations	380

1 Overview

1.1 Product Positioning

DSS Express is an important surveillance platform product in DSS family (Dahua Security Software), design for medium-small project. DSS Express supports simple, reliable, open and more features which bring user with HD, smart, safe experience. By extending to 512 channels via License, it needs to integrate access control and VDP device organizations in order to provide solutions. DSS Express is widely used for residence, supermarket, factory, casino and other scenarios.

1.2 Highlights

- GPU decoding, meantime support preview of more HD cameras.
- Vector graph design, perfect support over 4K display.
- Both administrator and operator use the client with powerful control experience.
- Export device list from SmartPSS, and import device list on DSS Express. No need to add device again when switching from SmartPSS to DSS Express.
- Within LAN, auto search device in different network segment and show device list. One-click to add management. Save deployment time effectively.
- Mobile phone APP. Realize access anytime when you are not there.
- Auto and manual backup of database. Quickly recover when system error occurs.
- Lock record, permanent storage of important record footage, without being overwritten.

2 Installation and Deployment

2.1 Preparations

2.1.1 Server Config Requirement

Please refer to Table 2-1 for the requirements of server config.

Table 2-1 Server config requirement

DSS Server Config Requirement	
Recommended config	CPU: Intel® Xeon® CPU E3-1220 v5 @3.00GHz RAM: 18GB Network adapter: 1Gps DSS installation directory space: Over 500G
Minimum config	CPU: i3-2120 RAM: 8GB Network adapter: 1Gps DSS installation directory space: Over 200G
System	Support Win7 and later systems.  The manual takes Windows Server 2012 R2 as an example to introduce how to configure server IP address and system time.

2.1.2 Configuring Server IP Address

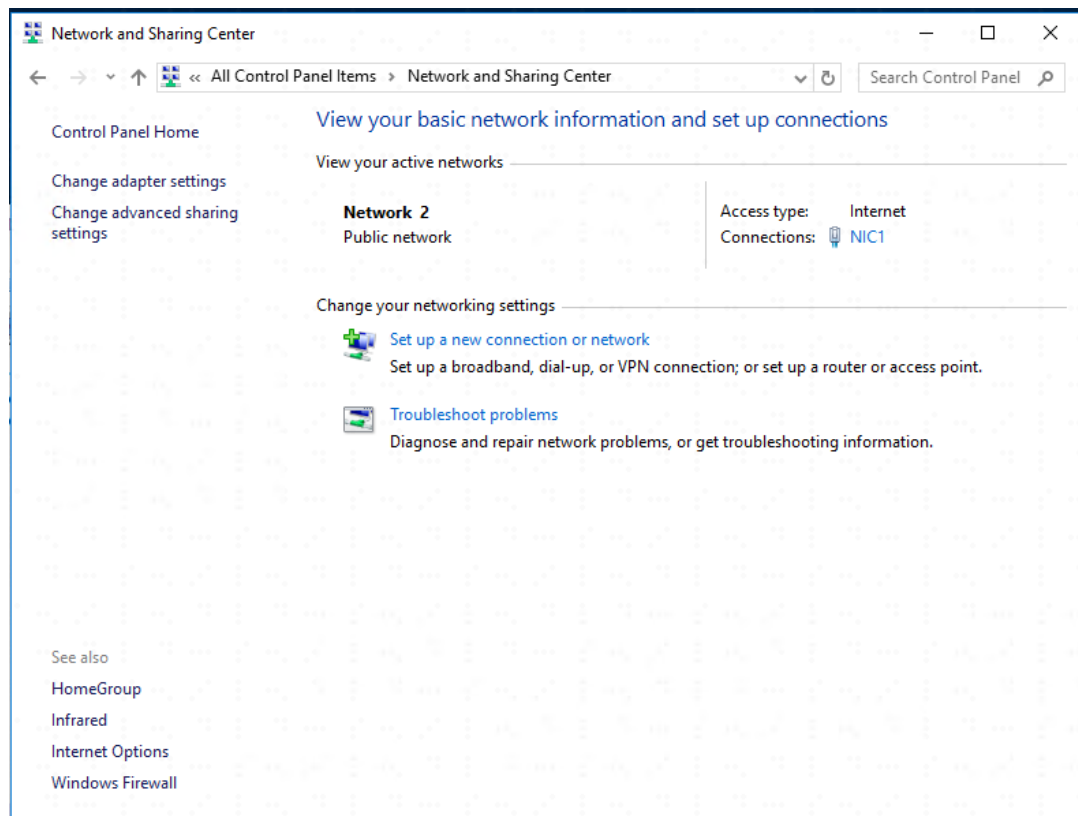
Server IP address is platform IP address, modify server IP address and make sure the platform is well connected with other devices in the networking.

Step 1 Connect server to mouse, keyboard and monitor, connect to network cable, power on and start the server.

Step 2 Select  > Control Panel > Network and Internet > Network and Sharing.

The **Network and Sharing** is displayed. See Figure 2-1.

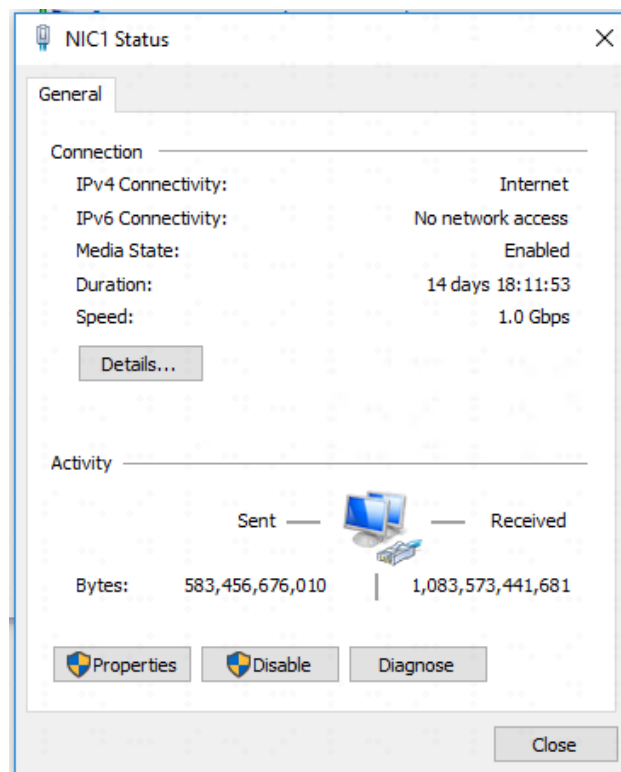
Figure 2-1 Network and sharing center



Step 3 Click **Ethernet0**.

The **Ethernet0 Status** interface is displayed. See Figure 2-2.

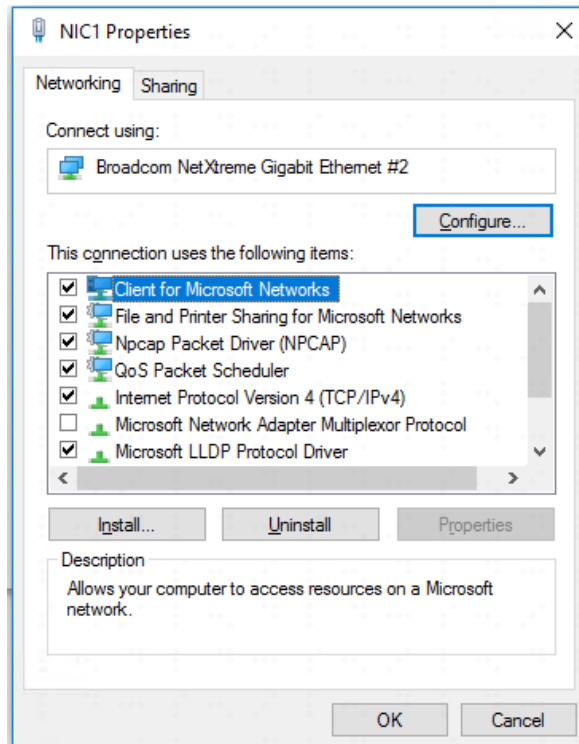
Figure 2-2 Ethernet0



Step 4 Click **Properties**.

The system displays network config info. See Figure 2-3.

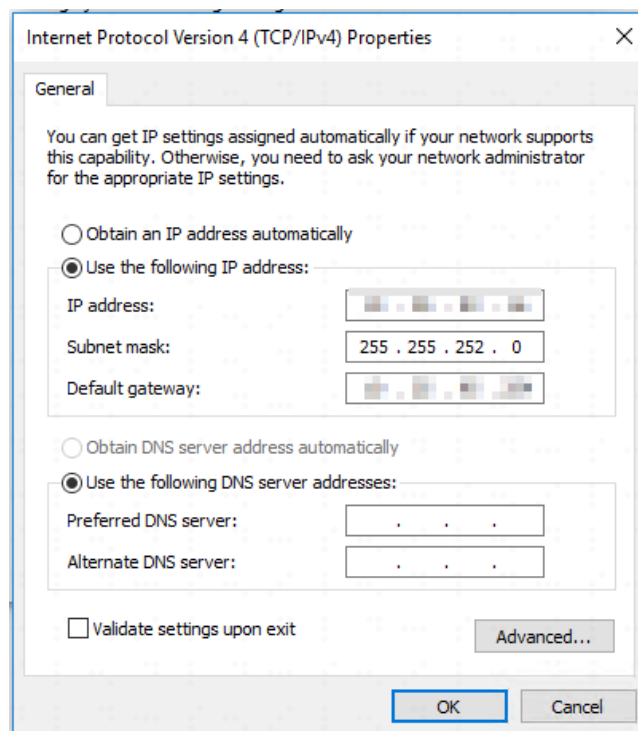
Figure 2-3 Ethernet0 properties



Step 5 Double click IPv6 or IPv4 according to network environment. The chapter takes IPv4 as an example.

The system displays Internet Protocol Version 4 (TCP/IPv4) Properties. See 0.
Internet protocol version 4 (TCP/IPv4) properties

Figure 2-4 TCP/IPv4 properties



Step 6 Select **Use Following IP Address(S)**; configure IP address info according to plan, and then click **OK**.

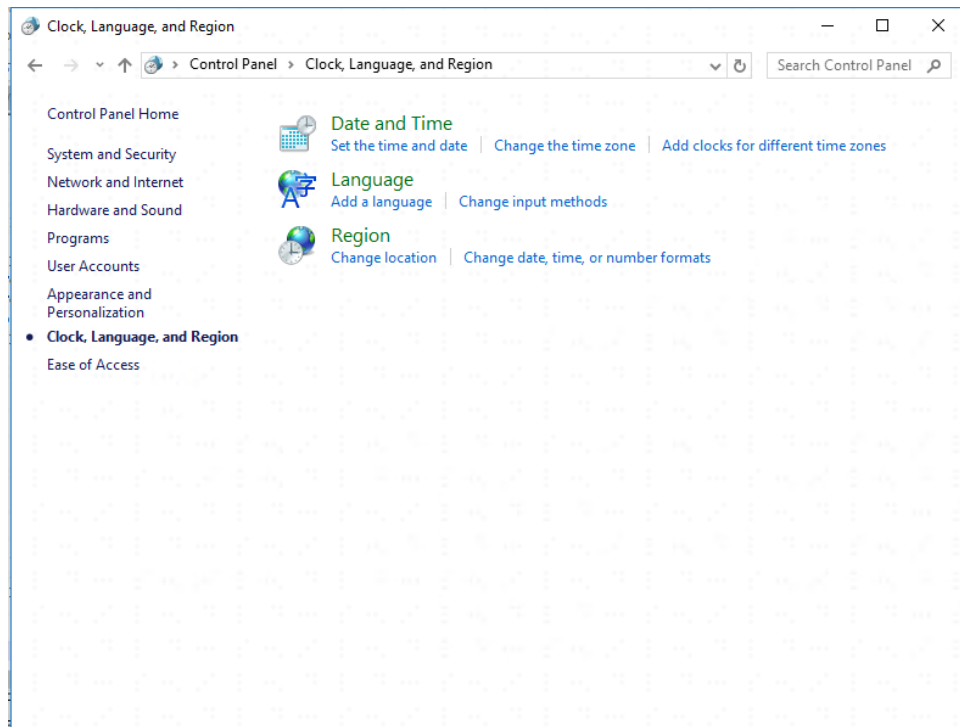
2.1.3 Configuring Server System Time

Modify server system time; make sure the server License is within expiry date and system time is in accordance with other devices in networking to avoid log and video loss.

Step 1 Select  > Control Panel > Clock, Language and Region.

The **Clock, Language and Region** interface is displayed. See Figure 2-5.

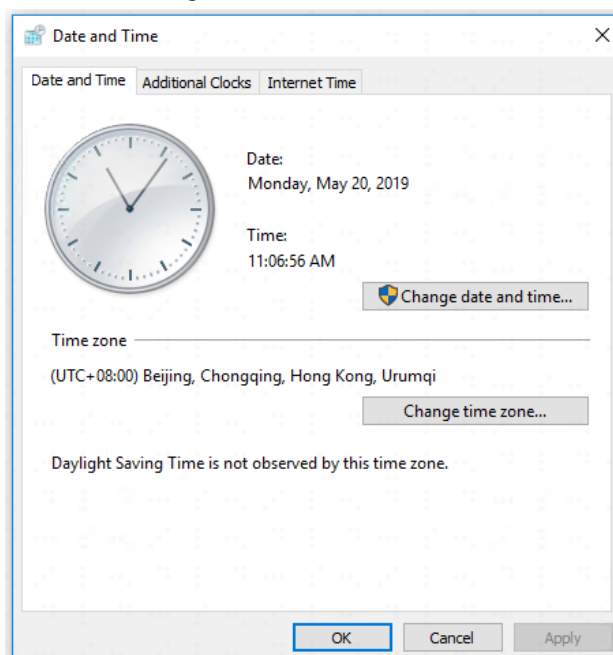
Figure 2-5 Clock, language and region



Step 2 Click **Date and Time**.

The **Date and Time** interface is displayed. See Figure 2-6.

Figure 2-6 Date and time



Step 3 Set date and time.

- 1) Click **Change Date and Time (D)**...

The Date and Time Setting interface is displayed. See Figure 2-7.

Figure 2-7 Date and time setting



- 2) Select date, set time, click **OK**.



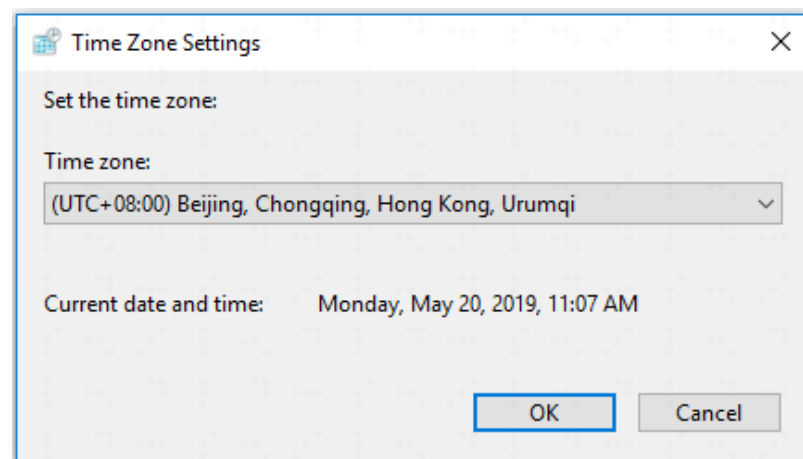
If you want to modify the calendar's date format or first day of week, click **Change Calendar Setting to modify**.

Step 4 Setting time zone.

- 1) Click **Change Time Zone (Z)**...

The **Time Zone Setting** interface is displayed. See Figure 2-8.

Figure 2-8 Time zone setting



- 2) Select your time zone, and click **OK**.

Step 5 Click OK.

Server system time setting is completed.

2.2 Installing Program (Update)



- Make sure you have acquired program before update, otherwise please contact technical support for update program.
- Program name includes version number and date, please check before installation.

Step 1 Double click installer.

The agreement interface is displayed. See Figure 2-9.

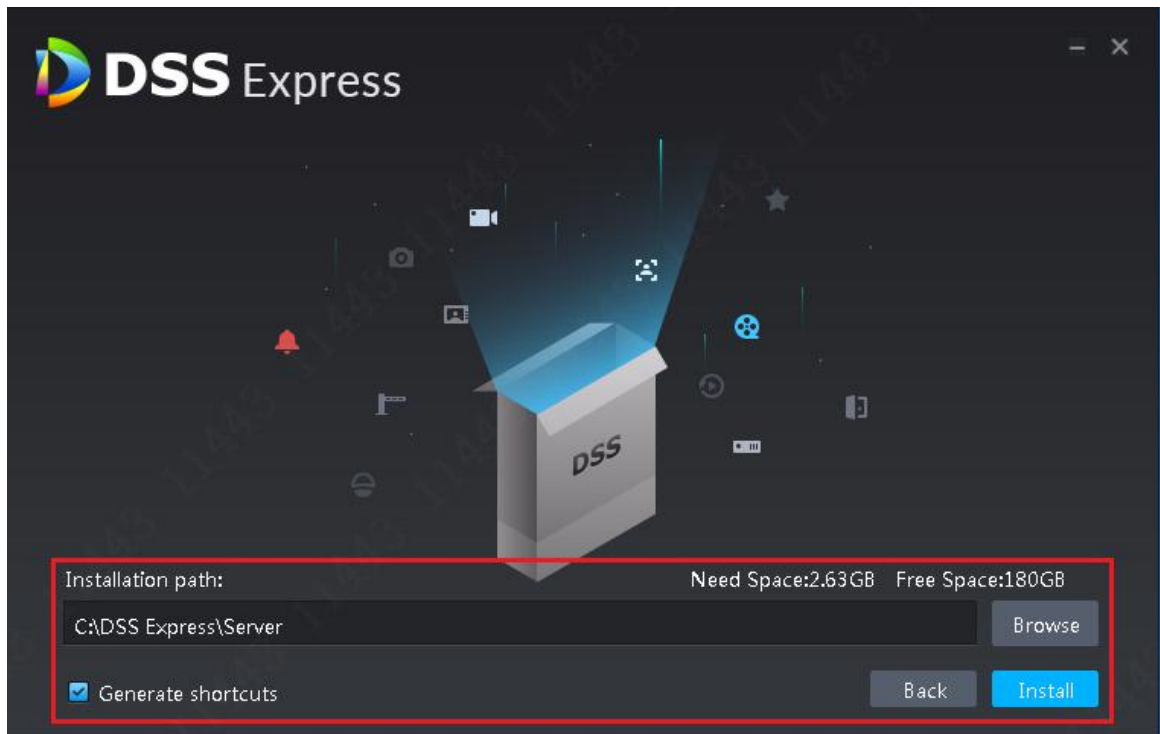
Figure 2-9 Agreement confirm



Step 2 Select **I have read and agree the DSS agreement**, click **Next**.

The installation path interface is displayed. See Figure 2-10

Figure 2-10 Select installation path



Step 3 Click **Browse** and select installation path, click **Install**.

The system displays installation progress, the whole installation needs 5-10 minutes. See Figure 2-11 after installation is completed. The server starts automatically after installation.



- The system automatically detects the available space of path after the installation path is selected, if available space is less than needed for system installation, then the icon **Install** becomes gray, and installation cannot be implemented.
- Do not select **Generate Shortcuts** if it is not necessary.
- If port conflict exists, the system will prompt conflicted port during installation. Open DSS Express Server and modify port after installation is completed. See 2.3.2 Modifying Service Port for more details.

Figure 2-11 Installation completed



2.3 Service Management

You can modify service port, stop service and start service. If both device and platform are in two different network segments, the platform supports configuring network mapping, make sure the platform can be accessed by two different network segments.

2.3.1 Logging in System Config Tool

Introduce login method and interface of server system config tool.

Double click  on the server desktop, or click Run on the interface after program installation is completed. The system displays the interface of system config tool. See Figure 2-12. For interface description, see Table 2-2.

Figure 2-12 System config

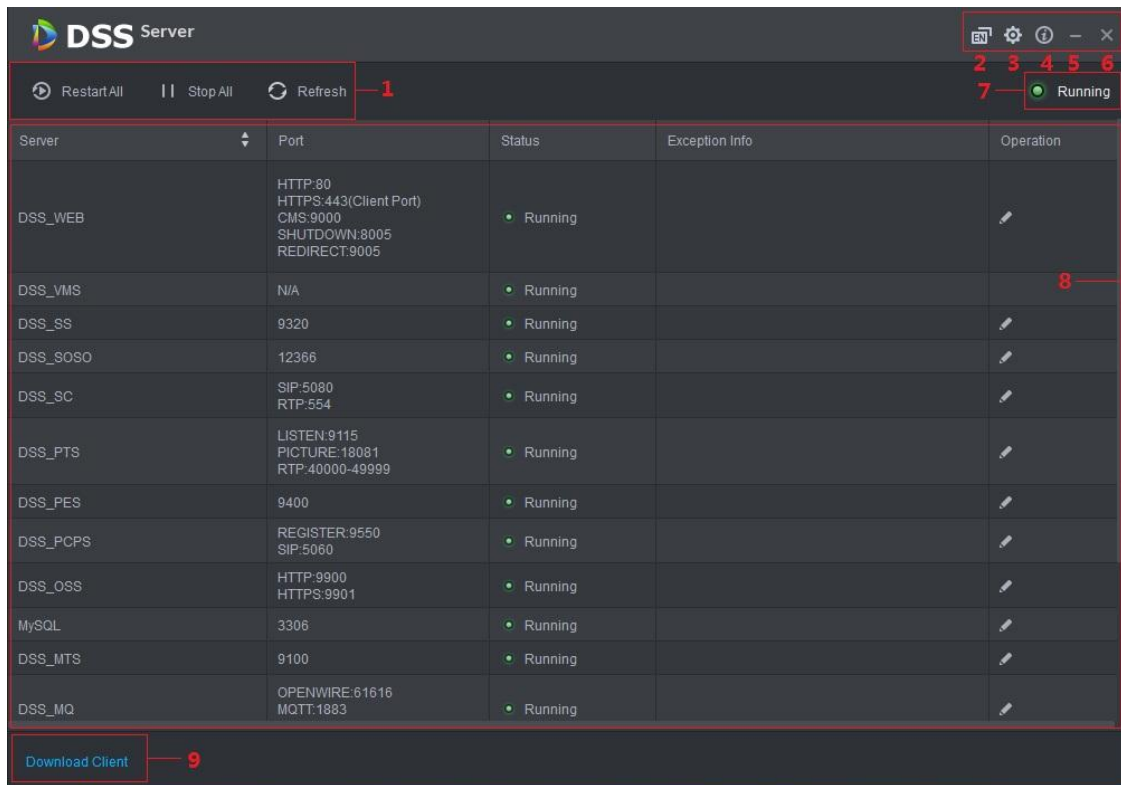
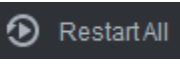
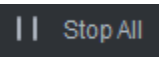
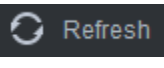
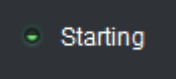
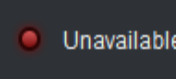
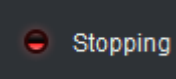
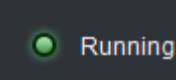
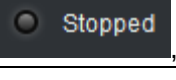


Table 2-2 Module introduction

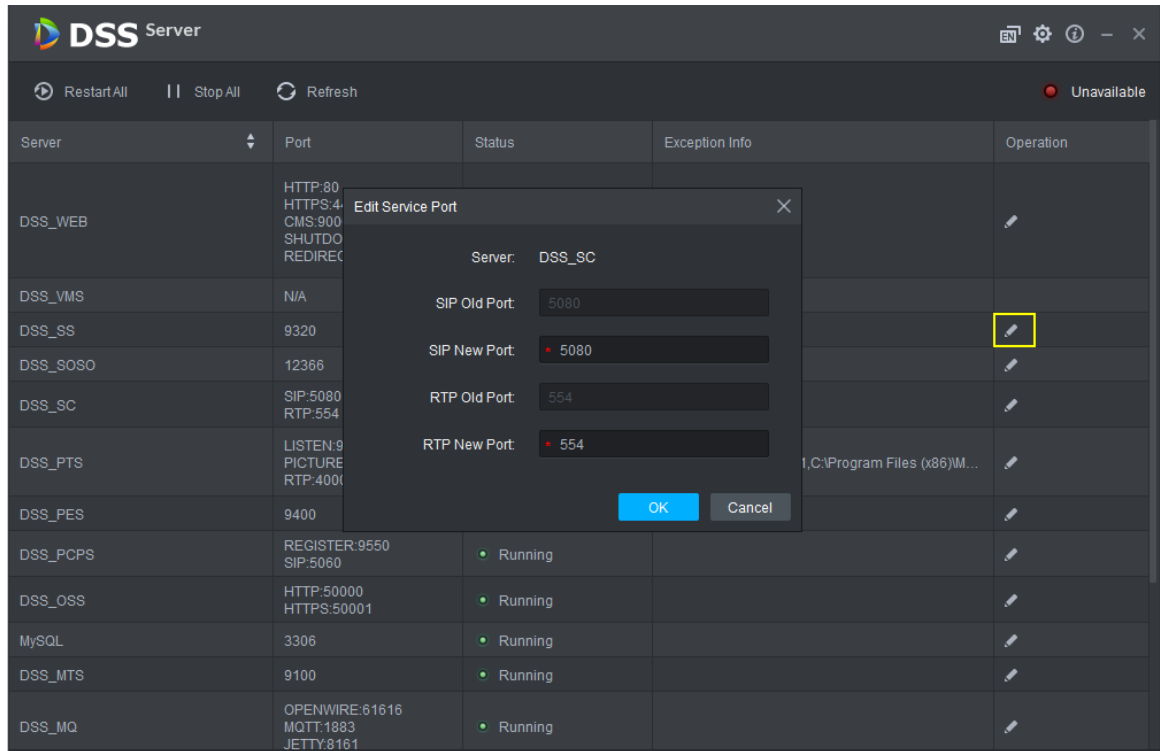
No.	Function	Description
1	Service Management	Service management, support following three types of operation. - Click  and restart all services. - Click  and stop all services. - Click  and refresh all services.
2	Language	Click the icon to switch language, the language takes effect after the server restarts.
3	Setting	Set CMS IP as server IP address. If device and platform exist in two different network segments, then you need to configure mapping address as IP address of the other network segment, make sure both segments can access platform.
4	About	Click the icon and view software version and release date.
5	Minimize	Click the icon and minimize config tool interface.
6	Close	Close config tool.

No.	Function	Description
7	Service Status	Include following service status.  Starting, service is being started.  Unavailable, service is abnormal.  Stopping, service is being stopped.  Running, all services are running normally.  Stopped, all services are stopped.
8	Server Display	Display each service and service status. Click  and you can modify server port, after that the system automatically restarts services.
9	Download Client	Click the icon and jump to WEB interface, then you can download client installation program.

2.3.2 Modifying Service Port

Step 1 On the interface of system config tool, click  of the target server whose port you want to modify. The system displays the interface of Edit Service Port. See Figure 2-13.

Figure 2-13 Edit service port



Step 2 Modify service port, click **OK**.

The system automatically restarts services after modified successfully.



- Default port of “DSS_PTS” service is “8081”, which is often occupied. You are recommended to modify the port.
- The system prompts when the port is occupied; please modify port according to prompt.

2.3.3 WAN and LAN Mapping

If both device and platform are in two different network segments, the platform supports configuring network mapping, and make sure two network segments can access platform.

2.3.3.1 Configuring Mapping Rule

Access platform according to the mapping rule formulated in advance. Mapping rule config method differs depending on different products; refer to corresponding user manual for more details. For the port need to be opened and its description, please refer to **Appendix 1 Service Module Introduction** for more details.



DMZ mapping is recommended if router is used in networking. If environment is not allowed, then port mapping is available.

If port is occupied by other mapping, for example, port 80 is occupied, then you need to modify it as 81, you need to modify port first, then add mapping rule on the router. For more details, please refer to **2.3.2 Modifying Service Port**.



WAN and LAN port of the server is not distinguished by system, port config options are unified and WAN/LAN ports are consistent. (Server port does not distinguish WAN or LAN, both belongs to the same port number.)

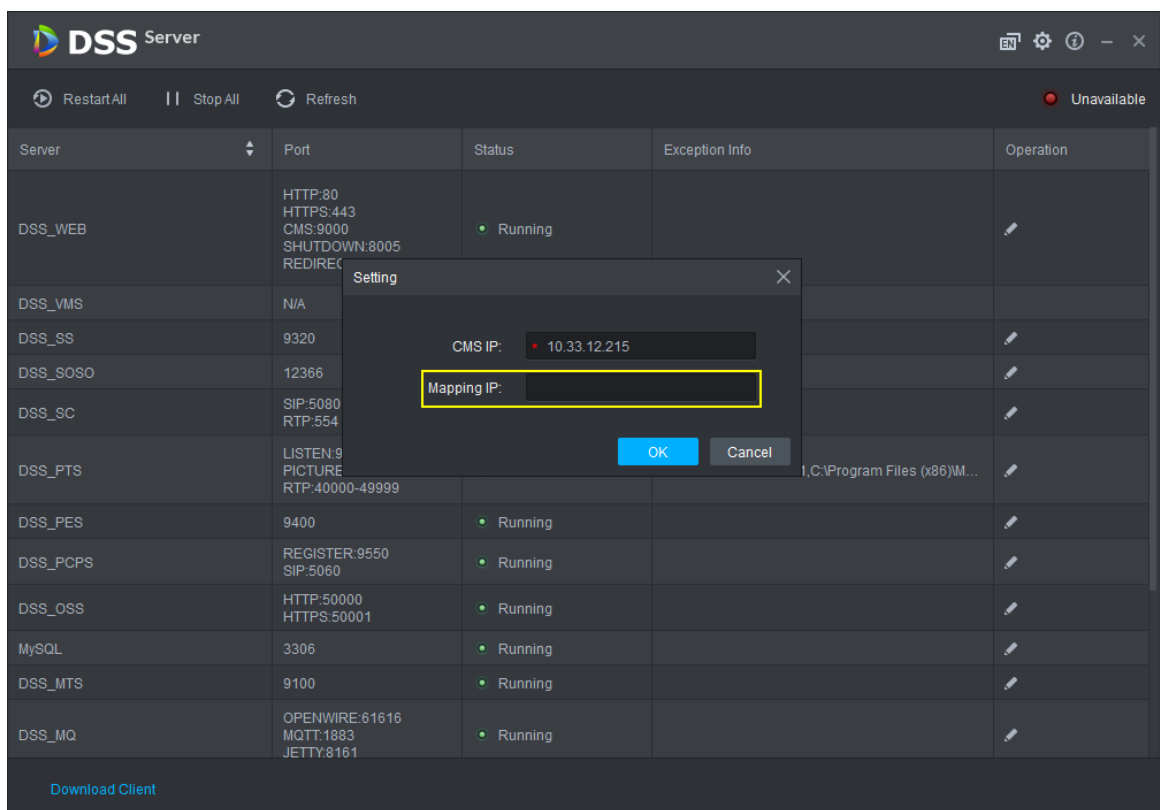
2.3.3.2 Configuring Mapping IP

If device and platform are in two different segments, the platform supports configuring network mapping and realizing access to different segments.

Step 1 On the interface of system config tool, click  on the upper right corner.

The system displays **Config** interface. See Figure 2-14.

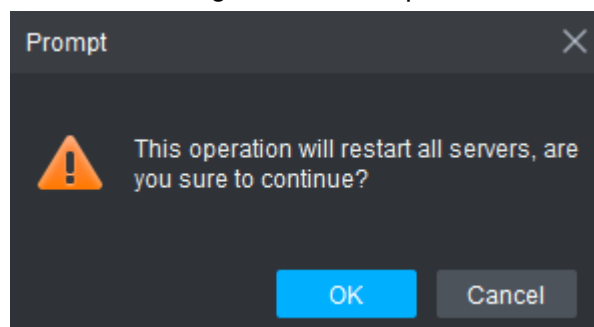
Figure 2-14 Config



Step 2 Set Mapping IP as IP address of the other segment, click OK.

The system pops up **Prompt** dialog box. See Figure 2-15.

Figure 2-15 Prompt



Step 3 Click OK and system restarts services.

2.4 Installing Client

2.4.1 Installing Client

You can manage and operate platform by client, client includes PC client and mobile APP.

2.4.1.1 PC Client

2.4.1.1.1 PC Config Requirement

For config requirement of PC where DSS Client is installed, see Table 2-3.

Table 2-3 Config requirement

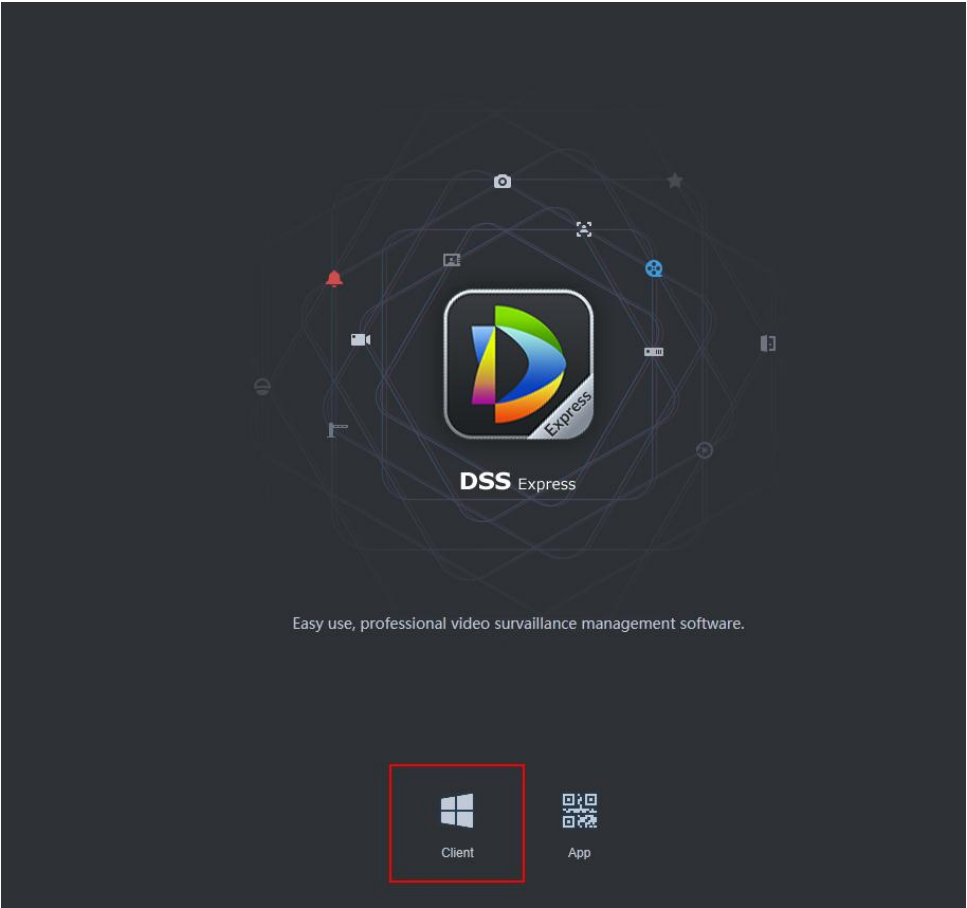
PC Config Requirement	
Recommended Config	CPU: i5-6500 Basic frequency: 3.20GHz Memory: 8GB Graphic card: Intel® HD Graphics 530 Network adapter: 1Gbps DSS client installation directory space: 100GB
Min Config	CPU: i3-2120 Memory: 4GB Graphic card: Intel (R) Sandbridge Desktop Gra Network adapter: 1Gbps DSS installation directory space: 50GB

2.4.1.1.2 Download and Install

Step 1 Enter server IP address into browser, click **Enter**.

The system displays the interface of downloading client. See Figure 2-16.

Figure 2-16 Download client



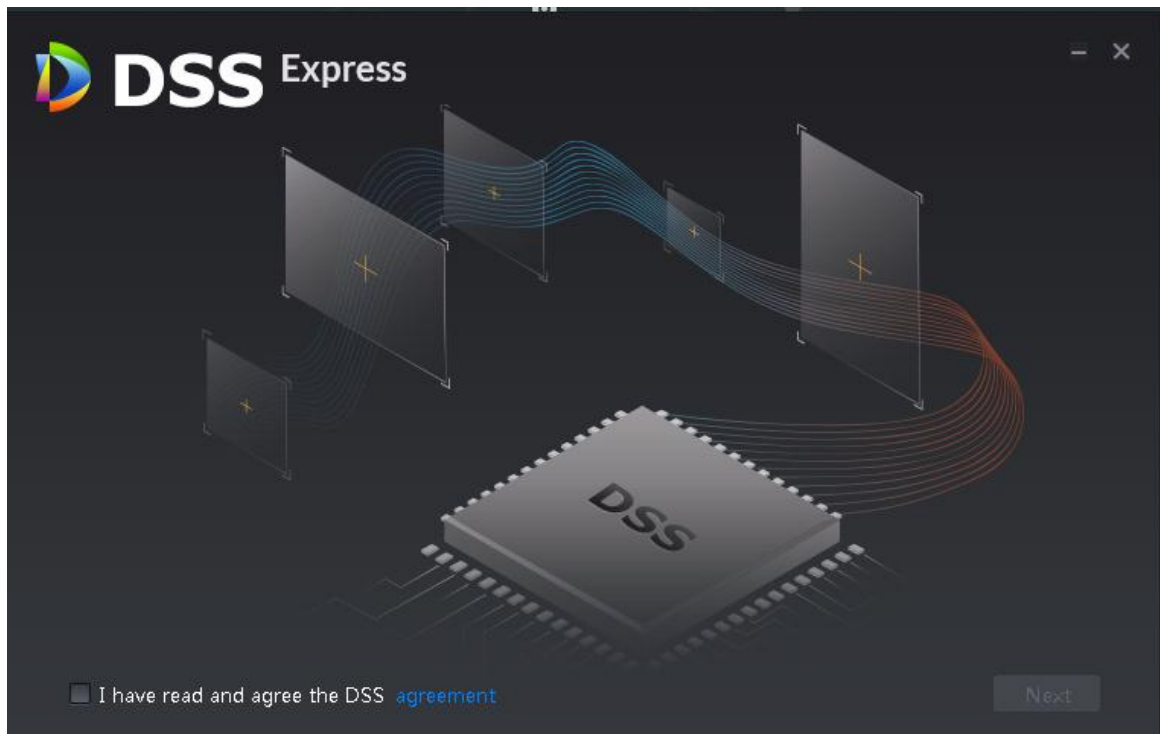
Step 2 Double click , run or download client according to interface prompt. For more download details, see Table 2-4.

Table 2-4 Download operation

Operation	Description
Run	Download temporary file, you can install after it is checked.
Save	Download installation package to IE default path.
Save as	Download installation package to designated path.
Save and Run	Download installation package to IE default path, and you can install after it is checked.

Step 3 Click **Run**, or double click client installation program under the save directory. The system displays agreement interface. See Figure 2-17.

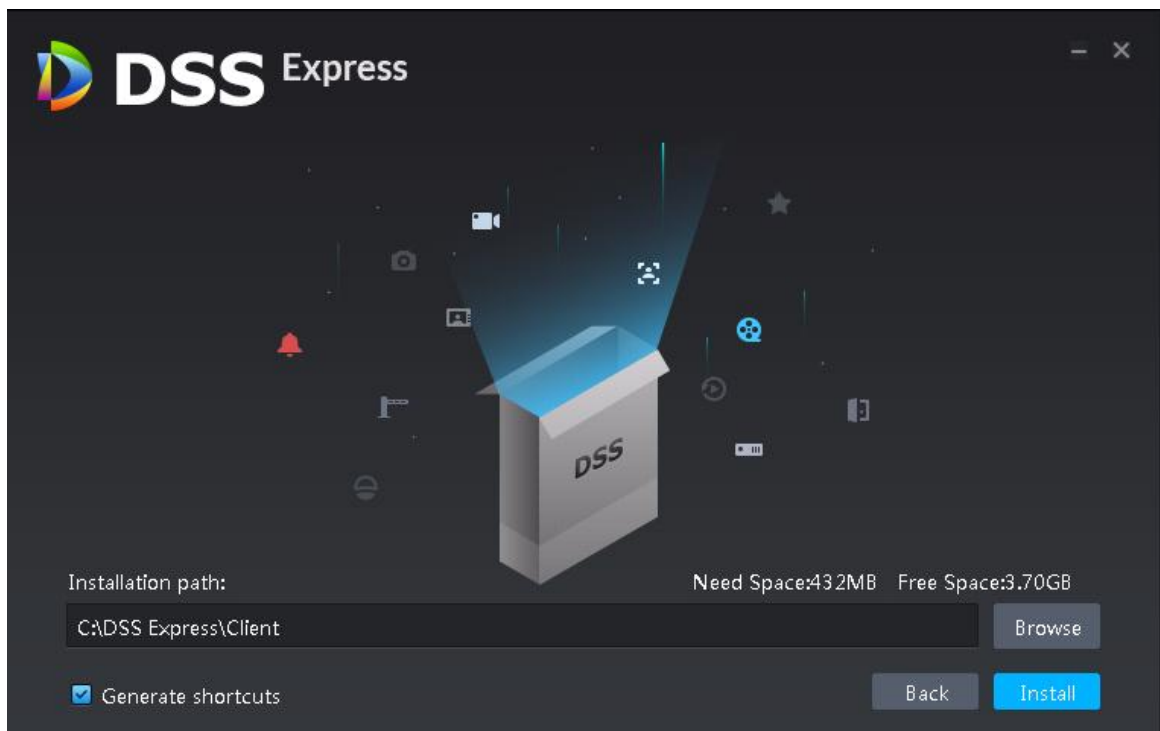
Figure 2-17 Confirm agreement



Step 4 Select I have read and agree the DSS agreement, click **Next**.

The system displays the interface of installation path, See Figure 2-18.

Figure 2-18 Select installation path



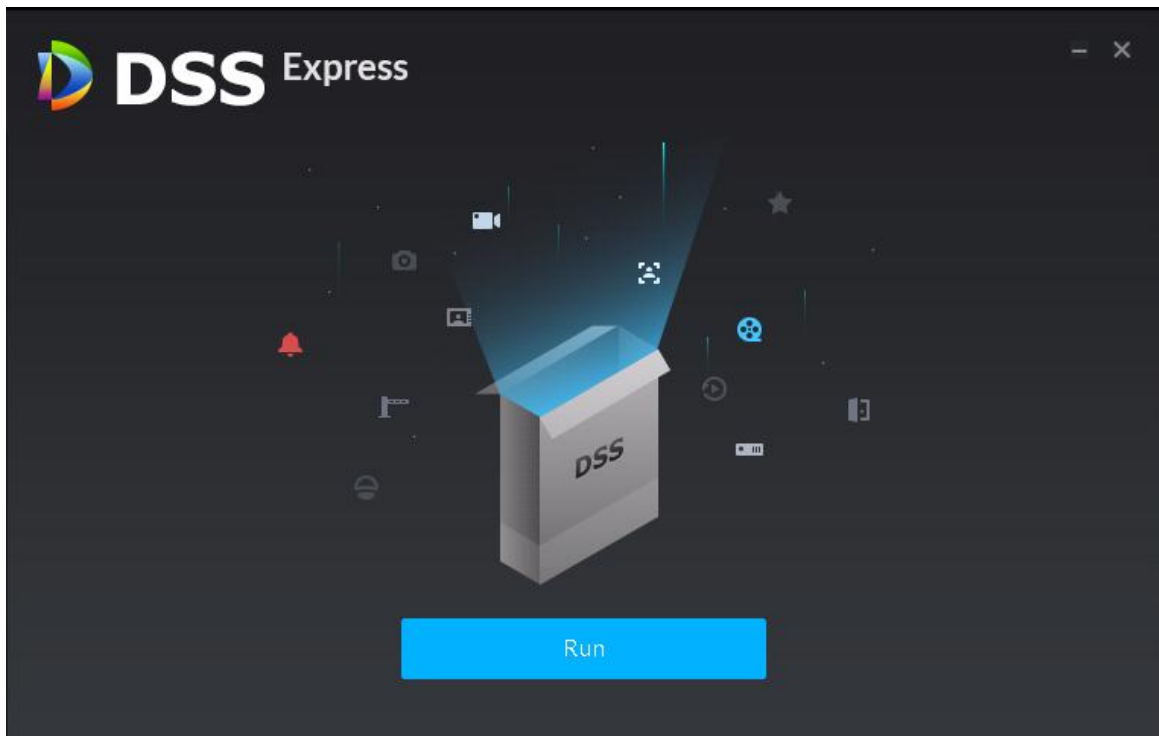
Step 5 Click **Browse** and select installation path, click **Install**.

The system displays installation progress, the installation takes about 2-3 minutes. The interface is shown in Figure 2-19 after installation is completed.



- The system automatically detects the available space of path after the installation path is selected, if available space is less than needed for system installation, then the icon **Install** beomes gray, and installation cannot be implemented.
- Do not select Generate Shortcuts if it is not necessary.

Figure 2-19 Installation completed



2.4.1.2 Mobile Phone APP

Currently mobile APP can be installed on IOS or Android.

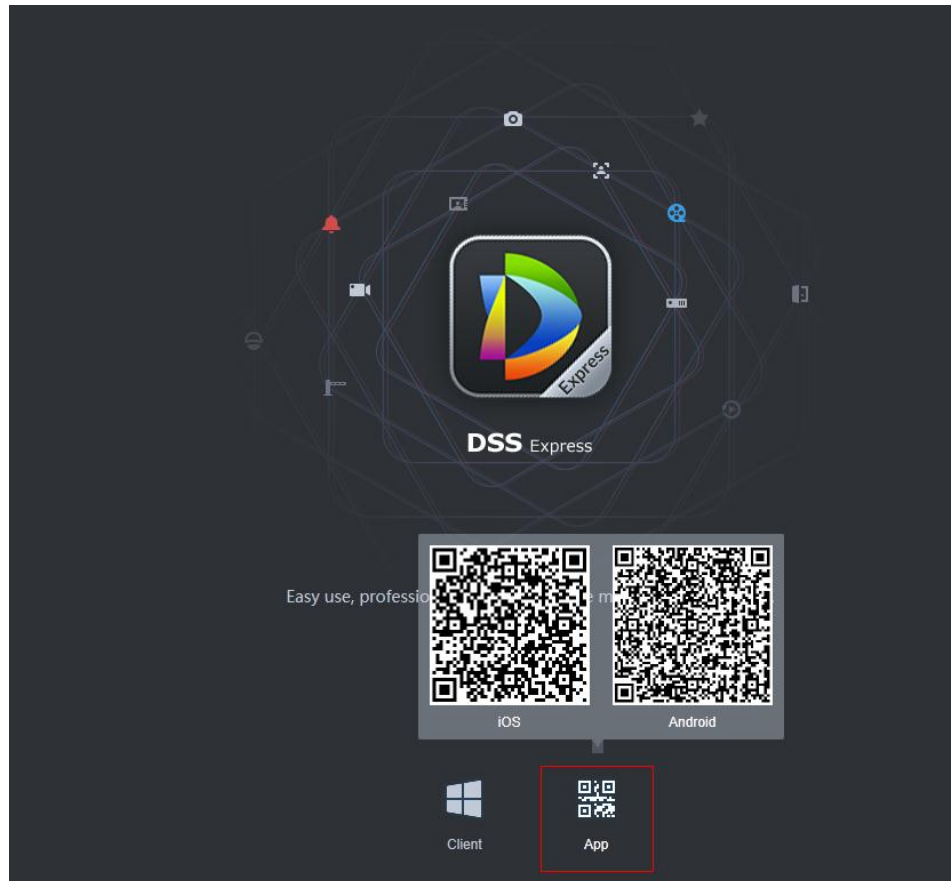


This manual only introduces how to install mobile phone APP, for more operation details, please refer to APP help document.

Step 1 Enter server IP address into browser, click **Enter**.

The system displays the interface of downloading client. See Figure 2-20.

Figure 2-20 Mobile APP QR code



Step 2 Move the mouse to , use mobile phone to scan corresponding QR code, then acquire and install APP according to prompt.

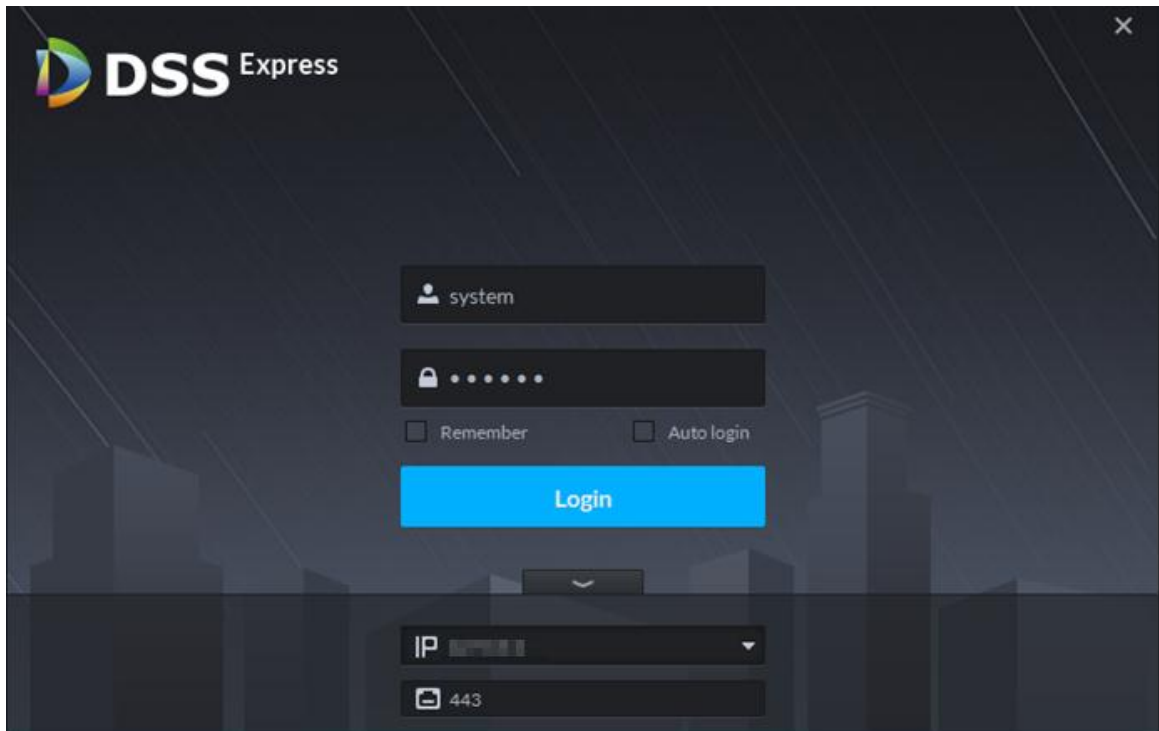
2.4.2 Initialization Config

You need to initialize server if you log in for the first time. Modify password, set security questions for system user. You can find password by answering questions when you forget password.



Step 1 Double click  on server desktop, or click Run on the interface after program is installed. The system displays client login interface. See Figure 2-21.

Figure 2-21 Client login interface



Step 2 Enter username and password.

The default username and password is system, 123456 respectively.

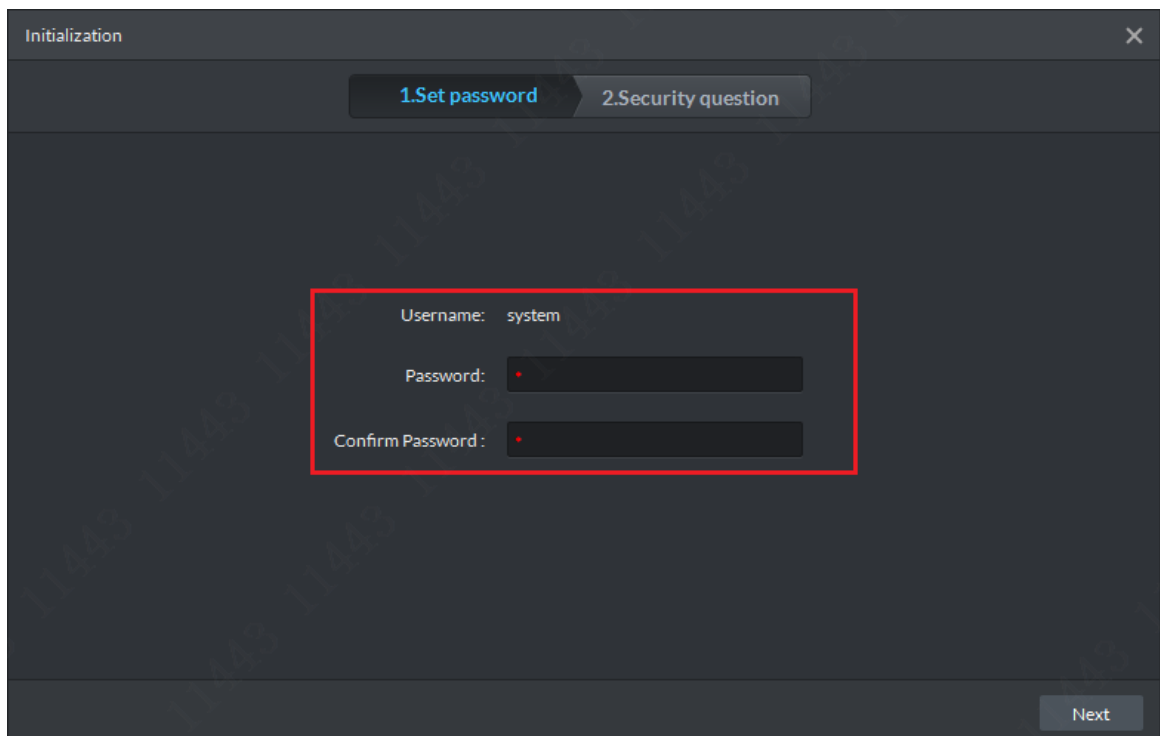
Step 3 Click , enter server IP address and HTTPS port number.

HTTPS port number is 441 by default.

Step 4 Click **Login**.

The system displays the interface of **Set Password**. See Figure 2-22.

Figure 2-22 Set password



Step 5 Enter new password, click **Next**.

The system displays the **Security Question** interface. See Figure 2-23.

Figure 2-23 Security question

The screenshot shows a window titled 'Initialization' with a close button (X) in the top right corner. Below the title bar, there are two tabs: '1.Set password' and '2.Security question'. The '2.Security question' tab is active. The main area contains three questions, each with a dropdown menu and an answer input field. The questions are: 'Question 1: Who is your favorite athlete?', 'Question 2: Who is your favorite pop star?', and 'Question 3: What is your favorite flower in s...'. Each answer field has a red asterisk (*) indicating it is required. An 'OK' button is located at the bottom right of the window.

Step 6 Select question, set answer, then click OK.

The system displays **Homepage** interface by default. See

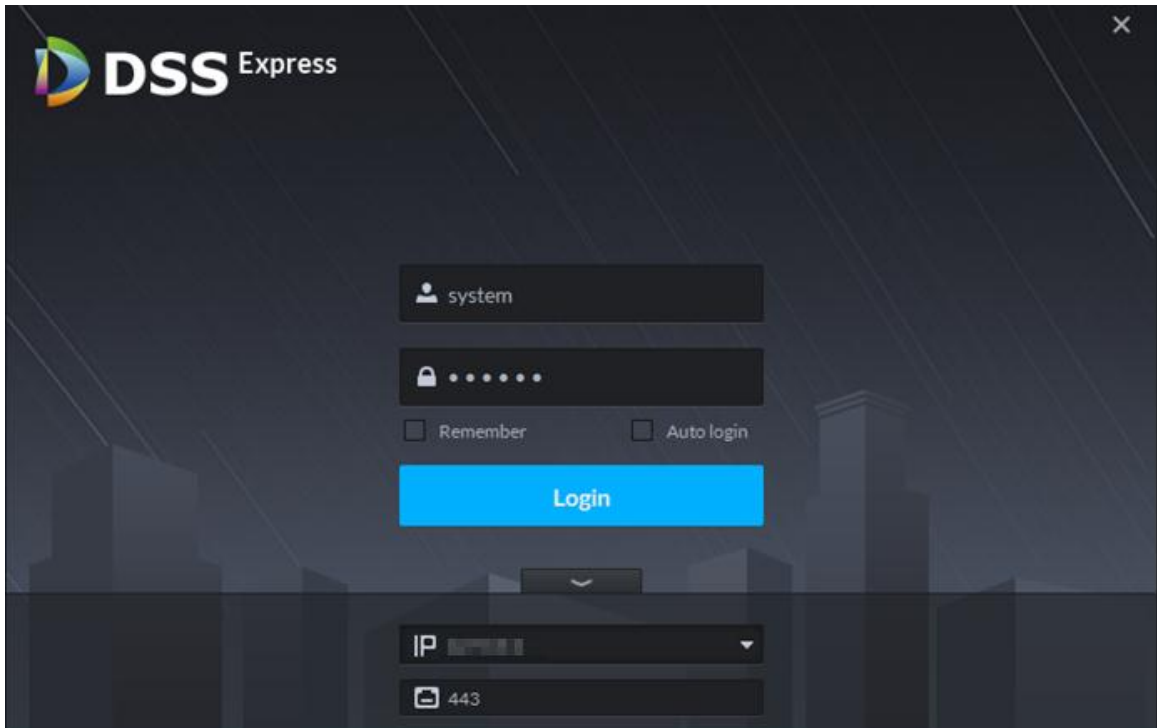
2.4.3 Logging in Client

You can configure and manage server remotely by login in client.

Step 1 Double click  on the server desktop, or click **Run** on the interface after program is installed.

The system displays client login interface, see Figure 2-24.

Figure 2-24 Client login interface



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

The system displays the **Homepage** interface. See Figure 2-25. For homepage description, see Table 2-5.



- If you need to switch server IP address, click , enter server IP address and HTTPS port number, HTTPS port is 443 by default.
- Select **Remember**, the system remembers the password when you log in again after logout.
- Select **Auto Login**, the system remembers the password and log in automatically when you log in again after logout.

Figure 2-25 Client homepage

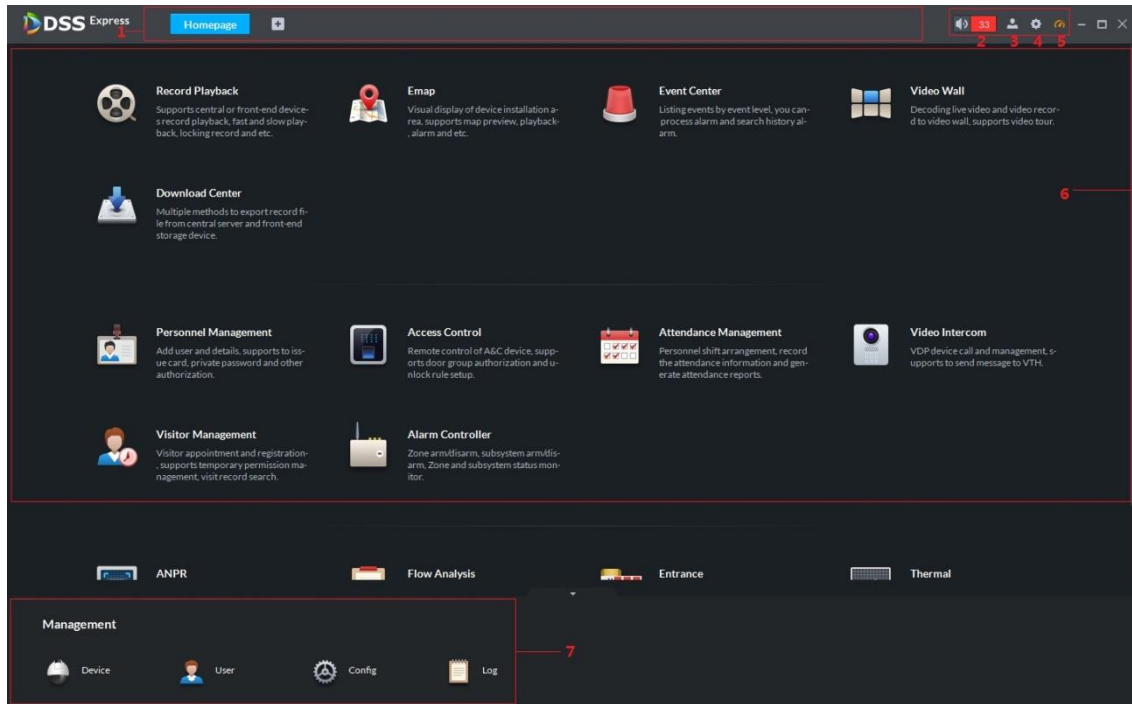


Table 2-5 Client homepage description

No.	Name	Description
1	Function Tab	Display all opened tabs. Click  and you can select the module you want to open. Homepage tab and  are displayed by default.
2	Alarm	: Alarm tone switch, the tone is on by default, click the icon and change to , tone is off. : Alarm quantity, when the number is not zero, you can click and jump to Event Center interface, and view alarm info.
3	User Info	Click the icon and select corresponding functions, you can modify password, lock client, view help and sign out. Supported operations are shown as follows: - View login username and service IP address. - Select Change Password and you can modify user password. - Select Lock Client, and you can lock client and client is not allowed to operate. If you want to operate, click anywhere on client and enter password to unlock. - Click Help to open user manual. - Select About and view client version info and release date. - Select Sign Out to log out, the system jumps to client login interface.
4	Config	Click the icon and you can make settings, such as basic setting, video setting, video playback, snapshot setting, record, alarm and shortcut button.

5	System Status	Click the icon and you can view the status of server network, CPU and memory.
6	Function	Display live preview, video playback, map, event center, video wall, download center, user management, access control and plate recognition. You can click corresponding function to enter.
7	Management	Display device management, user management, config management and log management. Click to enter corresponding management page. Click  and you can hide the section.

2.5 Importing License

License includes free version and paid version. The free license is imported by platform by default. If you want higher performance, please purchase license of paid version immediately.

2.5.1 License Introduction

For the functions supported by free version, see Table 2-6. For the restricted functions, see Table 2-7.

Table 2-6 License version description

Module	Free Version	Paid version
Video	64 channels	512 channels
POS	2 channels	50 channels
Access Control	64 IP, 64 doors	200 IP, 1024 doors
Video Intercom	128 IP	1024 IP
Alarm Host	1 IP	100 IP
ANPR	2 channels	32 channels
Face Recognition	2 channels	64 channels
Client	1	100 simultaneous login
Mobile APP	1	100 simultaneous login
Attendance Terminal	4 channels	512 channels
DSS Mobile for VDP	10	5000 register

Table 2-7 Restricted functions of paid version

Function Module	Sub Function
Login	Multi-client login
Device	Onvif > 8 channels
Storage Management	Network disk  IPSAN storage.
Video	Enable remote record
	Continuous snapshot

Function Module	Sub Function
	ROI
	Alarm output control
	Switch playback
	Smart track (fisheye+PTZ)
	Playback on video wall
Event Management	Link video wall
	Event forwarding
	Send email 
	Send email actively when dealing with event.
	Temporary disarm
	Alarm processing
Video Wall	Video wall tour
E map	Multi-layer map 
	Hot zone application (only single layer map can be used)
	Visible range 
Personnel Management	Restrict custom visible range.
	Issue cards in batch
	Import and export personnel in batch
Face Recognition	Access control track
	Face track

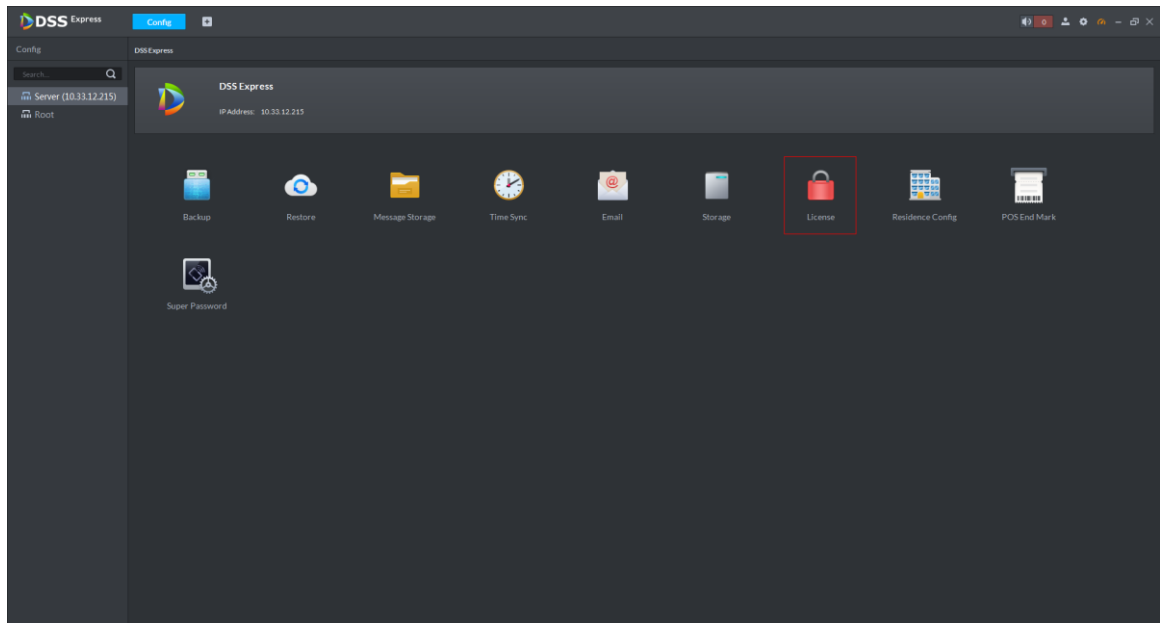
2.5.2 Applying License

Step 1 Acquire license request file.

- 1) Click **Config** on the client homepage.

The system displays the **Config** interface. See Figure 2-26.

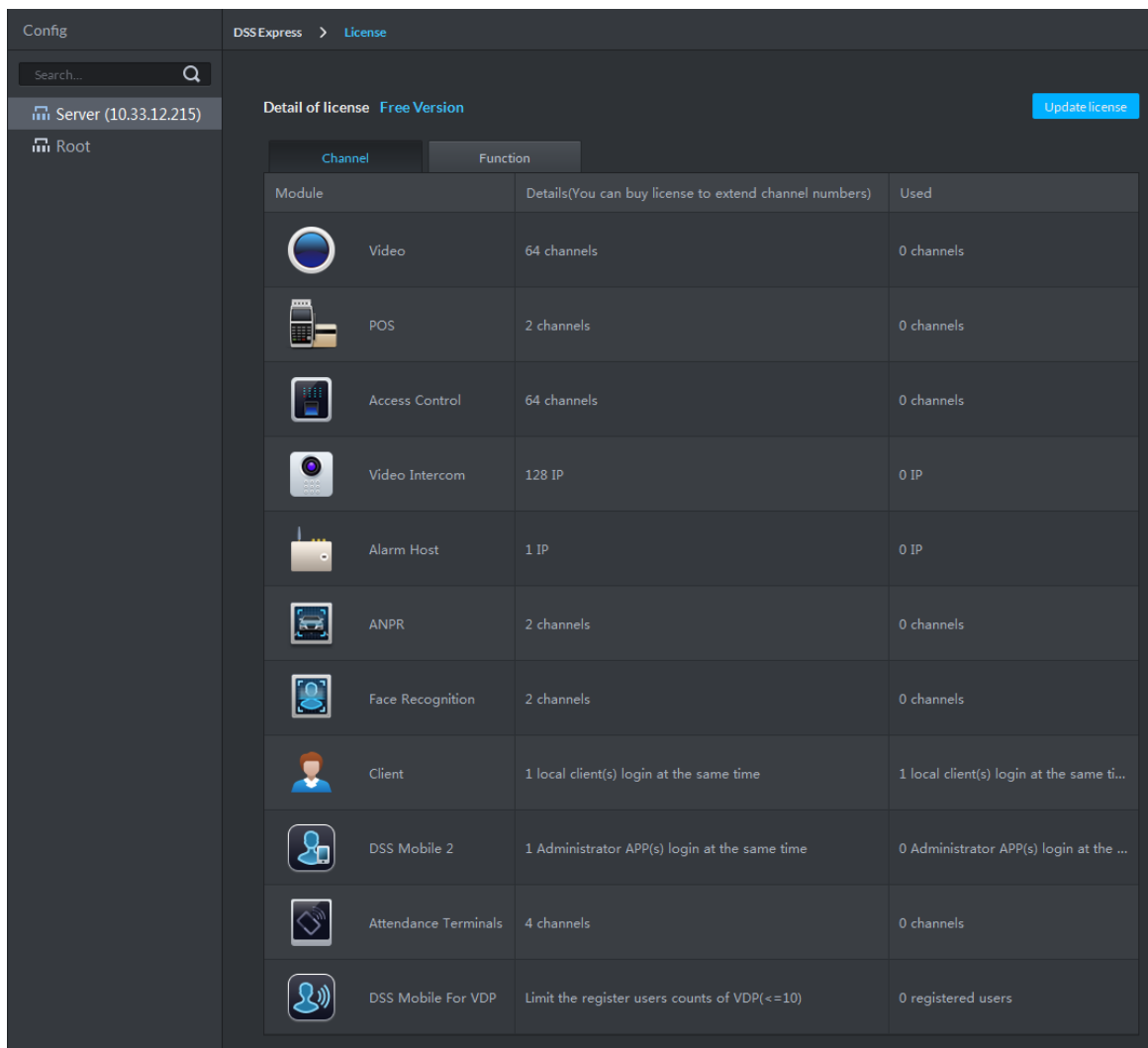
Figure 2-26 Config



2) Click **License**.

The system displays **License** interface. See Figure 2-27.

Figure 2-27 Export license request file



3) Click **Export**.

The system displays the interface of **Export License Request File**, See Figure 2-28.

Figure 2-28 Export license request file

The screenshot shows the 'Export License Request File' window. It has a dark theme. The left pane, titled 'Base License', contains several sections with green checkmarks indicating enabled features: 'Login' with 'Multiple Client Login'; 'DSS Mobile' with 'Multiple Administrator APP(s) login' and 'User registration of VDP(>10)'; 'Device' with 'Onvif > 8 channels'; 'Storage' with 'Net Disk'; and 'Video' with 'ROI', 'Quick Switch to Playback', 'Playback on Wall', 'Start Remote Record', 'Continuous Snapshot', and 'Alarm Output Control'. The right pane, titled 'Device License', contains five rows of settings, each with a label, a value in a dropdown menu, and a unit: 'Video' (64 channels), 'POS' (2 channels), 'Access Control' (64 channels), 'Video Intercom' (128 IP), and 'Alarm Host' (1 IP). At the bottom right of the window are two buttons: 'Export' (highlighted in blue) and 'Cancel'.

- 4) Enter channel and IP quantity according to actual situation, click **Export**.
License request file is saved in the DSS Express client installation path in the form of .zip

Step 2 Send license request file to sales.

Sales make and return License file according to license request file.

2.5.3 Loading License

Step 1 On the client homepage, select **Config > License**.

The system displays the interface of **License**.

Step 2 Click **Update License**.

The system moves to the license update section, see Figure 2-29.

Figure 2-29 Update license

Config

Search...

Server (10.33.12.215)

Root

DSS Express > License

	POS	2 channels	0 channels
	Access Control	64 channels	0 channels
	Video Intercom	128 IP	0 IP
	Alarm Host	1 IP	0 IP
	ANPR	2 channels	0 channels
	Face Recognition	2 channels	0 channels
	Client	1 local client(s) login at the same time	1 local client(s) login at the same ti...
	DSS Mobile 2	1 Administrator APP(s) login at the same time	0 Administrator APP(s) login at the ...
	Attendance Terminals	4 channels	0 channels
	DSS Mobile For VDP	Limit the register users counts of VDP(<=10)	0 registered users

Update license

Step1: Export license request file

Export

Step2: Contact sales person for license

Step3: Import license file

File Path:

Browse

Import

Step 3 Click **Browse**, select License file you want to upload according to system prompt.

Step 4 Click **Import**.

System loads License, after that the system prompts license info is changed and the program restarts.

Step 5 Log in client again, enter license config interface, and make sure the License is the same as applied.

3 Operation Guide

3.1 Installing Client

After installing and logging in client, you can configure and manage server remotely. For detailed operation, see **2.4 Installing Client**

3.2 Basic Config

After installation and deployment is completed, you need to configure basic information including add device, configure message storage, time sync, email, storage space, user and record plan.

3.2.1 System Setting

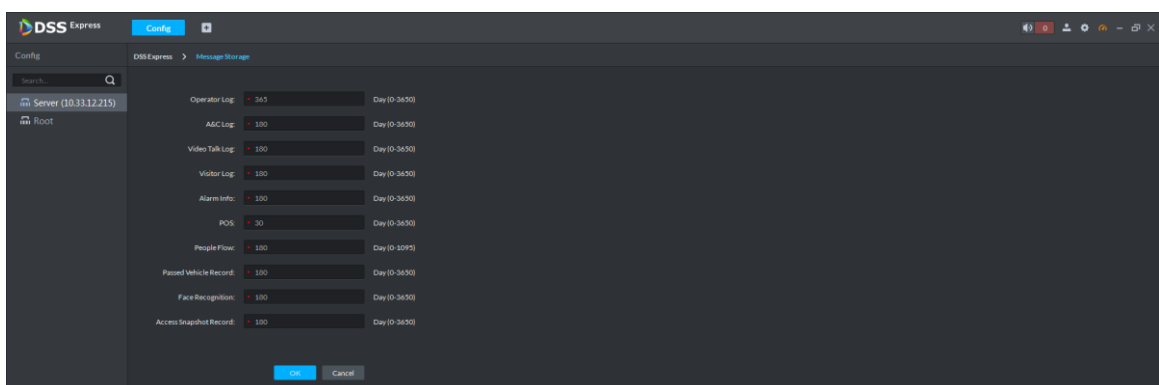
3.2.1.1 Setting Message Storage

You can set storage duration of operator log, A&C log, video talk log, alarm info, passed vehicle record, face recognition and picture storage. System deletes information when exceeding duration threshold.

Step 1 Enter the config interface of **Message Storage**.

- 1) On the client homepage, click **Config**.
The system displays **Config** interface.
- 2) Click **Message Storage**.
The system displays **Message Storage** interface. See Figure 3-1.

Figure 3-1 Message storage



Step 2 Set storage duration log.

Step 3 Click **OK**.

The config is saved and takes effect.

3.2.1.2 Time Sync

Time sync means synchronizing the time between server and PC where client is located, server and accessed encoder or access control. The system time of server is considered as standard time after sync. The platform supports two methods of time sync which are auto and manual.

3.2.1.2.1 Auto Time Sync

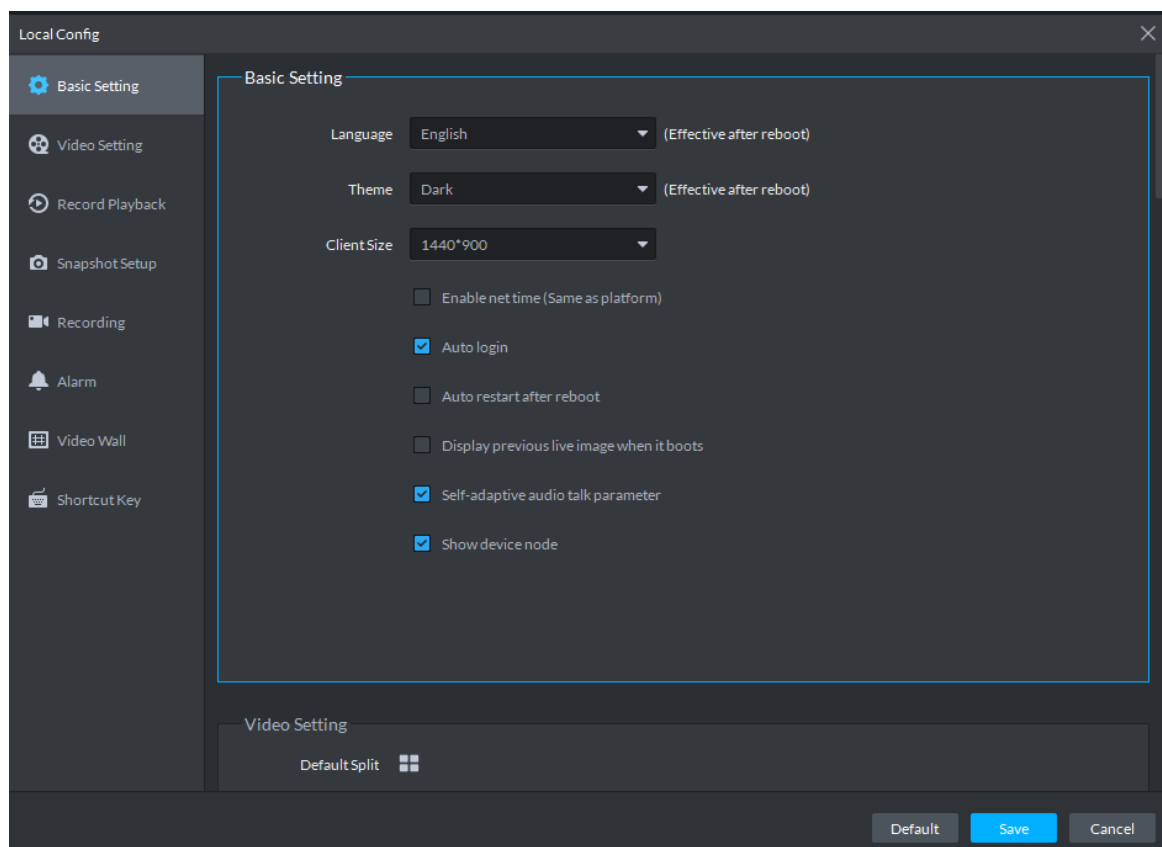
The system automatically starts time sync within designated period and time.

Step 1 Enable time sync on local config of client.(Optional)

Synchronize time between server and PC where client is located, the item is required to be configured. Skip the step if you only need to synchronize time of server and accessed device.

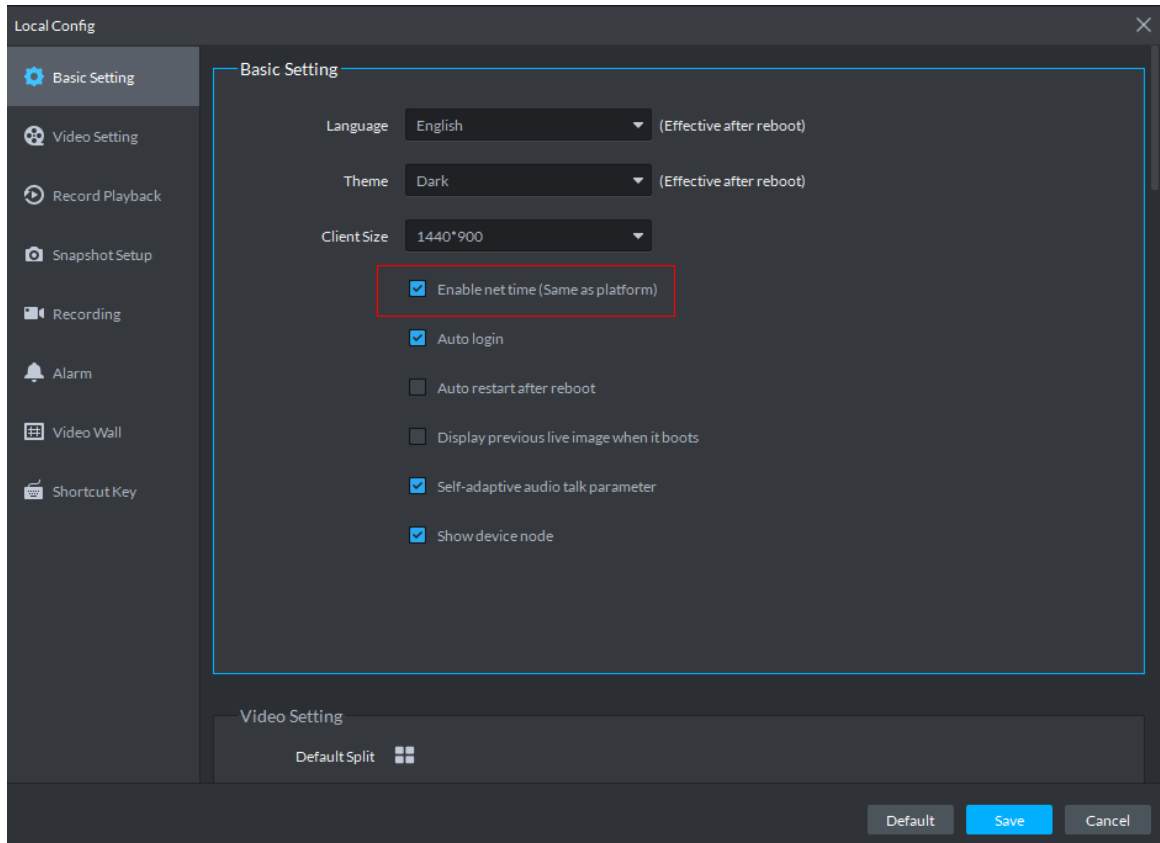
- 1) Click  on the upper right corner of client interface.
The system displays the interface of **Local Config**. See Figure 3-2.

Figure 3-2 Local config



- 2) Click the tab of **Basic Config**.
The system displays **Basic Config** interface. See Figure 3-3.

Figure 3-3 Enable net time



- 3) Select **Enable net time (Same as platform)**, click **Save**.

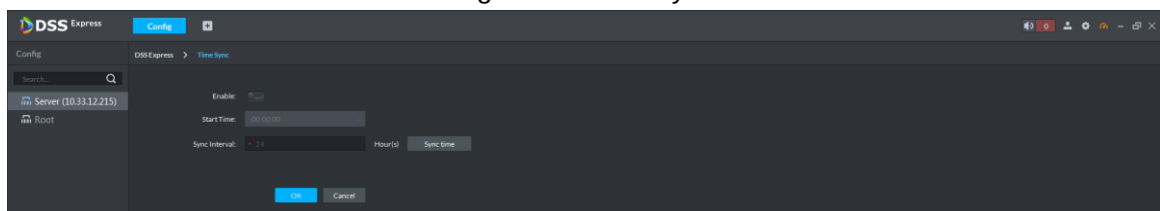


Enable net time on client of local config, the client immediately makes a net time request to server and complete time sync.

Step 2 Enter **Time Sync** config interface.

- 1) On client homepage, click **Config**.
The system displays **Config** interface.
- 2) Click **Time Sync**.
The system displays the interface of **Time Sync**. See Figure 3-4.

Figure 3-4 Time sync



- Step 3** Click  next to **Enable**, and enable auto time sync.

The icon becomes  and auto time sync is enabled.

Step 4 Set start time and sync interval, click **OK**.

Set start time of each period, synchronize time between server and PC client, and synchronize time between server and accessed device.

3.2.1.2.2 Manual Time Sync

Start time sync request manually, and the system responds to request immediately.

Step 1 Enable time sync on local config of client.(Optional)

Synchronize time between server and PC client, the item is required to be configured.

Skip the step if you only need to synchronize time of server and accessed device.

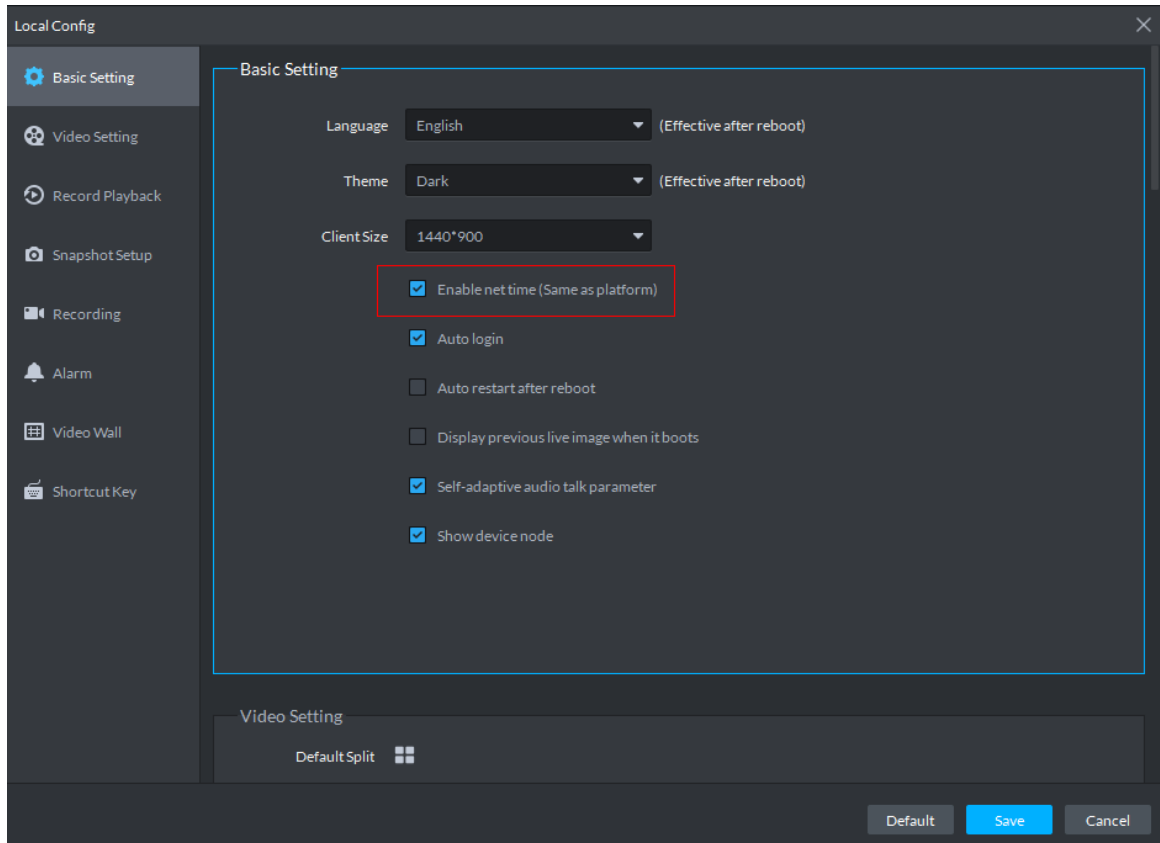
- 1) Click  on upper right corner of client interface.

The system displays the interface of **Local Config**.

- 2) Click the tab of Basic Setting.

The system displays the interface of **Basic Setting**. See Figure 3-5.

Figure 3-5 Enable client time sync



- 3) Select **Enable net time (Same as platform)**, click **Save**.



Enable net time on client of local config, the client immediately makes a net time request to server and complete time sync.

Step 2 Enter config interface of **Time Sync**.

- 1) On client homepage, click **Config**.

The system displays **Config** interface.

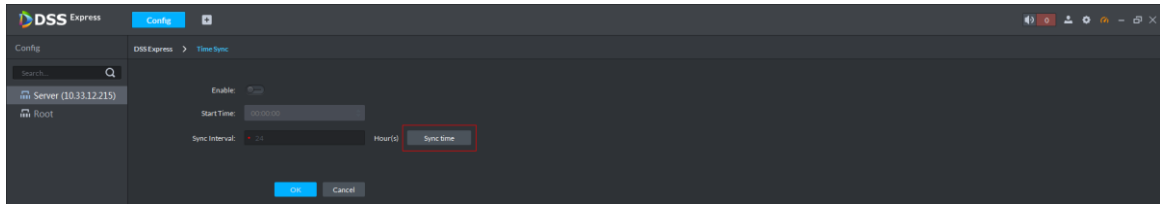
- 2) Click Time Sync.

The system displays the interface of Time Sync. See Figure 3-4.

Step 3 Click **Sync Time**, see Figure 3-6.

The system immediately synchronizes time between server and accessed device, server and PC client.

Figure 3-6 Sync time



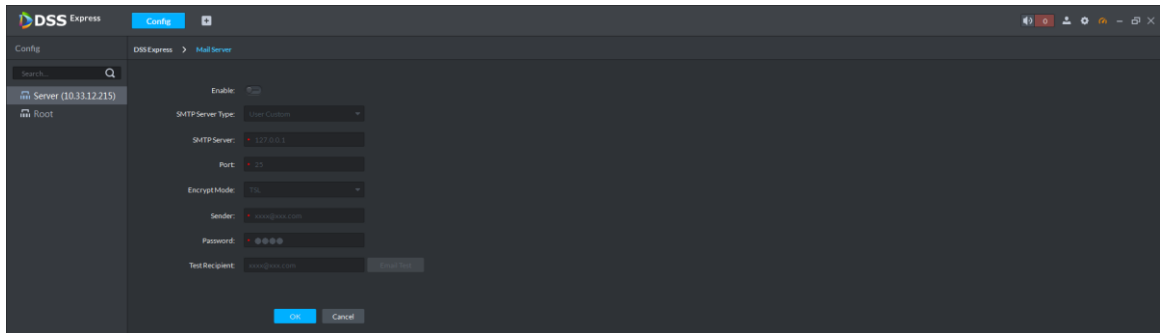
3.2.1.3 Setting Email

Set email address info, you can send email via designated email address when necessary. For example, after alarm linkage email is enabled, when alarm event occurs, the system automatically sends email to inform user.

Step 1 Enter the config interface of **Mail Server**.

- 1) Click **Config** on the client homepage.
The system displays **Config** interface.
- 2) Click **Email**.
The system displays **Mail Server** interface. See Figure 3-7.

Figure 3-7 Email server



Step 2 Click , and enable email.

The icon becomes  and the function is enabled.

Step 3 Select SMTP server type, set email address info, and click **OK**.



TSL encryption method is highly recommended.

3.2.1.4 Setting Storage Space

Configure local storage space or connect network storage device, used to store pictures and videos.

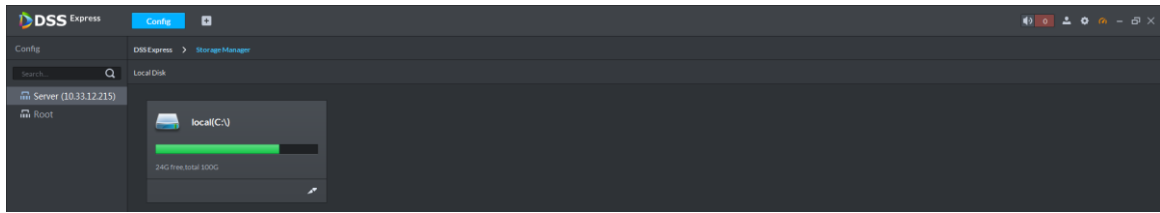
3.2.1.4.1 Setting Local Storage Disk

The system automatically detects storage space of all the disks in the system, and creates exclusive space for platform, used to store videos, general pictures and ANPR pictures.

Step 1 Enter config interface of **Storage Manager**.

- 1) Click **Config** on the client homepage.
The system displays the interface of **Config**.
- 2) Click **Storage**.
The system displays **Storage Manager** Interface; the system automatically detects disk info of server (Disk info of non PC client). See Figure 3-8.

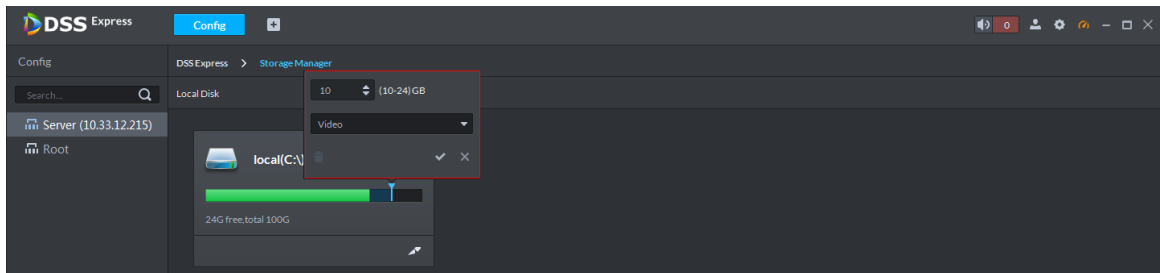
Figure 3-8 Storage manager



Step 2 Click .

The system pops out the dialog of setting storage space size and type. See Figure 3-9.

Figure 3-9 Create storage space



Step 3 Set storage space size, select storage space type and click .

Platform exclusive storage space is created on the disk, see Figure 3-10. The exclusive storage space is displayed in the red box.



- The minimum storage space is 10GB.
- Storage space type includes video, general picture and ANPR picture. Video disk is used to store video, ANPR picture disk is used to store ANPR snapshot, general picture is used to store all snapshots except ANPR pictures.
- One local disk can divide general pictures for once top, but it can also modify storage space of general pictures.
- If you want to delete the storage space, you can click the storage segment, and delete exclusive space setting according to system prompt. See Figure 3-11.

Figure 3-10 Disk status change

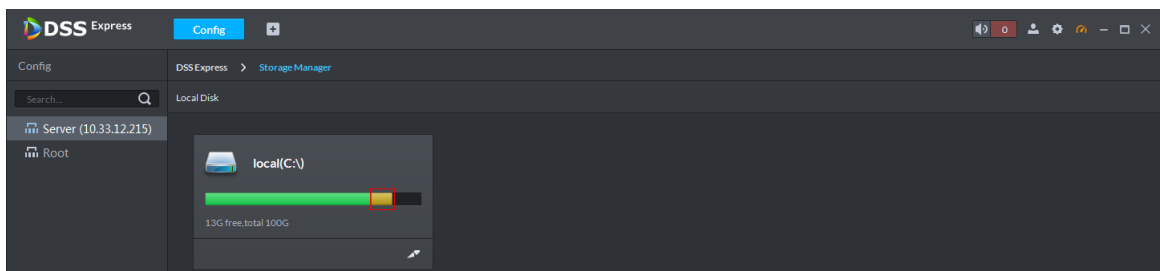
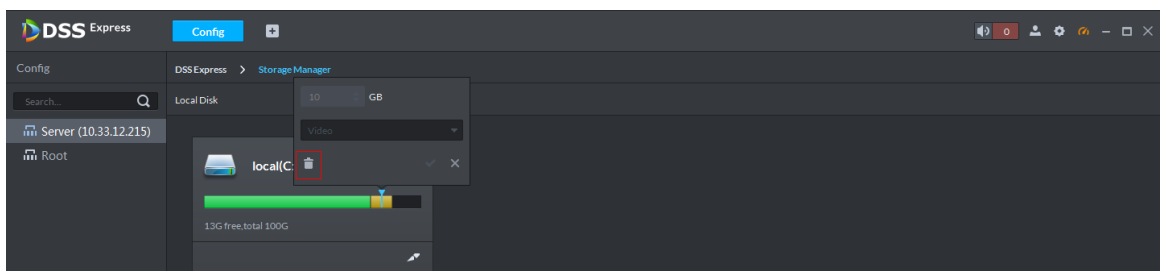


Figure 3-11 Delete exclusive storage space



3.2.1.4.2 Setting Network Disk

If network storage device exists in networking, you can create platform's exclusive storage space on network storage device, used to store video and ANPR pictures.

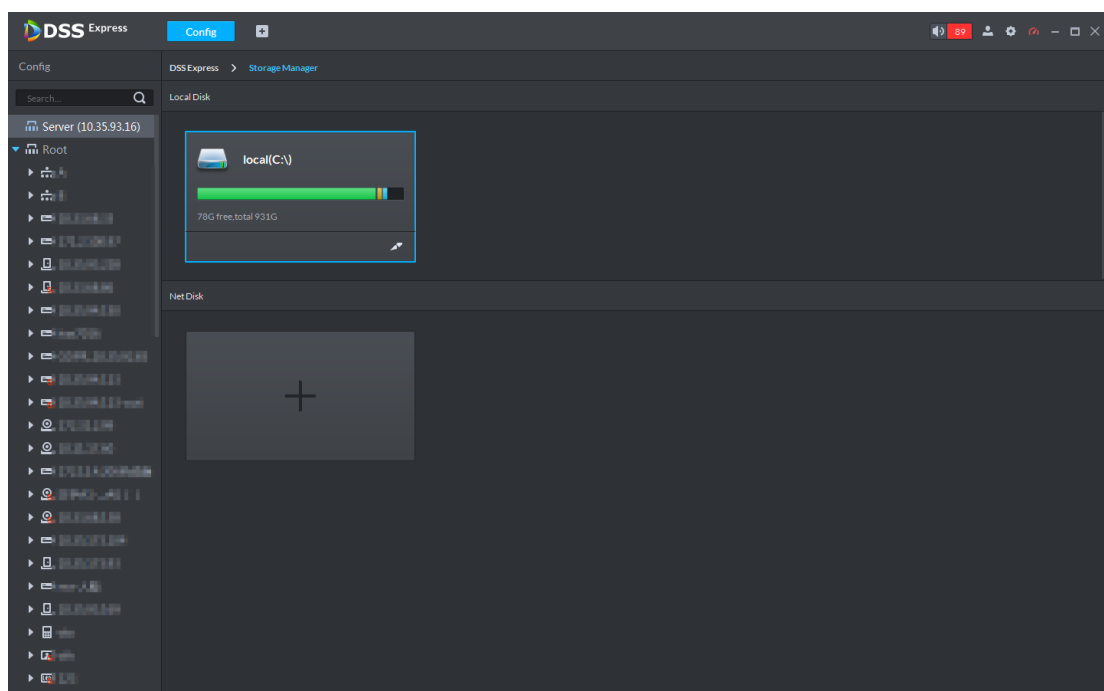


- Storage server is required to be deployed.
- One user volume of current network disk can only be used by one server at the same time.
- User volume needs to be formatted if you want to add network disk.

Step 1 Enter the config interface of **Storage Manager**.

- 1) Click **Config** on the client homepage.
The system displays the **Config** interface.
- 2) Click **Storage**.
The system displays **Storage Manager** interface. See Figure 3-12.

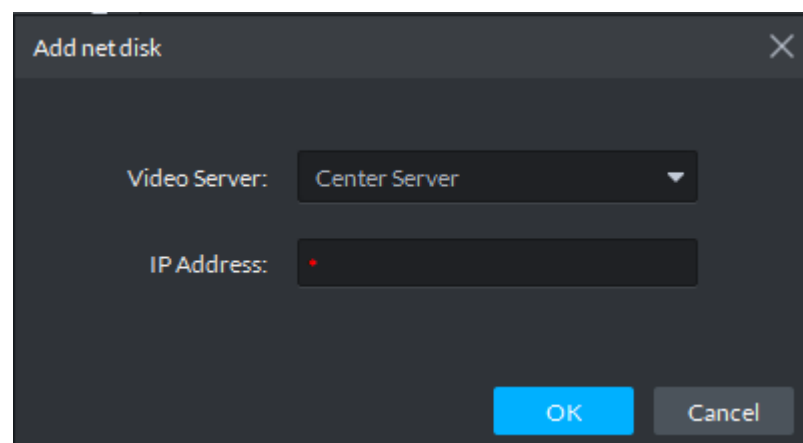
Figure 3-12 Storage manager



Step 2 Click .

The system pops out the interface of **Add Network Disk**. See Figure 3-13.

Figure 3-13 Fill in IP



Step 3 Enter IP address of network storage device, click **OK**.

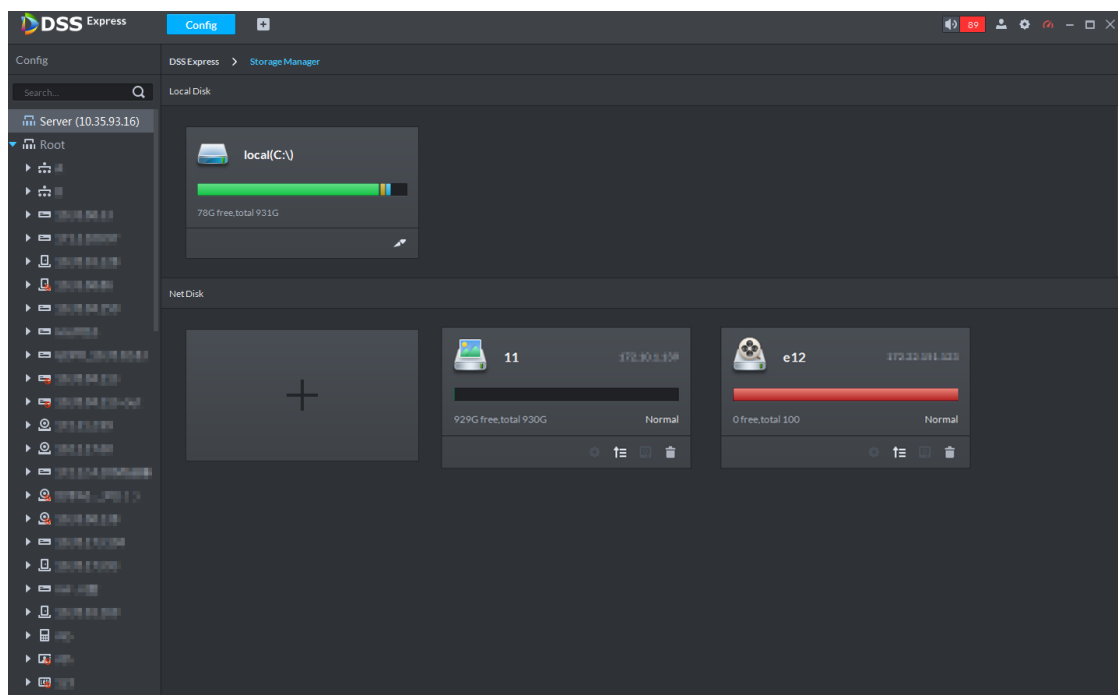
See Figure 3-14 for the adding result, green means remaining space, red means used space which can be overwritten.



If network disk is not formatted, please format it according to system prompt. The operations of adding network disk are shown as follows.

- Click  and modify storage space type of disk, including video and ANPR picture. Video disk is used to store video, ANPR picture disk is used to store ANPR snapshot. If you need to store ANPR device snapshot, storage space type must be set as ANPR picture.
- Click  and take the network disk used by other devices. Please make sure other device has stopped recording or snapshot before being taken, otherwise it will cause video or picture loss.
- Click  and delete network disk. Please make sure recording or snapshot has stopped before being deleted, otherwise it will cause video or picture loss.

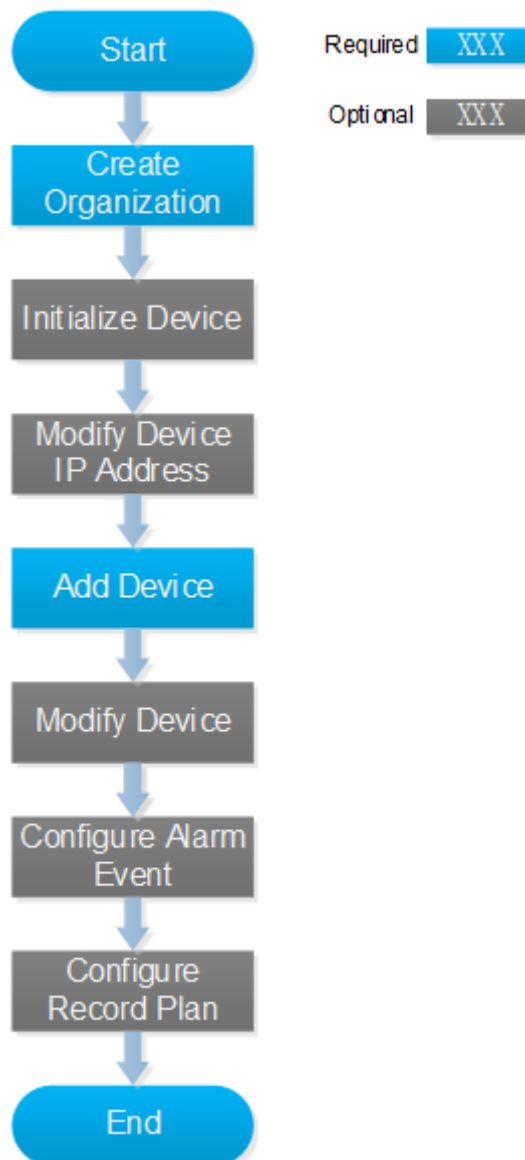
Figure 3-14 Network disk



3.2.2 Managing Device

After device is added on the server, you can operate device remotely by server. The flow of device management is shown in Figure 3-15.

Figure 3-15 Device management flow



3.2.2.1 Creating Organization

Create organization and realize device management by organizations. **Root Node** organization already exists by default, if no organization is created, then all the added devices belong to the root node.

Step 1 Click **Device** on the client homepage.

The system displays the **Device** interface. See Figure 3-16. The device is online if online status is green, device is offline if online status is red.

Figure 3-16 Device

Device ID	IP	Device Name	Device Type	Device Model	Organization	Online Status	Offline Reason	Operation
1000012	192.168.1.1	192.168.1.1	DVR		A	Offline	Abnormal network	✎ ✕
1000048	192.168.1.1	192.168.1.1	Remaining Parkin...		Root	Offline	Unknown reason	✎ ✕
1000046	192.168.1.1	192.168.1.1	Matrix Device		Root	Offline	Unknown reason	✎ ✕
1000037	192.168.1.1	192.168.1.1	ANPR Device		Root	Offline	Unknown reason	✎ ✕
1000031	192.168.1.1	192.168.1.1	IPC	SmartIPC	Root	Online		✎ ✕ ⚙
1000045	192.168.1.1	192.168.1.1	Access Snapshot ...		Root	Online		✎ ✕
1000000	192.168.1.1	192.168.1.1	DVR	N5	Root	Online		✎ ✕ ⚙
1000014	192.168.1.1	192.168.1.1	Access Controller	ASC1202B-D	Root	Offline	Unknown reason	✎ ✕
1000025	192.168.1.1	192.168.1.1	IPC	SmartIPC	Root	Offline	Abnormal network	✎ ✕
1000039	192.168.1.1	192.168.1.1	IPC	SmartIPC	Root	Offline	Abnormal network	✎ ✕
1000009	192.168.1.1	192.168.1.1	IPC	IPC-HF81200E	B	Offline	Abnormal network	✎ ✕
1000010	192.168.1.1	192.168.1.1	IPC	IPC-HF81200E	B	Offline	The account is in t...	✎ ✕
1000076	192.168.1.1	192.168.1.1	IPC	IP Camera	Root	Offline	The account is in t...	✎ ✕
1000077	192.168.1.1	192.168.1.1	DVR		Root	Offline	The account is loc...	✎ ✕
1000079	192.168.1.1	192.168.1.1	IPC	DH-SD6AE230F-HNI	Root	Offline	The account is in t...	✎ ✕
1000055	192.168.1.1	192.168.1.1	NVR	DHI-NVR5832-16P-4KS2	Root	Online		✎ ✕ ⚙
1000073	192.168.1.1	192.168.1.1	Alarm Host	ARC	Root	Online		✎ ✕
1000074	192.168.1.1	192.168.1.1	DVR	HDVR	Root	Online		✎ ✕ ⚙
1000075	192.168.1.1	192.168.1.1	NVR	DHI-NVR5208-4KS2	Root	Online		✎ ✕ ⚙
1000023	192.168.1.1	192.168.1.1	NVR	DH-NVR5832-4KS2	Root	Online		✎ ✕ ⚙

Step 2 Select organization, click  or right click organization, select Create Organization.

The system displays the interface of **Create Organization**. See Figure 3-17.

Figure 3-17 Create organization

CreateOrganization

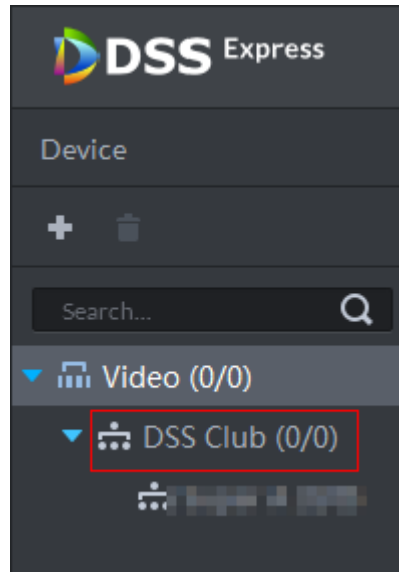
Organization:

OK Cancel

Step 3 Enter organization name, click **OK**.

The system displays info of added organization. See Figure 3-18.

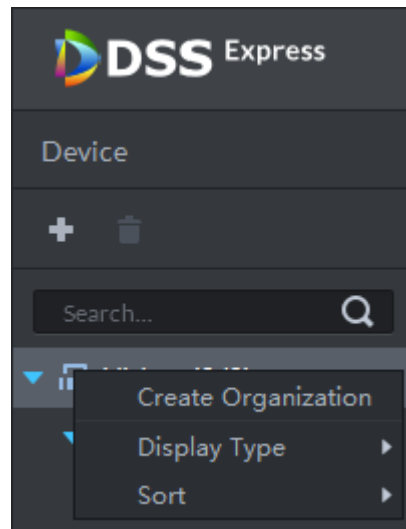
Figure 3-18 Organization list



More operations of organization are shown as follows:

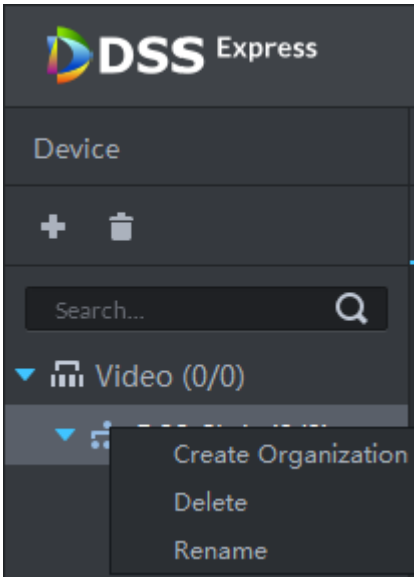
- Root node supports creating subordinate organization; Set display type means setting device display by name or IP; Set sort means setting sort mode of all devices and organizations under root node, including ascending, descending and default order. See Figure 3-19.

Figure 3-19 Root node operation



- Child node organization supports creating subordinate child node organization; delete and rename organization. See Figure 3-20.

Figure 3-20 Child node organization

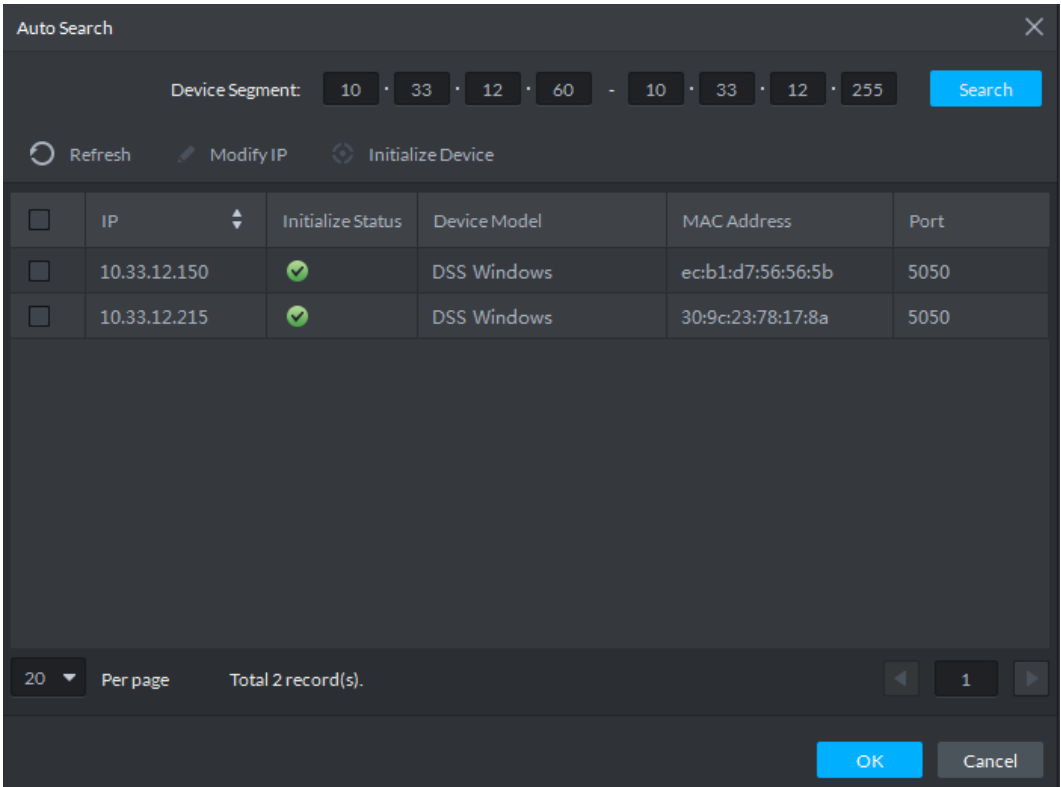


3.2.2.2 Initializing Device

The device is required to configure admin account password and security questions after being delivered out of factory; otherwise, it cannot be used normally. The platform supports initializing device remotely.

- Step 1 Click **Device** on the client homepage.
The system displays the **Device** interface.
- Step 2 Click **Auto Search**.
The system displays the **Auto Search** interface.
- Step 3 Enter start IP and end IP, click **Search**.
The system displays search results.

Figure 3-21 Search result



Step 4 Select uninitialized device, click **Initialize Device**.

The system displays **Set Password**. See Figure 3-22.



Several devices can be initialized together.

Figure 3-22 Set password

The screenshot shows a dark-themed window titled "Initialize Device" with a close button (X) in the top right corner. At the top, there are three tabs: "1. Set Password" (active), "2. Password Security", and "3. Modify IP". The main area displays the following fields:

- Username: admin
- Password: [Redacted]
- Confirm Password: [Redacted]

At the bottom right, there are two buttons: "Password Security" (highlighted in blue with a right arrow) and "Cancel".

Step 5 Enter password, click **Password Security**. See Figure 3-23.

Figure 3-23 Password security

Initialize Device

1. Set password 2. Password security 3. Change IP

☒ Email ☐ Tel

Bind email address: * Used to reset the password

Previous Step Modify IP → Cancel

Step 6 Select email or phone, enter corresponding email address or phone number, click **Modify IP**. The system displays **Modify IP** interface. See Figure 3-24.

Figure 3-24 Modify IP

Initialize Device

1. Set Password 2. Password Security 3. Modify IP

New IP: [] . [] . [] . []

Subnet Mask: [] . [] . [] . []

Gateway: [] . [] . [] . []

Previous OK Cancel

Step 7 Enter new IP address, subnet mask and gateway, click **OK**.

3.2.2.3 Modifying Device IP Address

You can modify device IP address on the auto search interface.

Step 1 Click **Device** on the client homepage.

The system displays **Device** interface.

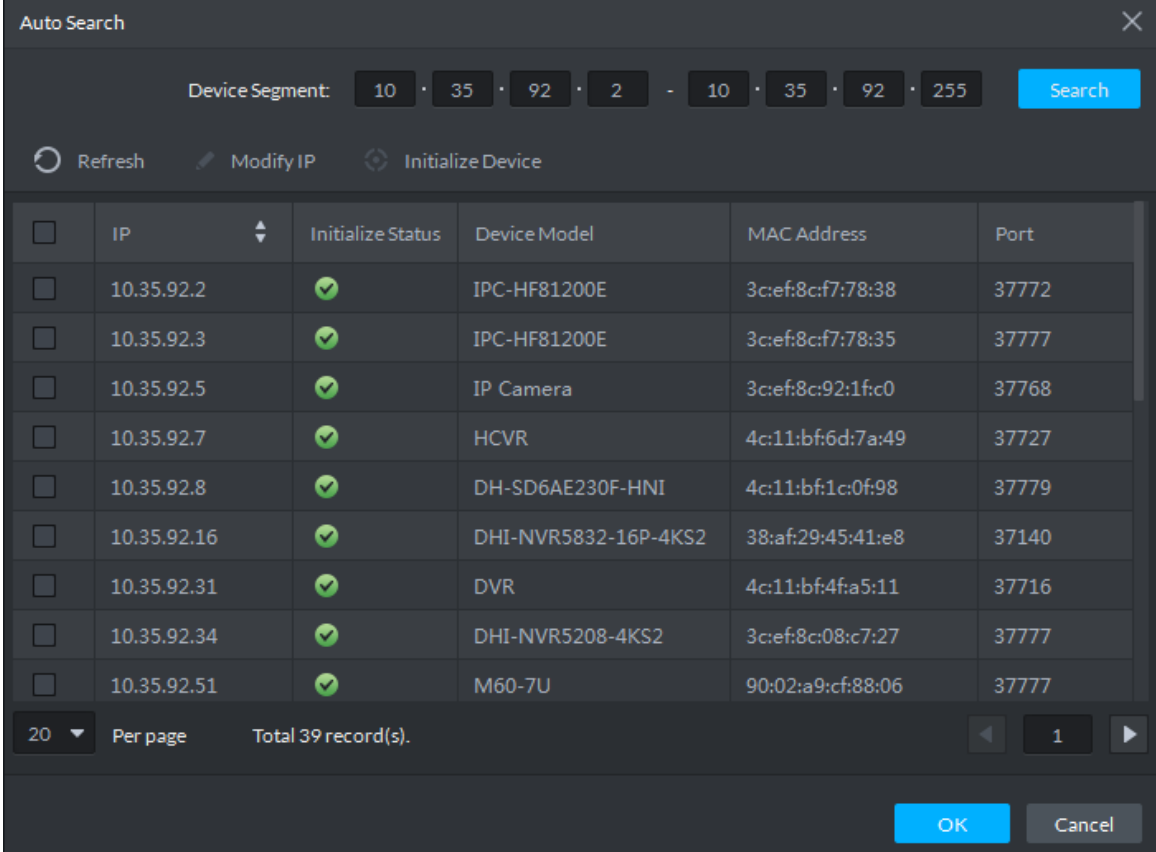
Step 2 Click **Auto Search**.

The system displays **Auto Search** interface.

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

The system displays search result. See Figure 3-25.

Figure 3-25 Search result



☐	IP	Initialize Status	Device Model	MAC Address	Port
☐	10.35.92.2	✓	IPC-HF81200E	3c:ef:8c:f7:78:38	37772
☐	10.35.92.3	✓	IPC-HF81200E	3c:ef:8c:f7:78:35	37777
☐	10.35.92.5	✓	IP Camera	3c:ef:8c:92:1f:c0	37768
☐	10.35.92.7	✓	HCVR	4c:11:bf:6d:7a:49	37727
☐	10.35.92.8	✓	DH-SD6AE230F-HNI	4c:11:bf:1c:0f:98	37779
☐	10.35.92.16	✓	DHI-NVR5832-16P-4KS2	38:af:29:45:41:e8	37140
☐	10.35.92.31	✓	DVR	4c:11:bf:4f:a5:11	37716
☐	10.35.92.34	✓	DHI-NVR5208-4KS2	3c:ef:8c:08:c7:27	37777
☐	10.35.92.51	✓	M60-7U	90:02:a9:cf:88:06	37777

20 Per page Total 39 record(s). 1

OK Cancel

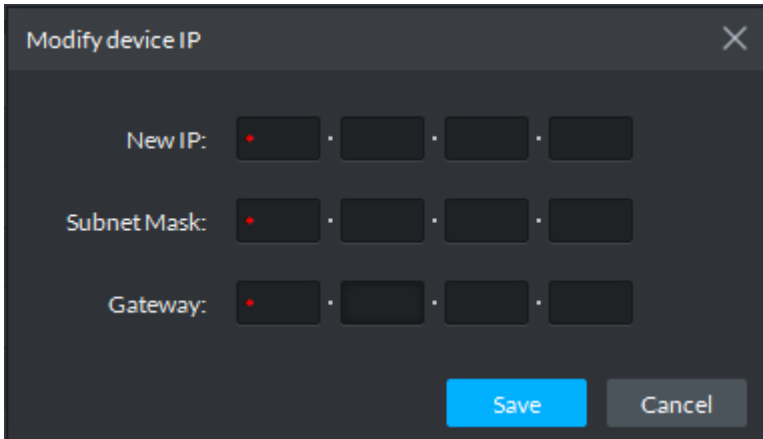
Step 4 Select device whose IP address needs to be modified, click **Modify IP**.

The system displays the interface of **Modify Device IP**.

Step 5 Modify device IP, click **OK**.

- When you select one device, the system pops out the **Modify Device IP** dialog box. See Figure 3-26.

Figure 3-26 Singly modify device IP



Modify device IP

New IP: . . .

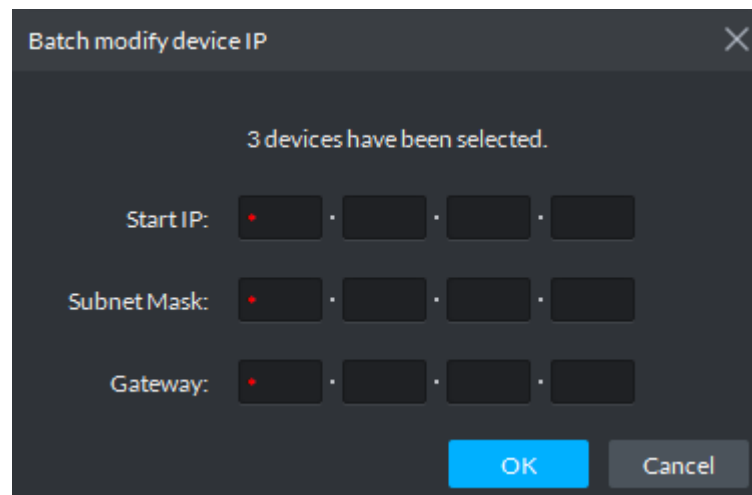
Subnet Mask: . . .

Gateway: . . .

Save Cancel

- When you select several devices, the system pops out the dialog box of **Batch Modify Device IP**. See Figure 3-27.

Figure 3-27 Batch modify device IP



The dialog box titled "Batch modify device IP" has a close button (X) in the top right corner. It displays the message "3 devices have been selected." Below this, there are three rows of input fields, each with a label and four separate boxes for IP octets. The first row is labeled "Start IP:", the second "Subnet Mask:", and the third "Gateway:". Each octet box has a red dot in its top-left corner. At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (gray).

Step 6 Set new IP address or start IP, subnet mask and gateway.

Modify in batches, IP address increases by 1 sequentially.

Step 7 Click **Save** or **OK**.

3.2.2.4 Adding Device

You can add access control, encoder, decoder, video wall, ANPR and matrix, after that you can manage and configure device remotely on client.



If users want to use the newly added device, enter **User** interface, edit user to make him have permission to use the device, otherwise, the device cannot be used.

3.2.2.4.1 Searching and Adding Device

Add several devices, and devices are in the same network segment, login username is the same as password. The system can search all the devices covered by server network.

Step 1 Click **Device** on the client homepage.

The system displays the **Device** interface.

Step 2 Click **Auto Search**.

The system displays the interface of **Auto Search**. See Figure 3-28. The system searches the device with the same segment as server by default.



- Click **Refresh** to refresh device info.
- Select device, click Modify IP and modify device IP address. For details, see 3.2.2.3 Modifying Device IP Address.
- Select uninitialized device, click Initialize Device and initialize device. For details, see 3.2.2.2 Initializing Device.

Figure 3-28 Auto search device

The 'Auto Search' window displays a table of discovered devices. The table has columns for selection, IP, Initialize Status, Device Model, MAC Address, and Port. The following table represents the data shown in the screenshot:

☐	IP	Initialize Status	Device Model	MAC Address	Port
☐	10.35.92.2	✓	IPC-HF81200E	3c:ef:8c:f7:78:38	37772
☐	10.35.92.3	✓	IPC-HF81200E	3c:ef:8c:f7:78:35	37777
☐	10.35.92.5	✓	IP Camera	3c:ef:8c:92:1f:c0	37768
☐	10.35.92.7	✓	HCVR	4c:11:bf:6d:7a:49	37727
☐	10.35.92.8	✓	DH-SD6AE230F-HNI	4c:11:bf:1c:0f:98	37779
☐	10.35.92.16	✓	DHI-NVR5832-16P-4KS2	38:af:29:45:41:e8	37140
☐	10.35.92.20	✓	DSS Windows	d4:ae:52:c9:60:00	5050
☐	10.35.92.31	✓	DVR	4c:11:bf:4f:a5:11	37716
☐	10.35.92.34	✓	DHI-NVR5208-4KS2	3c:ef:8c:08:c7:27	37777

Below the table, there is a pagination bar showing '20' items per page and 'Total 40 record(s)'. A search filter 'DHI-NVR5208-4KS2' is applied, showing '1' result. The window includes 'Refresh', 'Modify IP', and 'Initialize Device' buttons at the top, and 'OK' and 'Cancel' buttons at the bottom right.

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

The system displays search results.

Step 4 Select the device to be added, click **OK**.

The system displays the interface of **Add Device**. See Figure 3-29.

Figure 3-29 Add Device

The 'Add Device' window contains the following configuration fields:

- Video Server:** Center Server (dropdown menu)
- Organization:** Root (dropdown menu)
- Username:** admin (text input field)
- Password:** (password input field with masked characters)

At the bottom right, there are 'OK' and 'Cancel' buttons.

Step 5 Enter login username and password, click **OK**.



- The added device username is required to be the same as password when adding several devices.

- After device is added, the system continues to stay on the **Auto Search** interface, click **Cancel** or  to exit interface.
- After device is added, the platform logs in device automatically, the device is displayed as online after logging in successfully. If offline, please make sure if login username and password are correct, click  to modify username and password.

3.2.2.4.2 Adding Device Manually

Add single device, or the username and password of the added device are different, or the added device is not in the same segment.

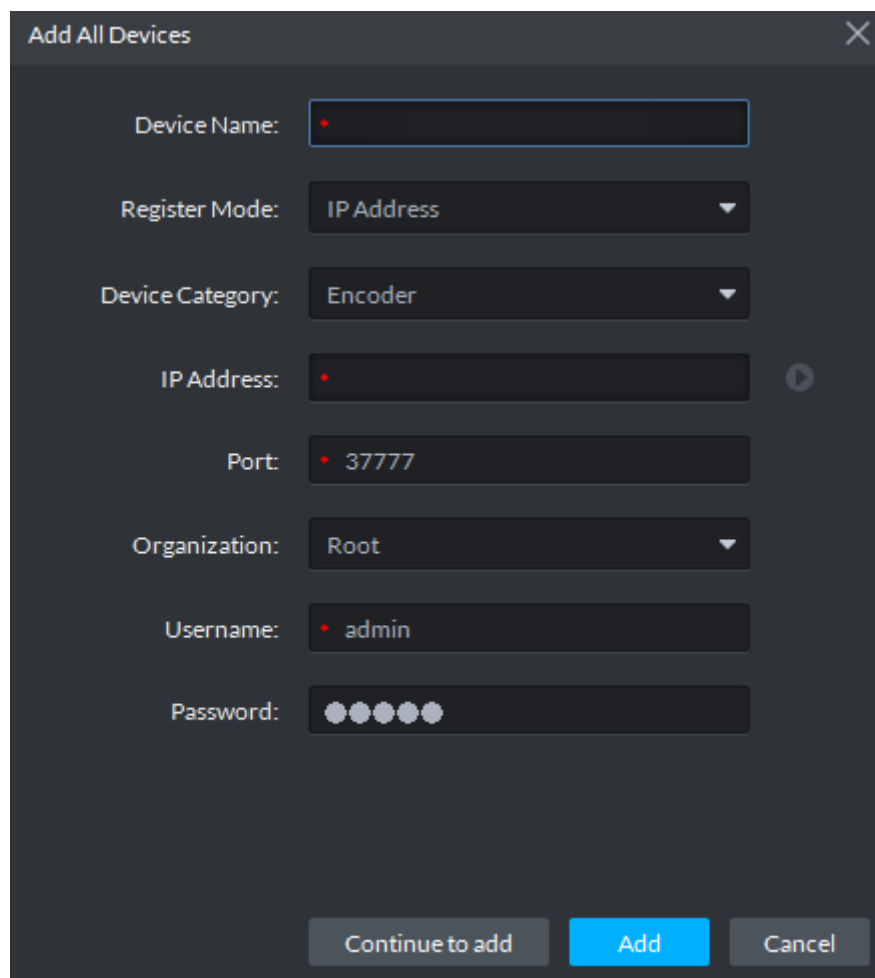
Step 1 Click **Device** on the client homepage.

The system displays the **Device** interface.

Step 2 Click **Add**.

The system displays the interface of **Add All Devices**, see Figure 3-30.

Figure 3-30 Manually add device



Step 3 Set parameters, for more details, refer to Table 3-1.



- The item with * is required to be filled in. You need to set different parameters if different device are connected.
- Add encoder, set correct parameters, and click  to preview device video.

Table 3-1 Parameter description

Parameter	Description
Device Category	Select according to the type of added device, currently support adding access control, encoder, decoder, video wall, ANPR, matrix, LED, alarm host and video intercom.
Register Mode	Support registration by following method: - IP address Add device to platform by adding device IP. - Serial number (Device with P2P function) If device supports P2P function, then you can add device to platform by adding device serial number. - Onvif If device enables Onvif protocol, then you can add device to platform by Onvif protocol. Generally it can be used when adding third-party device.
Port	TCP protocol communication provides service port, and keeps it in accordance with added device.
Organization	Select organization node of added device.
IP Address	When register by IP address or Onvif mode, set the IP address of added device.
SN	When register by serial number mode, set the serial number of added device.
Username	Enter login username and password of added device.
Password	
Decode mode	Select according to the decode mode of added device: - Pull Decoder extracts stream from platform by url address, the decode mode of device is pull. - Direct Decoder extracts stream directly from encoder, the decode mode is direct for device, under this mode; you need to add decoder IP address when trusted list is added by device. - Push VMS pushes stream directly to decoder, currently only support NVD without combination screen, the mode is not supported by matrix, video wall or NVD under combination mode.
Support Combination	Select when added device supports combination.
Picture Server	Select storage location of picture reported by ANPR.
LED Type	Support added LED including general screen and free parking screen, select corresponding device type according to the accessed device.

Step 4 Click **Add**.

Click **Continue to add** if necessary, then you can add more devices.

3.2.2.4.3 Importing Device

If there is device list exported by SmartPSS, or video intercom template already exists and its information is complete, or device is already added by easy4ip account. You can quickly add device to platform by importing existing file or account.

Import Local File

Import device list exported by SmartPSS, or video intercom template file, and add device to the platform quickly.



Please contact technical support for video intercom template.

Step 1 Click **Device** on the client homepage.

The system displays **Device** interface.

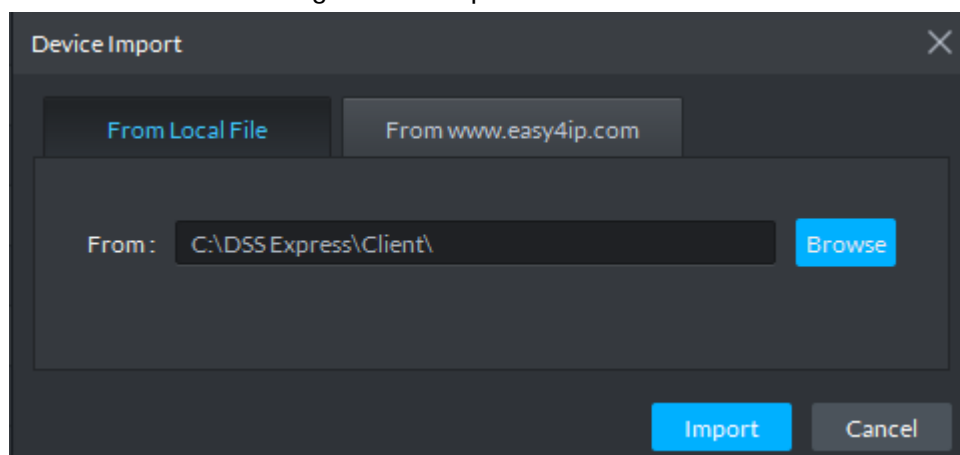
Step 2 Click **Import**.

The system displays **Device Import** interface.

Step 3 Click **From Local File** tab.

The system displays the interface of **From Local File**. See Figure 3-31.

Figure 3-31 Import from local file



Step 4 Click **Browse**, select device info file and click **Import**.

The system shows import results.

Import easy4ip Device Info

Import device info added on easy4ip account, and then device is added to the platform.

Step 1 Click Device on the client homepage.

The system displays Device interface.

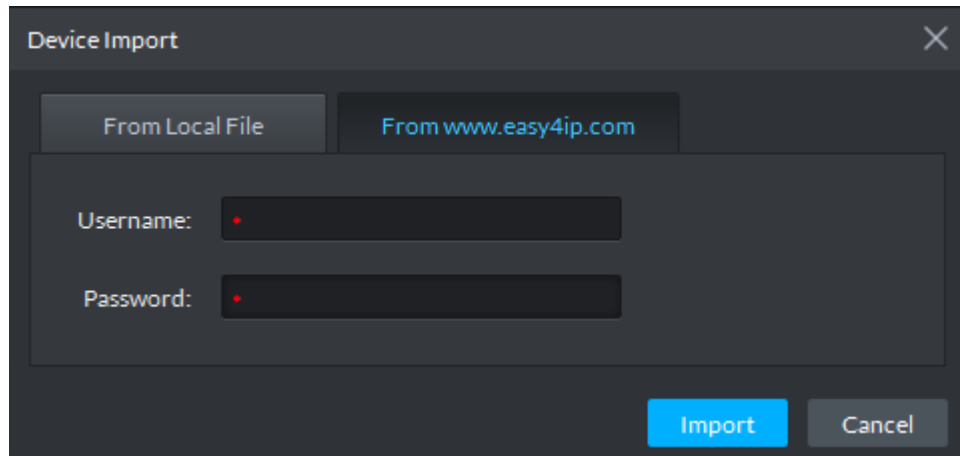
Step 2 Click **Import**.

The system displays **Device Import** interface.

Step 3 Click the tab **From www.easy4ip.com**

The system displays the **From www.easy4ip.com** interface. See Figure 3-32.

Figure 3-32 Import from www.easy4ip.com

A dark-themed dialog box titled "Device Import" with a close button (X) in the top right corner. It features two tabs: "From Local File" and "From www.easy4ip.com", with the latter being selected. Below the tabs are two input fields: "Username:" and "Password:", each with a red asterisk icon to its right. At the bottom right, there are two buttons: "Import" (highlighted in blue) and "Cancel".

Step 4 Enter username and password, click **Import**.
The system shows import result.

3.2.2.5 Editing Device

3.2.2.5.1 Modifying Device Info

Modify device info in the device list, including username, password and some basic info, video channel info, alarm input and output channel. The chapter takes NVR as an example to describe. There are two modification methods shown below.

- Please modify device according to the following method if you want to modify info except device IP address, port number, user and password.

Step 1 Click **Device** on the client homepage.
The system displays **Device** interface.

Step 2 Click  next to device list.

The system displays **Edit Device** interface. See Figure 3-33.

Figure 3-33 Edit device

The screenshot shows the 'Edit Device' window with a sidebar on the left containing tabs: 'Basic Info' (selected), 'Video Channel', 'Alarm Input Channel', 'Alarm Output Channel', and 'POS Channel'. The main area is divided into two sections: 'Basic Info' and 'Device Detail'. In the 'Basic Info' section, there are fields for Protocol (Dahua), Manufacturer (Dahua), IP Address (1.1.1.1), User (admin), Device Port (37755), Password (masked), Video Server (Center Server), and Organization (Root). The 'Device Detail' section has fields for Device Name (aa), Device SN, Type (DVR), and Device Model. At the bottom left is a 'Get info' button, and at the bottom right are 'OK' and 'Cancel' buttons.

Step 3 Select corresponding tab, click **Get Info** on the lower left corner of the interface, sync device info.

- Please modify device according to the following method if you want to modify device IP address, port number, user and password.

Step 1 Click **Device** on the client homepage.
The system displays the **Device** interface.

Step 2 Click  next to the device list.

The system displays **Edit Device** interface, see Figure 3-34.

Figure 3-34 Modify device basic info

Step 3 Click **Basic Info** tab, modify device IP address, username, password, device port, organization, device name and type.

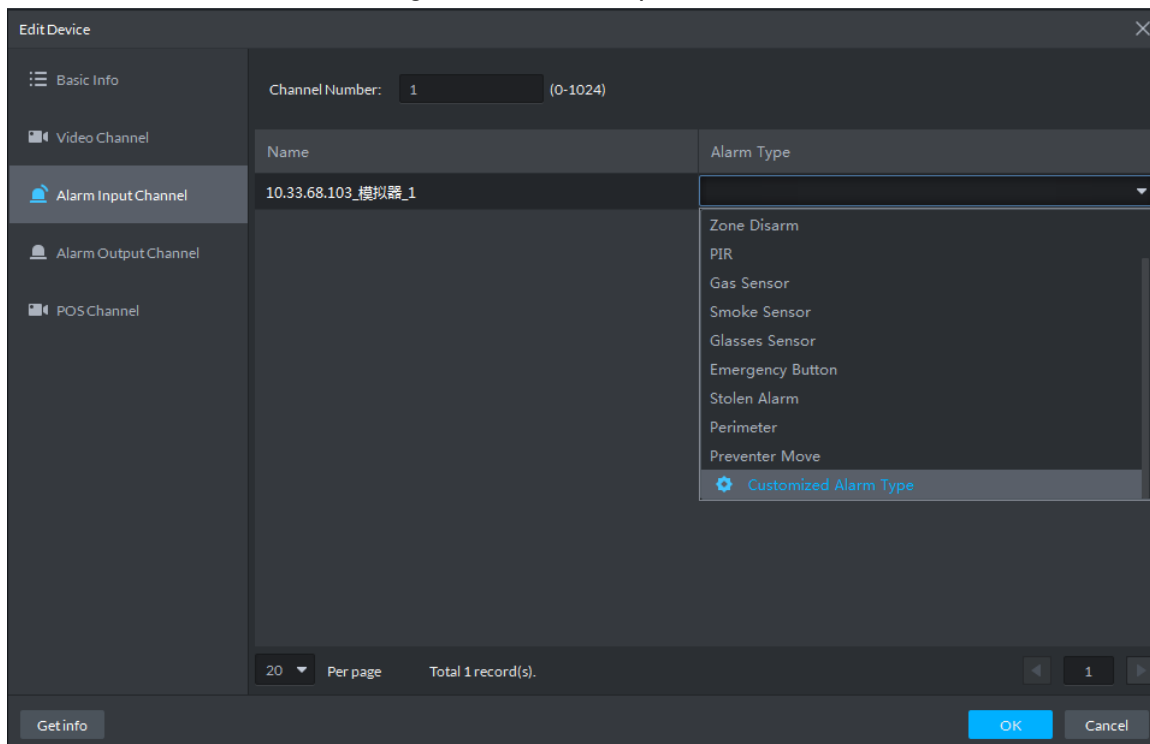
Step 4 Click **Video Channel** tab, modify channel number and stream type, and see Figure 3-35. You need to enable corresponding intelligent function if the added device owns intelligent functions. For example, the added camera is face recognition camera, the camera is required to detect face, and then you need to set **Features** as **Face Recognition**.

Figure 3-35 Video channel

Name	Camera Type	Features	SN	KeyBoard Code
aa_1	Speed Dome	Face Recognition		

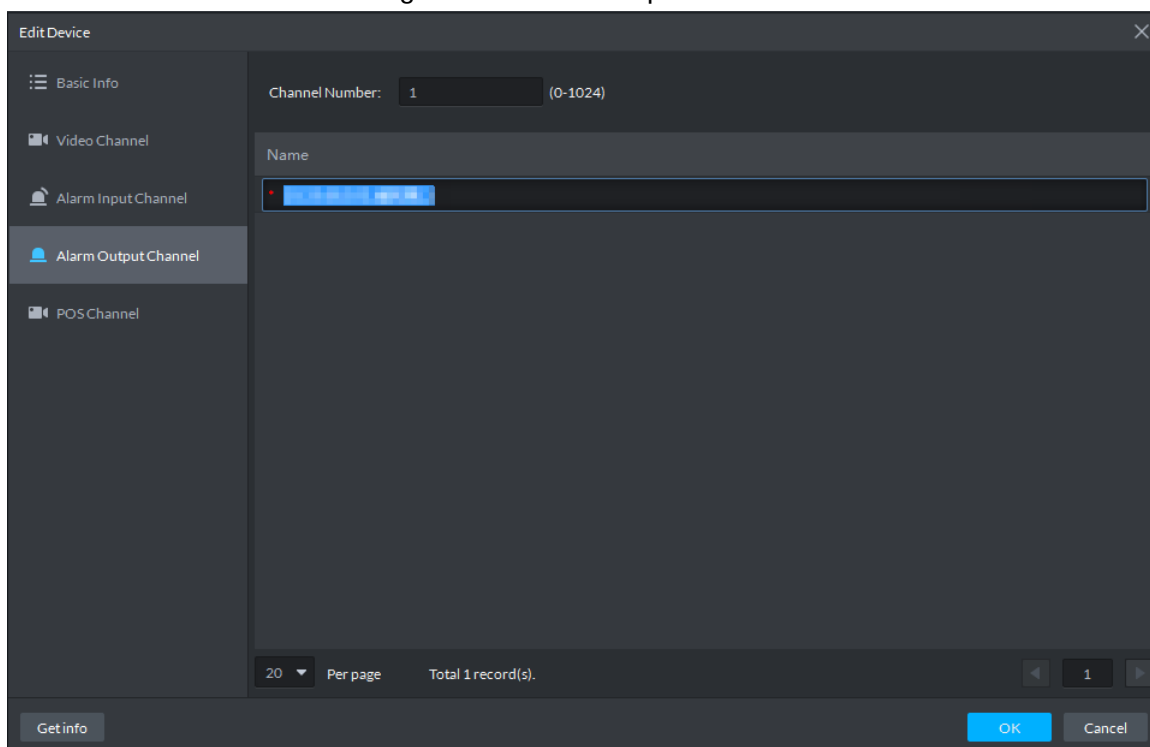
Step 5 Click **Alarm Input Channel** tab and modify alarm input channel number, see Figure 3-36. Alarm type supports custom. Select **Customized Alarm Type** from the drop-down box of **Alarm Type**, set needed alarm type, used to quickly identify alarm. After config, on the event config interface, you can configure corresponding alarm event for corresponding alarm input.

Figure 3-36 Alarm input channel



Step 6 Click **Alarm Output Channel** tab, modify device alarm output channel number, double click to modify corresponding channel name, see Figure 3-37.

Figure 3-37 Alarm output channel



Step 7 Click **POS Channel** tab, modify device POS channel number, double click and modify corresponding channel name, see Figure 3-38.

Figure 3-38 POS channel

The screenshot shows the 'Edit Device' window with the 'POS Channel' tab selected. The sidebar on the left contains the following items: 'Basic Info', 'Video Channel', 'Alarm Input Channel', 'Alarm Output Channel', and 'POS Channel'. The main content area displays 'Channel Number: 0 (0-1024)' and a 'Name' field. At the bottom of the window, there is a 'Get info' button, 'OK' and 'Cancel' buttons, and pagination controls showing '20' per page and 'Total 0 record(s)'.

Step 8 Click **OK**.

3.2.2.5.2 Modifying Device's Organization

You can move device from one organization to another.

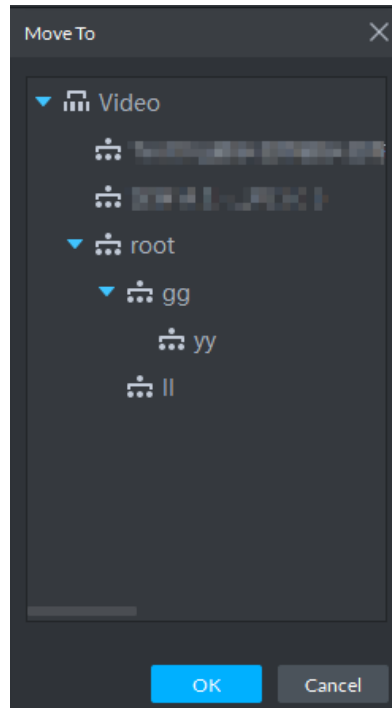
Step 1 Click **Device** on the client homepage.

The system displays **Device** interface.

Step 2 Select the device to be moved, click **Move To**.

The system displays **Move To** interface, see Figure 3-39.

Figure 3-39 Move device



Step 3 Select the organization node you want to move to, click **OK**.

3.2.3 Adding User

3.2.3.1 Adding Basic User

Create users with different permissions for platform and make sure the platform is safe. The platform provides three types of user, including administrator, advanced user and general user, different users have different permissions. Each type of user can adjust permission within certain permission range.

- Administrator: Owns all control permissions.
- Advanced user: Owns all permissions except system config.
- General user: Owns other permissions except device management, user management, system config, config management, video wall config, emap config, log management.

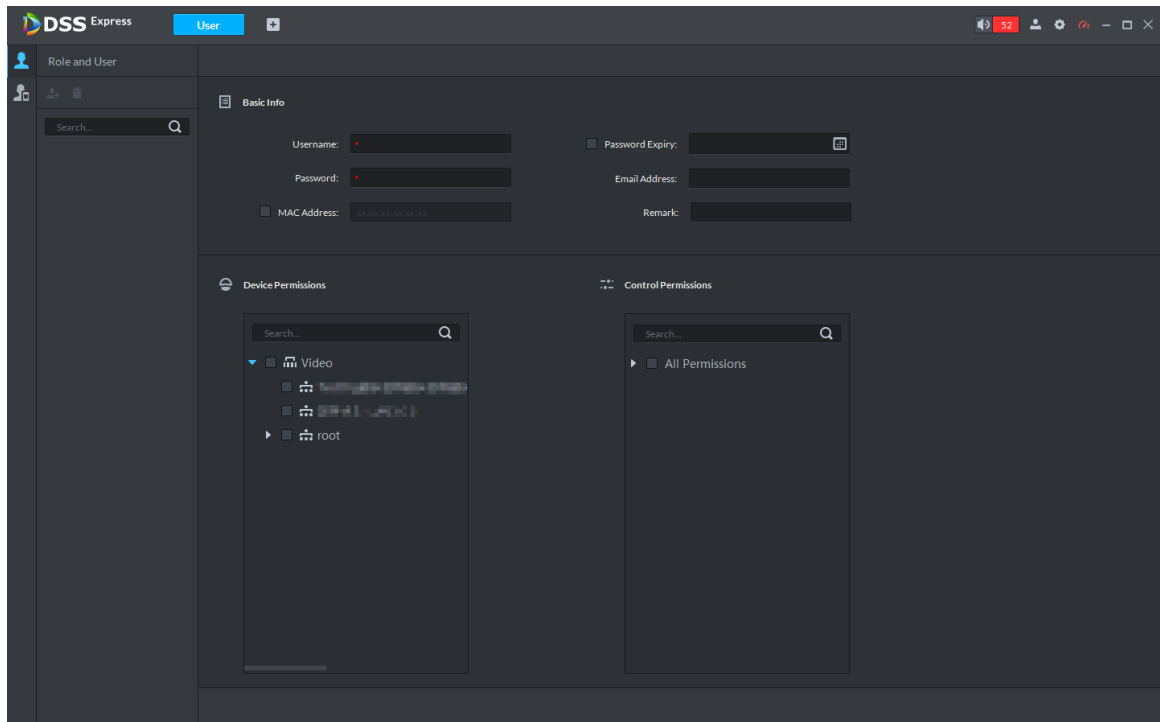


Added user can be deleted but the platform's system cannot.

Step 1 Click **User** on the client homepage.

The system displays **User** interface, see Figure 3-40.

Figure 3-40 User



Step 2

Click .

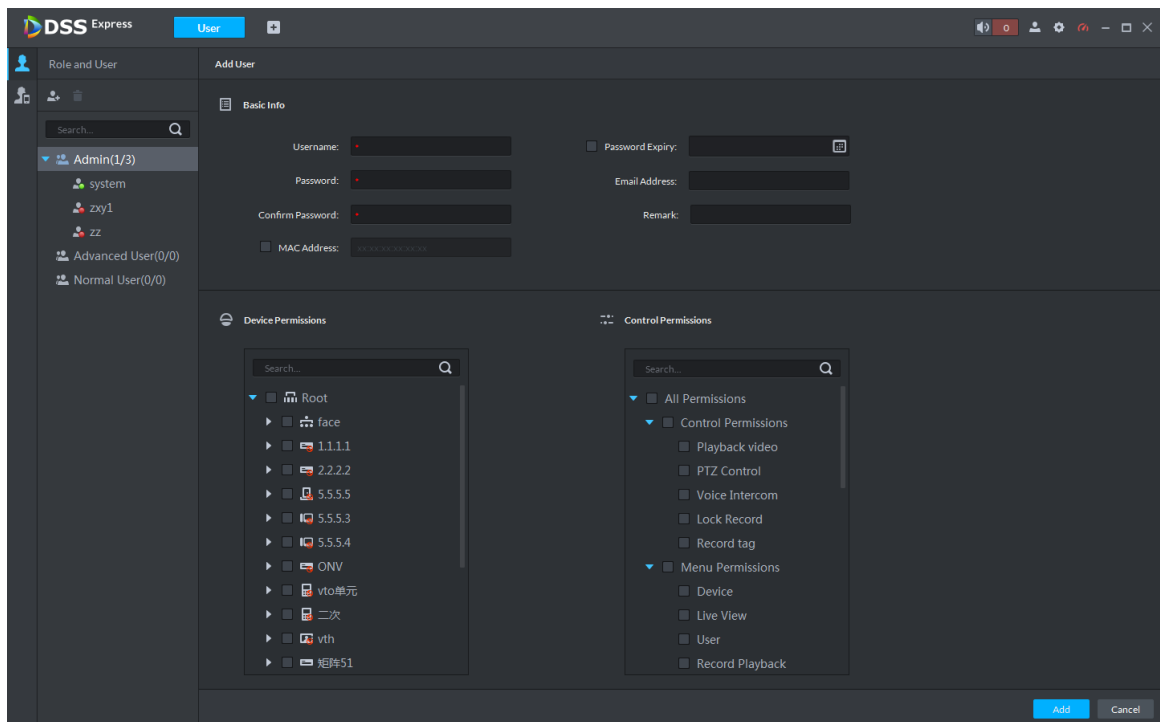
The system displays **User** interface.

Step 3

Select user type from the left list, click .

The system displays **Add User** interface. See Figure 3-41.

Figure 3-41 Add user



Step 4

Set user info, select device and permission that can be used by user, click **Add**.

3.2.3.2 Managing APP User

You can view APP user info, freeze user, modify login password and delete user.

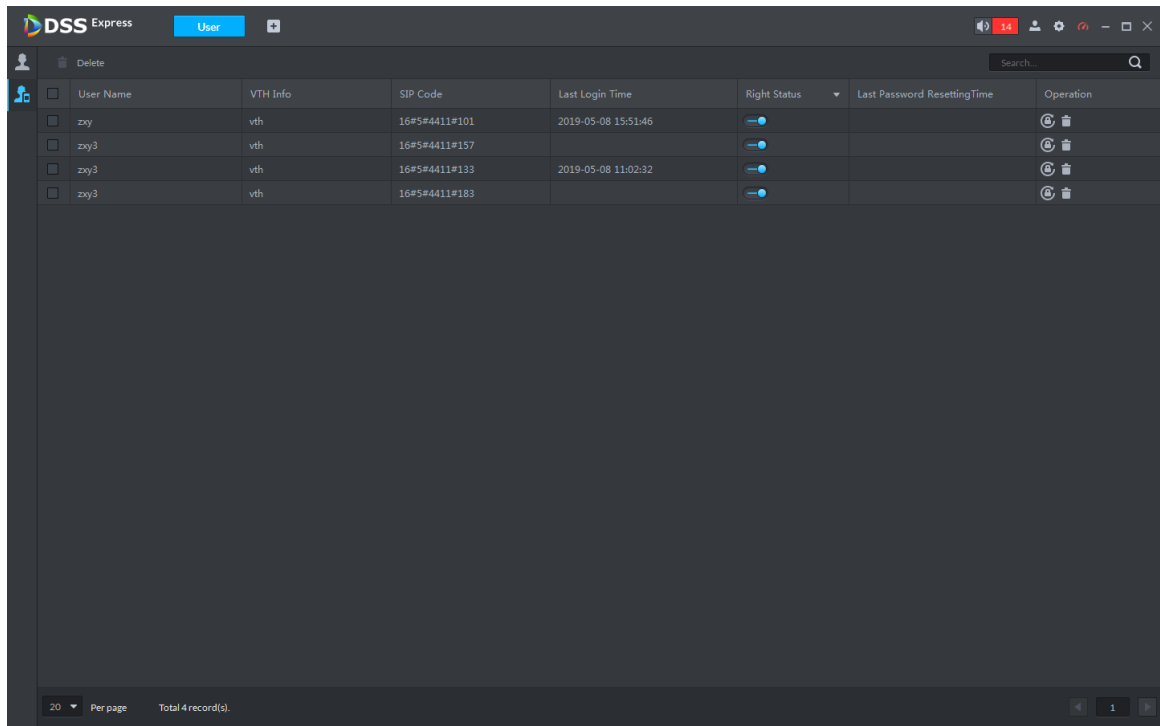


APP user can register by scanning QR code on the device, for more details, refer to APP user manual.



Click  on the **User** interface. The system displays APP User interface, and shows info of all registered APP users. See Figure 3-42. For operation details, see Table 3-2.

Figure 3-42 Enter APP user interface



The screenshot shows the 'DSS Express' application window with the 'User' tab selected. It displays a table of APP users with columns: User Name, VTH Info, SIP Code, Last Login Time, Right Status, Last Password ResettingTime, and Operation. There are four rows of data, each with a checkbox in the Operation column. The bottom of the window shows '20 Per page' and 'Total 4 record(s)'.

User Name	VTH Info	SIP Code	Last Login Time	Right Status	Last Password ResettingTime	Operation
zxy	vth	16#5#4411#101	2019-05-08 15:51:46	ON		
zxy3	vth	16#5#4411#157		ON		
zxy3	vth	16#5#4411#133	2019-05-08 11:02:32	ON		
zxy3	vth	16#5#4411#183		ON		

Table 3-2 Operation description

Operation	Description
Freeze APP User	After APP user is frozen, APP user cannot log in within 600s. means normal, means freeze, both can be mutually switched. The account can also be frozen if password attempts exceed 5 by APP user.
Modify APP User Login Password	Click and enter new password the interface of Reset Password, click OK. Password length is 8~16 characters, must include number and letter. means showin password; means enabling password protection and hiding password. Click icon to switch mutually.

Operation	Description
Delete APP User	Click  next to APP user or select APP user, you can select several users, click Delete and delete users according to prompt on interface.

3.2.4 Setting Alarm Event

Device reports all alarm messages. Alarm messages can be responded only when the platform configures corresponding alarm linkage scheme. Linkage actions are shown as follows when responding to alarm.

- Link camera
Play video of designated channel on client, or record upon designated channel, or take snapshot upon designated channel.

To play video of designated channel on client, you need to enable Open camera video on client when triggering alarm, and also select Open Alarm Associated Video on Local Config interface at client.
- Link PTZ
PTZ moves to designated preset.
- Alarm output
Output alarm signal on the designated alarm output channel. It responds to alarm if alarm output port is connected to alarm device.
- Link Video Wall
Display video channel onto video wall by sequence.
- Email
Send email to inform designated personnel of alarm.
- Link Access Control
Lock or unlock designated access control channel.

Alarm event types are different due to different device types, but the event parameters are the same. This chapter takes disk full alarm as an example to make introduction.



- Each alarm type needs to be configured independently.
- Linkage item is independent, you can link several items.

Step 1 Click **Config** on the client homepage.

The system displays **Config** interface.

Step 2 Select device or device channel from left device tree, click **Event Config**. See Figure 3-43.

The system displays **Event** interface, see Figure 3-44.



Select root node on the left device tree, device event config is displayed on the right. If

no config, click **No event config, click to config.** or  and enter config interface.

Figure 3-43 Config

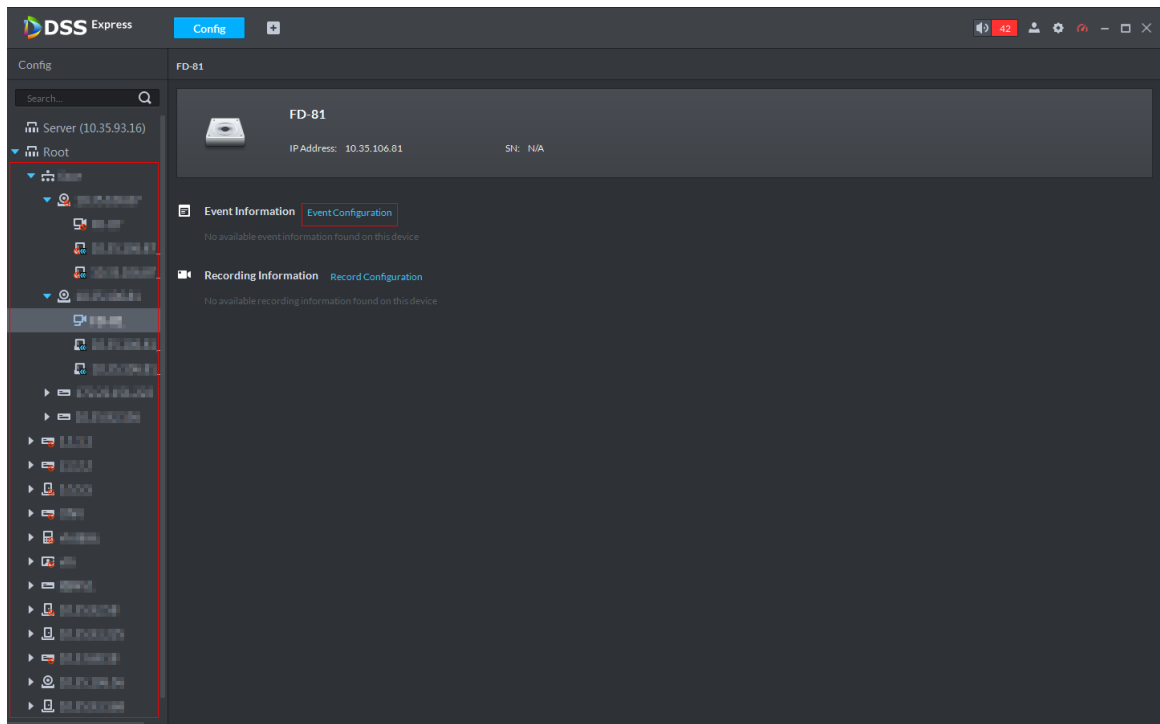
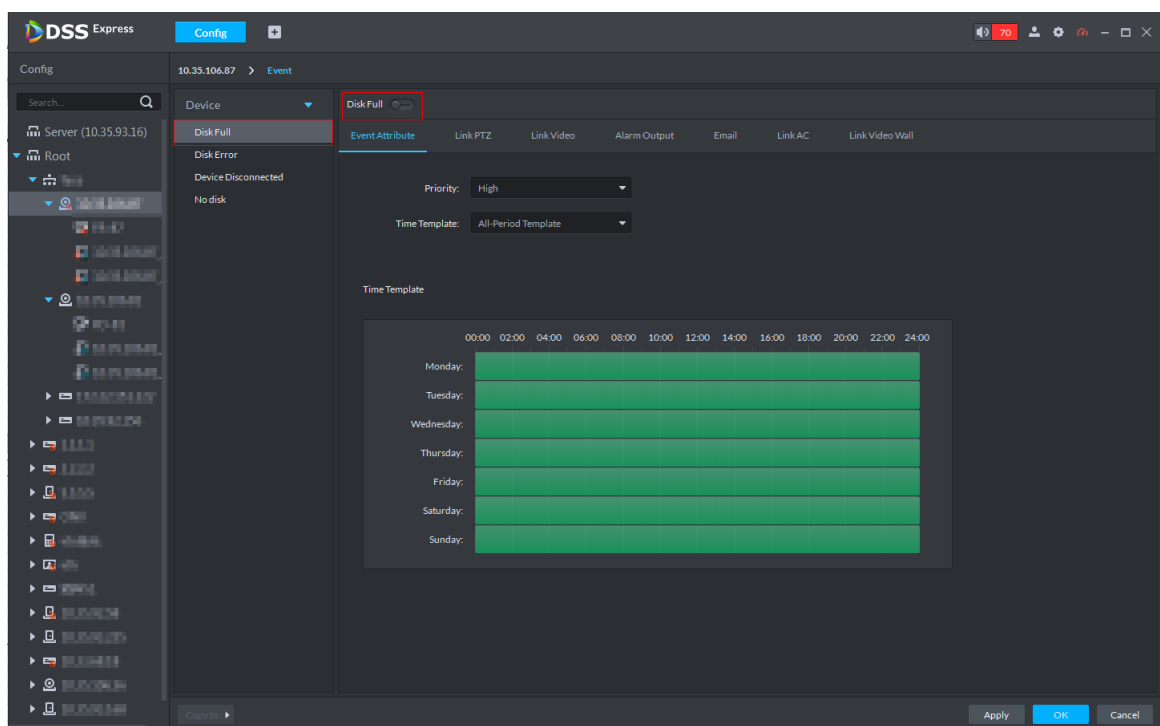


Figure 3-44 Event



Step 3 Select alarm event type as disk full, click .

Icon is switched to , enable disk full. At this moment,  is displayed next to the alarm event type on the left.

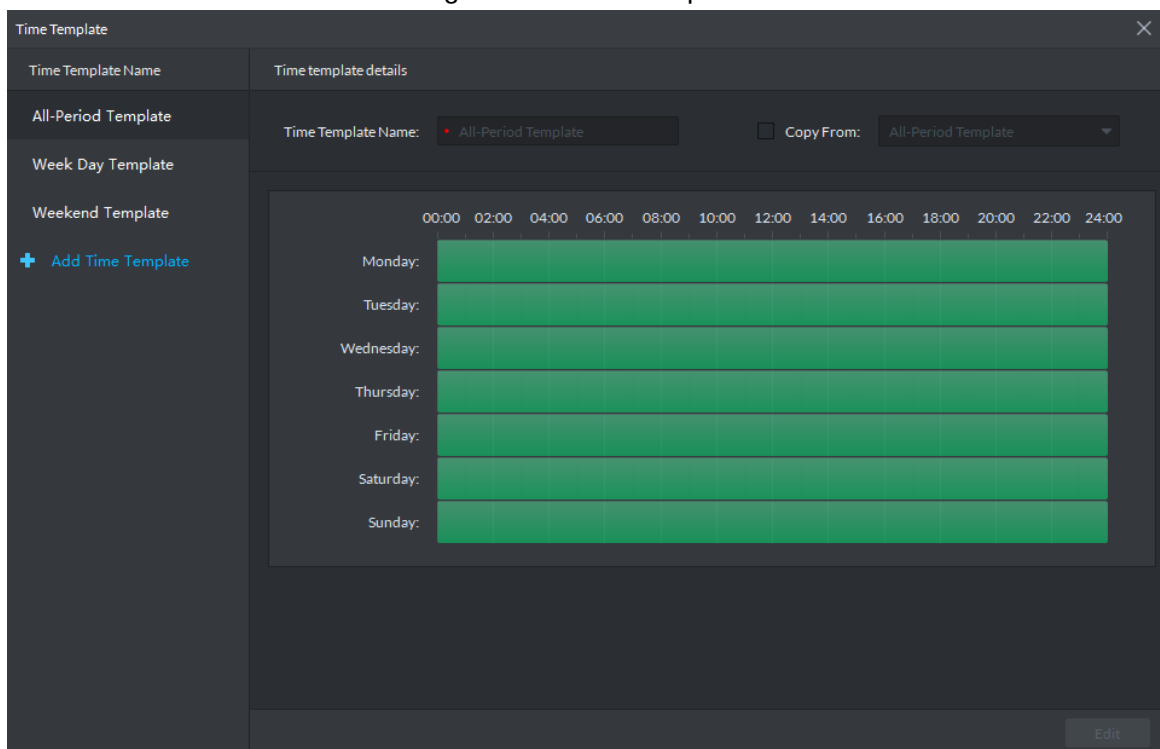
Step 4 Set event attribute

Include setting alarm event priority and effective period of event.

- Set Event Attribute

- 1) Click **Event Attribute** tab.
The system displays **Event Attribute** interface, see Figure 3-44.
 - 2) Select priority.
Priority is only used to recognize alarm message.
 - 3) Select time template, you need to configure again if default time template fails to meet requirement. For details, see **Set Time Template**.
After selected, the time info set by time template is displayed below.
- Set Time Template
Default time templates include all-period template, week day template and weekend template. If the default template fails to meet requirement, please add new template according to the following steps.
 - 1) Click **Event Attribute** tab.
The system displays **Event Attribute** interface, see Figure 3-44.
 - 2) Click **Time Template** and select **Manage Time Template**.
The system displays **Time Template** interface. See Figure 3-45.

Figure 3-45 Time template



- 3) Click **Add Time Template**.
The system displays **Time Template Details** interface. See Figure 3-46.

Figure 3-46 Add time template

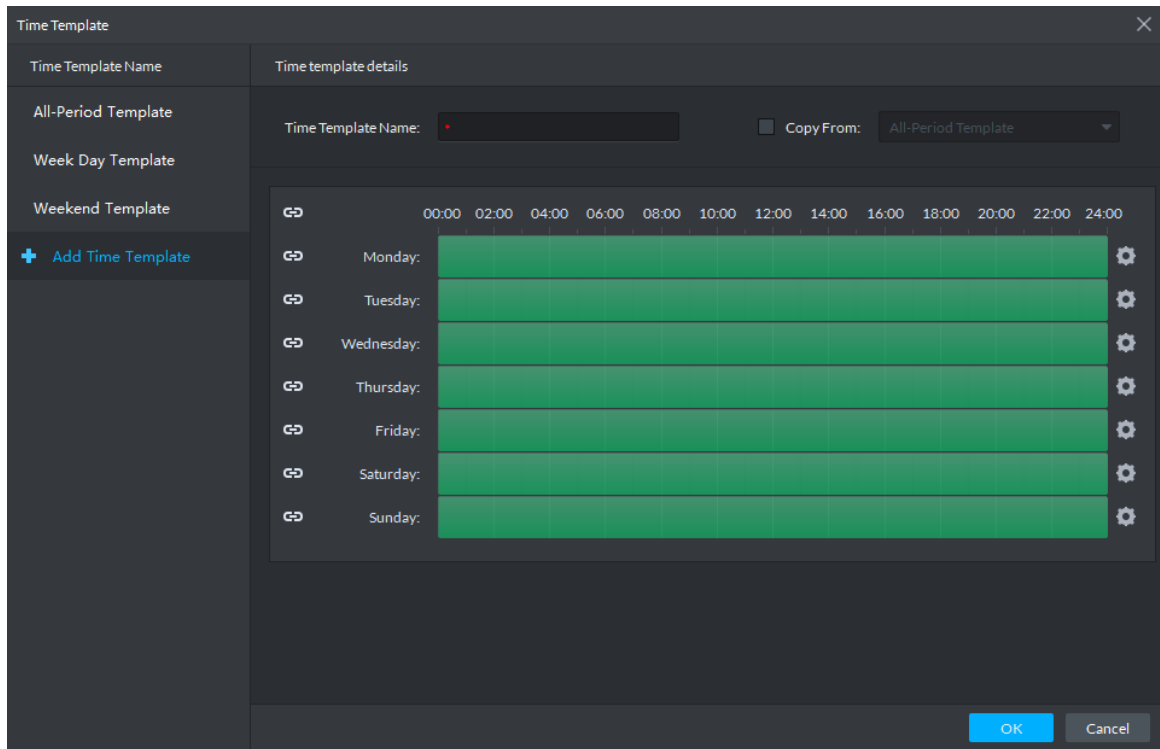
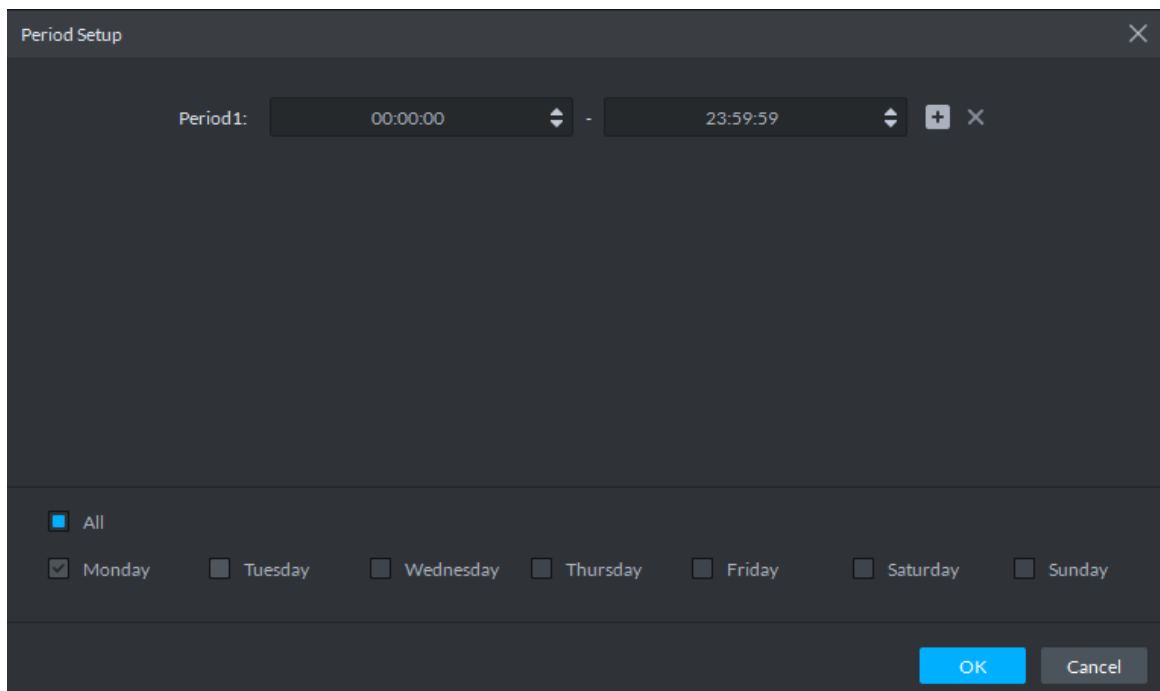


Figure 3-47 Period setting

- 4) Enter time template name, and set time by three following methods.
 - ◇ Select **Copy**, select existed default template, and copy time directly from default template.
 - ◇ Use mouse and drag time line, if time is set, then eraser is displayed, and erase the time of location where you drag; if time is not set, then pen is displayed, and add time of dragged location.
 - ◇ Click , set period and week, click  and add several periods, click  to delete time. Click OK after setting is completed, save and return to the interface of Time Template Details. See Figure 3-48.

Figure 3-48 Period setup



5) Click **OK** and time template is created.

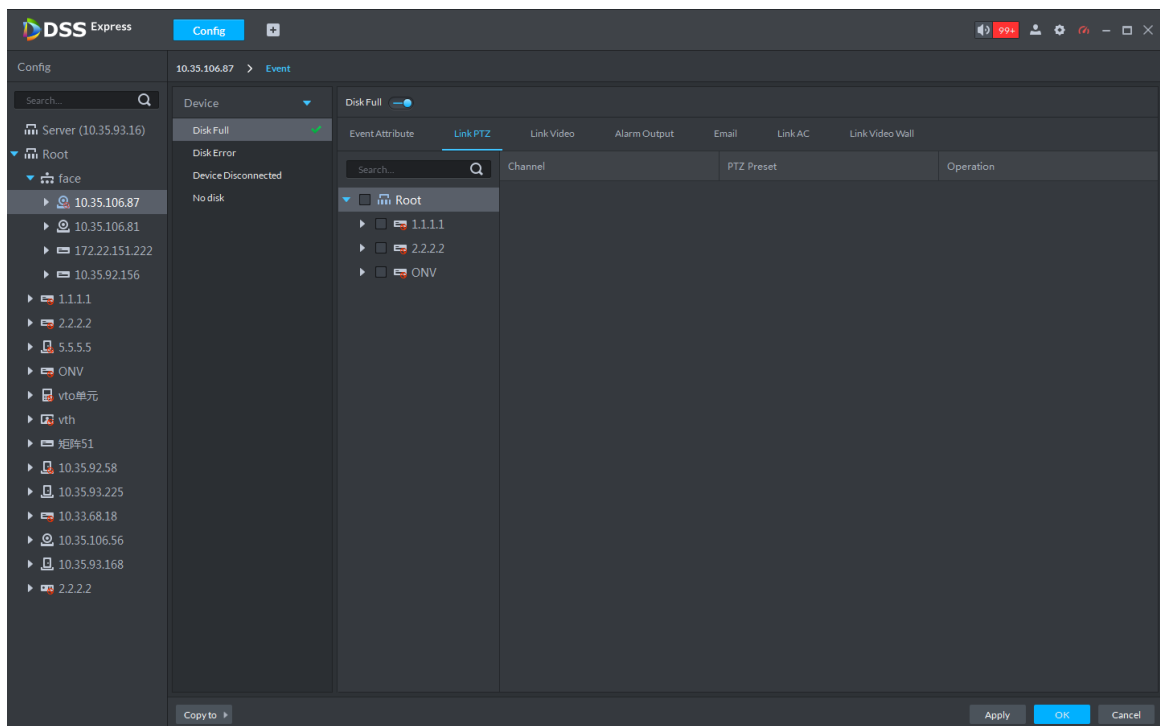
Step 5 Link PTZ.

When alarm event occurs, the linked PTZ moves to preset and realize monitoring.

1) Click **Link PTZ** tab.

The system displays **Link PTZ** interface, see Figure 3-49.

Figure 3-49 Link PTZ



2) Select PTZ device from device tree.

3) Click drop-down box and select PTZ preset.

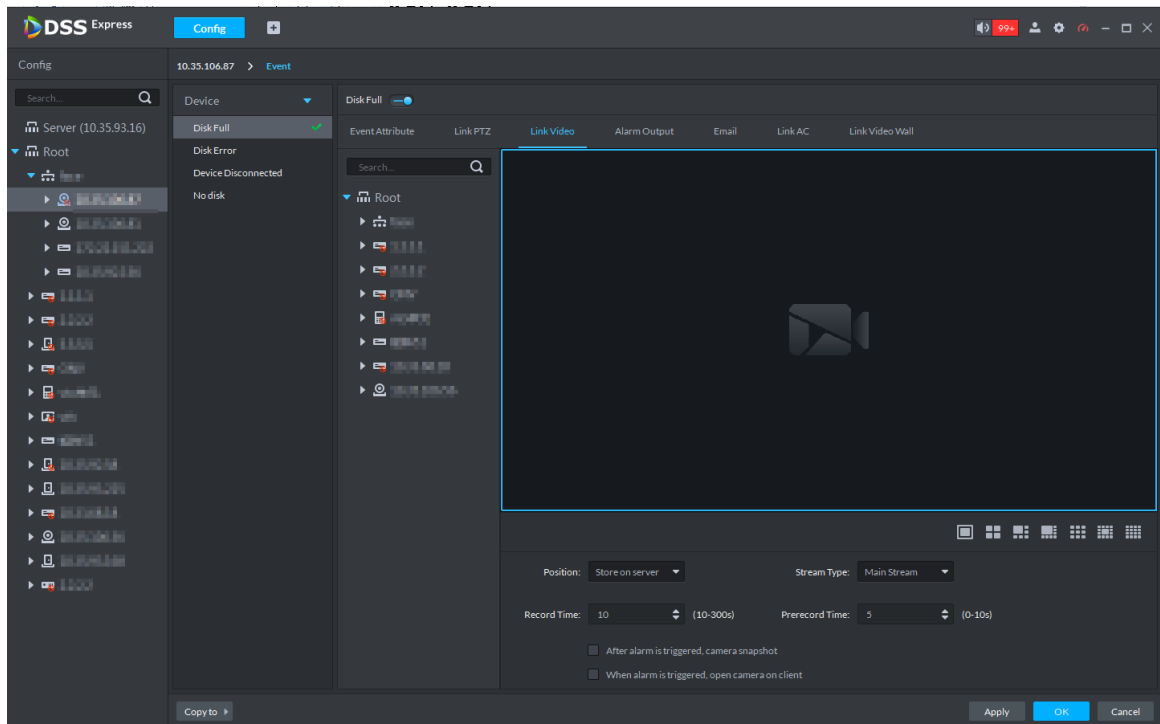
Step 6 Link Video.

When alarm event occurs, link associated device to record, capture and pop out video.

- 1) Click **Link Video** tab.

The system displays **Link Video** interface. See Figure 3-50.

Figure 3-50 Link video

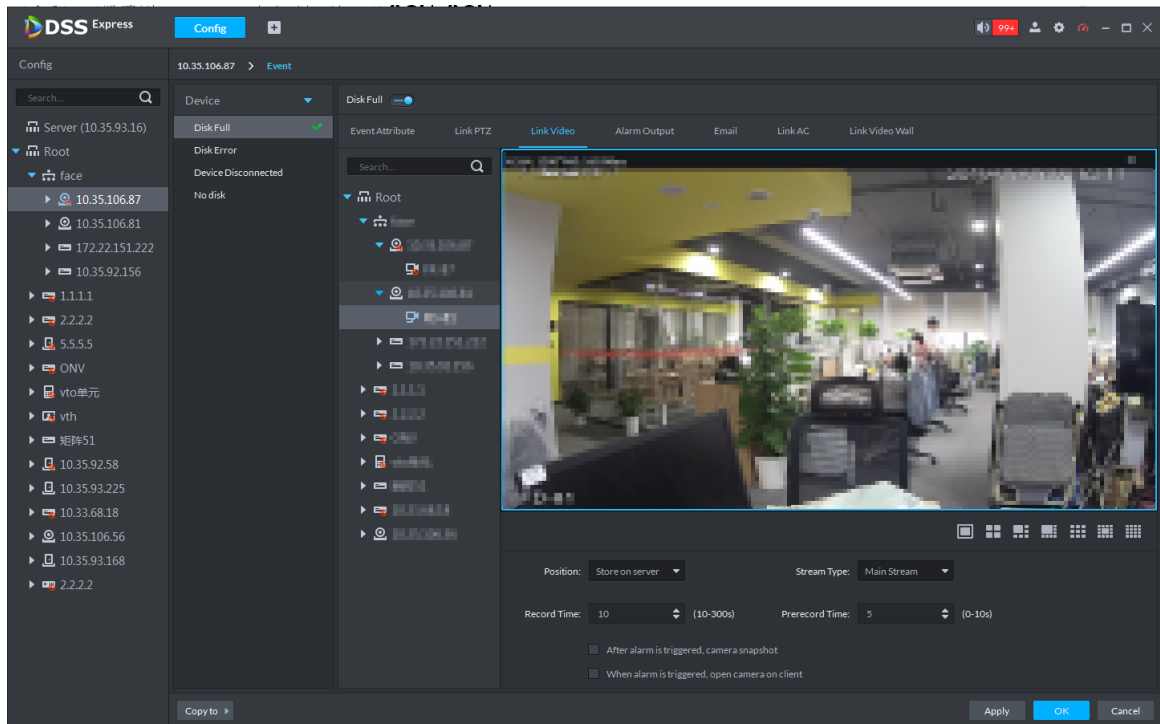


- 2) Select window, drag the linked device to the window, and see Figure 3-51.



- Click icon under the window, you can select number of windows.
- After channel is dragged into window, click  and display realtime video, click  to delete channel. If video is already played, please move the mouse to window, and click .

Figure 3-51 Bind device channel



3) Set linked parameters, for more details, see Table 3-3.

Table 3-3 Link video parameter

Parameter	Description
Storage Position	Set storage position of videos and snapshots, support store on server, store on device or not record.
Stream Type	Select video stream of channel, support main stream, sub stream 1 and sub stream 2.
Record Time	Set time of linking record after alarm event is triggered.
Prerecord Time	Set prerecord time before linking record.
After alarm is triggered, camera snapshot	Link corresponding camera snapshot after alarm event is triggered.
When alarm is triggered, open camera on client	After alarm output is triggered, you can open camera's realtime video on client.

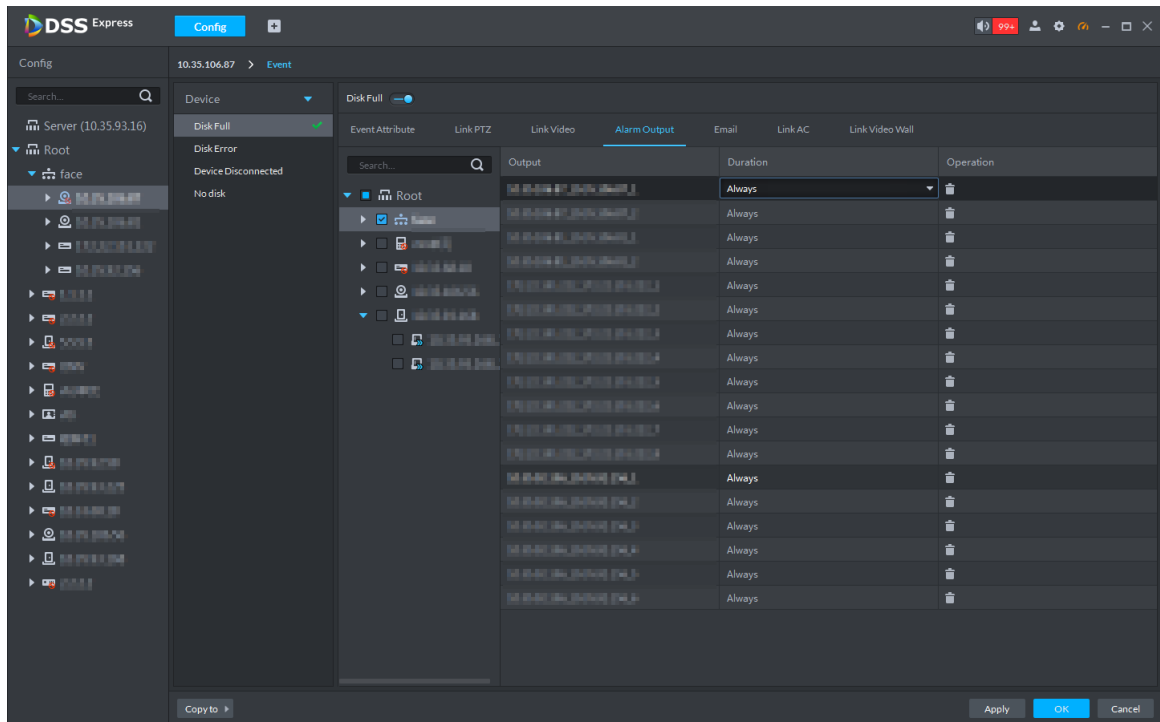
Step 7 Link Alarm Output.

Link external alarm output device and output alarm info when alarm event occurs.

1) Click **Alarm Output** tab.

The system displays **Alarm Output** interface, see Figure 3-52.

Figure 3-52 Alarm output



- 2) Select alarm output device.
- 3) Click the drop-down box of Duration on the right list, select alarm duration.



Click  in the list, or not select device, and then you can delete alarm output device.

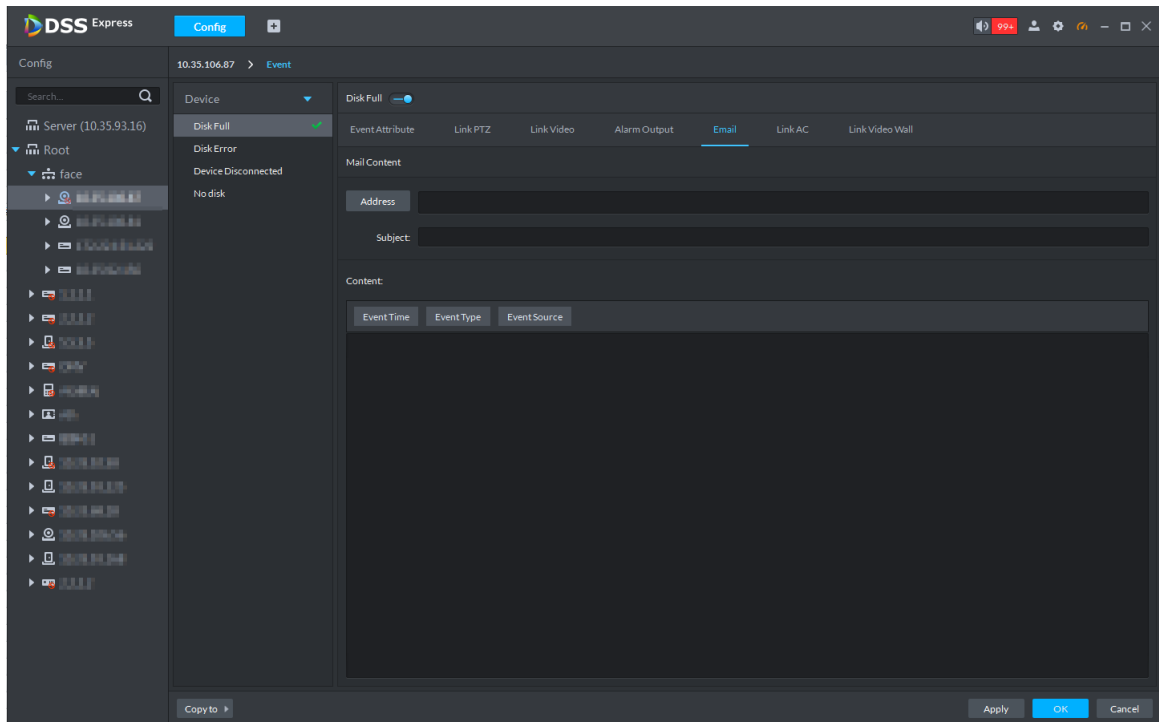
Step 8 Link Email.

When alarm event occurs, you can send email to remind user to deal with alarm event.

- 1) Click **Email**.

The system displays the **Email** interface, see Figure 3-53.

Figure 3-53 Email



- 2) Enter email address of the receiver into the address bar, or click **Address**, select email address of the receiver.



If you click Address and select receiver's email address, you need to make sure the email address of added user is already set; otherwise it cannot be displayed in the list.

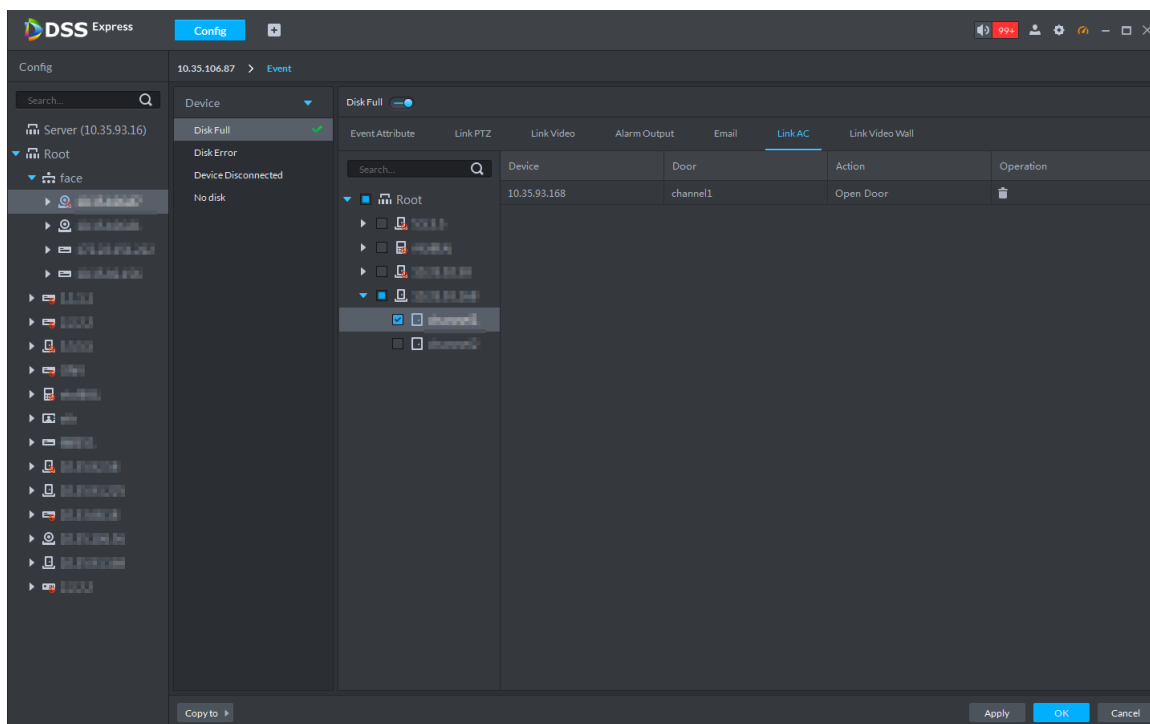
- 3) Enter email subject.
- 4) Click the item and set email content, or enter email content directly. For example, select **Event Time**, then the email content sent to receiver will have event time.

Step 9 Link Access Control

When alarm event occurs, it links several access control channels to close or open, each channel's status can be set independently.

- 1) Click **Link AC** tab.
The system displays **Link AC** interface, see Figure 3-54.

Figure 3-54 Link AC



- 2) Select channel of access control.
- 3) Select linkage action of the access control channel in the right list.
Support four types of action, open door, close door, always open and always close.
 - ◇ Open door: Link to open door when alarm event is triggered.
 - ◇ Close door: Link to close door when alarm event is triggered.
 - ◇ Always open: Linked door is always open when alarm event is triggered.
 - ◇ Always close: Linked door is always close when alarm event is triggered.



Click  in the list, or not select device, then you can delete access control channel.

Step 10 Link Video Wall.

When alarm event occurs, display video channel onto the video wall by sequence.



Please configure video wall before linking video wall setting. If video wall is not configured, enter Link Video Wall interface, the platform jumps to video wall config interface.

- 1) Click **Link Video Wall** tab.
The system displays **Link Video Wall** interface.
- 2) Select video wall channel from the middle device list.
The system displays info of linking video wall, see Figure 3-55.



If video wall window is not configured, click **OK** on the prompt box, configure window on the video wall config interface, and see Figure 3-55.

Figure 3-55 Link video wall

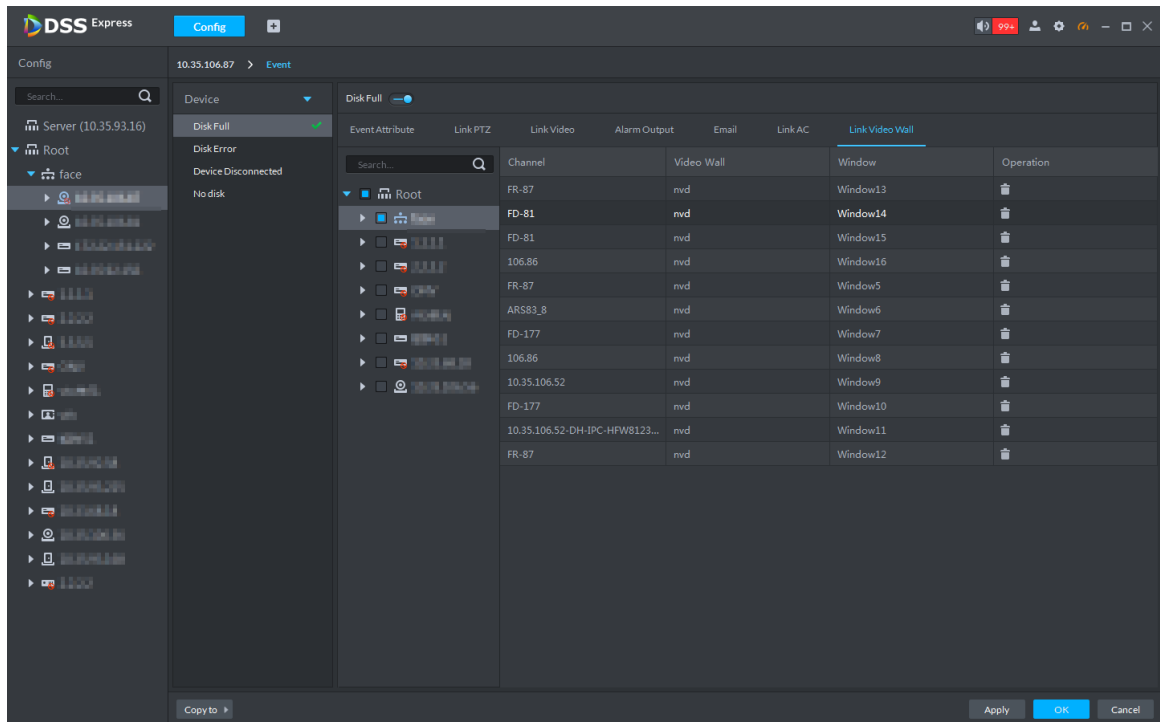
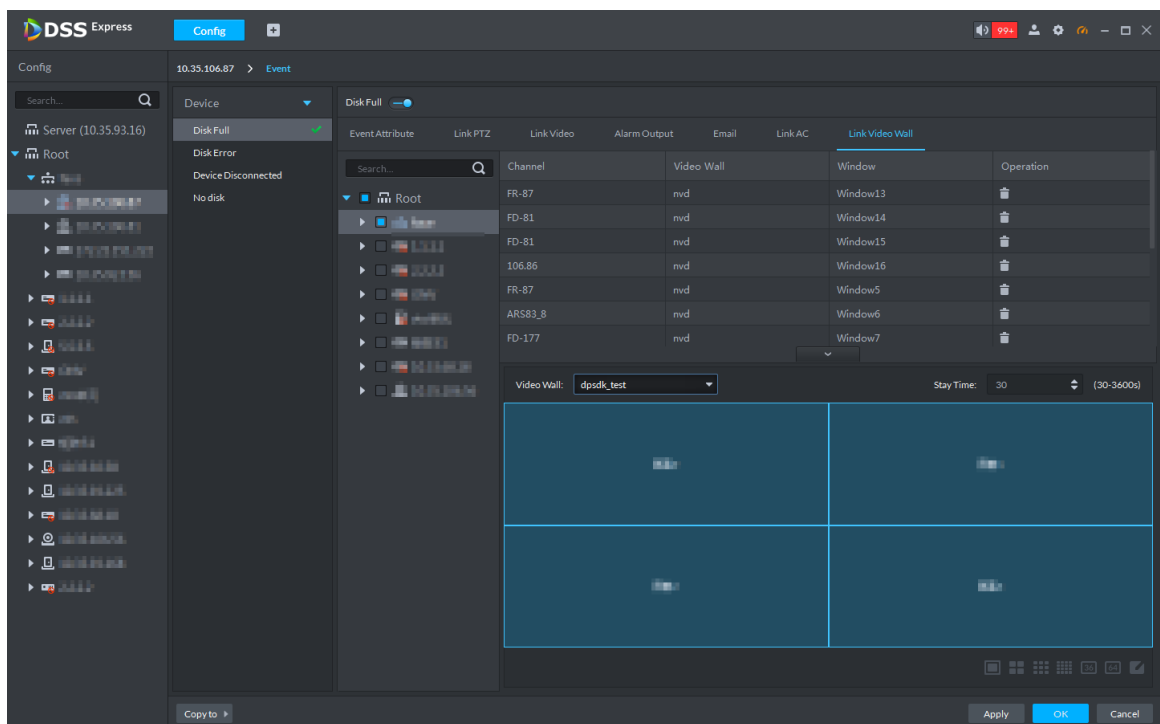


Figure 3-56 Configure video wall window.



- 3) Select **Video Wall** and **Window**, click **OK**.



If you want to configure new window, select New Window from the drop-down box, see Figure 3-55.

Step 11 Click **OK** and complete setting.

3.2.5 Setting Record Plan

If the device is equipped with video channel, it supports configuring different stream record plans (such as main stream, sub stream), and configure storage position of video (platform server or device).



For storage space config, refer to 3.2.1.4 Setting Storage Space. Following risks may exist if not configured.

- Record disk is not configured, system may fail to store record file.
- Local storage disk does not divide general picture disk, causing intelligent alarm event and linkage snapshot cannot be stored, snapshots are not displayed.

Step 1 Click **Config** on the client homepage.

The system displays **Config** interface.

Step 2 From the device tree on the left, select device channel, click **Record Configuration**, see Figure 3-57.

The system displays **Record** interface, see Figure 3-58.

Figure 3-57 Enter record config interface

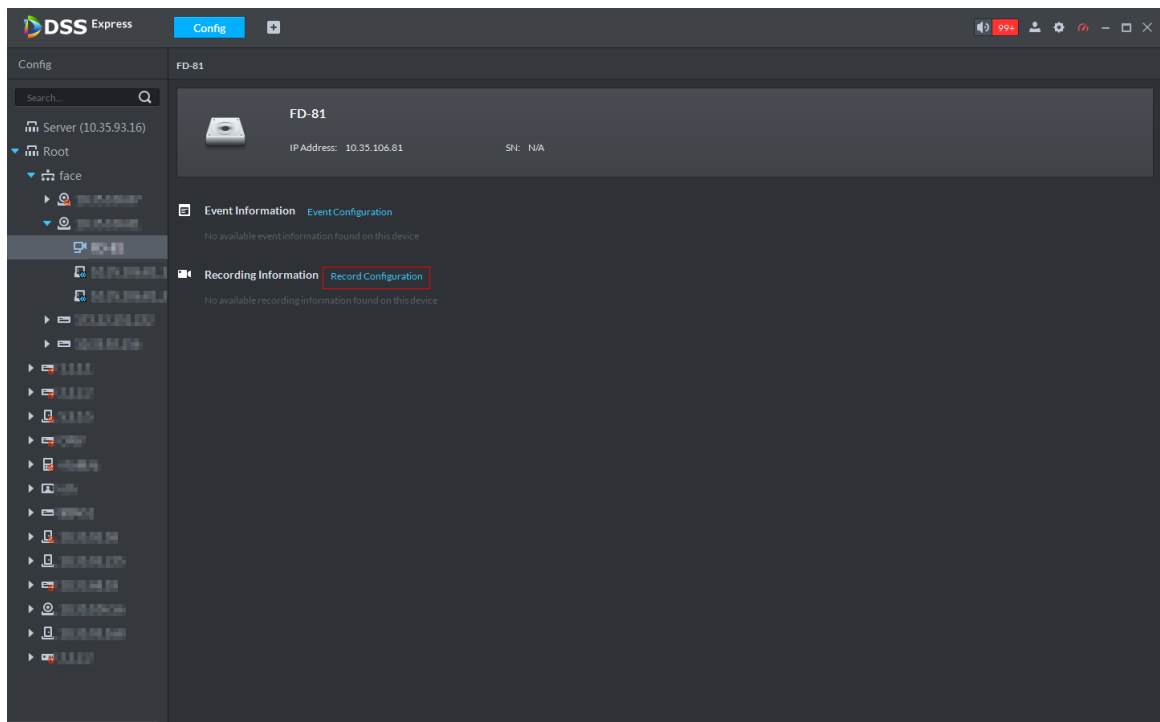
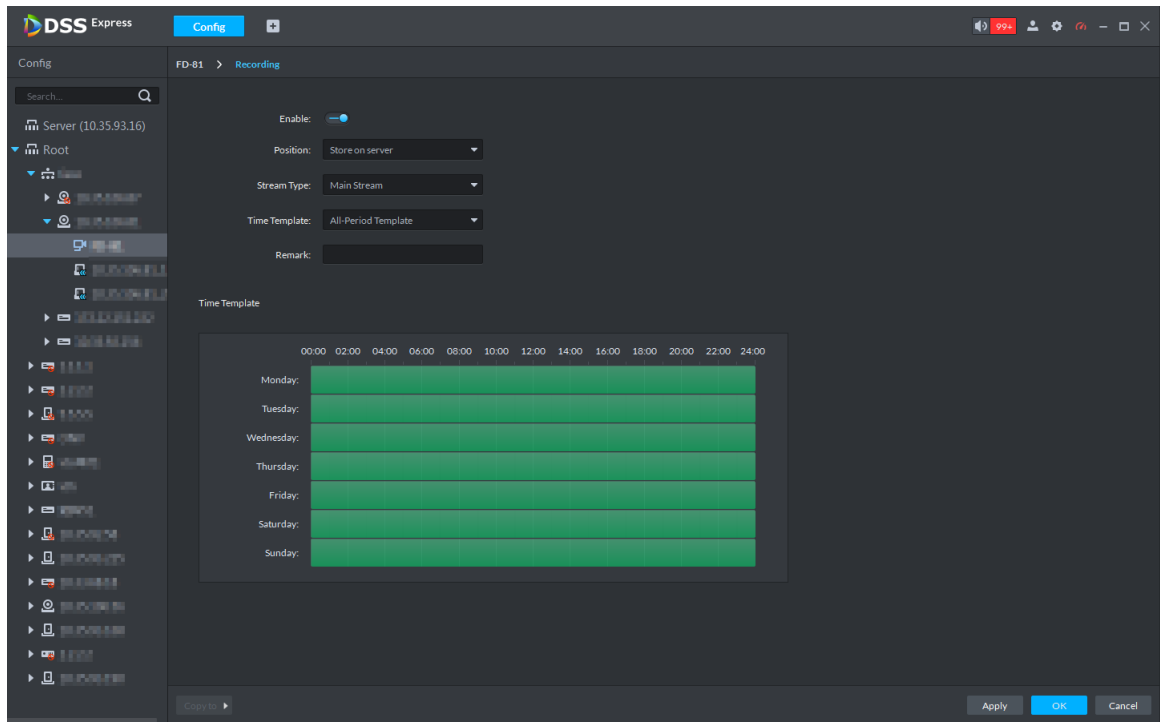


Figure 3-58 Record



Step 3 Click



The icon is switched to , enable record plan.

Step 4 Select **Position**, **Stream Type** and **Time Template**.

The default time template is provided by system, if requirement is not met, then you can create new template. For details, you can refer to **Configure Time Template**.

Step 5 Click **OK**, complete record plan config, and see Figure 3-59.

Figure 3-59 Record info

Save Path	Time Template	Stream Type	Operation
Store on server	All-Period Template	Main Stream	  

3.2.6 Configuring Emap

The platform supports to import raster map. Import raster map means importing a map picture on the platform. You can add device on the map and link device to map, you can view device and alarm on the map directly. Meanwhile, the track function of different modules (such as personnel management and face recognition) can call map and generate movement track.

3.2.6.1 Adding Map

Step 1 Click **Emap** on the client homepage.

The system displays **Emap** interface, see Figure 3-60 and Figure 3-61.

Figure 3-60 Emap-first use

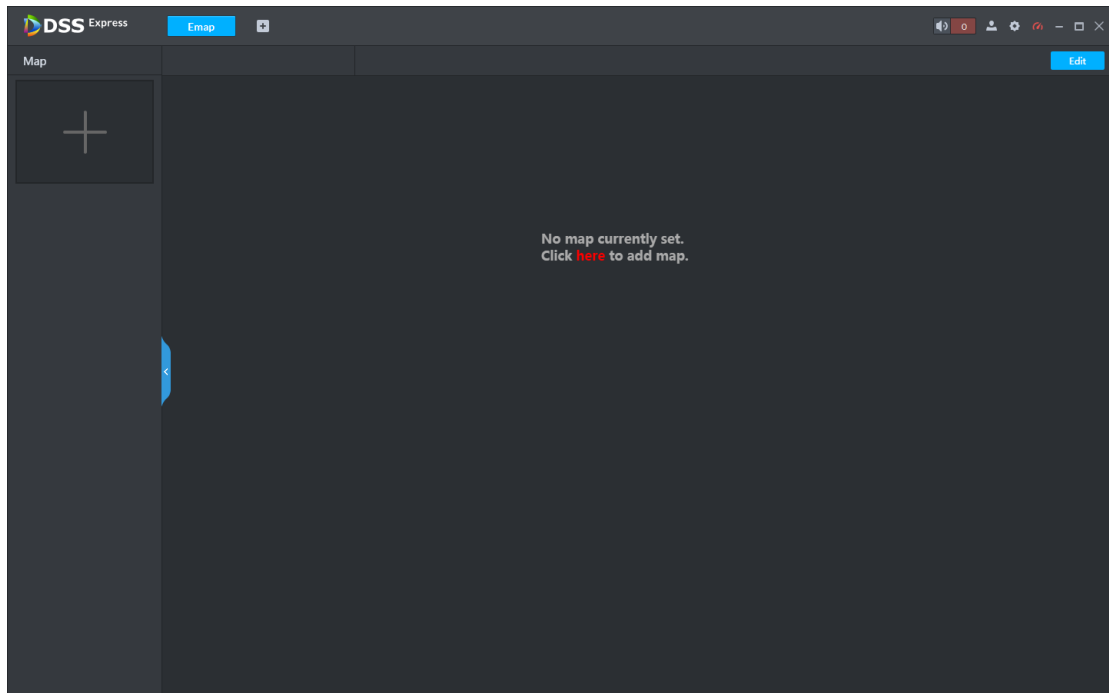
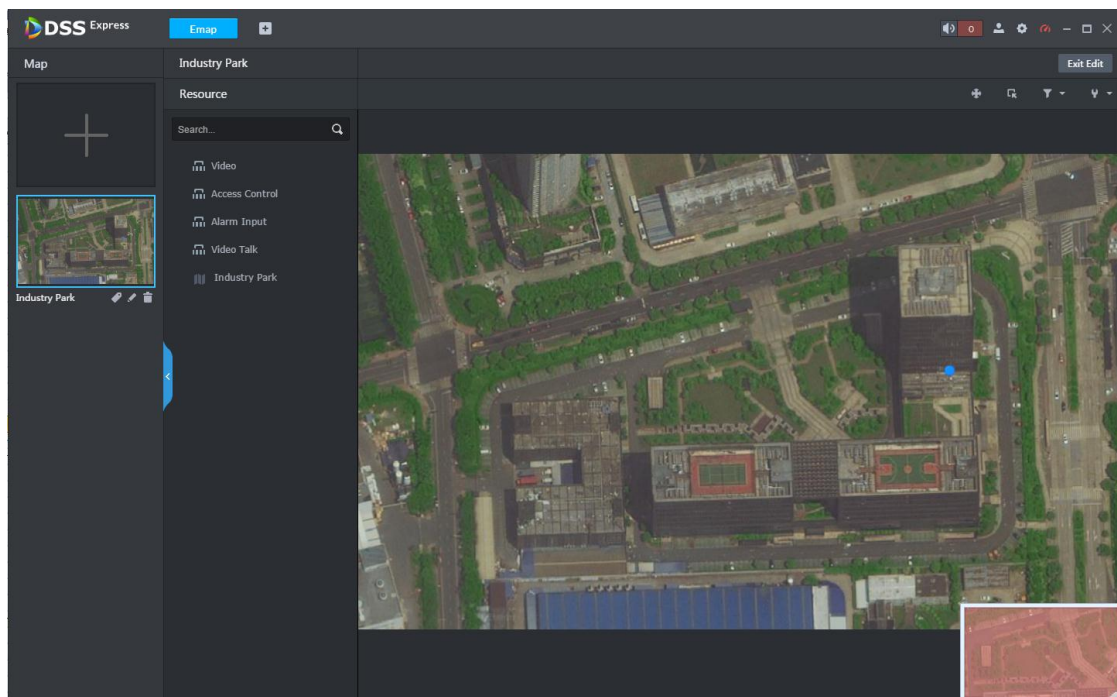


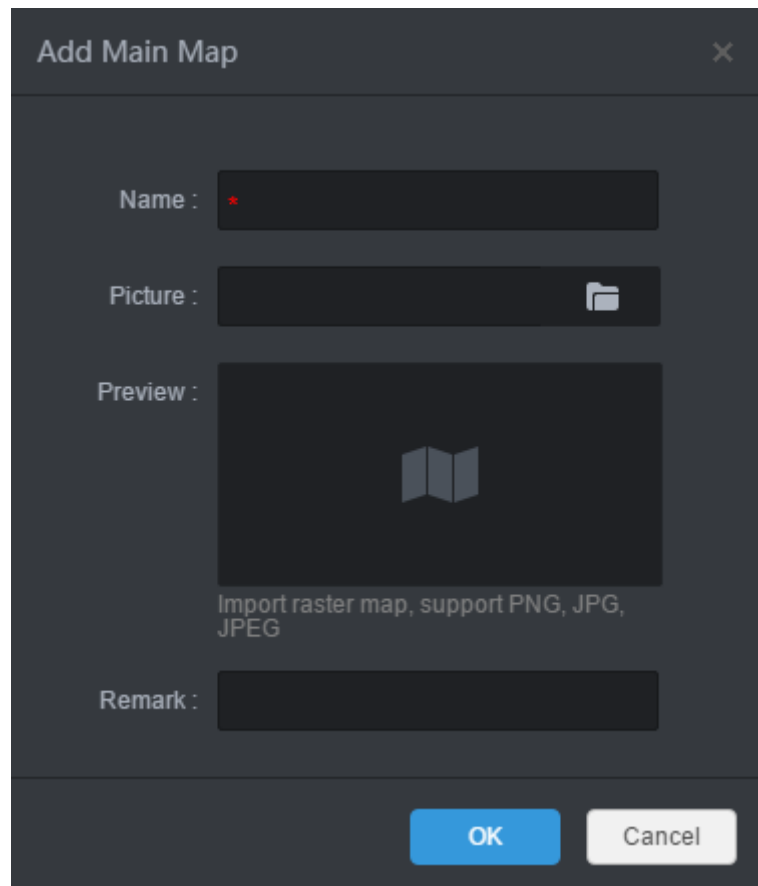
Figure 3-61 Emap-non first use



Step 2 Add main map.

- 1) Click Here for the first use, click + on the left if not use for the first time.
The system displays Add Main Map interface, see Figure 3-62.

Figure 3-62 Add main map

A dark-themed dialog box titled "Add Main Map" with a close button (X) in the top right corner. It contains four input fields: "Name" with a red asterisk indicating it is required, "Picture" with a folder icon, "Preview" with a map icon, and "Remark". Below the "Preview" field, there is a text label: "Import raster map, support PNG, JPG, JPEG". At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (gray).

- 2) Enter **Name** and **Remark**, click  and select picture.

After the picture is selected, selected pictures are displayed on the **Preview** area.

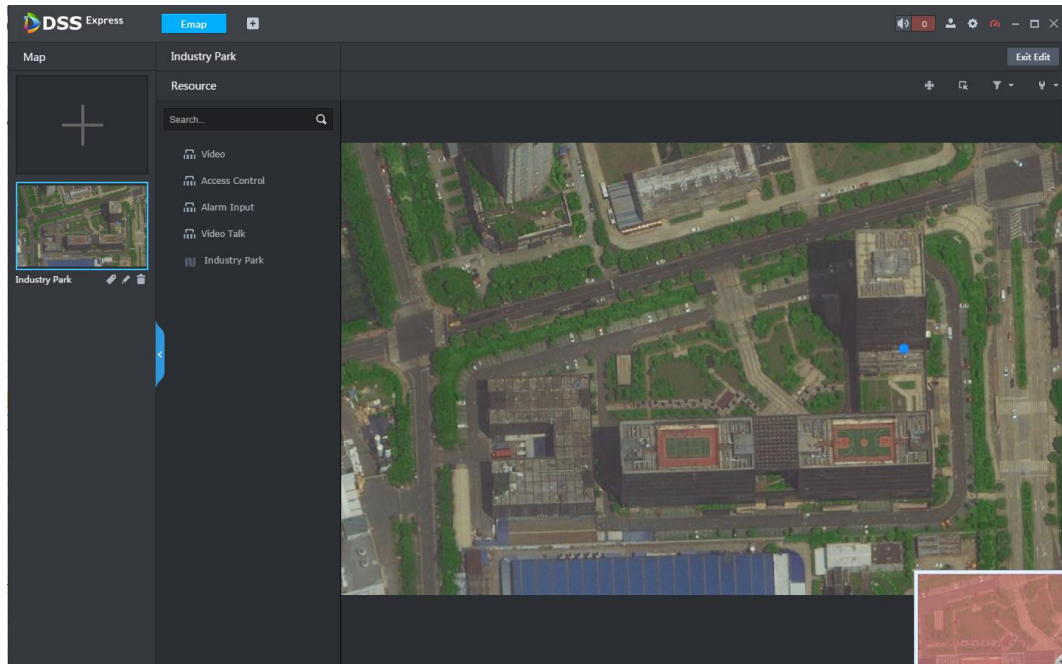


Picture supports raster map, supports PNG, JPG and JPEG.

- 3) Click **OK**.

The map is imported to platform, see Figure 3-63.

Figure 3-63 Added map



- 4) Click  under the map, set it as main map, yellow mark is displayed on the left upper corner, see Figure 3-64.

When several maps are added at the same time, the main map is displayed.

Figure 3-64 Set main map

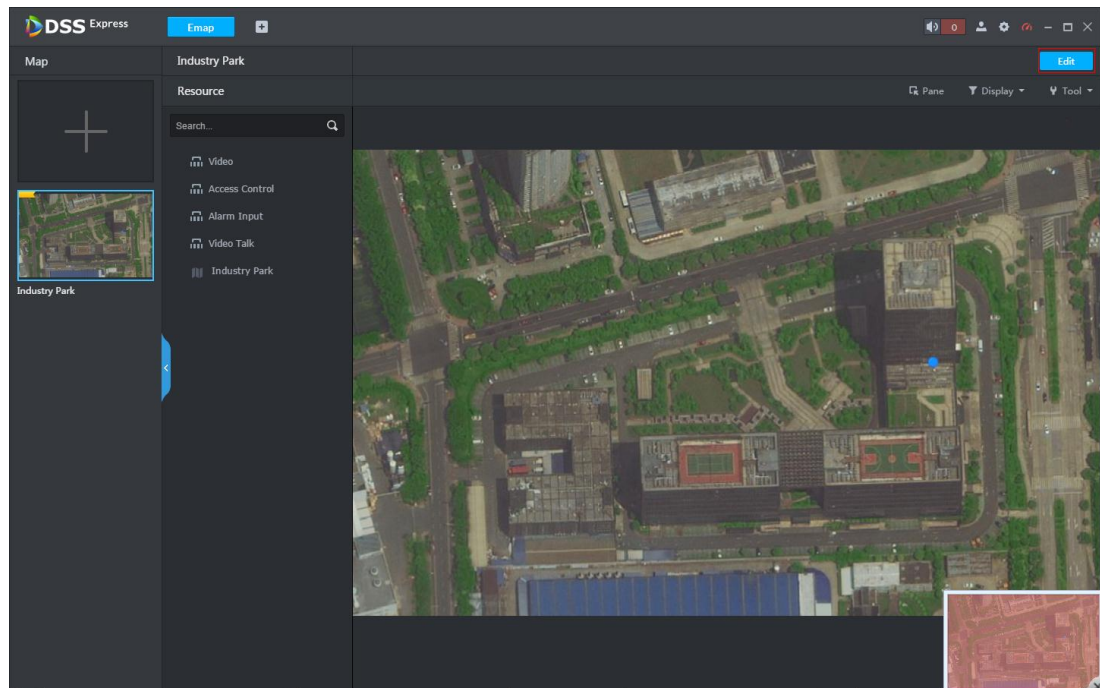


Step 3 Add hot zone in the map list.

The map can be configured with several layers, you can add lower level map to the existed map, and manage by levels.

- 1) Click map in the list, open the map, and see Figure 3-65.

Figure 3-65 Open map



- 2) Open map, click **Edit** on the upper right corner, and then you can edit the map.
- 3) Click , the mouse becomes map icon, select location on the map and click **Add**.

The system displays **Add Hot Zone** interface, see Figure 3-66.

Figure 3-66 Add hot zone

The 'Add Hot Zone' dialog box is shown. It has a dark gray background. The title bar at the top says 'Add Hot Zone' with a close button (X) on the right. Below the title bar, there are four input fields. The first is labeled 'Name :' and has a red asterisk next to it. The second is labeled 'Picture :' and has a folder icon to its right. The third is labeled 'Preview :' and has a map icon in the center of its text area; below the map icon, it says 'Import raster map, support PNG, JPG, JPEG'. The fourth is labeled 'Remark :'. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

- 4) Enter **Name** and **Remark**, click  and select picture.



- The format of imported raster map supports PNG, JPG and JPEG.
- After adding the picture, it is displayed on the preview area.

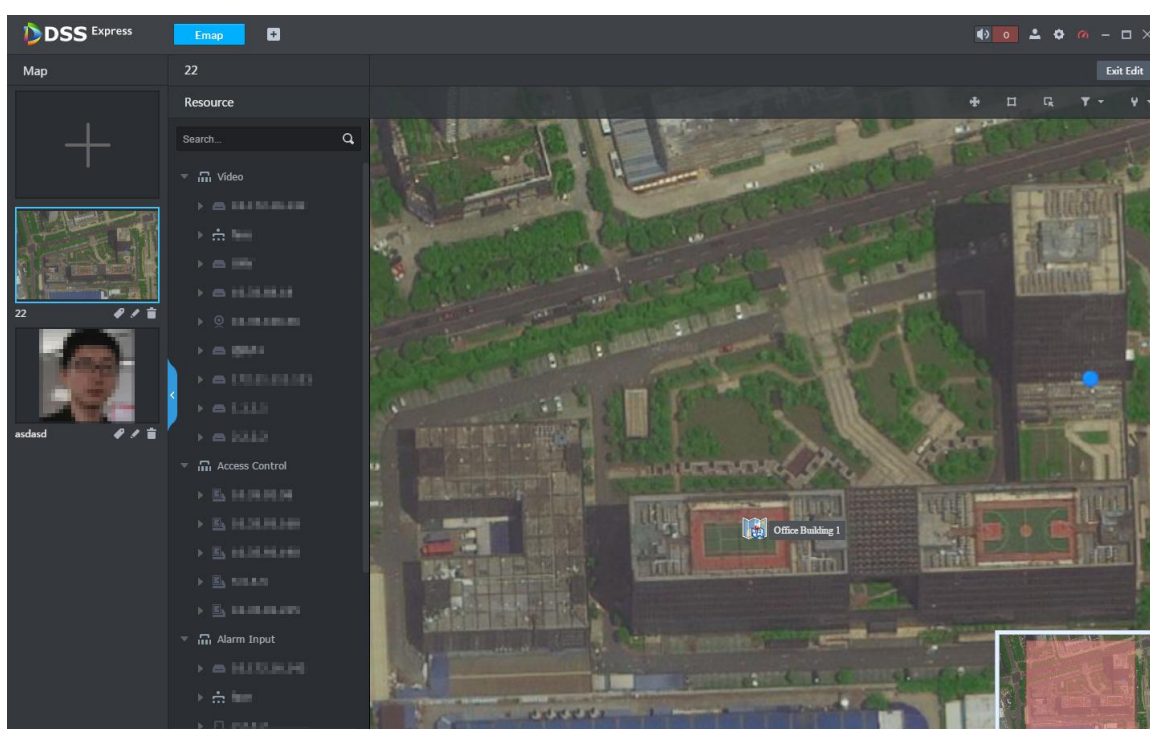
- 5) Click **OK**.

Hot zone is added, see Figure 3-67. Left list displays map levels, right map displays hot zone icon.



- After the hot zone is added, click hot zone on the left or hot zone icon on the right, then you can open hot zone for display.
- You can continue to add lower-level hot zone according to the operation above.

Figure 3-67 Hot zone added

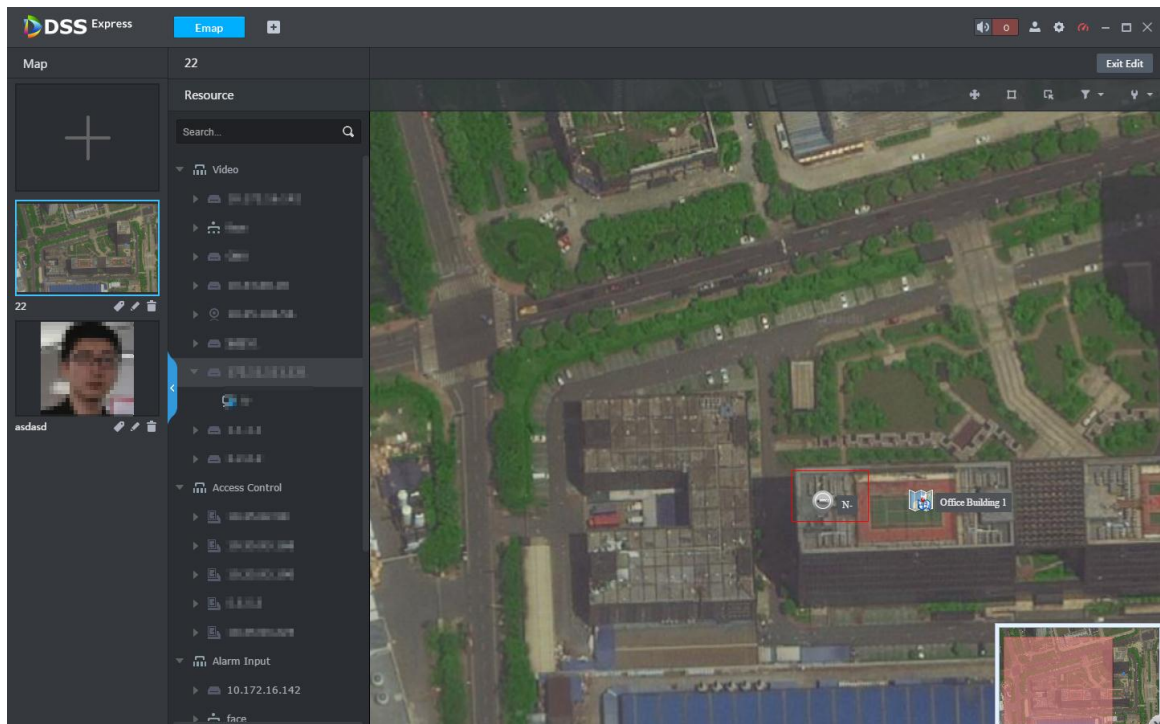


Step 4 Drag device channel onto the map for display.

According to actual requirement, add video channel, access control channel or alarm channel to the map, and device is linked to map, then you can see device and alarm on the map directly. Meanwhile, the track functions of different modules (such as personnel management and face recognition) can call map, and generate movement track.

- 1) Click the map in the list, and open the map, see Figure 3-65.
- 2) Click **Edit** on the upper right corner.
The map can be edited.
- 3) Select device channel from the resource list in the middle, drag to the proper location on the map, see Figure 3-68.

Figure 3-68 Add device channel



4) Click **Exit Edit** on the upper right corner.

3.2.6.2 Viewing Map

Step 1 Click **Emap** on the client homepage.

The system displays Emap interface.

Step 2 Click map in the list.

The system opens map, see Figure 3-69. For interface description, see Table 3-4.

Figure 3-69 Map

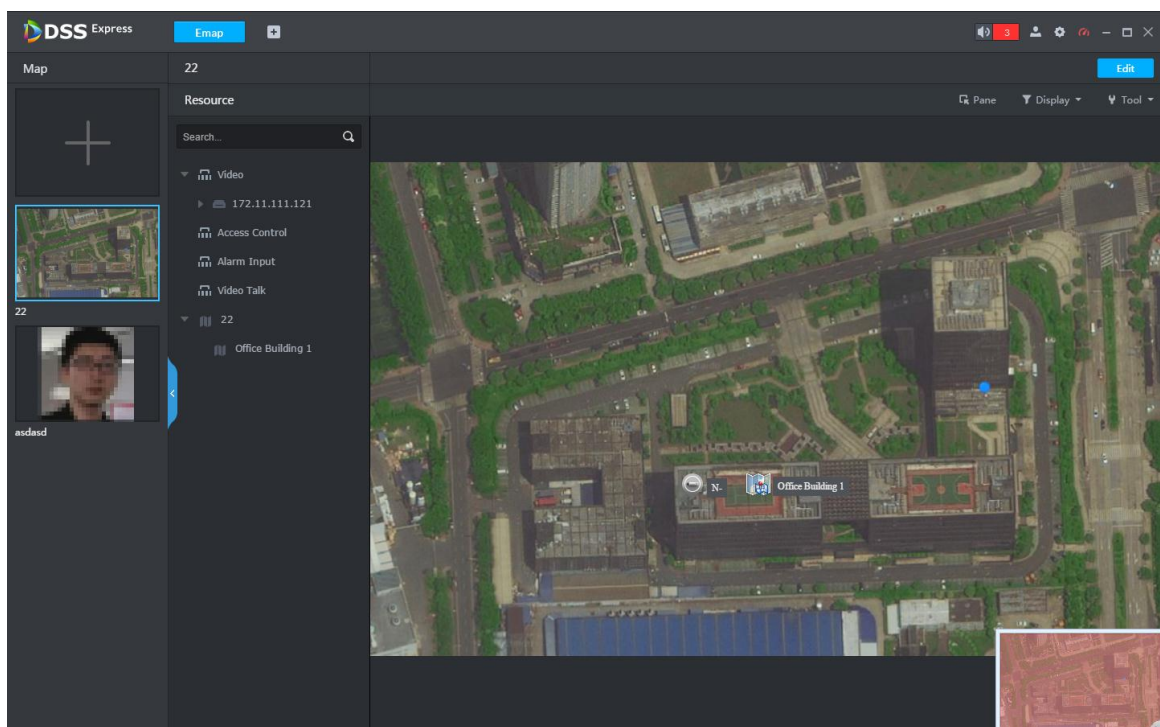


Table 3-4 Interface function description

Icon	Function	Description
	Select device	Click the icon and it becomes blue, select an area on the map and it displays the device list within the area. Select device, click corresponding icon, and then you can preview video, playback video and delete the device.
	Display device	Filter by device type, only the kept device type is displayed on the map.
	Mark or reset	Include mark and reset. ● Mark: Mark on the map. ● Reset: Restore the map to default position.

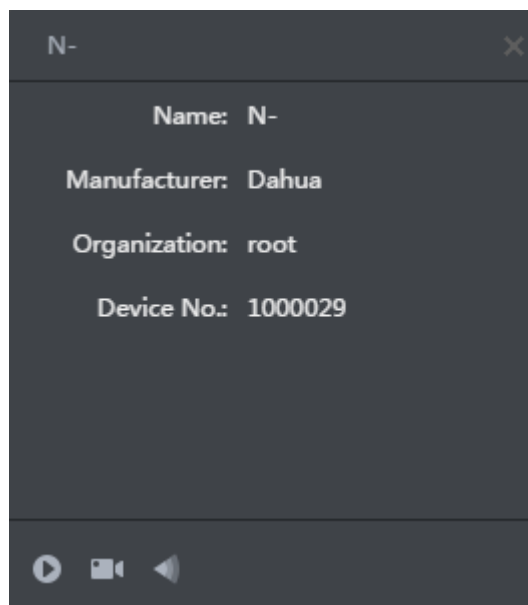
Following operations are supported on the map:

- View channels on map
Double click channel from the left device tree, and then you can view the channel position on the map.
 - ◇ Roll the mouse on the map and you can zoom in or out map.
 - ◇ If the picture is too big to be completely displayed, you can drag the red module on the lower right corner to display by mouse.
- View channel details
Click the channel on the map, the system displays device number, name, manufacturer and organization, see Figure 3-70.



Different devices may have different channel details and operations.

Figure 3-70 Channel info



- View channel video
Click  and open channel video.
- View playback
Click  and realize video playback.
- View visible range

Click  and view visible range.

- Edit map

Click **Edit** on the upper right corner, the map can be edited, see Figure 3-71. For operations, see

Figure 3-71 Edit map

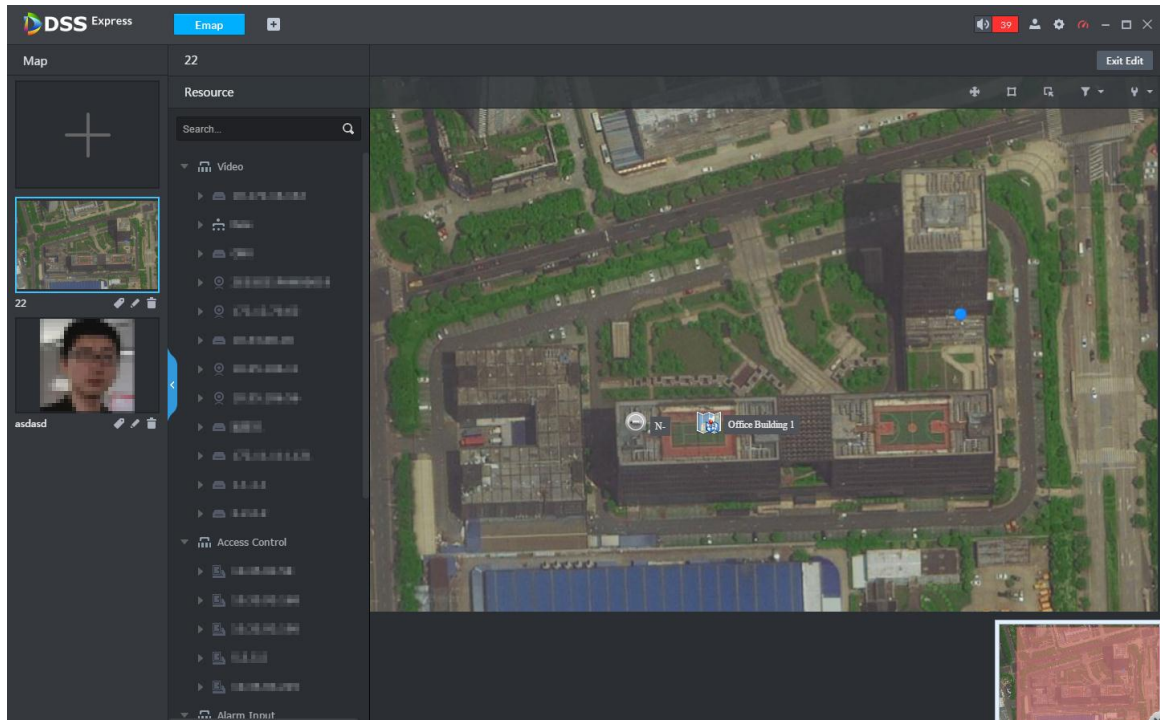
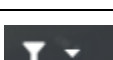


Table 3-5 Operation description

Icon	Function	Description
	Move device	Click the icon and it becomes blue, you can drag the device on map and change its position. Click again to exit move status
	Add hot zone	Refer to 3.2.6.1 Adding Map Step 3 Add hot zone in the map list.
	Select device	Click the icon and it becomes blue, select an area on the map and it will display device list within the area. Select device, click corresponding icon, and then you can preview view, playback video and delete the device.
	Display device	Filter by device type, only kept device type is displayed on the map.
	Mark or reset	Include mark and reset. ● Mark: Mark on the map. ● Reset: Restore the map to default position.

3.3 Local Config

Set client local config, including basic setting, video setting, playback setting, snapshot setting, record setting, alarm and shortcut key. All the settings only take effect to client.



If you want to restore default config, click **Default** and restart client according to system prompt.

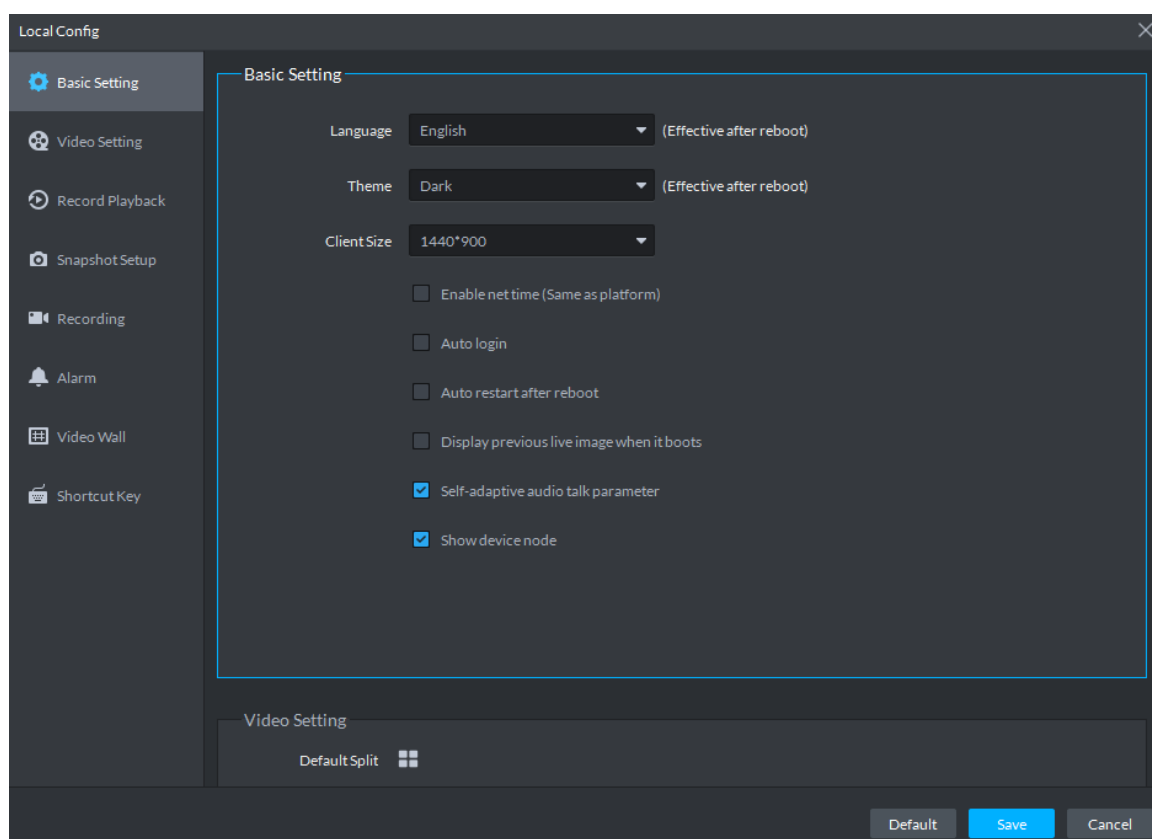
3.3.1 Setting Basic Parameter

Set client language, client size and sync time.

Step 1 Click  on the upper right corner on client interface.

The system displays **Local Config** interface, see Figure 3-72

Figure 3-72 Local config



Step 2 Click **Basic Setting** tab, set basic parameters, and see Figure 3-72. For parameter description, see Table 3-6.

Table 3-6 Basic parameter description

Parameters	Description
Language	Modify the language displayed on client; reboot the client to make it valid after setting.
Theme	Theme color includes dark and white. Reboot the client to make it valid after setting.
Client size	Select client proper resolution according to PC display screen.

Parameters	Description
Enable net time	If enabled, the client starts to synchronize network time with the server, and make the client time in accordance with that of server. The client will make following response when server requires net time. • If the parameter is selected, then client will respond to net time when server makes request. • If the parameter is not selected, then client will not respond when server makes request.
Auto login	• For login this time, Remember Password is selected on the Login interface, after selecting Auto Login, exit client and log in again, the system logs in automatically. • For login this time, Remember Password is not selected on the Login interface, after selecting Auto Login, exit client and log in again, Remember Password and Auto Login are selected by default on login interface, but still need to enter password authentication login.
Auto restart after reboot	• For login this time, Remember Password is selected on the Login interface, after selecting Auto restart after reboot, start PC again, and the system logs in client automatically. • For login this time, Remember Password is not selected on the Login interface, after selecting Auto restart after reboot, start PC again, the system displays client login interface.
Displayprevious live Image when it boots	If enabled, system displays the last live video automatically after rebooting the client.
Self-adaptive audio talk parameter	If enabled, the systems adapt to sampling frequency, sampling bit, and audio format to the device automatically during audio talk.
Show device node	Device tree displays device and channel info under device, otherwise it only displays channel.

Step 3 Click **Save**.

3.3.2 Setting Real-time Video Parameter

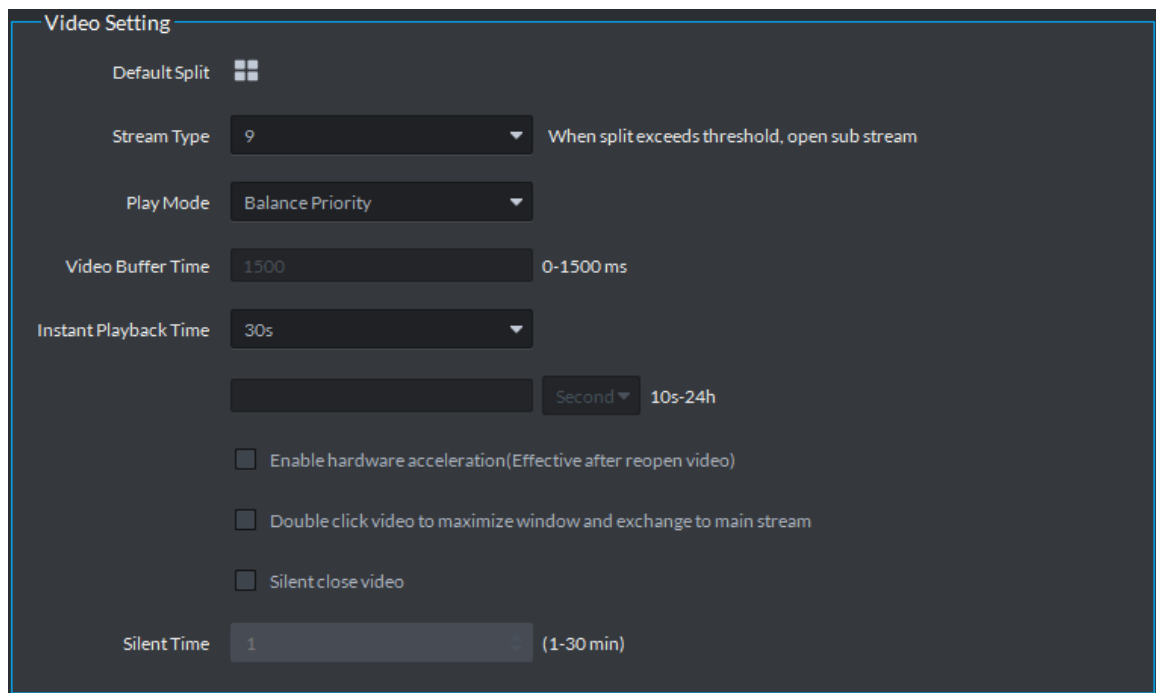
Set video window split mode, stream type, play mode and instant playback time.

Step 1 Click  on the upper right corner of client interface.

The system displays **Local Config** interface.

Step 2 Click **Video Setting** tab, set parameters, and see Figure 3-73. For parameter details, see Table 3-7.

Figure 3-73 Video setting



Video Setting

Default Split 

Stream Type 9  When split exceeds threshold, open sub stream

Play Mode Balance Priority 

Video Buffer Time 1500 0-1500 ms

Instant Playback Time 30s 

 10s-24h

☐ Enable hardware acceleration(Effective after reopen video)

☐ Double click video to maximize window and exchange to main stream

☐ Silent close video

Silent Time 1 (1-30 min)

Table 3-7 Video setting parameter description

Parameter	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 period.
Enable hardware acceleration	Check the box to enable the function. 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.
Silent 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 3 Click **Save**.

3.3.3 Setting Record Playback

Set video window split mode and record stream type.

Step 1 Click  on upper right corner of client interface.

The system displays **Local Config** interface.

Step 2 Click **Record Playback** tab, set parameters, and see Figure 3-74. For details, refer to Table 3-8.

Figure 3-74 Record playback

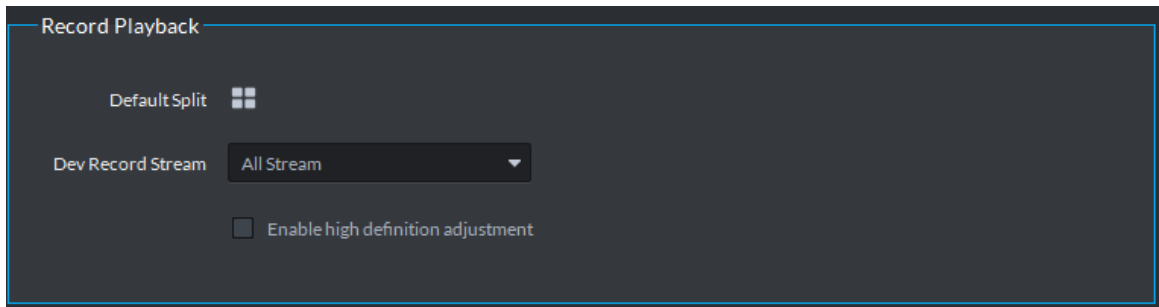


Table 3-8 Record playback parameter description

Parameters	Note
Default Split	Set default split mode of the playback window.
Device record stream	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 3 Click **Save**.

3.3.4 Setting Snapshot

Set snapshot save format, path and naming rule.

Step 1 Click  on upper right corner of client interface.

The system displays **Local Config** interface.

Step 2 Click **Snapshot Setup** tab, set snapshot format and save path, see Figure 3-75. For parameter details, see Table 3-9.

Figure 3-75 Snapshot setting

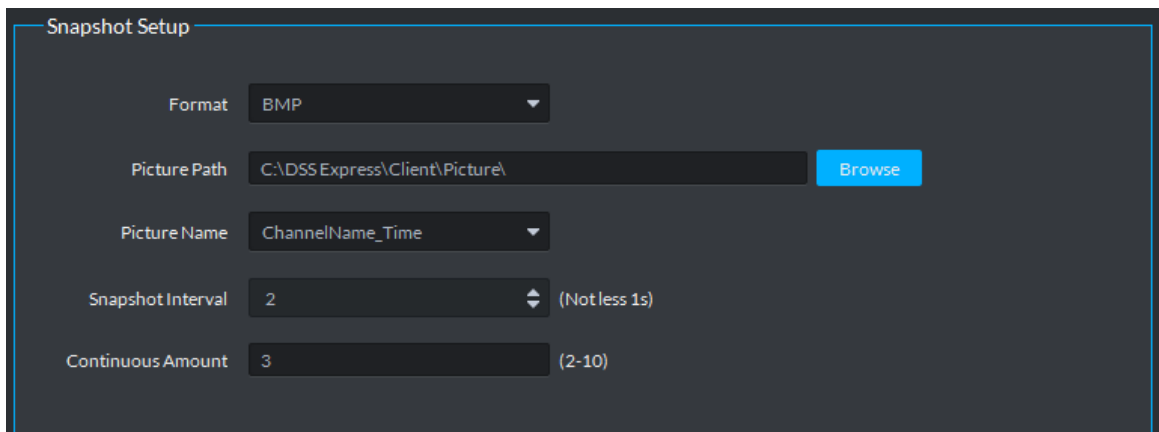


Table 3-9 Snapshot setting parameter description

Parameter	Description
Format	Set snapshot image format.
Picture path	Set snapshot storage path. The default path: C:\DSS Express\Client\Picture\.
Picture name	Select picture name rule.
Snapshot interval	Set snapshot interval. System snapshot once after the specified period.
Continuous amount	Snapshot amount at each time.

Step 3 Click **Save**.

3.3.5 Setting Recording Parameter

Set record path and record name of record file when recording on client.

Step 1 Click  on upper right corner of client interface.

The system displays **Local Config** interface.

Step 2 Click **Recording** tab, set record path and save path, see Figure 3-76. For parameter details, see Table 3-10.

Figure 3-76 Recording

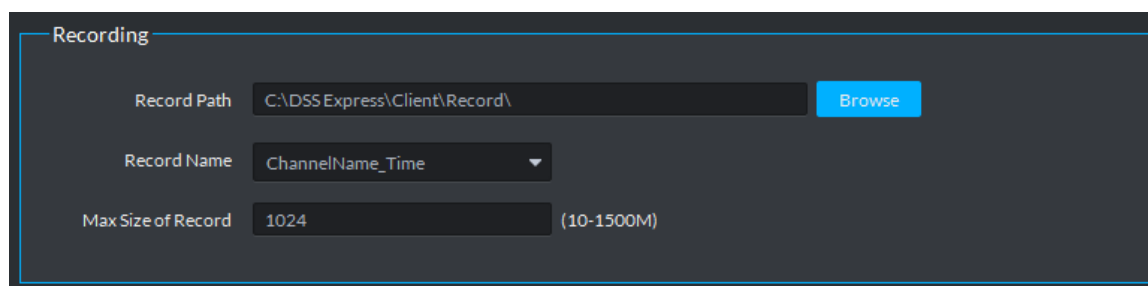


Table 3-10 Recording parameter description

Parameters	Note
Record path	Set record storage path. The default path: C:\DSS Express\Client\Record\.
Record name	Set record file name rule.
Max. record size	Set record file size.

Step 3 Click **Save**.

3.3.6 Setting Alarm Parameter

Set alarm type, sound path and video opening type.

Step 1 Click  on upper right corner of client interface.

The system displays **Local Config** interface.

Step 2 Click **Alarm** tab, set client alarm type, see Figure 3-77.

Figure 3-77 Alarm

Table 3-11 Alarm parameter description

Parameter	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.  This item is only valid when Play alarm sound function is enabled.
Alarm Type	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	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 3 Click **Save**.

3.3.7 Setting Video Wall

Set default stream type and stay time when linking video wall.

Click **Video Wall** and set parameters, see Figure 3-78. For parameter details, see Table 3-12.

Figure 3-78 Video wall

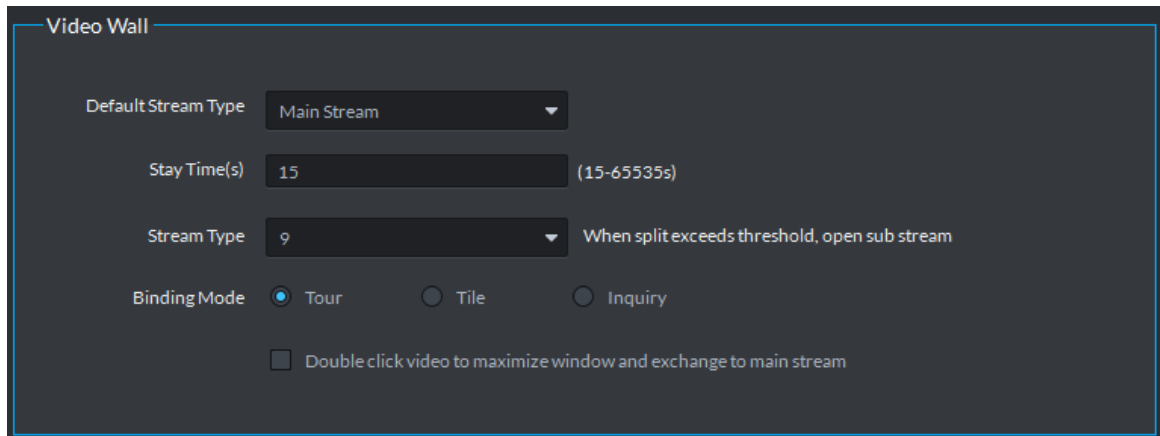


Table 3-12 Video wall parameter description

Parameter	Description
Stream type	When split exceeds threshold, open substream.
Binding mode	● Tour: Device nodes are displayed on 1 window by tour. ● Tile: Device nodes are aredisplayed 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.

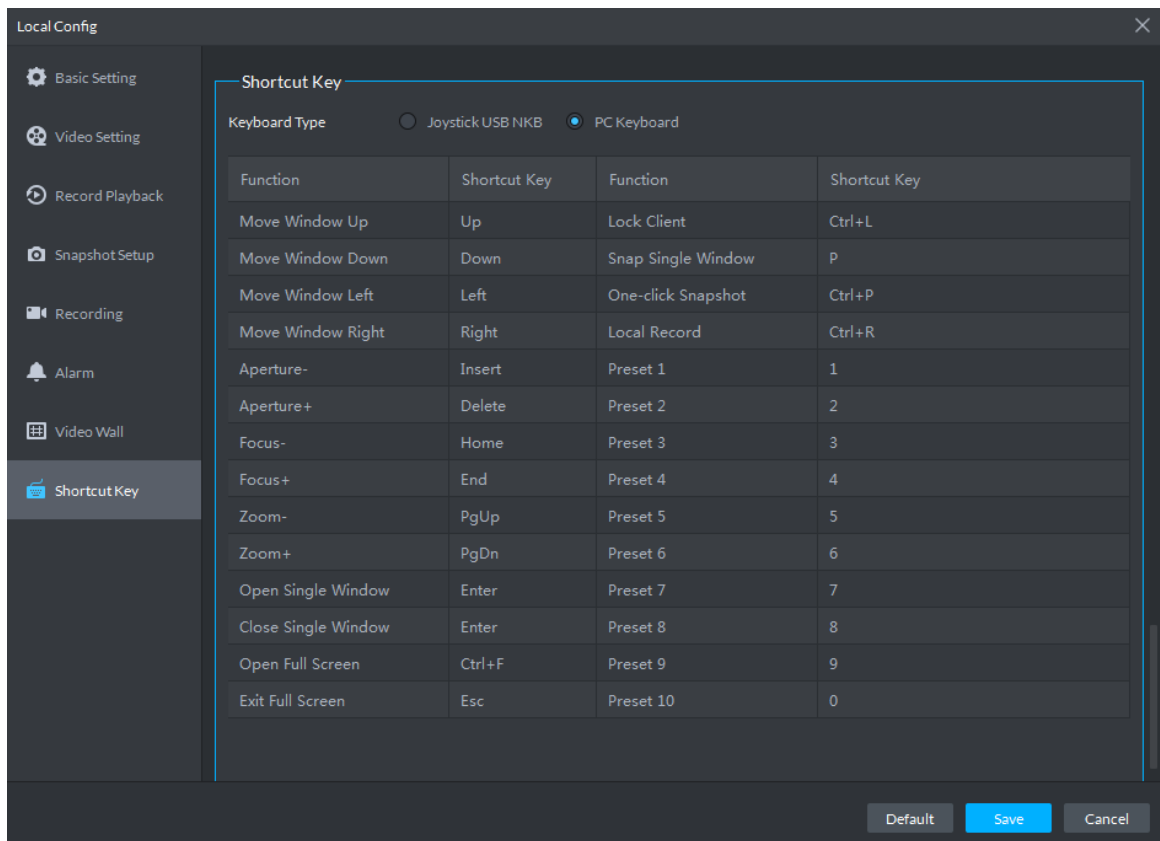
3.3.8 Setting Shortcut Key

Set client shortcut key and control client quickly.

Step 1 Click  on upper right corner of client interface.
The system displays **Local Config** interface.

Step 2 Click **Shortcut Key** tab, check PC keyboard or shortcut key of USB keyboard, see Figure 3-79.

Figure 3-79 Shortcut key



Step 3 Click **Save**.

3.4 Live View

You can check video of online channel. If the device is equipped with PTZ function, then you can operate PTZ on platform.

3.4.1 Entering Live View Interface

On client homepage, click **Live View**. The system displays **Live View** interface, see Figure 3-80. For interface description, see Table 3-13.

Figure 3-80 Live view

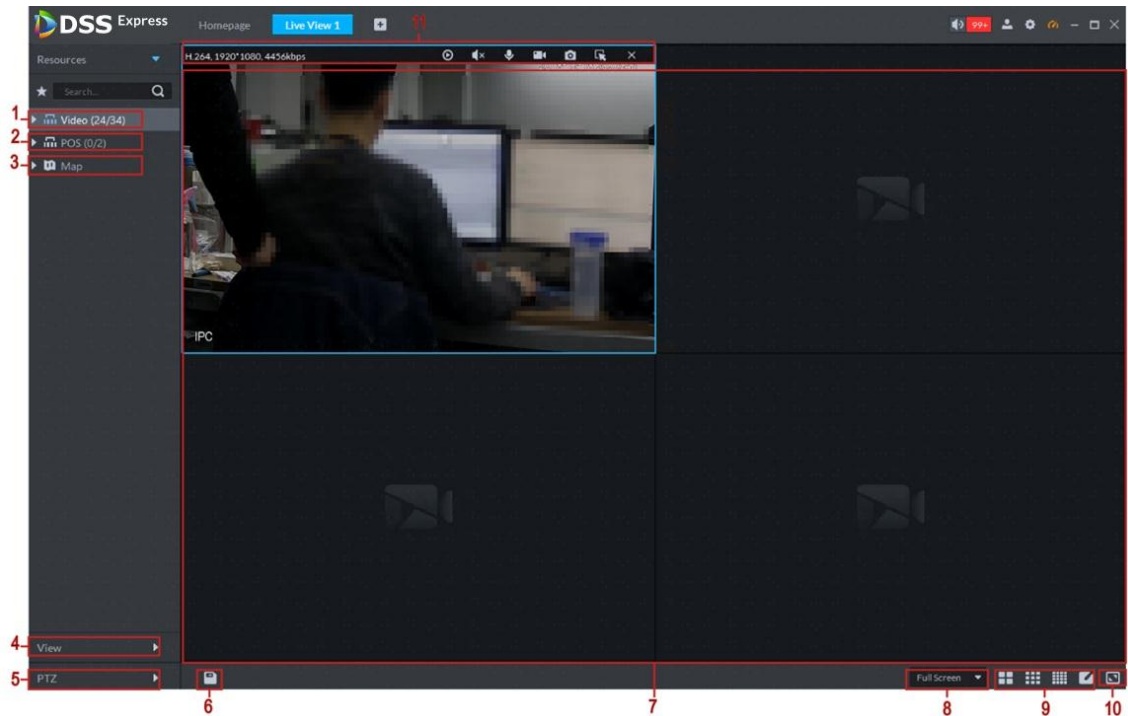


Table 3-13 Live view interface description

No.	Parameter	Description
1	Resources	- Click and enter favorite. - You can search device or channel in according to device name or channel name. - Display device list. If you enable Show Device Node in Local Config > Basic Setting, then the device tree displays device and its channels, or you can disable it and display all the device channels.
2	POS	You can open POS and related video channels from live window.
3	Map	Display added map, double click to open map, select device and support live view and cancel alarm.
4	View	Display created view list.
5	PTZ	For detailed operation of PTZ, refer to 3.4.5 Setting PTZ
6	Save View	Record live video window split and window play. Save as preview plan for quick call. For detailed operation, see 3.4.8 View
7	Video Play Window	Display live view image. Move the mouse to the video window which is being displayed; scroll the mouse to zoom in or out video. Right click and refer to 3.4.2 Enabling Live View .
8	Display Mode	Select height and width ratio of video window, you can play video by actual ratio or full window.

No.	Parameter	Description
9	Image Split Mode	Used to set image split mode, support 1, 4, 6, 8, 9, 13, 16, 20, 25, 36 and 64, or click  and customize split mode.
10	Full Screen	Switch video window to Full Screen mode. If you want to exit Full Screen , you can press Esc button or right click and select Exit Full Screen .
11	Stream and Shortcut	Display encode format, stream and shortcut operation. For detailed operation, see 3.4.2 Enabling Live View .

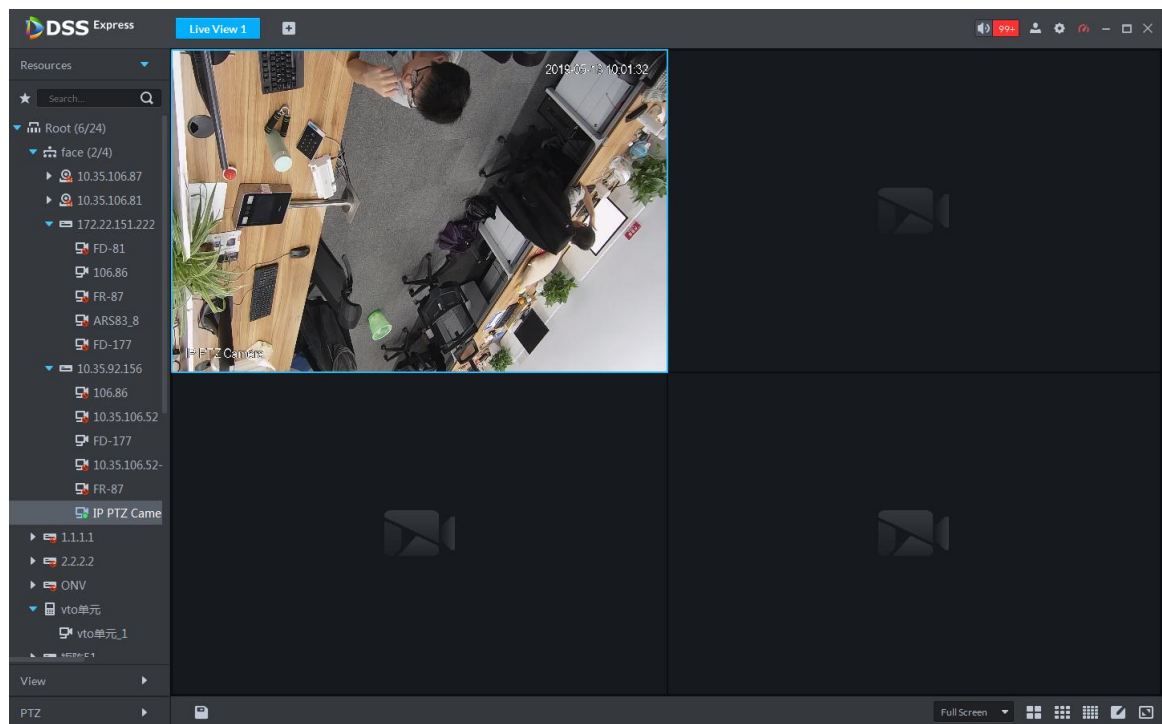
3.4.2 Enabling Live View

Select channel or device from device list on the **Live View** interface, double click or drag to video window. The system plays realtime video, see Figure 3-81.



- If number of window splits is less than number of device online channels, then you can select online channel by window splits in sequence.
- If number of window splits is more than number of device online channels, then channel video is displayed on window in sequence.
- You need to close tour and then display live view.

Figure 3-81 Enable live view



Related operations of live view are shown as follows:

- Move the mouse to video window, shortcut operation menu is displayed on upper right corner of the window, see Figure 3-82. For detailed description, see Table 3-14.

Figure 3-82 Shortcut menu

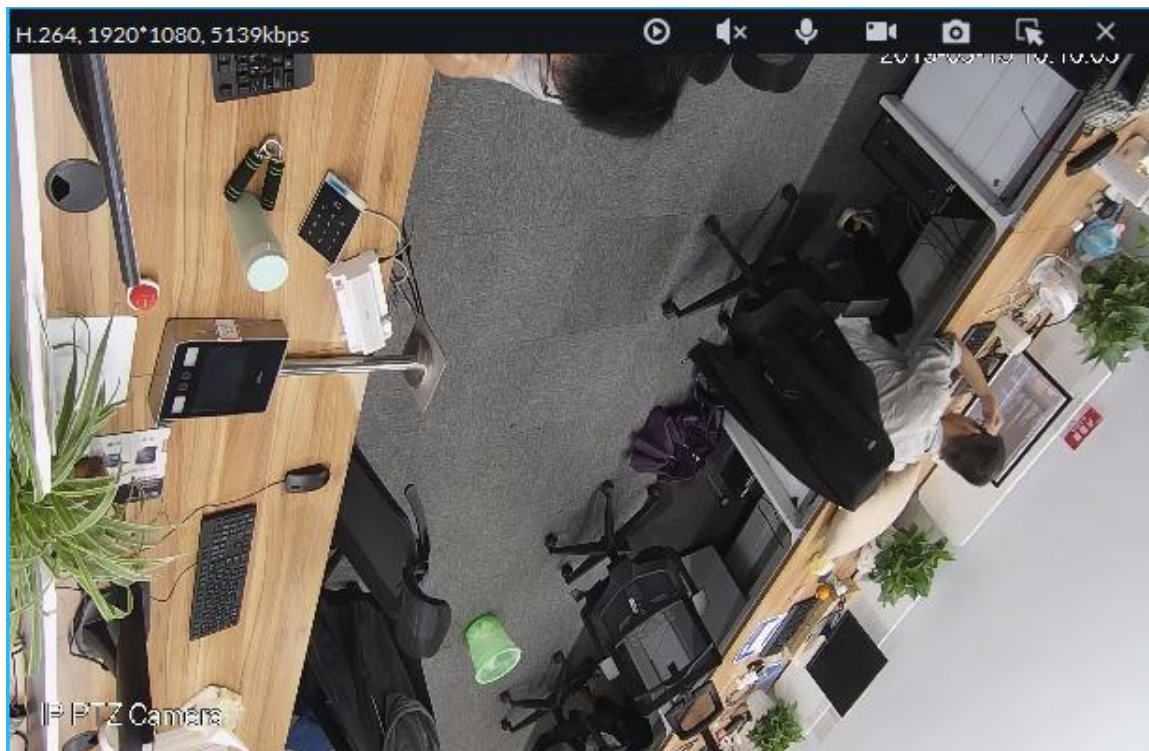


Table 3-14 Shortcut menu description

Icon	Name	Note
	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 top 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.

- Right click live view window, display menu shown in Figure 3-83. For operation description, see Table 3-15.



Different devices display different menu by right click, the actual interface shall prevail.

Figure 3-83 Right click menu

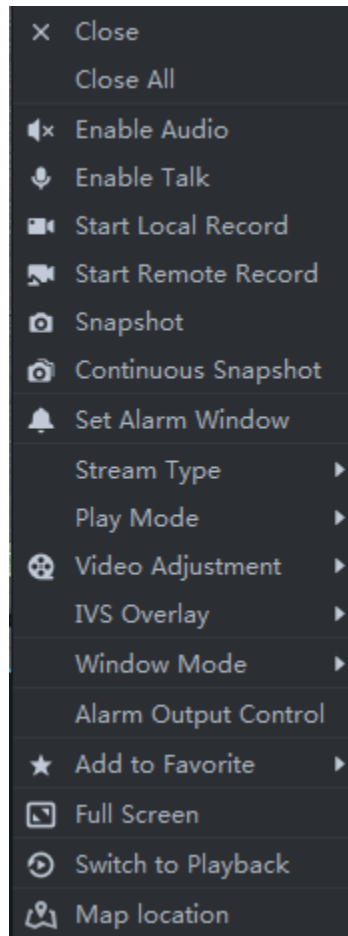


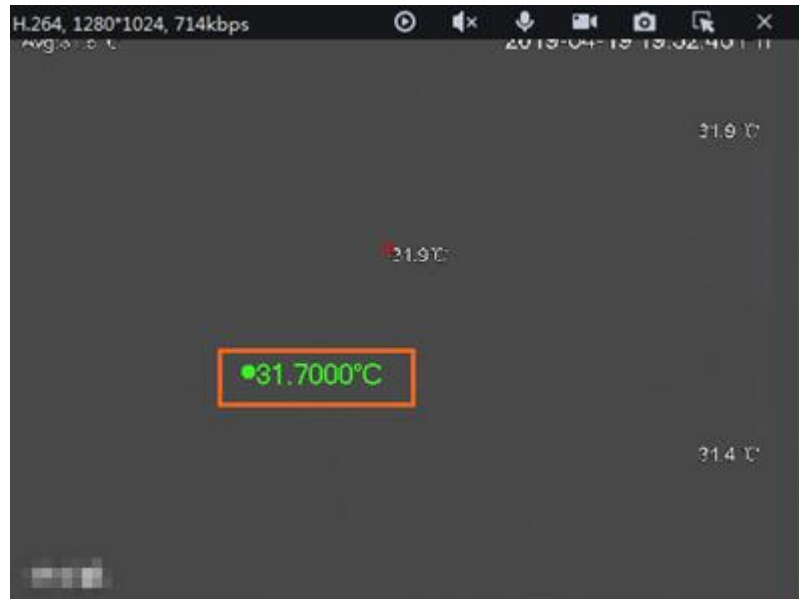
Table 3-15 Right click menu description

Parameters	Note
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.
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 Snapshot	To save image of the active video window as picture (three snapshots each time by default).
Set Alarm Window	Turn on/off alarm output.

Parameters	Note
Stream Type	Switch among Main stream, Sub stream and Third stream.  NOTE If selecting Sub stream or Third stream, you need to check enable Sub Stream and enable Third Stream in the Bit Stream dropdown list when adding encoder from the Manager.
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	Enable IVS rules and target box, after that IVS rule and target box will be displayed during live view. The config is only valid to the configured channel. The IVS rule and target box are not displayed by default.
Installation mode	 NOTE 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	 NOTE 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. • 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	Support standard mode, 1+3 mode, 1+5 mode.
Alarm output control	It control alarm input/output.
Add To Favorites	You can add the active channel or all channels into Favorite.
Full Screen	Switch the video window to full screen mode. To exit full screen, double click video window, or right click to select exit full screen.
Switch to Playback	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.

- If you preview thermal channel, move the mouse and lay it any position of the image, and then the platform displays realtime temperature of the position, see Figure 3-84.

Figure 3-84 Spot temperature measurement



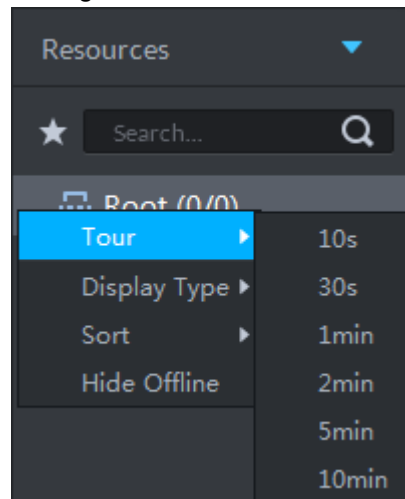
3.4.3 Enabling Tour View

Right click device or organization in the device list on **Live View** interface, select **Tour** and set duration. See Figure 3-85. The system plays video image of all online channels in loop, click



or right click window to stop. Select **Stop Tour** if you want to.

Figure 3-85 Tour interface



3.4.4 Device Config

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

NOTE

Device config differs by the capacities of the devices. Snapshots in this Manual are taken from IPC-HDW7341X-E2 (Software version V2.622.0000000.4.T). The actual interfaces of other models shall prevail.

3.4.4.1 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.

3.4.4.1.1 Configuring Property Files

Step 1 On the **Preview** interface, right-click the video device and select **Device Config**. See Figure 3-86.

The **Device Config** interface is displayed. See Figure 3-87.



NOTE

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

Figure 3-86 Entering device config

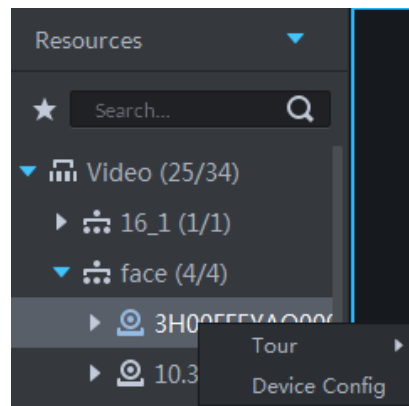
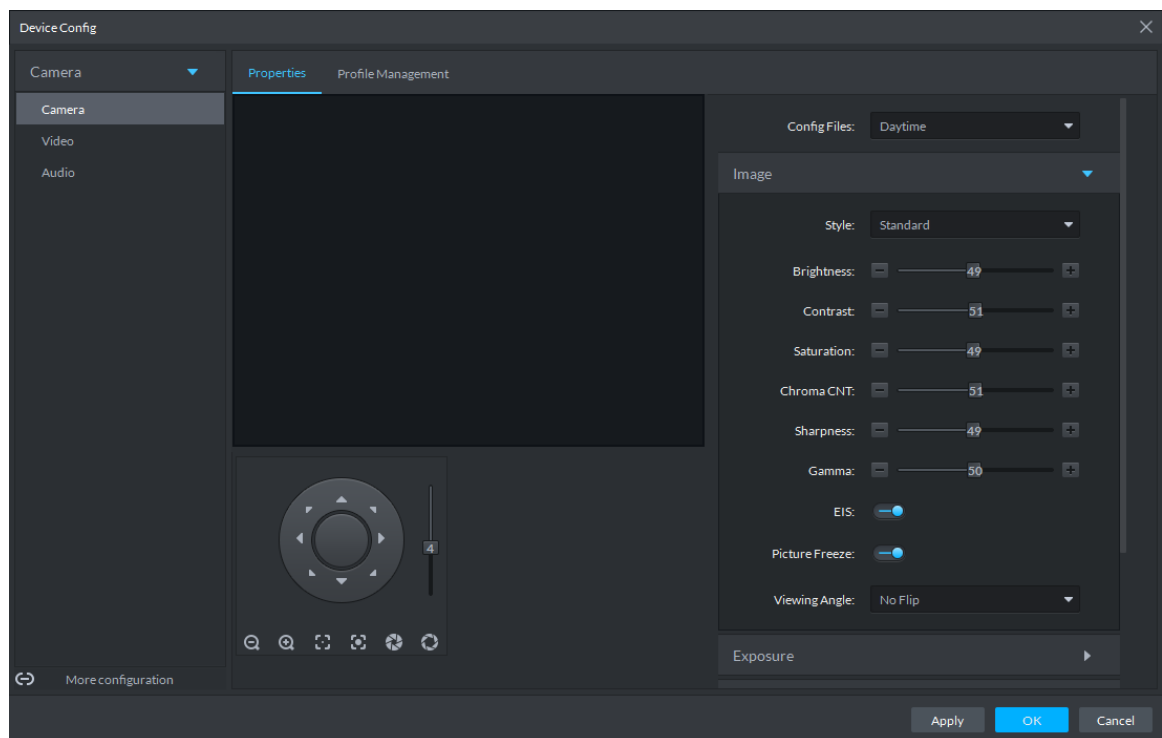


Figure 3-87 Device config



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

The **Properties** interface is displayed. See Figure 3-87.

Step 3 Select **Profile Management**.

Step 4 Click **Image**. See Figure 3-87. For details of the parameters, see Table 3-16.

Table 3-16 Image parameter description

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. See Figure 3-88. For details of the parameters, see Table 3-17.



NOTE

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

Figure 3-88 Exposure

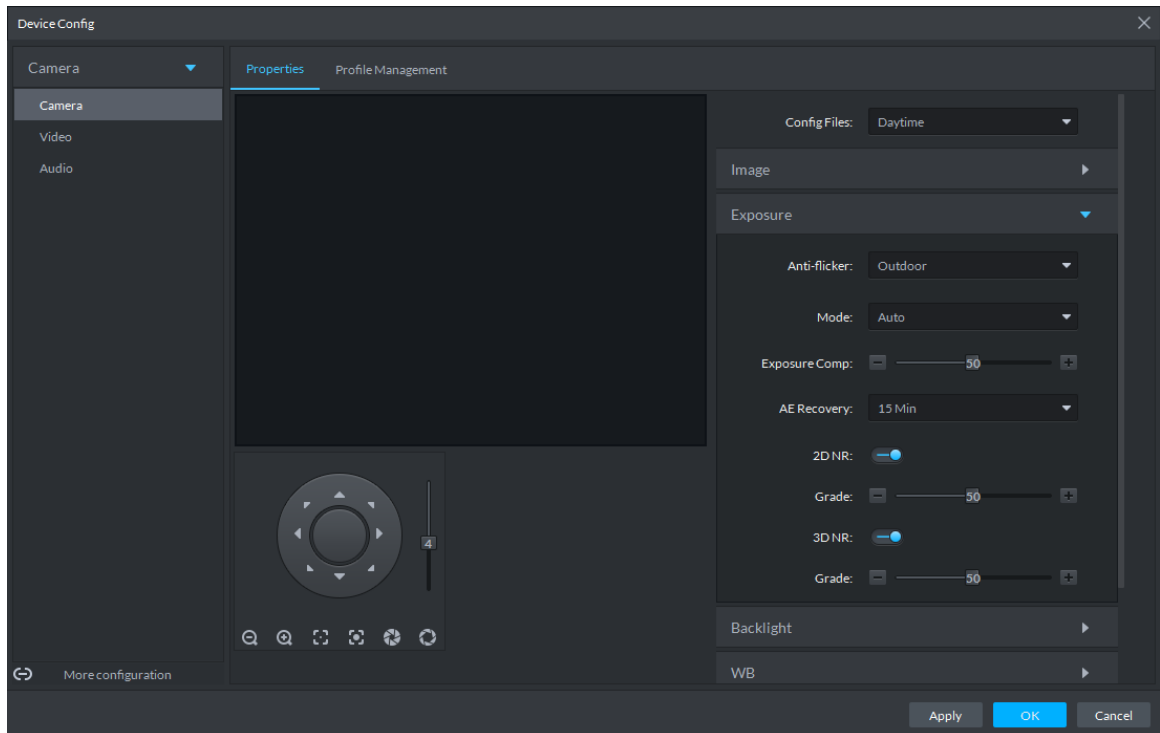


Table 3-17 Exposure parameter description

Parameter	Description
Anti-flicker	You can select from these three modes: 50Hz, 60Hz, or Outdoor. 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	The following options are available for the different exposure modes of the camera:  - 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	When 3D NR is On, you can set up this parameter. The higher the grade, the better the noise reduction effect.

Step 6 Click **Backlight** to set up relevant parameters. See Figure 3-89. For details of the parameters, see Table 3-18.

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 3-89 Backlight

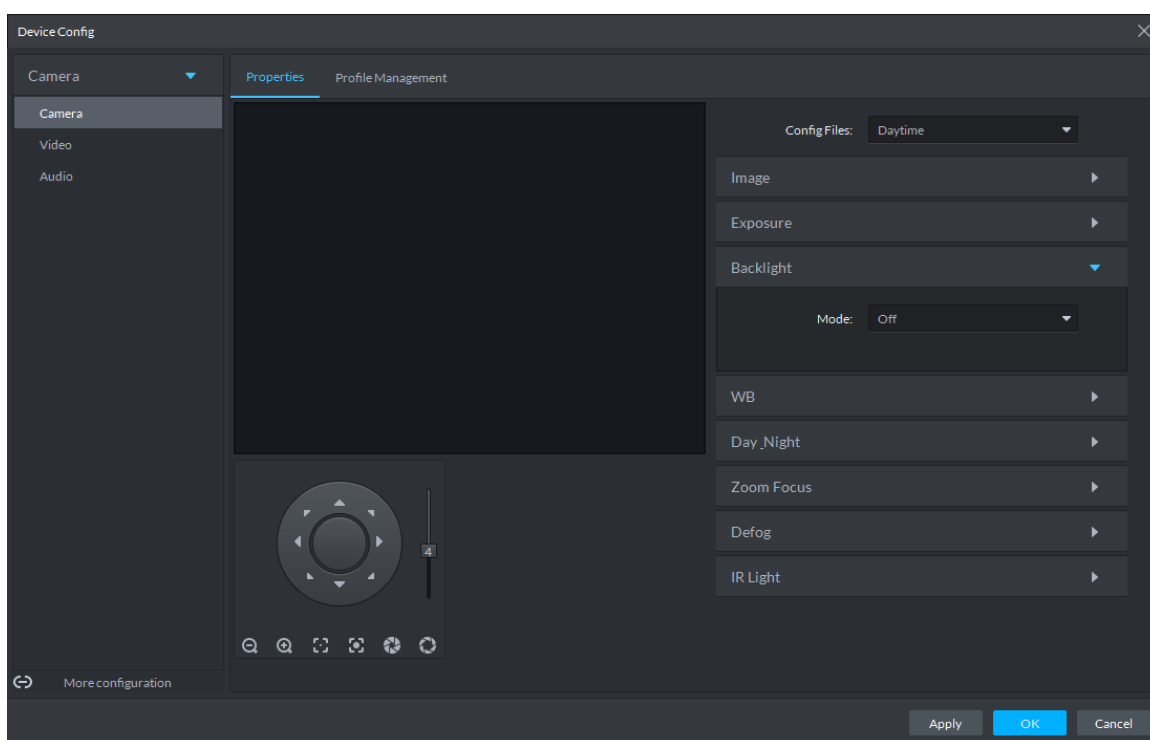


Table 3-18 Backlight mode description

Backlight mode	Description
SSA	The system adjusts image brightness automatically based on the environmental lighting conditions to show image details clearly.
Backlight Correction	You can select Default mode or Custom mode. • When selecting the Default mode, the system adjusts exposure automatically to adapt to the environment and make the images taken in the darkest regions clear. • When selecting the Custom mode and setting up a custom region, the system exposes the selected custom region to give the images taken in this region proper brightness.
Wide Dynamic	To adapt to the environmental lighting conditions, the system reduces the brightness in bright regions and increases the brightness in dark regions. This ensures clear display of objects in both bright and dark regions.  The camera might lose seconds of video recordings when switching from a non-wide dynamic mode to Wide Dynamic.

Backlight mode	Description
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. See Figure 3-90. For details of the parameters, see Table 3-19.

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 3-90 WB

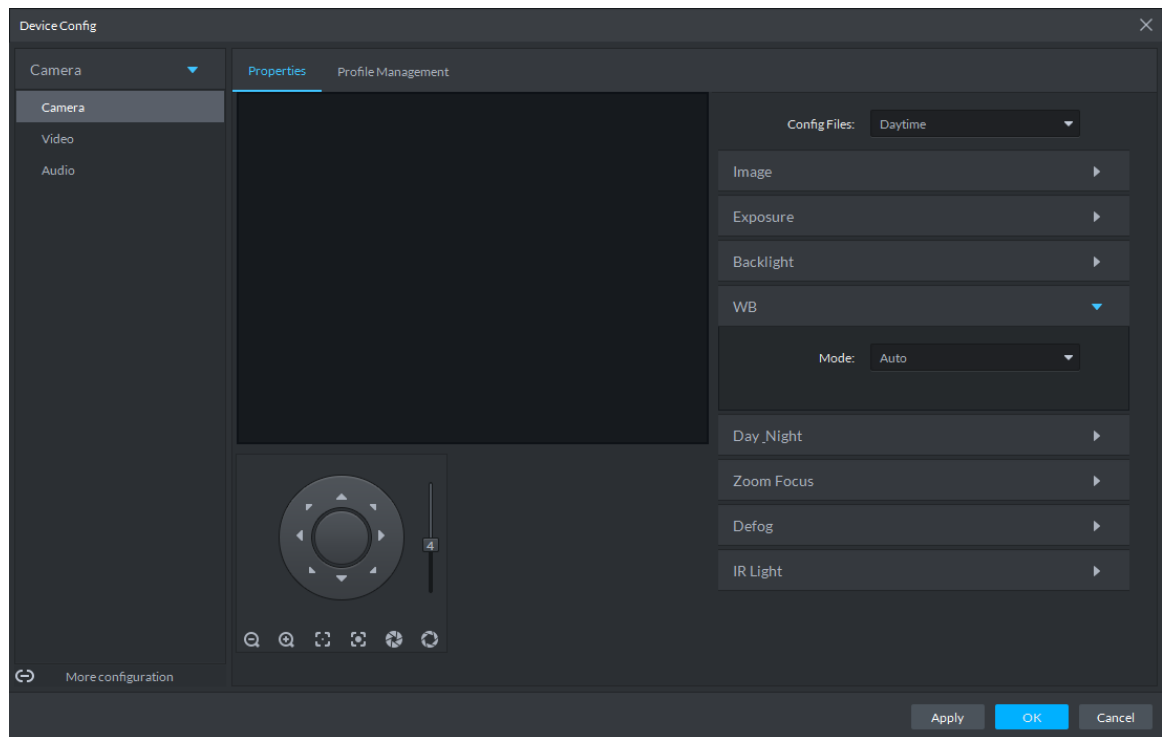


Table 3-19 WB mode description

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. See Figure 3-91. For details of the parameters, see Table 3-20.

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 3-91 Day/Night

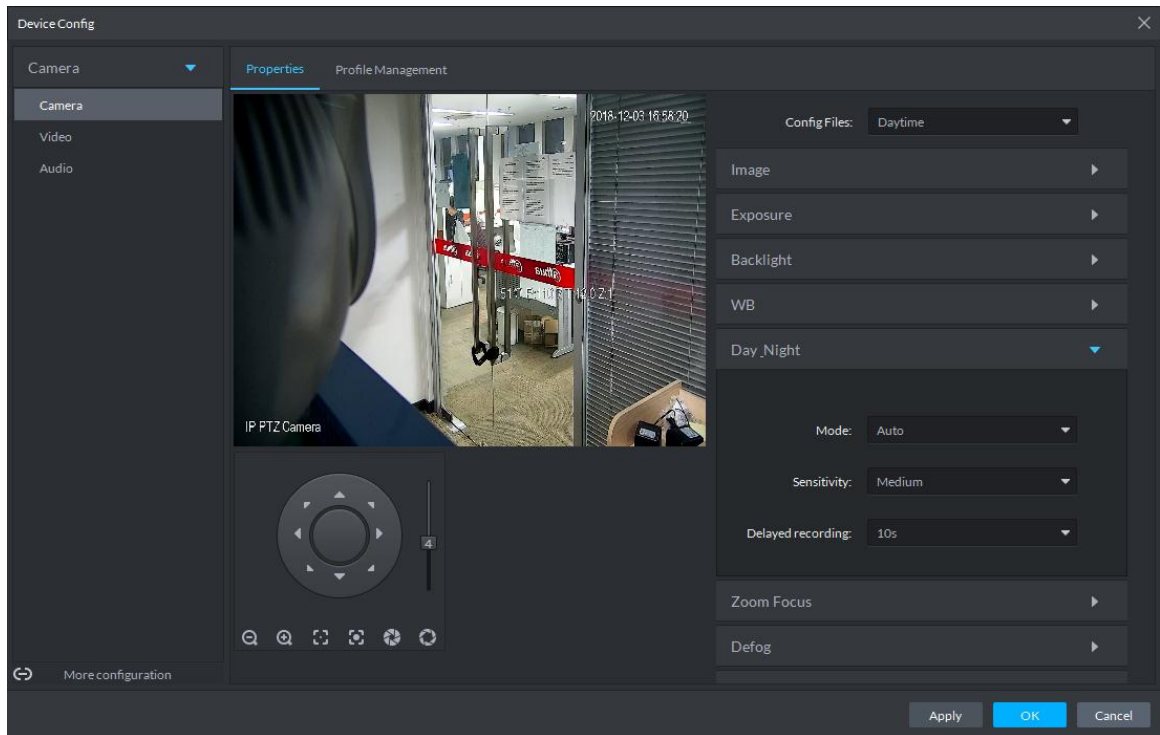


Table 3-20 Day/night mode parameter description

Parameter	Description
Mode	You can set up the image display of the camera to the Colored mode or the Black&White mode, including the following options:  The Day & Night settings are independent of the Config Files settings. - 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	You can set up this parameter when the Day & Night mode is set to Auto. Defines the sensitivity of the camera in switching between the Colored mode and the Black&White mode.
Delayed recording	You can set up this parameter when the Day & Night mode is set to Auto. Defines the delay of the camera in switching between the Colored mode and the Black&White mode. The lower the delay, the faster the switch between the Colored mode and the Black&White mode.

Step 9 Click **Defog** to set up relevant parameters. See Figure 3-92. For details of the parameters, see Table 3-21.

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 3-92 Defog

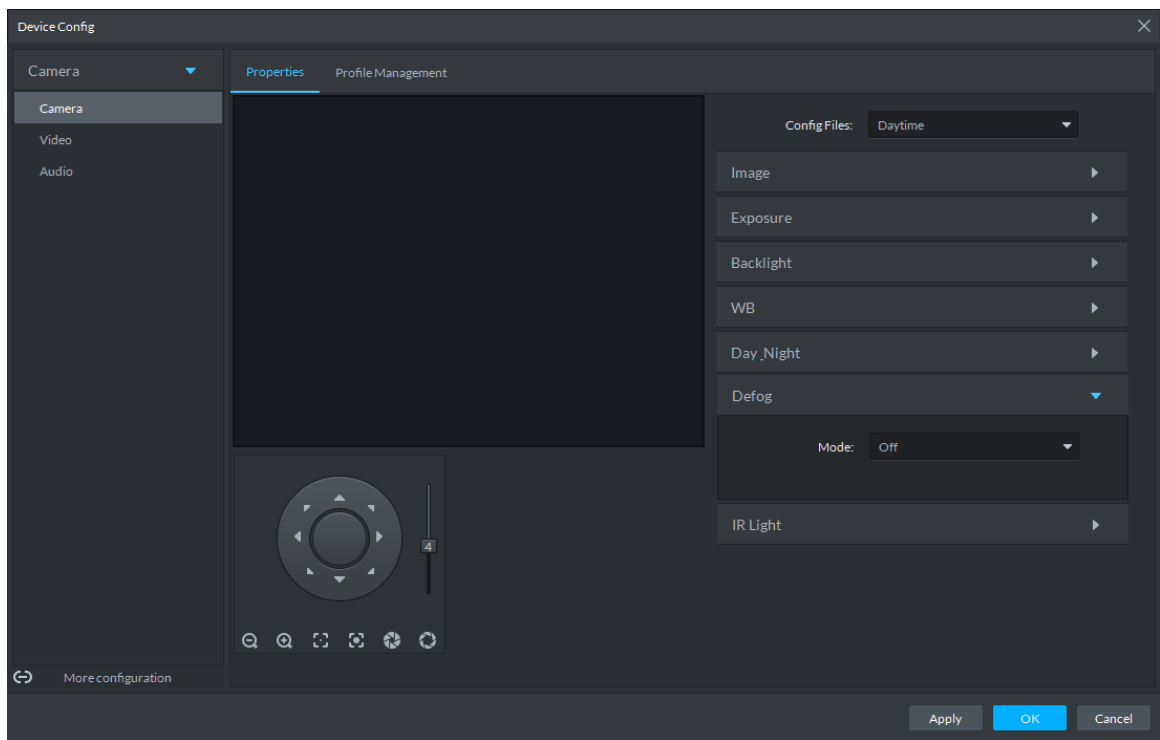


Table 3-21 Defog mode description

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. See Figure 3-93. For details of the parameters, see Table 3-22.

Figure 3-93 IR light

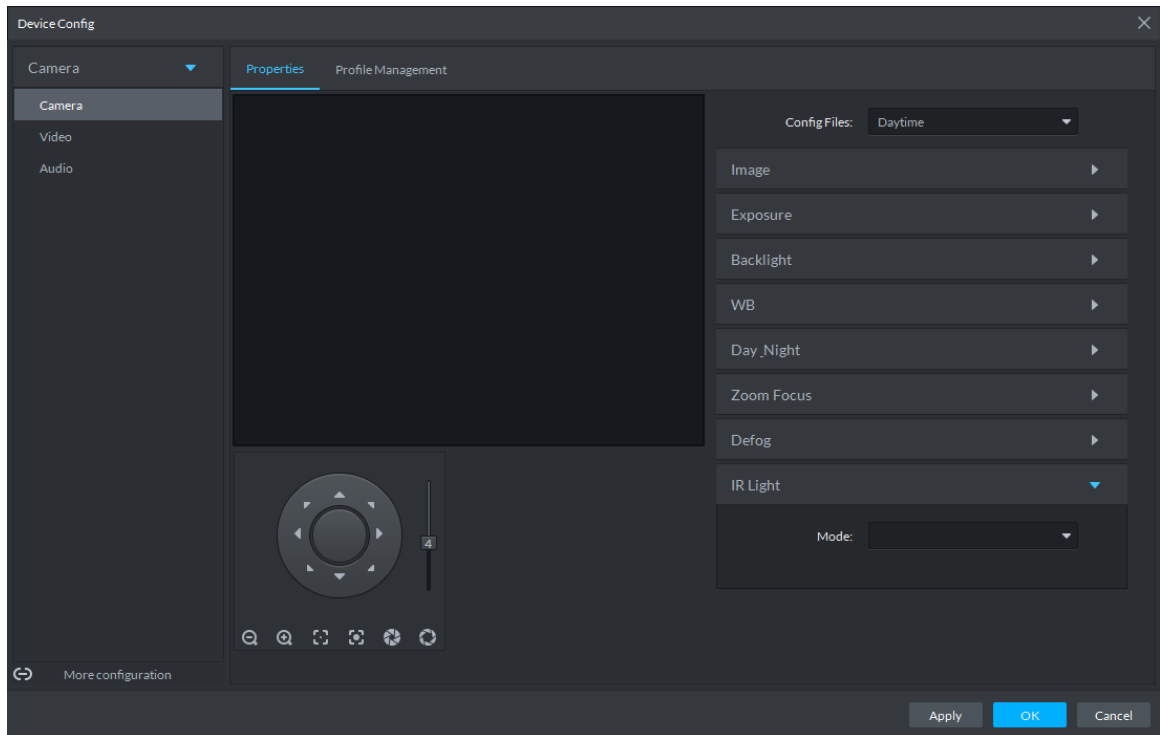


Table 3-22 IR light mode description

IR Light mode	Description
Manual	You can set up the IR Light brightness manually. The system fills light for images as per the preset IR Light brightness.
SmartIR	The system adjusts the brightness of the light to adapt to the surrounding conditions.
ZoomPrio	The system adjusts the IR Light automatically to adapt to the brightness changes in the environment. - 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 Config Files in a different mode, repeat the steps to complete the configurations.

3.4.4.1.2 Applying Config Files

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

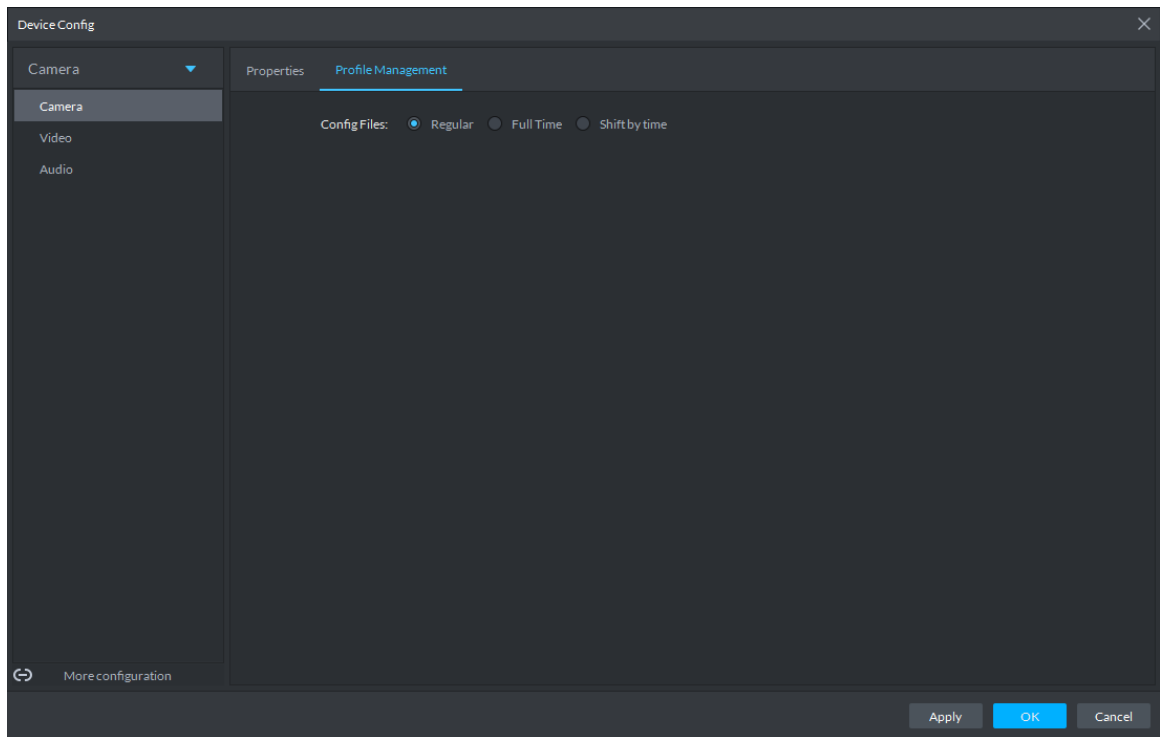
Step 1 Select **Camera > Camera > Properties > Profile Management**.

The **Profile Management** interface is displayed.

Step 2 Setting up config files.

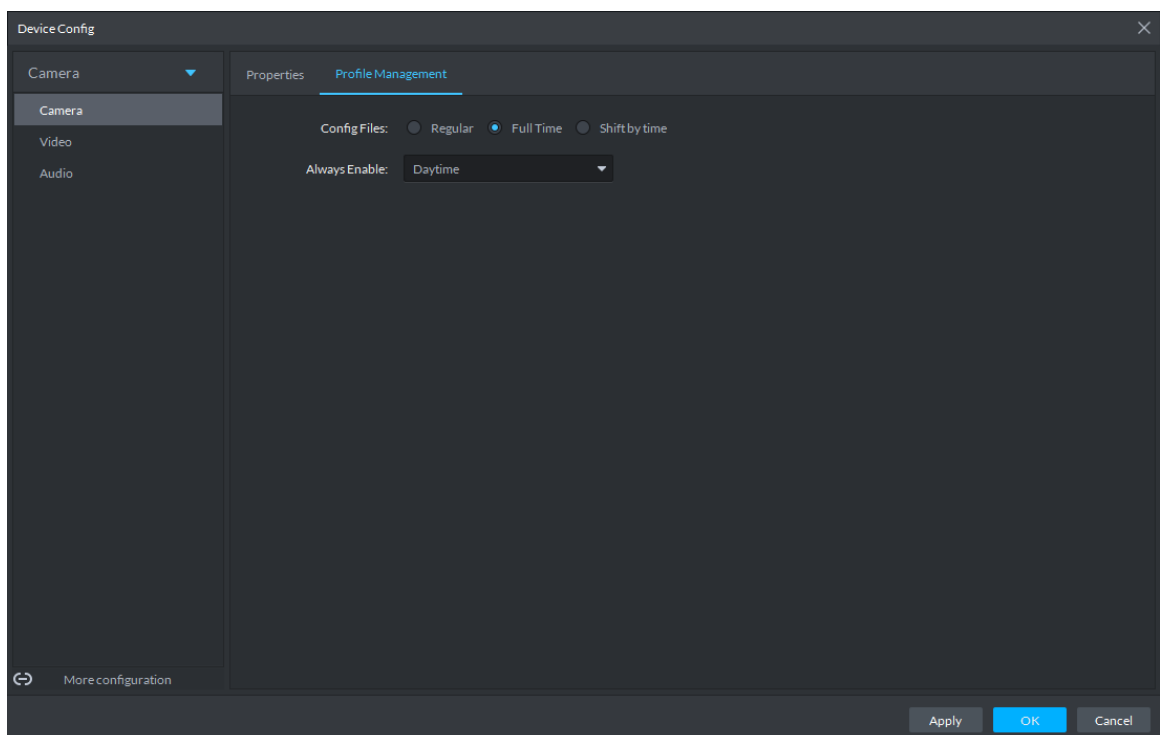
- When **Config Files** is set to **Regular**, the system monitors the objects as per regular configurations.

Figure 3-94 Regular



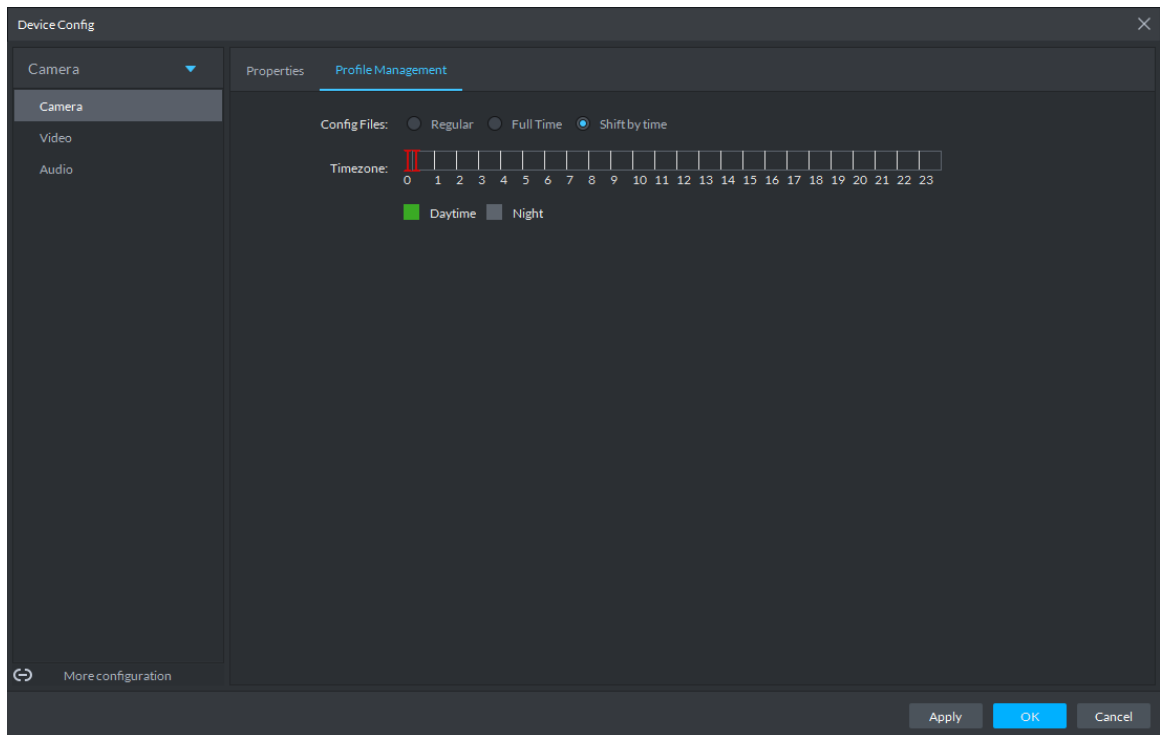
- When **Config Files** is set to **Full Time**, you can set **Always Enable** to **Daytime** or **Night**. The system monitors the objects as per the **Always Enable** configurations.

Figure 3-95 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 3-96 Shift by time



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

3.4.4.2 Video

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

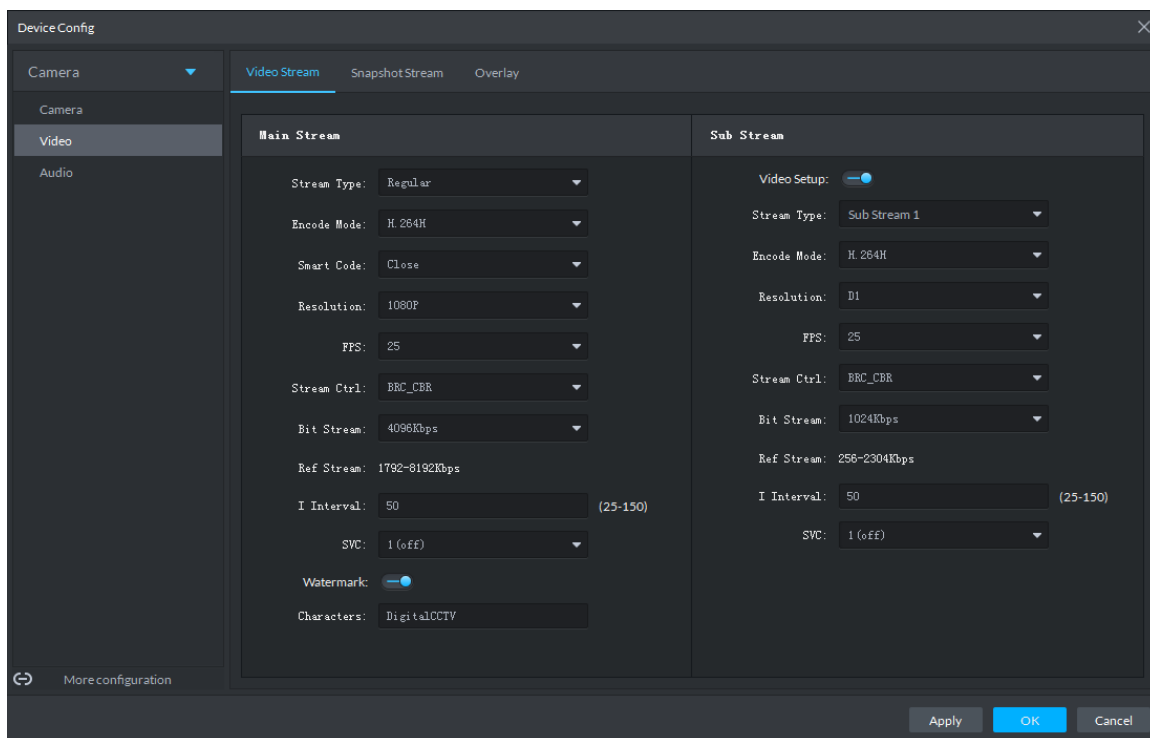
3.4.4.2.1 Video Stream

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**.

The **Video Stream** interface is displayed. See Figure 3-97.

Figure 3-97 Video stream



Step 2 To set up Video Stream, see Table 3-23 for the details of various parameters.



NOTE

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

Table 3-23 Video stream parameter description

Parameter	Description
Video Setup	Indicates whether to set up the Sub Stream parameters.
Encode Mode	The following video encoding modes are available: • 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. When Smart Code is on, the device does not support sub stream 2, ROI, IVS event detection. The actual screens shall prevail.
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: • BRC_CBR: The bit stream changes slightly around the preset value. • BRC_VBR: The bit stream changes according to the monitored scenes. When the Encode Mode is set to MJPEG, BRC_CBR remains the only option for stream control.

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.

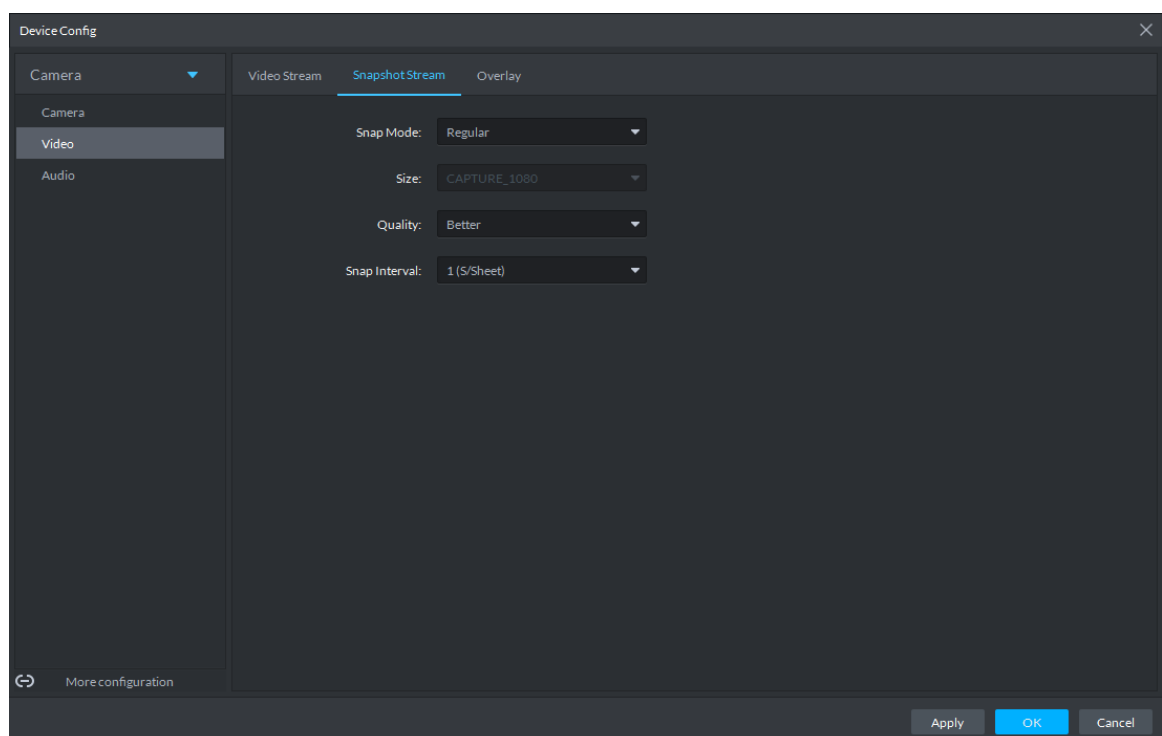
3.4.4.2.2 Snapshot Stream

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**.

The **Snapshot Stream** interface is displayed. See Figure 3-98.

Figure 3-98 Snapshot stream



Step 2 To set up Snapshot Stream, see Table 3-24 for the details of various parameters.

Table 3-24 Snapshot stream parameter description

Parameter	Description
Snap Mode	It includes Regular and Trigger . • 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.

3.4.4.2.3 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**.

The **Overlay** interface is displayed.

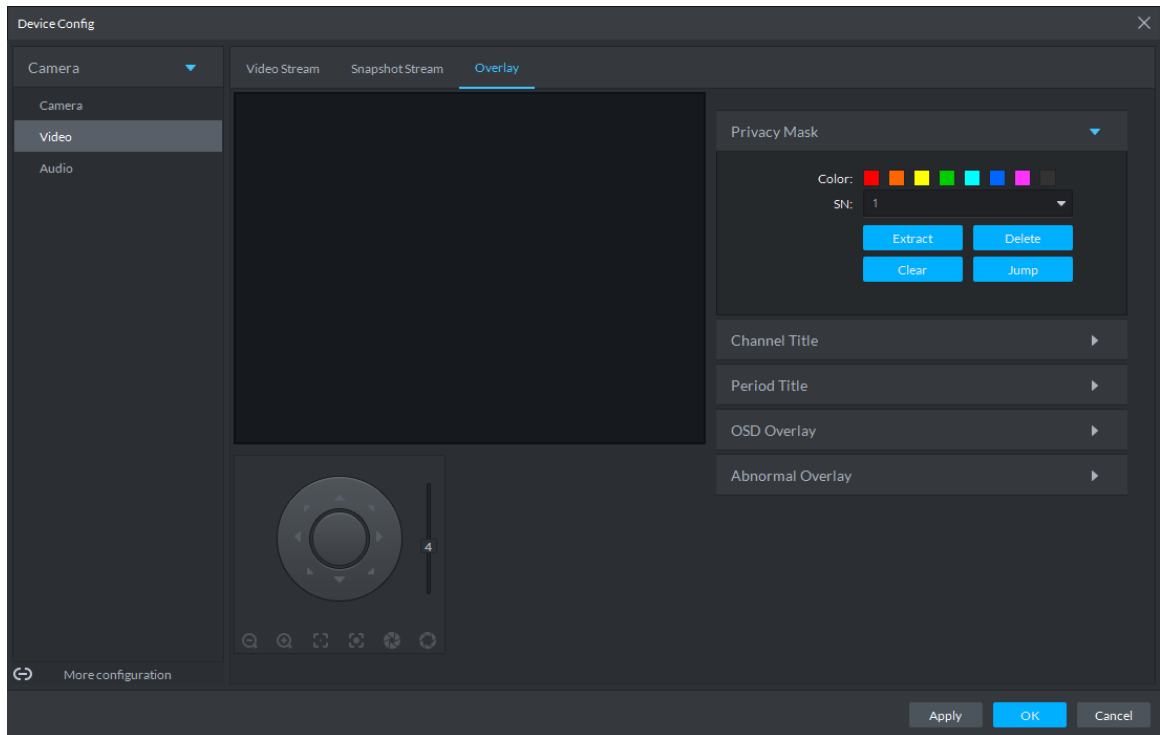
Step 2 (Optional) Set up Privacy Mask.

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

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

The **Privacy Mask** interface is displayed. See Figure 3-99.

Figure 3-99 Privacy mask



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



NOTE

- 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.

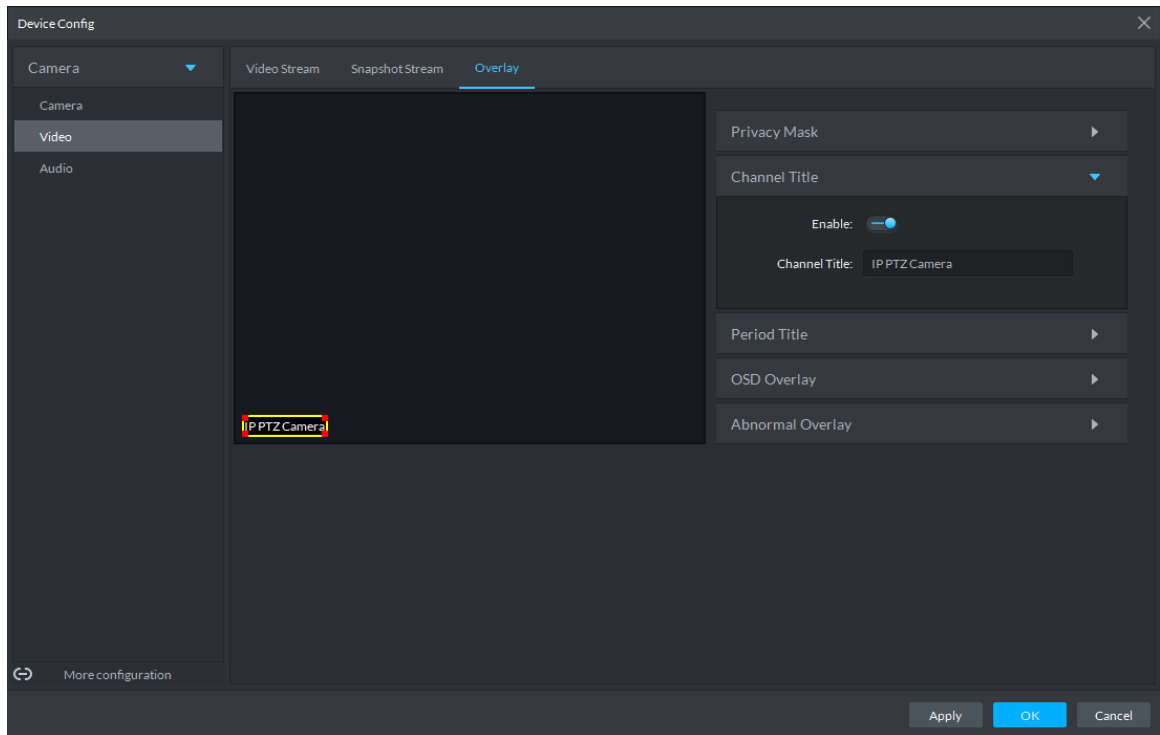
Step 3 (Optional) Set up Channel Title.

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

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

The **Channel Title** interface is displayed. See Figure 3-100.

Figure 3-100 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.

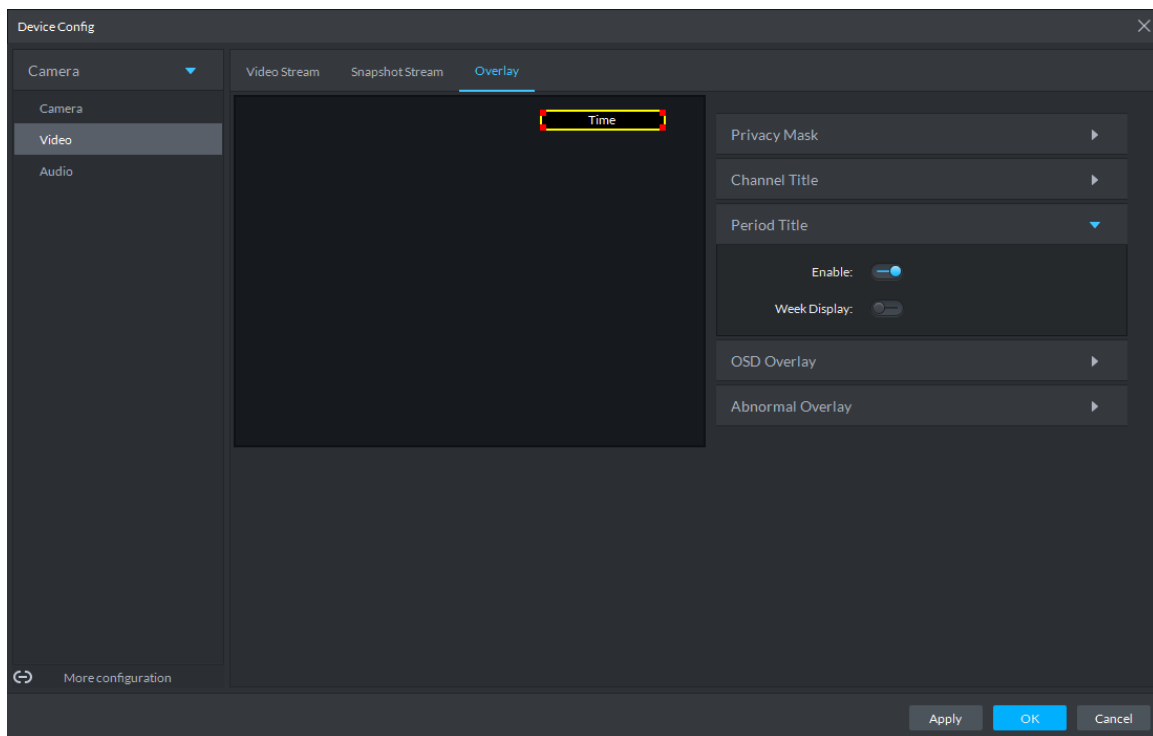
Step 4 (Optional) Set up Period Title.

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

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

The **Period Title** interface is displayed. See Figure 3-101.

Figure 3-101 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.

3.4.4.3 Audio

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

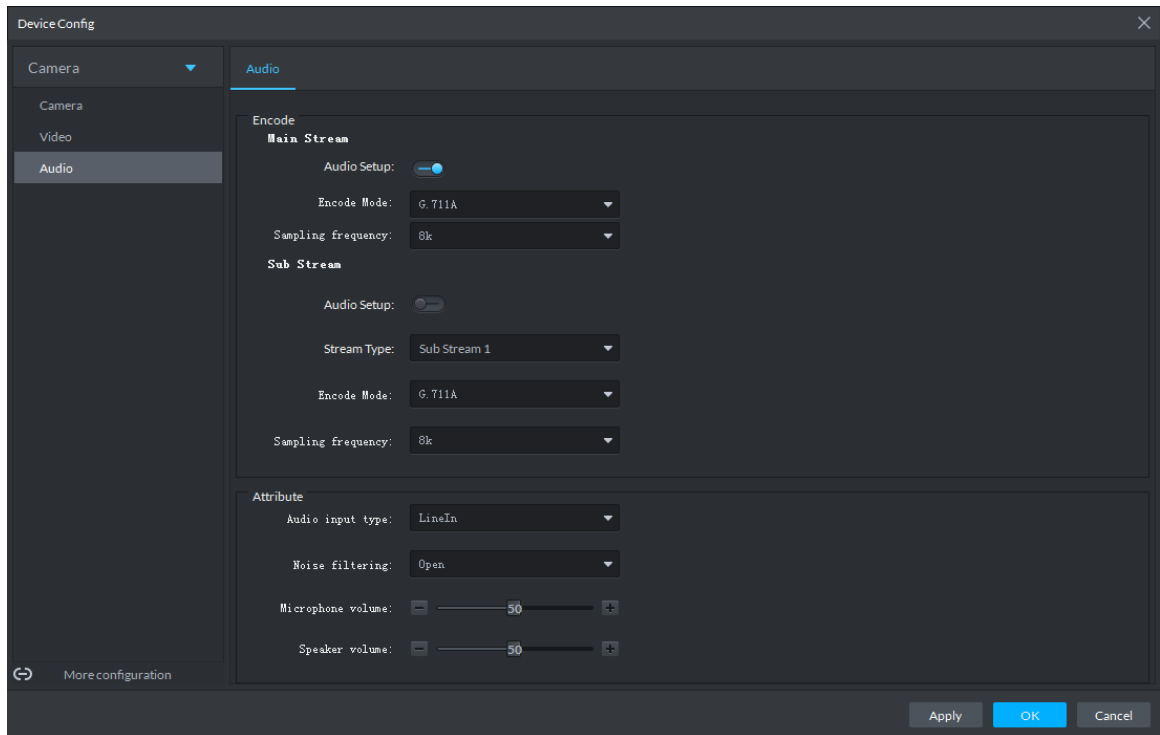


Some devices do not support audio functions.

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

The **Audio** interface is displayed. See Figure 3-102.

Figure 3-102 Audio



Step 2 To set up audio parameters, see Table 3-25 for details.

Table 3-25 Audio parameter description

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: - 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.

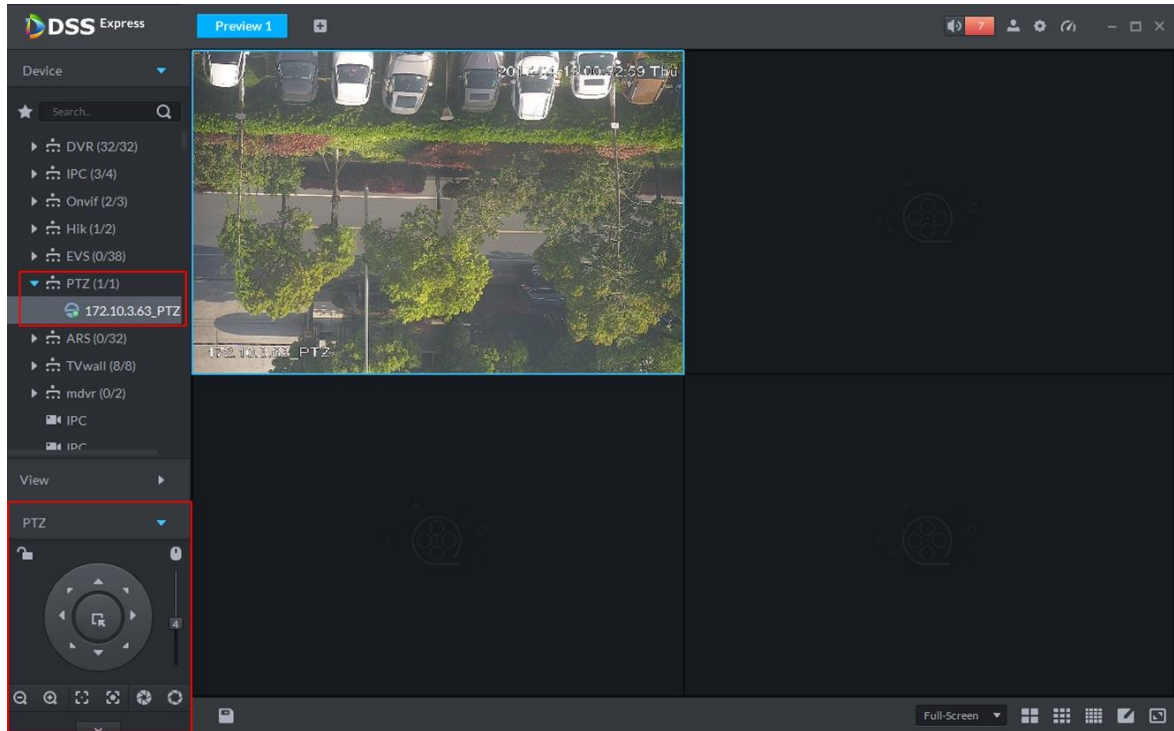
Step 3 Click **OK** to save the configurations.

3.4.5 Setting PTZ

3.4.5.1 PTZ Operation Interface

Step 1 On Preview interface, open video from the PTZ camera, you can see PTZ operation interface on the left. See Figure 3-103.

Figure 3-103 Live view



Step 1 Click  at the bottom of the interface to operate. See Figure 3-104.

Figure 3-104 PTZ

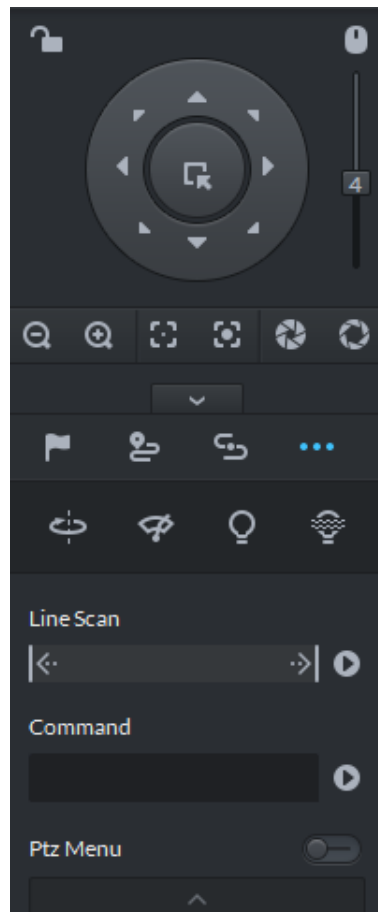
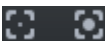


Table 3-26 PTZ operation description

Parameters	Note
	Click  to lock the current PTZ. Locked status shows as . Control over PTZ varies depending on user level. - 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.  Default time for automatically unlocking PTZ is 30s.
	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.

Parameters	Note
	3D Location and Partially Zoom In (for Speed Dome PTZ), to zoom in or zoom out the selected area.  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 3.4.5.2 PTZ Settings for more information.

3.4.5.2 PTZ Settings

3.4.5.2.1 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 SN, and click .

Adding preset point completed.

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

3.4.5.2.2 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.

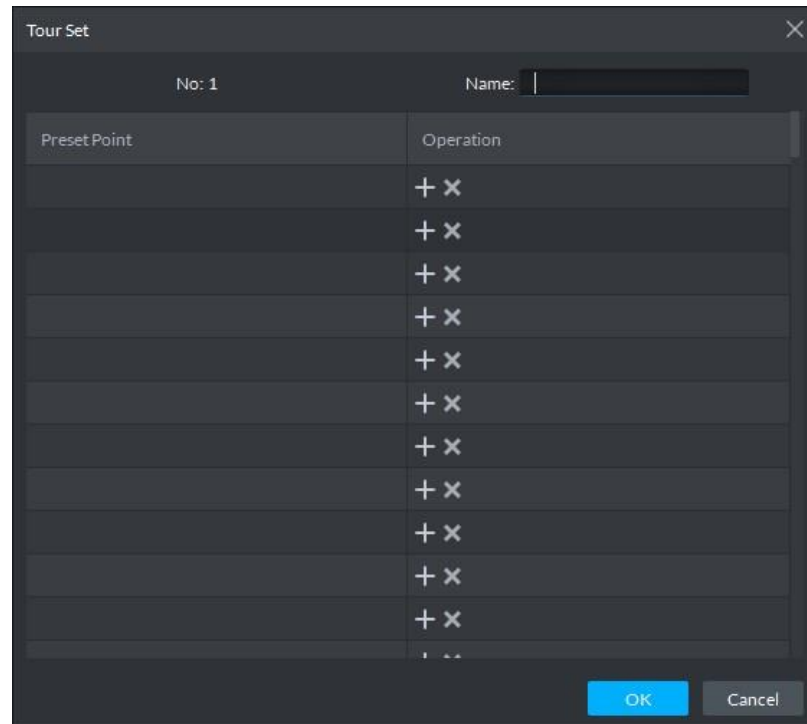
Step 1 Click .

Step 2 Place mouse over 1 and click .
New tour dialogue box pops up.

Step 3 Input name, and click Operation bar .

Choose preset points from the dropdown list on the left. See Figure 3-105.

Figure 3-105 Add preset



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.

3.4.5.2.3 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.

3.4.5.2.4 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.

3.4.5.2.5 Enable/Disable Pan

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

3.4.5.2.6 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.

3.4.5.2.7 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.

3.4.5.2.8 Enable/Disable IR light

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

3.4.5.2.9 Configuring custom commands

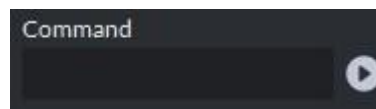
NOTE

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

Step 1 Click .

Step 2 Input command on the customized command interface. See Figure 3-106.

Figure 3-106 Command



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

3.4.5.2.10 PTZ Menu

Step 1 Click .

The PTZ menu is shown as in Figure 3-107.

Figure 3-107 Menu

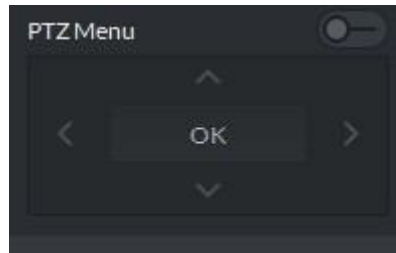


Table 3-27 PTZ menu parameter description

Parameters	Note
	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. • 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**.

The monitor window displays main menu. See Figure 3-108.

Figure 3-108 Display main menu interface

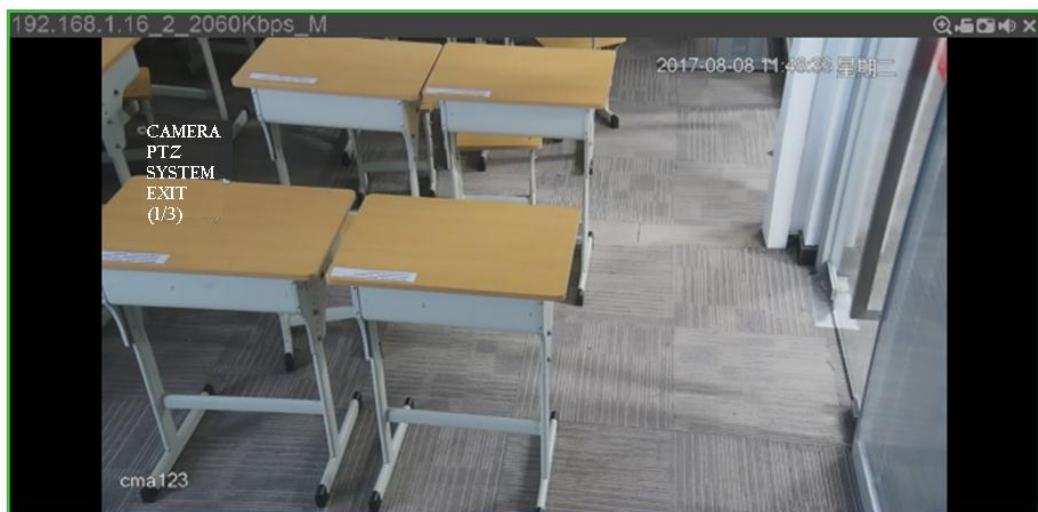


Table 3-28 Main menu parameter description

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

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

3.4.6 Smart Track

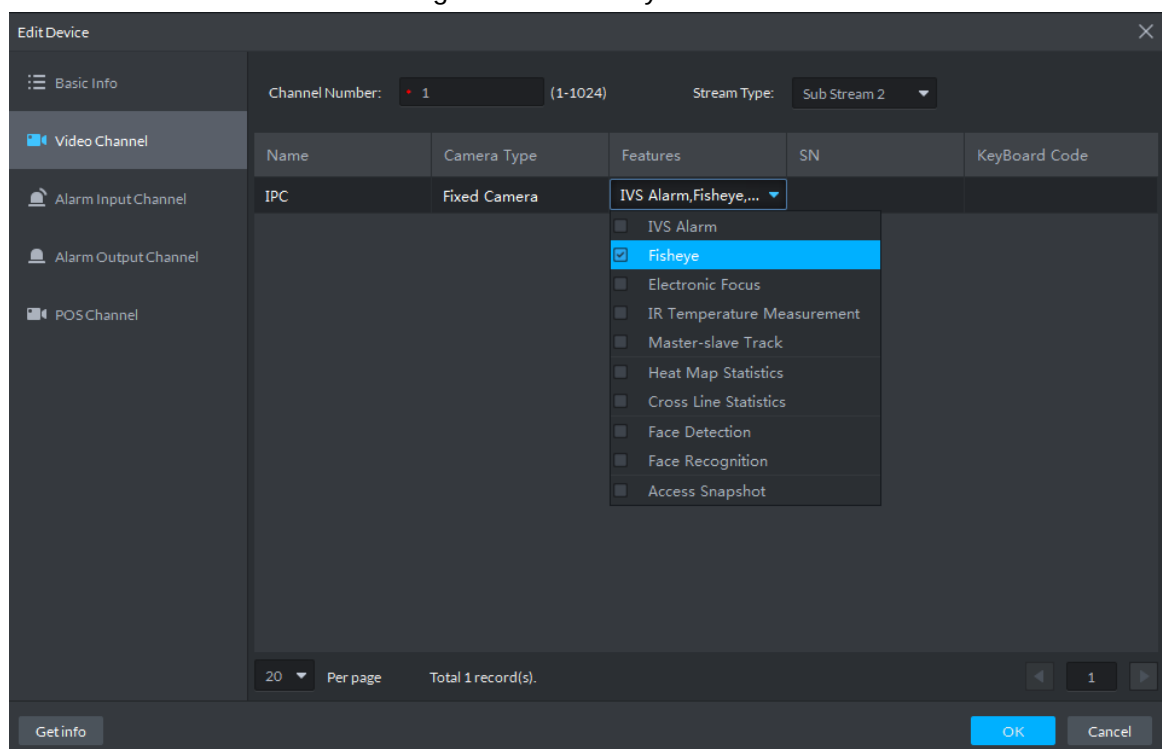
DSS Client supports smart track which links fisheye speed dome to general speed dome to better control each monitoring position.

3.4.6.1 Adding Device

Step 1 Add fisheye and speed dome. For more details, see **3.2.2.4 Adding Device**.

Step 2 On **Device** interface, click  next to the fisheye device, then you can modify the device features as **Fisheye**. See Figure 3-109.

Figure 3-109 Fisheye device



3.4.6.2 Adding Smart Track Config

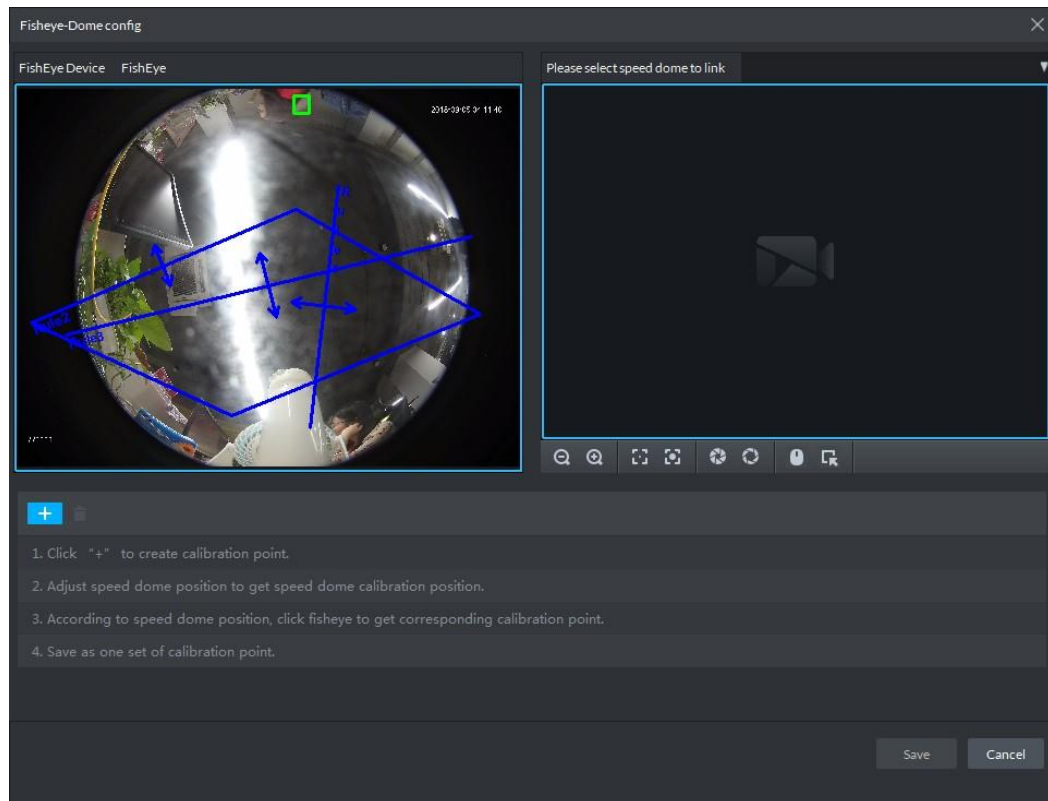
Step 1 Select the fisheye device on the device tree and then right click to select Smart track.



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

The Smart track interface is displayed. See Figure 3-110.

Figure 3-110 Smart track config

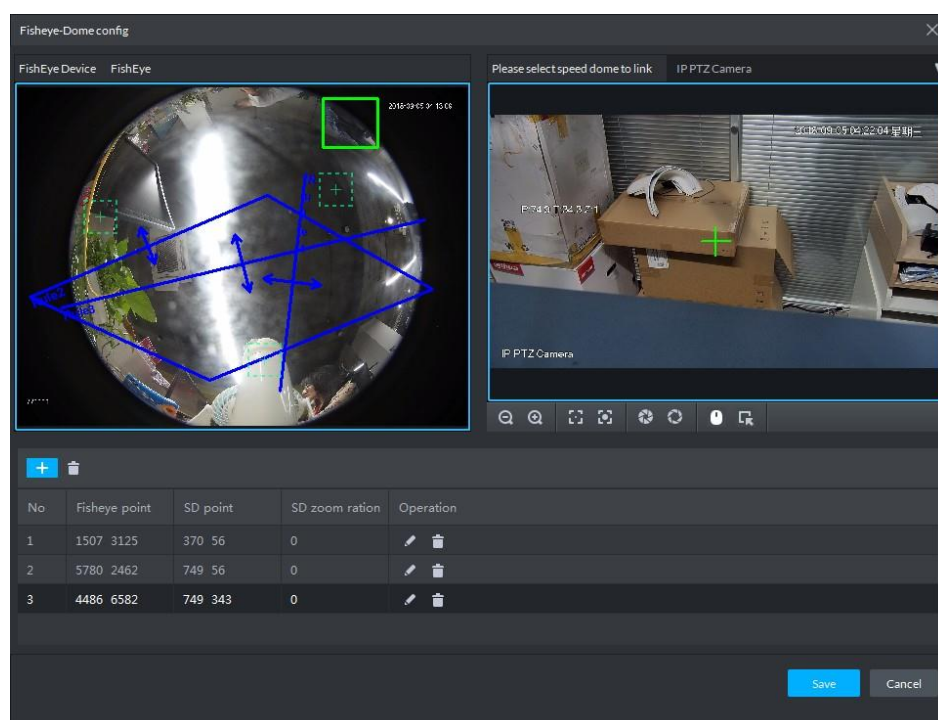


Step 2 Click  after the Select linkage PTZ camera and then select a PTZ camera.

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). See Figure 3-111.

Figure 3-111 Configure calibration point





- 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.

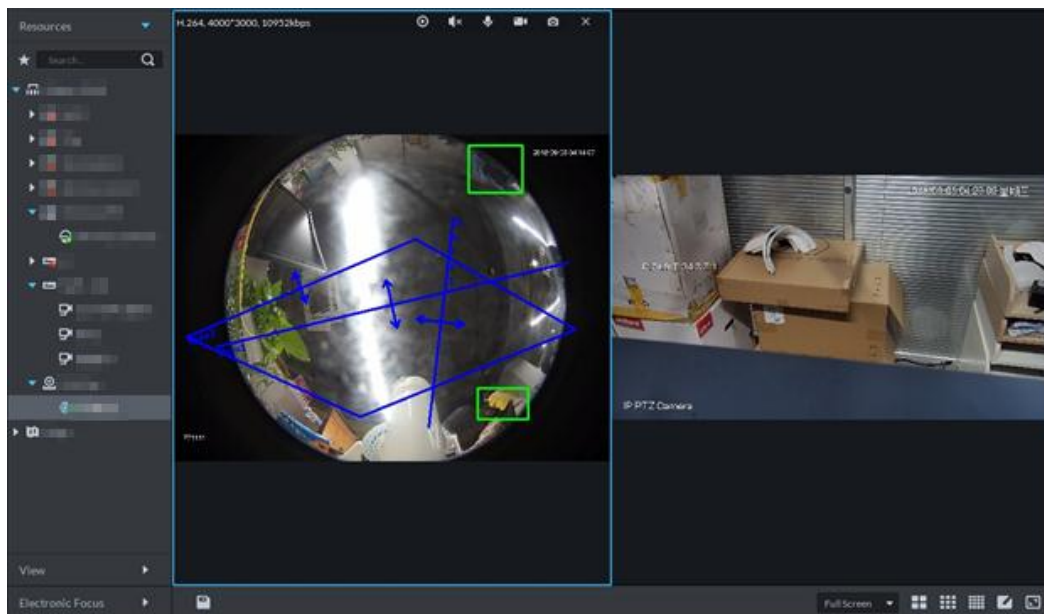
Refer to above steps to add at least three calibration points. These three points shall not be on the same straight line.

Step 5 Click **Save**.

3.4.6.3 Enabling Smark Track Function

Step 1 Select the fisheye device on the device tree and then right click to select **Smart Track**. See Figure 3-112.

Figure 3-112 Smart track



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

3.4.7 Smart Track

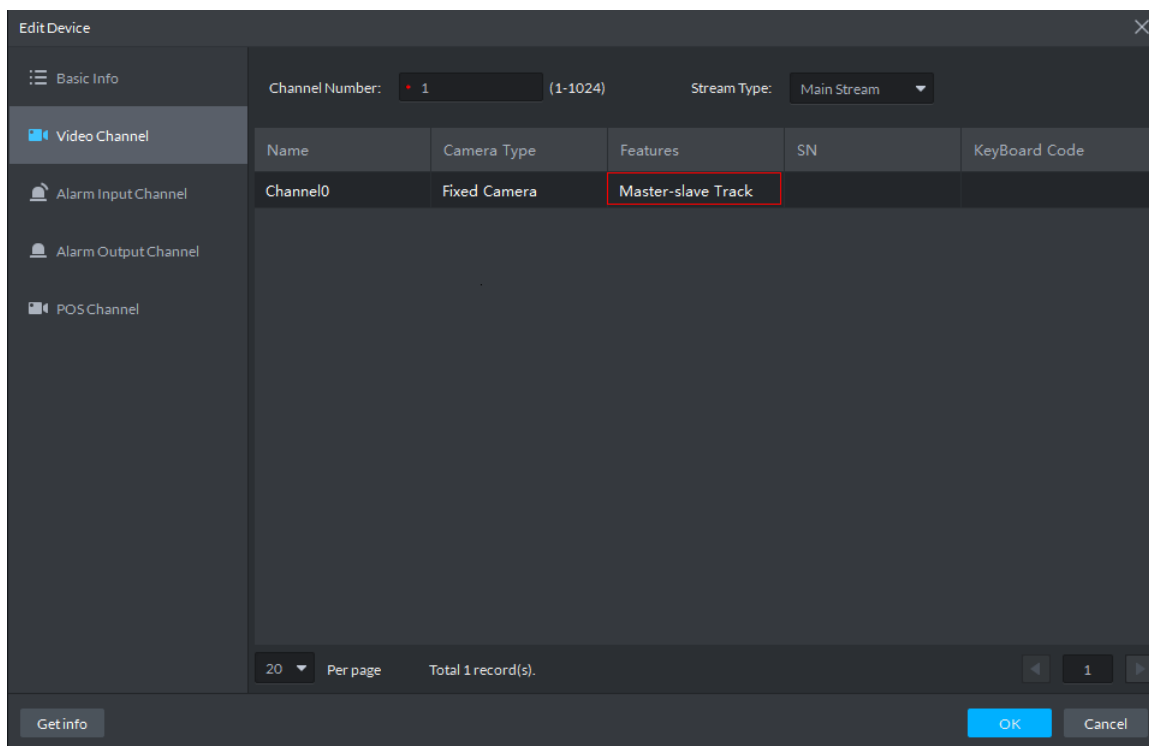
Support smart track which links bullet with PTZ camera, and it is good for panoramic monitoring and details tracking. Currently smart track supports bullet PTZ all-in-one camera and panoramic+PTZ camera etc. Besides, it also supports individual bullet and PTZ camera which have been bound and calibrated.

3.4.7.1 Preparations

- 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 **3.2.2.4 Adding Device**

- Click  after adding bullet, and select **Master Slave Track**. Tracking function can be realized after configuring master slave track.

Figure 3-113 Master slave track



- 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.

3.4.7.2 Applying Smart Track

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

3.4.7.2.1 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. See Figure 3-114. Click the red spot on the bullet image, and the PTZ central point will move to the corresponding location automatically.

Figure 3-114 Manual positioning



3.4.7.2.2 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. See Figure 3-115.
- Draw rectangular box from lower right to upper left; zoom out after being positioned by PTZ camera. See Figure 3-116.

Figure 3-115 3D positioning (Zoom in after positioning)



Figure 3-116 3D positioning (Zoom out after positioning)



3.4.7.2.3 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 3-117 Manual track



3.4.7.2.4 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. See Figure 3-118 and Figure 3-119.

Figure 3-118 Auto track

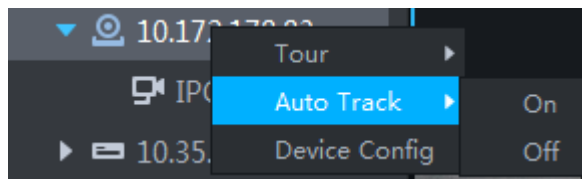


Figure 3-119 Auto track



3.4.7.2.5 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.

3.4.8 View

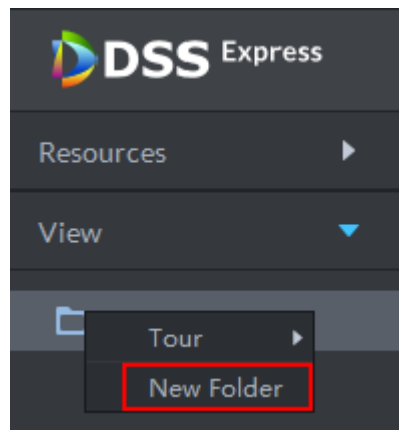
3.4.8.1 Creating View

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

Step 1 Create groupd.

- 1) Click **View** tab on the **Live View** interface.
- 2) Right click **View**, select **New Folder**, and see Figure 3-120.
The system displays **New Folder** interface.

Figure 3-120 New folder

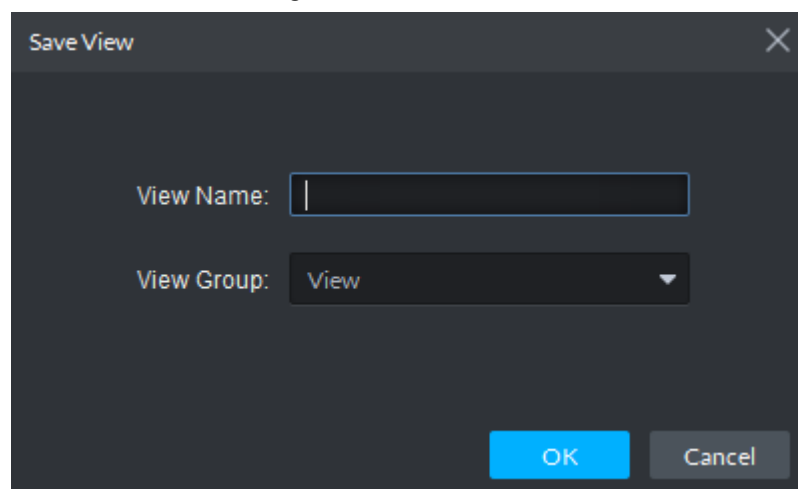


- 3) Enter folder name, click **OK**.
All new groups are displayed under view.

Step 2 Create view.

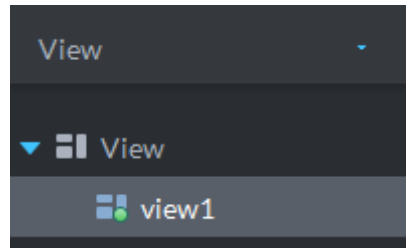
- 1) On **Live View** interface, click  according to your needs.
The system displays Save View interface, see Figure 3-121.

Figure 3-121 Save view



- 2) Enter **View Name**, select **View Group** and click **OK**.
New view is created under view group, see Figure 3-122.

Figure 3-122 Generate view



3.4.8.2 Previewing View

- Live view

Select view from the list on **Live View** interface, double click or drag to video window, the system starts to preview.

- Tour

On Live View interface, right click view group or root node, select Tour and tour period, see Figure 3-123. The system tours according to view group or root node; see Figure 3-124.

Click  to stop tour.

Figure 3-123 Entering video tour interface

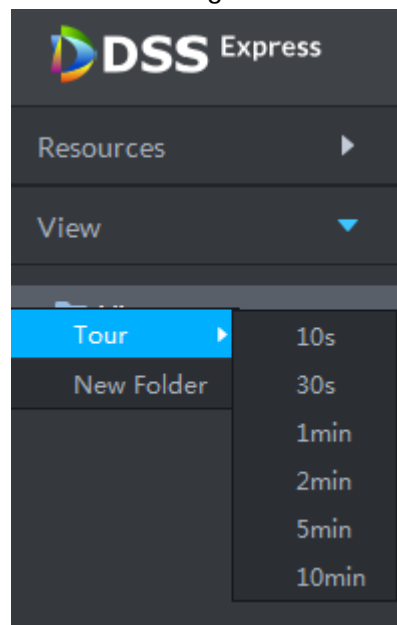
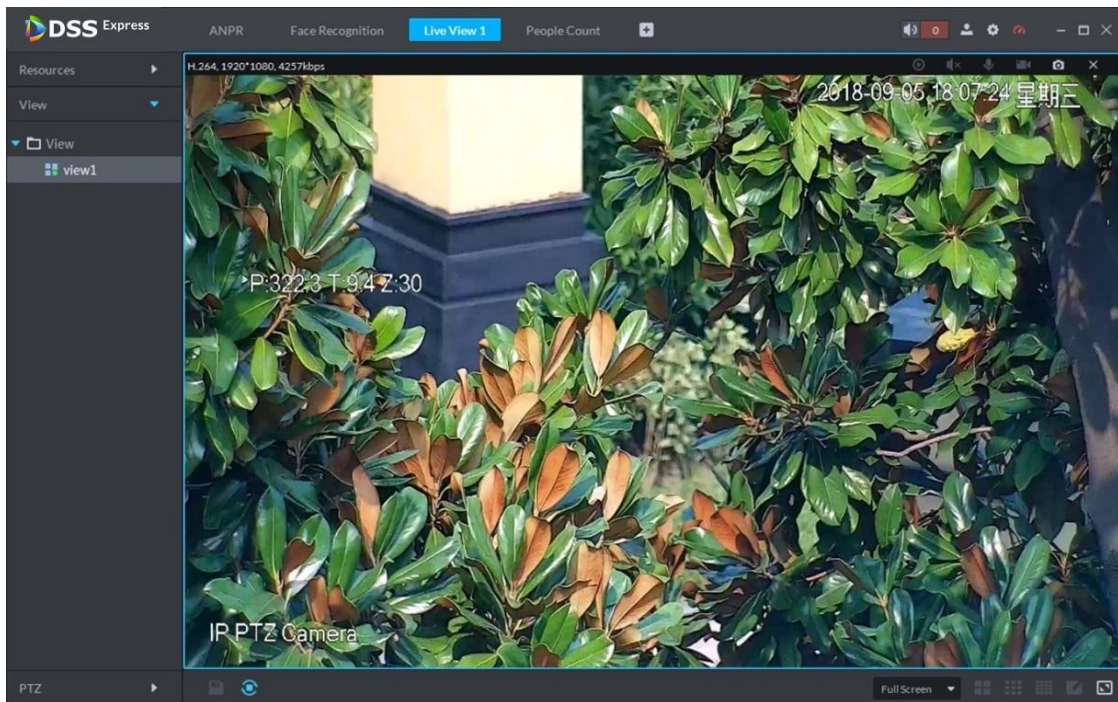


Figure 3-124 View tour



3.4.9 Favorites

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

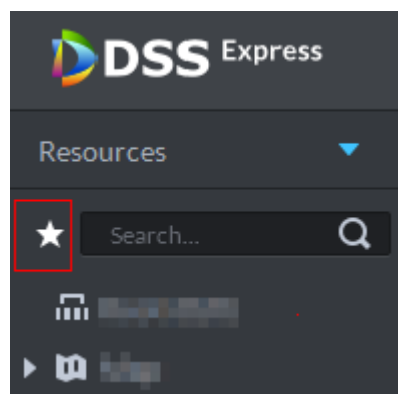
3.4.9.1 Creating Favorites

Step 1 Create favorites.

- 1) On **Live View** interface, click , see Figure 3-125.

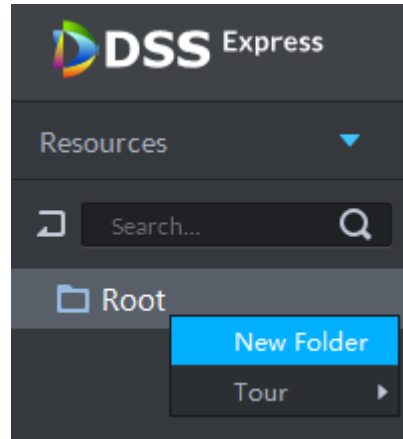
The system displays favorites list.

Figure 3-125 Enter favorites list



- 2) Right click root node or created favorites, select **New Folder**, see Figure 3-126. The system displays **Create Folder** interface.

Figure 3-126 Favorites list



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

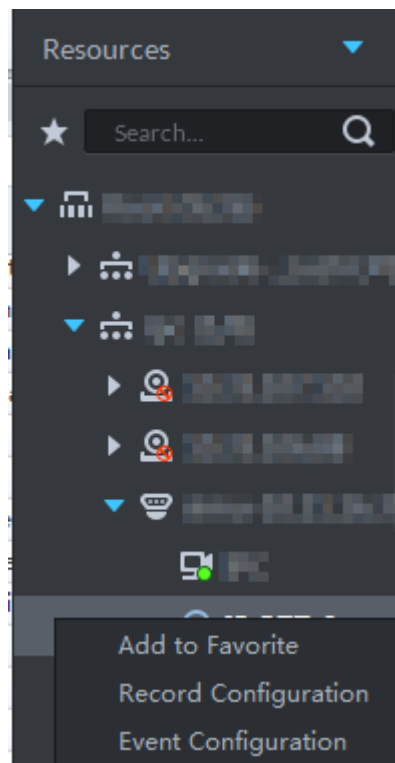
- 4) Click .

The system returns to device list.

Step 2 Favorite channel.

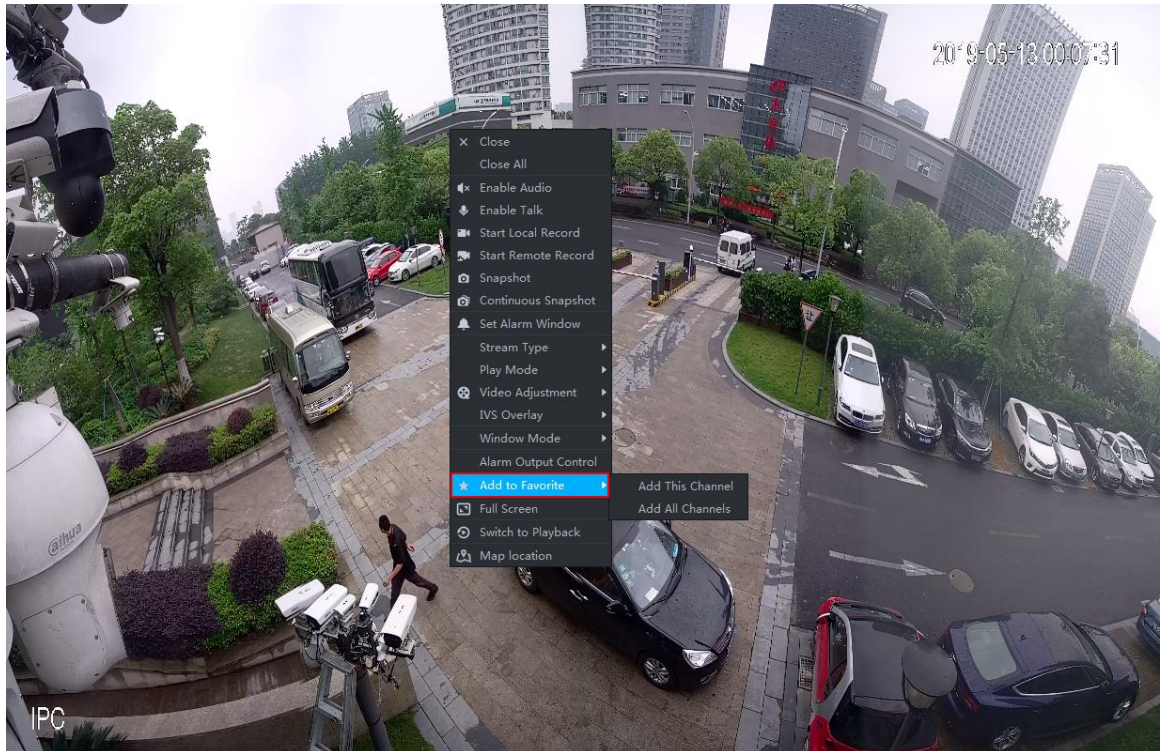
- In the device list on **Live View** interface, right click channel, select **Add to Favorites**, and add the channel to favorite according to system prompt. See Figure 3-127.

Figure 3-127 Favorite channel (1)



- On **Live View** interface, right click the window with live view, and select **Add to favorite**, add it to favorite according to system prompt, see Figure 3-128.

Figure 3-128 Favorite channel (2)



3.4.9.2 Viewing Favorites

- Live view

On **Live View** interface, click , open favorite list, select favorite or channel, double click or drag to video window and the system starts to preview.

- Tour

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

Click  to stop tour.

3.4.10 Region of Interest (RoI)

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

On **Live View** interface, right click the window under live view, select **Split Mode**, and see Figure 3-129. The system displays split image. For example, select 1+3 mode. See Figure 3-130.

Figure 3-129 Split mode

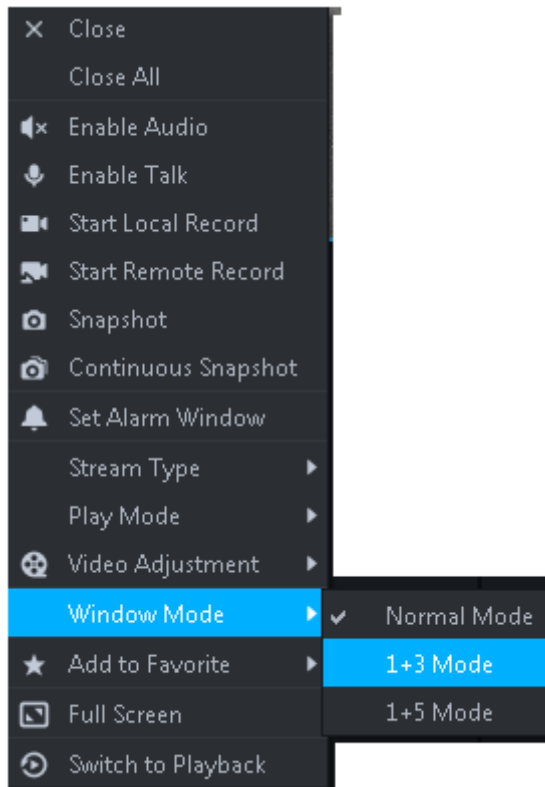
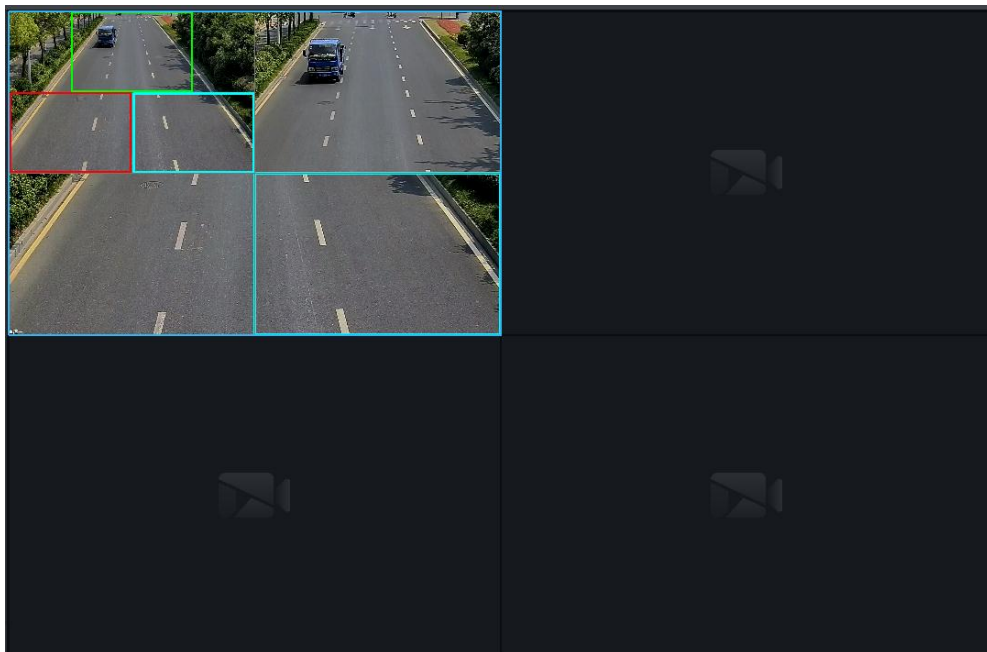


Figure 3-130 1+3 mode



3.5 Record

View videos recorded on device or server, you can download video and save to local.

3.5.1 Record Playback



If neither device nor platform is configured with record plan, then you can search no video. If you want to configure platform record plan, refer to **3.2.5 Setting Record Plan** for more details.

3.5.1.1 Entering Record Playback Interface

On client homepage, click **Record Playback**. The system displays **Record Playback** interface, See Figure 3-131. For interface description, see Table 3-29.

Figure 3-131

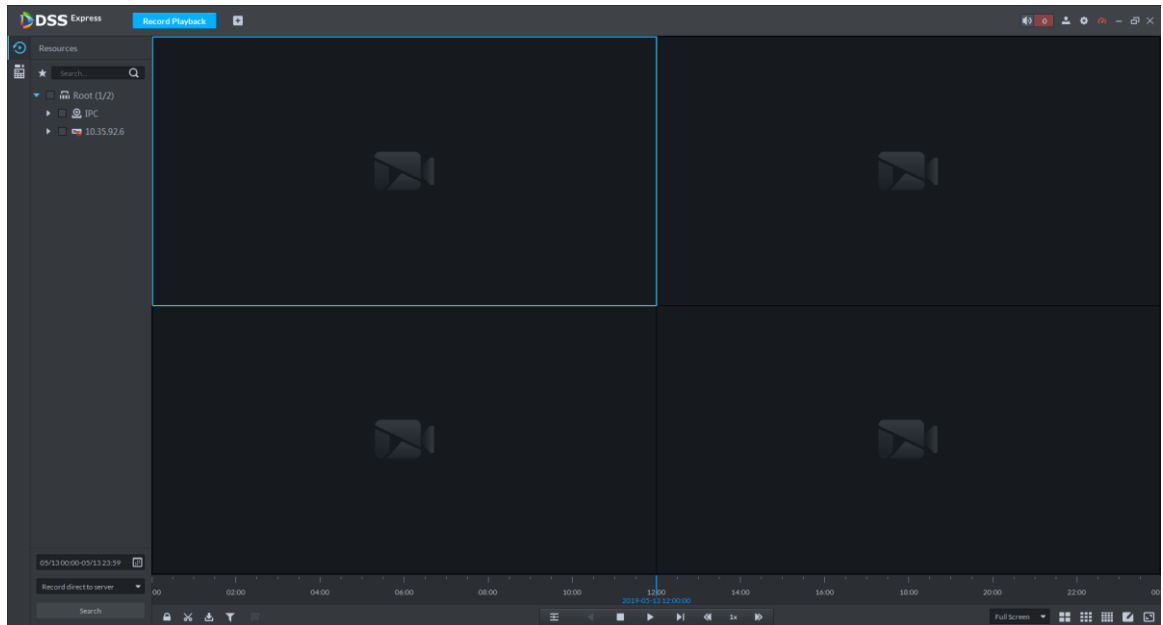


Table 3-29 Record playback icon description

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.

3.5.1.2 Playback Video

Step 1 In the device tree on **Record Playback** interface, select channel, time and record storage position, click **Search**.

When selecting time, the date with blue spot means record file exists on this date.

Step 2 Select window with video, click .

The corresponding window plays video of the channel, see Figure 3-132. For operation description, see Table 3-30.

Figure 3-132 Playback video

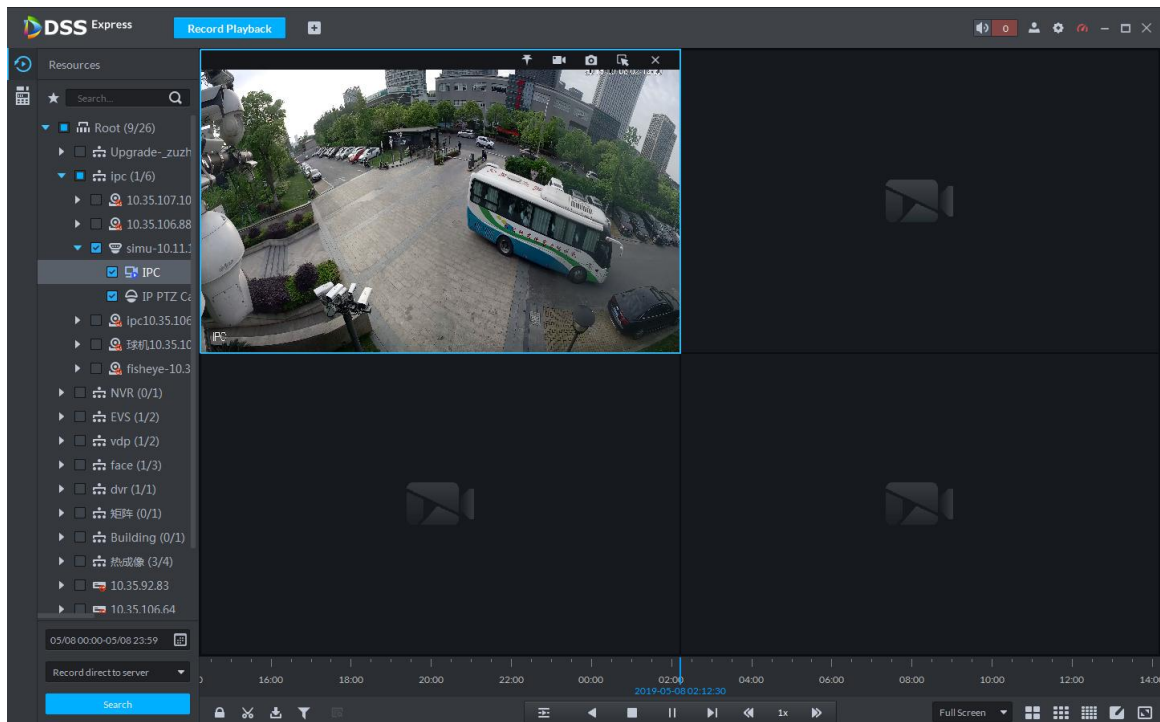


Table 3-30 Shortcut menu description

Icon	Icon Name	Description
	Record Tagging	Mark the record if you are interested in, convenient for future search. For detailed operations, see 3.5.1.4 Tagging Record
	Local Record	Click the icon and system begins to record audio and video of current video window, recording duration is displayed on the upper left corner of the window; click the icon again, stop record and store to local PC. The default save path is "C:\DSS Express\Client\Record\". If you want to modify save path, refer to 3.3.5 Setting Recording Parameter .
	Snapshot	Save the image in the form of snapshot (one snapshot for once). Default save path is "C:\DSS Express\Client\Picture\". If you need to modify save path, refer to 3.3.4 Setting Snapshot .
	Zoom in	Select and zoom in regionally, you can scroll the mouse to zoom in or out.
	Close	Click the icon to close video.

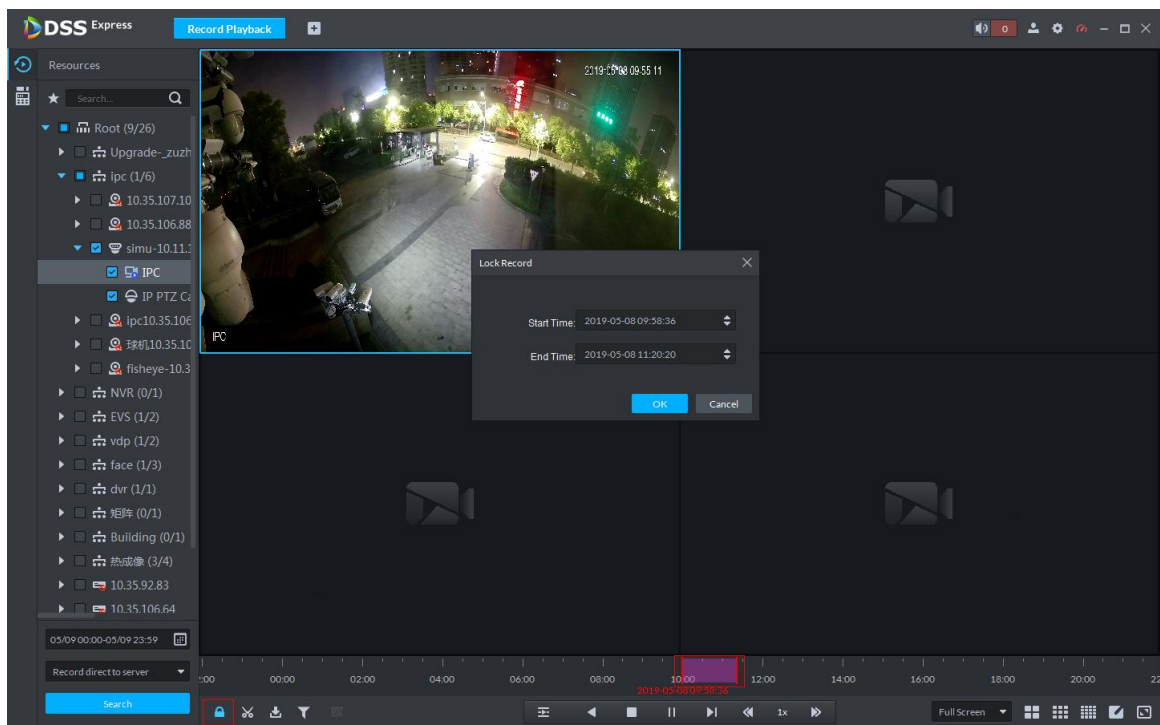
3.5.1.3 Locking Record

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

Step 1 On **Record Playback** interface, set search condition and search videos.

Step 2 Click  at the bottom of the **Record Playback** interface (make sure the window has the record). The system pops out **Lock Record** interface. See Figure 3-133.

Figure 3-133 Select lock time



Step 3 Confirm time, click **OK**.

3.5.1.4 Tagging Record

Tag the video that you are interested in, convenient for future search.

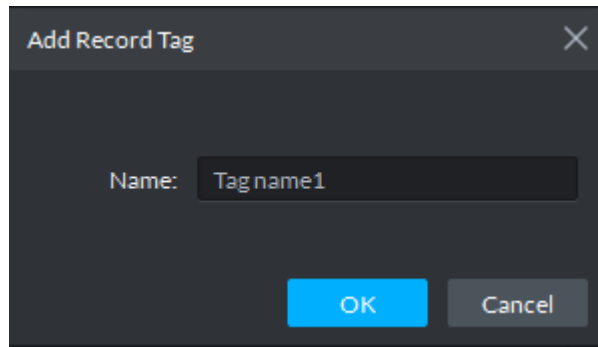
Step 1 On Record Playback interface, set search condition and search video.

Step 2 Select video, click  and play video.

Step 3 Move the mouse to the window with video, click  on top of the window.

The system pops out Add Record Tag interface. See Add record tag.

Figure 3-134 Add record tag



Step 4 Enter **Name**, click **OK**.

3.5.1.5 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 . See Figure 3-135.

The system displays the interface of **Record Type Filter**. See Figure 3-136.

Figure 3-135 Record type filter

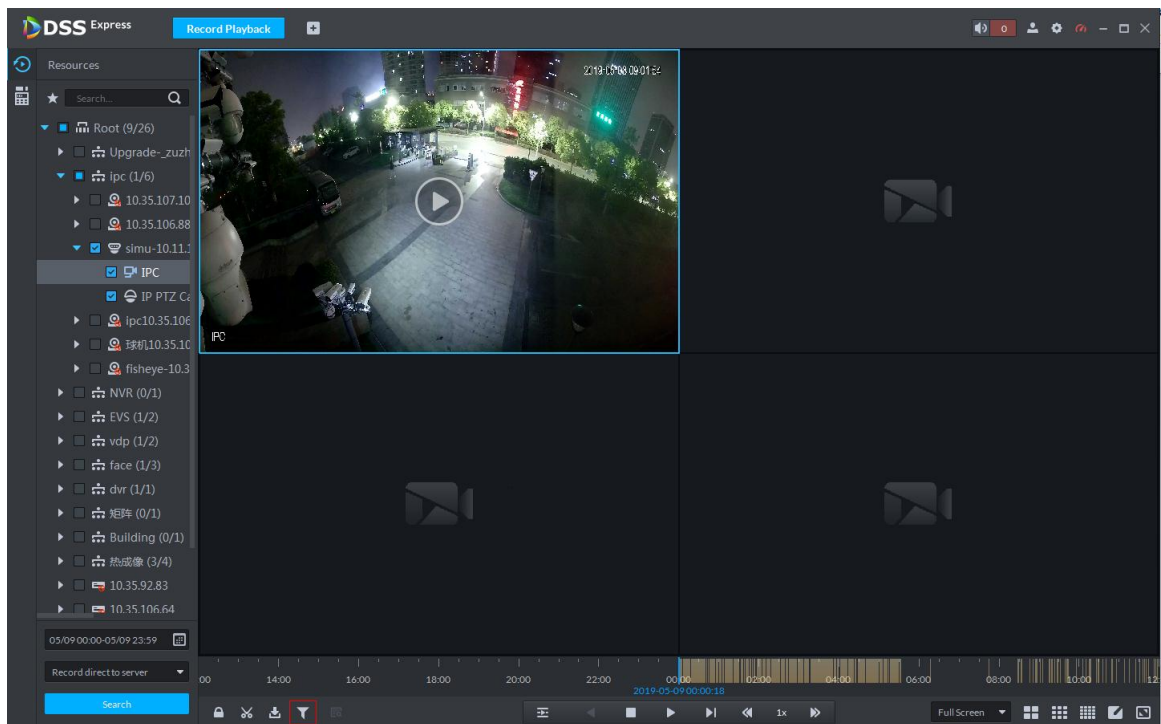
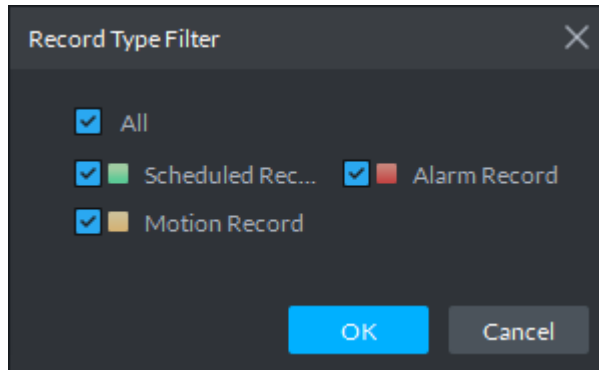


Figure 3-136 Record filter



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

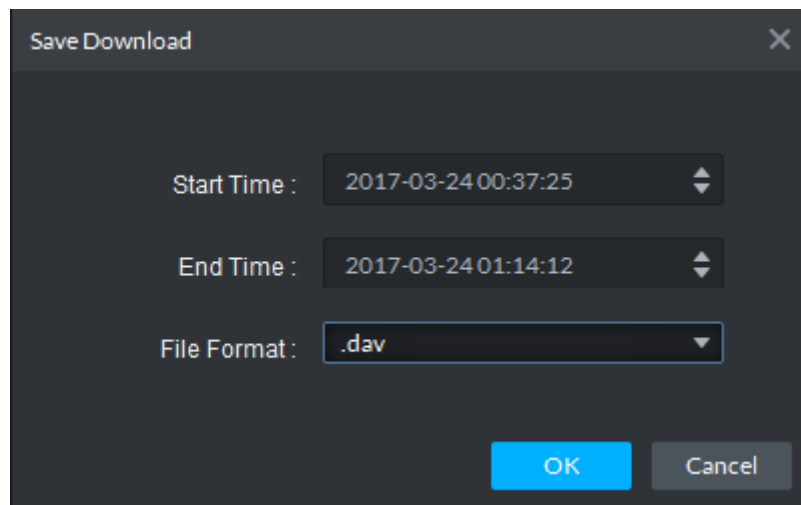
3.5.1.6 Clip Record

Step 1 On **Record Playback** interface, set search condition and search videos.

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

Step 3 During the timeline, click to start clip and then drag the mouse, click to stop clip.
The **Save Download** interface is displayed. See Figure 3-137.

Figure 3-137 Save download



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

3.5.1.7 Smart Search

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

Step 1 Click  on the interface of **Record Playback**. See Figure 3-138.

The system displays the interface of Smart Search. See Figure 3-139. 22×18 squares are displayed in the window.

Figure 3-138 Enable smart search

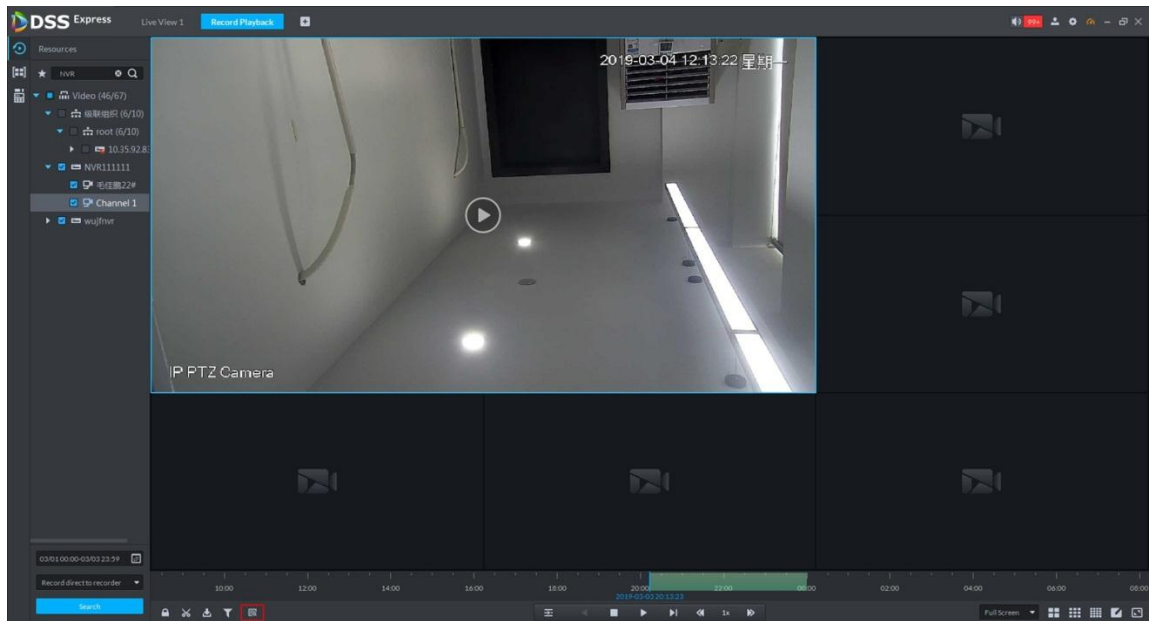
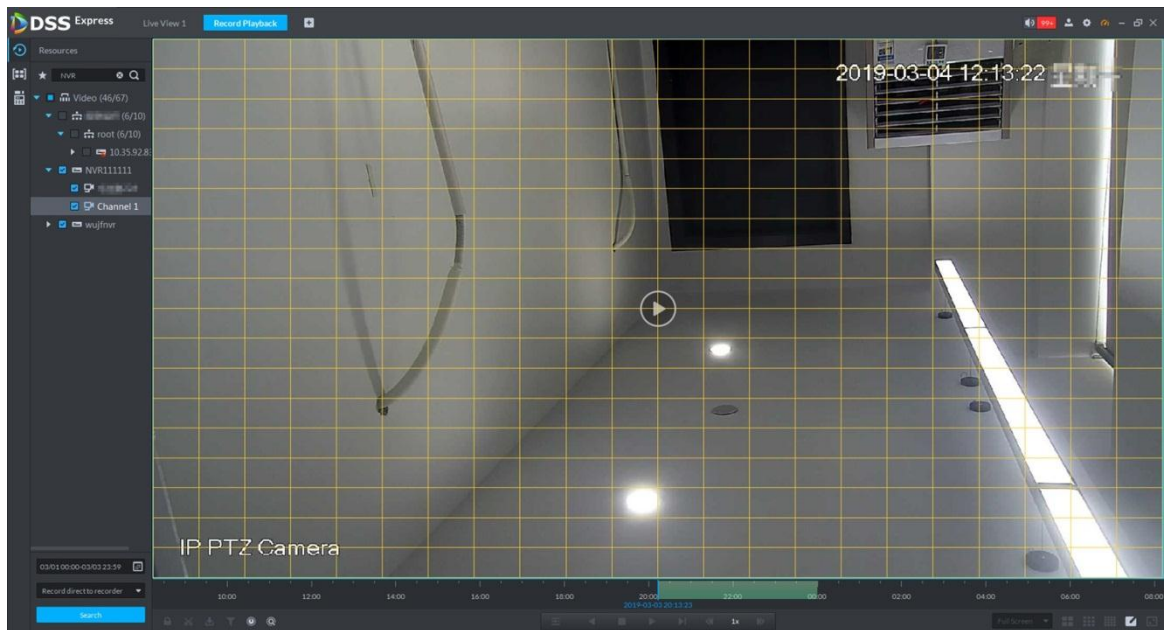


Figure 3-139 Smart search



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.

3.5.1.8 Downloading Record

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

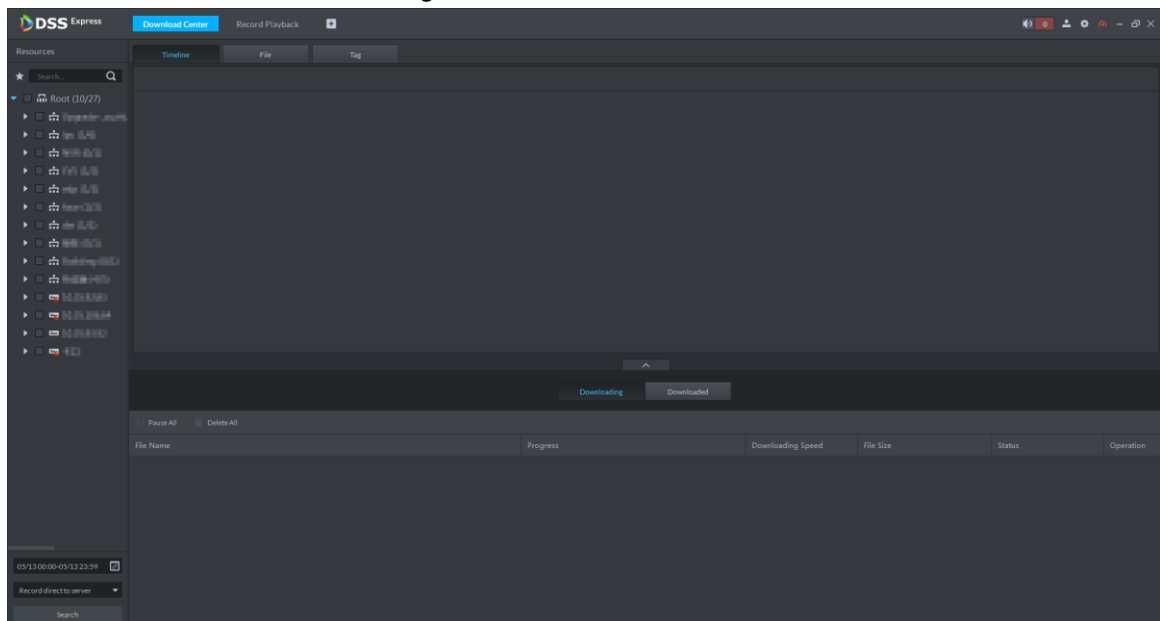
3.5.1.8.1 Timeline

Download video of some period for record file.

Step 1 On **Record Playback** interface, click , or click **Download Center** on the client homepage.

The system displays **Download Center** interface, see Figure 3-140.

Figure 3-140 Download center



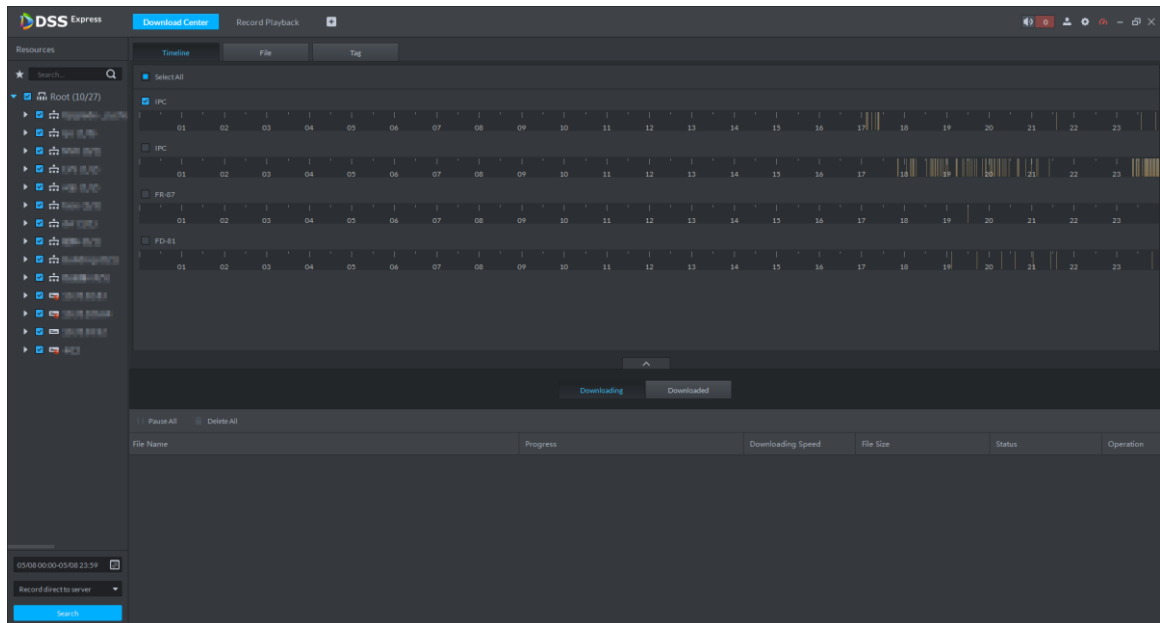
Step 2 Set search condition, click **Search**.

The system displays search results.

Step 3 Click **Timeline** tab.

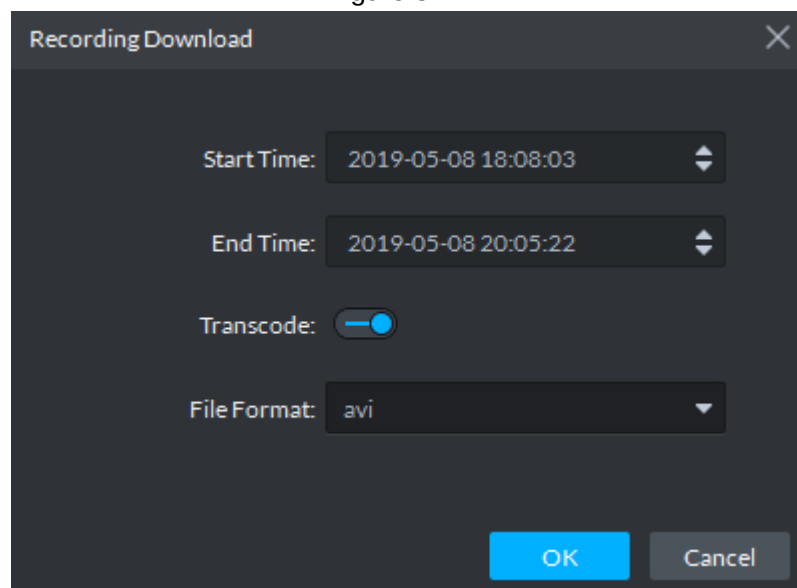
The system displays search results in the form of timeline, see Figure 3-141.

Figure 3-141 Record search result



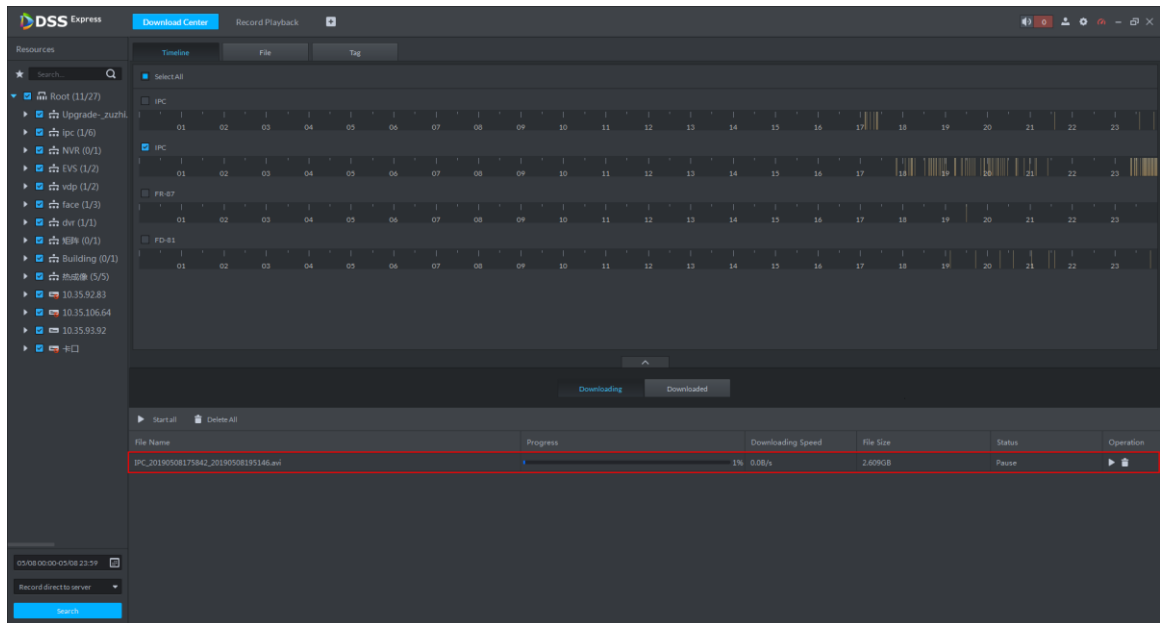
- Step 4** Move the mouse to timeline, select start time and end time.
The system displays **Recording Download** interface, see Figure 3-142.

Figure 3-142



- Step 5** Confirm recording time, select file format, including dav, avi, mp4, flv and asf. Click **OK**.
The system displays download progress, see Figure 3-143. You can pause, start and delete downloaded recording. A prompt task will pop out in the lower right corner of client. The downloaded tasks are displayed on the **Downloaded** interface.

Figure 3-143 Download progress



3.5.1.8.2 File

Within search period, the system automatically generates a record file after half an hour.



If hour or half an hour exists within search time, then the first file list starts from record time to the first hour or half an hour. For example, if video starts from 4:15, then the time of first record file is 4:15-4:30.

Step 1 On **Record Playback** interface, click , or click **Download Center** on the client homepage.

The system displays **Download Center** interface.

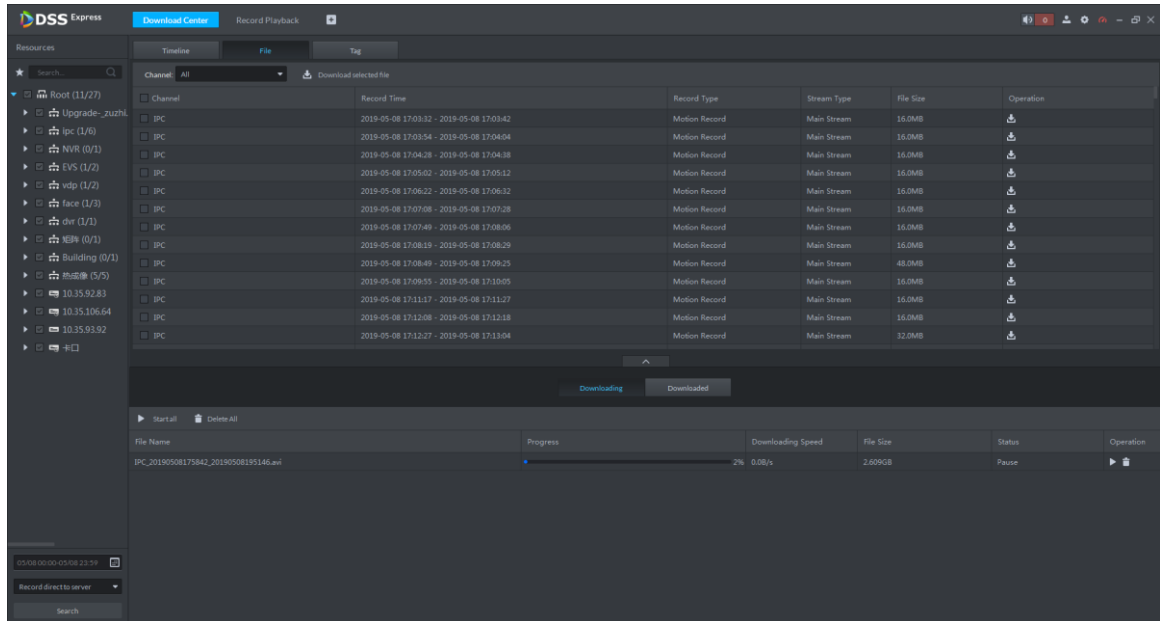
Step 2 Set search condition, click **Search**.

The system displays search result.

Step 3 Click **File** tab.

The system displays searched result in the form of file list, see Figure 3-144.

Figure 3-144 Record search result



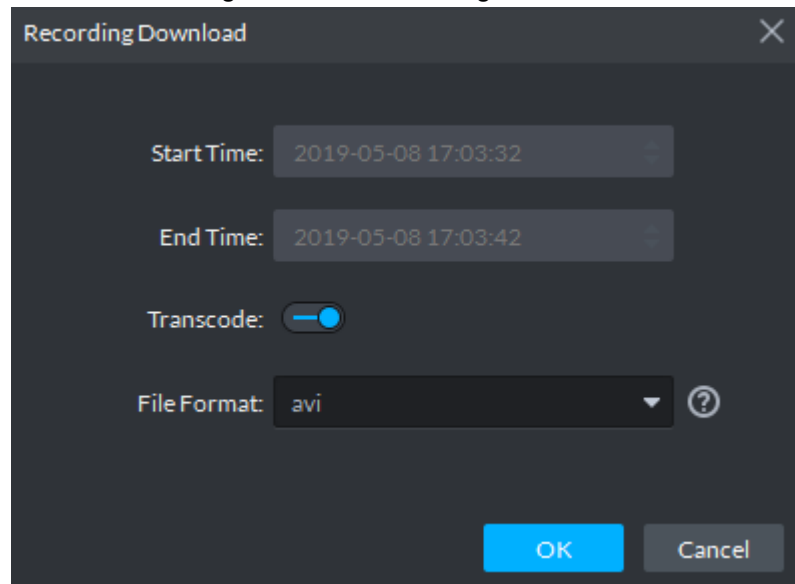
Step 4 Click  in the back of file list.

The system displays **Recording Download** interface, see Figure 3-145.



Select several file lists, click  on top of the interface, then you can download in batched and saved in .dav by default.

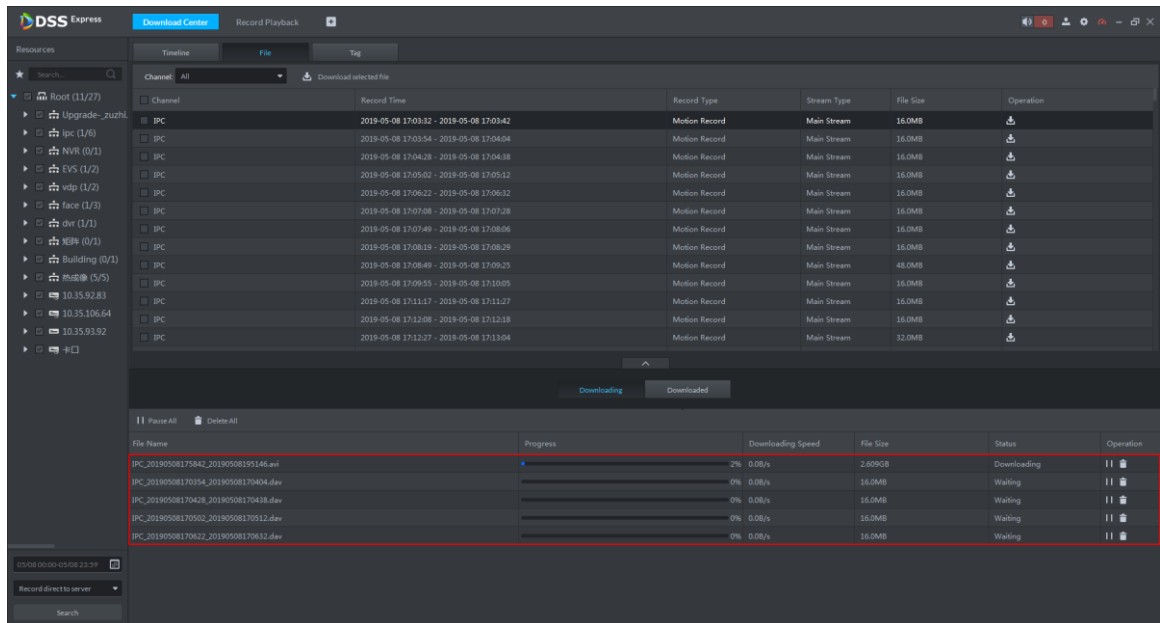
Figure 3-145 Recording download



Step 5 Select file format, including dav, avi, mp4, flv and asf, click **OK**.

The system displays download progress, see Figure 3-146. You can pause, start and delete downloaded recording. A prompt task will pop out in the lower right corner of client. The downloaded tasks are displayed on the **Downloaded** interface.

Figure 3-146 Download progress

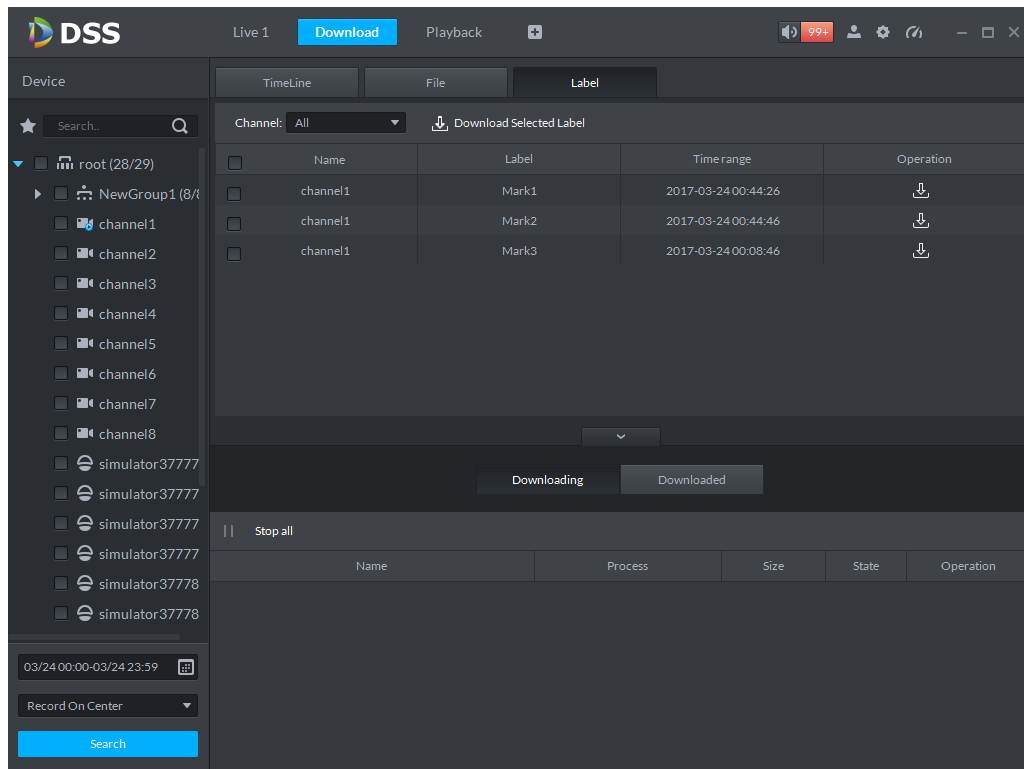


3.5.1.8.3 Tag

If record is tagged, then the system supports downloading video within some period before and after tag time.

- Step 1** On **Record Playback** interface, click , or click **Download Center** on client homepage.
The system displays **Download Center** interface.
- Step 2** Set search condition, click **Search**.
The system displays searched results.
- Step 3** Click **Tag** tab.
The system displays tag file result, see Figure 3-147.

Figure 3-147 Record search result



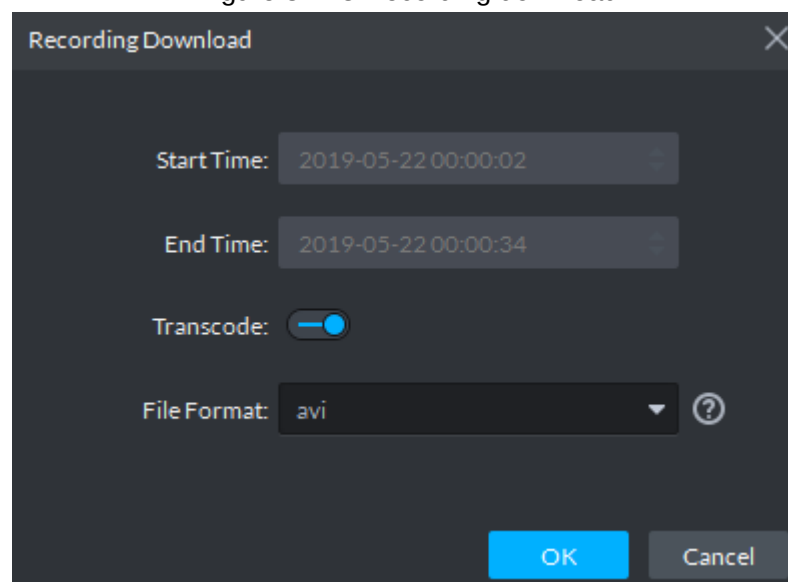
Step 4 Click  in the back of tag list.

The system displays Recording Download interface, see Figure 3-148.



Select several file lists, click  on top of interface, supports download in batches.

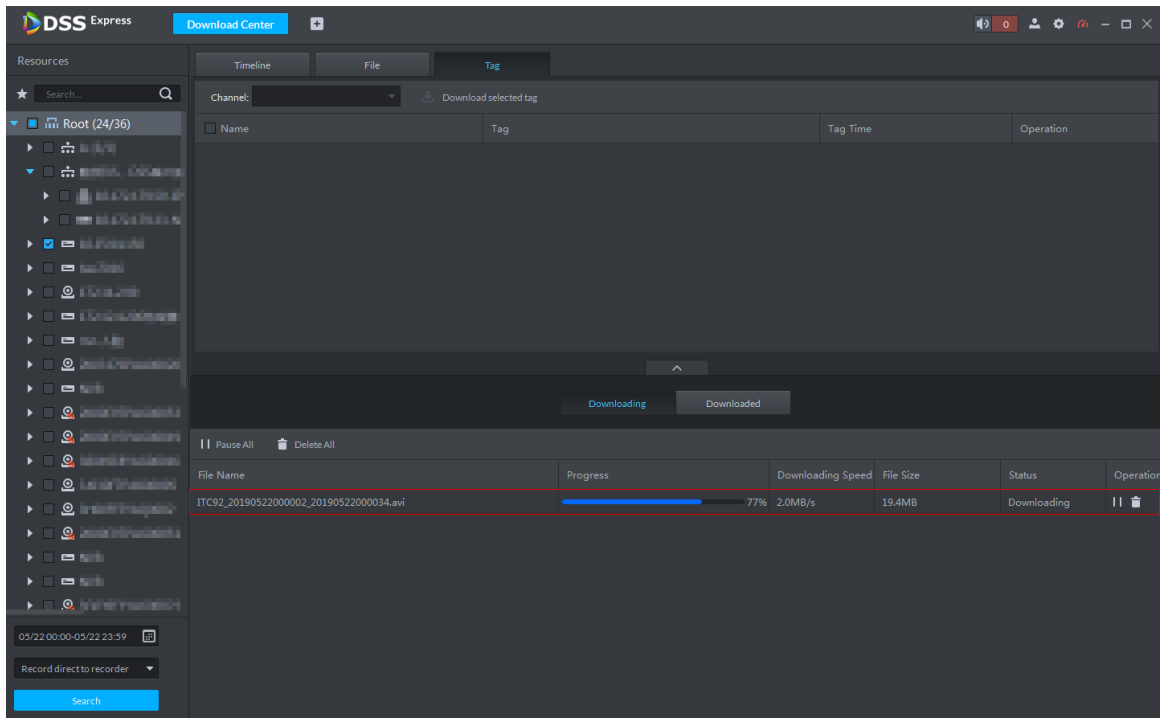
Figure 3-148 Recording download



Step 5 Select file format, including dav, avi, mp4, flv and asf, click **OK**.

The system displays download progress, see Figure 3-146. You can pause, start and delete downloaded recording. A prompt task will pop out in the lower right corner of client. The downloaded tasks are displayed on the **Downloaded** interface.

Figure 3-149 Download progress



3.5.2 POS Record Playback

Search POS receipt, check related video record. Search the video half an hour before and half an hour after POS receipt is printed, play the video 30s before the receipt is printed. For more details, refer to **3.8 POS**.

3.6 Event Center

Device reports all alarm messages, client responds to alarm message only when corresponding alarm event is enabled. You can view and deal with corresponding alarm message on client.



For detailed operation of alarm event config, see **3.2.4 Setting Alarm Event**

3.6.1 Setting Alarm Parameters

Configure alarm display mode on client, including alarm tone, whether flash alarm on map. Please skip the chapter if config is already done in local config.

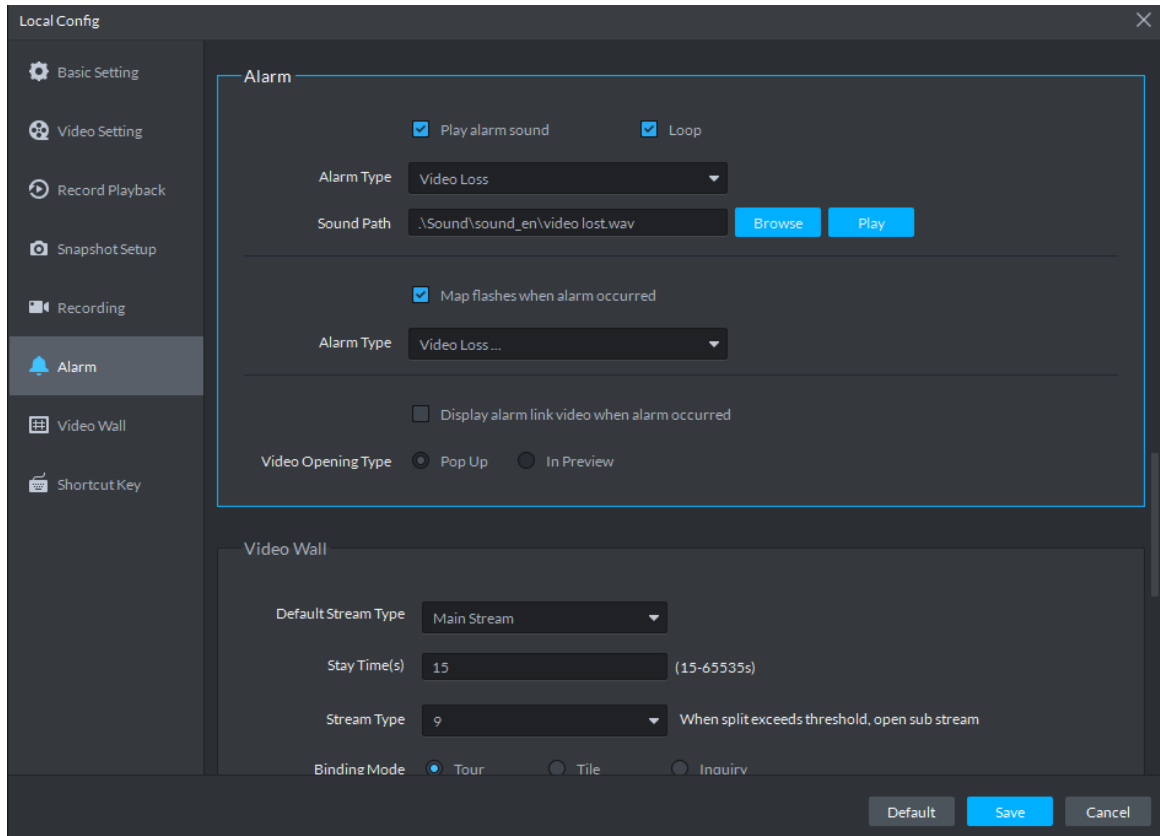
Step 1 Click  at the top right corner on client interface.

The system displays **Local Config** interface.

Step 2 Click **Alarm** tab.

The system displays **Alarm** interface, see Figure 3-150.

Figure 3-150 Alarm



Step 3 Set alarm parameters and then click **Save**. Refer to Table 3-31 for detailed information.

Table 3-31 Alarm parameter description

Parameters	Note
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.  NOTE This item is only valid when Play alarm sound function is enabled.
Alarm type	Set alarm type. System can play sound when corresponding alarm occurs.  NOTE 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.

3.6.2 Searching and Processing Real-Time Alarm

After alarm is reported to client, users can claim alarm, view and confirm alarm, process alarm and register processed alarm. If alarm is claimed by user A, then other users cannot see the alarm record in real-time alarm. They can view the alarm details in histor alarm, but cannot deal with it. Client displays max 1000 realtime alarm messages.

Step 1 If alarm quantity is not zero on upper right corner of client, click the number, such as



, or click **Event Center** on client homepage.

The system displays **Event Center** interface, see Figure 3-151.

Figure 3-151 Event center

Alarm Time	Alarm Sort	Alarm Type	Alarm Source	Priority	Handling user	Operation
2019-05-13 20:10:21	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:09:57	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:08:31	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:08:03	Person Type Matched	3	FR123456789FR123456789FR...	High		
2019-05-13 20:08:03	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:08:55	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:07:40	Person Type Matched	4	FR123456789FR123456789FR...	High		
2019-05-13 20:07:40	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:07:37	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:08:12	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:06:44	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:07:41	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:07:28	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:06:52	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:06:10	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:04:24	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:04:00	Person Type Matched	3	FR123456789FR123456789FR...	High		
2019-05-13 20:04:00	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:03:38	Person Type Matched	3	FR123456789FR123456789FR...	High		
2019-05-13 20:03:38	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:04:33	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:03:17	Person Type Matched	3	FR123456789FR123456789FR...	High		
2019-05-13 20:03:17	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:03:12	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:03:12	Person Type Matched	4	FR123456789FR123456789FR...	High		
2019-05-13 20:03:45	Video Channel	Motion Detect	8242-196	High		

Total 258/1000 record(s).



Step 2 Click

The system displays **Real-time Alarm** interface, see Figure 3-152.

Figure 3-152 Real-time alarm

Alarm Time	Alarm Sort	Alarm Type	Alarm Source	Priority	Handling user	Operation
2019-05-13 20:11:31	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:12:24	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:11:15	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:10:49	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:10:21	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:09:57	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:08:31	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:08:03	Person Type Matched	3	FR123456789FR123456789FR...	High		
2019-05-13 20:08:03	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:08:55	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:07:40	Person Type Matched	4	FR123456789FR123456789FR...	High		
2019-05-13 20:07:40	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:07:37	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:08:12	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:06:44	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:07:41	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:07:28	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:06:52	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:06:10	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:04:24	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:04:00	Person Type Matched	3	FR123456789FR123456789FR...	High		
2019-05-13 20:04:00	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:03:38	Person Type Matched	3	FR123456789FR123456789FR...	High		
2019-05-13 20:03:38	Face Matched	app	FR123456789FR123456789FR...	High		
2019-05-13 20:04:33	Video Channel	Motion Detect	8242-196	High		
2019-05-13 20:03:17	Person Type Matched	3	FR123456789FR123456789FR...	High		

Total 262/1000 record(s).



- System refreshes to display real-time alarm by default. Click to

pause refresh, click to continue refresh.

- Click and delete all alarms on real-time alarm interface, but not the data on server, you can still find it in history alarm.

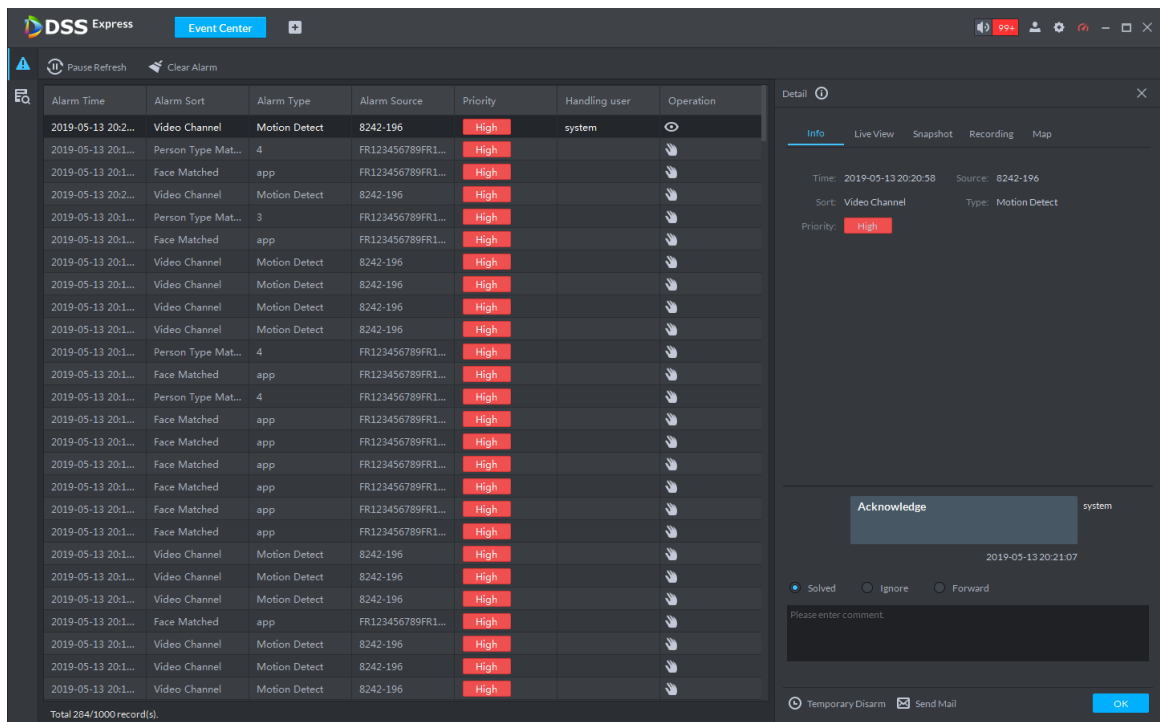
Step 3 Click of corresponding alarm.

The icon becomes , current login user claimed alarm, and then user name is displayed in the **User** column.

Step 4 Click .

The system displays alarm processing interface, see Figure 3-153.

Figure 3-153 Alarm processing



Step 5 Click **Info**, **Live View**, **Snapshot**, **Recording** and **Map** on the right of interface, and view related information of the alarm.

Step 6 Process alarm.

- Select processing result and enter comment.
Forward the alarm event to other users to process.
- Temporary disarm means receiving no alarm events during specific period.
- Send email, send email and inform related personnel of alarm event.

Step 7 Click **OK**.

3.6.3 Searching and Processing History Alarm

Step 1 If alarm quantity is not zero on upper right corner of client, click the number, such as



, or click **Event Center** on client homepage.

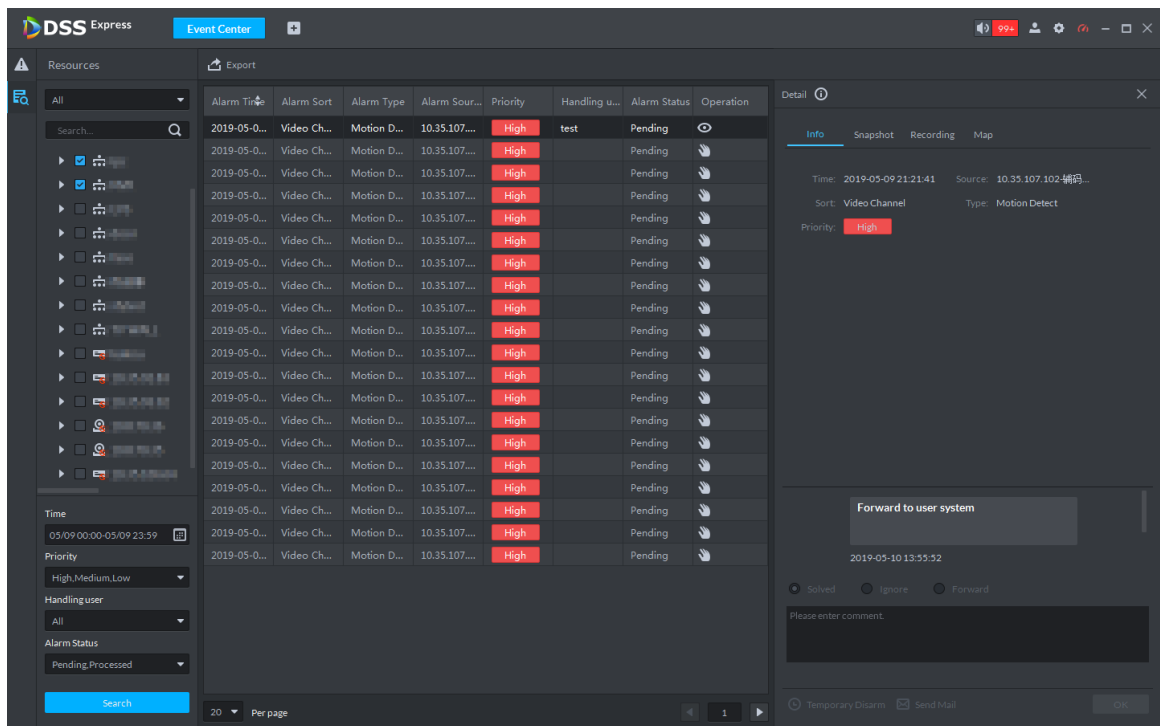
The system displays **Event Center** interface,



Step 2 Click

The system displays **History Alarm** interface, see Figure 3-154.

Figure 3-154 Select alarm type



Step 3 Set search condition, click Search.

The system displays result. You can only search alarm within one month.

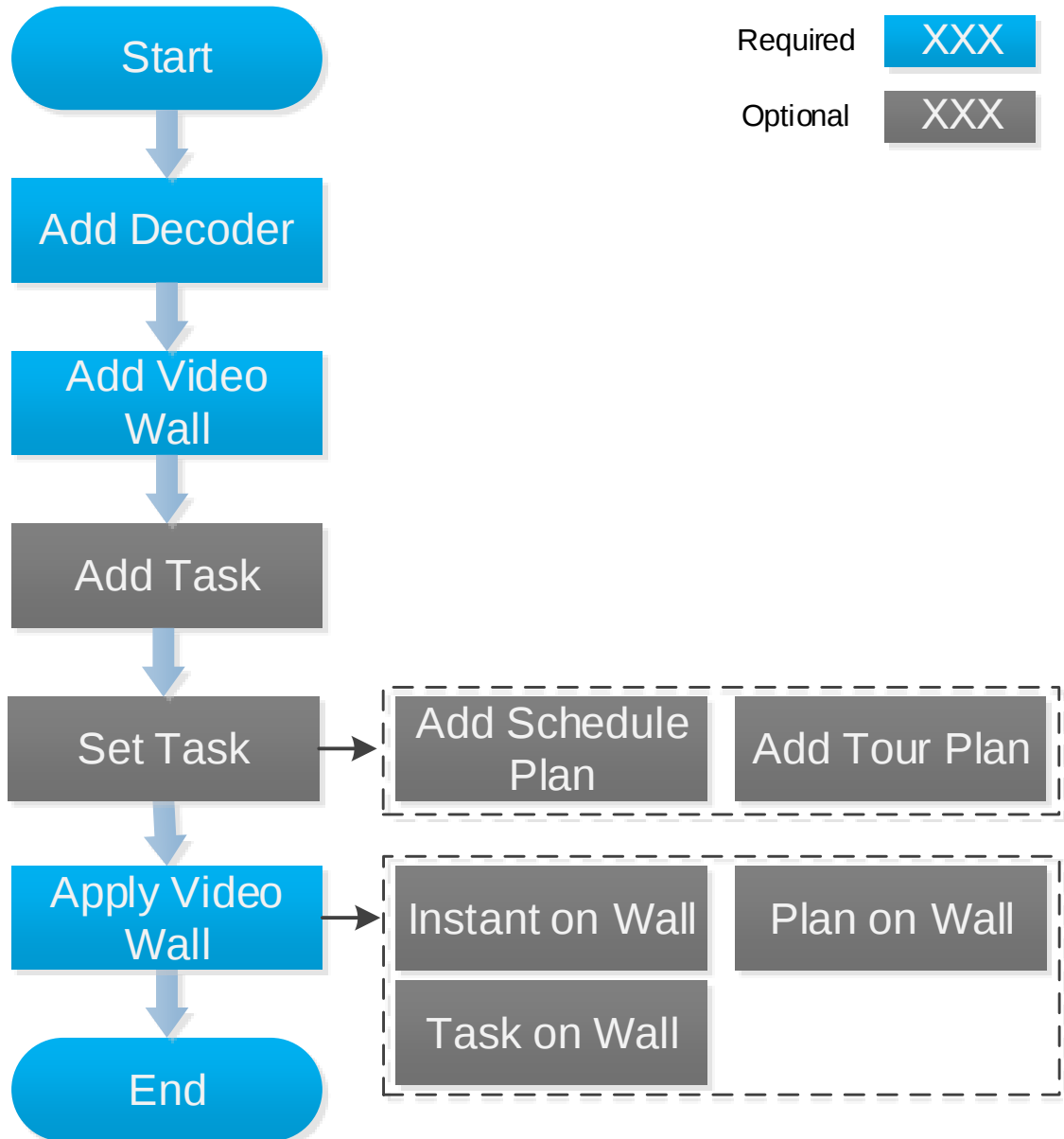
Step 4 View and process alarm. For operations, refer to **3.6.2 Searching and Processing Real-Time Alarm**.

Step 5 Click **Export**, export alarm record, saved to local in the form of .xls.

3.7 Video Wall

Decoder decodes video source, output image and display on video wall. The operation flow of video wall is shown in Figure 3-155.Video wall flow

Figure 3-155 Video wall flow



3.7.1 Adding Encoder

Add decoding devices; currently support decoder, matrix and video wall. For details, see **3.2.2.4 Adding Device**

3.7.2 Entering Video Wall Interface

On client homepage, click **Video Wall**. The system displays **Video Wall** interface. See Figure 3-156. For interface description, see Table 3-32.

Figure 3-156 Video wall

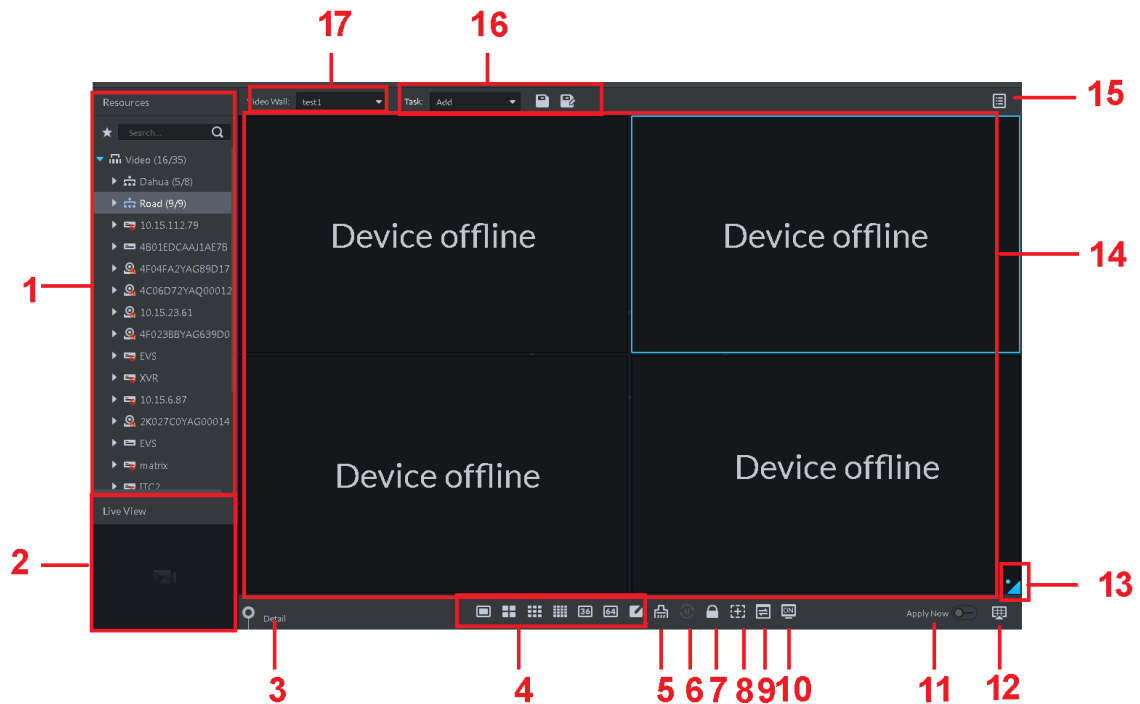


Table 3-32 Interface description

SN	Name	Function
1	Device tree	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. Click to view the channels on the favorites folder. Search is supported by input device name or channel name in here.
2	Preview	View channel video.
3	Detailed information	Click to view the screen, window, and channel bound information. - Click to preview the video at the bottom left pane. It is to check current channel is what you want or not. - Click to adjust sequence. - Click to delete the video channel that adds to current window. - Click Stay time column or click , modify signal interval on current channel when tour. - Click Stream column or , modify video bit stream.
4	Window split	Set window split mode.
5	Clear	Clear information on all screens.

SN	Name	Function
6	Start/stop all tours	Start or stop all tours.
7	Lock window	Click to lock the window. You cannot operate on the locked window.
8	Add box	You can click to add a box, and click again to cancel box.
9	Back display	View current layout
10	Screen On/Off	In Screen On mode, the system will automatically display the video after configuring the tasks.
9	Apply now	If you enable the function, system automatically outputs the video to the wall after you set the task.
10	Decode to wall	Click to manually output the video to the wall.
11	Eagle eye	View current video wall layout
12	Video wall	Video wall area.
13	Video wall task	Set schedule task and tour task. Refer to 3.7.5 Setting Video Wall Plan for detailed information.
14	Task management pane	Add, save delete task.
15	Video wall selection	Select a video wall to configure.

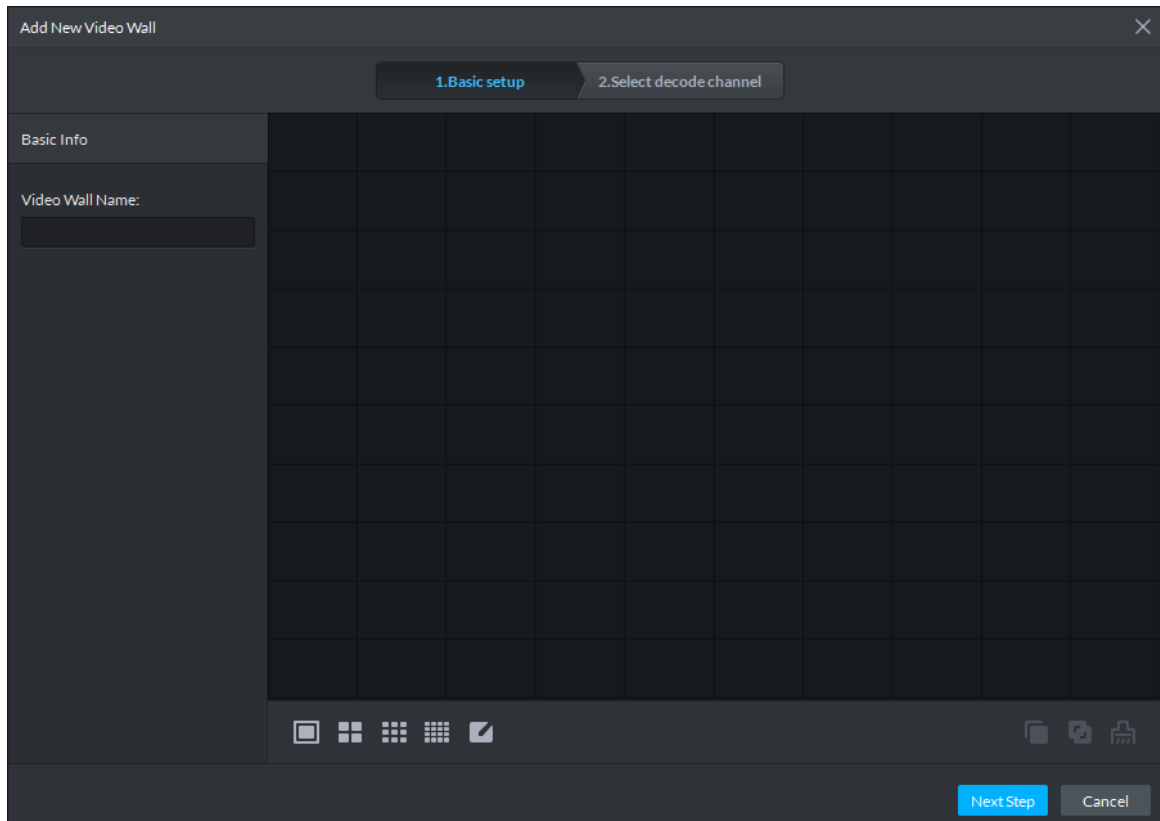
3.7.3 Adding Video Wall

Create video wall, and bind decoding channel to screen.

Step 1 On **Video Wall** interface, click drop-down box and select **Add New Video Wall**.

The system displays **Add New Video Wall** interface, see Figure 3-157.

Figure 3-157 Add new video wall



Step 2 Enter **Video Wall Name**, select screen quantity icon on the bottom, and click add anywhere on the screen.



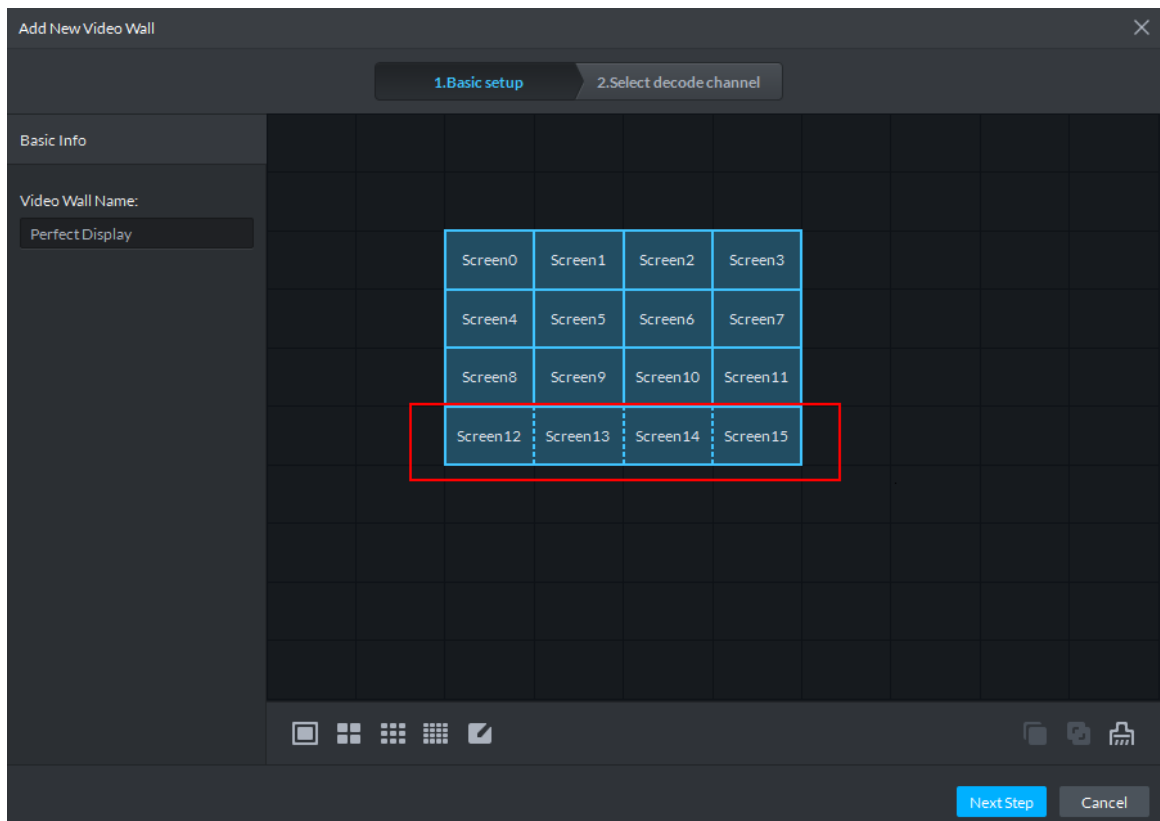
- You can add 1 window, 4 windows, 9 windows and 16 windows, click  to customize window.
- If the added window is not right, you can click  to delete and add again.

Step 3 (Optional) Press **Shift** button, select several screens, click  and combine the screens, see Figure 3-158.



- Please skip the step if combination screen is not needed.
- Select combination screen, click  to cancel.

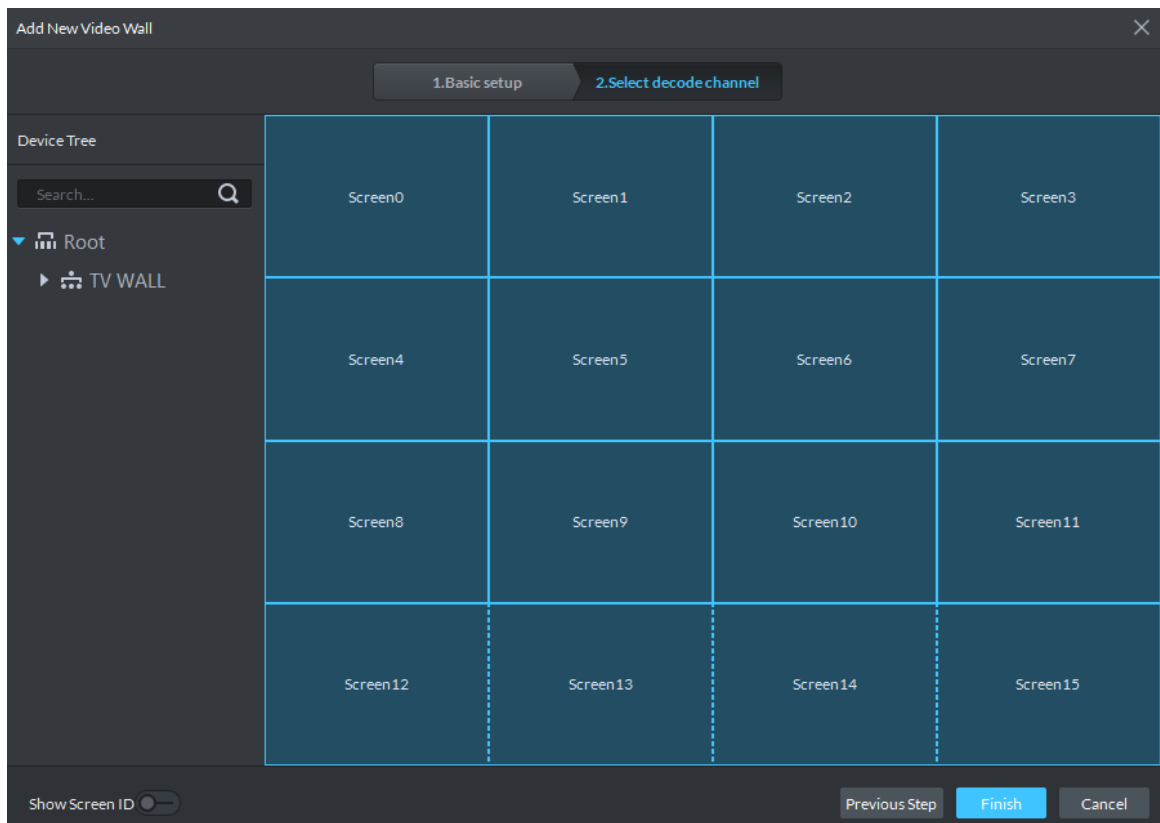
Figure 3-158 Combination Screen



Step 4 Click **Next Step**.

The system displays **Select Decode Channel**, see Figure 3-159.

Figure 3-159 Bind decode channel

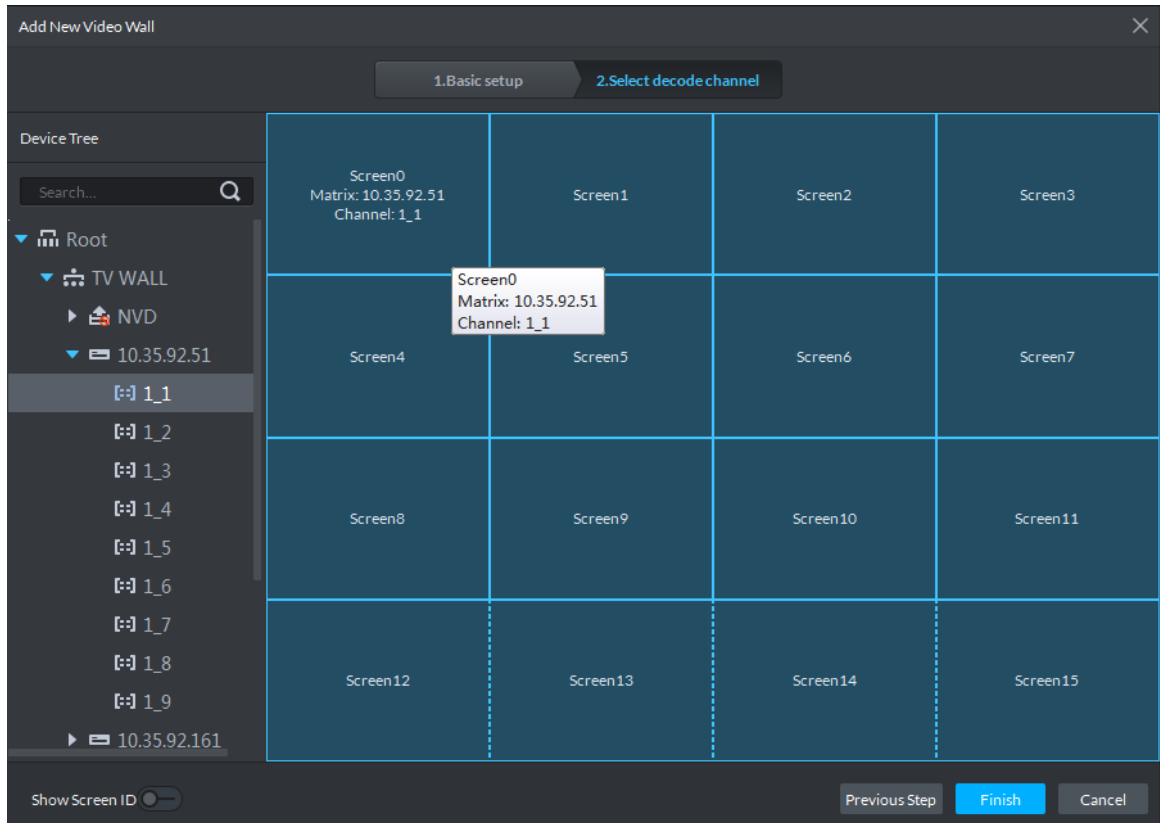


Step 5 Drag the decode channel on the left to each screen on the right for binding, see Figure 3-160.



- Each screen in combination screen must bind with decode channel.
- One video wall can bind several channels of decode device.

Figure 3-160 Binding result



Step 6 Click **OK** and video wall is added.

3.7.4 Adding Task

Save the task plan and next time you can directly call task and realize quick display on wall.

Step 1 Select **Add** from the **Task** box.

Step 2 Drag the video channel on the left to the screen on the right.

Step 3 Click .

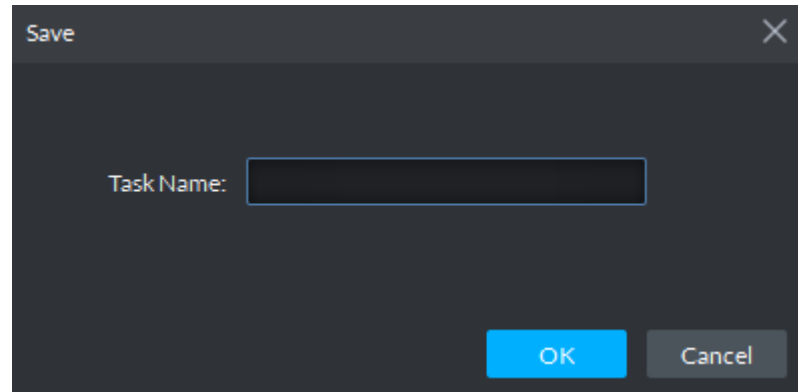
The system displays **Save** interface, see Figure 3-161.



If you select created task from task box, then drag video channel for binding, click 

and save as other task. The saved task displays on wall automatically.

Figure 3-161 Save task

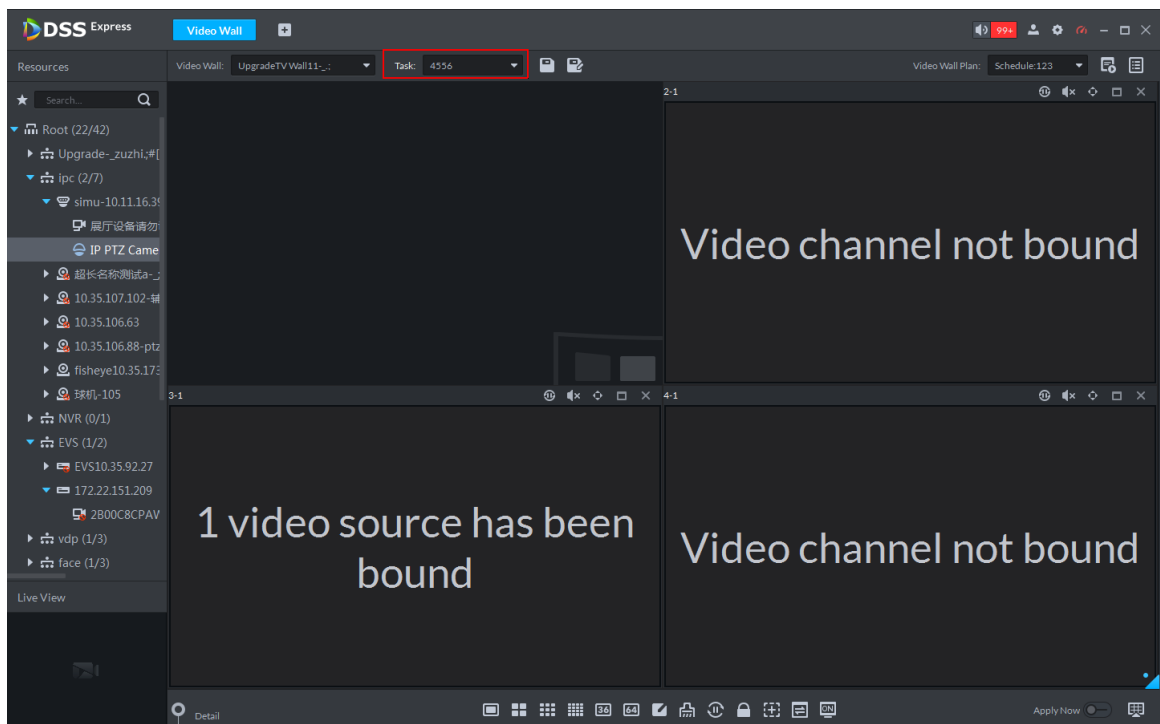


Step 4 Enter task name, click OK and save.



- After task is displayed on wall, and bound video channel is modified, then you need to click  to display on wall manually.
- Click   and you can stop tour or start tour.

Figure 3-162 Task display on wall



3.7.5 Setting Video Wall Plan

3.7.5.1 Adding Scheduel Plan

If task is configured, you can set task start time, end time and duration of each task, form plan and realize by schedule. If the set task occupies less than 1 day, then you can set remaining time to implement other tasks.

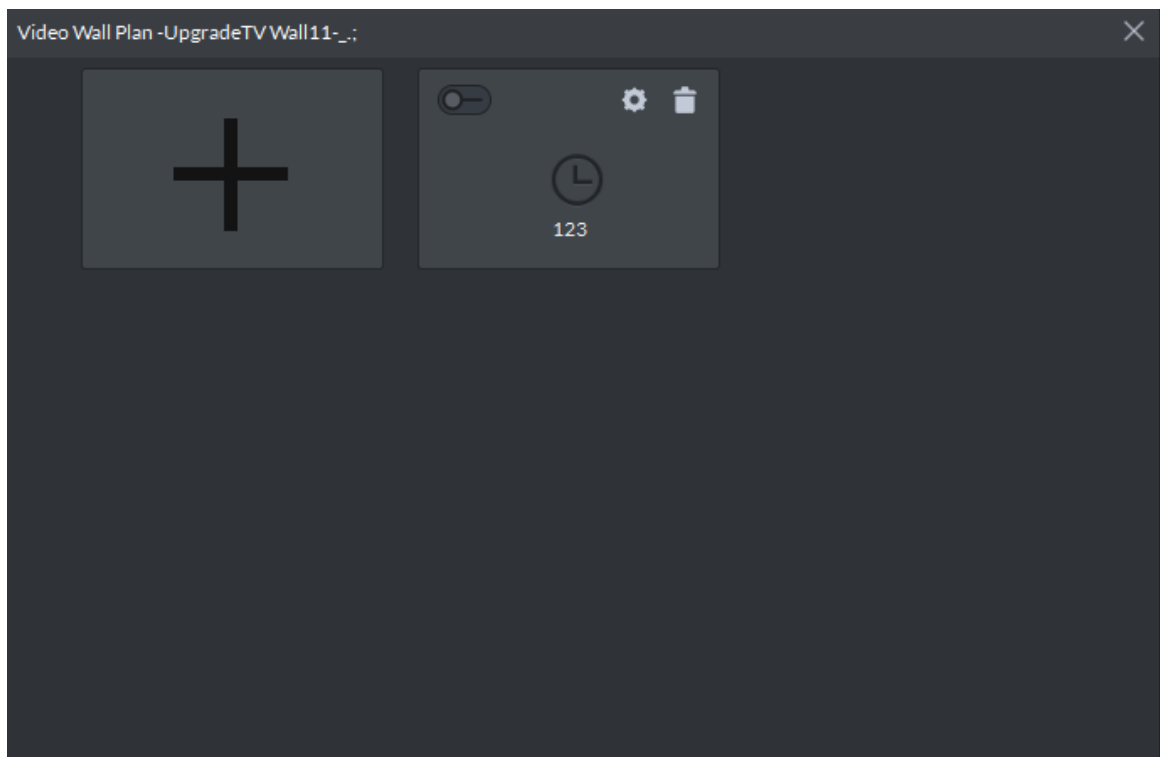


The task is required to be configured. For detailed operations, see **3.7.4 Adding Task**.

Step 1 On **Video Wall** interface, click  on upper right corner.

The system displays interface of video wall plan, see Figure 3-163. Video wall plan

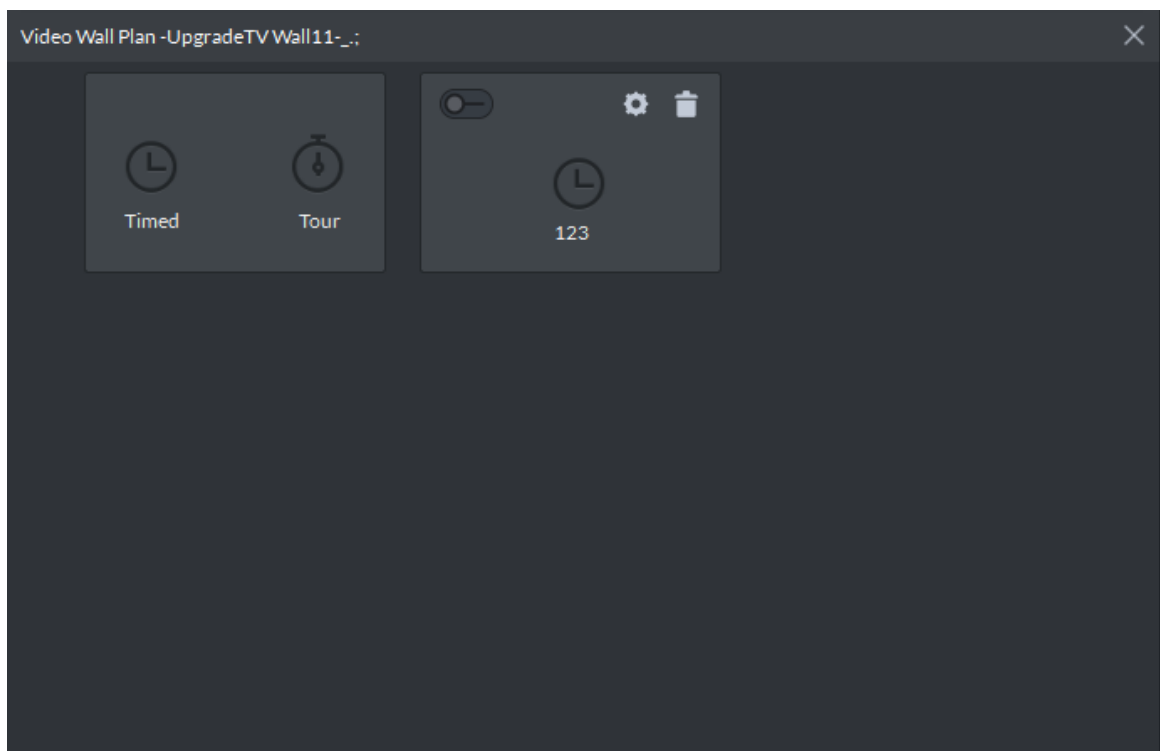
Figure 3-163 Video wall plan



Step 2 Move the mouse to "+", select **Schedule**, see Figure 3-164.

The system displays Schedule Plan interface, see Figure 3-165.

Figure 3-164 Plan type



Schedule Plan-UpgradeTV Wall11-_:

×

Plan Name:

Task: 123 ▼

Start Time: 00:00:00 ⬆⬇⬆

End Time: 23:59:59 ⬆⬇⬆

+

Task Name	Start Time	End Time	Operation

☐ Enable Remaining Time Plan

123 ▼

Save

Cancel

Step 4 Select task, enter start time and end time, click "+", add to list.

Figure 3-166 Added task

Schedule Plan-UpgradeTVWall11-_:

Plan Name: 456

Task: 123 ▼ Start Time: 00:00:00 ▲ End Time: 23:59:59 ▲ +

Task Name	Start Time	End Time	Operation
123	00:00:00	23:59:59	🗑

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

☐ Enable Remaining Time Plan

123 ▼

Save Cancel

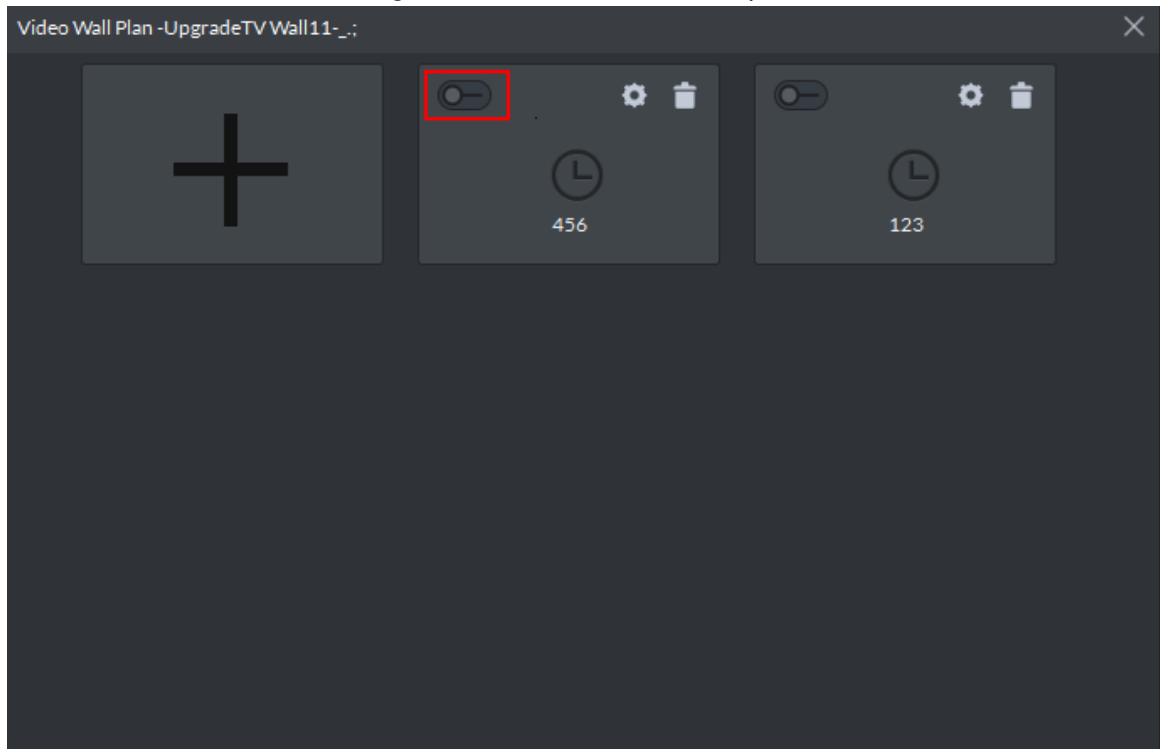
Step 5 Click **Save** to add.

Step 6 In the plan list, click  and realize schedule plan, see Figure 3-167.



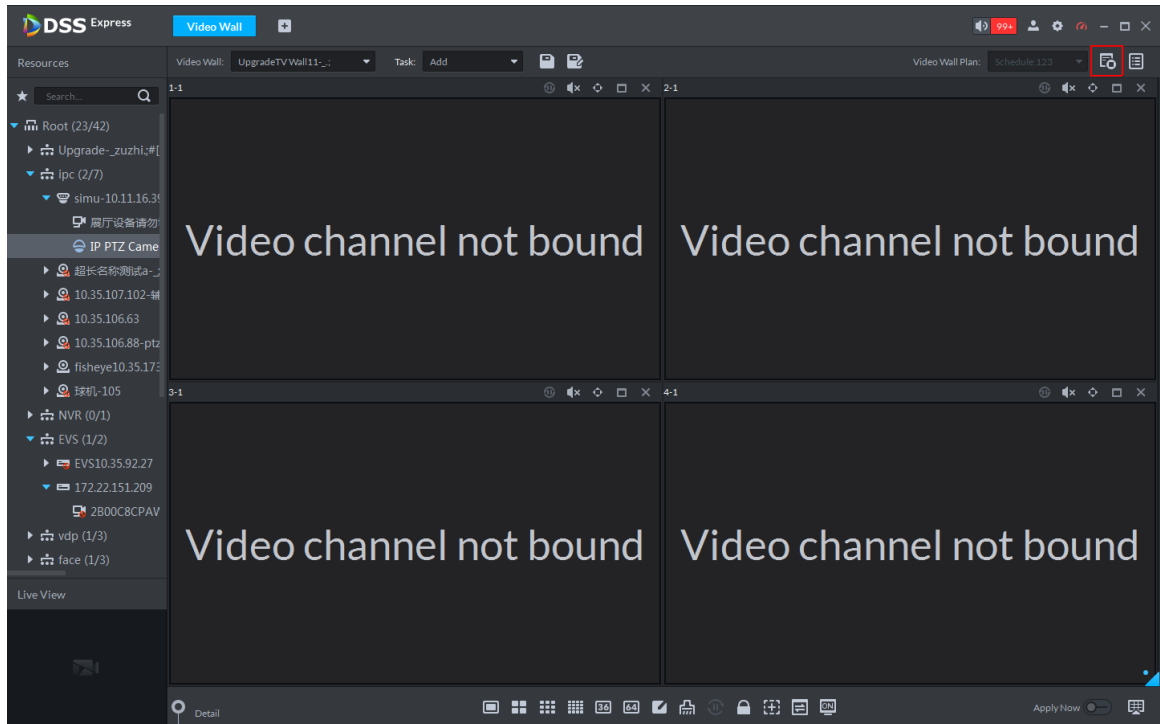
- Several plans cannot be displayed on wall at the same time; the previous plan is closed when you open another plan.
- Click  and modify plan.
- Click  and delete plan.

Figure 3-167 Enable schedule plan



If you want to stop plan, click , see Figure 3-168. The icon is switched to , click again to display on wall; If you want to switch other plans, you can enable other plan in the list.

Figure 3-168 Stop/Start plan



3.7.5.2 Adding Tour Plan

If the plan is configured, you can set sequence of several tasks and stay duration of each task. Display on wall in a cycle.



The task is required to be configured. For details, refer to **3.7.4 Adding Task**.

Step 1 On Video Wall interface, click  on upper right corner, the system displays plan management interface, see Figure 3-169.

Step 2 Move the mouse to “+”, select **Tour**, see Figure 3-169.
The system displays **Tour Plan** interface, see Figure 3-170.

Figure 3-169 Plan type

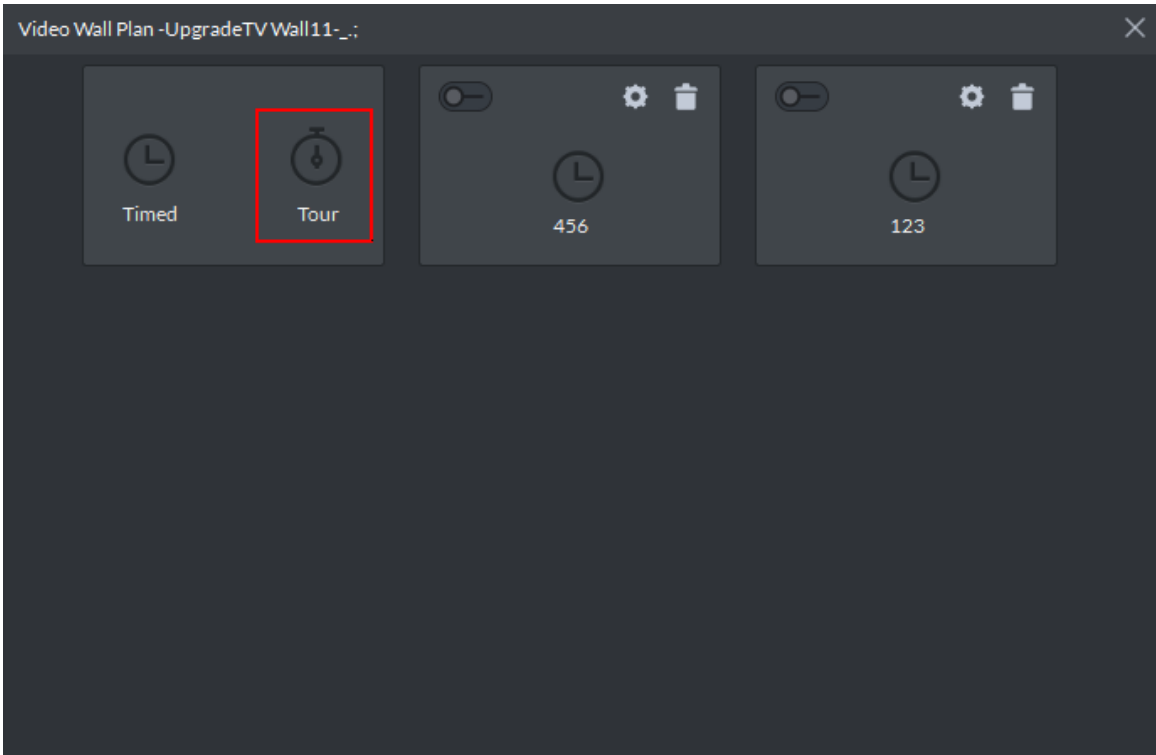
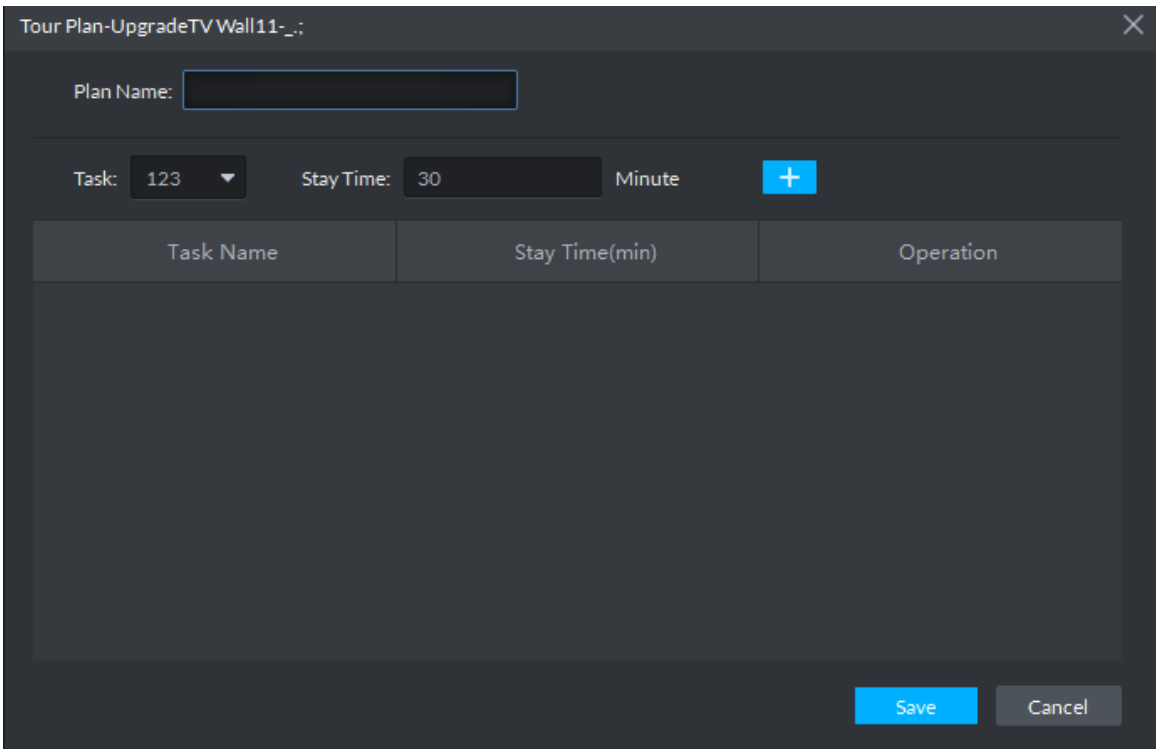


Figure 3-170 Add tour plan



- Step 3 Enter plan name.
- Step 4 Select task, enter stay time, click "+", add to list.
Repeat the operation and you can add several tasks, see Figure 3-171.



Click   and adjust the display sequence of tasks.

Figure 3-171 Added task

Tour Plan-UpgradeTVWall11-_-;

Plan Name: 1818

Task: 123 Stay Time: 30 Minute +

Task Name	Stay Time(min)	Operation
123	00:30	↑ ↓ 🗑️

Save Cancel

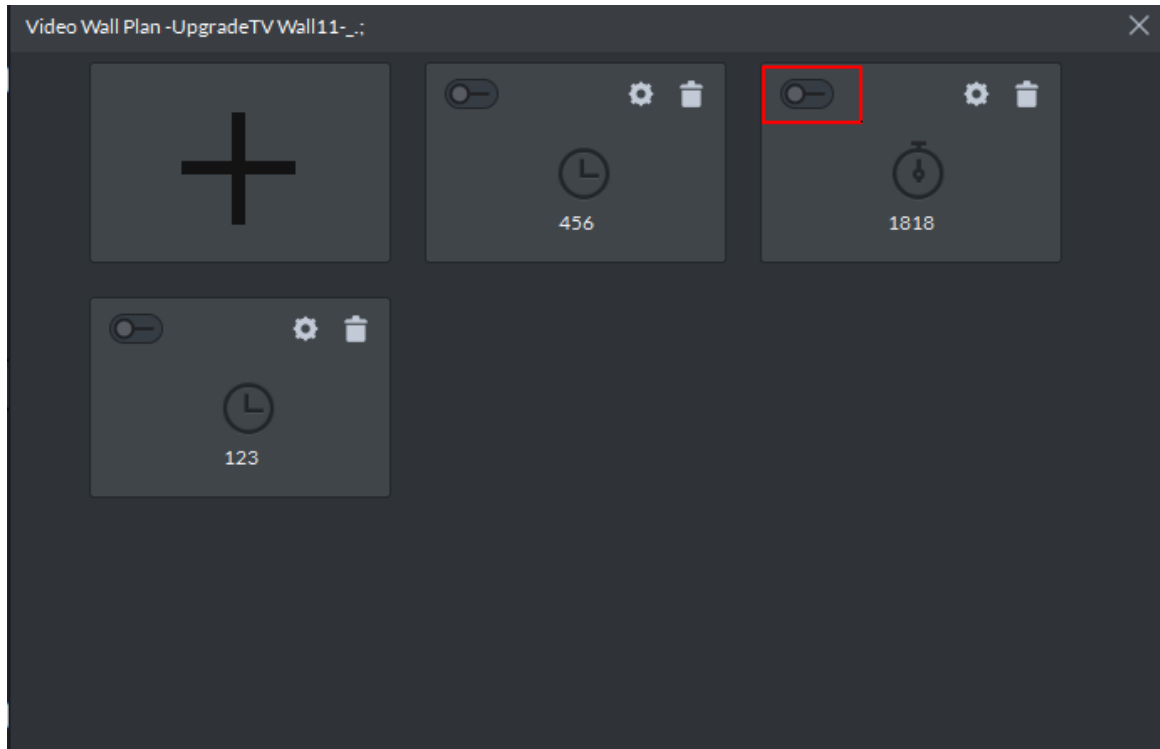
Step 5 Click **Save**, and plan is added.

Step 6 In plan list, click  and enable tour plan, see Figure 3-172.



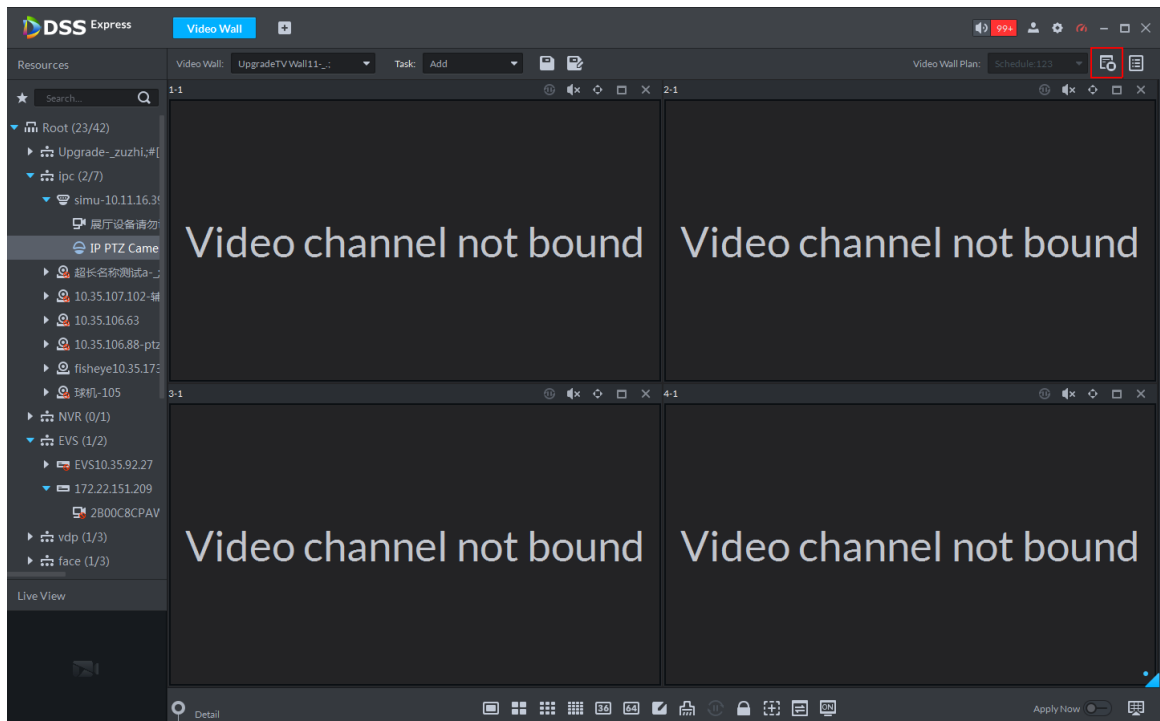
- Several plans cannot be displayed on wall at the same time; the previous plan is closed when you open another plan.
- Click  and modify plan.
- Click  and delete plan.

Figure 3-172 Enable tour plan



If you want to stop plan, click , see Figure 3-173. The icon is switched to , click again to display on wall; If you want to switch other plans, you can enable other plan in the list.

Figure 3-173 Stop/Start plan



3.7.6 Applying Video Wall

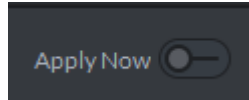


Encoding device is required to be connected to video wall, otherwise it cannot be displayed on wall.

3.7.6.1 Apply Now

Drag video channel to screen and display on wall directly.

Step 1 Select video wall from the box.



Step 2 Click on lower right corner, and enable the function of displaying on wall instantly.

Step 3 Drag left video channel to right screen for binding, see Figure 3-174.



If you select fisheye channel display on wall, right click to select fisheye mounting mode and realize fisheye dewarping, see Figure 3-175.

Figure 3-174 Bind video channel

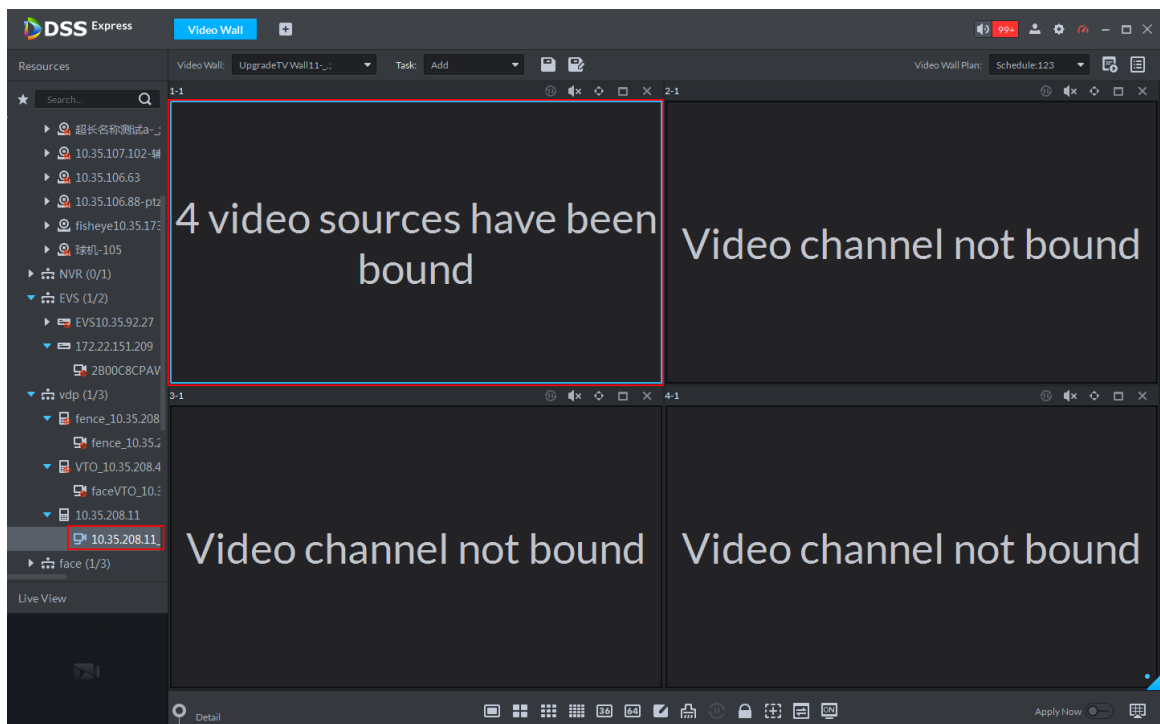
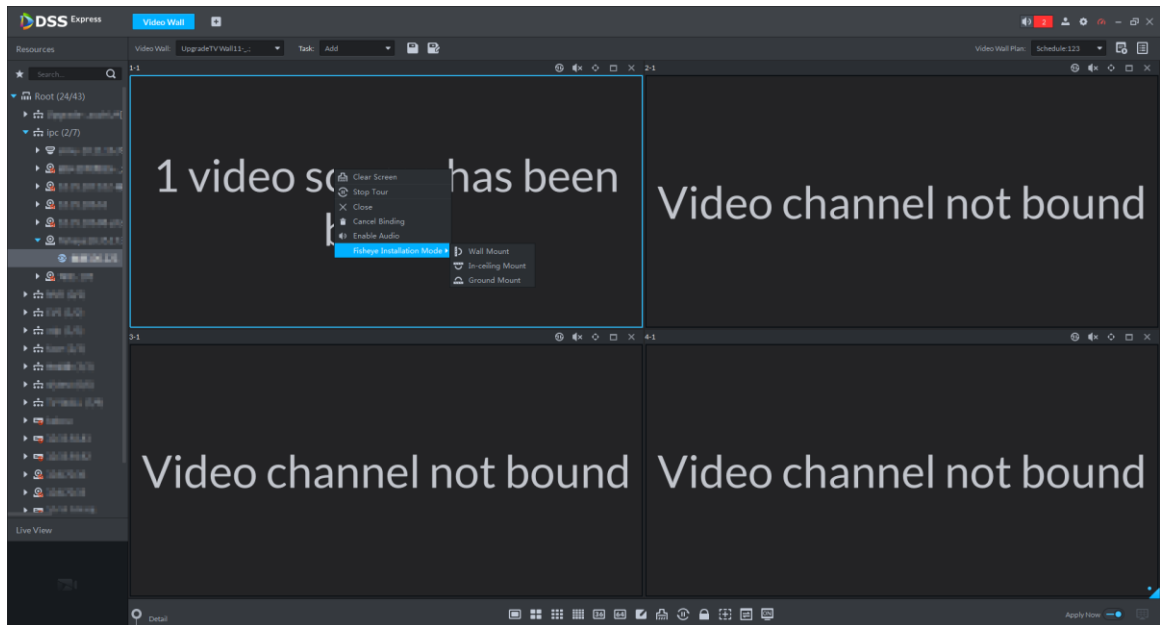


Figure 3-175 Fisheye dewarp

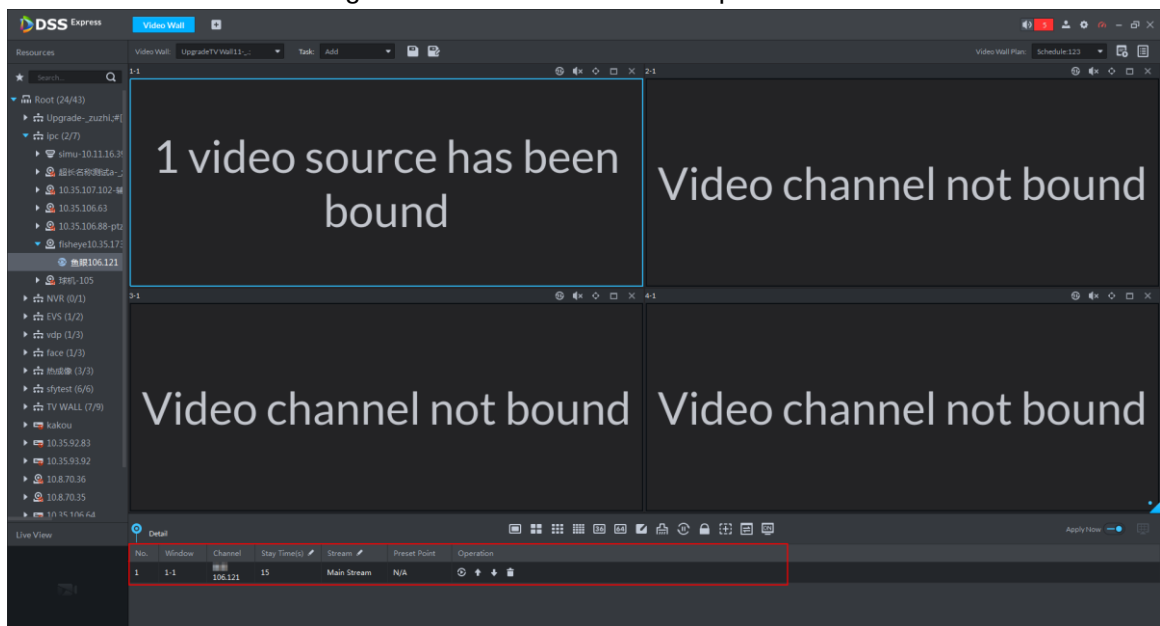


Step 4 Select screen, click **Detail** on the bottom.

System displays setting interface of channel, see Figure 3-176. View the bound video channel info, meanwhile you can set stay time, stream type, preset and operation of each video channel.

- Click and open the channel's real-time video on lower left corner.
- When binding several video sources; click , adjust display sequence.
- Click and delete video source.

Figure 3-176 Set video channel parameter



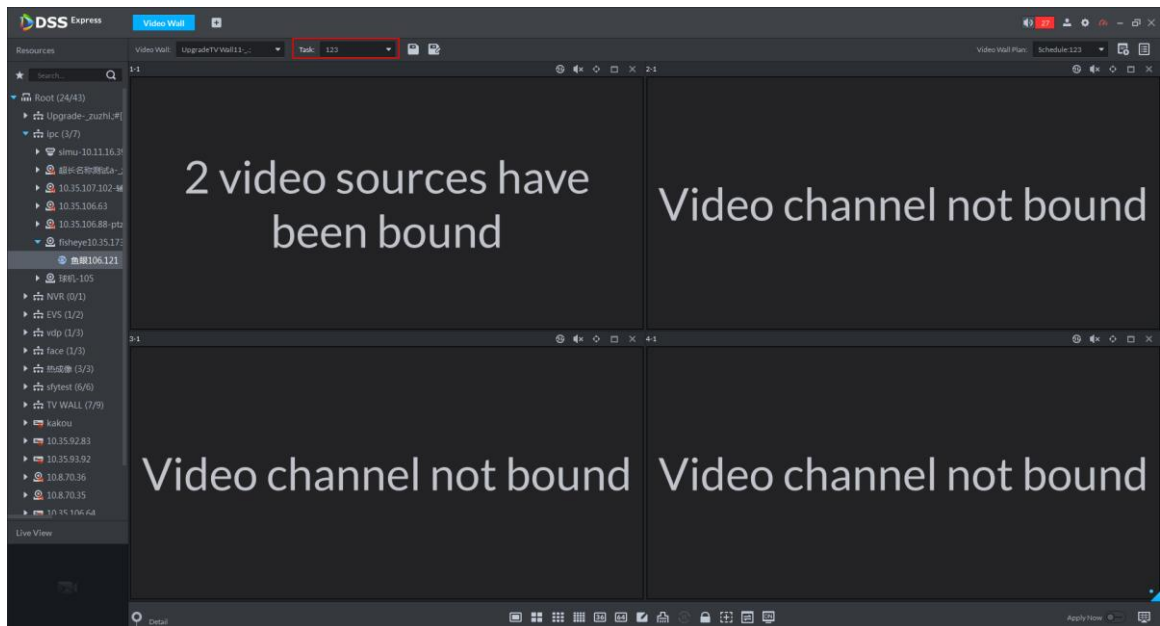
3.7.6.2 Task Displayed on Wall

Call configured task plan and realize quick display on wall.



The task is required to be configured, for detailed config operation, see **3.7.4 Adding Task**. Select task from the box, task is automatically displayed on wall. See Figure 3-177.

Figure 3-177 Task displayed on wall



Support following operations after displayed on wall.

- After task is displayed on wall, if bound video channel is modified, then you need to click



on lower right corner and display on wall manually.

- Task displayed on wall, click   on the bottom, then you can stop or start tour.
- Select screen, click **Detail** on the bottom. You can view info of bound video channel; meanwhile you can set stay time, stream type, preset and operation for each video channel.

- ◇ Click , open real-time video of the channel on lower left corner.
- ◇ When binding several video sources, click  , and adjust display sequence of video source.
- ◇ Click  and delete video source.

3.7.6.3 Plan Displayed on Wall

According to the timed plan and tour plan that have been set, display on wall automatically with specific period. For details of config plan, refer to **3.7.5 Setting Video Wall Plan**

3.8 POS

If NVR with POS channel is added on Web, then you can view related video and playback of POS channel on client.

3.8.1 Adding Encoder

Platform needs to connect to NVR with POS channel, and then POS function is realized.

Step 1 Add NVR with POS channel. For detailed operation, refer to **3.2.2.4 Adding Device**

Step 2 On **Bind Resource** interface, bind POS channel as video channel.

After video channel is bound, you can view related channel video in live view, during record playback, you can play the video before and after POS receipt is generated, and then bind video of video channel.



- The added NVR binds at least one POS channel.
- 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 left device tree, select POS channel, click **Bind Resource**, and see Figure 3-178.

The system displays **Bind Resource** interface, see Figure 3-179.

Figure 3-178 Enter bind resource interface

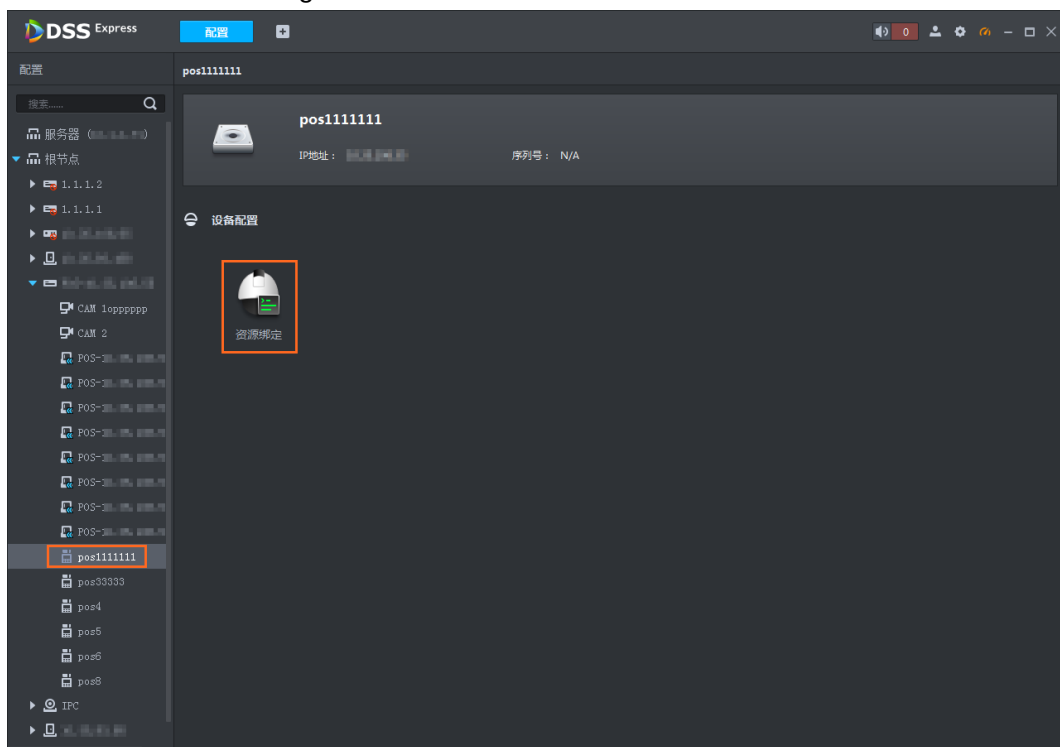
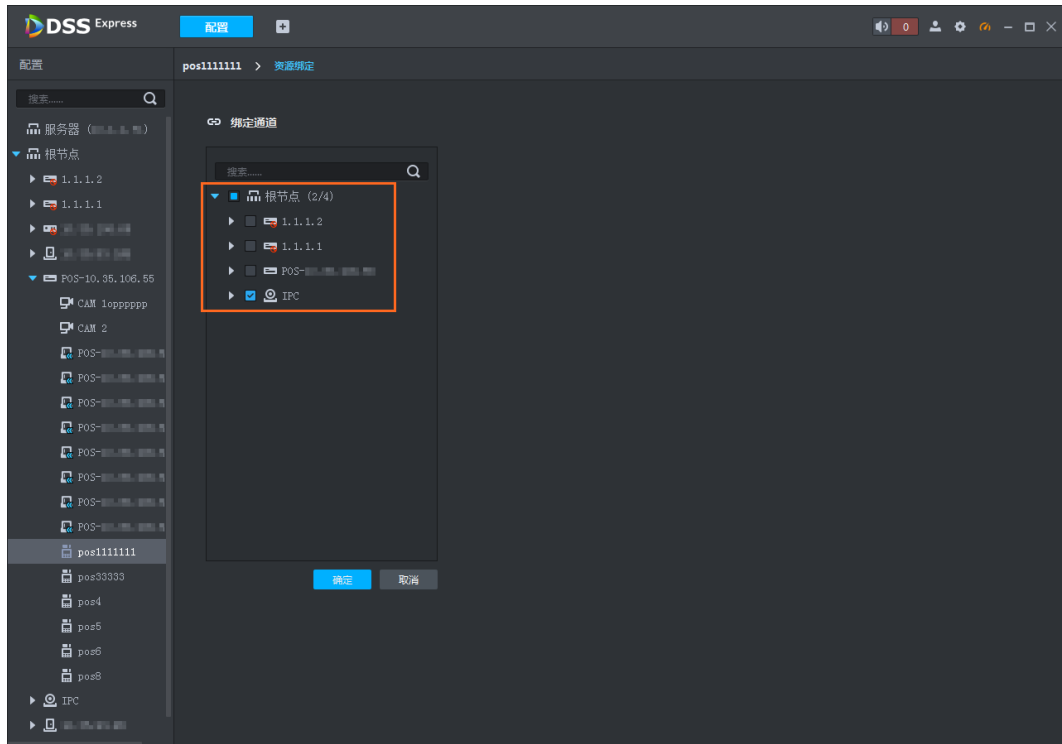


Figure 3-179 Bind resource



3) Select bound video channel, click **OK**.

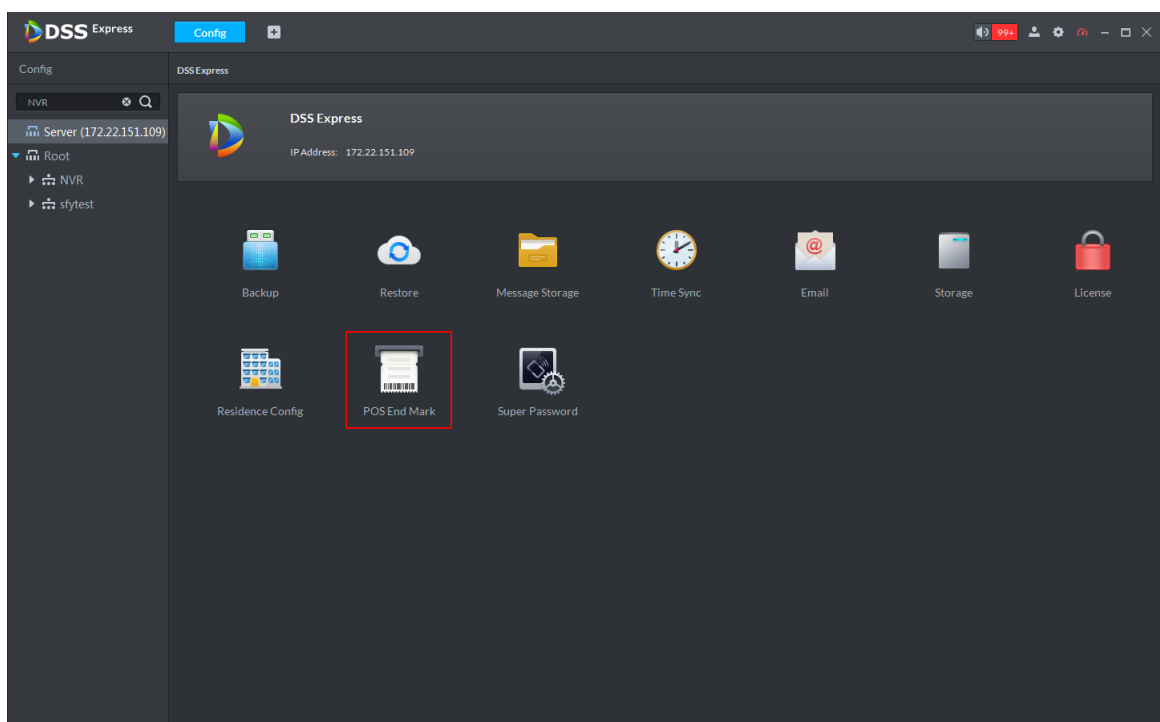
3.8.2 Modifying POS End Mark

POS end mark is the mark printed on the bottom of the POS receipt, mark that POS receipt is completely printed. The default end mark is “Thank You!”, refer to the chapter if you want to modify.

Step 1 Click **Config** on client homepage.

The system displays **Config** interface, see Figure 3-180.

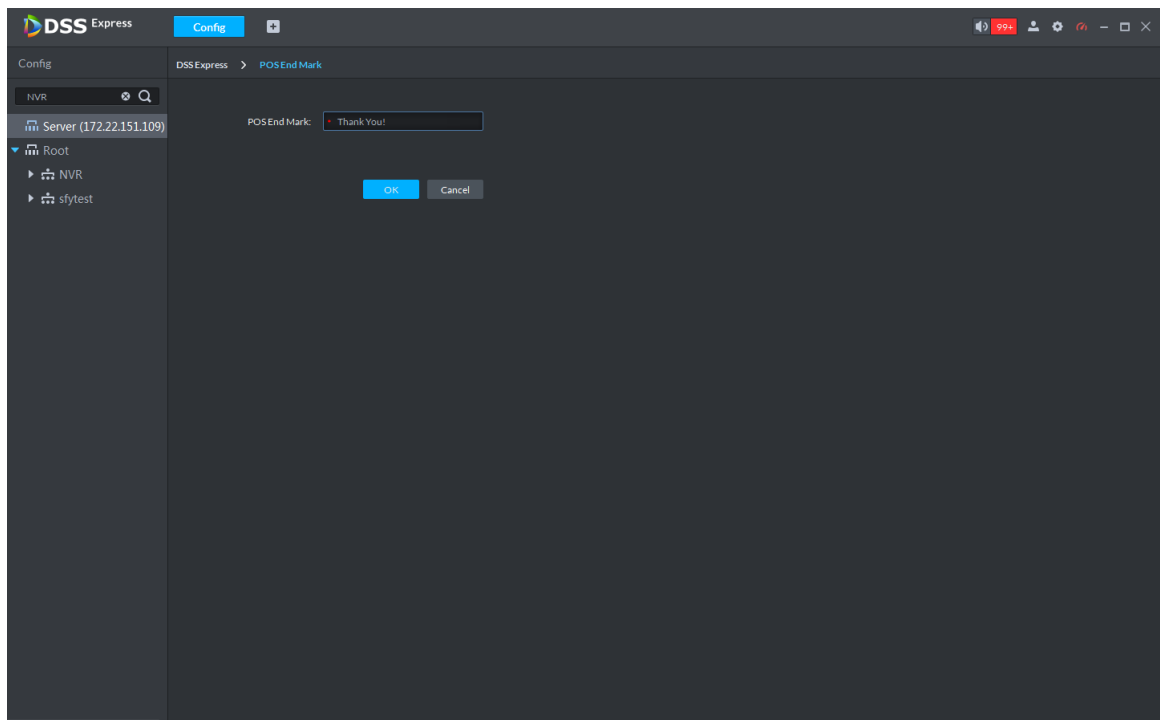
Figure 3-180 Config interface



Step 2 Click **POS End Mark**.

The system displays **POS End Mark** interface, see

Figure 3-181 POS End Mark



Step 3 Modify end mark, clock **OK**.

3.8.3 Live View

Preview realtime video and POS info of video channel linked to POS channel.

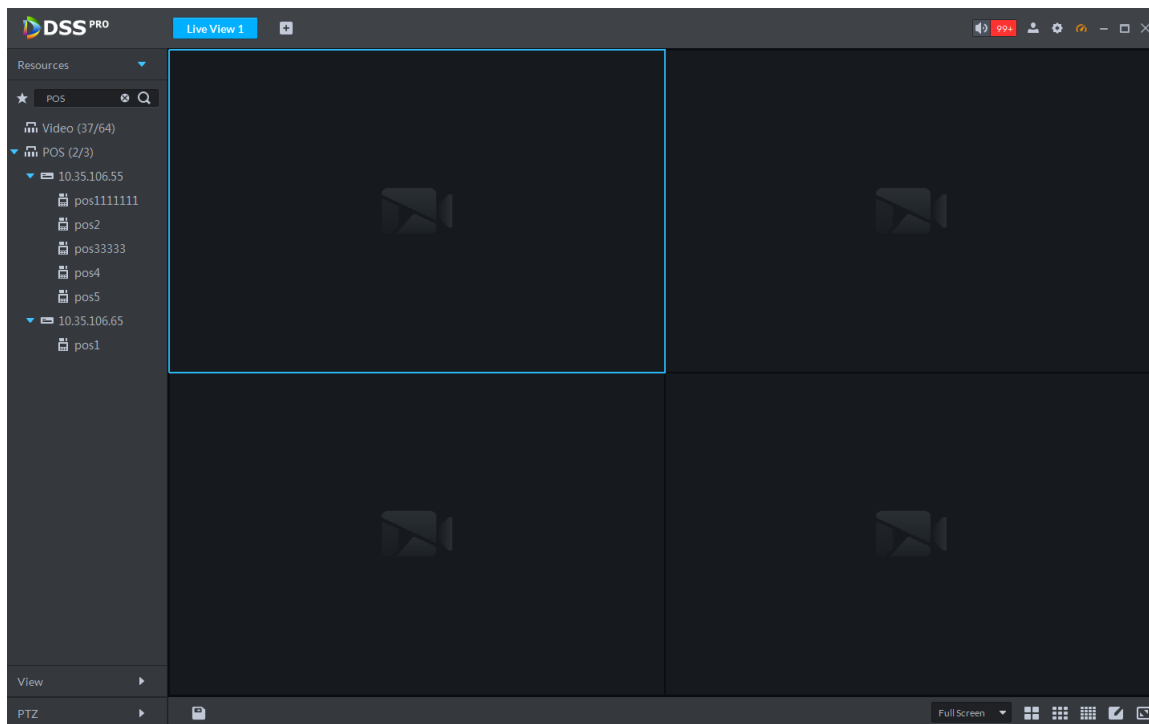


In this chapter, it introduces how to enable settings of video preview and POS format. For more details, refer to 3.4 Live View.

Step 1 Click **Live View** on the client homepage.

The interface of **Live View** is displayed. See Figure 3-182.

Figure 3-182 Open live view interface



Step 2 Click  next to POS on the left of interface.

The system displays POS channel info.

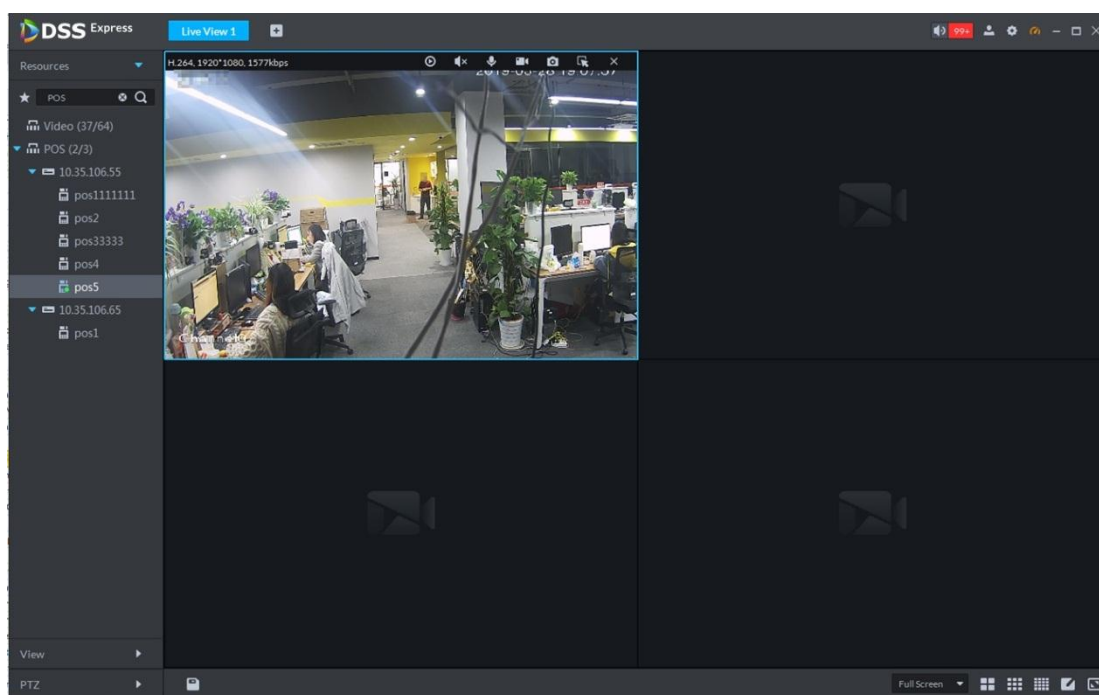
Step 3 Preview realtime channel video linked by POS.

Support following methods to preview.

- Select channel in the POS channel list, double click or drag to window.
- Double click device in the POS channel list, open all the channels of the device.

Corresponding video and POS info of linked channel are displayed. See Figure 3-183.

Figure 3-183 Start live view

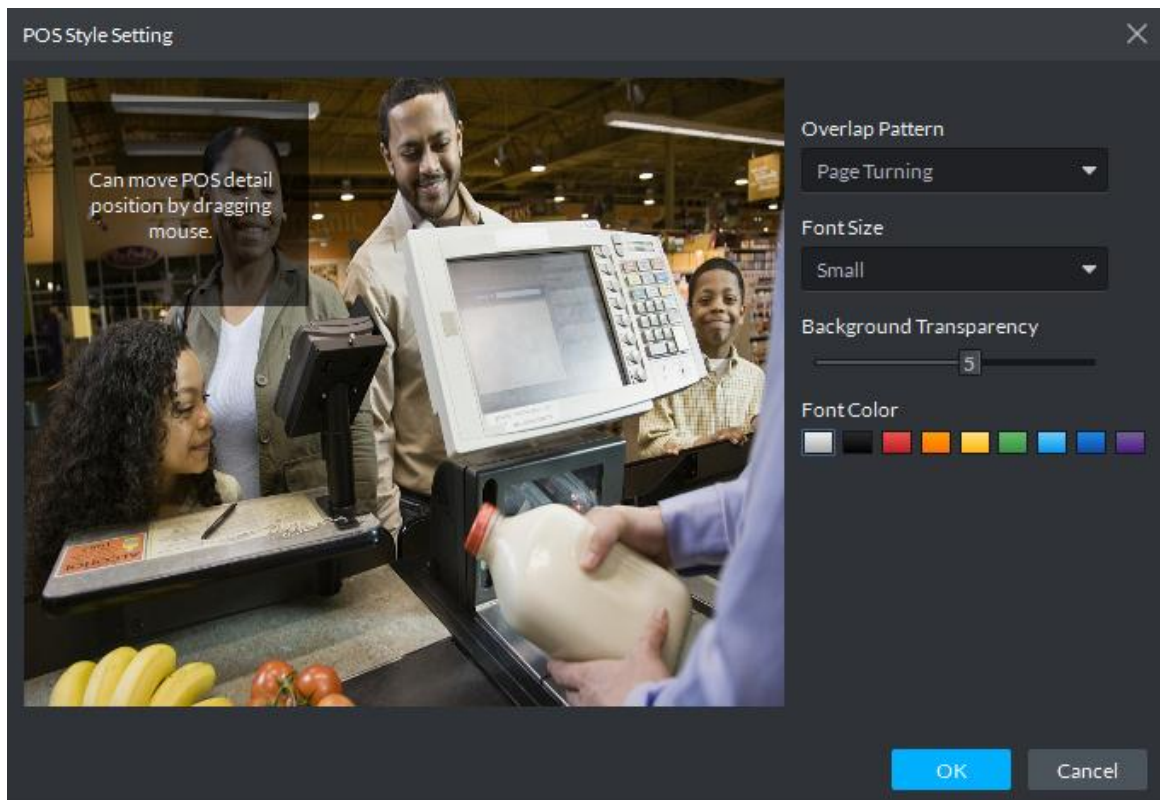


Step 4 Set POS format.

POS overlay info of all windows will be valid after setting POS style.

- Right click and select Set POS Style on the live interface.
The interface of **POS Style Setting** is displayed. See Figure 3-184.

Figure 3-184 POS style setting



- Set **Overlap Pattern**, **Font Size**, **Background Transparency** and **Font Color**.
- Move the mouse to POS info overlay area, press mouse left button and move it to adjust POS info overlay position.
- Click **OK** and save config.

3.8.4 Record Playback

Search POS receipt, view related video of receipt. You can search the video half an hour before and half an hour after the time when POS receipt is printed, and you can start to play video 30s before the time when POS receipt is printed.



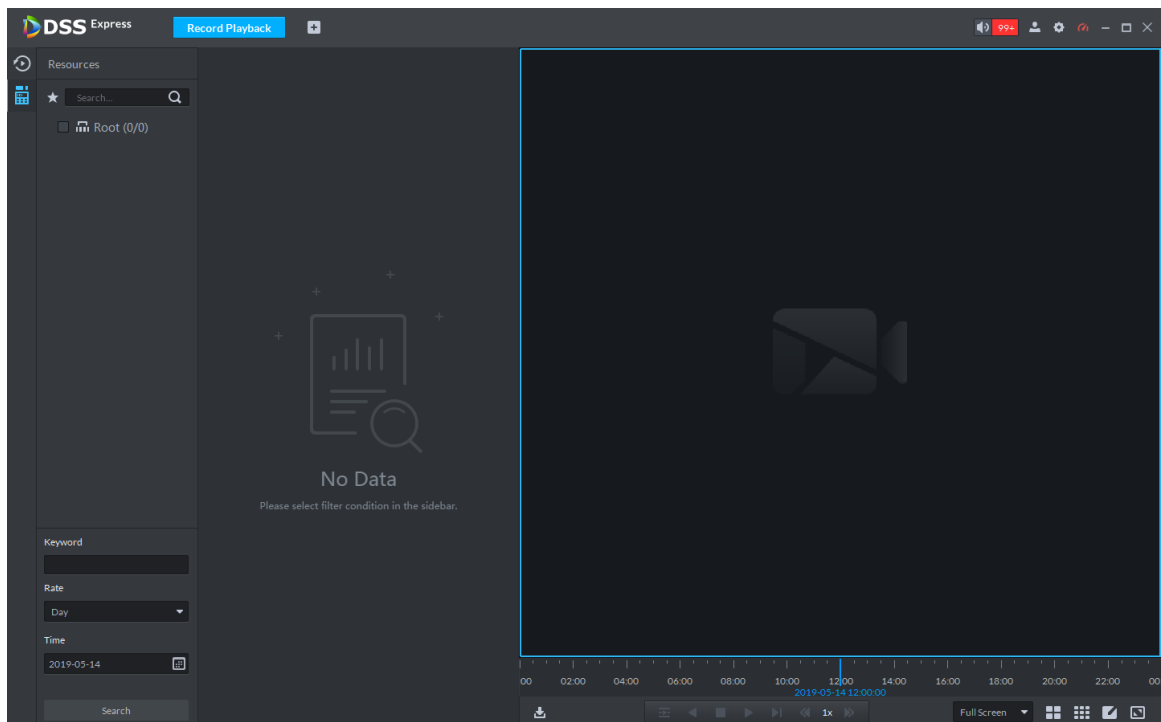
In this chapter, it mainly introduces how to replay related video of POS receipt. For more operation details, refer to **3.5 Record**

Step 1 Click  and select **Record Playback** on the interface of **Homepage**.

Step 2 Click 

The interface of **POS Search** is displayed. See Figure 3-185.

Figure 3-185 POS search

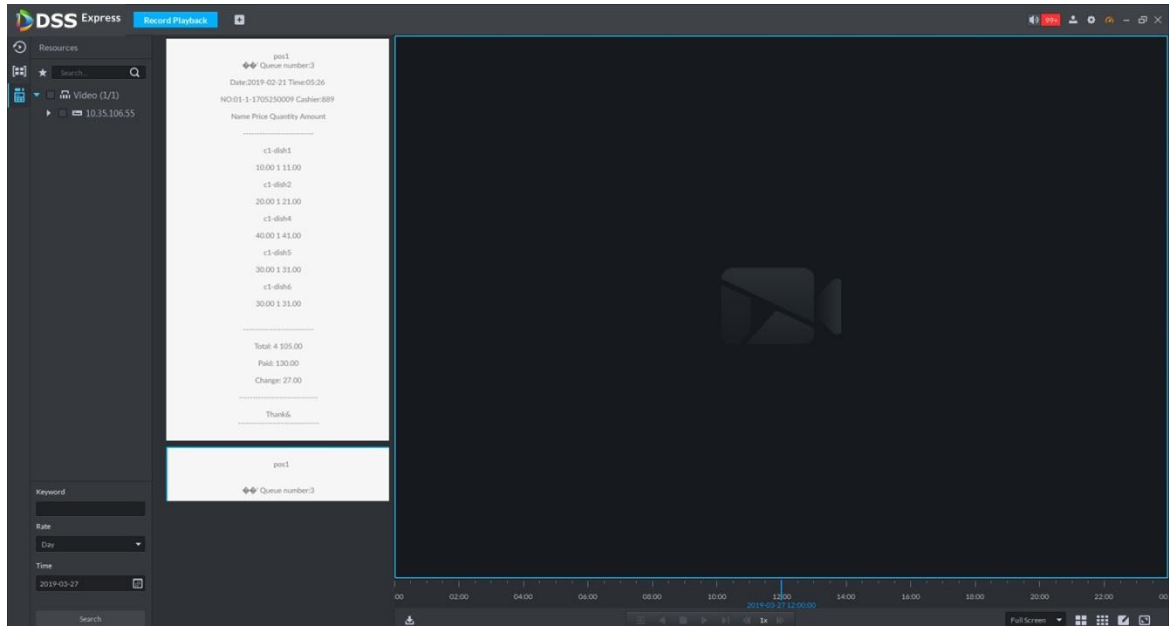


Step 3 Select channel from the device tree.

Step 4 Enter **Keyword**, select **Date** and **Time**, click **Search**.

The search result is displayed. See Figure 3-186

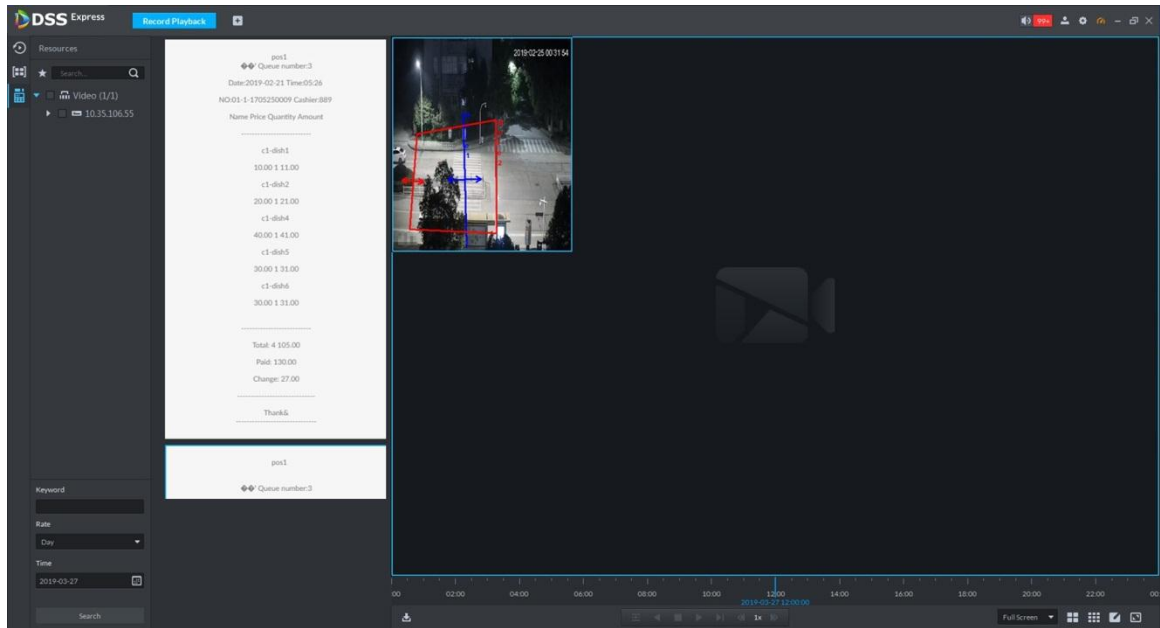
Figure 3-186 POS search result



Step 5 Double click the POS info of related video that needs to be replayed.

The window will play related video of POS. See Figure 3-187.

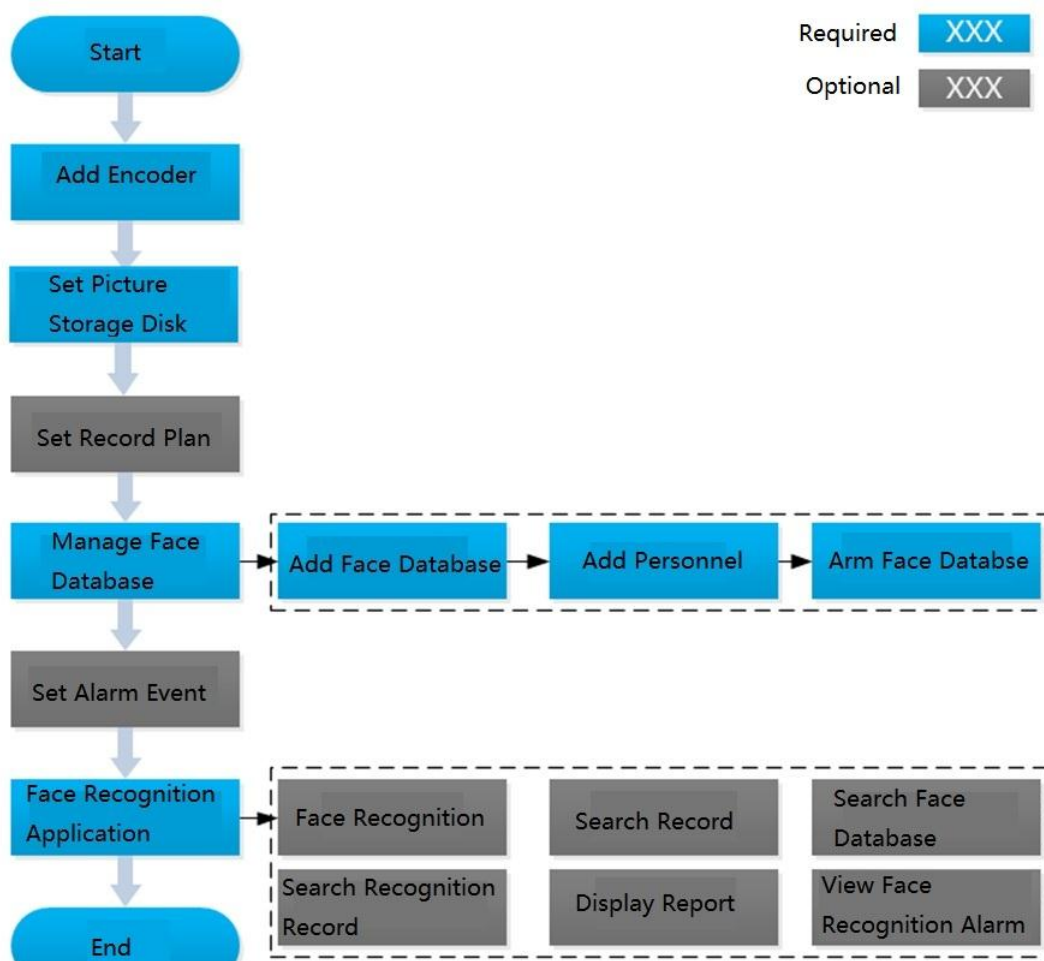
Figure 3-187 Playback video



3.9 Face Recognition

After face recognition device is added to platform, platform displays face recognition results. The operation of face recognition is shown in Figure 3-188.

Figure 3-188 Face recognition flow



3.9.1 Adding Encoder

Face recognition function can be realized only when the platform is connected to face recognition device. Intelligent devices include face recognition camera, NVR and IVSS that support face recognition function.



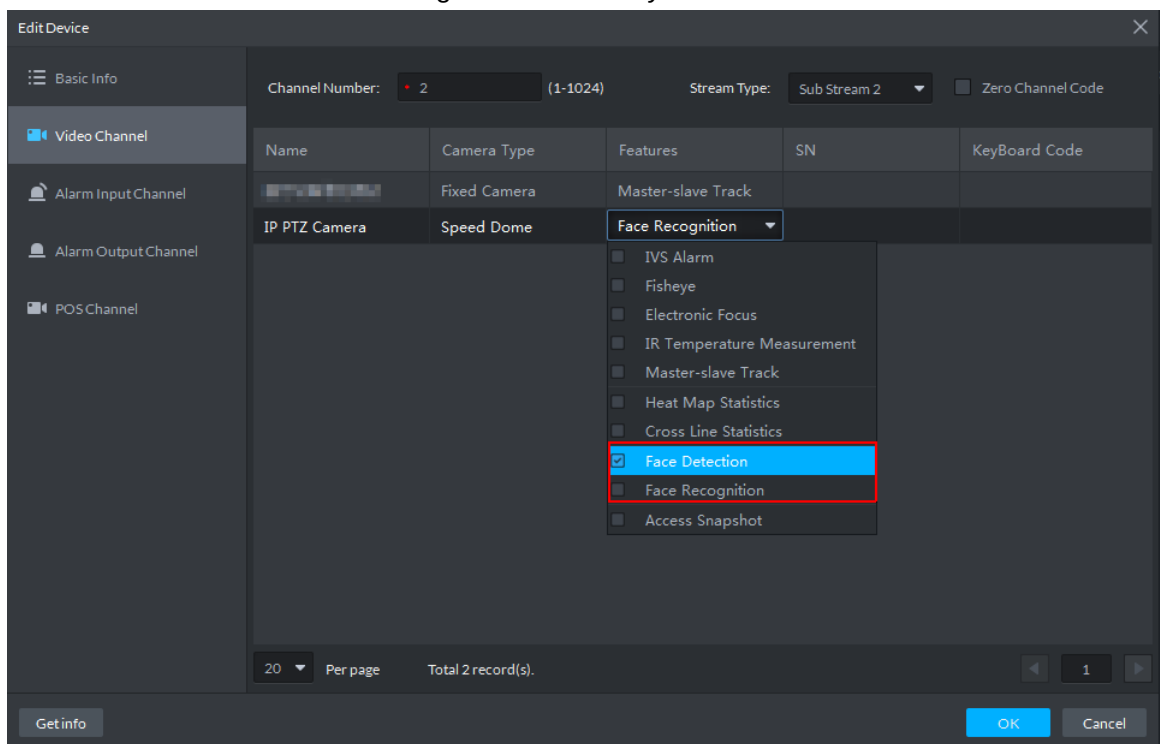
- Platform only displays face recognition results reported by device. Please make sure the added device is equipped with face recognition function, and the function is already enabled. Please refer to user manual for more details.
- If the intelligent device is IVSS or NVR, please make sure camera is added to IVSS or NVR. Please refer to device user manual for more details.

Step 1 Add face recognition camera, NVR or IVSS. For detailed operations, refer to **3.2.2.4 Adding Device.**

Step 2 Modify device channel features. On Device interface, click  next to device, modify device channel **Features**, see Figure 3-189.

- If face detection is realized by camera, then select **Face Detection** from **Features** of device channel.
- If face recognition is realized by camera, then select **Face Recognition** from **Features** of device channel.

Figure 3-189 Modify feature



3.9.2 Setting Picture Storage Disk

Configure local storage disk, you have to reserve a general picture disk to store snapshots, otherwise snapshots cannot be stored and displayed. For detailed operations, refer to **3.2.1.4 Setting Storage Space**.

3.9.3 Setting Record Plan

After record storage plan is configured, the video before and after face detection snapshot is stored, the platform can playback video 10s before and after snapshot. If you want to set record storage plan, refer to **3.2.5 Setting Record Plan**.

3.9.4 Managing Face Database

Face database management includes following functions.

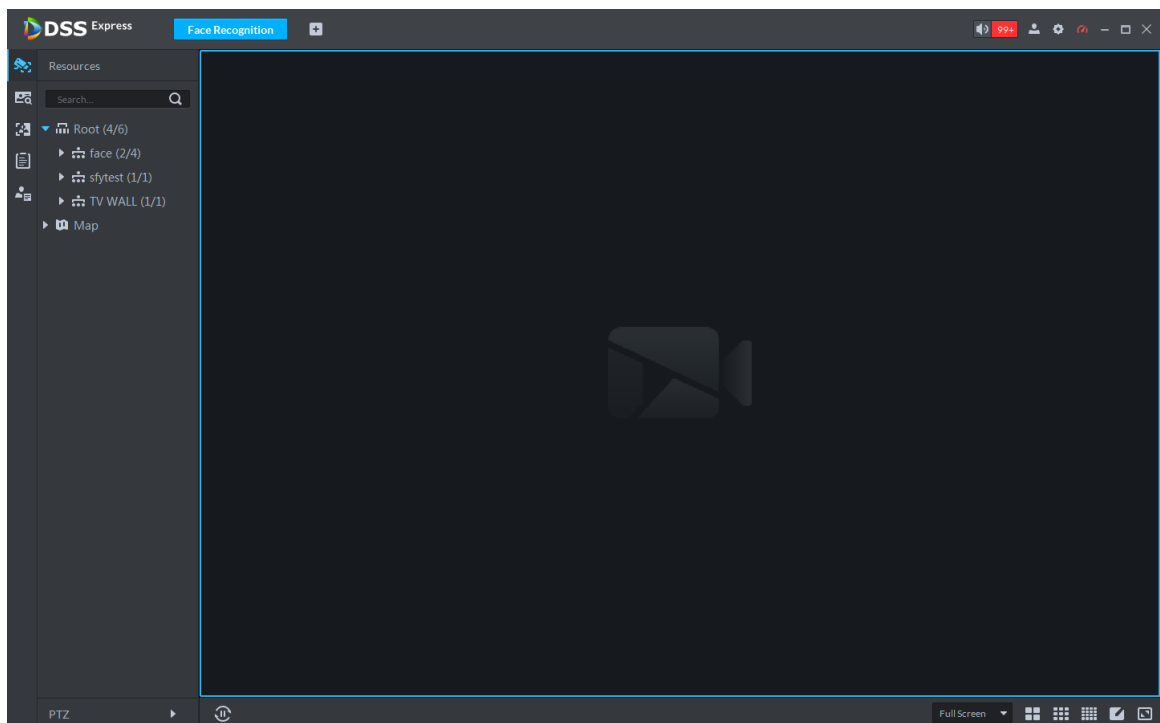
- Add face database, used to store personnel info, convenient for unified deployment over personnel in database. Meanwhile, you can edit and delete face database.
- Add personnel, you can add personnel into face database. Meanwhile, you can edit and delete personnel.
- Arm face database. After database is armed, face recognition device (such as FR camera, NVR and IVSS) compares snapshot with picture in database, if the similarity is $\geq$ threshold, then face recognition device (such as FR camera, NVR and IVSS) makes judgment that two pictures show the same person, and then report comparison record to the platform.

3.9.4.1 Adding Face Database

Step 1 On client homepage, click **Face Recognition**.

The system displays **Face Recognition** interface, see Figure 3-190.

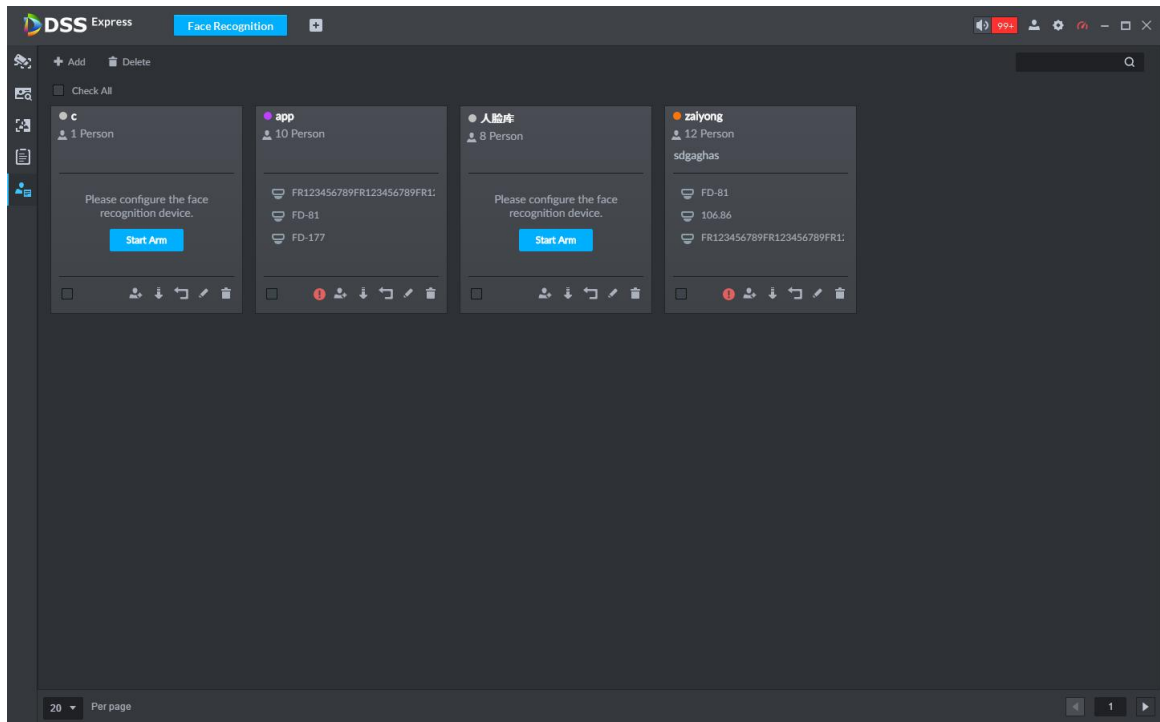
Figure 3-190 Face recognition



Step 2 Click .

The system displays **Face Database** interface, see Figure 3-191.

Figure 3-191 Face database management



Step 3 Click Add.

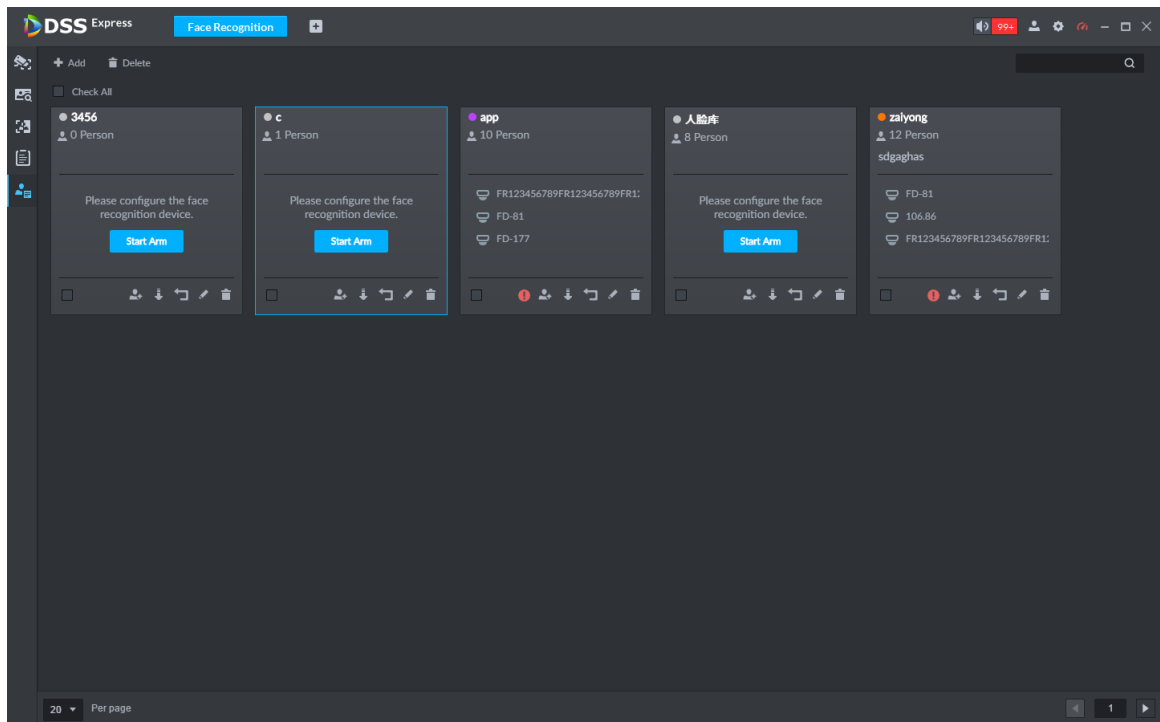
The system displays **Add face library** interface, see Figure 3-192.

Figure 3-192 Add face library

Step 4 Set face database info, click **OK**.

Library color is identified, the system displays new face database info, see Figure 3-193.

Figure 3-193 Added face database



3.9.4.2 Adding Personnel

The platform can add personnel info to face database singly or in batches, you can also register captured personnel into face database.

3.9.4.2.1 Adding Personnel Singly

Step 1 On **Face Database** interface, click  on face database or click face database, see Figure 3-194.

The system displays interface of adding personnel, see Figure 3-195.

Figure 3-194 Enter add interface

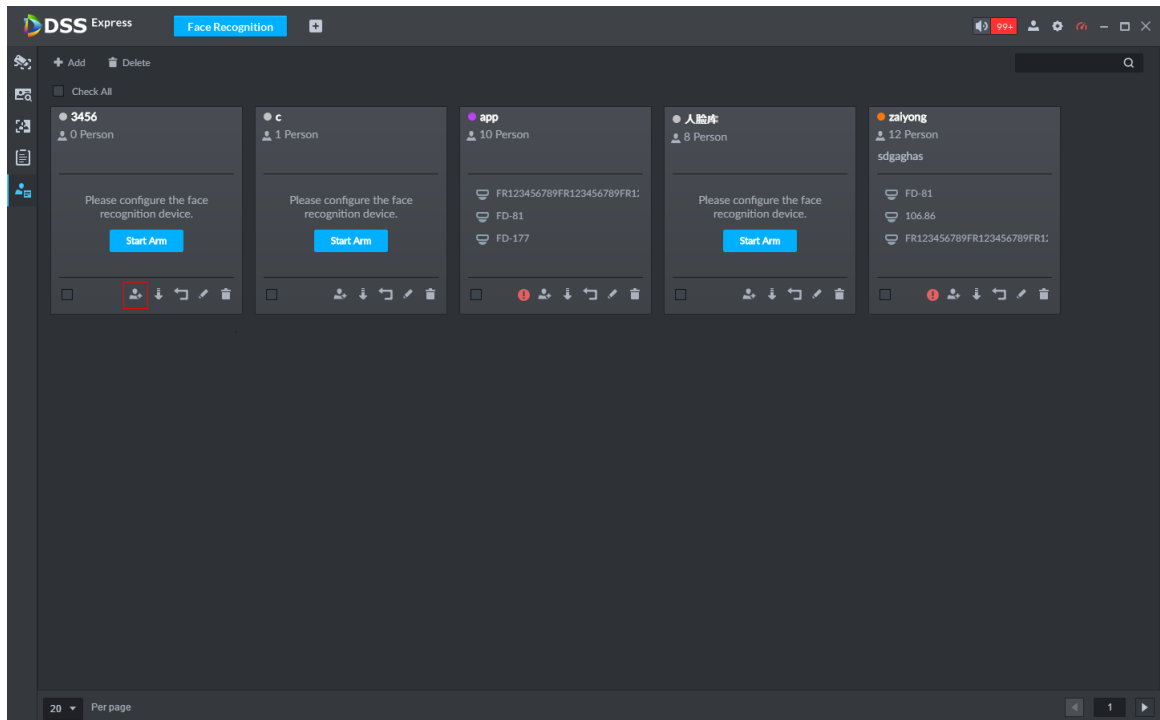
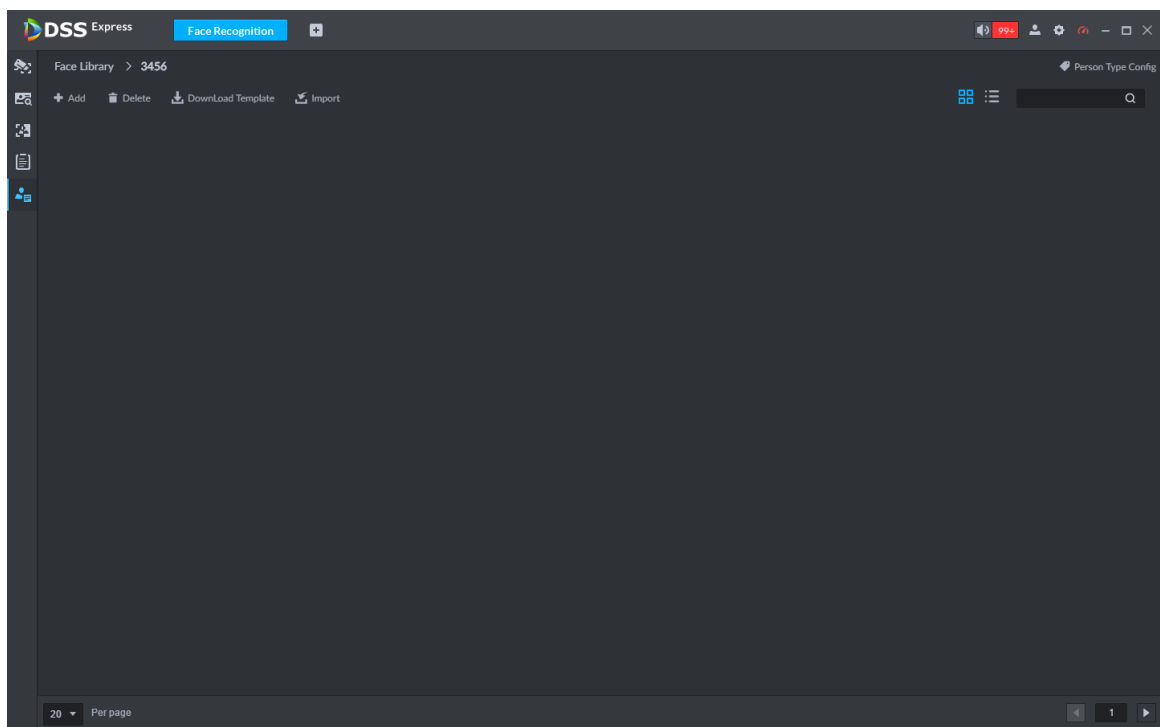


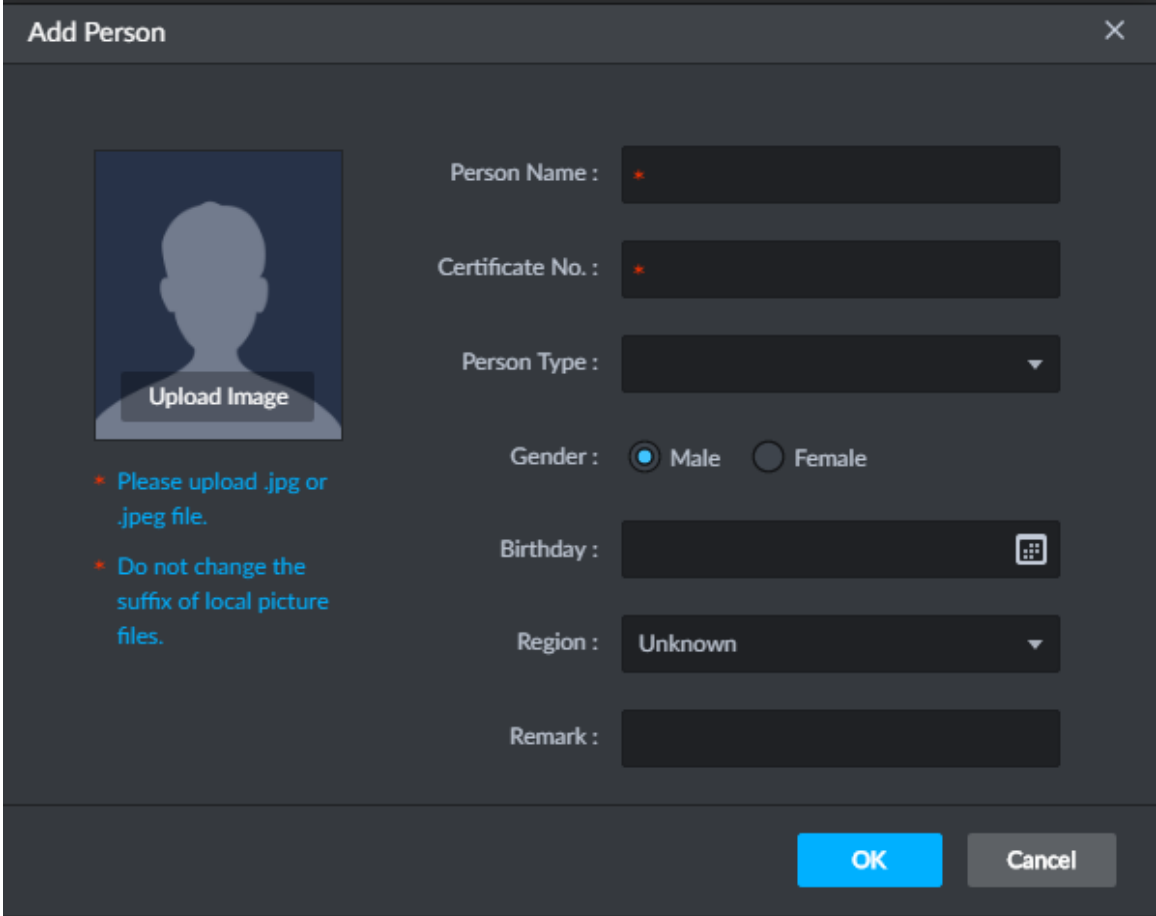
Figure 3-195 Add personnel (1)



Step 2 Click **Add**.

The system displays **Add Person** interface, see Figure 3-196.

Figure 3-196



The 'Add Person' dialog box features a dark gray background. On the left, there is a placeholder for a person's image with a silhouette and an 'Upload Image' button. Below this, two red asterisks indicate upload requirements: 'Please upload .jpg or .jpeg file.' and 'Do not change the suffix of local picture files.' To the right of the image area, there are several input fields: 'Person Name' and 'Certificate No.' both marked with a red asterisk; 'Person Type' is a dropdown menu; 'Gender' has radio buttons for 'Male' (selected) and 'Female'; 'Birthday' is a date picker; 'Region' is a dropdown menu currently showing 'Unknown'; and a 'Remark' text area. At the bottom right, there are 'OK' and 'Cancel' buttons.

Step 3 Click drop-down box of **Person Type**, select **Add Person Type**, and configure person type according to prompt on interface.

Person type is considered as person property to distinguish person.

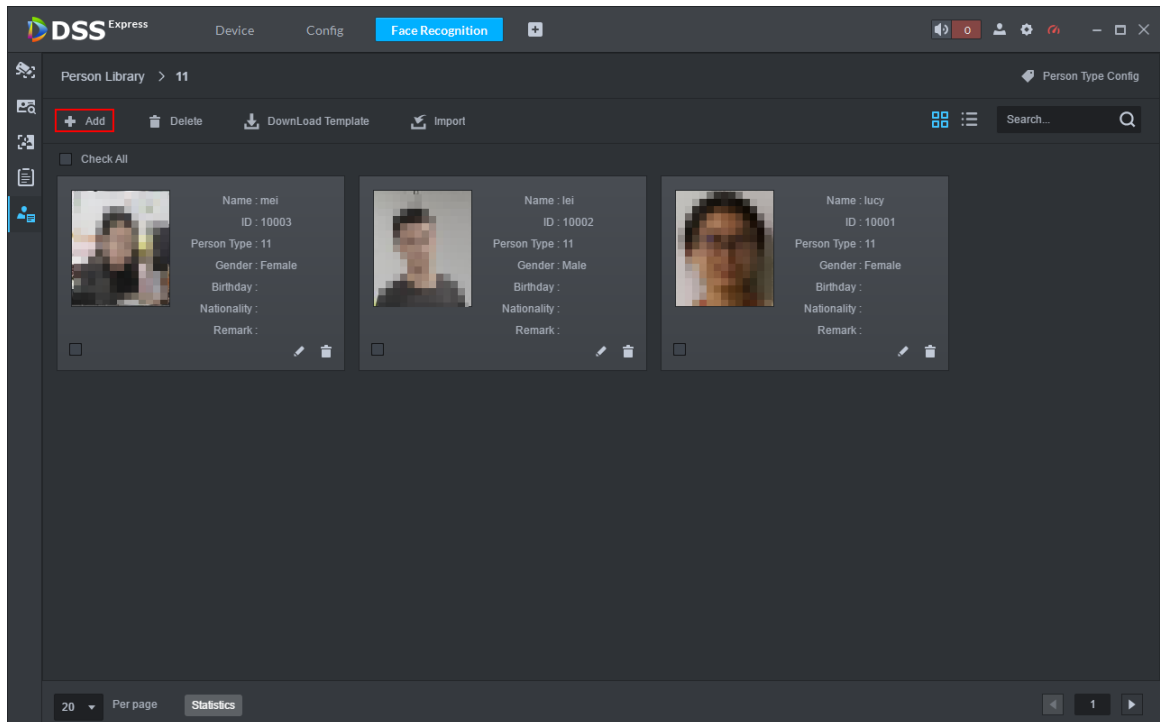


Click  **Person Type Config** on upper right corner of Figure 3-195, and you can configure person type as well.

Step 4 Upload person picture (You are required to clip the picture before upload), fill in person info, click **OK**.

The system displays info of added person, see Figure 3-197.

Figure 3-197 Add



3.9.4.2.2 Importing Personnel

Step 1 On **Face Database** interface, click  or the face database, see Figure 3-194.

The system displays interface of adding person, see Figure 3-195.

Step 2 Click **Download Template**, save template according to system prompt.

Step 3 Make upload file.

- 1) Edit personnel info excel table, Picture info is required to be in accordance with picture file name, see Figure 3-198.

Figure 3-198

Fill Requirements : 1.* indicates this blank must be filled. 2.ID : ID contains letters and numbers, letters are not case sensitive 3.Type: Fill in the type created on the web manager. 4.Gender: "Male"or"Female",you can selcet it from drop-down box. 5.Birthday : Year/Month/Day 6.Face Image: It must be jpg format, name in the blank must keep same with picture's name .							
*Name	*ID	*Type	*Gender	Birthday	Nationality	Remark	*Face Image
Jerry	35125	Staff	Male	1988/5/6	China	Joined on October 2th	face.jpg

- 2) Compress personnel picture and info excel tables into zip/rar/7z.

Step 4 Click **Import**, and upload compression package according to interface prompt.
The system displays import progress and result.

3.9.4.2.3 Captured Person Register Library

Step 1 Enter person register interface.

Support following methods to enter register interface.

- On **Face Recognition** interface, double click person snapshot, see Figure 3-199.
Enter person detail interface, see Figure 3-200. Click  and enter register interface.

Figure 3-199 Double click snapshot

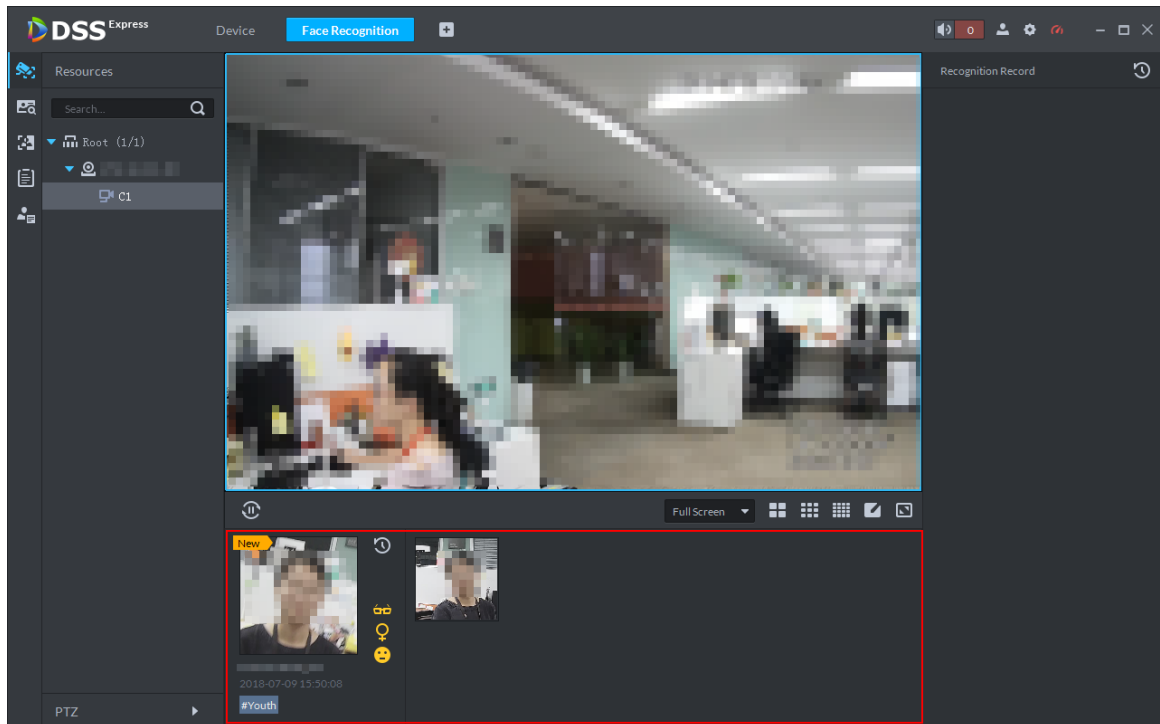
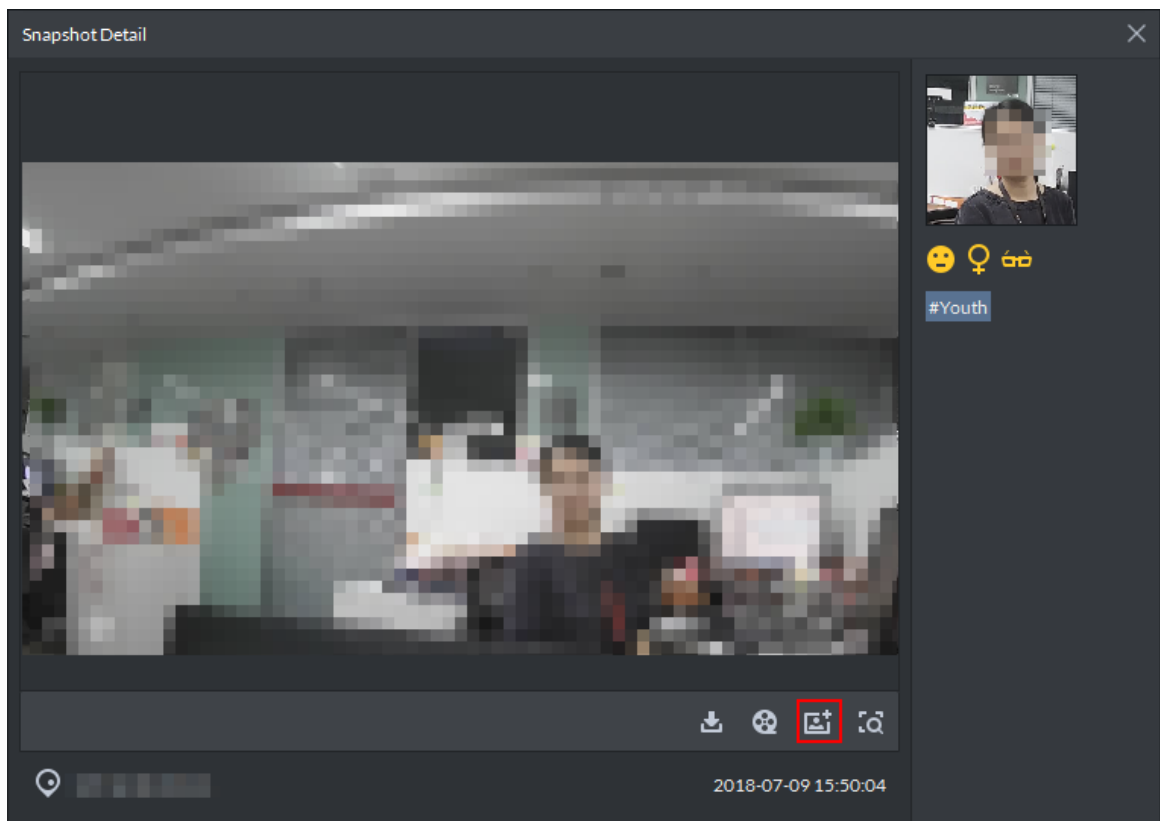
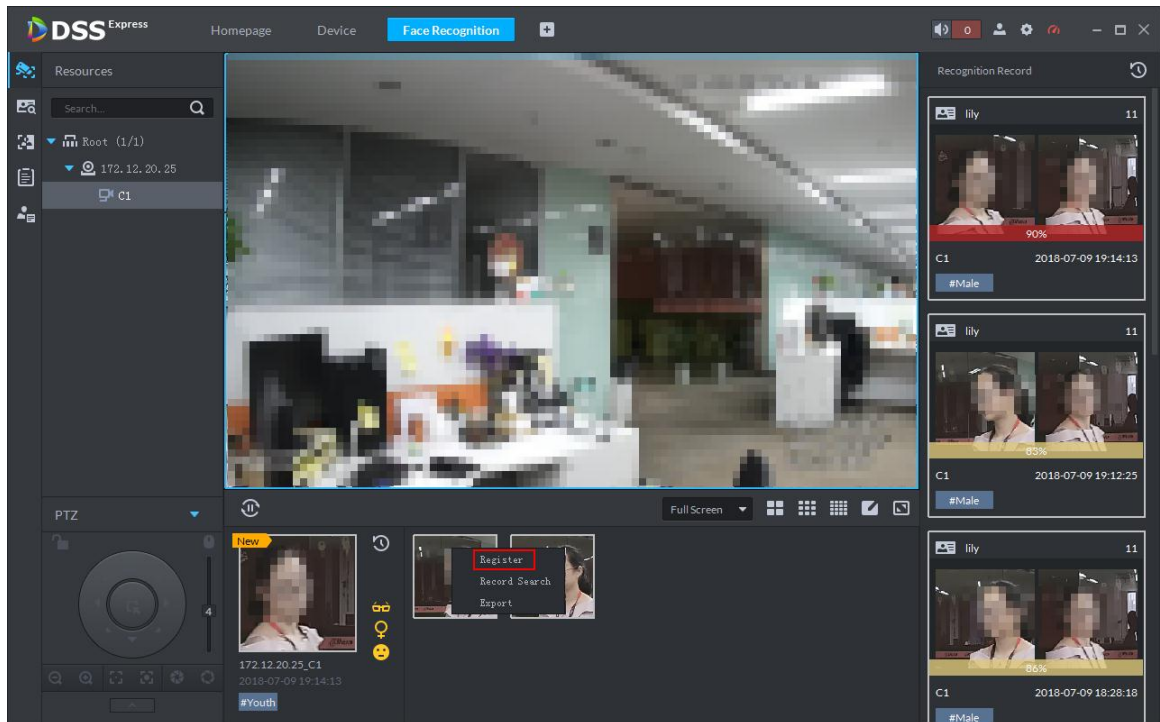


Figure 3-200 Person detail



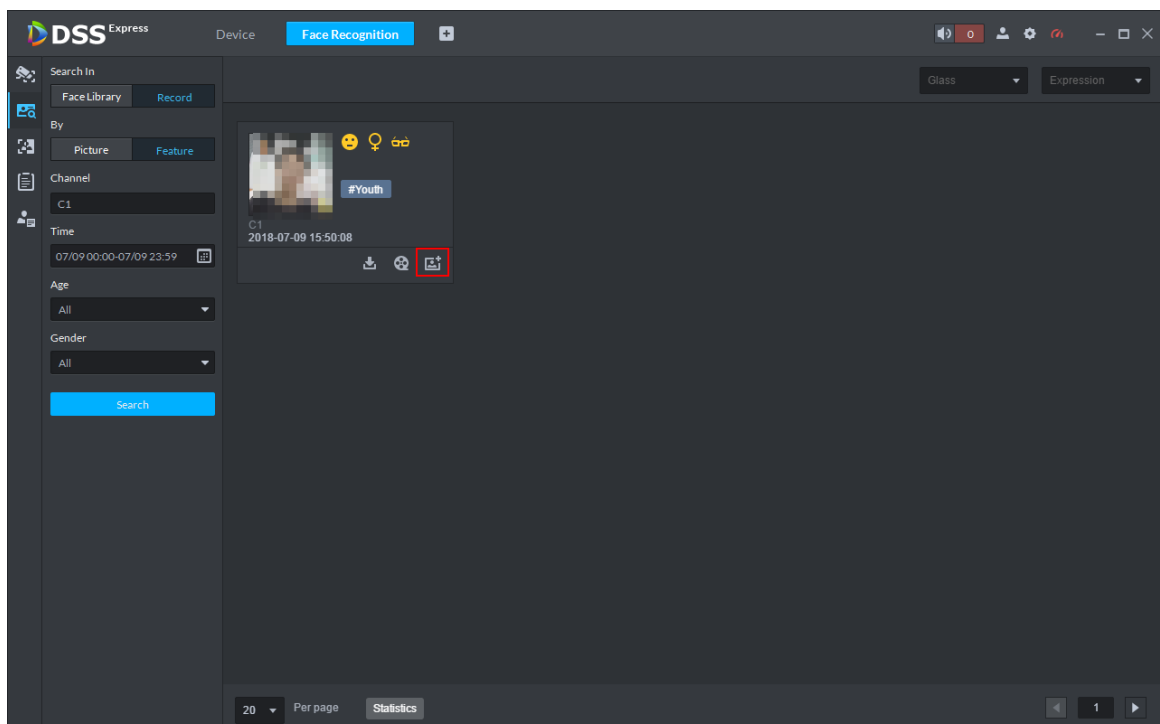
- On **Face Recognition** interface, move mouse to person snapshot, right click and select **Register**, and enter register interface. See Figure 3-201.

Figure 3-201 Register captured person



- On record search interface, click  and enter register interface, see Figure 3-202. Or double click searched result, enter person detail, click  and enter register interface.

Figure 3-202 Record search



Step 2 Select face database you want to add, enter person info. Click **OK**, see Figure 3-203.

Figure 3-203 Register person

The screenshot shows a 'Snapshot Detail' window with a dark theme. It contains several input fields and buttons. On the right side, there is a small image of a person's face, a gender icon (female), and a tag labeled '#Youth'. At the bottom right, there is a timestamp '2018-07-09 15:50:08'.

Field	Value
Face Library	11
Name	lily
ID	10006
User Type	11
Gender	Male
Birthday	2018-07-09
Nationality	
Remark	

Buttons: Confirm, Cancel

3.9.4.3 Arming Face Database

Step 1 On **Face Recognition** interface, click .

The system displays **Face Database** interface.

Step 2 Click **Start Arm** or  on the face database, see Figure 3-204.

The system displays **Face Config** interface, see Figure 3-205.



- Start Arm button only displays after face databased is created. After armed, the button will no longer display on the interface.
- Click  and cancel arm.

Figure 3-204 Arm button

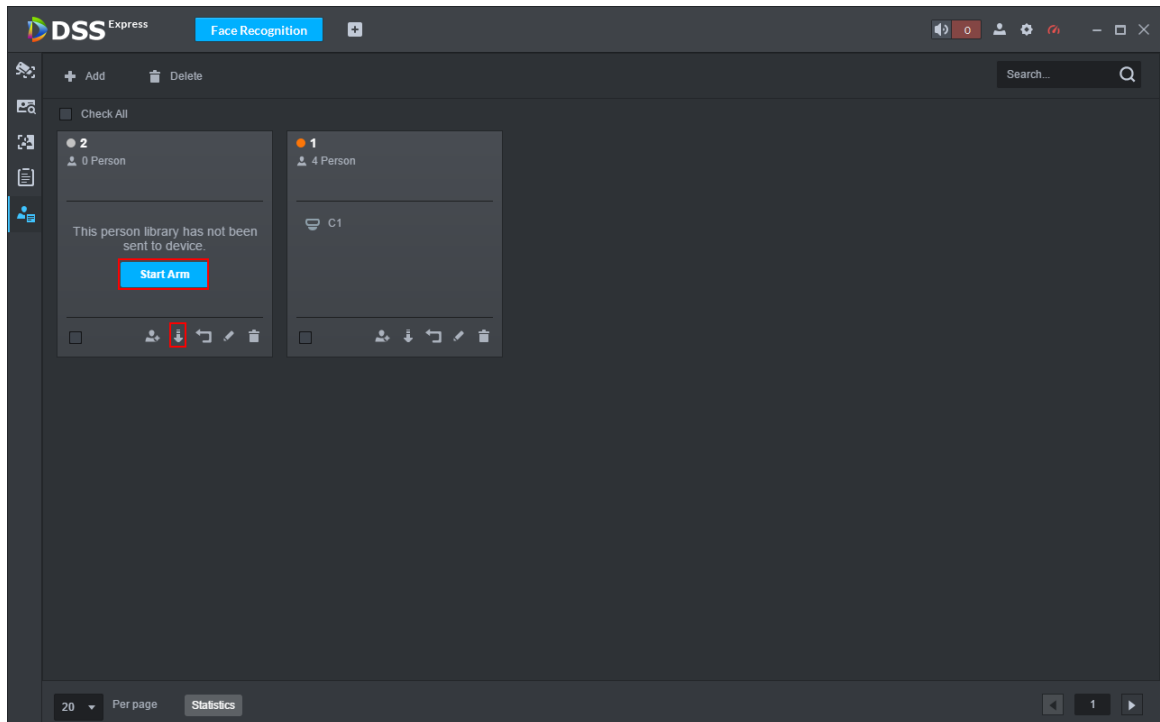
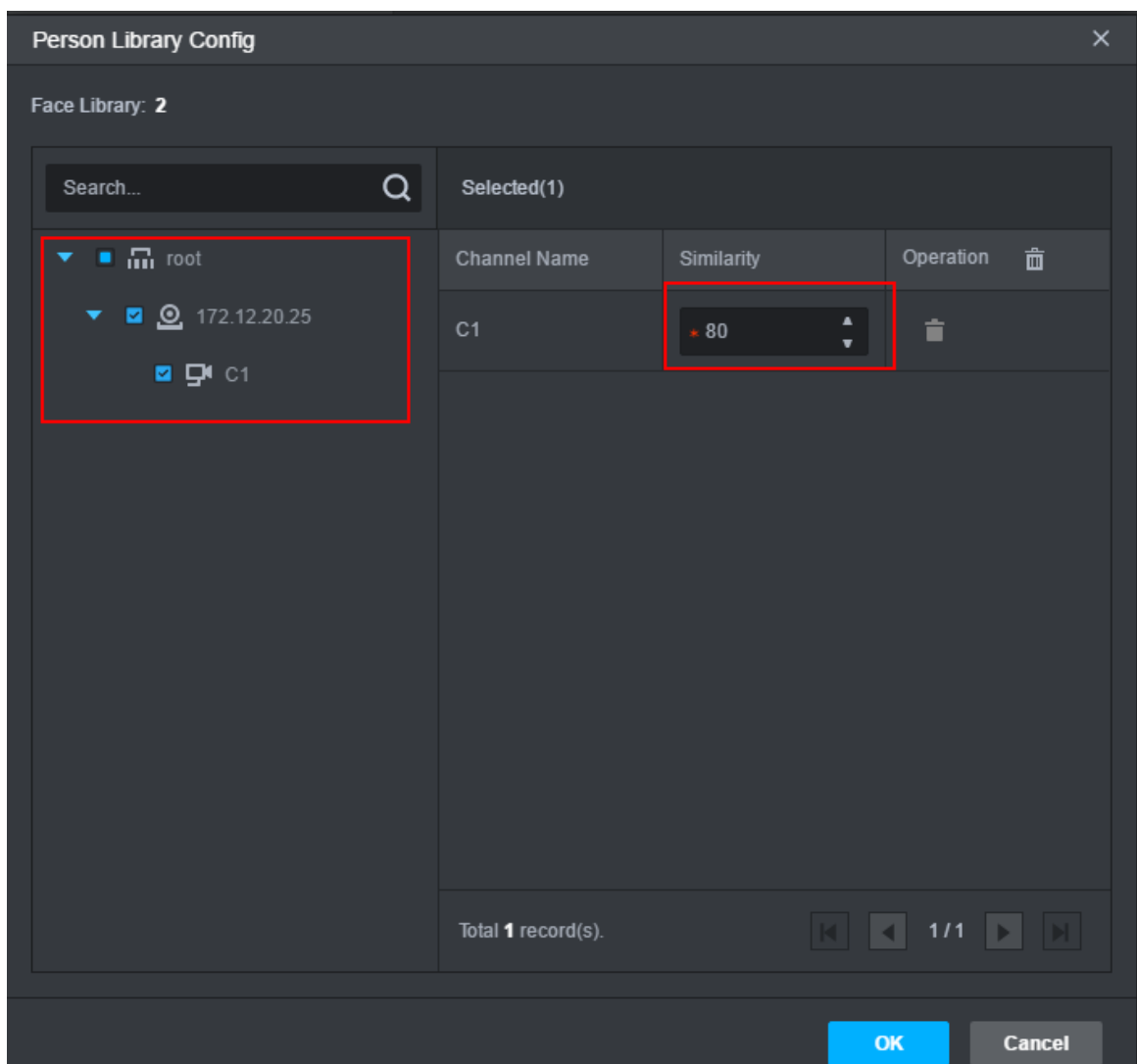


Figure 3-205 Arm config



Step 3 Select the channel you want to arm (multiple choice supported), set similarity, and click **OK**.

Recognition record is reported when similarity is $\geq$ threshold.

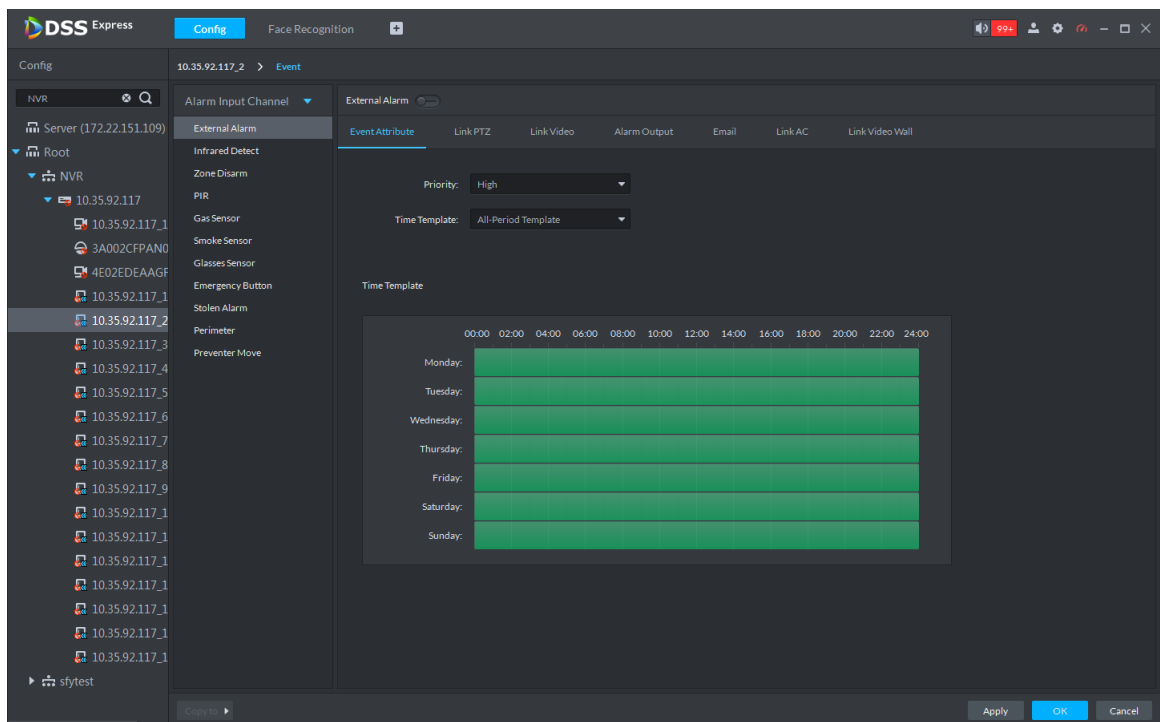
3.9.5 Setting Alarm Event

This chapter only introduces related alarm about face recognition, for more alarm event setting, see **3.2.4 Setting Alarm Event**. Face recognition alarms include following types.

- Person type alarm, alarm is triggered when target person type is recognized. Person type is set when adding person.
- Face recognition alarm, alarm is triggered when face database is recognized. The classification under face recognition alarm is face database name.

Set alarm event, see Figure 3-206.

Figure 3-206 Face recognition alarm event



3.9.6 Face Recognition Application

Application of face recognition business client includes:

- Live Preview
Live preview supports view of live view, person snapshot and recognition record. Meantime it supports view of corresponding panorama and link video of person snapshot, download link video, sign up snapshot person and etc.
- Snapshot Search
Via feature info or person picture, search matched person in face library or snapshot record.
- Recognition Search
Via set feature info, search matched recognition record in recognition record.
- Report

For a certain channel, according to snapshot time, snapshot person age, create a report of snapshot person.



Face snapshot storage info

- Snapshot is stored in server installation path
“..\\WEBCLIENT\\webclient\\apache-tomcat\\webapps\\upload\\face”. Pictures are stored for 30 days by default, if you want to modify storage days, refer to 3.2.1.1 Setting Message Storage
- Take 2 snapshots a time, one face snapshot and the other panoramic picture. In general the picture size is 100KB.
- Snapshots are stored for 30 days by default. If you want to modify details, refer to 3.2.1.1 Setting Message Storage

3.9.6.1 Face Recognition



When setting storage space, local storage disk must reserve a general picture disk; otherwise, snapshot cannot be seen.

3.9.6.1.1 Live View

View and recognize video, capture face and recognize face info.

Step 1 On Face Recognition interface, click .

The system displays **Face Recognition** interface.

Step 2 Enable realtime monitoring, enable realtime monitoring interface, and see Figure 3-207.

- Select monitoring window, double click channel on the left and enable live monitoring.
- Drag channel on the left to monitoring window.

Figure 3-207 Live view

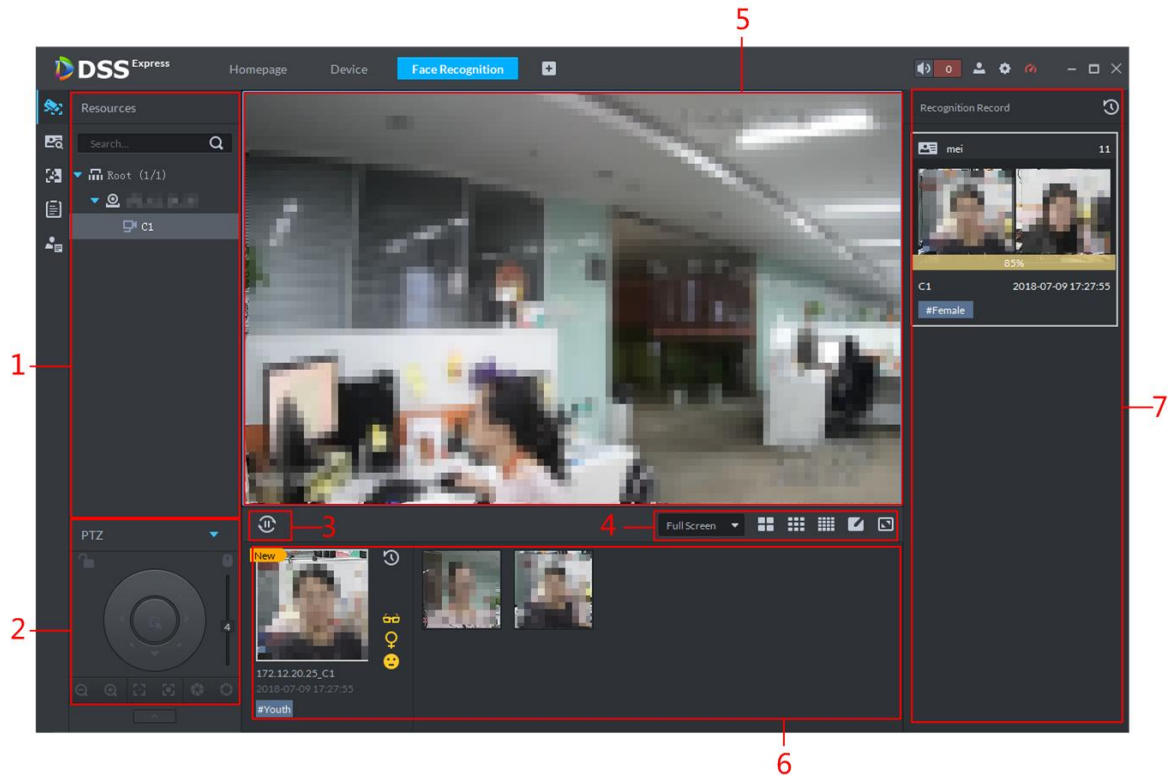
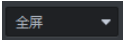


Table 3-33 Live video interface description

No.	Name	Description
1	Device Tree	Display device and device channel info. - Right click root node, support display type. You can set display by name and IP. Support ranking, by ascending and descending and default sequence. Support to hide and show offline node. - Right click device, select tour, support to set all channel tour preview of this device. After you enter touring, if you want to stop touring, then you can right click in preview video, select "Stop Touring", to end tour. - Right click channel to enter Record Configuration and Event Configuration.
2	PTZ	Speed dome adjust. If you want to expand PTZ operation zone, click  behind PTZ to hide PTZ area. When PTZ area is hidden, click  behind PTZ to expand PTZ zrea.
3	Pause Refresh/Start Refresh	, page shows this icon, snapshot area does not refresh face snapshot. Click this icon, live refresh face snapshot. , page shows this icon. Snapshot display area shows refresh of face snapshot. Click this icon, refresh face snapshot.

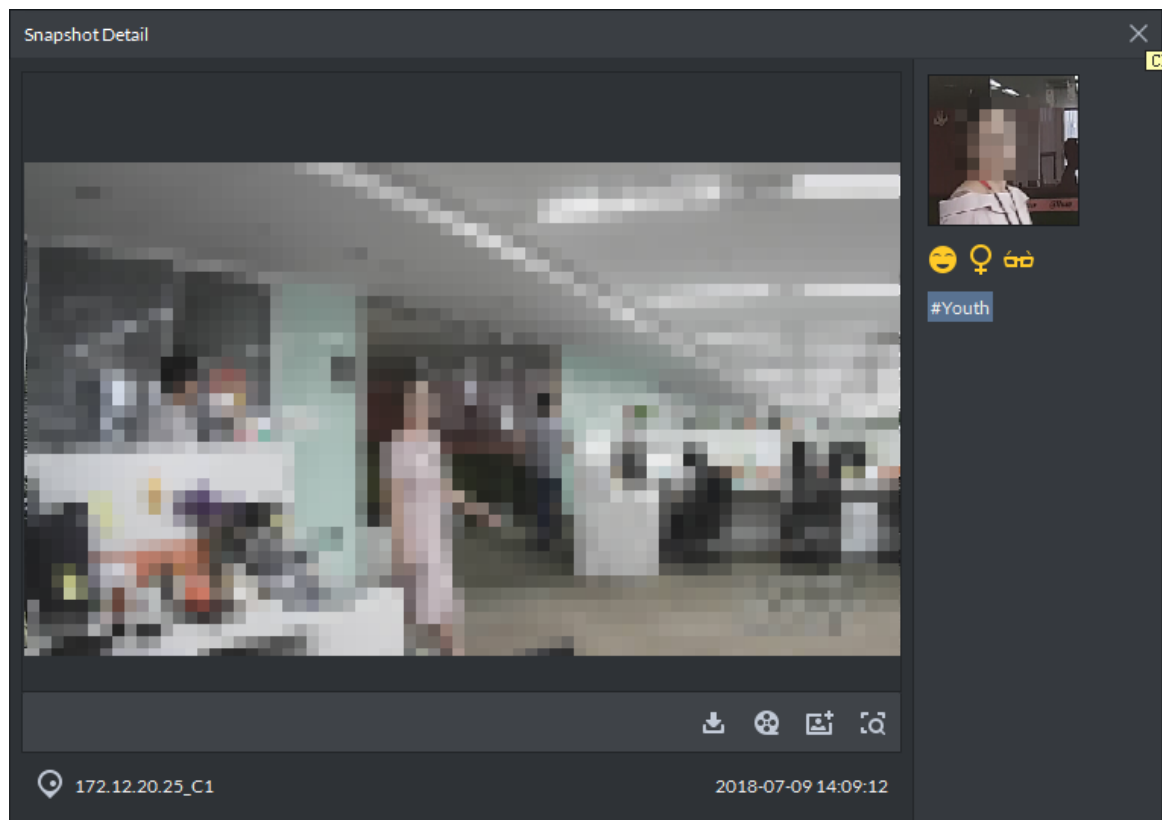
No.	Name		Description
4		Picture Display Scale	Support full screen and original scale.
		Window Switch Number	Support switch display of window quantity, and customized setup.
		Full Screen	Show full screen.
5	Monitor Window		Show channel preview channel. - Multiple window/single window switch Multiple window display mode, double click window, switch to single display mode and double click again to return to multiple window display mode. - Full screen mode Right click window to select to enter full screen mode. If it is already in full screen mode, right click to exit full screen. - Exit tour. - If it is in touring mode, to stop touring, you can right click in the preview window and select "Stop Tour".
6	Person Snapshot Record Display Area		Show snapshot face snapshot. Move mouse to person snapshot and right click the snapshot, you can: - If this person is only snapshot but not recognized ◇ Select "sign up", add person to library following prompt. ◇ Select "record search", go to snapshot search page and search picture by picture. In snapshot history record, search all snapshots of this person. ◇ Select "Export", save person snapshot to client locally. Path is default path: ..\DSS Express\Client\Picture\Face\Export\Capture. - If this person is recognized ◇ Select "Recognition Record Search", go to search page, and in snapshot history record search all recognition records of this person. ◇ Select "Export", save person snapshot and pictures this person in library all to client locally. Path is default path: ..\DSS Express\Client\Picture\Face\Export\Recognize. Double click person snapshot, to view person details, including snapshot person cutout and panorama.

No.	Name	Description
7	Recognition Record Display Area	Show recognition record. • Move mouse to person snapshot, and right click support to: ◇ Select“Recognition Record Search” , go to recognition search page, and in snapshot history record, search all recognition records of this person. ◇ Select“Export”,and save person snapshot and snapshot of this person already uploaded to library all to client locally, default path is ..\DSS Express\Client\Picture\Face\Export\Recognize。 • Double click recognition record, you can view person cutout, panorama, used to person picture and info in face library. • Click  at the upper right corner, go to recognition search page.

3.9.6.1.2 Viewing and Processing Snapshot Detail

- View snapshot detail
In the area of person snapshot record, double click person snapshot to view face cutout and panoramic picture, see Figure 3-208.

Figure 3-208 Snapshot detail



- Register captured person

Step 1 On snapshot detail window, click .

The system displays **Snapshot Detail** interface, see Figure 3-209.

Figure 3-209 Snapshot detail

Snapshot Detail

Face Library:

Name:

ID: User Type:

Gender: ☒ Male ☐ Female Birthday: 2018-07-10

Nationality:

Remark:

Confirm Cancel

2018-07-10 13:34:56

Step 2 Configure person info, click **OK**.

- View video

On the snapshot detail window, click  and enter record playback interface. If corresponding video exists in central server or device, then playback video, otherwise, system prompts no record file. Video source priority is central server > device.

- Download video

On snapshot detail window, click  and enter download center, download video according to requirement. For details, refer to **3.5.1.8 Downloading Record**.

- Search record

On snapshot detail window, click  to enter record search page, search picture by picture. See Figure 3-210. Set search time and channel, click **Search** to search result. See Figure 3-211.

Figure 3-210

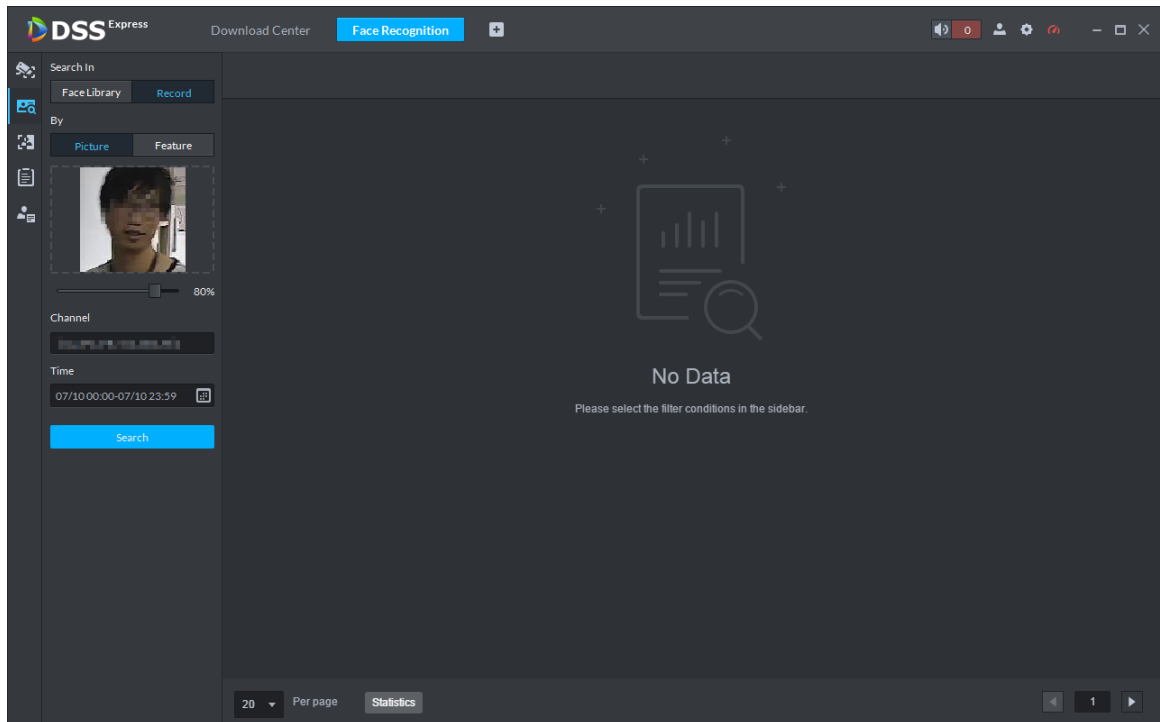
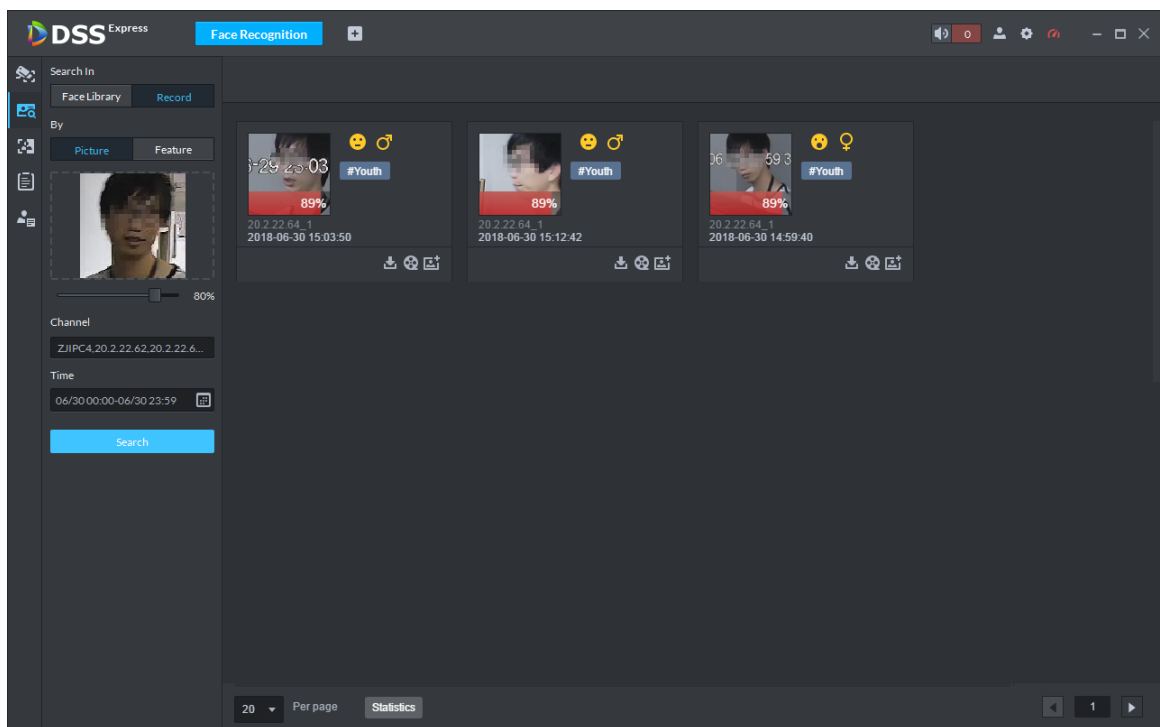


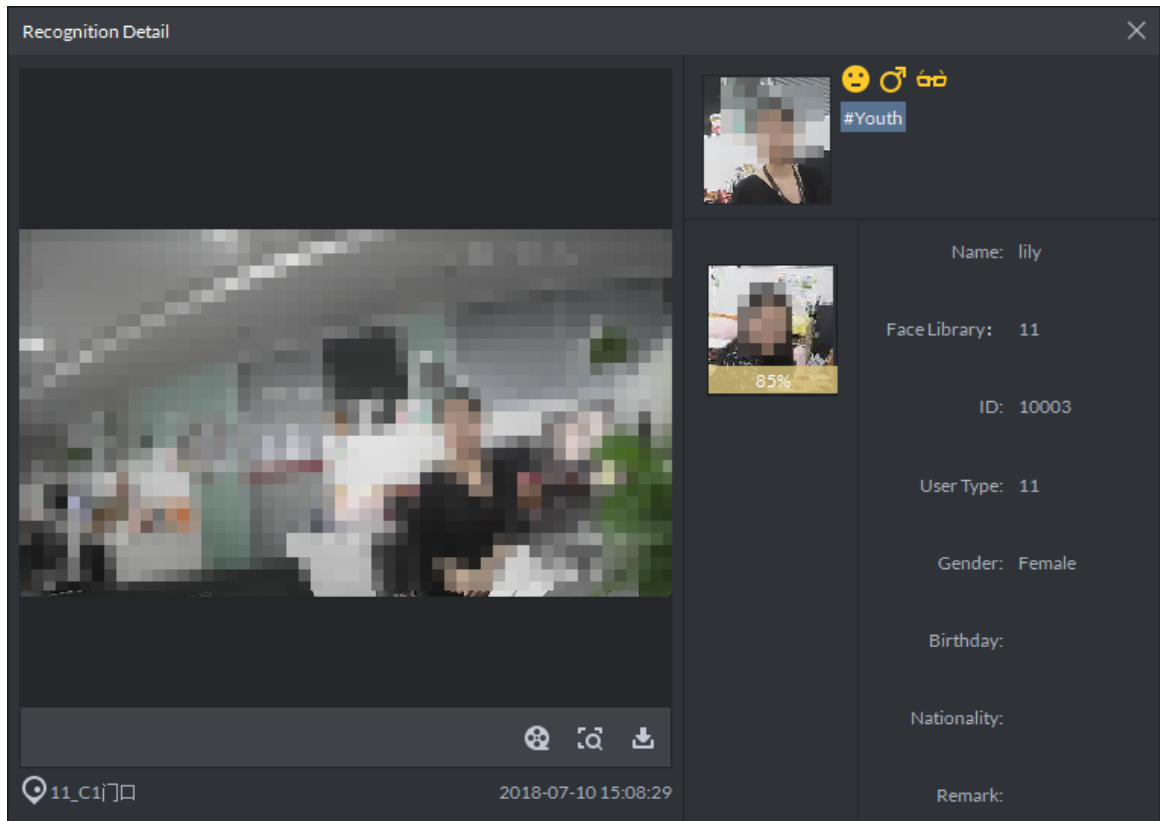
Figure 3-211



3.9.6.1.3 Viewing and Processing Recognition Record Detail

- View recognition detail
In recognition record display area, double recognition record to view snapshot person cutout, panorama, person picture and person info used to compare, see Figure 3-212

Figure 3-212 Recognition detail



- View video

On the snapshot detail window, click  and enter record playback interface. If corresponding video exists in central server or device, then playback video, otherwise, system prompts no record file. Video source priority is central server > device.

- Download video

On snapshot detail window, click  and enter download center, download video according to requirement. For details, refer to **3.5.1.8 Downloading Record**.

- Search record

On snapshot detail window, click  to enter record search page, search picture by picture. See Figure 3-213. Set search time and channel, click **Search** to search result. See Figure 3-214.

Figure 3-213 Search recognition

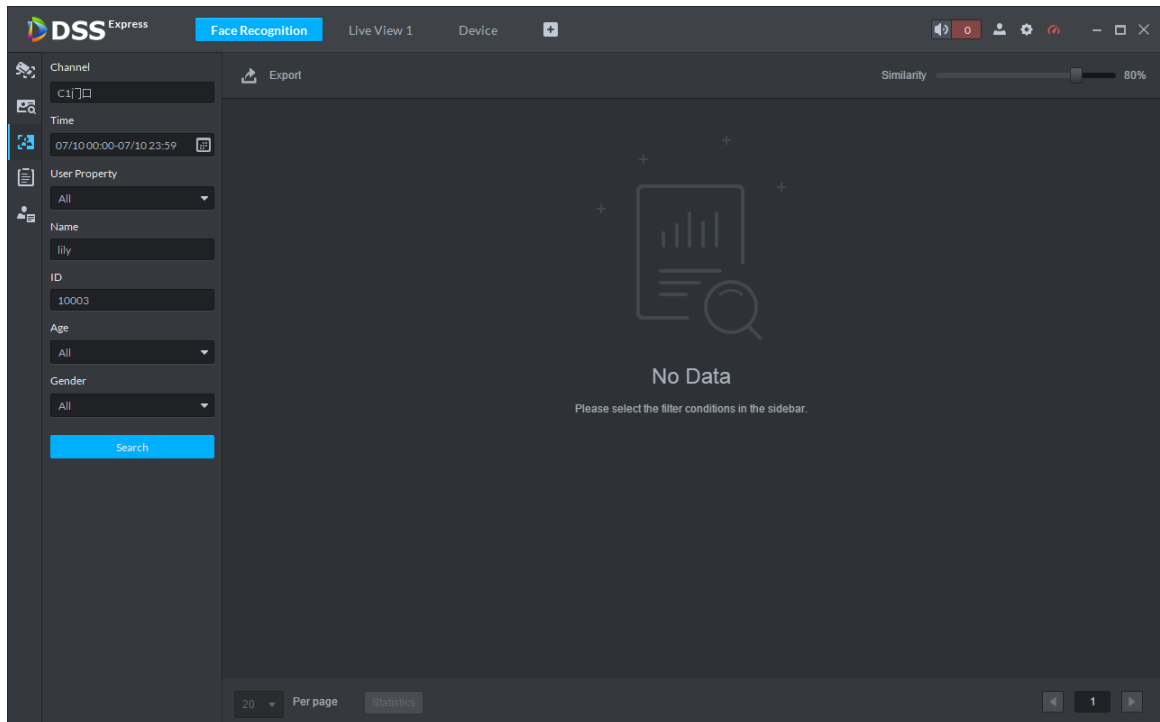
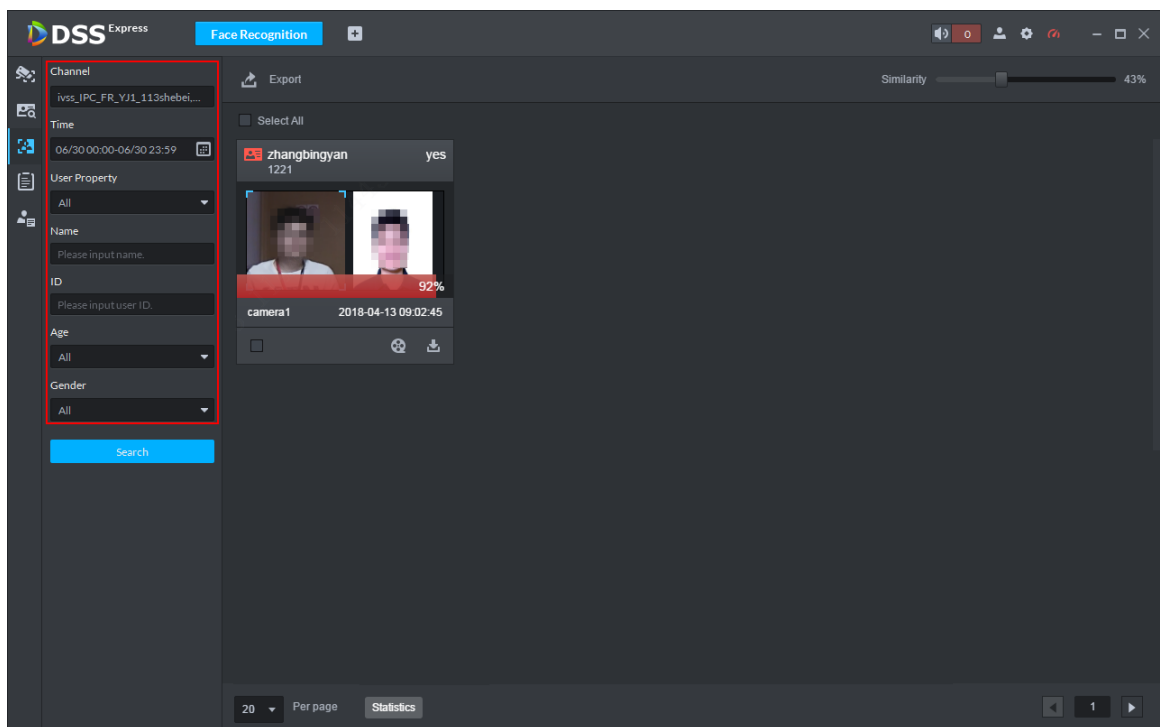


Figure 3-214 Search result



3.9.6.2 Searching Person

You can search qualified person by features or pictures. The supported search methods are shown as follows.

- Set feature info, search person who conforms to conditions in face database.
- Import picture, search person whose similarity conforms to threshold in face database.
- Set feature info, search person who conforms to conditions in face database. You can view and search person movement track on map.

- Import picture and search person whose similarity conforms to threshold in snapshot record. You can view and search person movement track on map.

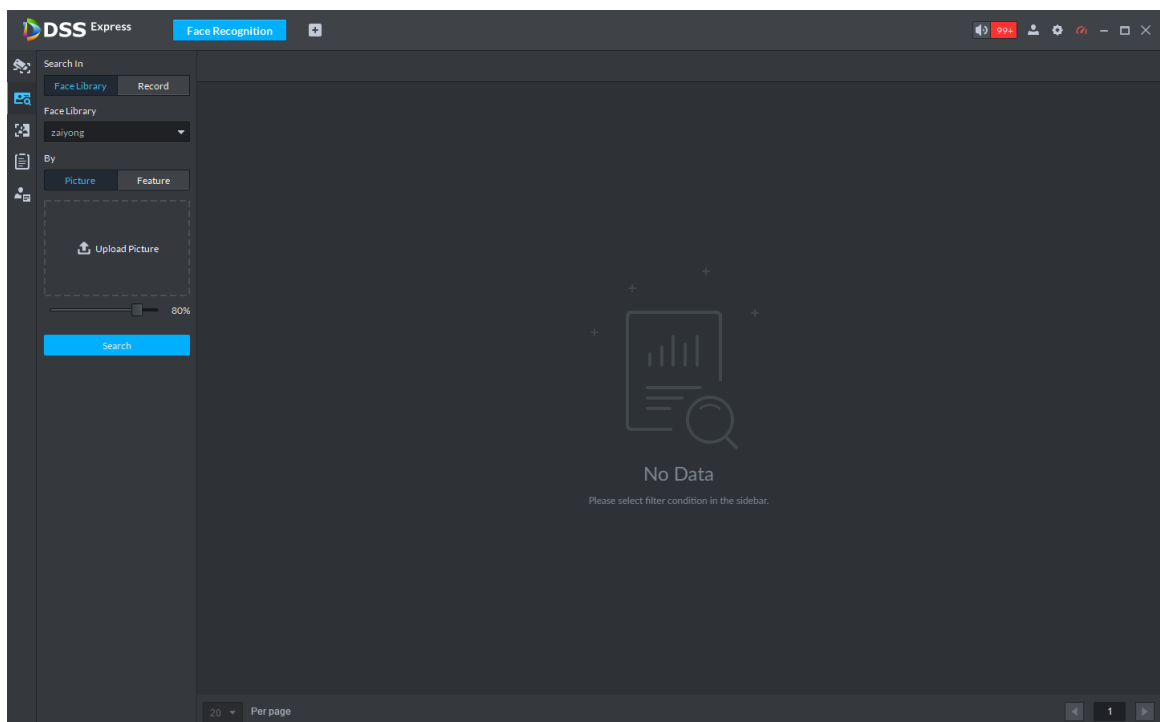


- If the device does not support search by picture, then the platform cannot search by picture either. If not supported by device, the platform prompts that channel not supported when selecting channel.
- In this chapter, it takes search by importing picture as an example to introduce operation. You can refer to the operation in this chapter for other search operations.

Step 1 On Face Recognition interface, click .

The system displays **Face Search** interface, see Figure 3-215.

Figure 3-215 Face search



Step 2 Select **Record** and **Picture**; click **Upload Picture**; set similarity; click **Search**.

You need to set search condition during operation.

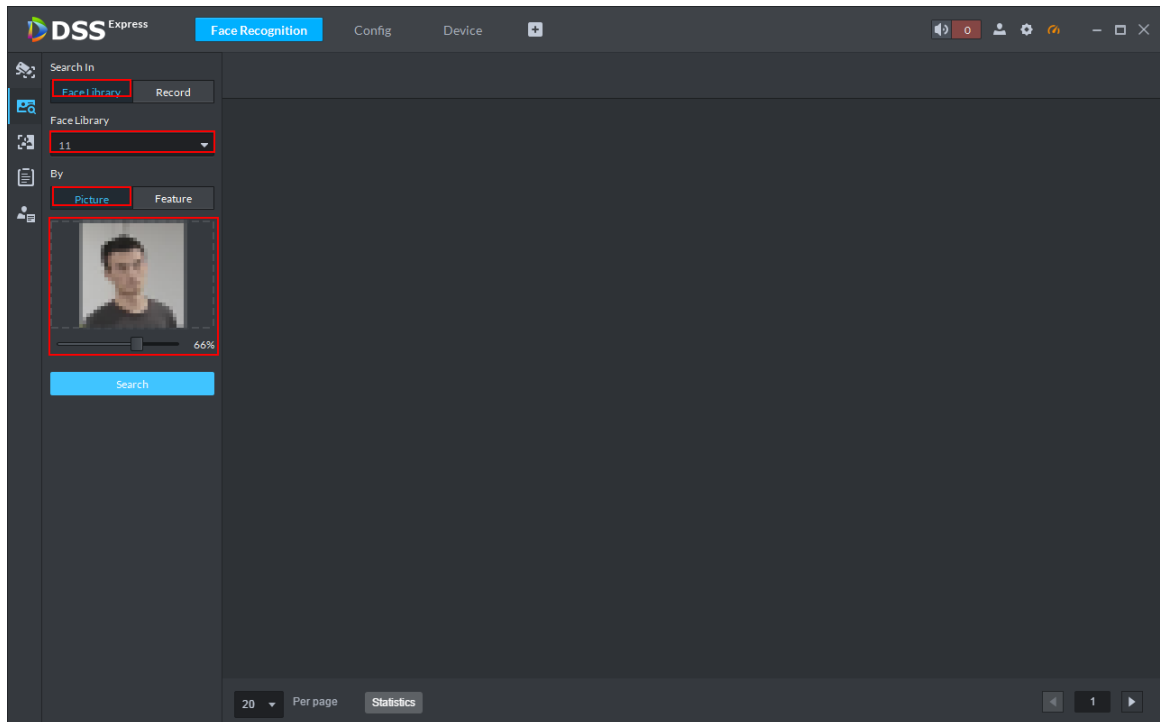
- Select **Face Library** and you can search from the face library, select **Record** and you can search from snapshot records.
- Select **Picture** and you can search by picture, you are required to upload picture and set similarity; select **Feature** and you can search by feature info.

Searched result is shown in Figure 3-216.



Similarity is not displayed if you search by feature.

Figure 3-216 Search by picture



The supported operation of search result is similar.



The following are the operations of snapshot record search results, if it is the face database

search result, then only support click , skip to recognition search interface, and search the recognition record of the person.

- Search detail
Double click to view detail.
- Download video

On snapshot detail window, click  and enter download center, download video according to requirement. For details, refer to **3.5.1.8 Downloading Record**.

- View video

On the snapshot detail window, click  and enter record playback interface. If corresponding video exists in central server or device, then playback video, otherwise, system prompts no record file. Video source priority is central server > device.

- Register captured person to face database

Click  and display window of registered person.

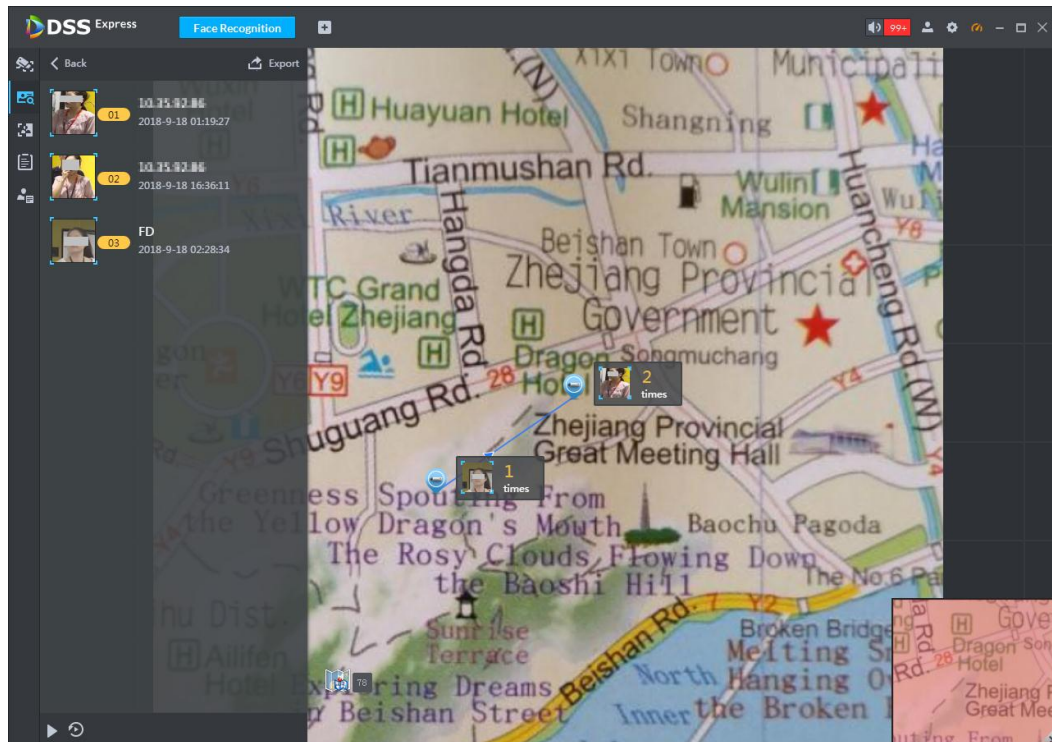
- View track on map



View track, you are required to drag device to map for display in advance. For more details, see 3.2.6 Configuring Emap.

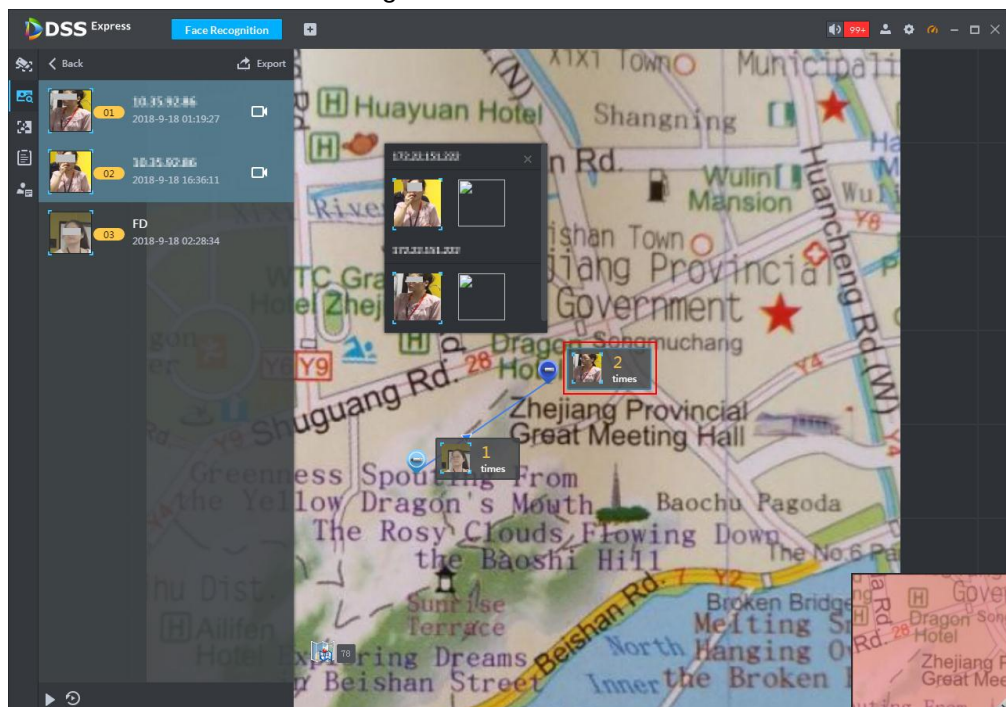
Click **Generate Track**, and display track map, see Figure 3-217.

Figure 3-217 Generate track



- ◇ Double click the device on the map, and it will display all the snapshot records of the device, the device record is marked by blue in the left snapshot record list. See Figure 3-218.

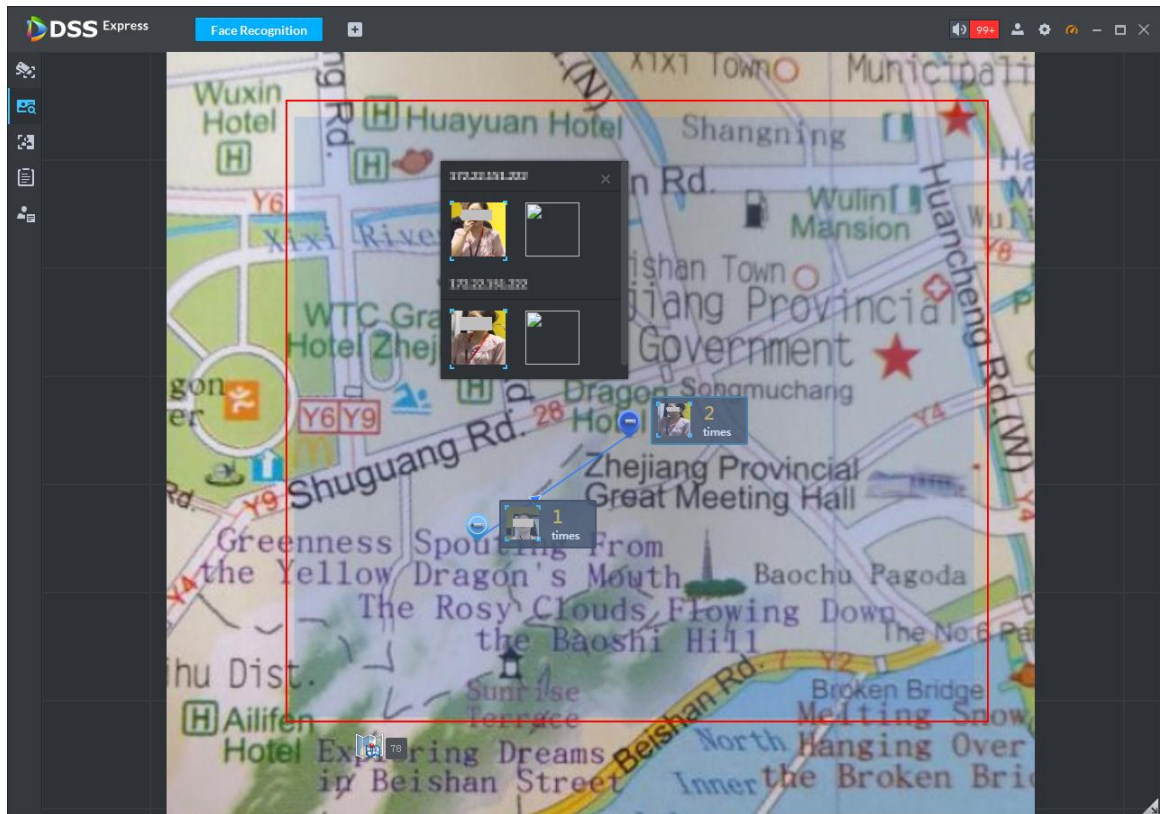
Figure 3-218 View detail



- ◇ Click  to play movement trajectory; click  to pause movement track; click  to play again.
- ◇ Click  to playback video in the left snapshot record list.

- ◇ Playback video calls the stored video on the face recognition device; there will be no playback video if the device fails to store relevant video.
- ◇ Export trackcture.
- ◇ Click **Export**, press left mouse button on the map, and drag the mouse the select region. See Figure 3-219.
- ◇ Save it in the local as the form of picture according to the interface prompt.

Figure 3-219 Export track



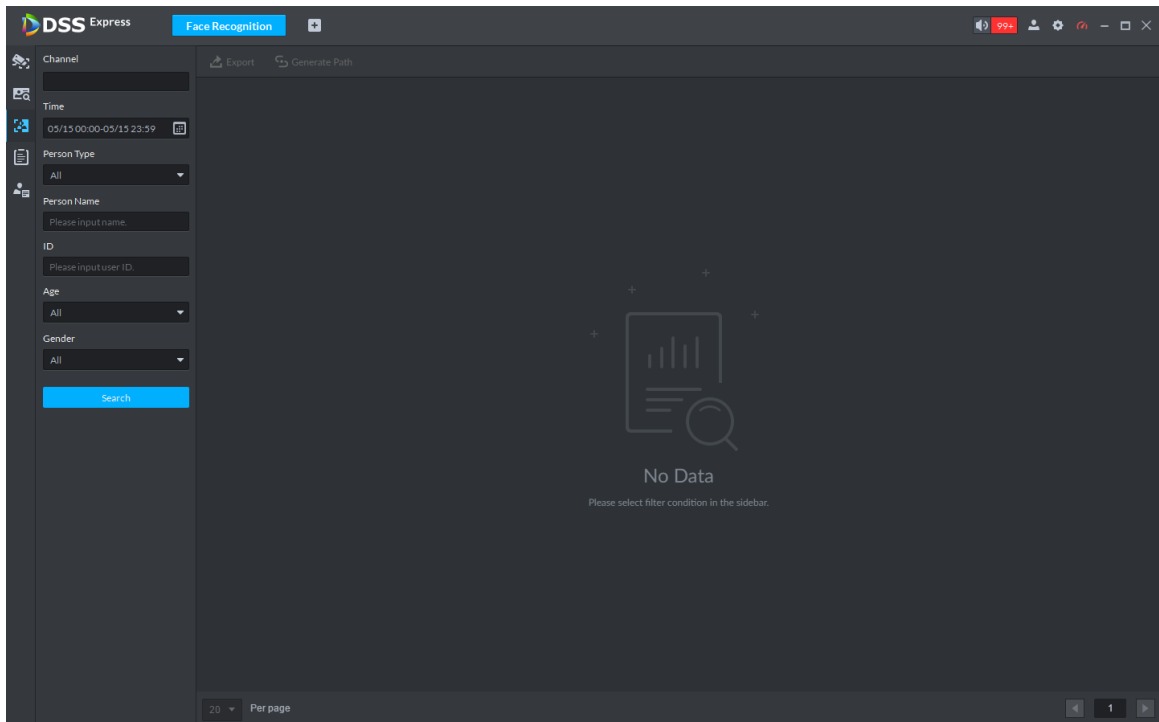
3.9.6.3 Searching Recognition Record

You can search qualified record from recognition record.

Step 1 On **Face Recognition** interface, click .

The system displays **Recognition Search** interface, see Figure 3-220.

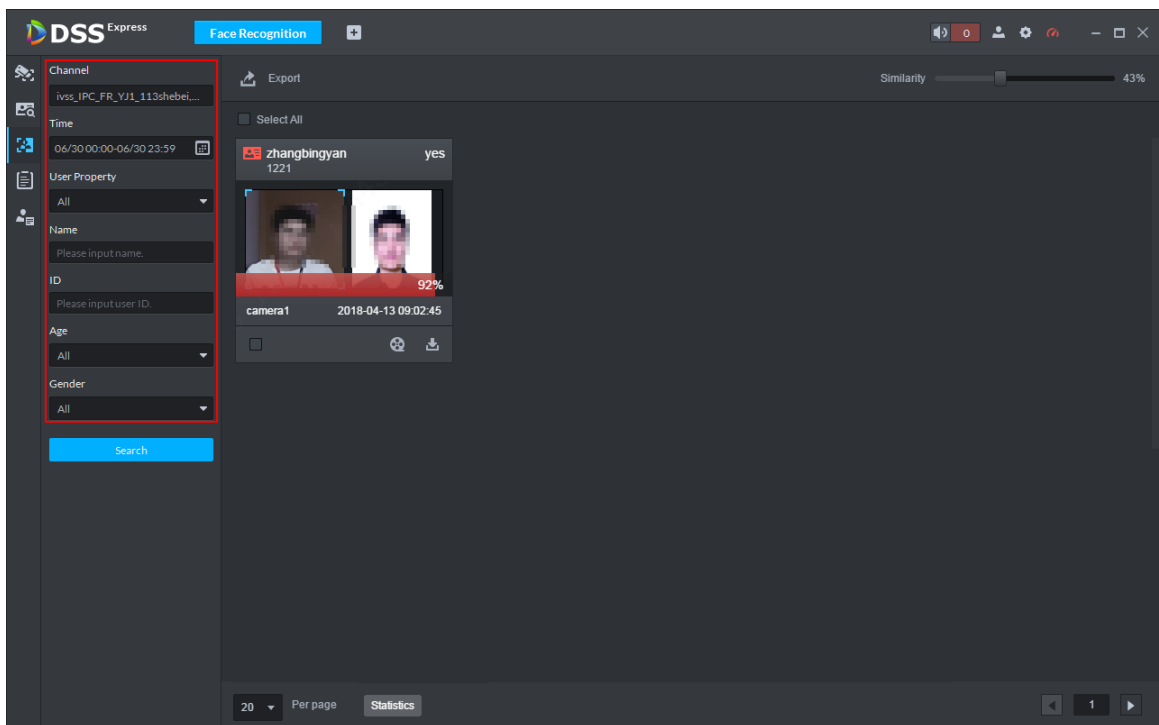
Figure 3-220 Recognition search



Step 2 Set search condition, click **Search**.

The system displays search result, see Figure 3-221.

Figure 3-221



3.9.6.4 Showing Report

Step 1 On **Face Recognition** interface, click .

The system displays **Report** interface.

Step 2 Select channel of data report you want to view (multiple choice), select data period (day, week, and month), and click **Search** to create a report of the selected period.

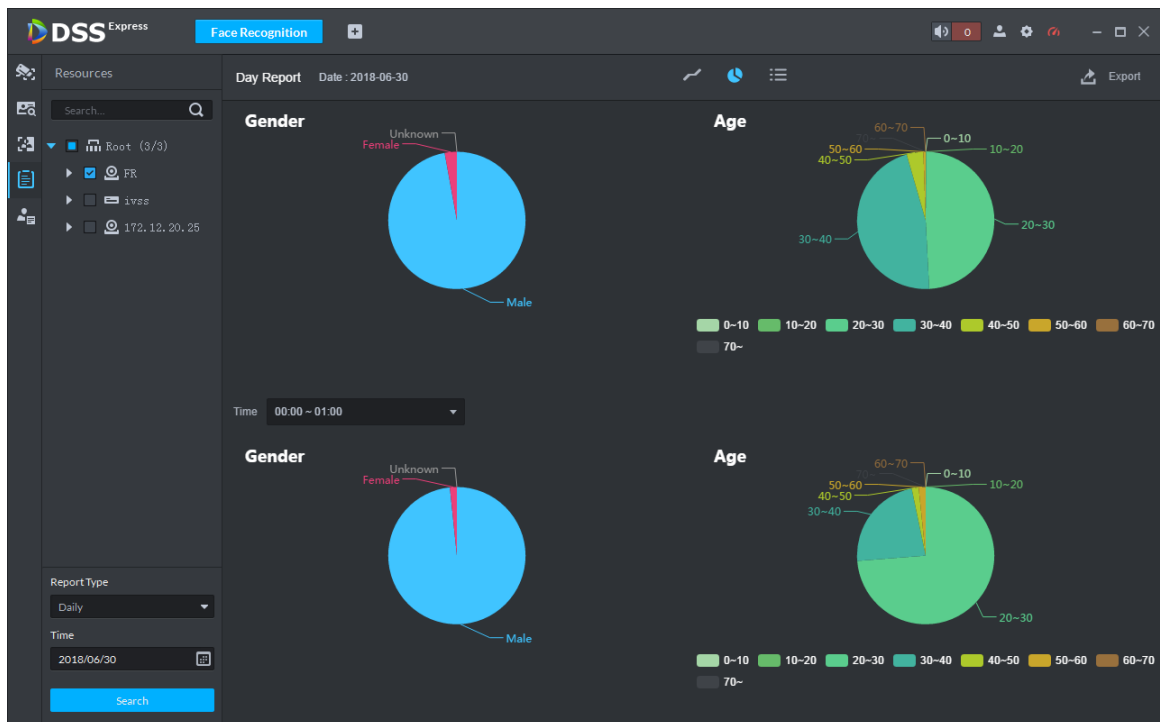
- Line chart is shown in Figure 3-222.

Figure 3-222 Face report line chart



- Pie chart is shown in Figure 3-223.

Figure 3-223 Face report pie chart



- List is shown in Figure 3-224.

Figure 3-224 List display

The screenshot shows the 'Face Recognition' section of the DSS Express interface. On the left, there is a 'Resources' sidebar with a search bar and a tree view showing 'Root (8/3)' with sub-items 'FR' and 'ivss'. Below this, there are filters for 'Report Type' (set to 'Daily'), 'Time' (set to '2018/06/30'), and a 'Search' button. The main area displays a 'Day Report' for 'Date: 2018-06-30'. It contains a table with columns: 'Time', 'Channel Name', 'Gender', and 'Age'. The table lists 20 entries, all with 'Gender' as 'Male' and 'Age' ranging from 21 to 40. At the bottom, there is a 'Per page' dropdown set to '20' and a 'Statistics' button.

Time	Channel Name	Gender	Age
2018-06-30 14:59:03	ivss_IPC_FR_YJ1_113shebei	Male	31
2018-06-30 14:58:55	ivss_IPC_FR_YJ1_113shebei	Male	21
2018-06-30 14:58:06	ivss_IPC_FR_YJ1_113shebei	Male	32
2018-06-30 14:58:03	ivss_IPC_FR_YJ1_113shebei	Male	33
2018-06-30 14:53:40	ivss_IPC_FR_YJ1_113shebei	Male	26
2018-06-30 14:53:40	ivss_IPC_FR_YJ1_113shebei	Male	24
2018-06-30 14:53:10	ivss_IPC_FR_YJ1_113shebei	Male	33
2018-06-30 14:53:03	ivss_IPC_FR_YJ1_113shebei	Male	26
2018-06-30 14:52:59	ivss_IPC_FR_YJ1_113shebei	Male	35
2018-06-30 14:52:58	ivss_IPC_FR_YJ1_113shebei	Male	25
2018-06-30 14:52:58	ivss_IPC_FR_YJ1_113shebei	Male	27
2018-06-30 14:52:51	ivss_IPC_FR_YJ1_113shebei	Male	36
2018-06-30 14:52:48	ivss_IPC_FR_YJ1_113shebei	Male	29
2018-06-30 14:52:15	ivss_IPC_FR_YJ1_113shebei	Male	29
2018-06-30 13:47:44	ivss_IPC_FR_YJ1_113shebei	Male	28
2018-06-30 13:46:53	ivss_IPC_FR_YJ1_113shebei	Male	26
2018-06-30 13:46:49	ivss_IPC_FR_YJ1_113shebei	Male	29
2018-06-30 13:46:47	ivss_IPC_FR_YJ1_113shebei	Male	27
2018-06-30 13:44:24	ivss_IPC_FR_YJ1_113shebei	Male	28
2018-06-30 13:02:03	ivss_IPC_FR_YJ1_113shebei	Male	40

3.9.6.5 Viewing Face Recognition Alarm

View and process face recognition alarm event in event center, see Figure 3-225. For more details, see **3.6 Event Center**.

Figure 3-225 List display

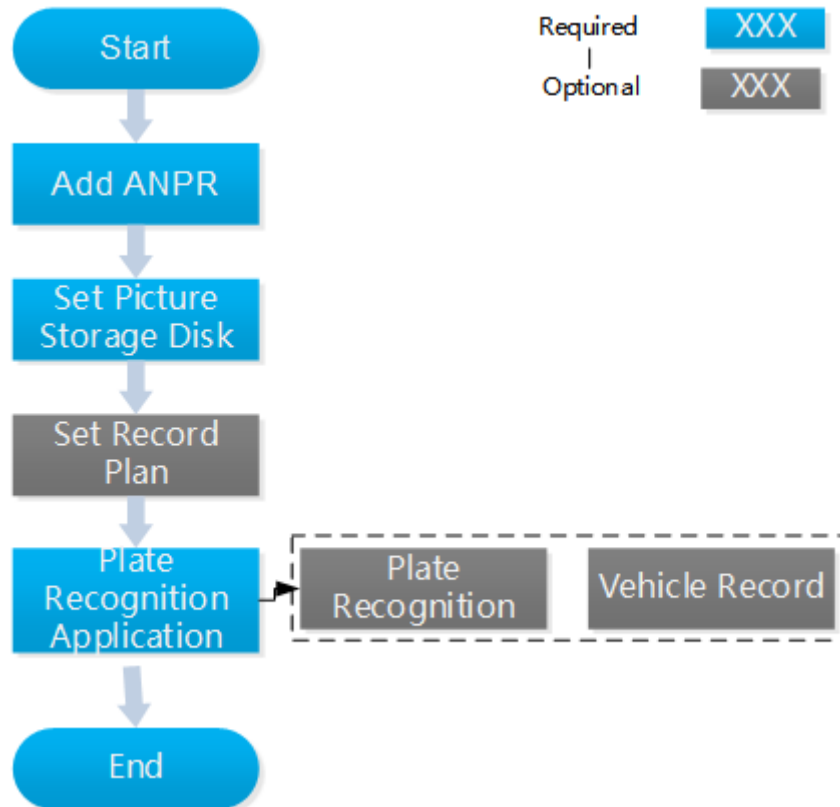
The screenshot shows the 'Event Center' section of the DSS Express interface. On the left, there is a 'Resources' sidebar with a search bar and a tree view showing 'All' and 'Face Recognition'. Below this, there are filters for 'Time' (set to '05/14 00:00-03/14 23:59'), 'Priority' (set to 'High, Medium, Low'), 'Handling user' (set to 'All'), and 'Alarm Status' (set to 'Pending, Processed'). The main area displays a list of alarms with columns: 'Alarm Time', 'Alarm Sort', 'Alarm Type', 'Alarm Source', 'Priority', 'Handling user', 'Alarm Status', and 'Operation'. The table is currently empty. At the bottom, there is a 'Per page' dropdown set to '20' and a 'Search' button.

Alarm Time	Alarm Sort	Alarm Type	Alarm Source	Priority	Handling user	Alarm Status	Operation
------------	------------	------------	--------------	----------	---------------	--------------	-----------

3.10 ANPR

After ANPR is added to platform, the platform can receive plate recognition result reported by ANPR. The plate recognition operation flow is shown in Figure 3-226.

Figure 3-226 Plate recognition flow



3.10.1 Adding ANPR

Add ANPR; see **3.2.2.4 Adding Device** for more details.

3.10.2 Setting Picture Storage Disk

Configure local storage disk, you have to reserve a ANPR picture disk to store ANPR snapshot, otherwise, snapshot cannot be stored, and snapshots are not displayed. For more details, see **3.2.1.4 Setting Storage Space**

3.10.3 Setting Record Plan

Only when record storage plan is configured, then video before and after snapshot can be stored, the platform can playback video 10 seconds before and after ANPR snapshot. If you need to set record storage plan, see **3.2.5 Setting Record Plan**.

3.10.4 Plate Recognition Application

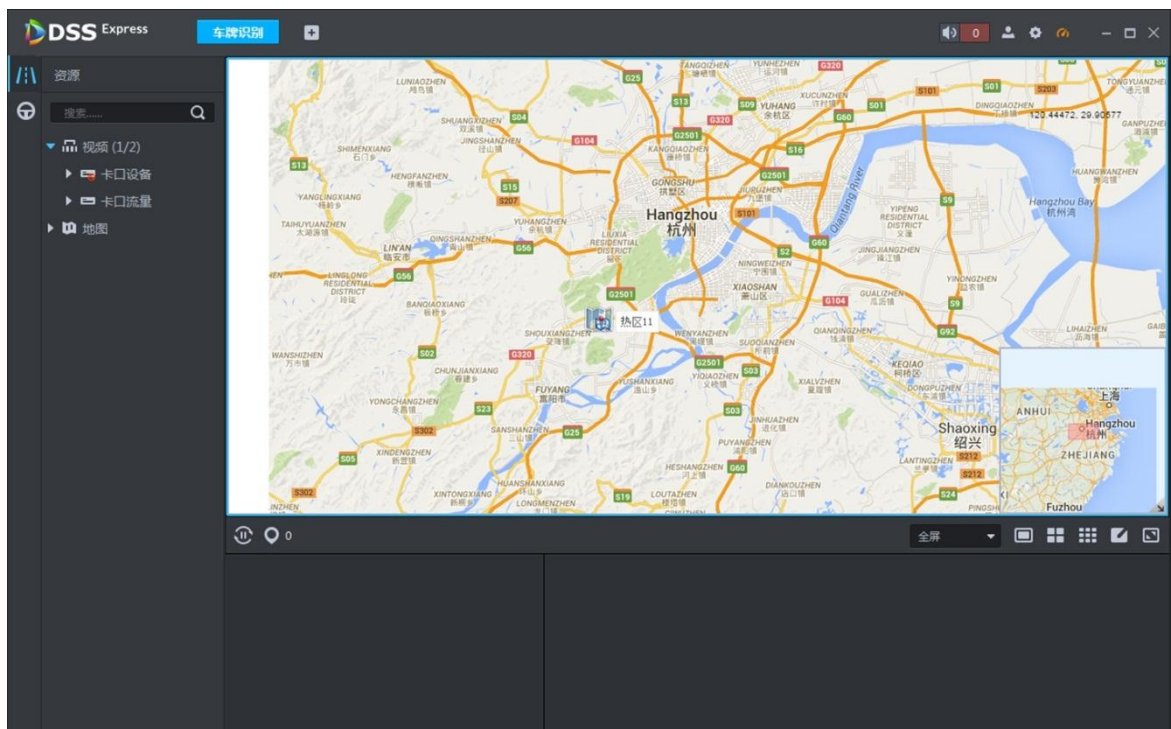
3.10.4.1 Plate Recognition

Step 1 On client homepage, click **ANPR**.
The system displays **ANPR** interface.

Step 2 Click .

The system displays **ANPR** interface. The map is displayed with single window by default; you can switch number of windows. See Figure 3-227.

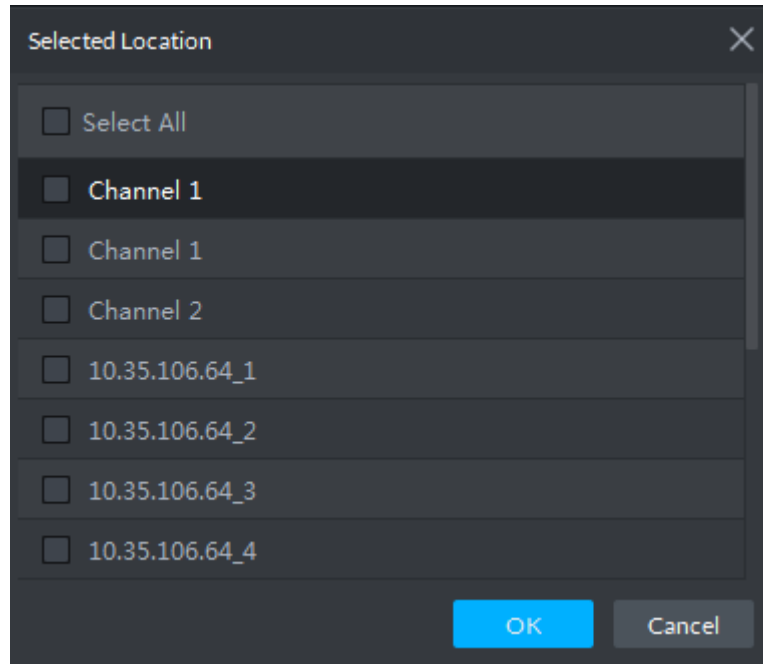
Figure 3-227 Plate recognition



Step 3 Click .

The system displays **Selected Location** interface, see Figure 3-228.

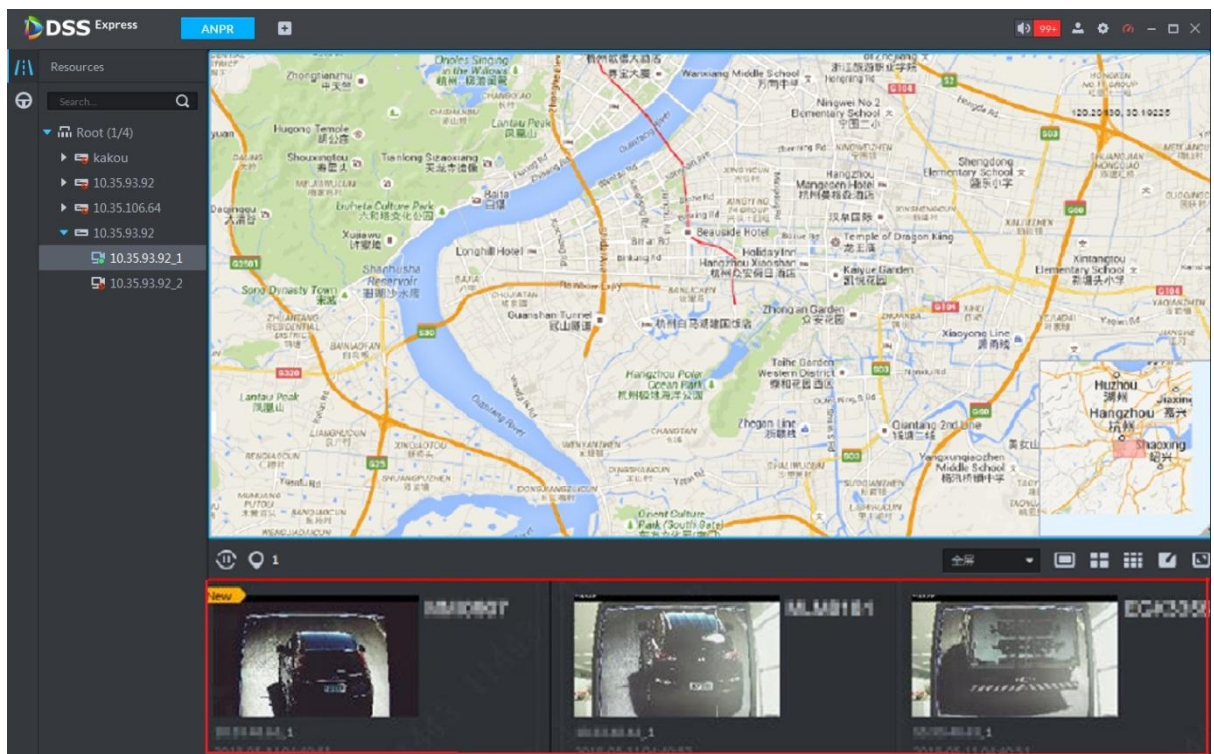
Figure 3-228 Select ANPR channel



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 3-229.

Figure 3-229 Plate recognition result



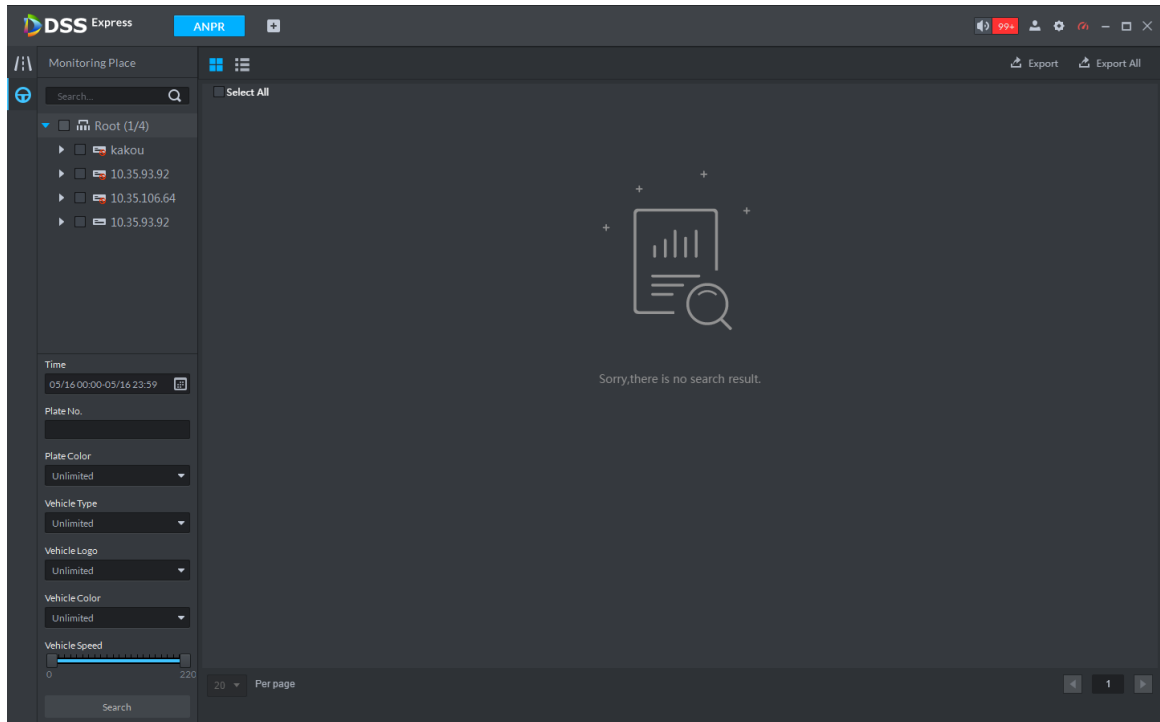
Step 5 Double-click the image to view image details. It includes plate number, snapshot time, ANPR channel name, vehicle logo, vehicle color.

3.10.5 Vehicle Record

Step 1 On ANPR interface, click .

The system displays **Vehicle Record** interface, see Figure 3-230.

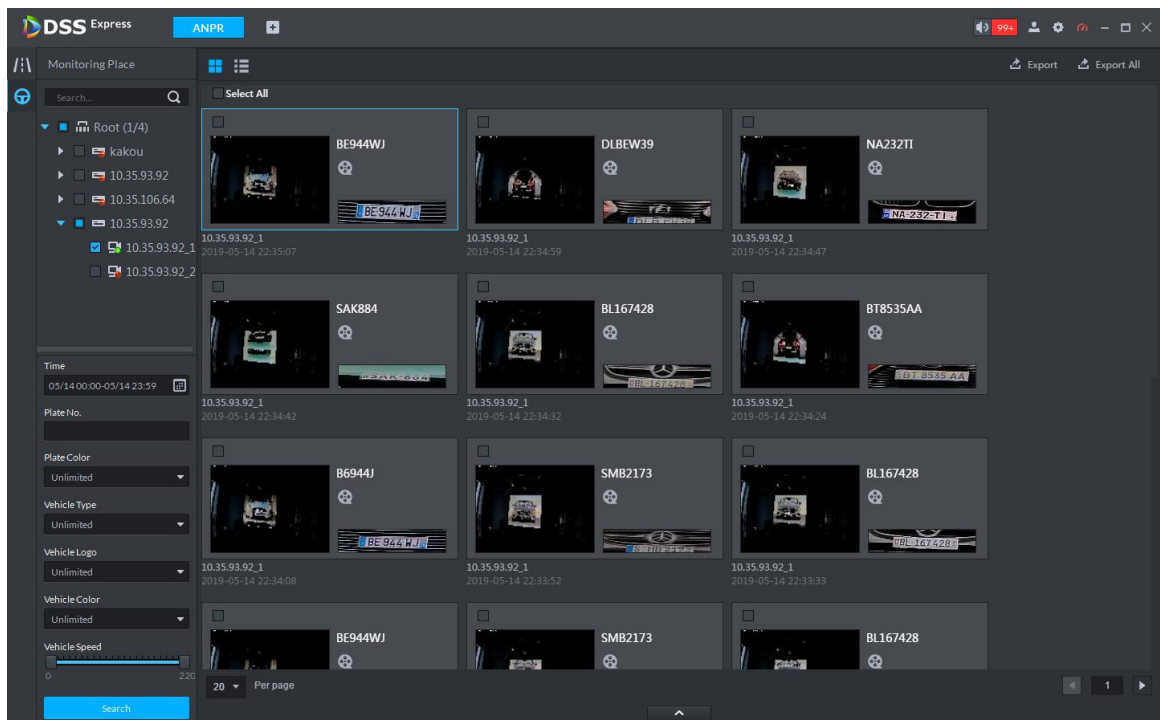
Figure 3-230 Vehicle record



Step 2 Select video channel and set search conditions. Click **Search**.

System displays search result. See Figure 3-231.

Figure 3-231 Passed vehicle search result



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 (), it is to select different display mode.
- Select a snapshot image and then click  or double click the image, system displays detailed information. See Figure 3-232. Move the cursor to the middle to select the specified zone, you can zoom in it. See Figure 3-233.

Figure 3-232 Vehicle details

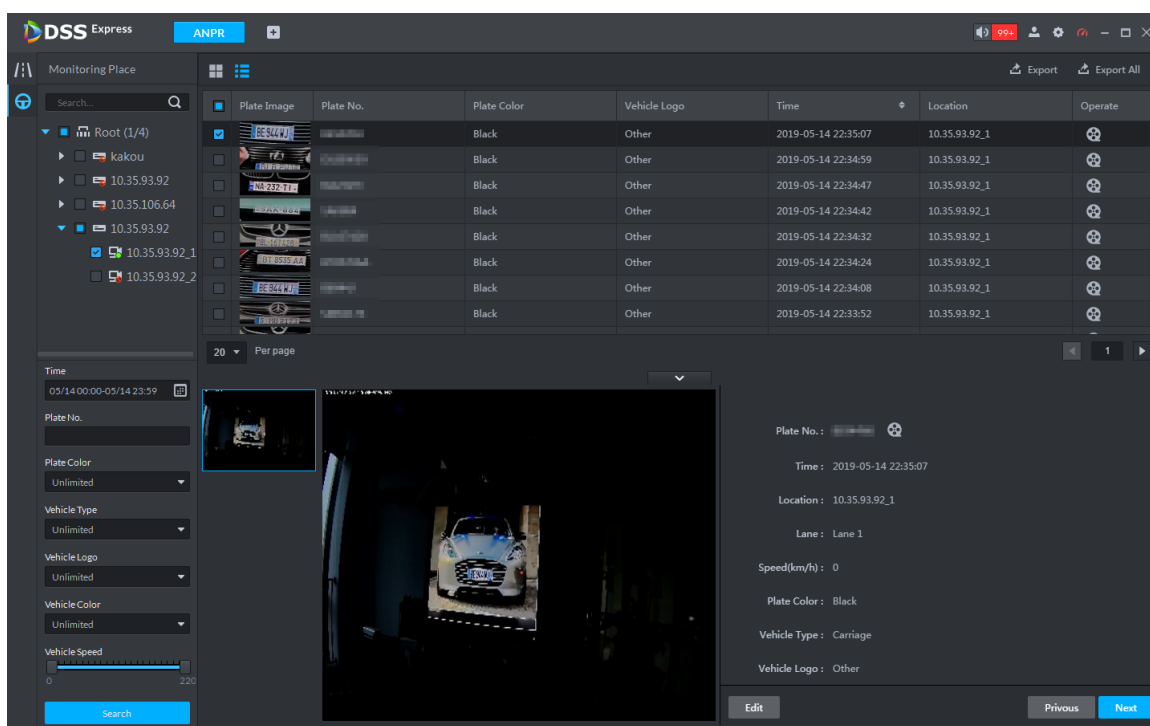
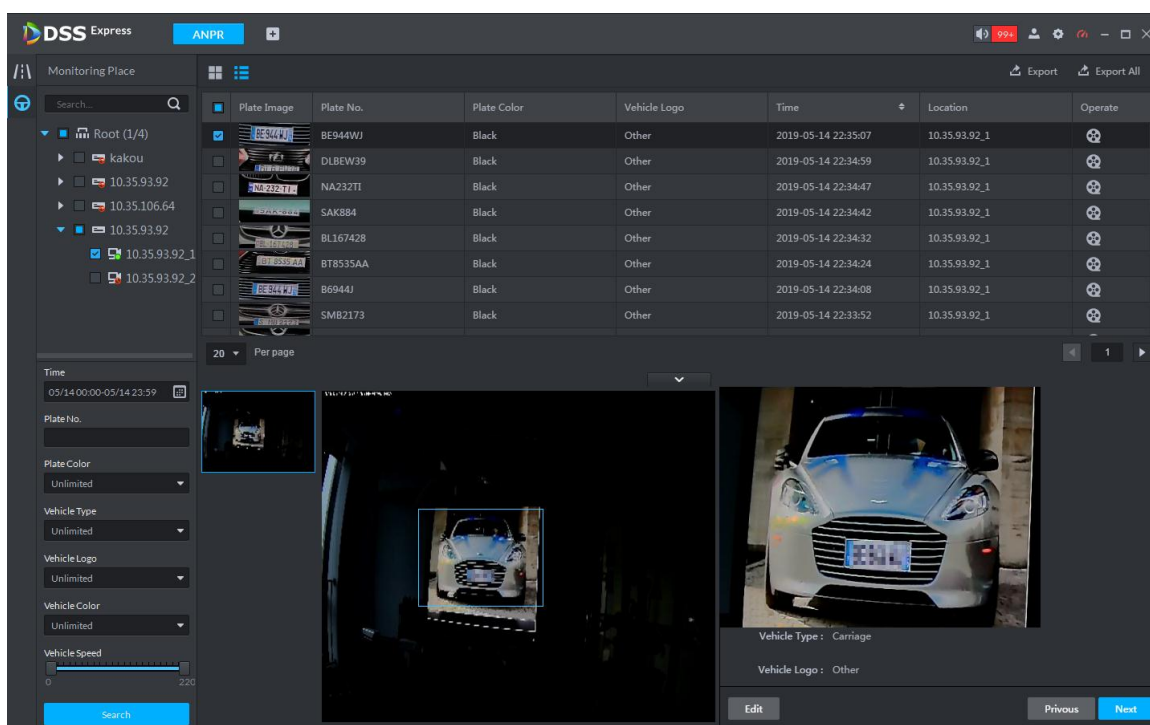
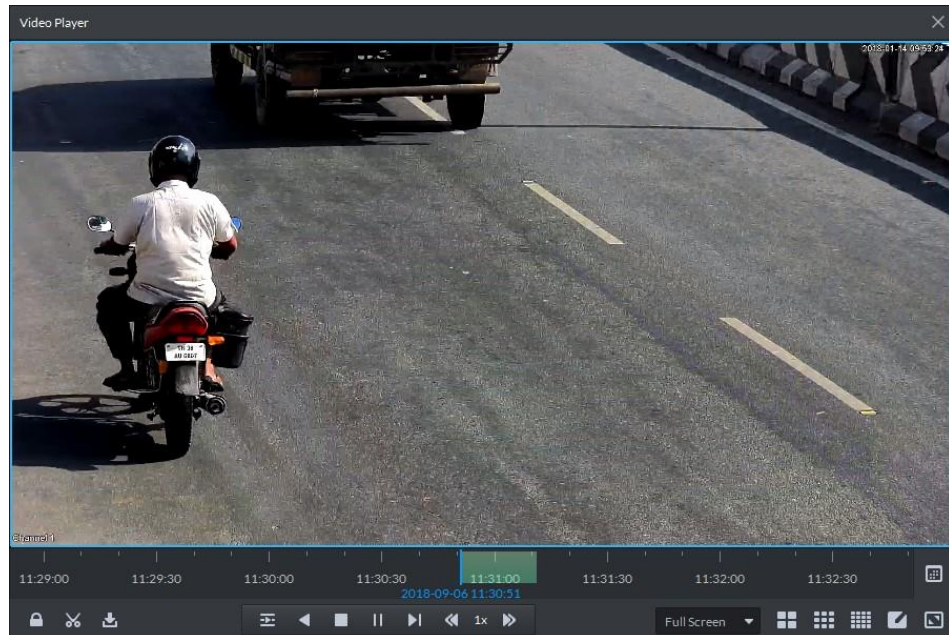


Figure 3-233 Regional zoom



- Click  to playback the 15-second video before and after the vehicle passed time. See Figure 3-234. The video file is total 30 seconds. Display the 15-second video before and after the vehicle passed.

Figure 3-234 Playback video

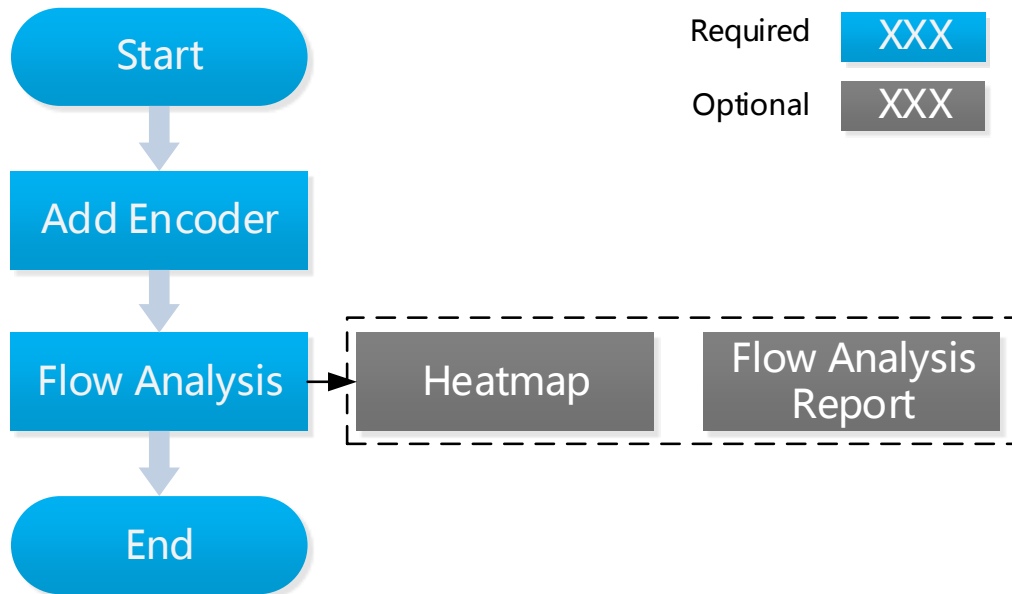


- Click  to view the vehicle running track.
- Export: Select the passed vehicle information and then click **Export** and export selected passed vehicle. Click **Export All**, and export all searched passed vehicle information.

3.11 Flow Analysis

After adding stereo vision flow analysis camera to platform, the platform supports searching flow analysis report and heat map. The operation of flow analysis is shown in Figure 3-235.

Figure 3-235 Flow analysis



3.11.1 Adding Encoder

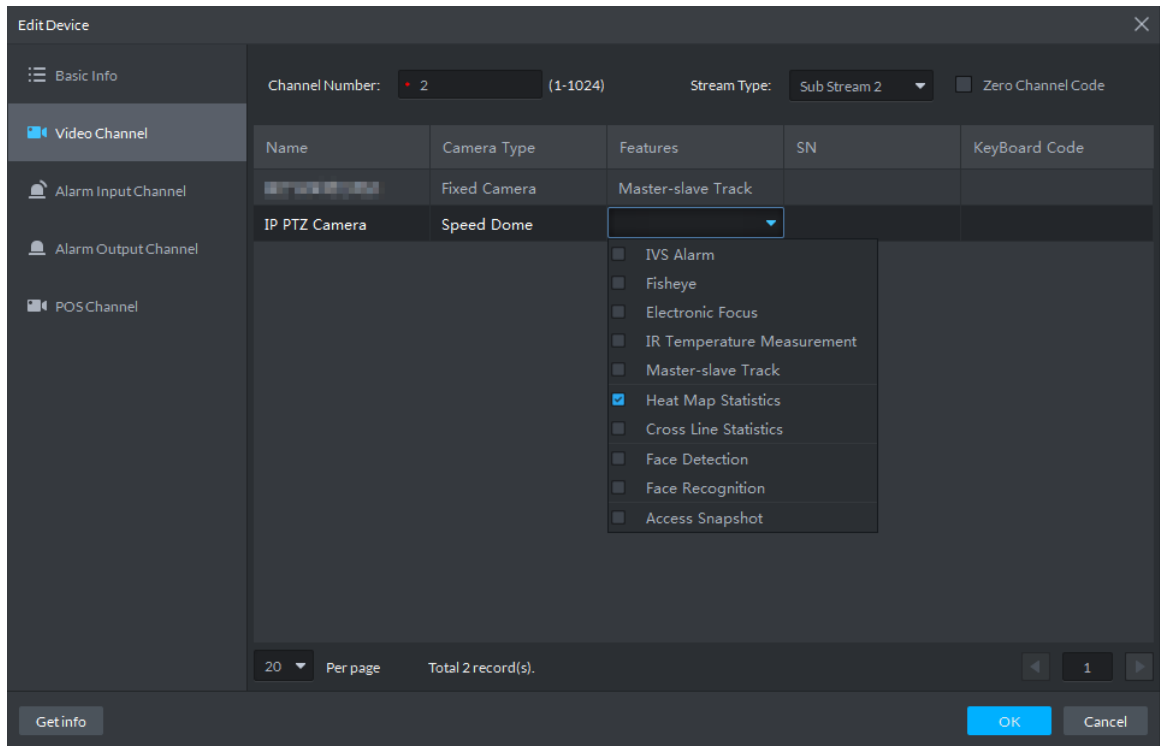


The platform only displays results reported by camera. Please make sure the added stereo vision camera already enables people counting function. For detailed operation, please refer to device user manual.

Step 1 Add stereo vision camera. For detailed operation, see **3.2.2.4 Adding Device**.

Step 2 Modify device feature. On **Device** interface, click  and modify device **Features** as **Heatmap Statistics**. See Figure 3-236.

Figure 3-236 Modify feature



3.11.2 Flow Analysis Application

3.11.2.1 Heatmap

Present distribution of moving objects according to color.



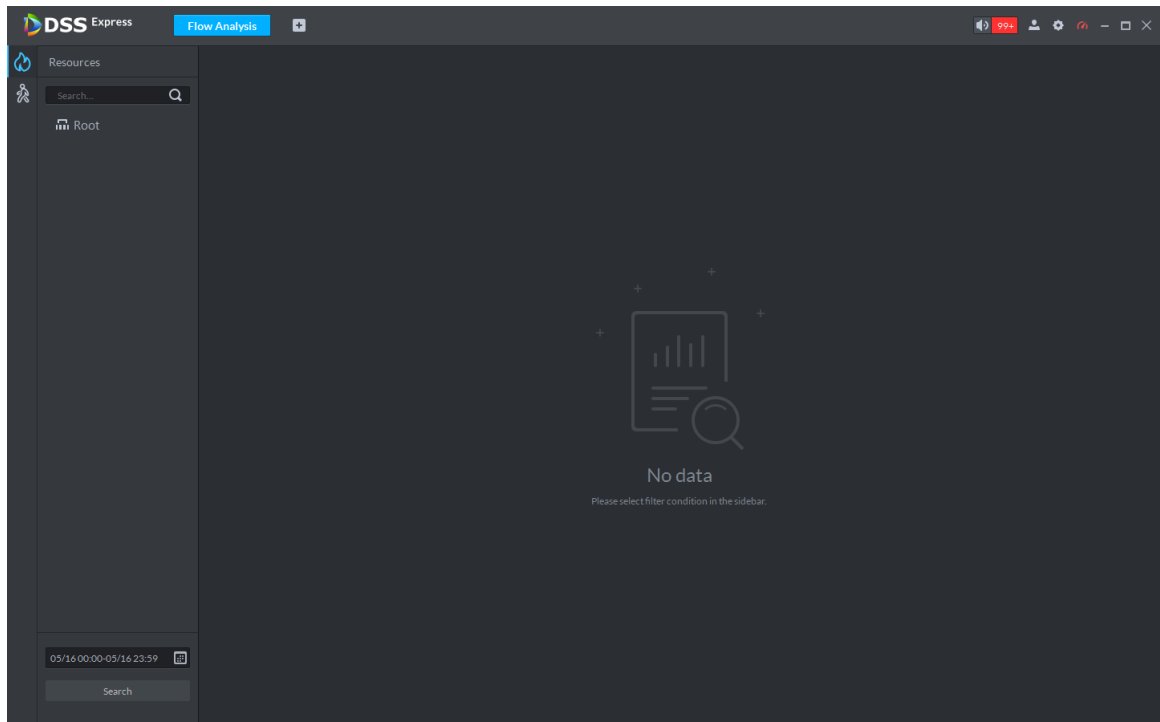
The device uploads heatmap statistics data to platform. You can view the uploaded statistics data.

Step 1 On client homepage, click **Flow Analysis**.
The system displays **Flow Analysis** interface.

Step 2 Click .

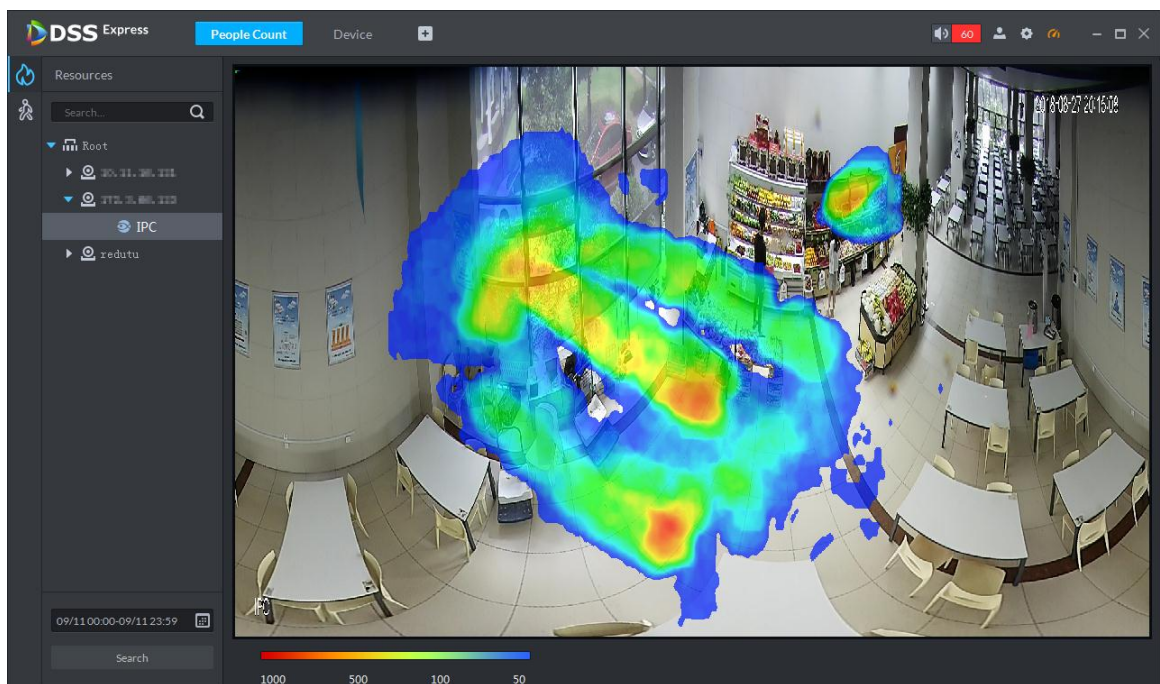
The system displays **Heatmap** interface, see Figure 3-237.

Figure 3-237 Heatmap



Step 3 Select the channel that displays heatmap, select time and click **Search**.
The system displays heatmap, see Figure 3-238.

Figure 3-238 Heatmap search result



Step 4 Click Export on upper right corner of the interface, save heatmap picture to local in bmp according to prompt on interface.

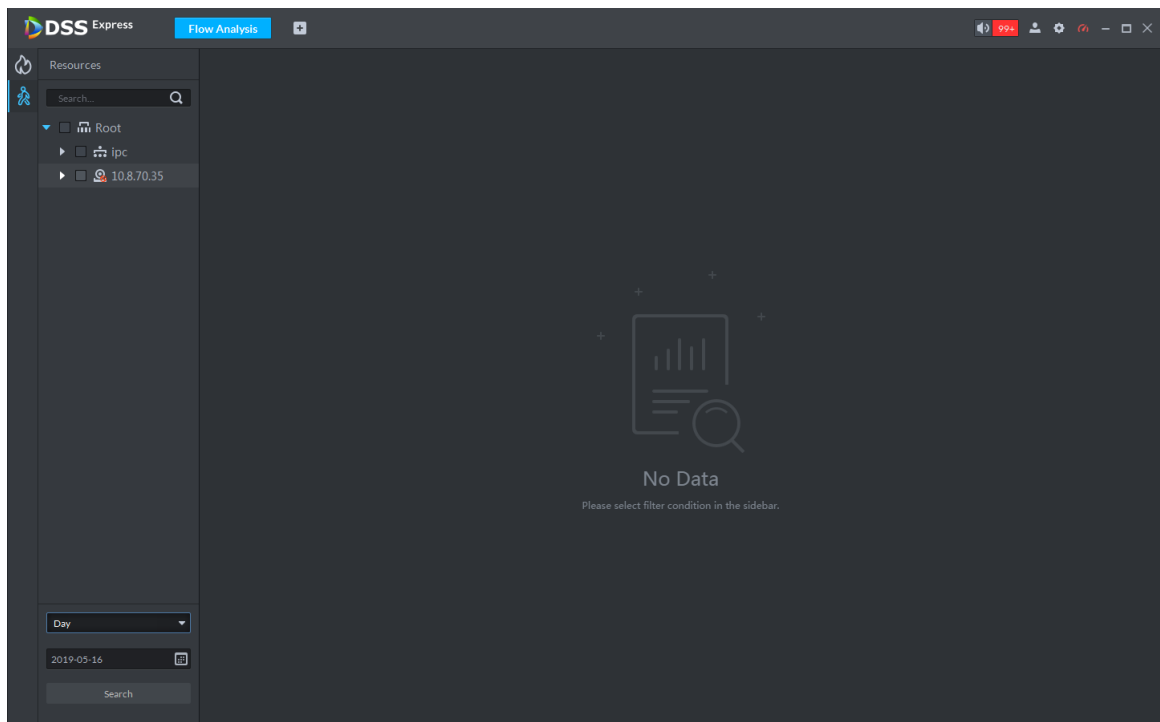
3.11.2.2 Flow Analysis Report

Search in and out people number, and form data report. Support searching stay people number if it is day report.

Step 1 On **Flow Analysis** interface, click .

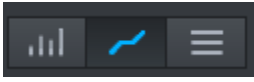
The system displays **Flow Analysis** interface, see Figure 3-239.

Figure 3-239 Flow analysis



Step 2 Select device channel, search period and statistics time, and click **Search**.

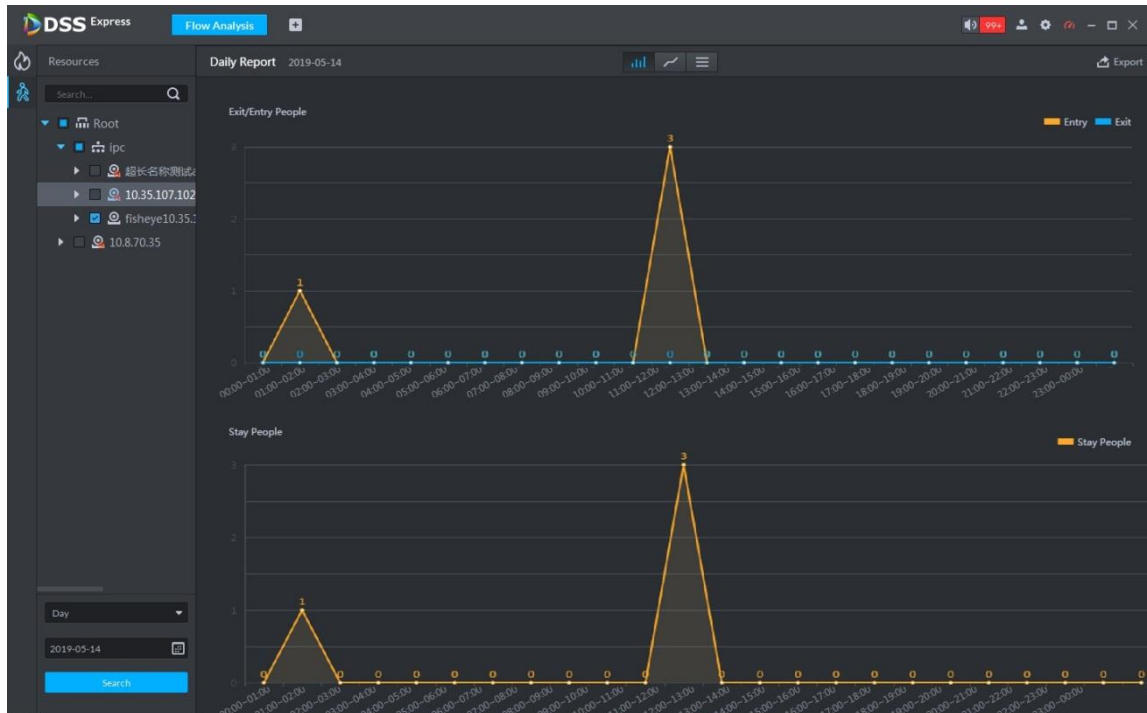
The system generates report, see Figure 3-240.

Report includes bar chart, line chart and list, click  on top of interface and switch display mode.



Statistics about stay people number is not implemented if search period is week, month or year.

Figure 3-240 Search result

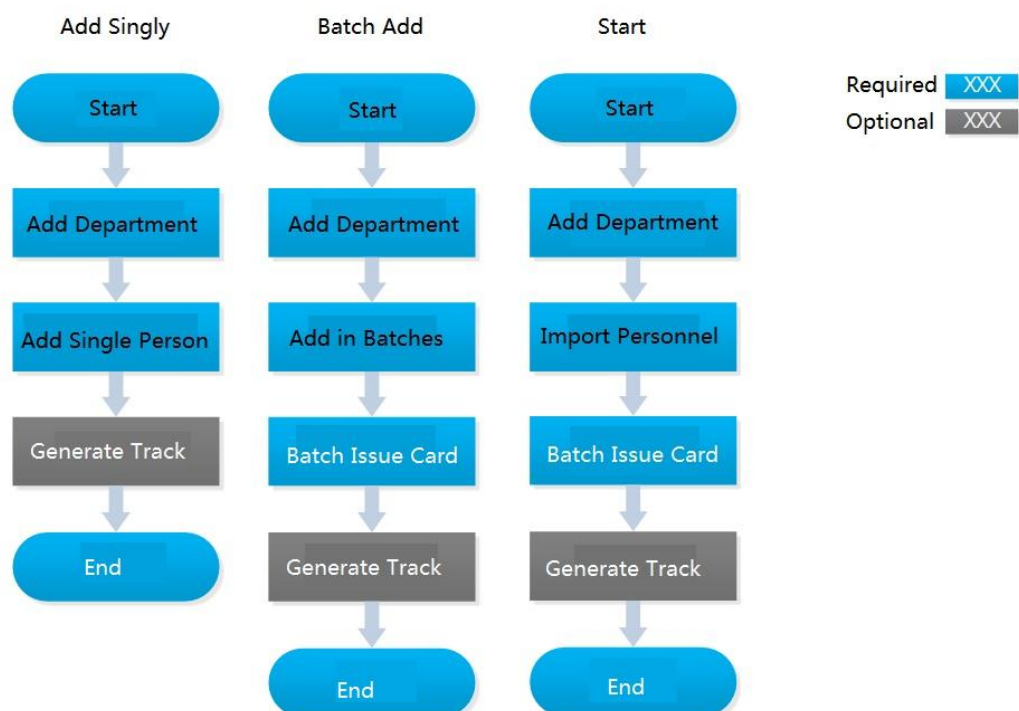


Step 3 Click **Export** on upper right corner of interface, save report to local in pdf according to prompt on interface.

3.12 Personnel Management

Personnel refer to the people responsible for access control management. They have the authorization to unlock doors with password, fingerprint, card, or face recognition. Operation flow is shown in Figure 3-241.

Figure 3-241 Personnel management flow



3.12.1 Adding Department

Adding department is to manage personnel in the added departments.

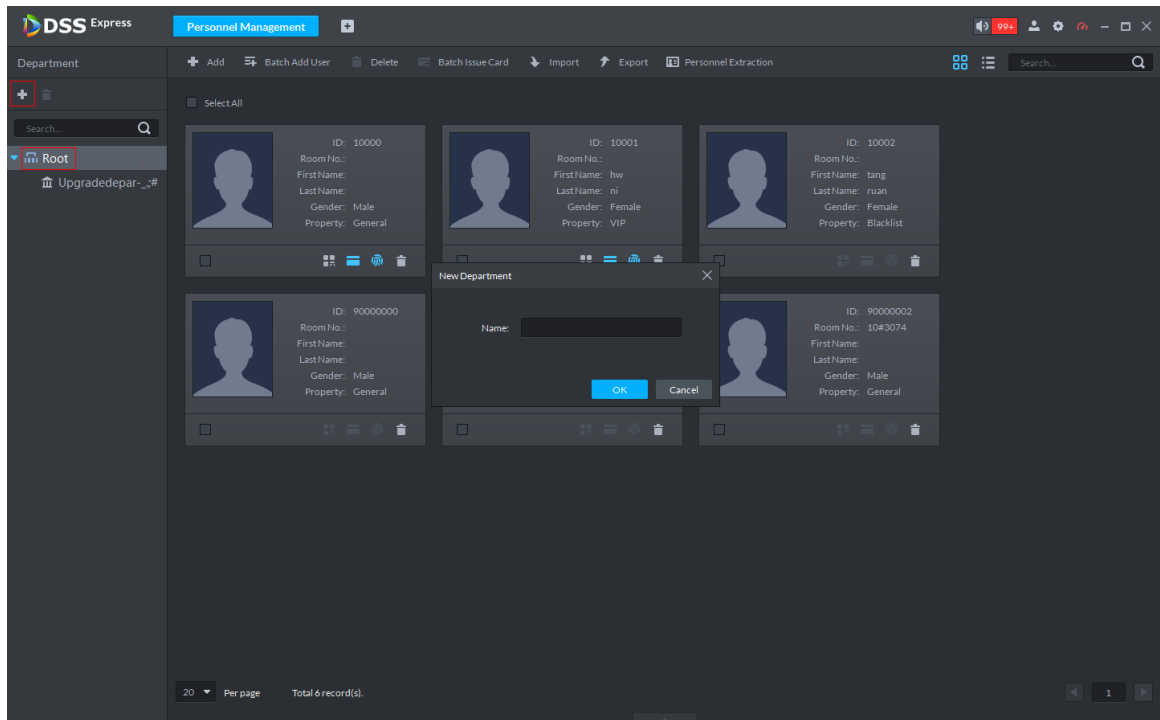
Step 1 Click . On the **Homepage** interface, select **Personnel Management**.

The **Personnel Management** interface is displayed.

Step 2 Select a node from the department list on the left side, and click **Add**.

The **New Department** interface is displayed. See Figure 3-242. The new department is directly under the selected node.

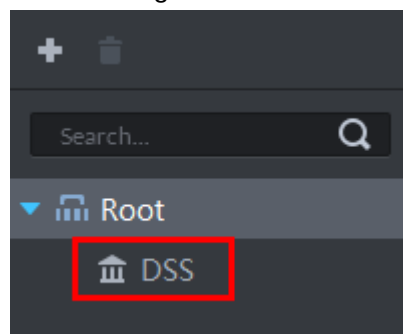
Figure 3-242 New department



Step 3 Input the department name and click **OK**.

The newly added department is displayed. See Figure 3-243.

Figure 3-243



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, right-click it and select **Rename** to modify the name.

3.12.2 Adding Personnel

Add personnel and authorize them to unlock doors. When adding personnel, system uploads the collected personnel information to the server for proper protection.



- The ID of added personnel should be in accordance with personnel ID of attendance device, otherwise, attendance data cannot be synchronized.
- If you want to read or import fingerprint or card from fingerprint collector, reader, please make sure fingerprint collector or reader is connected.
- IR face feature code needs to add personnel, enter edit status and read from IR face access control.

3.12.2.1 Adding Person Singly

Step 1 On the **Personnel Management** interface, click **Add**.

The **Add Person** interface is displayed. See Figure 3-244.

Figure 3-244 Add personnel

Step 2 Configure personnel details.

- 1) Move the mouse to the picture section, 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. For parameter details, see Table 3-34.

Table 3-34 Personnel detail description

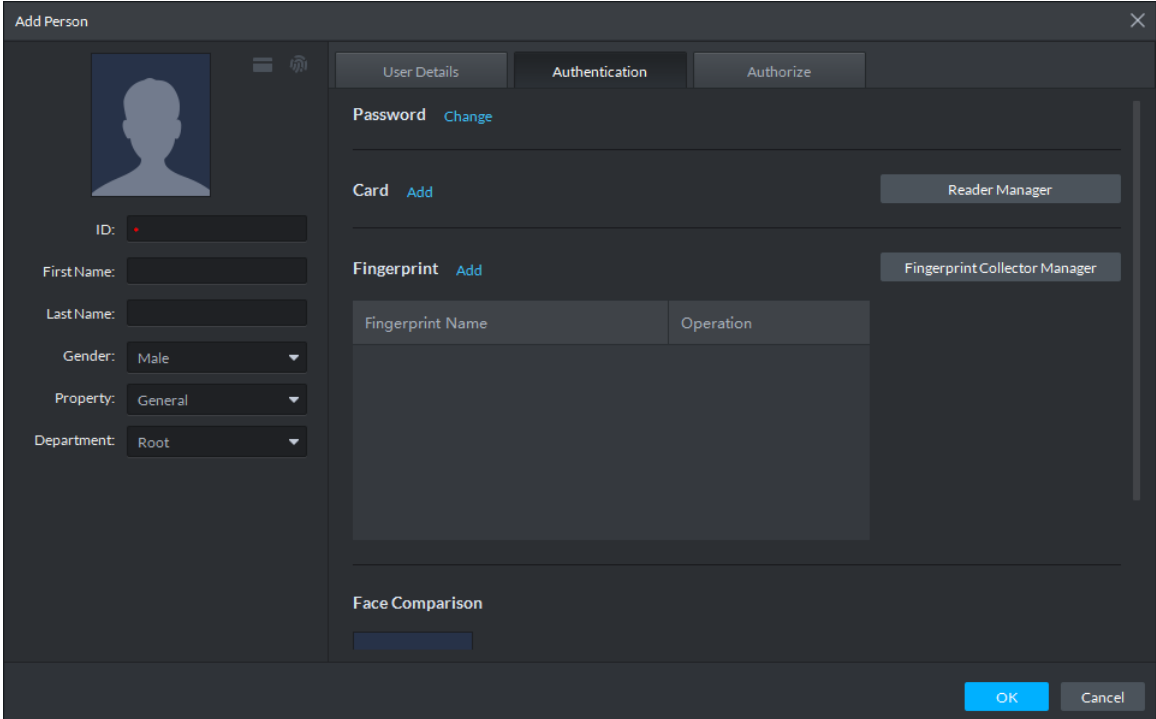
Parameter	Description
ID	Required, used to recognize personnel, each ID number is unique.

Parameter	Description
Property	Set person as different types.  If the person is the first card unlock, then person property is set as General.
Householder	If the added personnel belong to the same household, then you can set one person as householder, you can issue contacts and householder info under video intercom.
Admin	Personnel divided into general and admin. Admin has the permission to operate device interface. The parameter takes effect only when personnel info issued to 2 nd generation access control.

Step 3 Click the **Authentication** tab.

The **Authentication** interface is displayed. See Figure 3-245.

Figure 3-245 Authentication



The screenshot shows the 'Add Person' window with the 'Authentication' tab selected. On the left, under 'User Details', there are input fields for ID, First Name, Last Name, Gender (set to Male), Property (set to General), and Department (set to Root). On the right, under 'Authentication', there is a Password field with a 'Change' link, a Card field with an 'Add' link and a 'Reader Manager' button, a Fingerprint field with an 'Add' link and a 'Fingerprint Collector Manager' button, and a Face Comparison section with a button. At the bottom right are 'OK' and 'Cancel' buttons.

Step 4 Set a password.

1) Click **Change**.

The system displays password setting. See Figure 3-246.

Figure 3-246 Set password

- 2) Enter a password, and click **OK** to save the password settings.

Step 5 Issue cards to personnel.

The system supports issuing card by entering card No. manually and card reader.

- Issue card by entering card No. manually

- 1) Click **Add** next to **Card**.

The **Issue Card** interface is displayed. See Figure 3-247.

Figure 3-247 Add card

- 2) Enter personnel card number and click **OK** to save the card added. See Figure 3-248. For more details, refer to Table 3-35.

Figure 3-248 Card added

Table 3-35 Card operation

Icon	Description
------	-------------

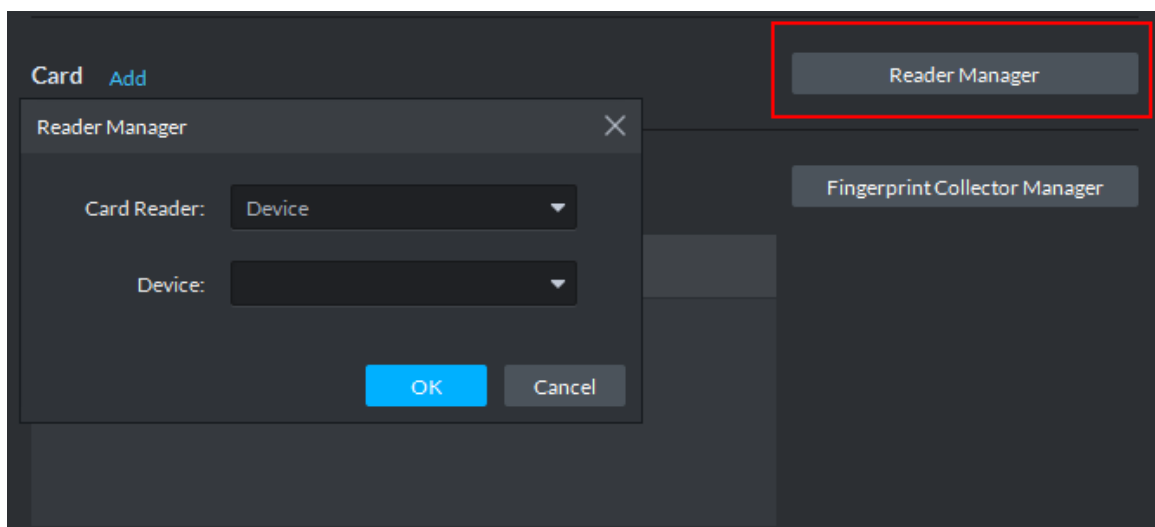
Icon	Description
	If a person has several cards, only the main card can be issued to 1st generation access control device. The first added card is considered as main card by default. Click the icon and it becomes , and then  is displayed on upper right corner of the interface, which means that the card is set as main card. Click  to cancel main card setting.
	Set the card as duress card, after that use the card to unlock, then duress alarm is generated. After clicking the icon, it becomes ,  is displayed on upper right corner of the interface, which means that the card is set as duress card. Click  to cancel duress card setting.
	Card cannot be used if it is damaged, so you can change a new card.
	Delete card info, after that the card has no unlock permission.

- Issue card by card reader.

1) Click **Reader Manager**.

The **Reader Manager** interface is displayed. See Figure 3-249.

Figure 3-249 Reader manager



2) Select from **Card Reader** or **Device**, and click **OK**.

3) Swipe the card on the card reader or device.

Complete issuing cards.

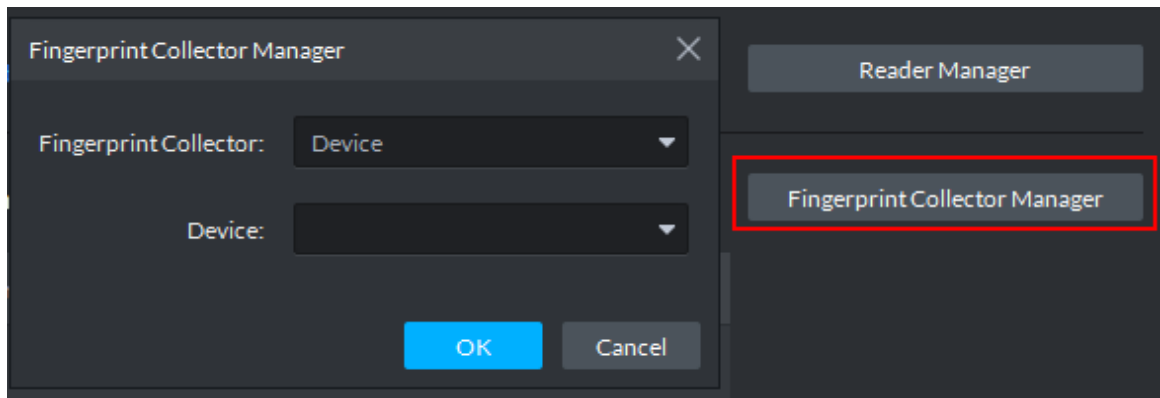
Step 6 Collect fingerprint.

When the system is connected to access control, unlocks by fingerprint, you need to collect personnel fingerprint. Each person can collect max 10 fingerprints.

1) Click **Fingerprint Collector Manager**.

The **Fingerprint Collector Manager** interface is displayed. See Figure 3-250.

Figure 3-250 Fingerprint collector manager

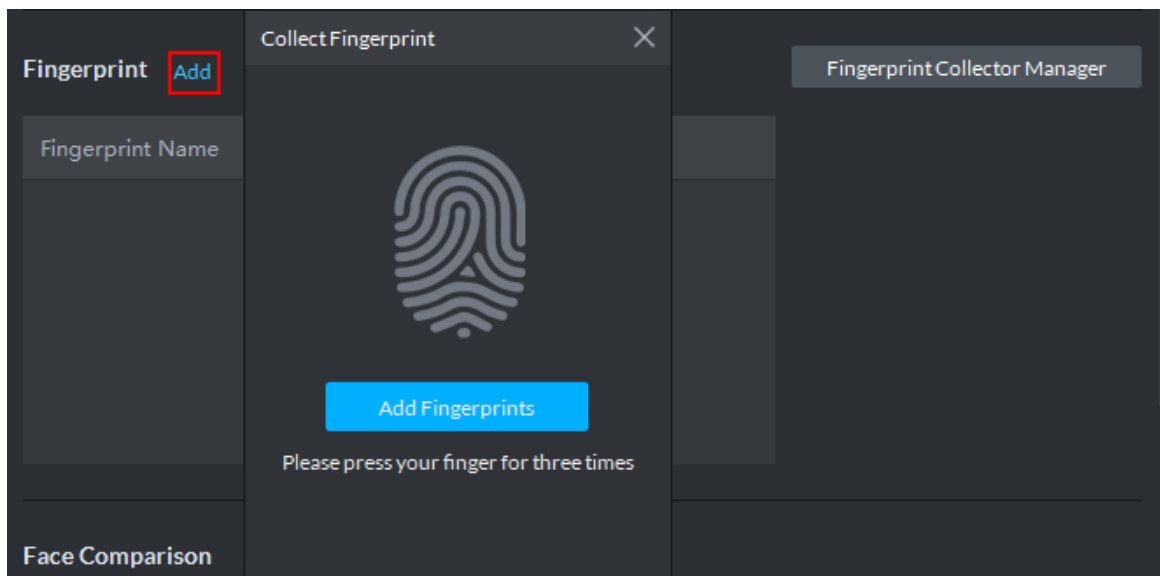


2) Select from **Fingerprint Collector** and click **OK**.

3) Click **Add**.

The **Collect Fingerprint** interface is displayed. See Figure 3-251.

Figure 3-251 Collect fingerprint



4) Click **Add Fingerprints**.

The **Collect Fingerprint** interface is displayed. See Figure 3-252.

Figure 3-252 Collect fingerprint



- 5) Records fingerprint on the reader by raising and then laying down the finger upon hearing the beep sound. Repeat this for three times. See Figure 3-253. Fingerprint collection is completed, see Figure 3-254. For more details, see Table 3-36.

Figure 3-253 Collecting fingerprint



Figure 3-254 Fingerprint collection completed

Fingerprint Add	
Fingerprint Name	Operation
Fingerprint 1	  

Table 3-36 Fingerprint operation

Icon	Description
------	-------------

Icon	Description
	If more than 3 fingerprints are imported, then only then main fingerprint can be issued to access control device. The latest three fingerprints are considered as main fingerprint by default. One person can set max three main fingerprints. After clicking the icon, it becomes , which means that the fingerprint is set as main fingerprint. Click and cancel main fingerprint setting.
	Set fingerprint as duress fingerprint, after that you can unlock the door by the fingerprint and generate duress alarm. Click the icon, it becomes , which means the fingerprint is set as duress fingerprint. Click and cancel duress fingerprint setting.
	Modify fingerprint name.
	Delete fingerprint, after that the fingerprint has no permission to unlock door.

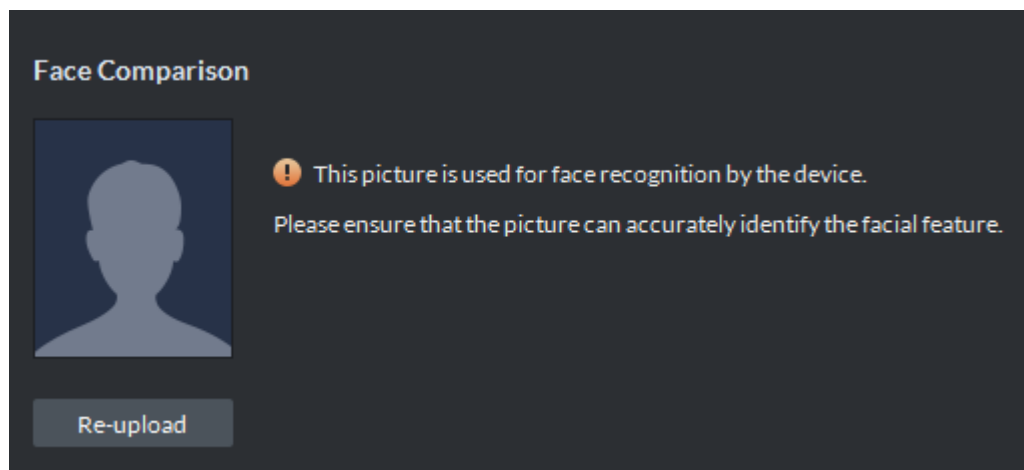
Step 7 Upload pictures for face recognition.

Click Add, and select picture to upload according to system prompt. See Figure 3-255.



- If the picture is wrong, or need to be replaced. Click Re-upload and upload new picture.
- Move the mouse to uploaded picture, shows up on the picture, click the icon and delete the uploaded picture.

Figure 3-255 Face picture upload



Step 8 Add vehicle info.

Added vehicle info is synced to entrance module, used as recognition info for vehicle entrance and exit.

Set the available spots for personnel, click **Add**, set plate No. and see Figure 3-256. If the person has several cars, then you need to add vehicle plate No. one by one.



If the number of added vehicles is more than available spots, then the number of entered vehicles cannot exceed the number of available spots which has been set.

Figure 3-256 Add vehicle info

Step 9 Click **Authorize** and select the channels to which the authorized users can have access. See Figure 3-257.

Figure 3-257 Authorize

Step 10 Click **OK**.

For the information of the added personnel, see Figure 3-258. If there are authorized fingerprint and card, the corresponding icon displays in blue.

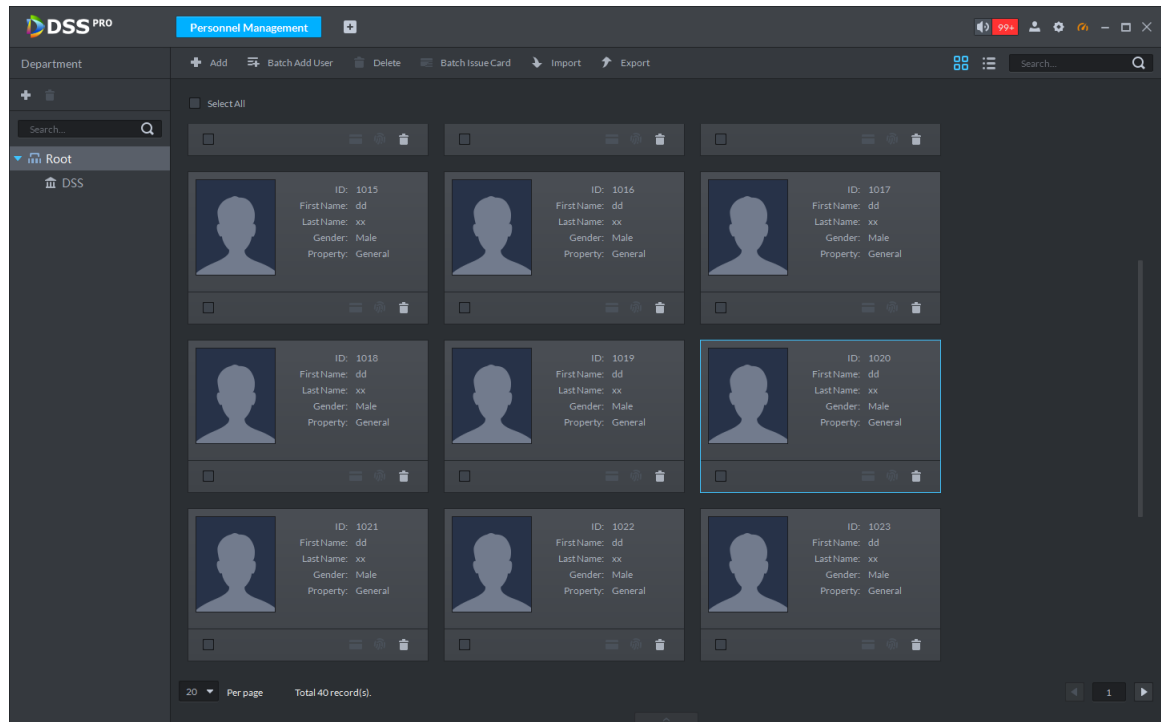


- Double-click personnel information, or select a person and click  to go to the

interface for editing personnel information. The system supports modifying personnel information.

- Select a person, click **Delete**, and follow the instructions on the interface to delete the selected personnel. Click **Select All** to quickly delete all personnel on the current page.

Figure 3-258 Personnel list



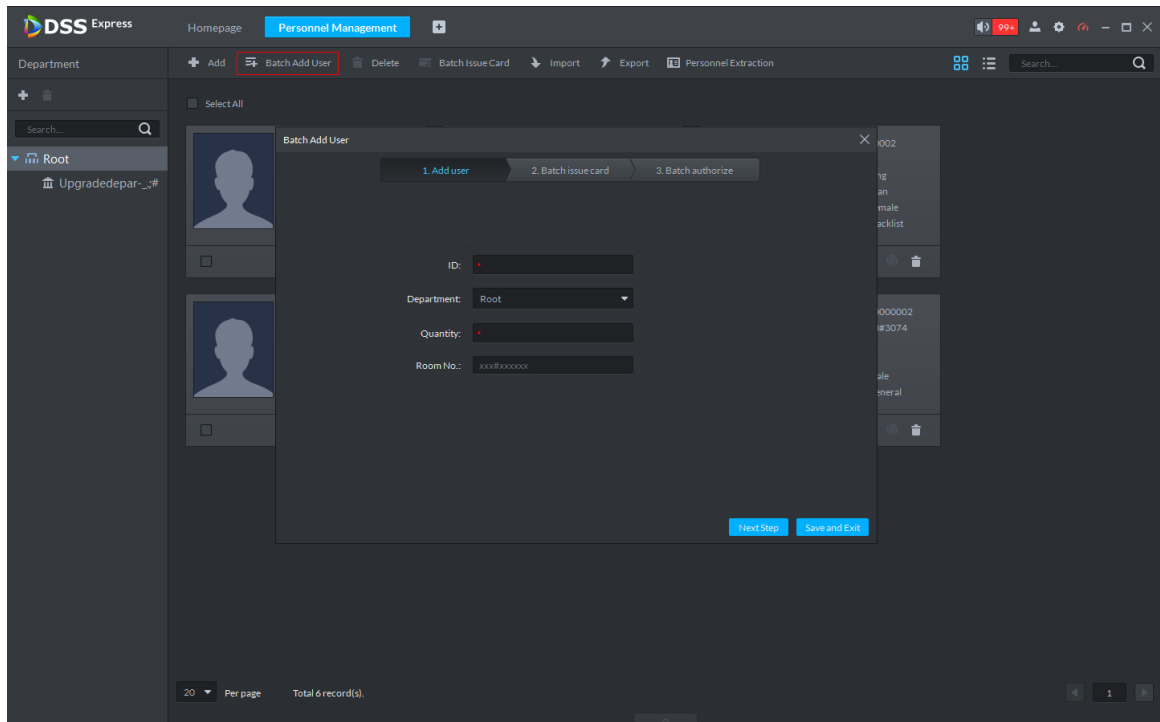
3.12.2.2 Batch Add

If multiple persons are added in one time, you can authorize them by issuing cards only. You cannot authorize password and fingerprint. If necessary, you can edit personnel authorization separately.

Step 1 On the **Personnel Management** interface, click **Batch Add User**.

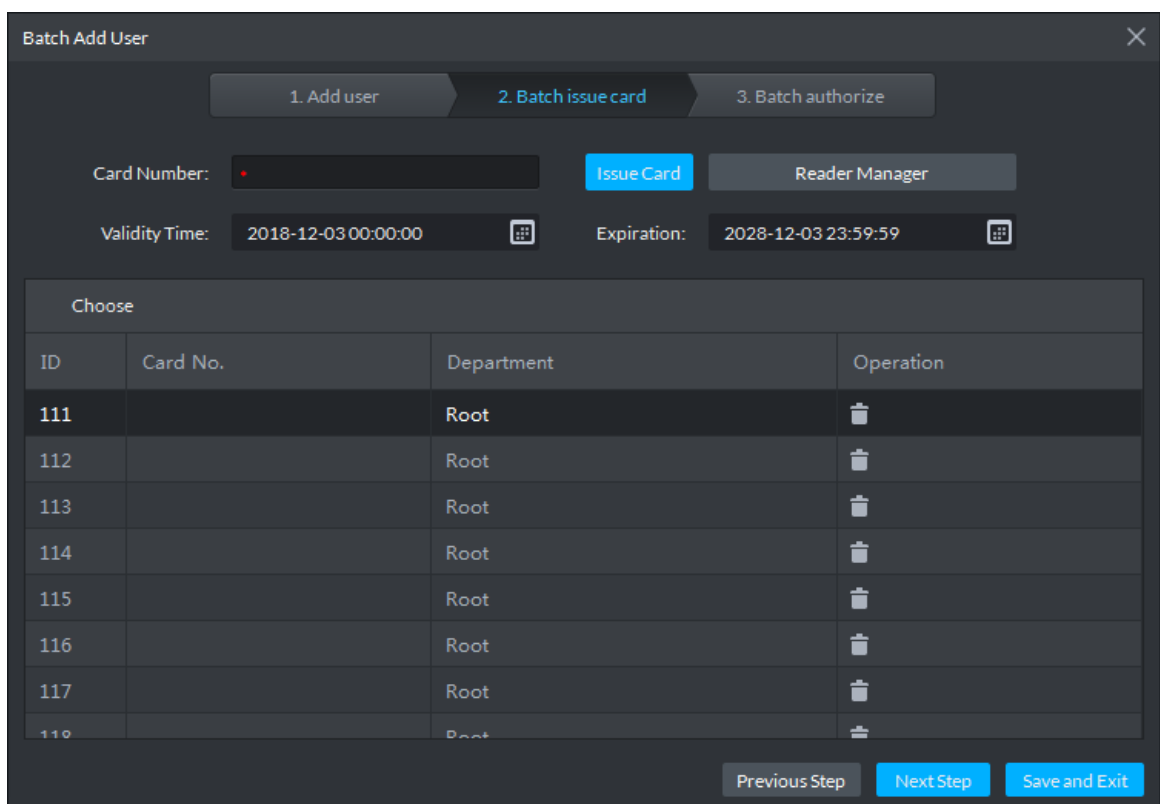
The **Batch Add User** interface is displayed. See Figure 3-259.

Figure 3-259 Batch add user



Step 2 Enter the starting ID and user quantity, select their departments, and click **Next Step**. The **Batch issue card** interface is displayed. See Figure 3-260.

Figure 3-260 Add batch info



Step 3 Issue cards to personnel.

The device supports issuing card by entering card No. manually and card reader.

- Issue card by entering card No. manually

1) Select a person, input the card number, and set up the validity time and expiry

time.

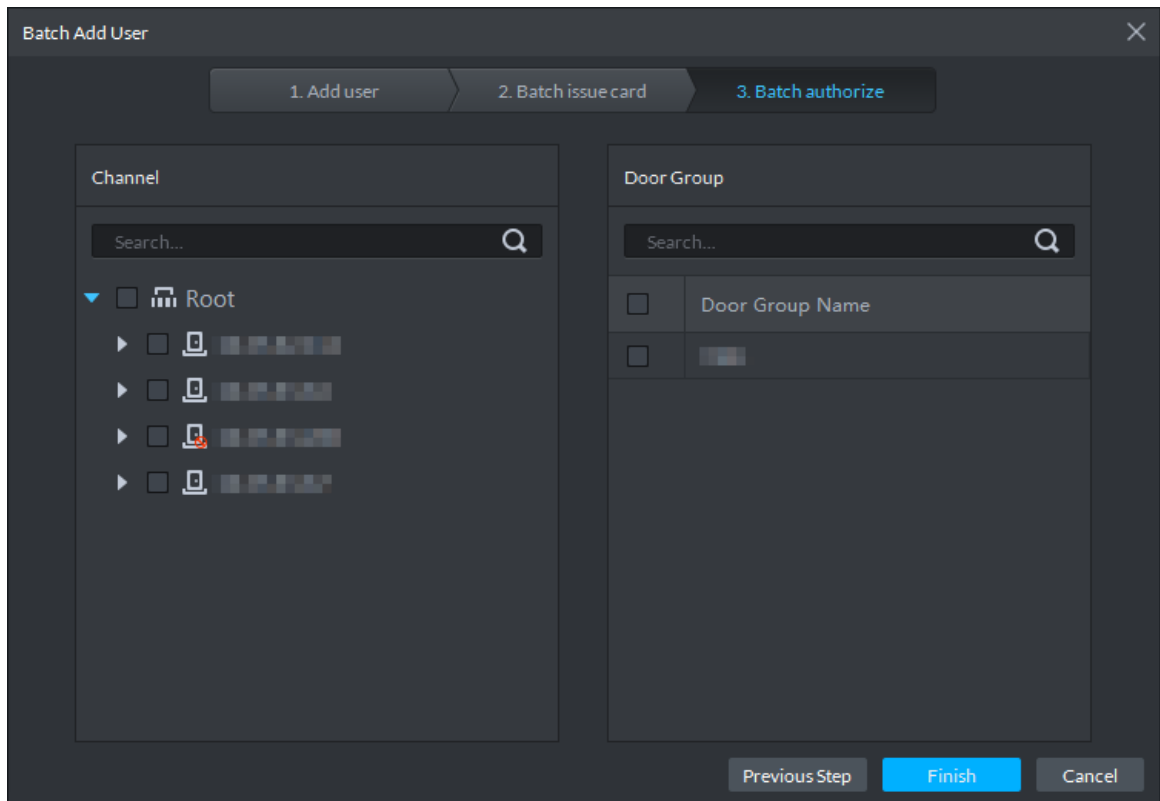
- 2) Click **Issue Card**.

Complete issuing card to the selected personnel and the interface shows the personnel card number.

- 3) Repeat the steps until all personnel get their cards.
- 4) Click **Next Step**.

The **Batch authorize** interface is displayed. See Figure 3-261.

Figure 3-261 Batch authorize

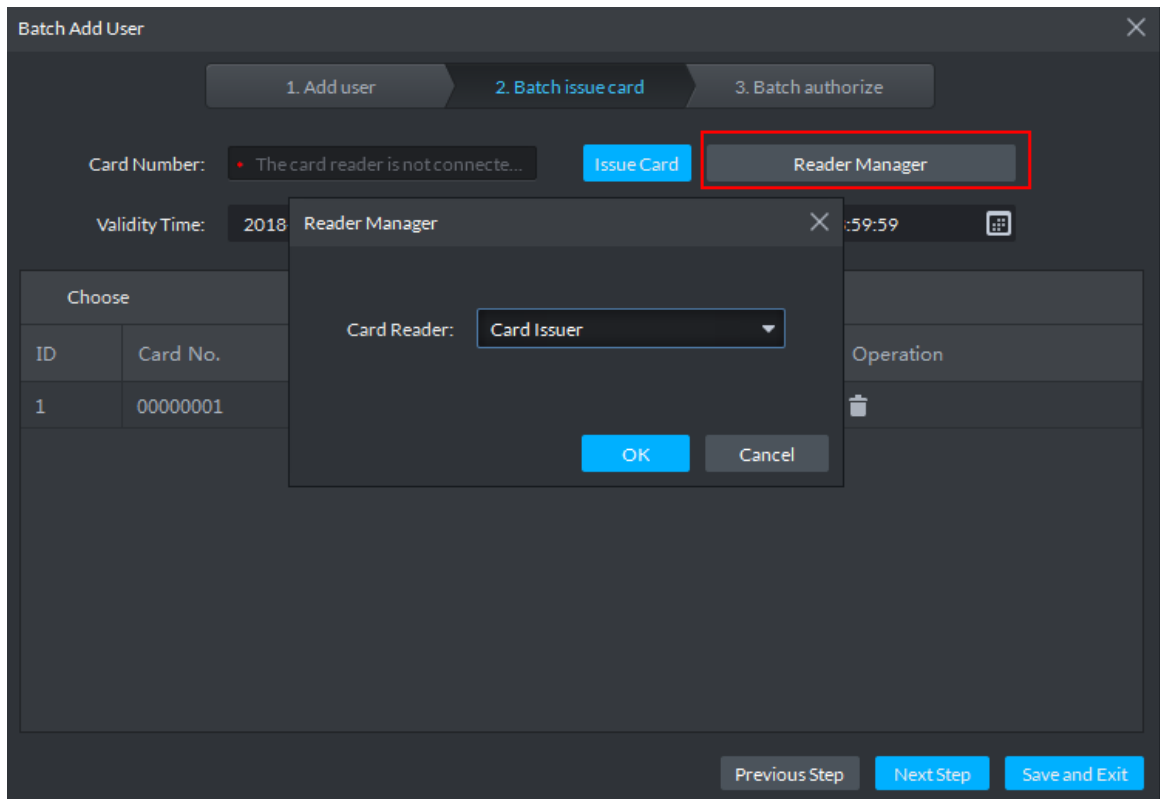


- Issue card by card reader

- 1) Click **Reader Manager**.

The **Reader Manager** interface is displayed. See Figure 3-262.

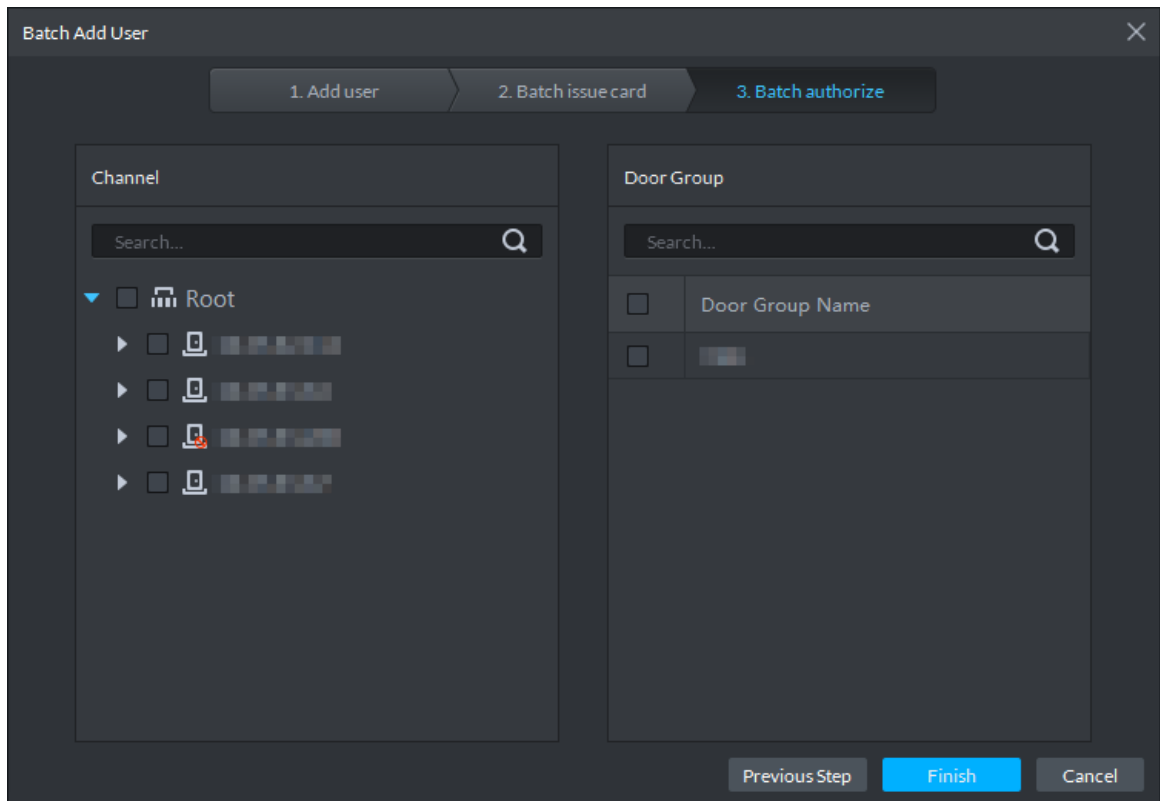
Figure 3-262 Reader manager



- 2) Select from **Card Reader** or **Device**, and click **OK**.
- 3) Swipe the card on the card reader or device.
- 4) Select a person, set up the validity time and expiry time, and click **Issue Card**.
- 5) Repeat the steps until all personnel get their cards.
- 6) Click **Next Step**.

The **Batch authorize** interface is displayed. See Figure 3-263.

Figure 3-263 Batch authorize



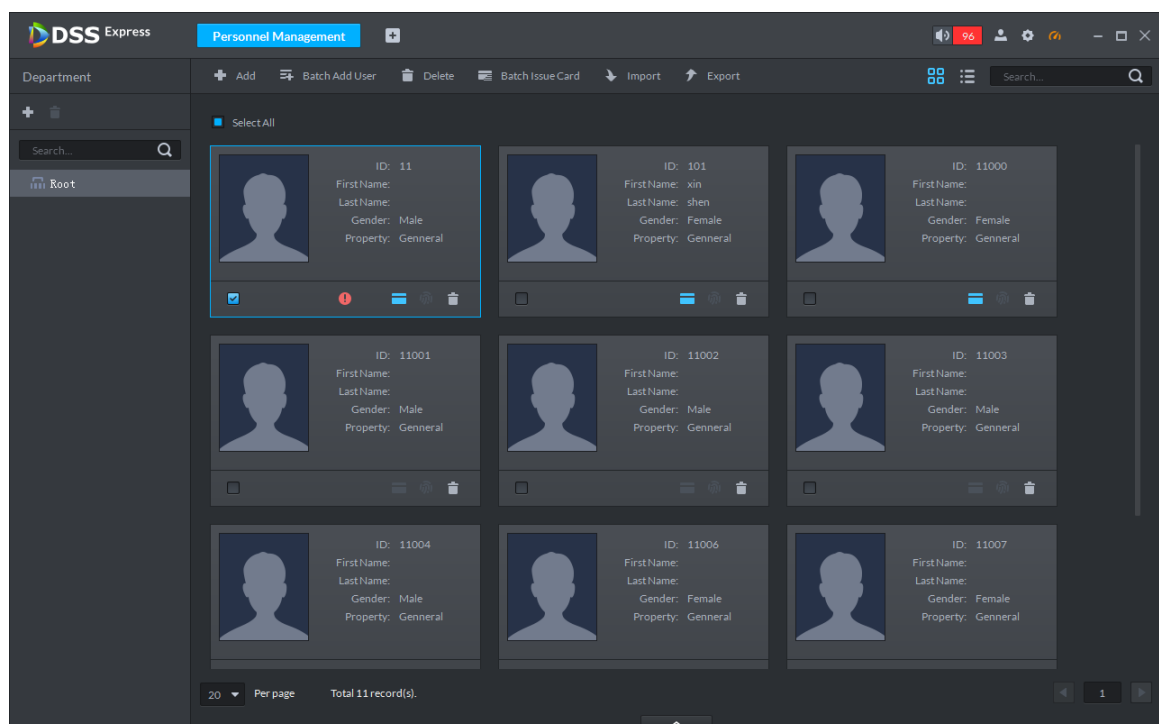
Step 4 Select the access control channels or door groups to which the personnel have access, and click **Finish**.

The interface displays info of added personnel. See Figure 3-264.



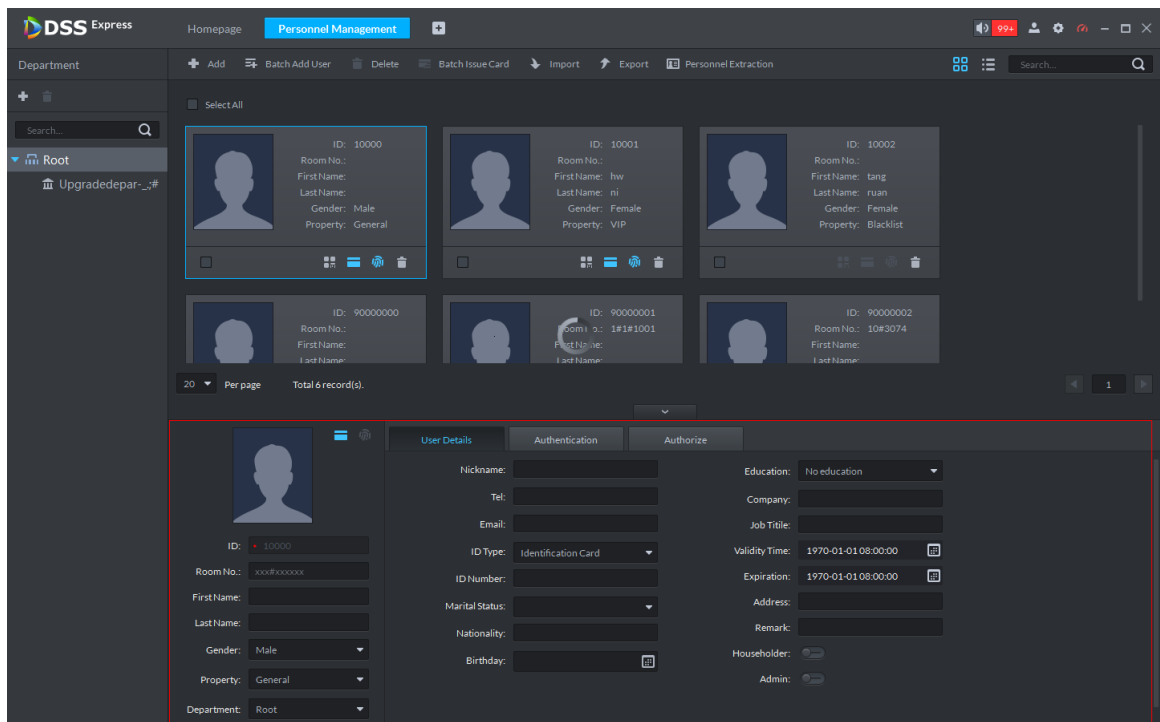
Door group is introduced in access control, for more details, see Access Control.

Figure 3-264 Batch add user



Step 5 Double-click a person, or select a person and click  to go to the screen for editing personnel information, where you can modify the personnel information. See Figure 3-265. Modification takes effect immediately.

Figure 3-265 Edit personnel



3.12.3 Editing Personnel

You can modify information of added person like user details, authentication and authorize except ID.

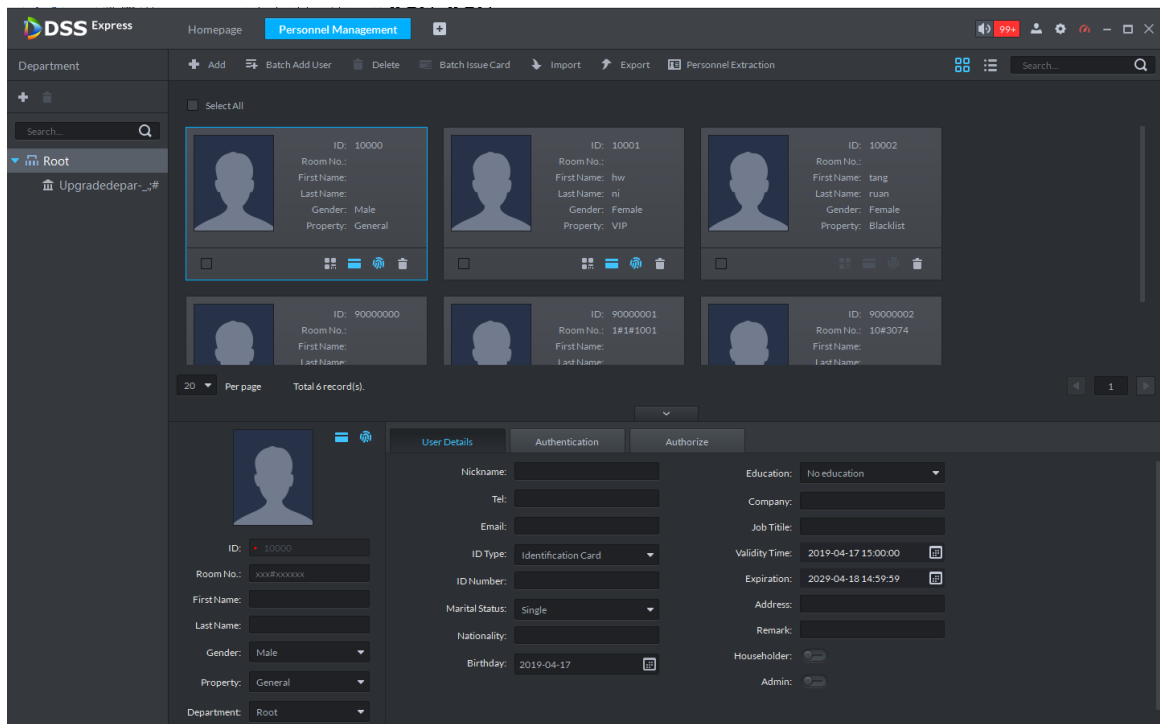


- If system adopts IR face attendance, you have to edit personnel and extract face feature code of person with same ID from IR face attendance device.
- If you want to read or import fingerprint, card or face feature from fingerprint collector, reader or IR face access control, please make sure the device is connected.

Step 1 On **Personnel Management** interface, double-click person, or select the person and click .

The interface of **Editing Personnel Info** is displayed. See Figure 3-266.

Figure 3-266 Edit personnel



Step 2 Modify personnel info and details except ID.

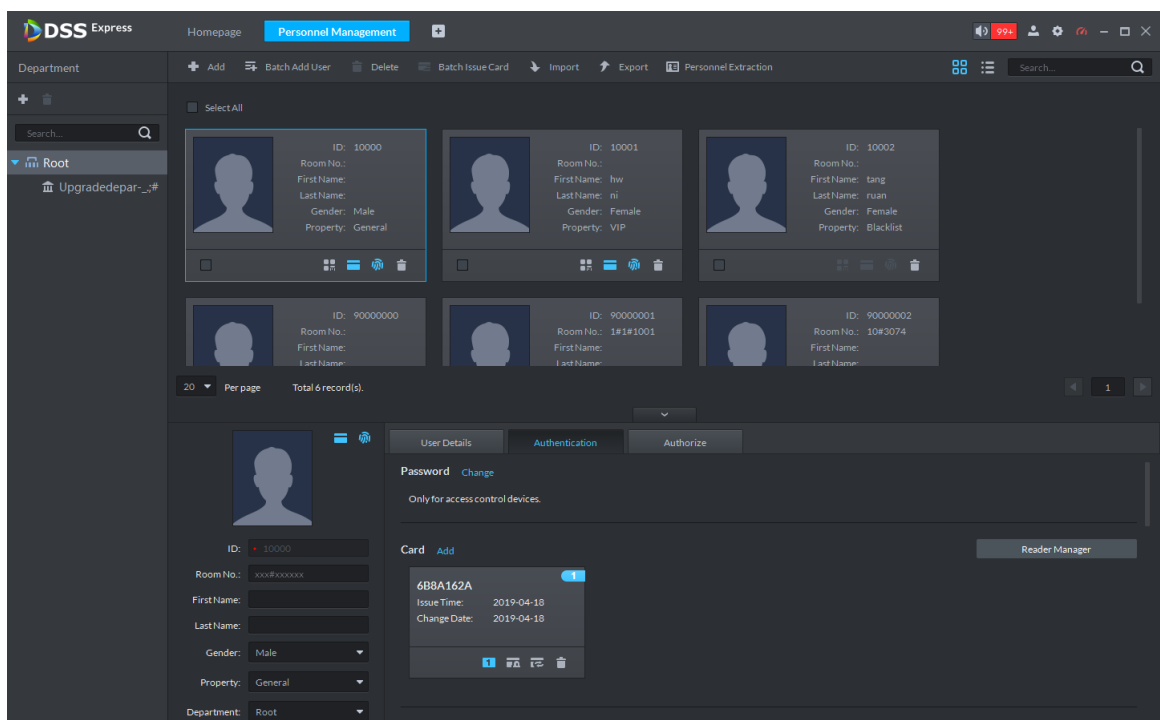


If the person is the first card unlock, then you need to set person property as **General**.

Step 3 Click **Authentication** tab.

The system displays **Authentication** interface, see Figure 3-267.

Figure 3-267 Authentication



Step 4 Click **Change**, you can set new password according to prompt, click **OK**. See Figure 3-268.

When the system is connected to access control, use password to unlock door, you need to set password.

Figure 3-268 Set password

Step 5 Manage card info.

After door card is added, and you can modify card. For more details, see Figure 3-269 and Table 3-37.

Figure 3-269 Add card

Table 3-37 Card operation

Icon	Description
	If a person has several cards, only the main card can be issued to 1st generation access control device. The first added card is considered as main card by default. Click the icon and it becomes , and then is displayed on upper right corner of the interface, which means that the card is set as main card. Click to cancel main card setting.
	Set the card as duress card, after that use the card to unlock, then duress alarm is generated. After clicking the icon, it becomes , is displayed on upper right corner of the interface, which means that the card is set as duress card. Click to cancel duress card setting.

Icon	Description
	Card cannot be used if it is damaged, so you can change a new card.
	Delete card info, after that the card has no unlock permission.

Step 6 Manage fingerprint.

Personnel fingerprint is collected, and you can modify status and name. For more details, see Figure 3-270.

Figure 3-270 Fingerprint collected

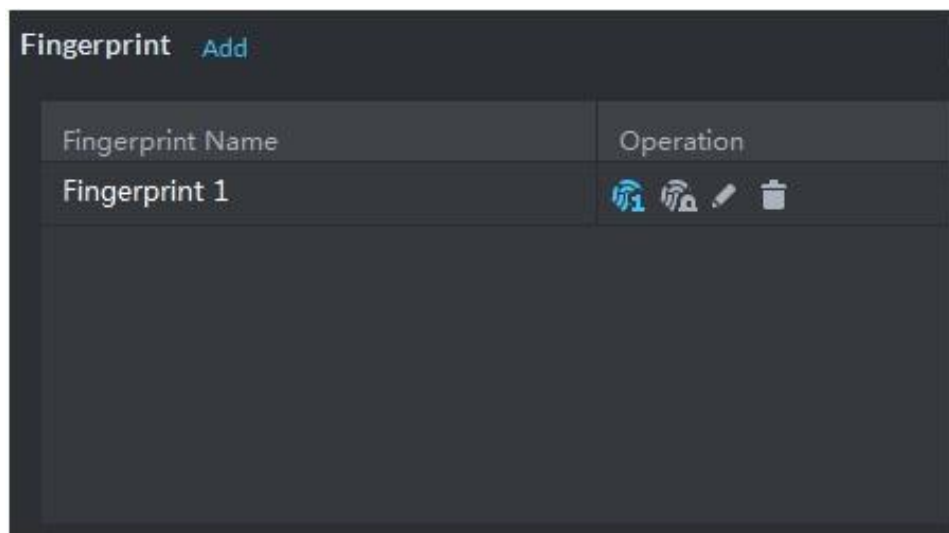


Table 3-38 Fingerprint operation

Icon	Description
	If more than 3 fingerprints are imported, then only then main fingerprint can be issued to access control device. The latest three fingerprints are considered as main fingerprint by default. One person can set max three main fingerprints. After clicking the icon, it becomes , which means that the fingerprint is set as main fingerprint. Click  and cancel main fingerprint setting.
	Set fingerprint as duress fingerprint, after that you can unlock the door by the fingerprint and generate duress alarm. Click the icon, it becomes , which means the fingerprint is set as duress fingerprint. Click  and cancel duress fingerprint setting.
	Modify fingerprint name.
	Delete fingerprint, after that the fingerprint has no permission to unlock door.

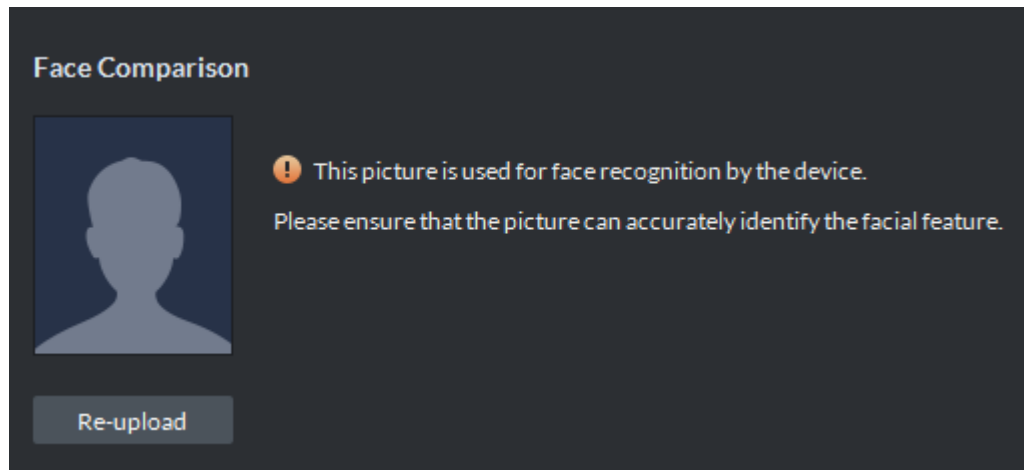
Step 7 Update face recognition picture.

Click **Re-upload** and upload new face picture according to system prompt.



Move the mouse to uploaded picture,  shows up on the picture, click the icon and delete the uploaded picture.

Figure 3-271 Upload face picture

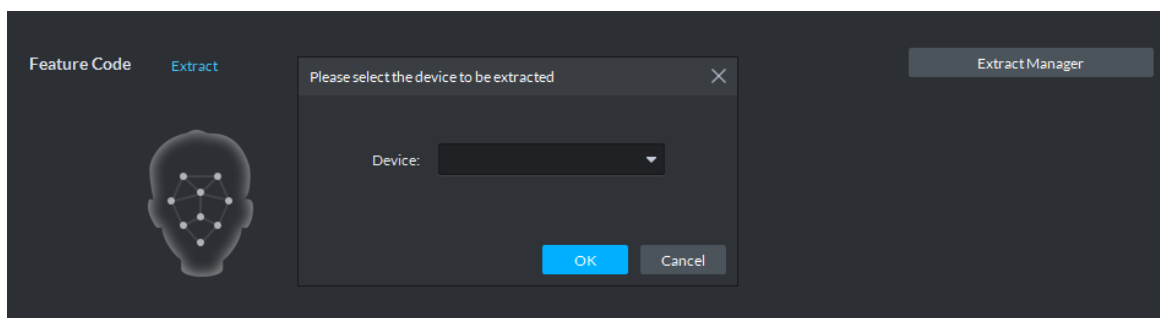


Step 8 Extract IR face feature code.

- 1) Click **Extract Manager**.

The system displays the interface of **Please select the device to be extracted**, see Figure 3-272.

Figure 3-272 Extract IR face feature code



- 2) Select IR face device, click **OK**.

- 3) Click **Extract**.

The system extracts IR face feature code from device, and prompts that extracted successfully.



The IR face feature code is extracted; click **Re-extract** to update IR face feature code.

Step 9 Modify available spots and plate number.

Click **Spots Available**, modify spots, click **Plate No.** and modify plate No.



Click  next to plate, or select plate and click  to delete plate.

Figure 3-273 Add vehicle

Vehicle

Spots Available: 0

	Plate No.	Operation
☐	[Redacted]	☐

Step 10 Click **Authorize**, modify access control and entrance is open to personnel. See Figure 3-274.

Figure 3-274 Authorize

AC channel Entrance

Search...

Door Group

Search...

☒	[Redacted]
☒	[Redacted]

Step 11 Click **OK** and confirm modification.

3.12.4 Importing/Exporting Personnel

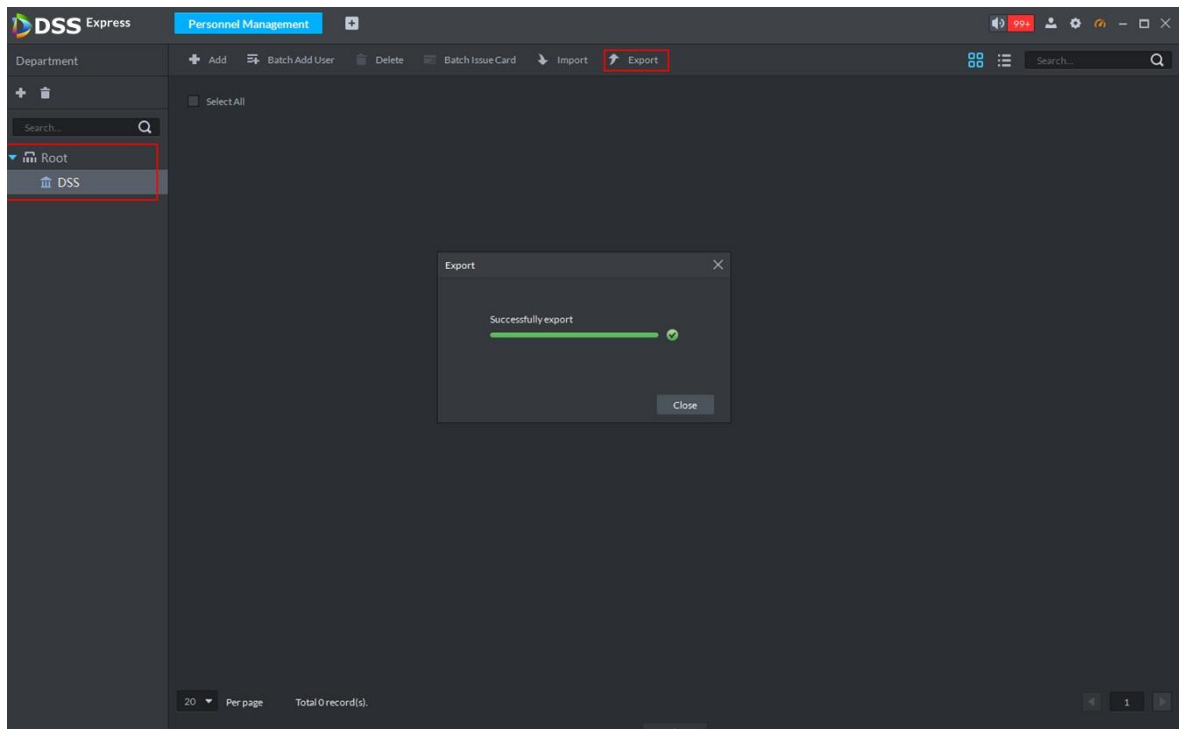
3.12.4.1 Exporting Personnel

Back up personnel data to restore damaged data or complete personnel configuration on the platform when there is a need for quick import of the personnel information.

Step 1 On the left side of the **Personnel Management** interface, select an organization, click **Export**, and follow the instructions on the interface to save the exported information to a local disk.

The system displays the progress of the export. See Figure 3-275.

Figure 3-275 Export personnel



Step 2 Select save path, click **Save**.

The system pops up **Export** dialog box, displays export progress.

Step 3 Click **Close** to close dialog box.

3.12.4.2 Importing Personnel

Edit the template or import information of existing personnel to quickly add them. You can import a file in .xls no larger than 1 M.

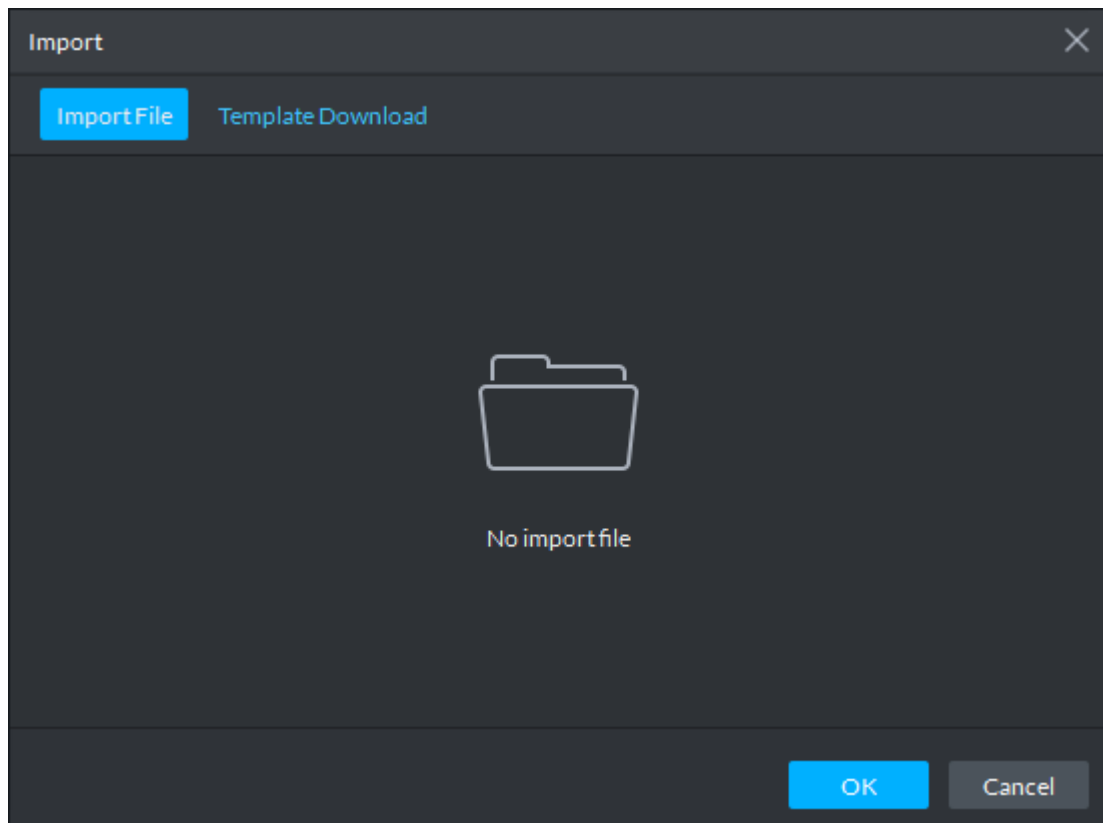


You can import personnel info exported from SmartPSS.

Step 1 On the **Personnel Management** interface, click **Import**.

The **Import** interface is displayed. See Figure 3-276.

Figure 3-276 Import



Step 2 Import personnel information files.

- 1) Click **Import**, and follow the instructions on the interface to select the 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**.

Complete the import of personnel information.

The following might occur during an import:

- The system prompts that the imported personnel already exist on the platform.
- Personnel ID duplicate in the imported file. If the same ID does not exist, the system accepts it as a new ID; if it already exists, the system gives a prompt.
- The system prompts that the imported personnel information is improperly filled, such as field length exceeding the limit on the client, and timeout resulting in a failure to upload to the database.
- Abnormal default values. The rules are: Gender (male), property (common staff), department (root node), ID type (Identification Card), marital status (null) and education (No education). The valid period starts from now and ends in 2028 by default.
- A person does not exist. If the department does not exist, a new department is 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.

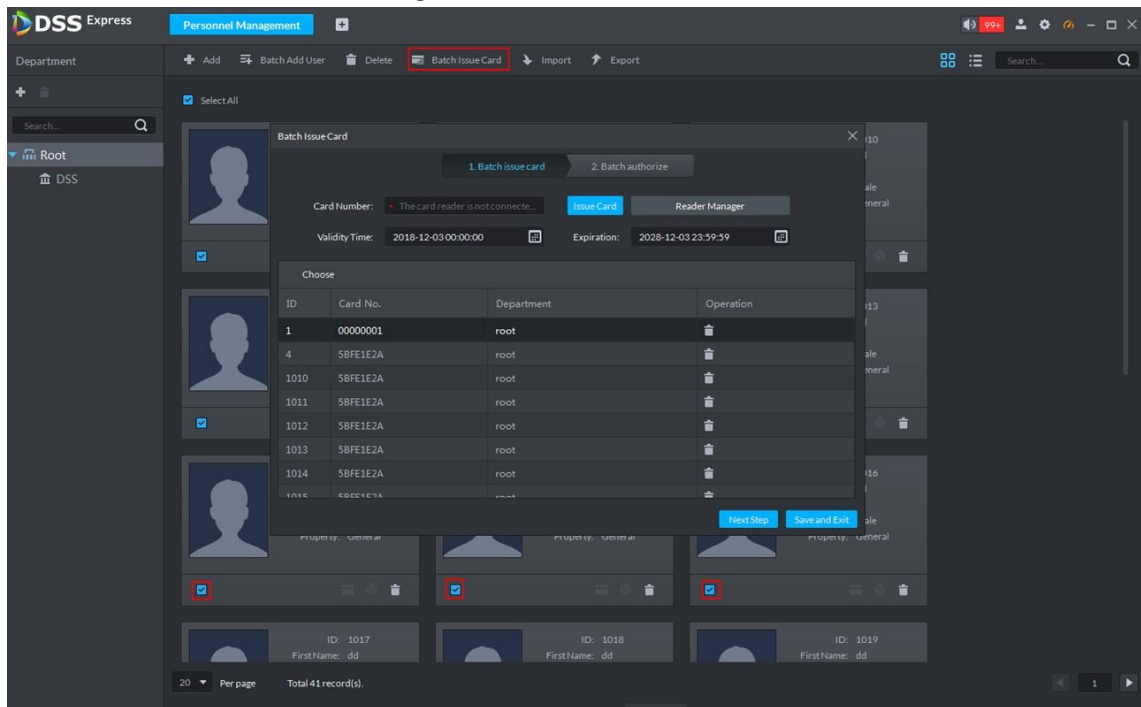
3.12.5 Batch Issue Card

Supports batch issuing cards to personnel to complete access control authorization.

Step 1 On the **Personnel Management** interface, select the personnel to issue card to, and click **Batch Issue Card**.

The **Batch issue card** interface is displayed. See Figure 3-277.

Figure 3-277 Batch issue card



Step 2 Issue cards to personnel.

You can issue card by entering card No. manually or card reader.

- Issue card by entering card No. manually

1) Select a person, enter the card number, and set up the validity time and expiry time.

2) Click **Issue Card**.

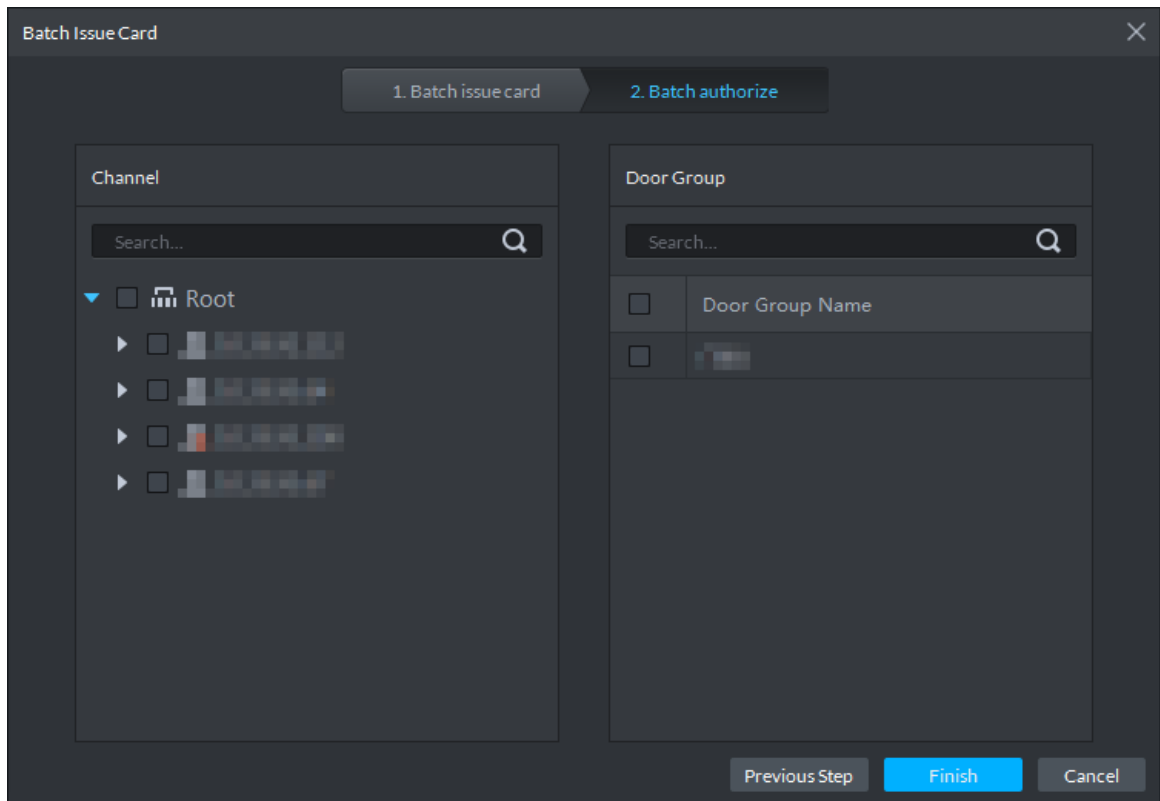
Complete issuing card to the selected personnel and the interface shows the personnel card number.

3) Repeat the steps until all personnel get their cards.

4) Click **Next Step**.

The **Batch authorize** interface is displayed. See Figure 3-278.

Figure 3-278 Batch authorize

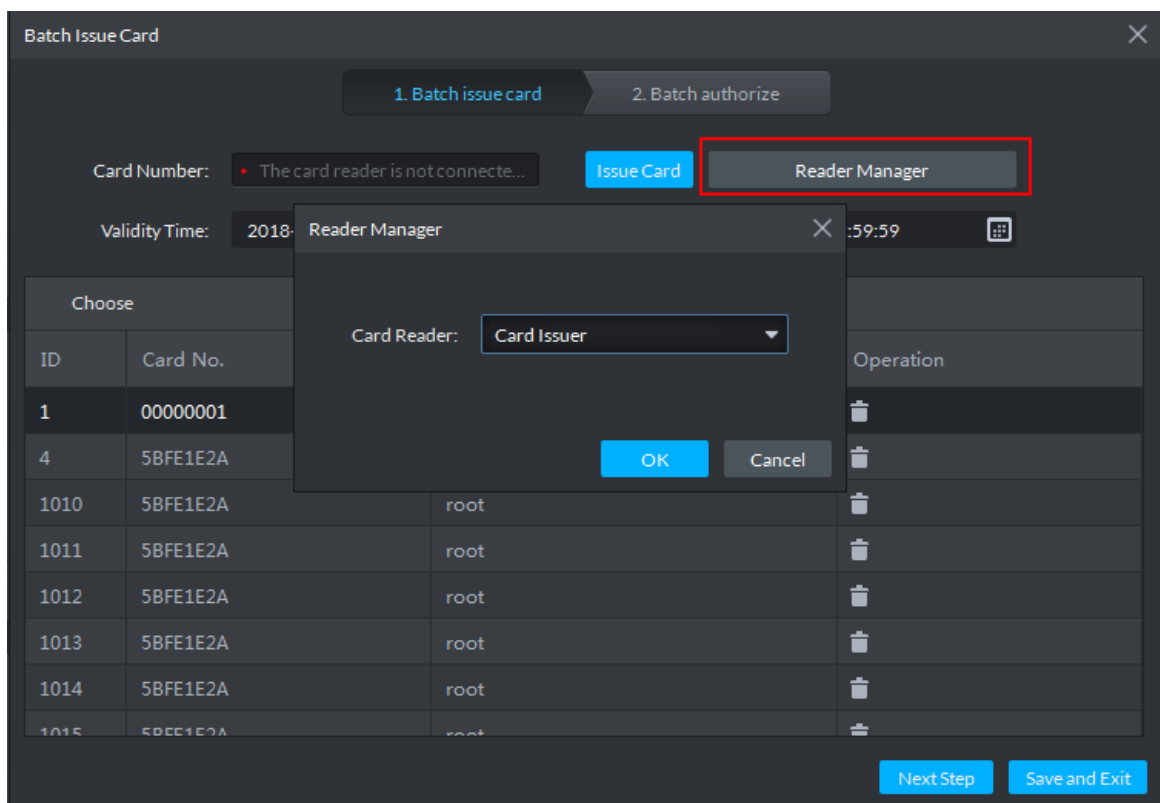


- Issue card by card reader

1) Click **Reader Manager**.

The **Reader Manager** interface is displayed. See Figure 3-279.

Figure 3-279 Reader manager

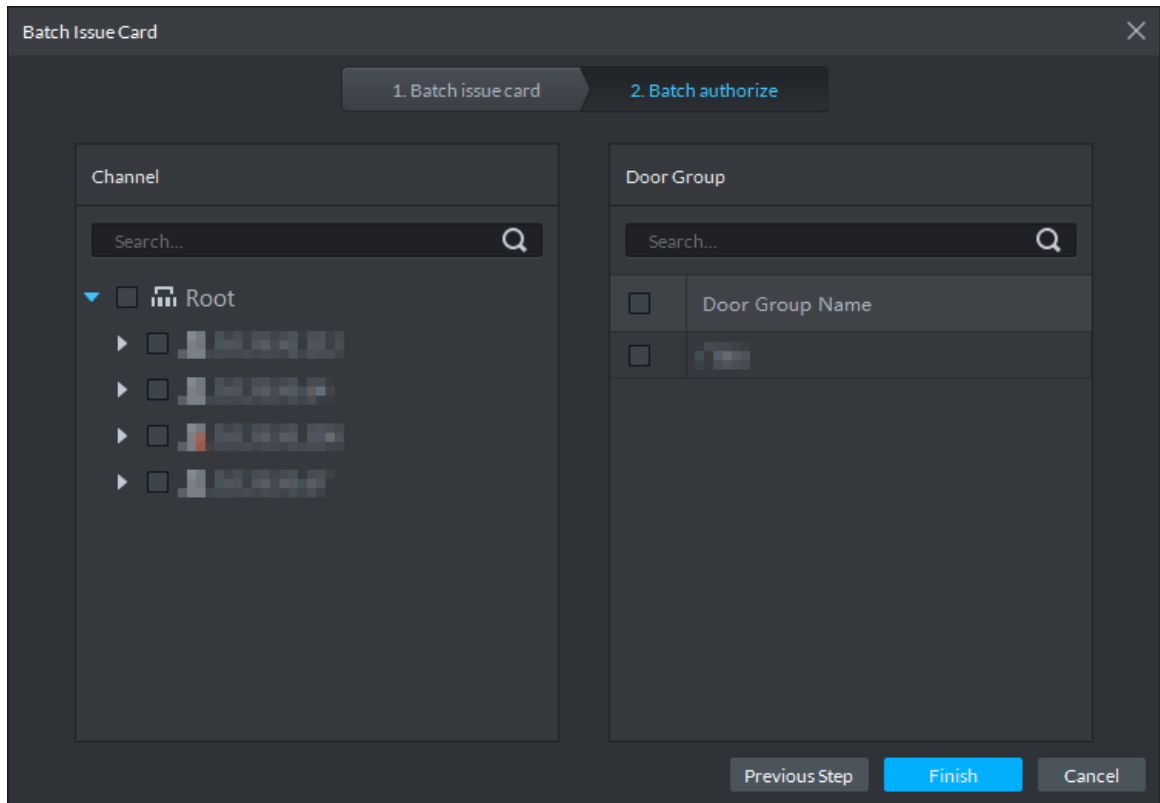


2) Select from **Card Reader** or **Device**, and click **OK**.

- 3) Swipe the card on the card reader or device.
- 4) Select a person, set up the validity time and expiry time, and click **Issue Card**.
- 5) Repeat the steps until all personnel get their cards.
- 6) Click **Next Step**.

The **Batch authorize** interface is displayed. See Figure 3-280.

Figure 3-280 Batch authorize

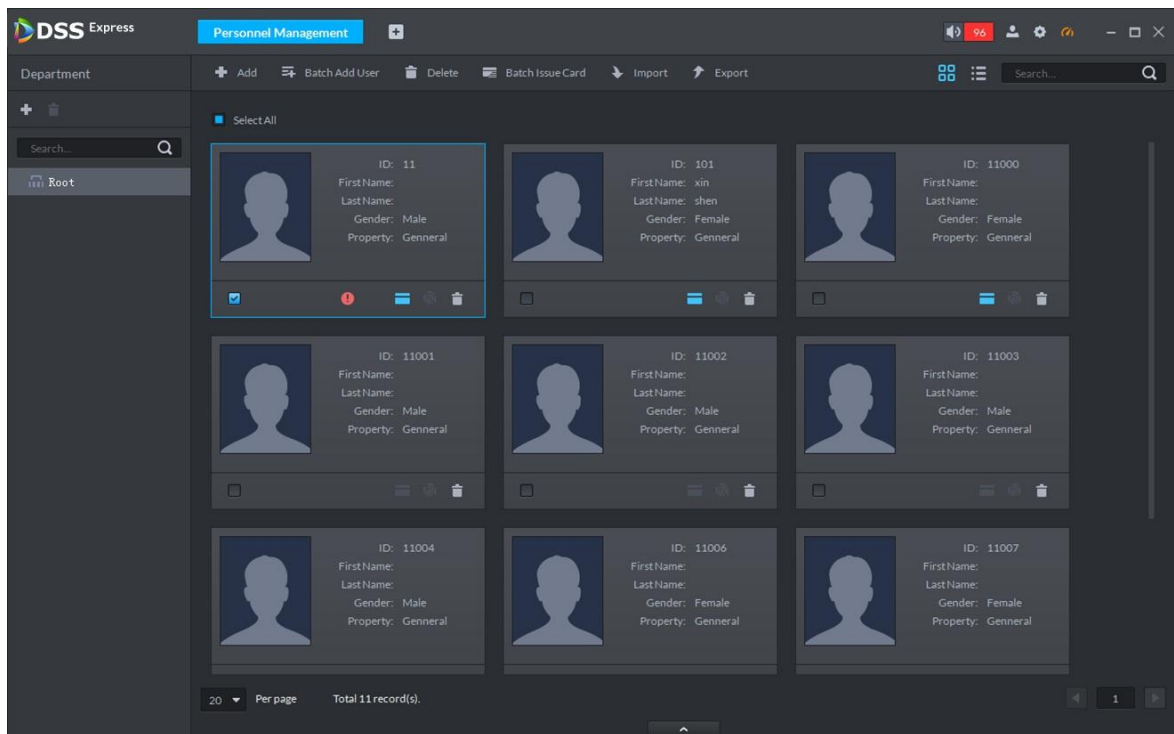


Step 3 Select the access control channels or door groups to which the personnel have access, and click **Finish**.

The interface displays the card issuing results. See Figure 3-281. The card icon

changes into blue, as  and it means that you have issued a card to the person.

Figure 3-281 Issue card result



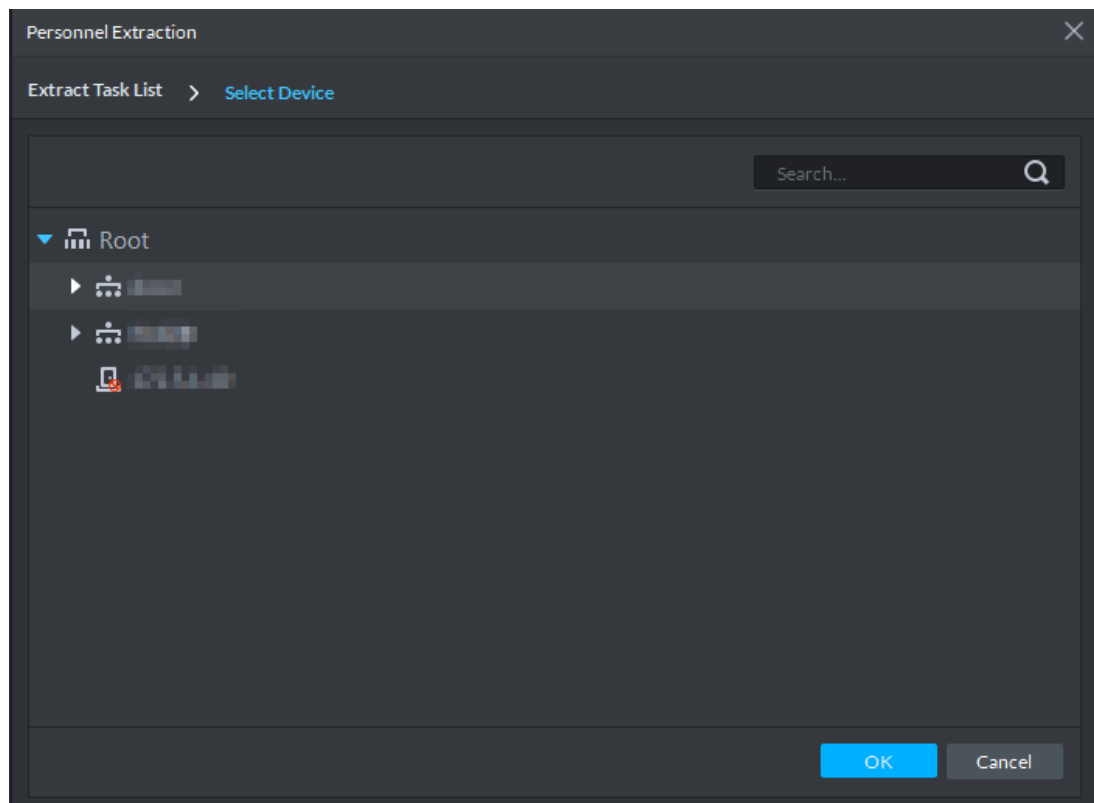
3.12.6 Personnel Extraction

Extract personnel info from access control, and sync it to platform.

Step 1 On **Personnel Management** interface, click **Personnel Extraction**.

The system displays **Personnel Extraction** interface, see Figure 3-282.

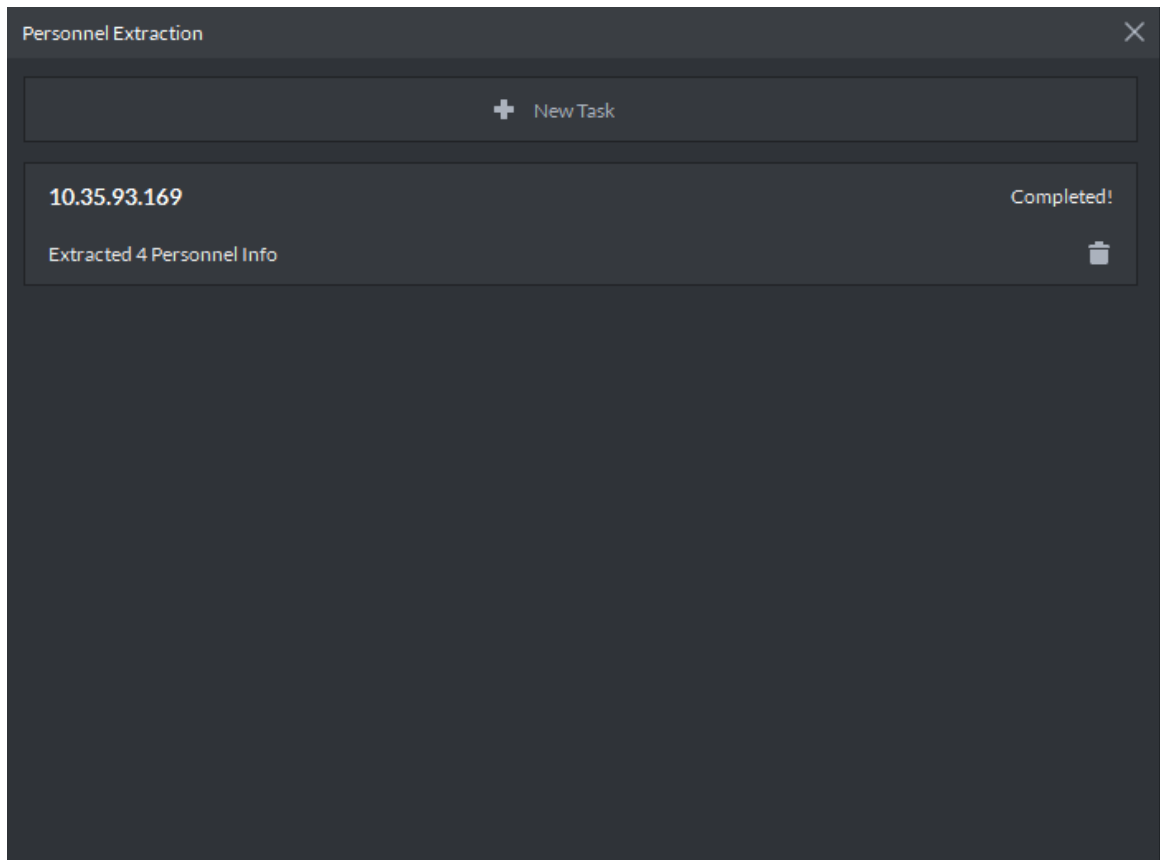
Figure 3-282 Personnel extraction



Step 2 Select access control device, click **OK**.

The system displays extraction result, see Figure 3-283.

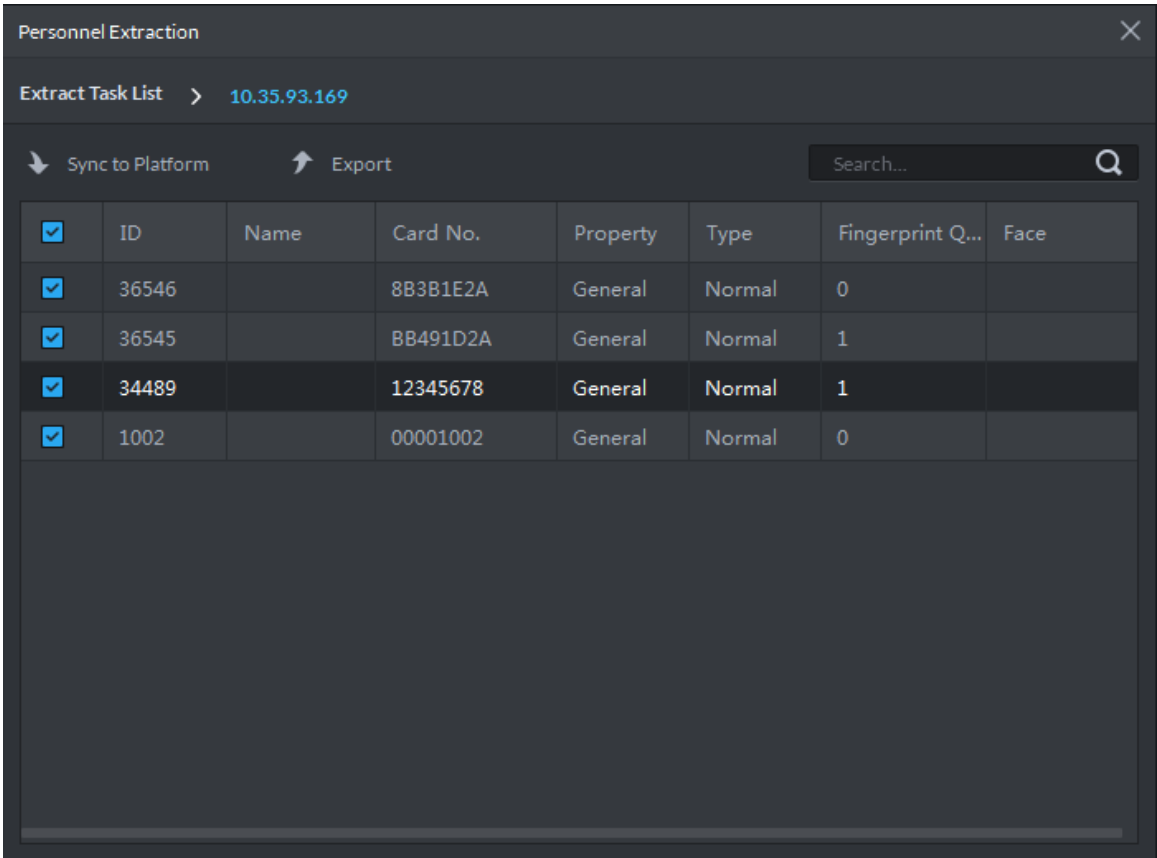
Figure 3-283 Extraction result



Step 3 Double click record.

The system displays info of extracted personnel, see Figure 3-283.

Figure 3-284 Extracted personnel detail



The screenshot shows a window titled "Personnel Extraction" with a close button (X) in the top right corner. Below the title bar, there is a breadcrumb navigation: "Extract Task List > 10.35.93.169". Below this, there are two buttons: "Sync to Platform" with a downward arrow icon and "Export" with an upward arrow icon. To the right of these buttons is a search bar with the placeholder text "Search..." and a magnifying glass icon. Below the buttons and search bar is a table with 8 columns: "ID", "Name", "Card No.", "Property", "Type", "Fingerprint Q...", and "Face". The table contains 5 rows of data, each with a blue checkmark in the first column. Below the table is a large, empty dark gray area.

☒	ID	Name	Card No.	Property	Type	Fingerprint Q...	Face
☒	36546		8B3B1E2A	General	Normal	0	
☒	36545		BB491D2A	General	Normal	1	
☒	34489		12345678	General	Normal	1	
☒	1002		00001002	General	Normal	0	

Step 4 Select personnel, click **Sync to platform**.

Select personnel and add to list.



Select personnel, click **Export** and save personnel info to local PC.

3.12.7 Generating Path

You can check all door unlocking records by personnel and generate a path.



To view the generated path, you have to drag the access control device to the map for display first. See 3.2.6 Configuring Emap for detailed steps.

Step 1 On **Personnel Management** interface, click  or  of the person.

Step 2 The **History** interface is displayed. See Figure 3-285.

Figure 3-285 Personnel history record

Time	ID	Card No.	Device	Door	Event	Person Name	Status
------	----	----------	--------	------	-------	-------------	--------

Step 3 Set up time for the search and click **Search**.

The system displays the search results.

Step 4 Click **Generate Path**.

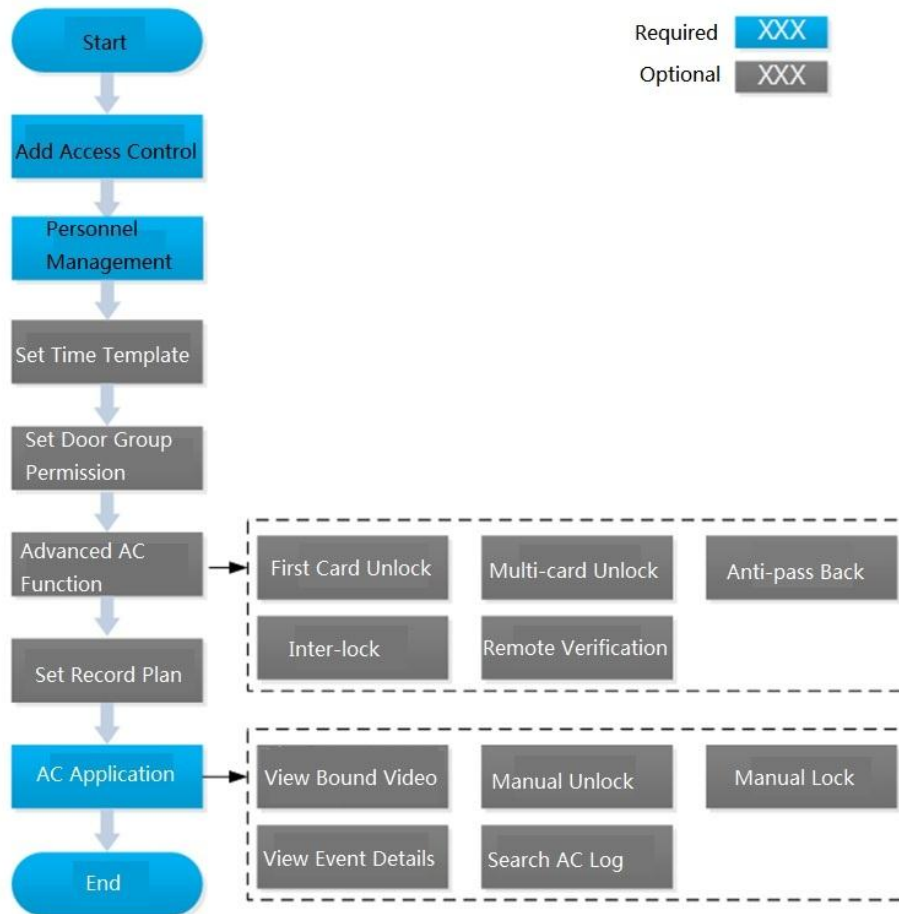
The system displays the map interface to show the activity path of the person.

Step 5 Click **Export**, and drag the mouse on the interface to select a region. Follow the instructions on the interface to save the path as a picture to a local disk.

3.13 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. For operation flow, see Figure 3-286.

Figure 3-286 AC management flow



3.13.1 Adding Access Control

Step 1 Add access control device. For more details, see **3.2.2.4 Adding Device**.

Support access control devices including general AC device, AC integrated controller, 2nd generation AC, face AC and IR face AC. 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, click **Resource Bind**, and see Figure 3-287. The system displays **Resource Bind** interface, see Figure 3-288.

Figure 3-287 Enter resource bind interface

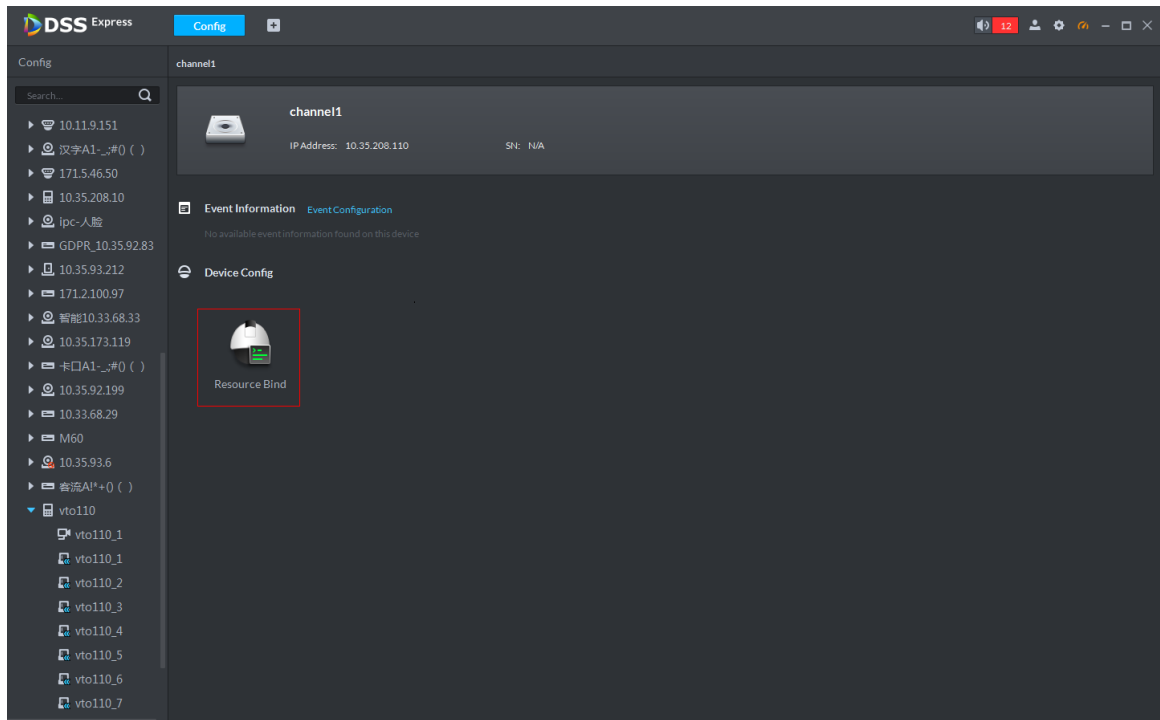
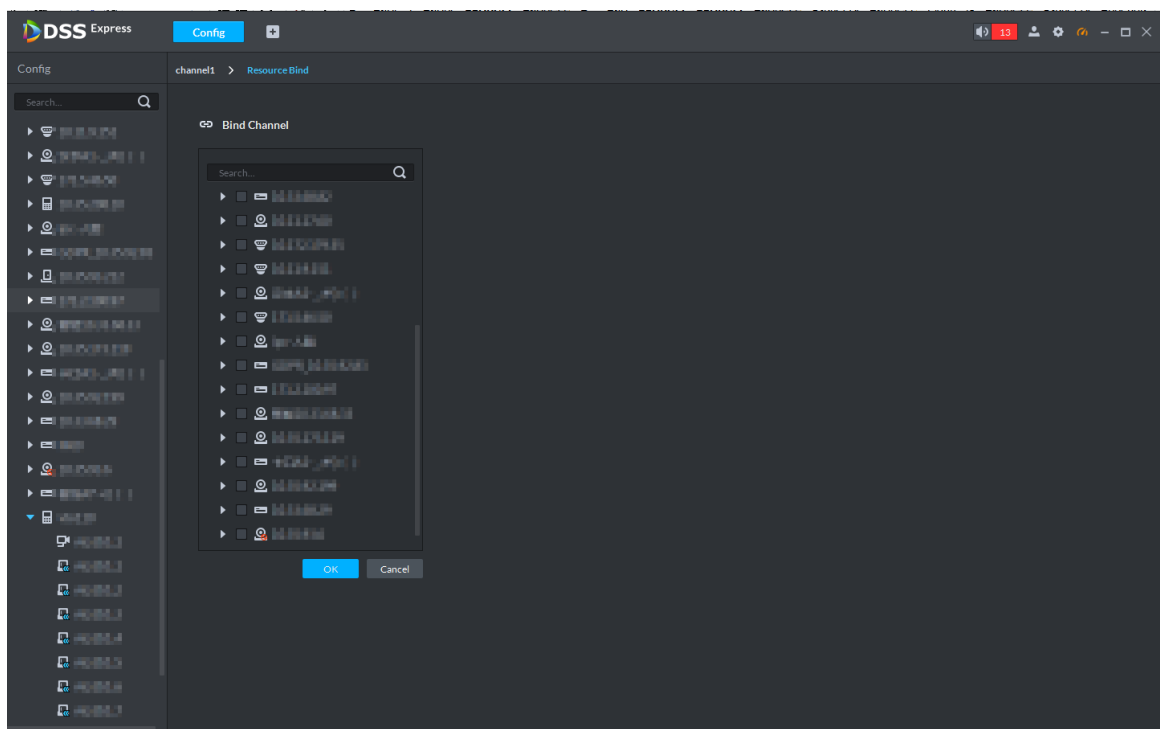


Figure 3-288 Resource bind



- 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**.
The system displays **Config** interface.
- 2) In left device tree, select AC channel, click **Door Configuration**, and see Figure 3-289.
The system displays **Door Config** interface, see Figure 3-290.



For the console on access control interface, right-click **AC Channel**, select **AC Channel Config** and enter **Door Config** interface.

Figure 3-289 Enter config interface

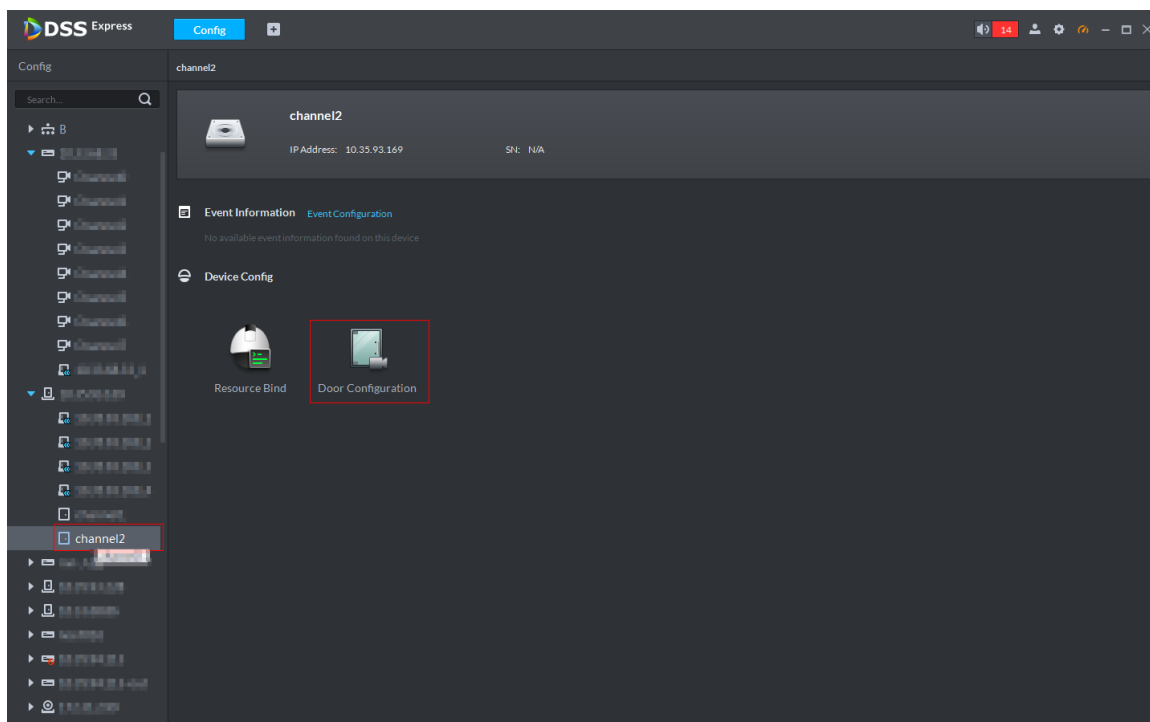


Figure 3-290 Door config

The screenshot shows a 'Door Config' window with the following settings:

- Set reader direction:** In **Reader 1** ⇌ Out **Reader 2**
- Door Status:** Always Open (dropdown)
- NO Period:** Disabled (toggle), All-Period Template (dropdown)
- NC Period:** Disabled (toggle), All-Period Template (dropdown)
- Alarm Enable:** Enabled (toggle)
- Alarm Types:** Intrusion (disabled), Timeout (disabled), Duress (checked), Over Times (disabled)
- Door Sensor Enable:** Disabled (toggle)
- Unlock Length:** 2 s
- Unlock timeout:** 60 s
- Unlock Method:** or (dropdown), with a help icon (?)
- Access Methods:** Card (checked), Fingerprint (checked), Password (checked)
- Buttons:** Copy to, Apply, OK, Cancel

- 3) Configure door information and click **OK**. For details of the parameters, see Table 3-39.



The interface might be different for different access control devices connected. The actual interfaces shall prevail.

Table 3-39 Door config 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.

Parameter	Description
Alarm Enable	• 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.
Door Sensor Enable	Enables the door sensor. The intrusion alarm and timeout alarm take effect only when door sensor is enabled.
Unlock Length	Sets up the duration of door unlocking. The door is automatically locked when the duration is over.
Unlock timeout	Unlock duration exceeding the Unlock timeout triggers a timeout alarm.
Unlock Method	You can use any one of the methods: card, fingerprint, face, and password, or any of their combinations to unlock the door.
Inter-door Lock	Indicates whether to enable Inter-door Lock.
Malicious Alarm	Swiping an unauthorized card for five times continuously within 50s triggers a malicious alarm. In the next 50s, every swipe of the card triggers a same alarm.

3.13.2 Personnel Management

If you want to add personnel, see 3.12 **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.

3.13.3 Managing Time Template

3.13.3.1 Setting Time Template

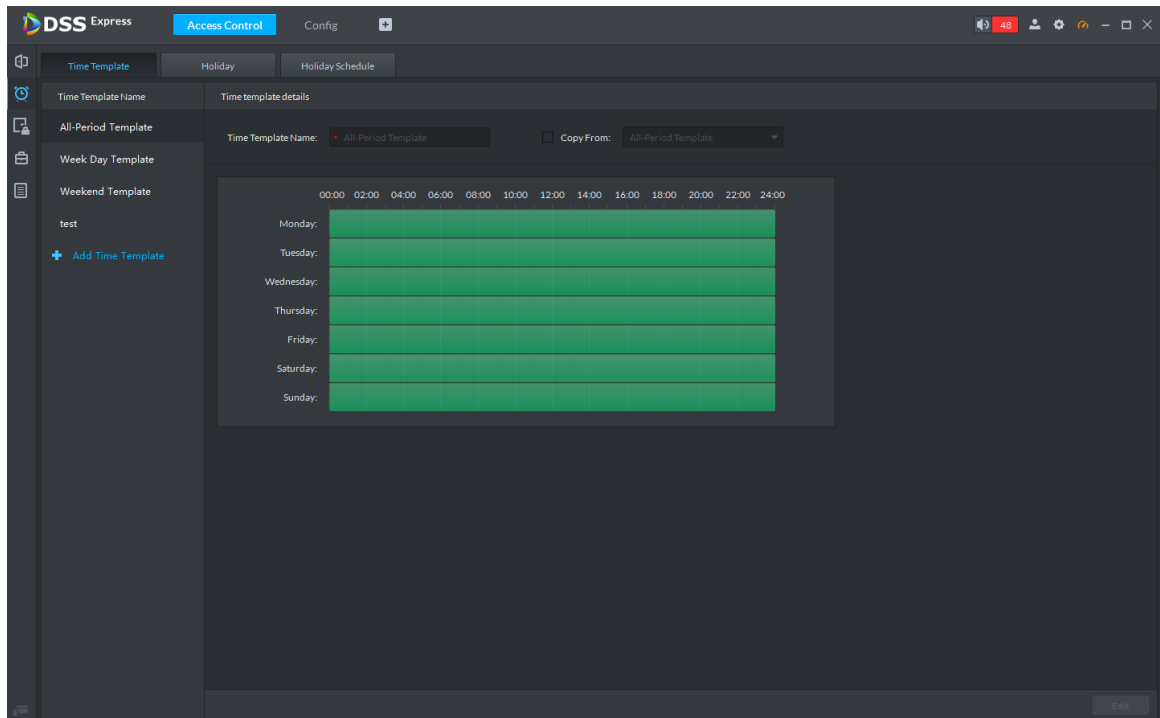
Default time template includes all-period template, week day template and weekend template. If default template fails to meet requirement, then set time template and you can adopt different unlock modes at different time.

Step 1 On client homepage, click **Access Control**.

The system displays **Access Control** interface.

Step 2 Click  and the system displays **Time Template** interface, see Figure 3-291.

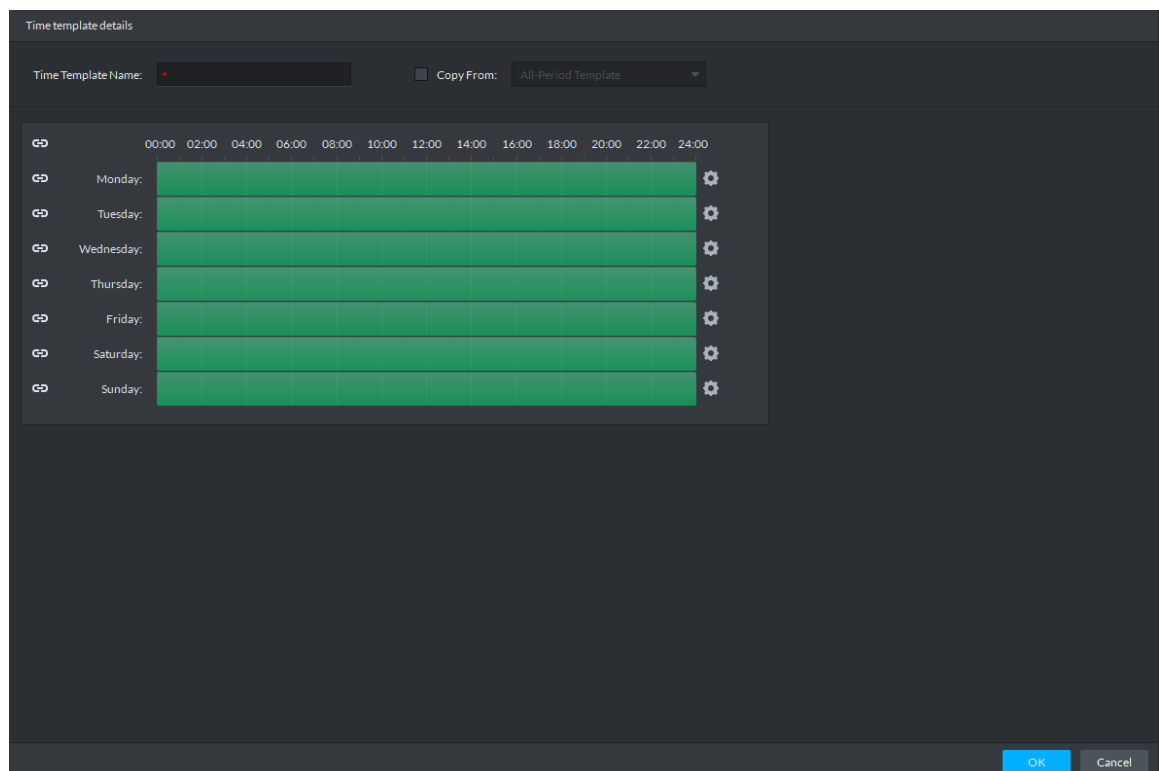
Figure 3-291 Time template



Step 3 Click **Add Time Template**.

The **Time template details** interface is displayed. See Figure 3-292.

Figure 3-292 Add time template



Step 4 Set up **Time Template Name** and the required time period, and click **OK**.



Select **Copy From** and the copied template, and you can use the time periods of the copied template. In this way, you can quickly configure the time periods by modifying the ones of the copied template.

Methods to set up the time period:

- Method I: Press and hold the left button of the mouse. Over the time periods not selected, the mouse displays as a pen, and you can drag the mouse on the setting interface to select a time period. Over the selected time periods, the mouse displays as an eraser, and you can erase selected time periods with it.



Click the icons  in front of multiple week numbers one by one and the icons change to . In this way, you can configure the time periods corresponding to the week numbers. You can quickly select all the week numbers by clicking  on the top.

- Method II: Click  and set up the time periods in the popup interface. You can set up six time periods at most.

Step 5 The new time template is displayed in the left list.

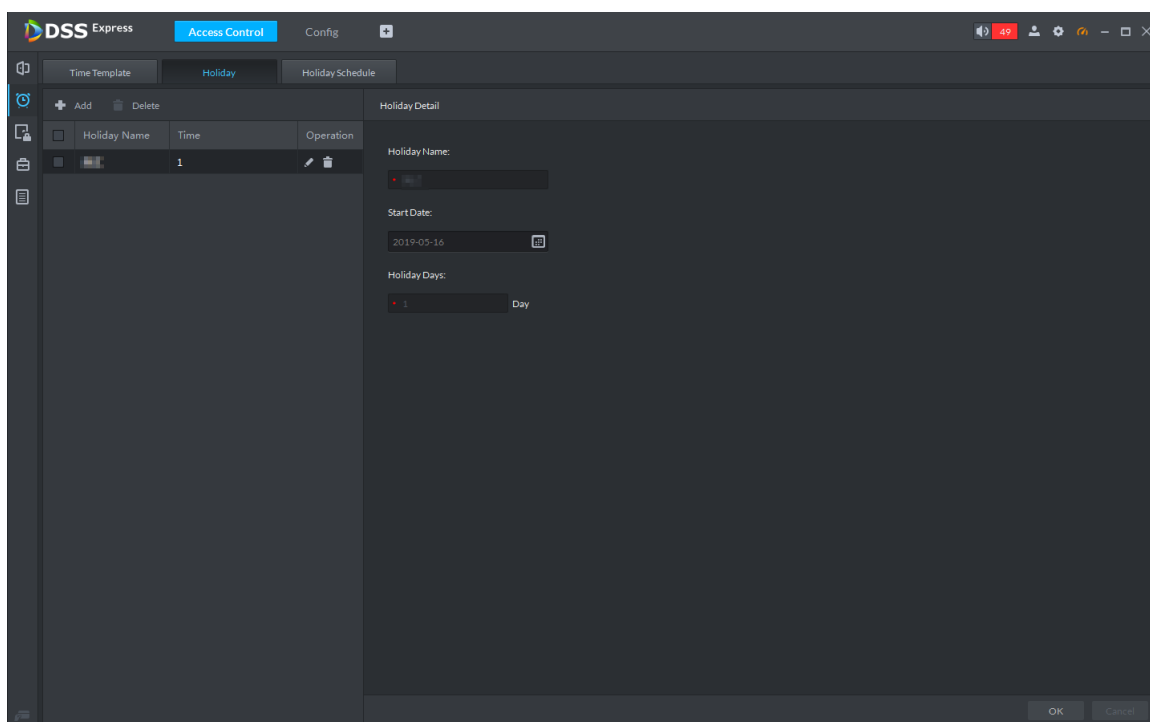
3.13.3.2 Setting Holiday

Set holiday according to actual situation, used to configure holiday plan, and you can unlock according to holiday plan.

Step 1 On **Access Control** interface, click  and select **Holiday**.

The system displays **Holiday** interface, see Figure 3-293.

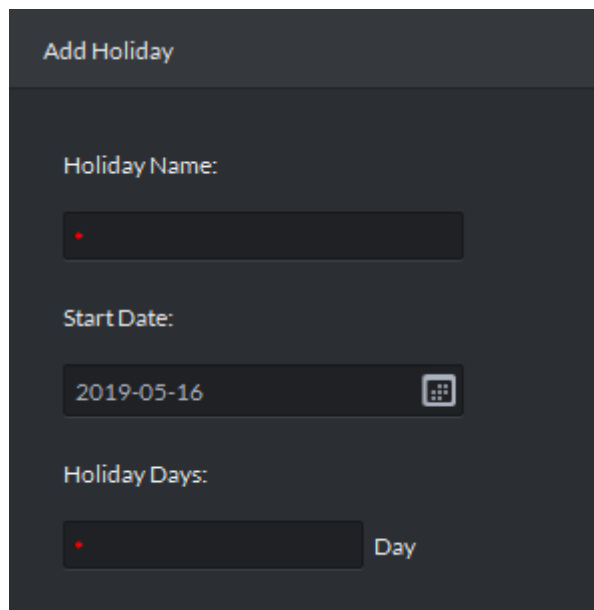
Figure 3-293 Holiday



Step 2 Click **Add**.

The system displays holiday config interface, see Figure 3-294.

Figure 3-294 Add holiday



The 'Add Holiday' dialog box contains the following fields:

- Holiday Name:** A text input field with a red asterisk indicating it is required.
- Start Date:** A date picker showing '2019-05-16' with a calendar icon.
- Holiday Days:** A text input field with a red asterisk, followed by a 'Day' button.

Step 3 Set holiday info, click **OK**.

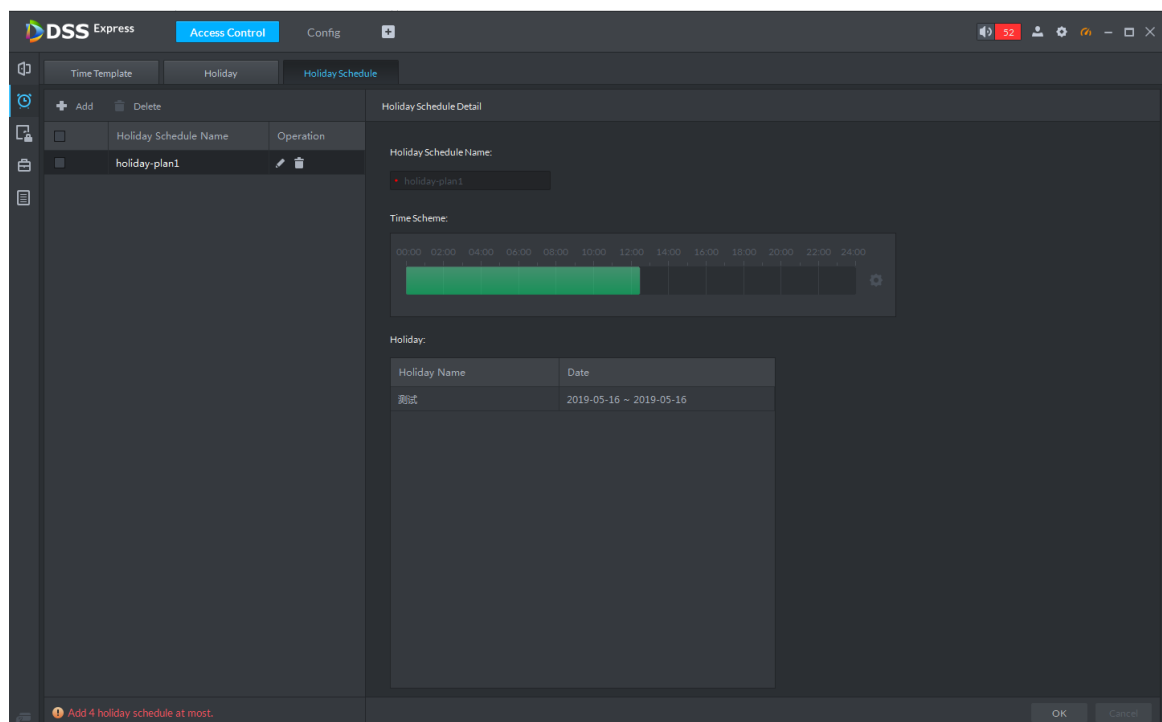
3.13.3.3 Setting Holiday Schedule

Door group can unlock according to the holiday schedule that is set.

Step 1 On **Access Control** interface, click  and select **Holiday Schedule**.
The system displays **Holiday Schedule** interface.

Step 2 Click **Add**.
The system displays interface of add holiday schedule, see Figure 3-295.

Figure 3-295 Add holiday schedule



The 'Add holiday schedule' interface in DSS Express includes the following components:

- Navigation:** 'Time Template', 'Holiday', and 'Holiday Schedule' tabs.
- Left Panel:** A list with 'Add' and 'Delete' buttons, showing 'holiday-plan1' with an edit icon.
- Holiday Schedule Detail:**
 - Holiday Schedule Name:** A text field containing 'holiday-plan1'.
 - Time Scheme:** A timeline from 00:00 to 24:00 with a green bar from 00:00 to 12:00.
 - Holiday:** A table with the following data:

Holiday Name	Date
测试	2019-05-16 ~ 2019-05-16

At the bottom, there is a status bar with the message 'Add 4 holiday schedule at most.' and 'OK'/'Cancel' buttons.

Step 3 Set holiday schedule parameters, click **OK** and complete config.

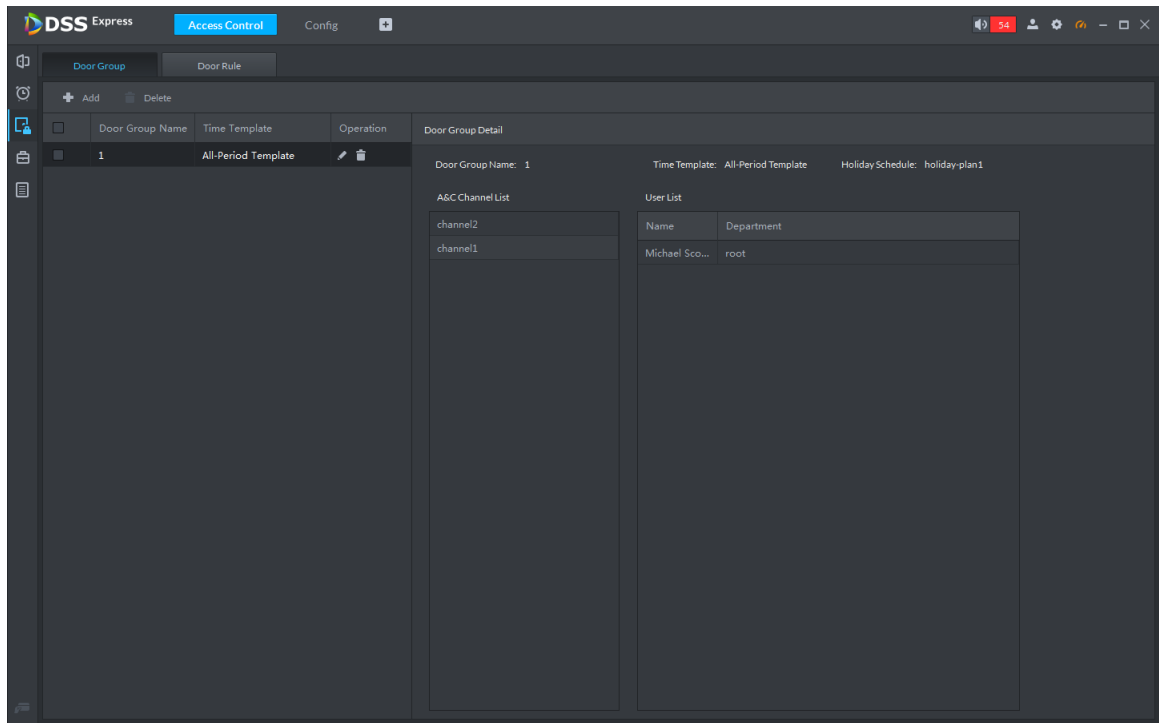
3.13.4 Setting Access Level

If you manage the doors by groups, you can quickly grant users with the authorizations to unlock the doors in a specific group.

Step 1 On the **Access Control** interface, click .

The **Access Level** interface is displayed. See Figure 3-296.

Figure 3-296 Access level



Step 2 Create door groups.

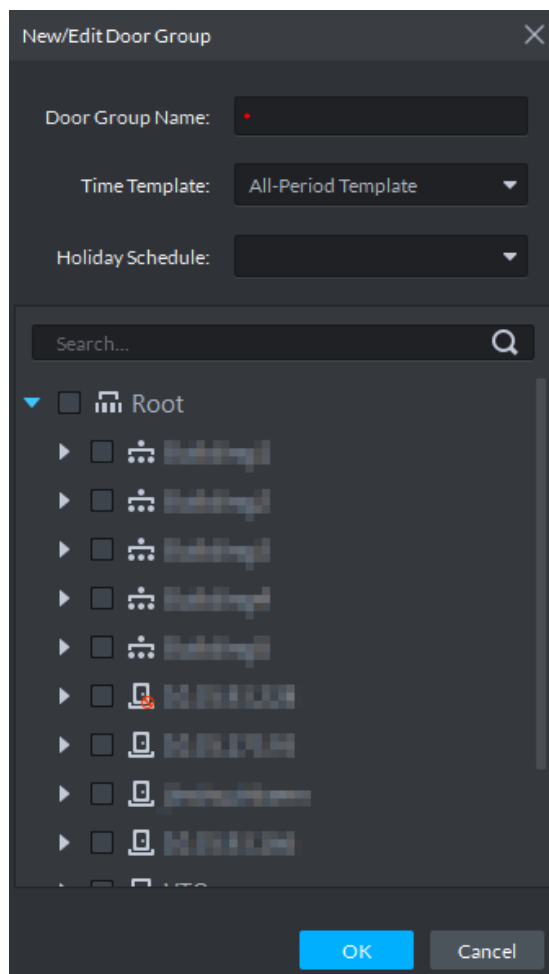
- 1) Click the **Door Group** tab.

The **Door Group** interface is displayed.

- 2) Click **Add**.

The **New/Edit Door Group** interface is displayed. See Figure 3-297.

Figure 3-297 New/Edit door group



The image shows a 'New/Edit Door Group' dialog box. It has a title bar with a close button. Inside, there are three input fields: 'Door Group Name' with a red asterisk indicating it is required, 'Time Template' with a dropdown menu showing 'All-Period Template', and 'Holiday Schedule' with a dropdown menu. Below these is a search bar with the placeholder text 'Search...'. Under the search bar is a tree view starting with 'Root' (expanded), followed by several sub-items, each with a checkbox and a folder icon. The last item in the list has a red error icon. At the bottom right are 'OK' and 'Cancel' buttons.

- 3) Enter **Door Group Name**, select **Time Template** and an access control channel, and click **OK**.

After selecting the time template and access control channel, you can only use the time periods of the selected time template and the selected access control channel when granting authorizations to users. The interface displays the information of the newly created door groups.

Step 3 Authorize users.

- 1) Click the **Door Rule** tab.
The **Door Rule** interface is displayed.
- 2) Click **Add**.
The **Add door rule** interface is displayed. See Figure 3-298.

Figure 3-298 Add door rule

Door Rule Name: *

Remark:

Person

Root Search...

☐	ID	Name
☐	1	
☐	4	ic4
☐	1010	dd xx
☐	1011	dd xx
☐	1012	dd xx

Selected(0)

ID	Name	Department	Operation

Door Group

☐	Door Group Name
☐	Group1

OK Cancel

- 3) Enter **Door Rule Name**, select **Person** and **Door Group**, and click **OK**.
The interface displays the authorization information.

3.13.5 Advanced Function

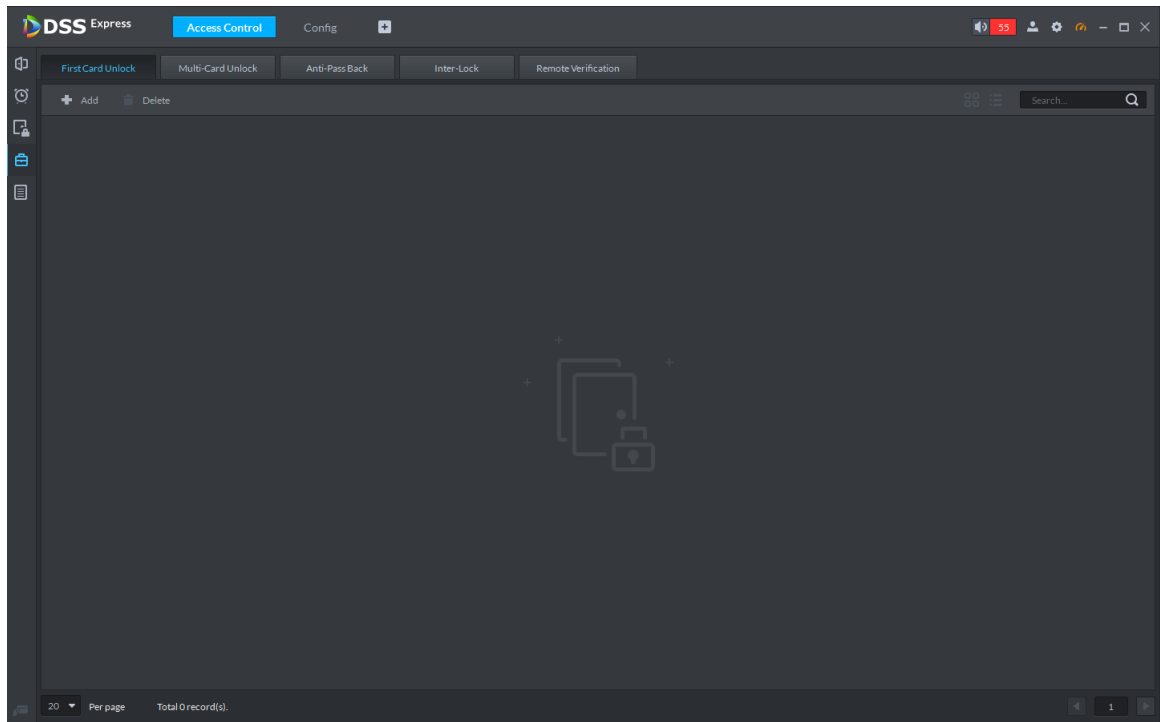
3.13.5.1 First Card Unlock

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.

Step 1 On the **Access Control** interface, click and select **First Card Unlock**

The **First Card Unlock** interface is displayed. See Figure 3-299.

Figure 3-299 First card unlock



Step 2 Click **Add**.

The **First Card Unlock Configuration** interface is displayed. See Figure 3-300.

Figure 3-300 First card unlock config

Door:

Time Template:

All-Period Template

Status:

Normal

User List

Root

Search...

	ID	Name
☐	1	
☐	4	ic4
☐	1010	dd xx
☐	1011	dd xx
☐	1012	dd xx
☐	1013	dd xx
☐	1014	dd xx
☐	1015	dd xx
☐	1016	dd yy

Selected(0)

ID	Name	Department	Operation
----	------	------------	-----------

OK

Cancel

Step 3 Configure the **First Card Unlock** parameters and click **OK**. For details of the

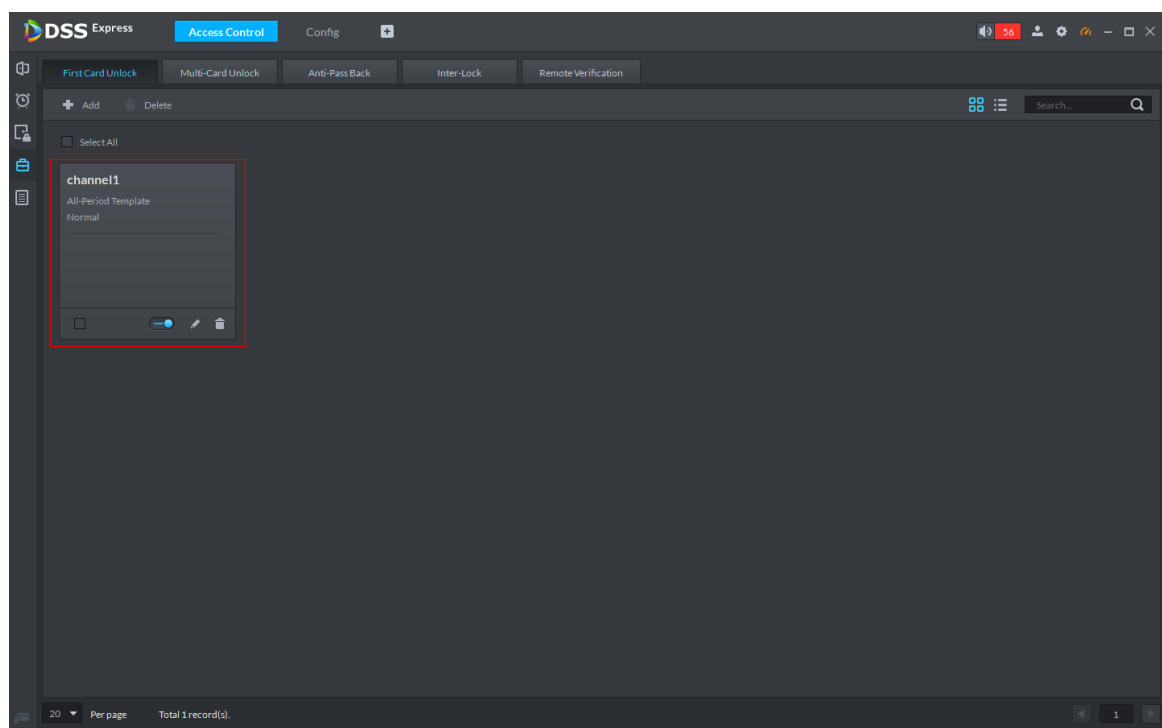
parameters, see Table 3-40.

The system displays the **First Card Unlock** information. See Figure 3-301. First Card Unlock is enabled by default.

Table 3-40 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 3-301 First card info list



Step 4 Click .

The icon changing into  indicates **First Card Unlock** is enabled.

3.13.5.2 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.

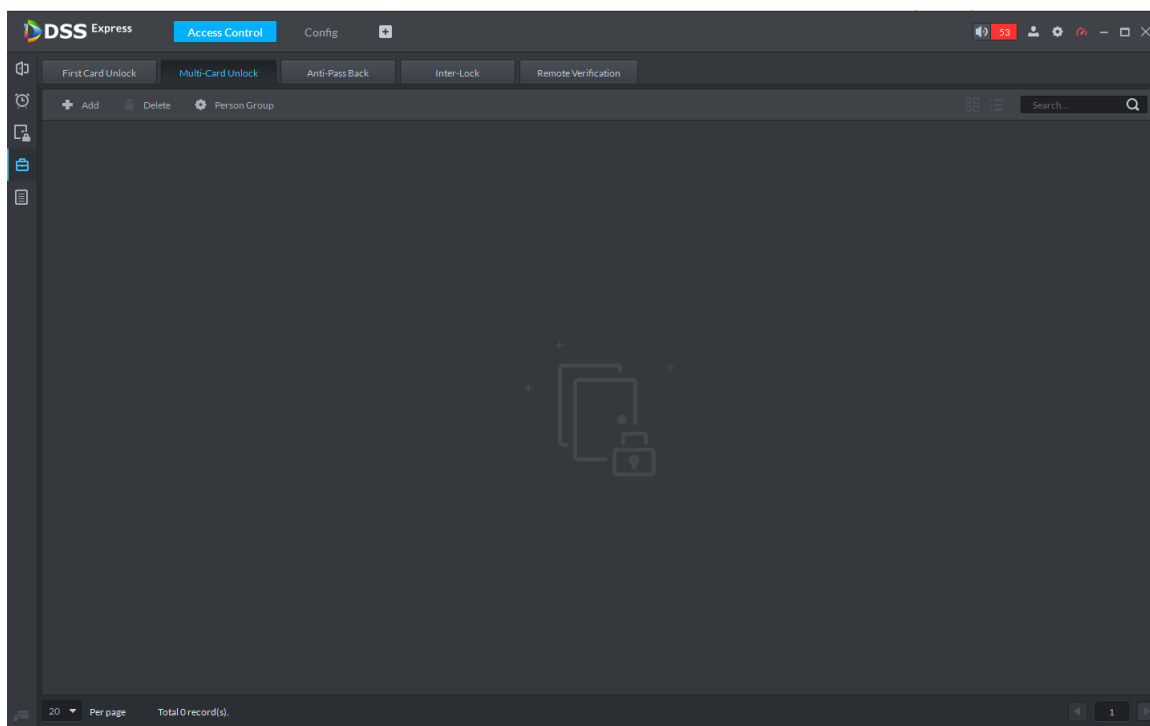


- One group can have up to 64 users.
- With Multi-Card Unlock enabled for an access control channel, it supports up to four groups of users being on site at the same time for verification. The total number of users can be 64 at most, with up to five valid users.

Step 1 On the Access Control interface, click  and select **Multi-card Unlock**.

The **Multi-Card Unlock** interface is displayed. See Figure 3-302.

Figure 3-302 Multi-card unlock

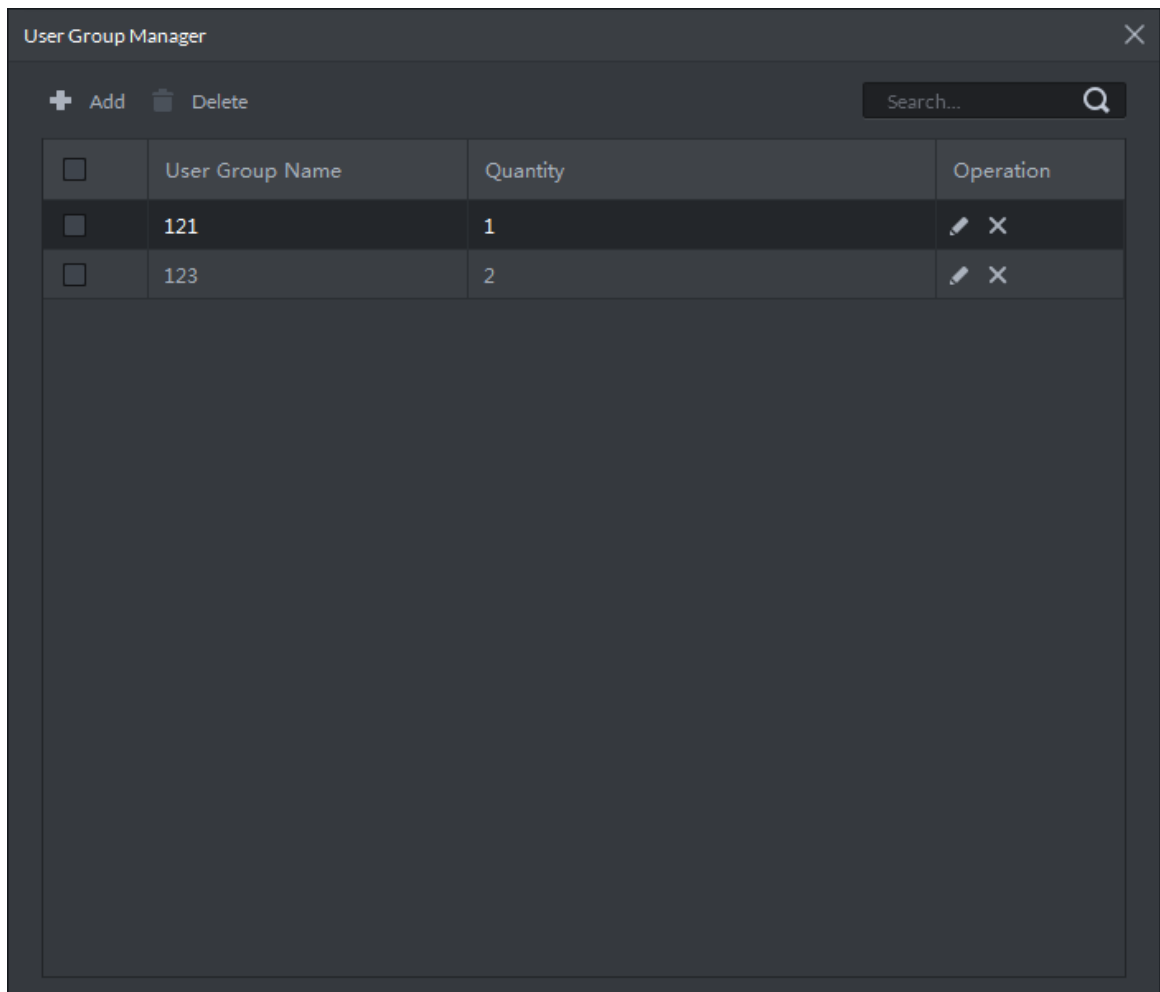


Step 2 Add user group.

1) Click **Person Group**.

The **User Group Manager** interface is displayed. See Figure 3-303.

Figure 3-303 User group manager



- 2) Click **Add**.

The **User Group Manager** interface is displayed. See Figure 3-304.

Figure 3-304 User group config

User Group Manager

User Group List > User Group Configuration

User Group Name:

User List:

☐	ID	Name
☐	1001	w w
☐	1002	m m
☐	1003	z z

Selected(0)

ID	Name	Department	Operation
----	------	------------	-----------

OK Cancel

- 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.

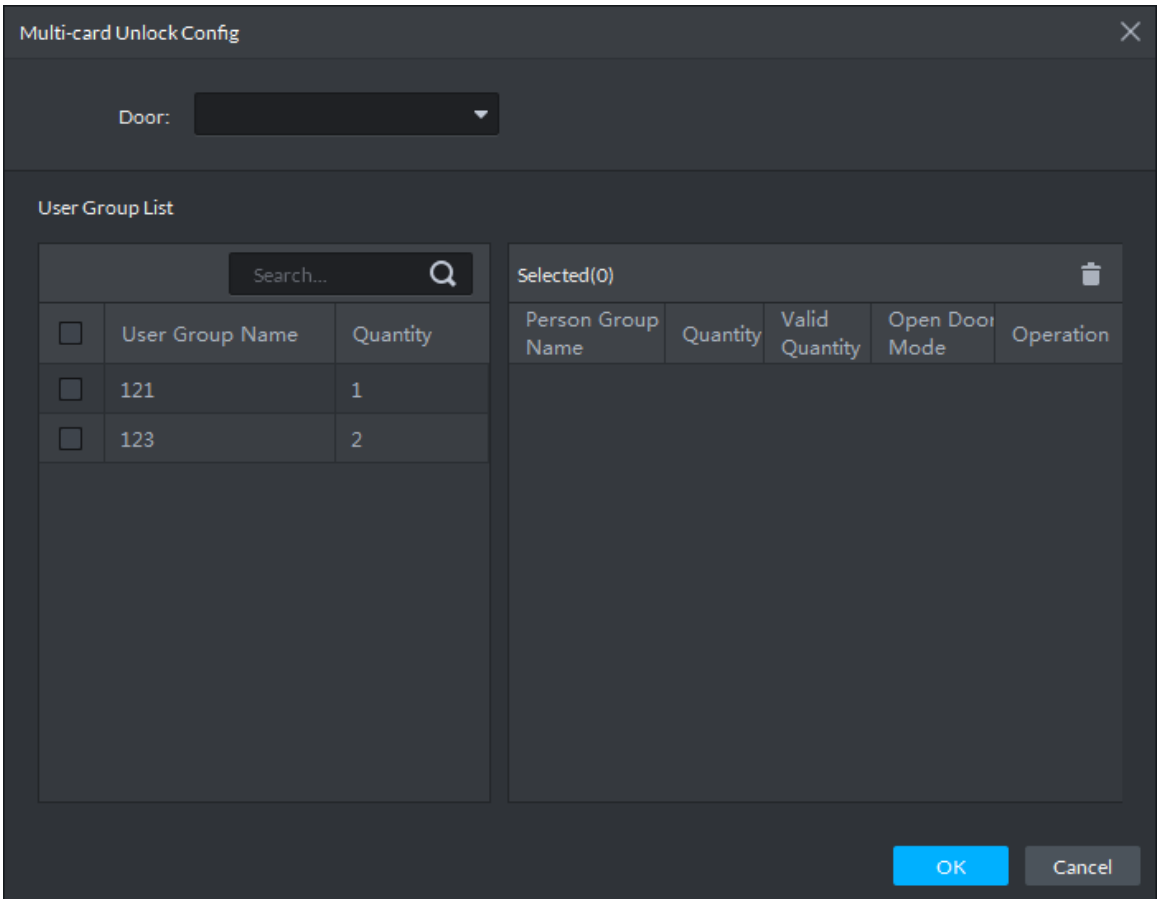
- 4) Click  in the upper right corner of the **User Group Manager** interface.

Step 3 Config Multi-Card Unlock.

- 1) Click **Add**.

The **Multi-card Unlock Config** interface is displayed. See Figure 3-305.

Figure 3-305 Configure user group



The dialog box is titled "Multi-card Unlock Config" and has a close button (X) in the top right corner. Below the title bar, there is a "Door:" label followed by a dropdown menu. The main area is titled "User Group List" and contains two tables. The left table has a search bar at the top and two columns: "User Group Name" and "Quantity". It lists two groups: "121" with quantity "1" and "123" with quantity "2". The right table is titled "Selected(0)" and has five columns: "Person Group Name", "Quantity", "Valid Quantity", "Open Door Mode", and "Operation". It is currently empty. At the bottom right, there are "OK" and "Cancel" buttons.

Door:

User Group List

	User Group Name	Quantity
☐	121	1
☐	123	2

Selected(0)				
Person Group Name	Quantity	Valid Quantity	Open Door Mode	Operation

OK Cancel

- 2) Select the door to set up Multi-Card Unlock.
- 3) Select the user group. You can select up to four groups.
The system displays the user group information. See Figure 3-306.

Figure 3-306 Select user group

The screenshot shows a window titled "Multi-card Unlock Config". At the top, there is a "Door:" dropdown menu. Below it, the "User Group List" section contains a search bar and a table with two columns: "User Group Name" and "Quantity". Two groups are listed: "121" with quantity "1" and "123" with quantity "2". To the right, the "Selected(2)" section shows a table with five columns: "Person Group Name", "Quantity", "Valid Quantity", "Open Door Mode", and "Operation". The same two groups are listed here, with "Valid Quantity" and "Open Door Mode" filled in. At the bottom right, there are "OK" and "Cancel" buttons.

Person Group Name	Quantity	Valid Quantity	Open Door Mode	Operation
121	1	1	Card	↑ ↓ ×
123	2	2	Card	↑ ↓ ×

- 4) Fill in the **Valid Quantity** for each group to be on site and the **Open Door Mode**.

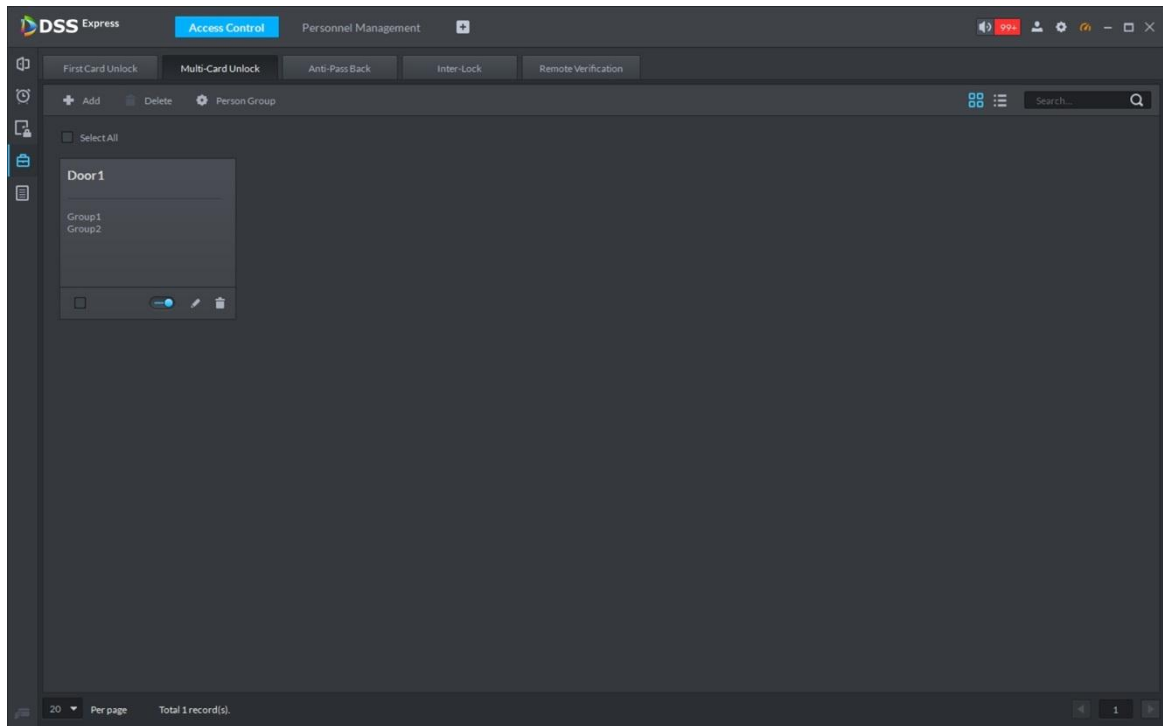
Click  or  to adjust the user sequence for each group to unlock the door.

The valid quantity refers to the number of users in each group that must be on site to swipe their cards.

- 5) Click **OK**.

The system displays the Multi-Card Unlock information. See Figure 3-307.

Figure 3-307 Multi-card unlock



Step 4 Click .

The icon changing into  indicates Multi-Card Unlock is enabled.

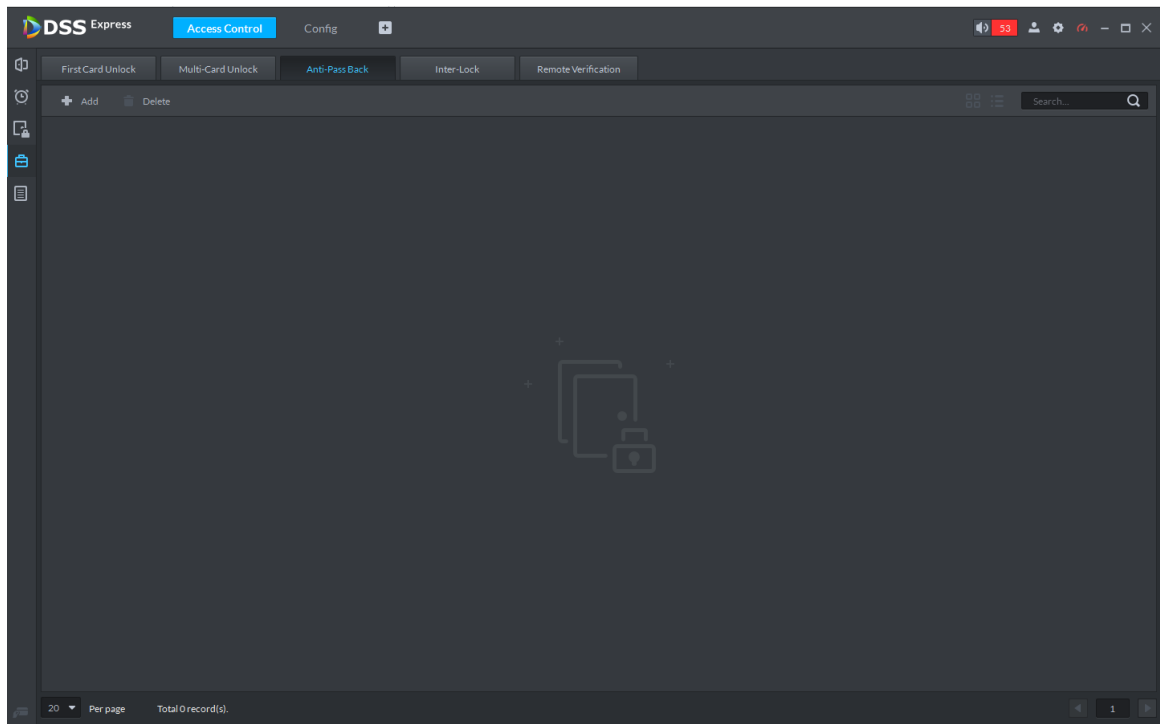
3.13.5.3 Anti-Pass Back

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**

The **Anti-Pass Back** interface is displayed. See Figure 3-308.

Figure 3-308 Anti-pass back



Step 2 Click **Add**.

The **Anti-pass back config** interface is displayed. See Figure 3-309.

Figure 3-309 Anti-pass back config

Step 3 Configure the anti-pass back parameters and click **Next Step**. For details of the parameters, see Table 3-41.

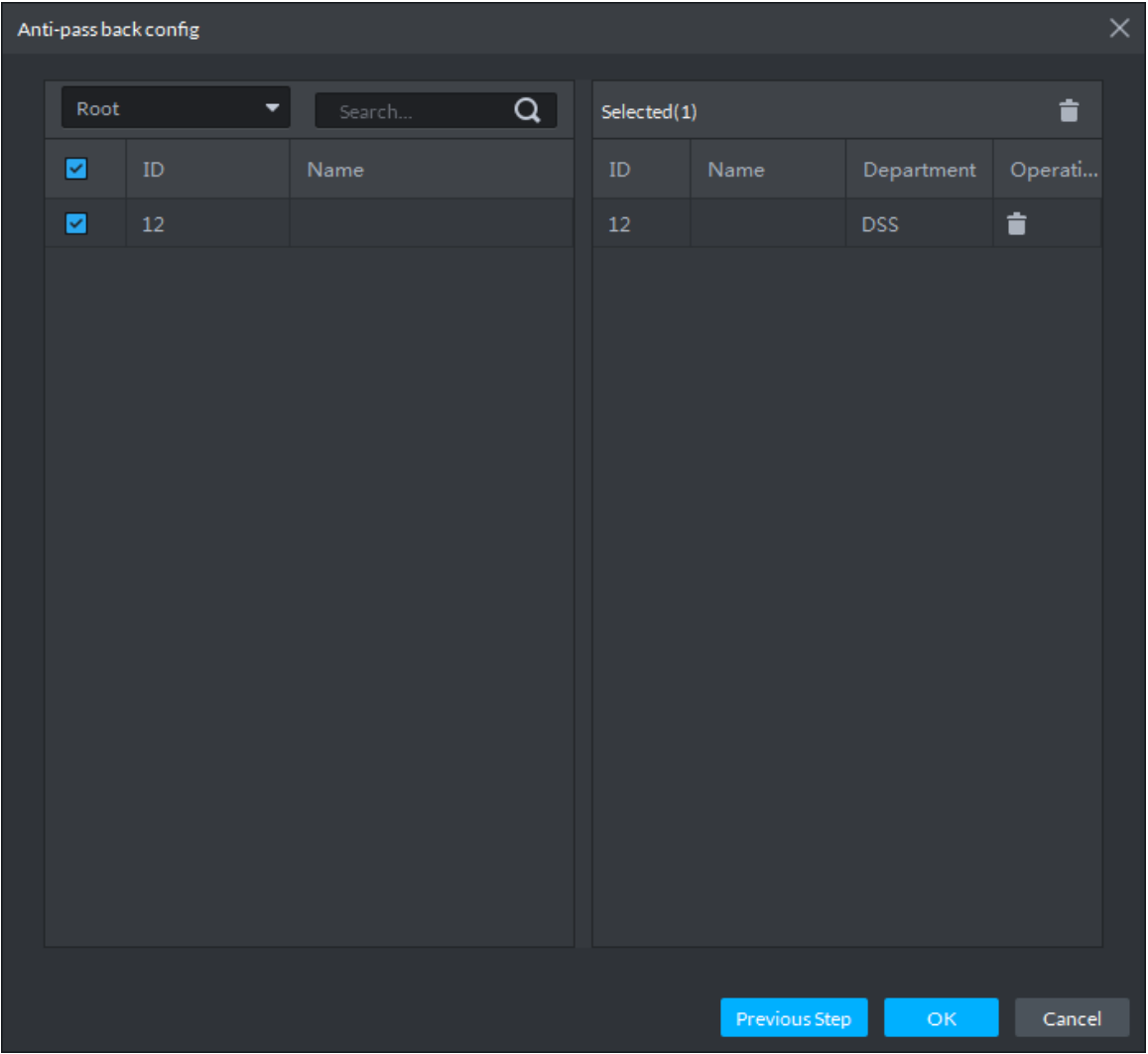
The system displays the user selection information. See Figure 3-310.

Table 3-41

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
Time Template	You can select the time periods to implement the anti-pass back rules.	
Remark	Note info.	
Group X X is a number.	The group sequence here is the sequence for swiping cards. You can add up to 16 readers for each group. Each group can swipe cards on any of the readers.	

Parameter	Description	
		parameters.

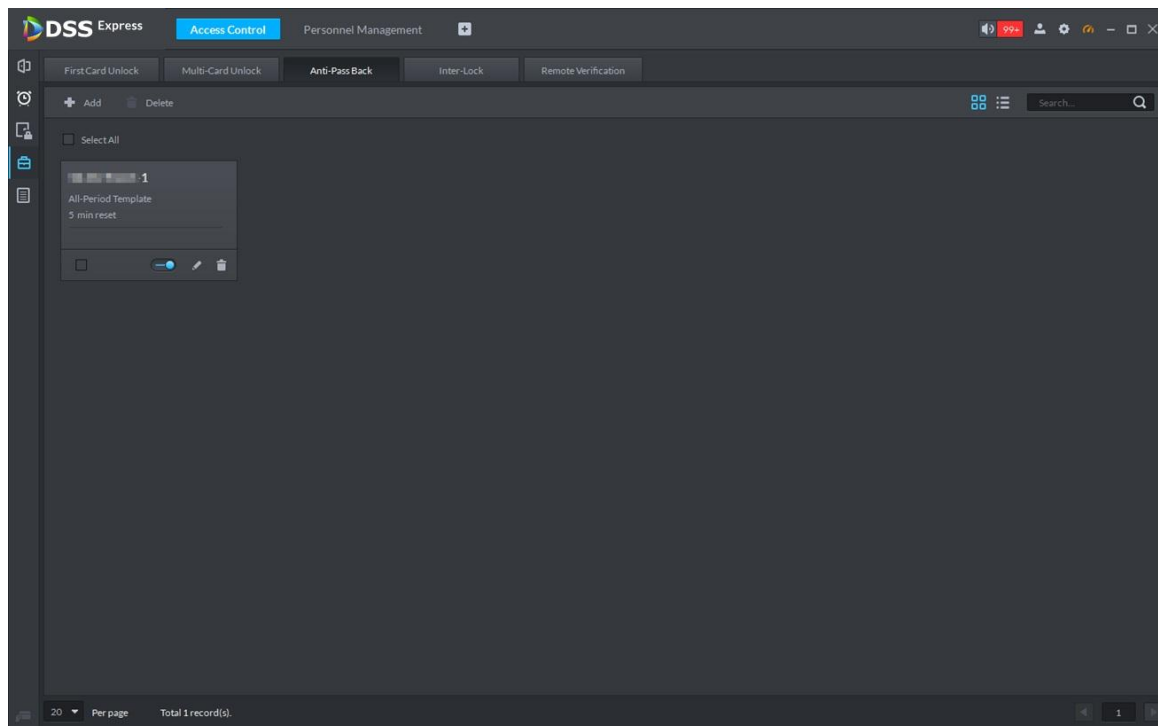
Figure 3-310 Select user



Step 4 Select users and click **OK**.

The system displays the anti-pass back information. See Figure 3-311.

Figure 3-311 Anti-pass back



Step 5 Click .

The icon changing into  indicates Anti-Pass Back is enabled.

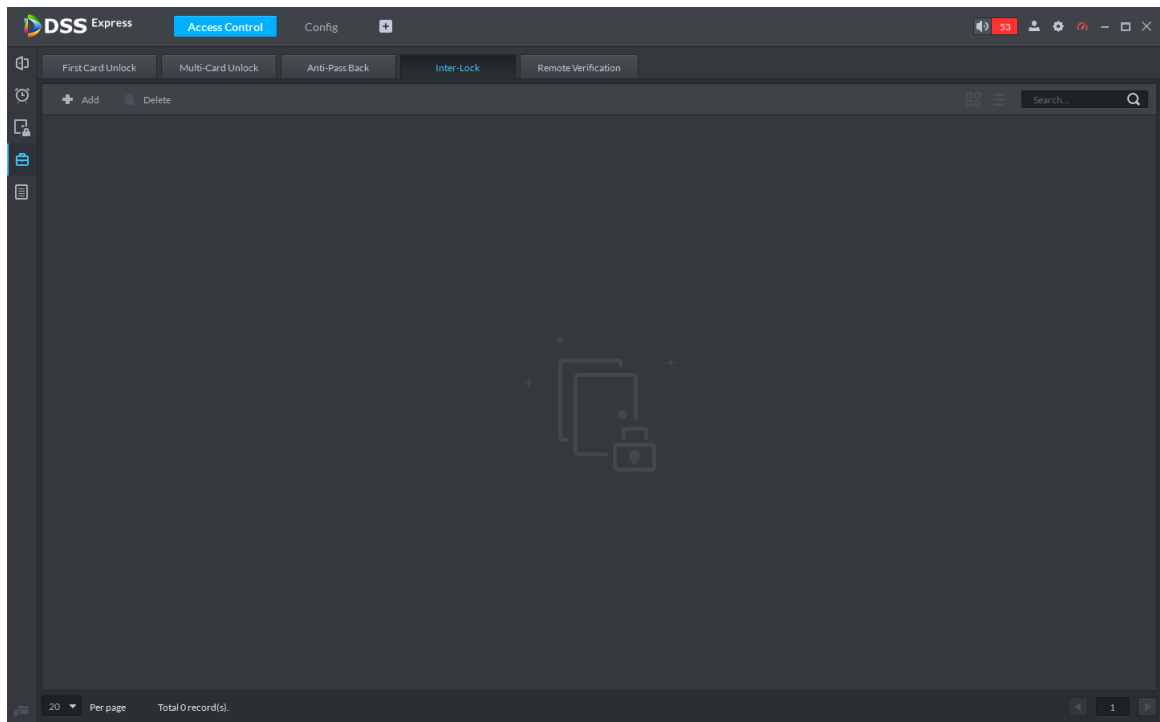
3.13.5.4 Inter-door Lock

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. The A&C Central Controller employs inter-group inter-lock, where the access control channels are independent of the inter-lock and can all be opened. However, whenever an access control channel in a group is opened, no channels of other groups can be opened. The configuration steps in this chapter are for an A&C Central Controller.

Step 1 On the **Access Control** interface, click  and select **Inter-lock**.

The **Inter-Lock** interface is displayed. See Figure 3-312.

Figure 3-312 Inter-lock



Step 2 Click **Add**.

The **Inter-lock Config** interface is displayed. See Figure 3-313.

Figure 3-313 Inter-lock config

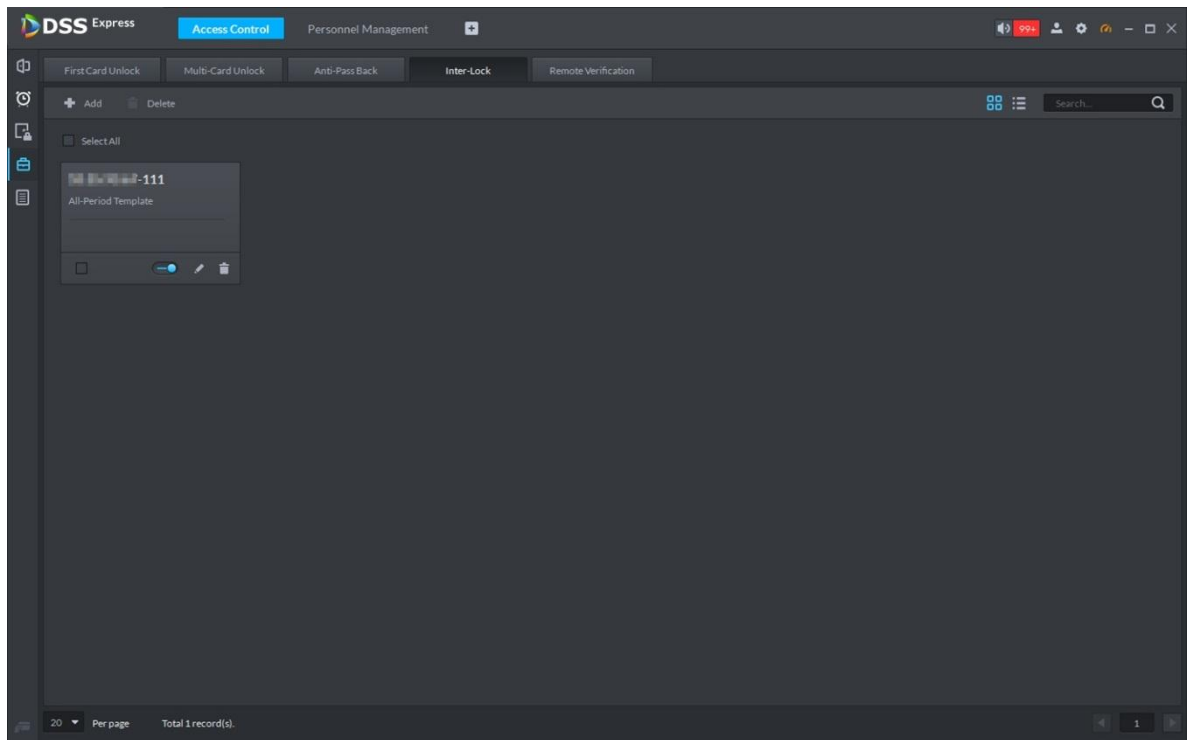
Step 3 Configure inter-lock parameters and click **OK**. For details of the parameters, see Table 3-42.

The system displays the inter-lock information. See Figure 3-314.

Table 3-42 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 3-314 Inter-lock list



Step 4 Click .

The icon changing into  indicates Inter-Lock is enabled.

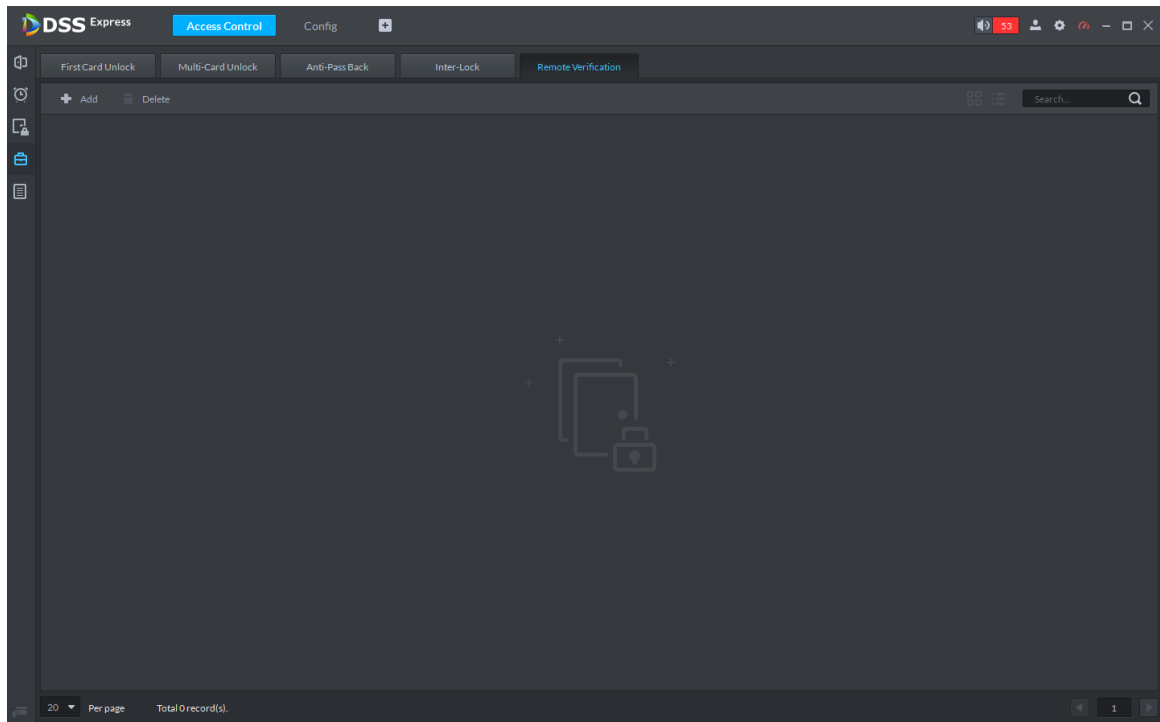
3.13.5.5 Remote Verification

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**.

The **Remote Verification** interface is displayed. See Figure 3-315.

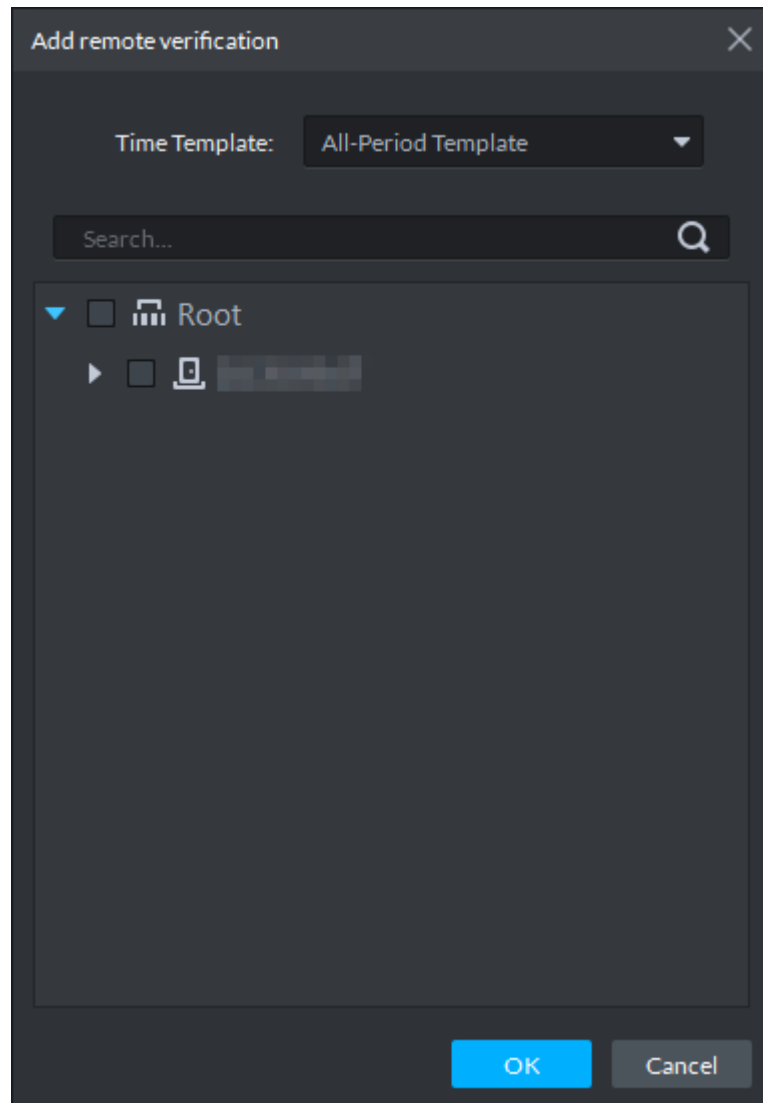
Figure 3-315 Remote verification



Step 2 Click **Add**.

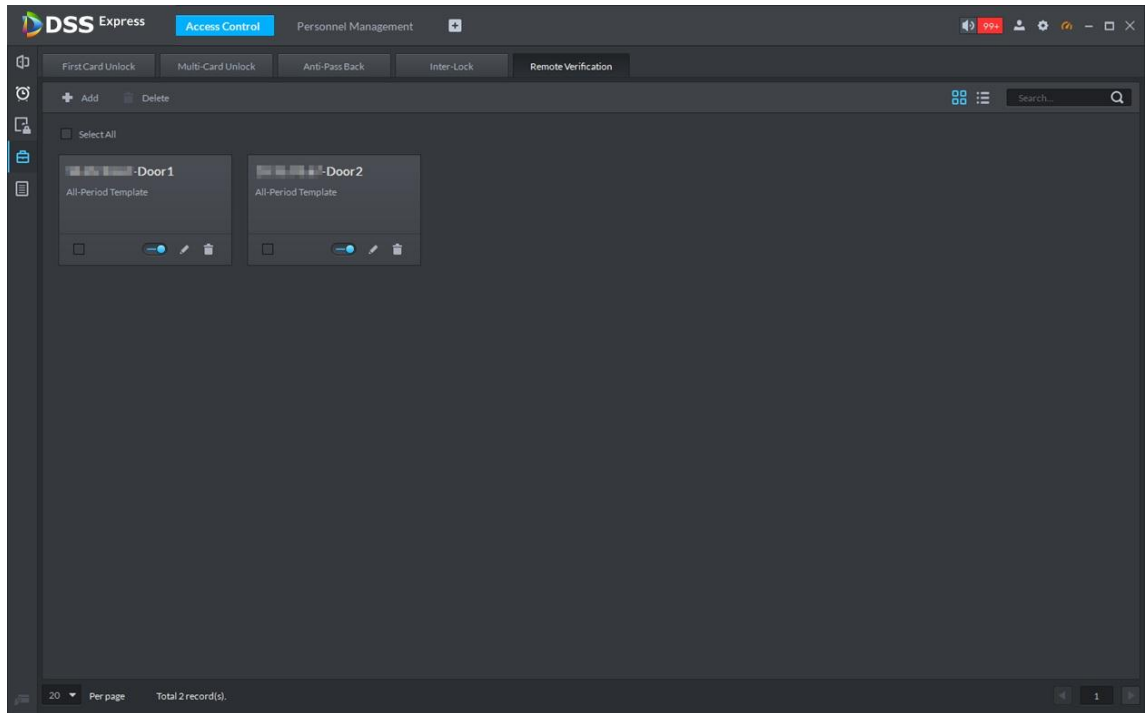
The **Add remote verification** interface is displayed. See Figure 3-316.

Figure 3-316 Add remote verification



Step 3 Select **Time Template** and access control channel, and click **OK**.
The system displays the remote verification information. See Figure 3-317.

Figure 3-317 Remote verification list



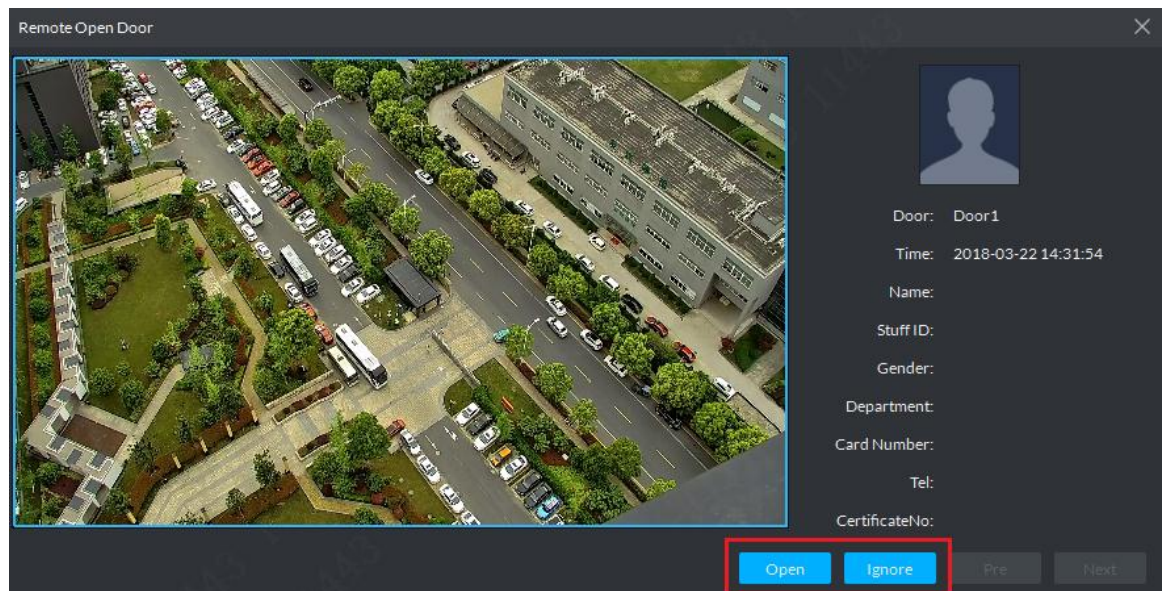
Step 4 Click .

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. See Figure 3-318.

Step 6 You can choose to unlock the door or ignore it by clicking the corresponding button, and the popup automatically disappears.

Figure 3-318 Remote open door



3.13.6 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 **3.2.5 Setting Record Plan**

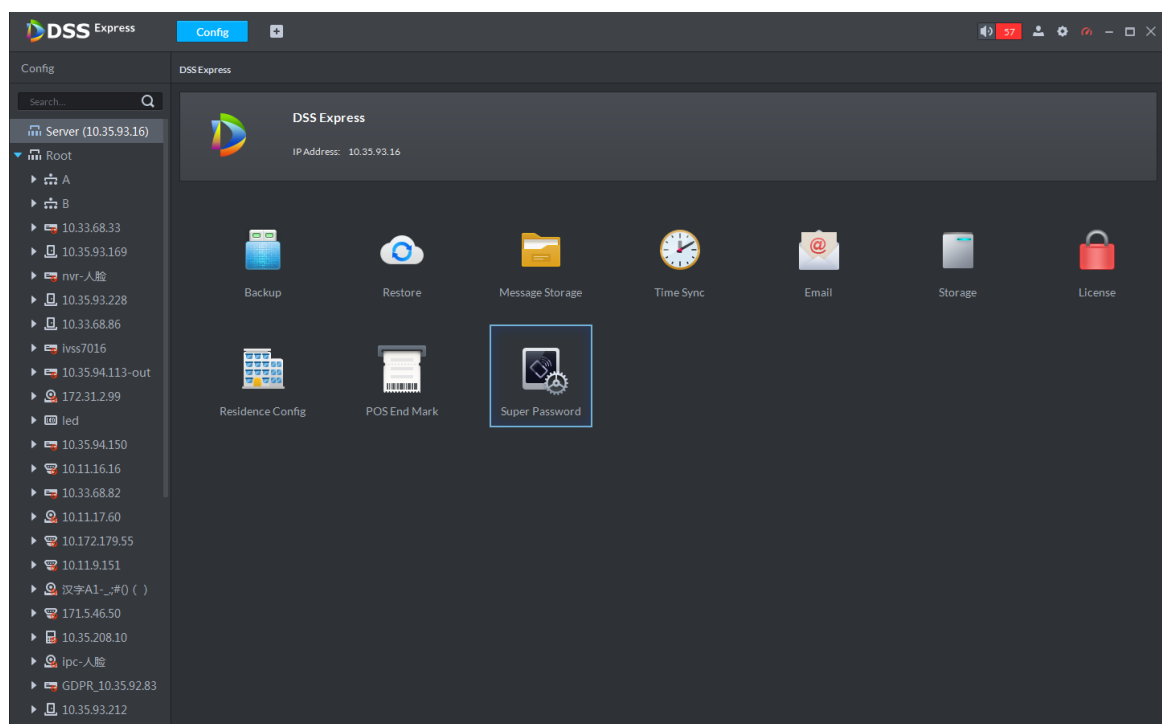
3.13.7 Configuring Super Password

2nd generation access control supports using super password to open door. You only need to enter super password to open door.

Step 1 On client homepage, click **Config**.

The system displays **Config** interface, see Figure 3-319.

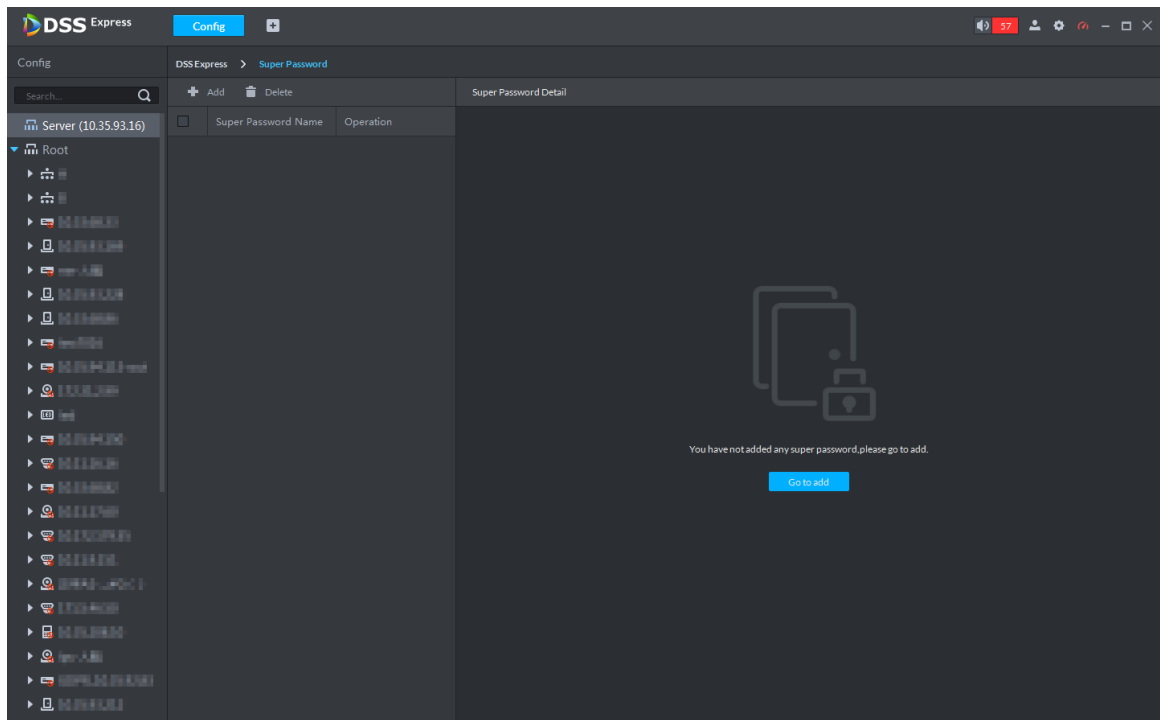
Figure 3-319 Config interface



Step 2 Click **Super Password**.

The system displays Super Password interface, see Figure 3-320.

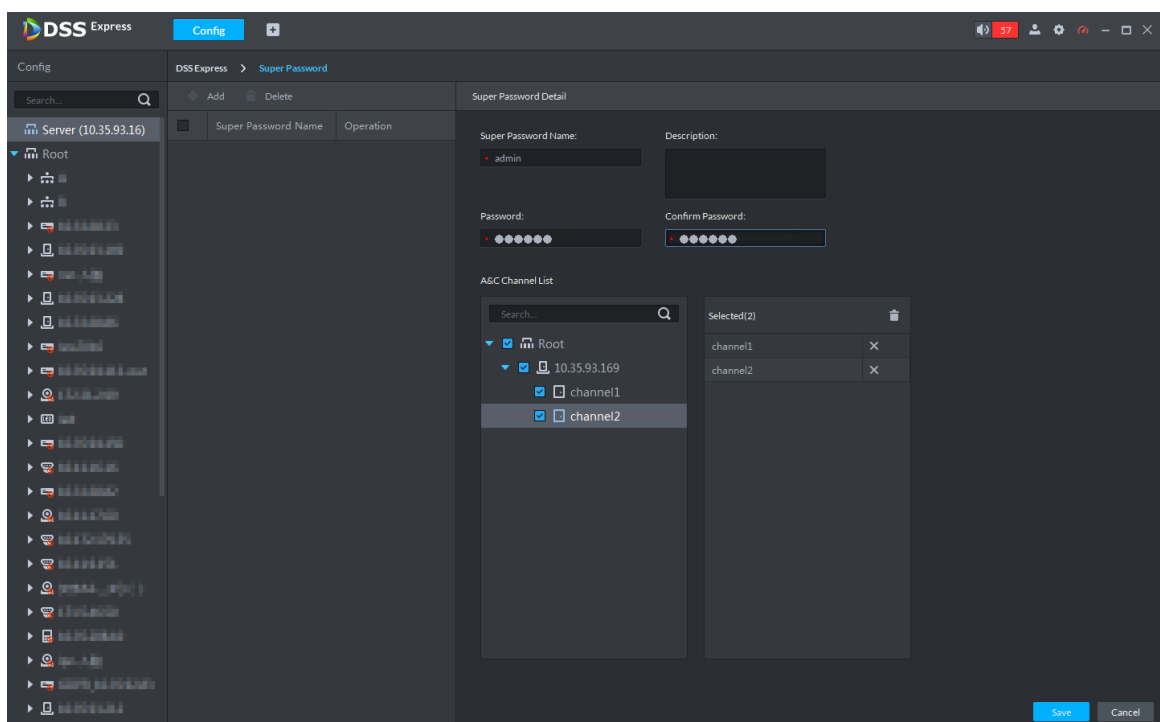
Figure 3-320 Super password



Step 3 Click **Add**.

The system displays interface of adding super password, see Figure 3-321

Figure 3-321 Add super password



Step 4 After setting super password, you can select AC channel (only supported by 2nd generation device), click **Save** and complete config.

3.13.8 Access Control Application

You can control lock, unlock and view related video and event info on console, and enter door config interface.

3.13.8.1 Viewing Video of Bound Channel

When adding access control devices, if you have already bound a video channel to the channel, you can preview the real-time videos of the bound video channels on the console. To bind video channels, see **3.13.1 Adding Access Control**

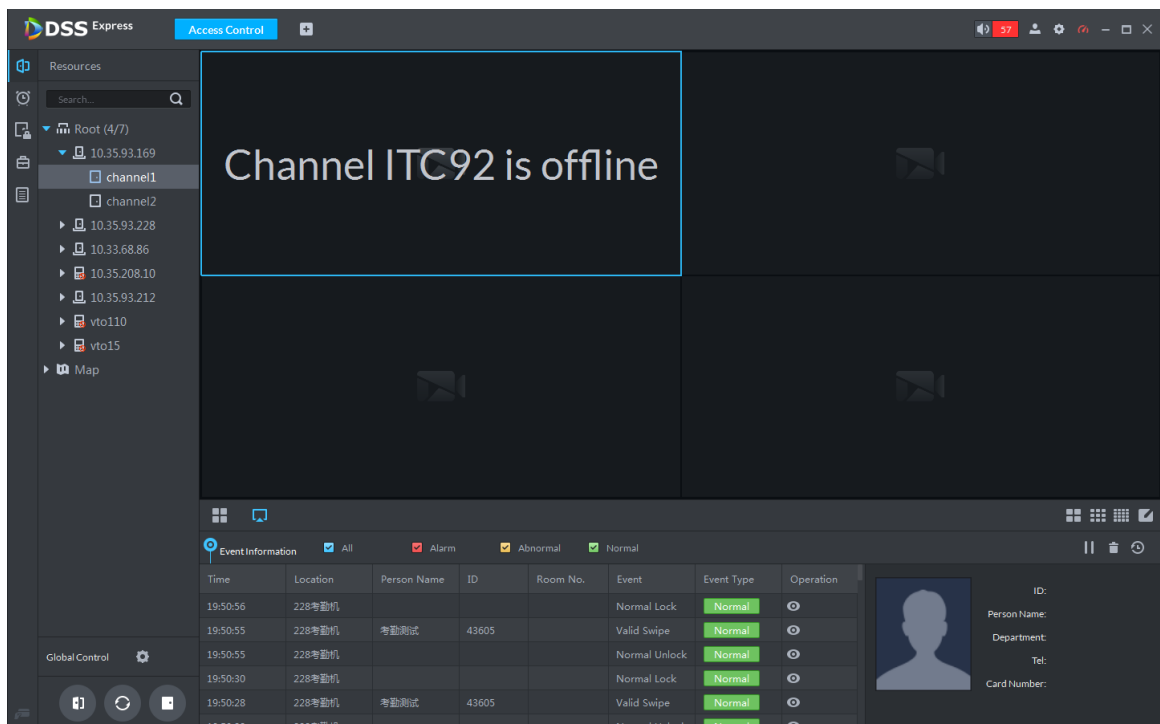
Step 1 On client homepage, click **Access Control**.

The system displays **Access Control** interface.

Step 2 Click .

The system displays **Console** interface, see Figure 3-322.

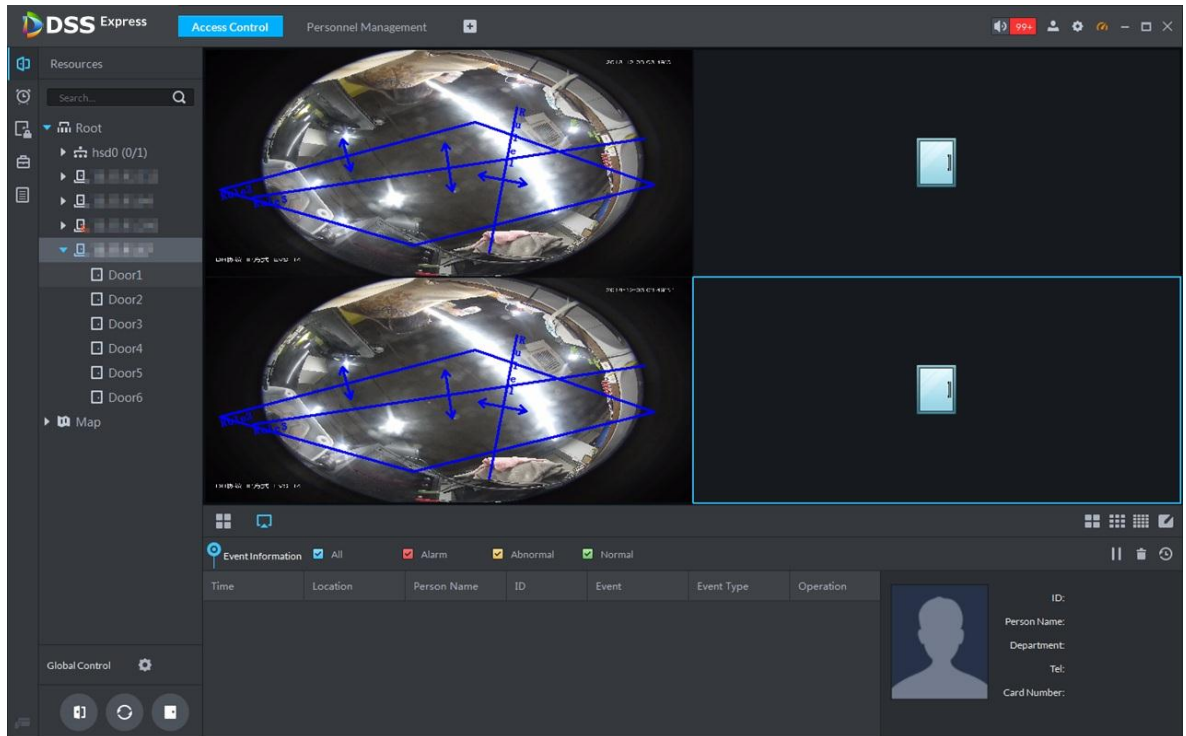
Figure 3-322 Console



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. See Figure 3-323
- 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 preview interface on the right side. The system displays videos in real time. See Figure 3-323

Figure 3-323 Linked channel video



3.13.8.2 Manual Unlock

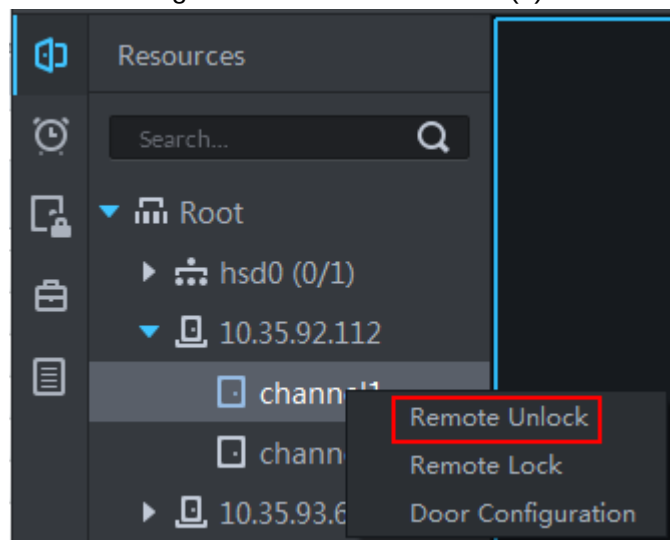
In addition to Always Open or linked unlock in specified periods, the console also supports unlocking by manually controlling the access control channel. After unlock, the door automatically locks up after a specified time period (5s by default, and 10s in this example) set up in Door Config.

You can unlock the door in the following ways:

- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Unlock** in the popup menu. See Figure 3-324. After unlocking, the door status in the access control channel list on the right side of the interface changes to open,

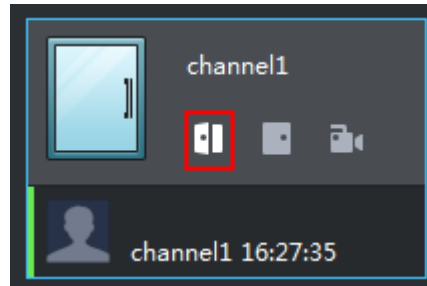
as .

Figure 3-324 Remote unlock (1)



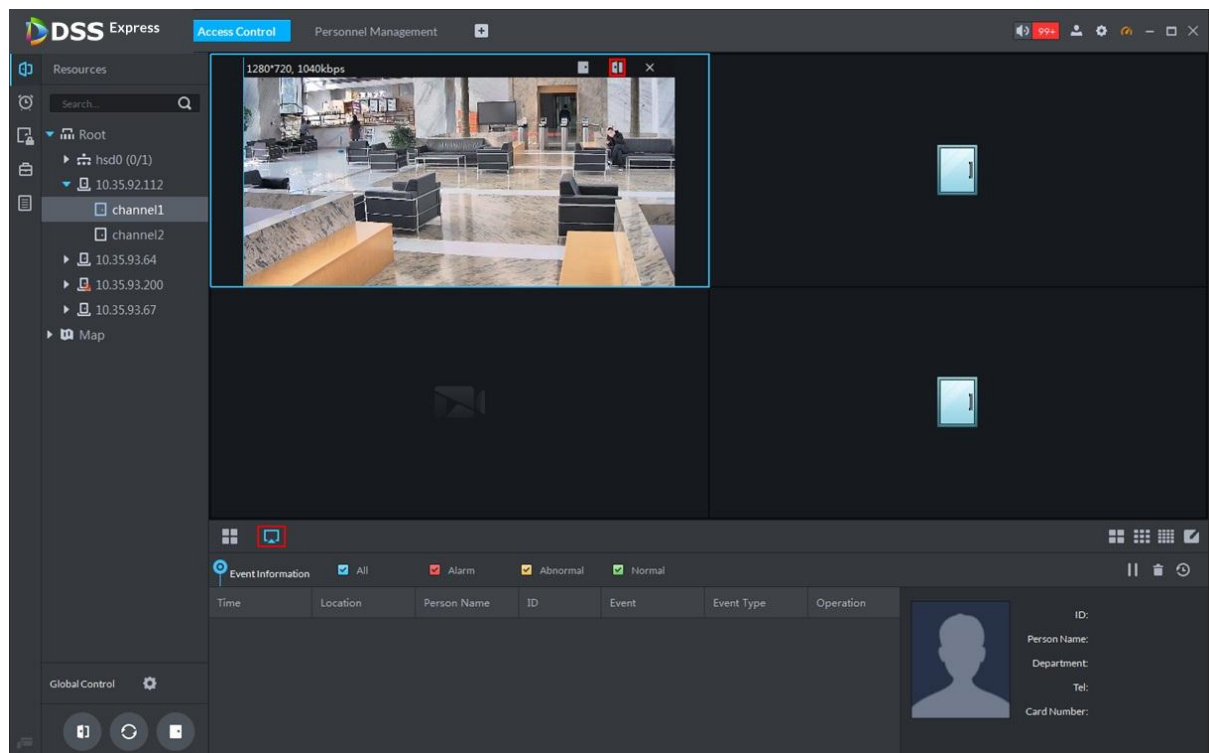
- Click  on the door channel interface to unlock the door. See Figure 3-325. After unlocking, the door status in the access control channel list on the right side of the interface changes to open, as .

Figure 3-325 Unlock (2)



- When viewing videos bound to the channel, click  on the video interface to unlock the door. See Figure 3-326.

Figure 3-326 Unlock(3)

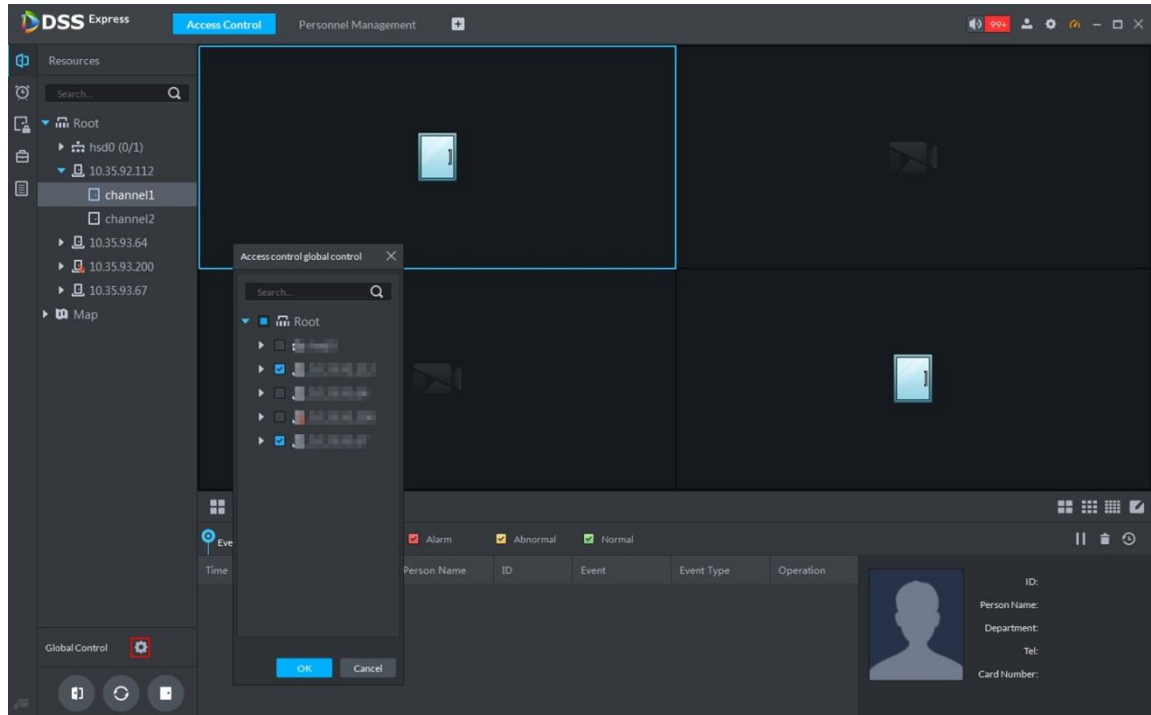


- Temporary Always Open of multiple doors
Select a door channel through global control and you can set the door to be Always Open. Recovery to normal status after unlocking requires manual operations.

Step 1 Click  on the bottom left of the console interface of the Access Control module.

Step 2 The **Access control global control** interface is displayed. See Figure 3-327.

Figure 3-327 Global control



Step 3 Select an access control channel to be set to Always Open via global control, and click **OK**.

Step 4 Click **Always Open** on the bottom left of the interface.
The **Password Verification** interface is displayed.

Step 5 Input current user's password, and click **OK**.

Step 6 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.

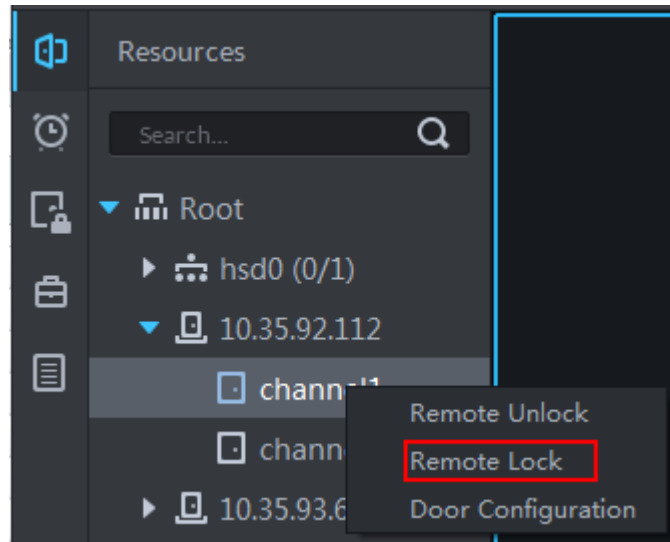
3.13.8.3 Manual Lock

In addition to Always Close or linked lock in specified periods, the console also supports locking by manually controlling the access control channel. You can lock the door in the following ways:

- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Lock** in the popup menu. See Figure 3-328. After locking, the door status in

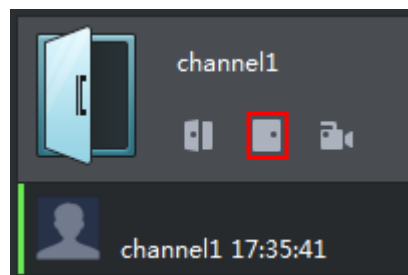
the access control channel list on the right side of the interface changes to closed, as .

Figure 3-328 Lock (1)



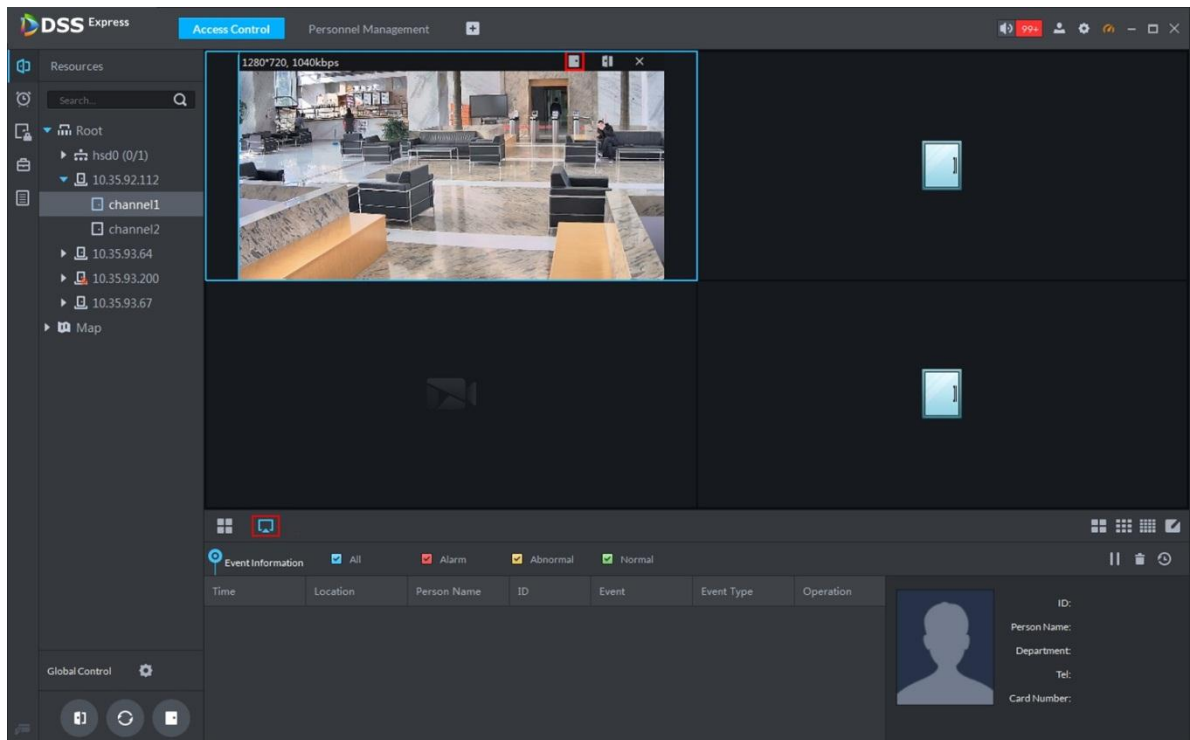
- Click  on the door channel interface to lock the door. See Figure 3-329. After locking, the door status in the access control channel list on the right side of the interface changes to closed, as .

Figure 3-329 Lock (2)



- When viewing videos bound to the channel, click  on the video screen to lock the door. See Figure 3-330.

Figure 3-330 Lock (3)

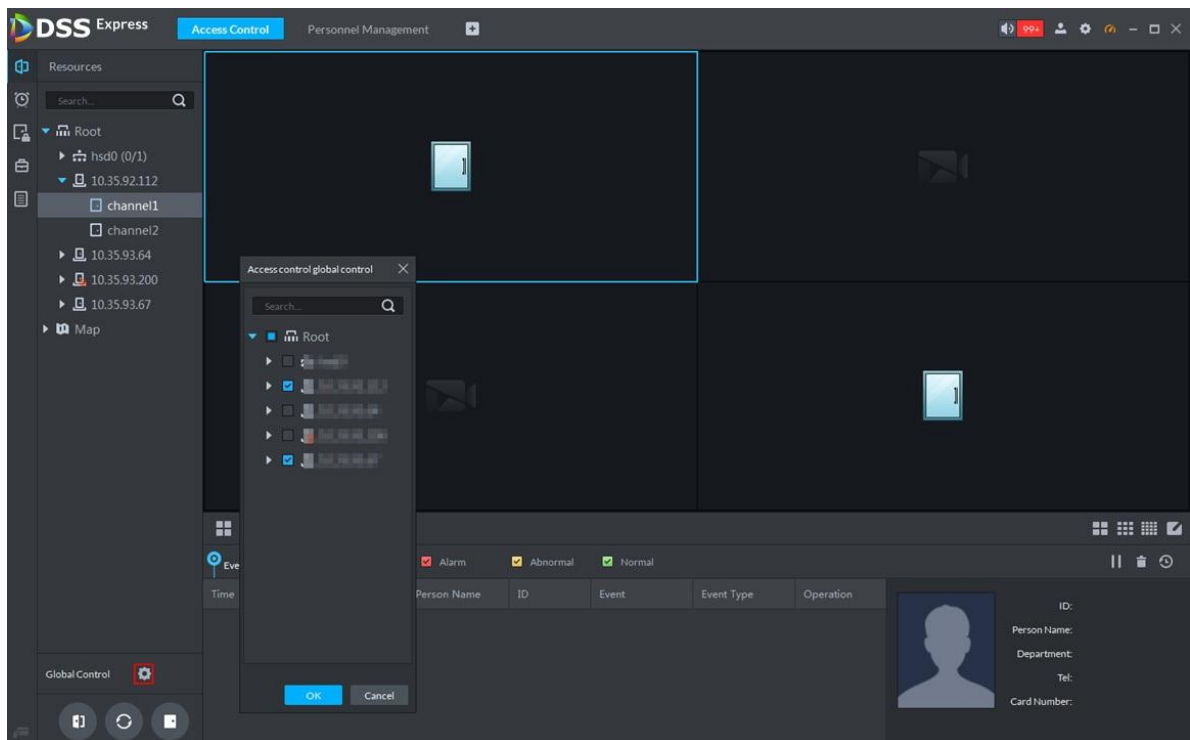


- Temporary Always Open of multiple doors
Select a door channel through global control and you can set the door to be Always Close. Recovery to normal status after locking requires manual operations.

Step 1 Click  on the bottom left of the console interface of the Access Control module.

The **Access control global control** interface is displayed. See Figure 3-331.

Figure 3-331 Global control



Step 2 Select an access control channel to be set to Always Close via global control, and click **OK**.

Step 3 Click **Always Close** on the bottom left of the interface.

The **Password Verification** interface is displayed.

Step 4 Input current user's password, and click **OK**.

Step 5 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.

3.13.8.4 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, invalid swipe.

Step 1 In the event list below the console interface, click  next to the event records.

Step 2 The **AC Event Info** interface is displayed. See Figure 3-332. See Table 3-43 for more descriptions on the controls.

Figure 3-332 Event detail

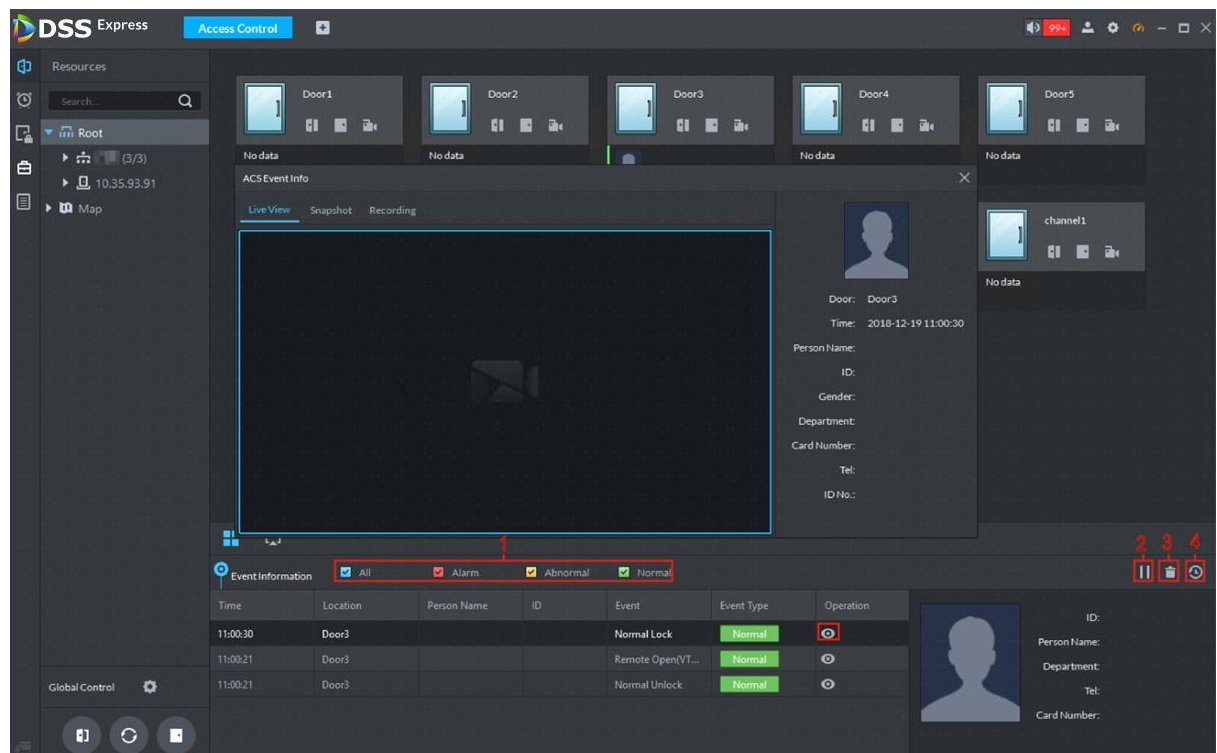


Table 3-43 Operation description

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.
2	- 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 3 Click the corresponding tab to view the live view, snapshots, and video recordings of the linked video channel.

3.13.9 Searching Access Control Log

You can view the reported AC log and device local log.

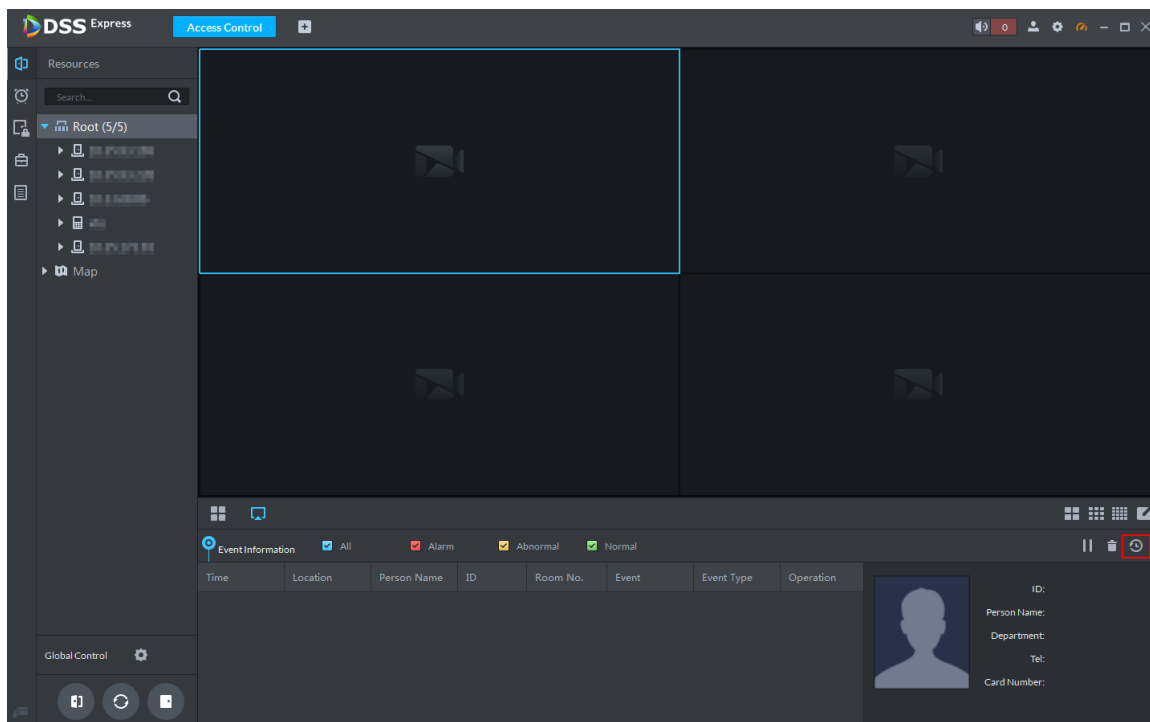
3.13.9.1 Searching Logs on Platform

Step 1 Enter AC log interface.

Supports following two methods.

- On **Access Control** interface, click .
- On **Access Control** interface, click  and enter console, click  and see Figure 3-333.

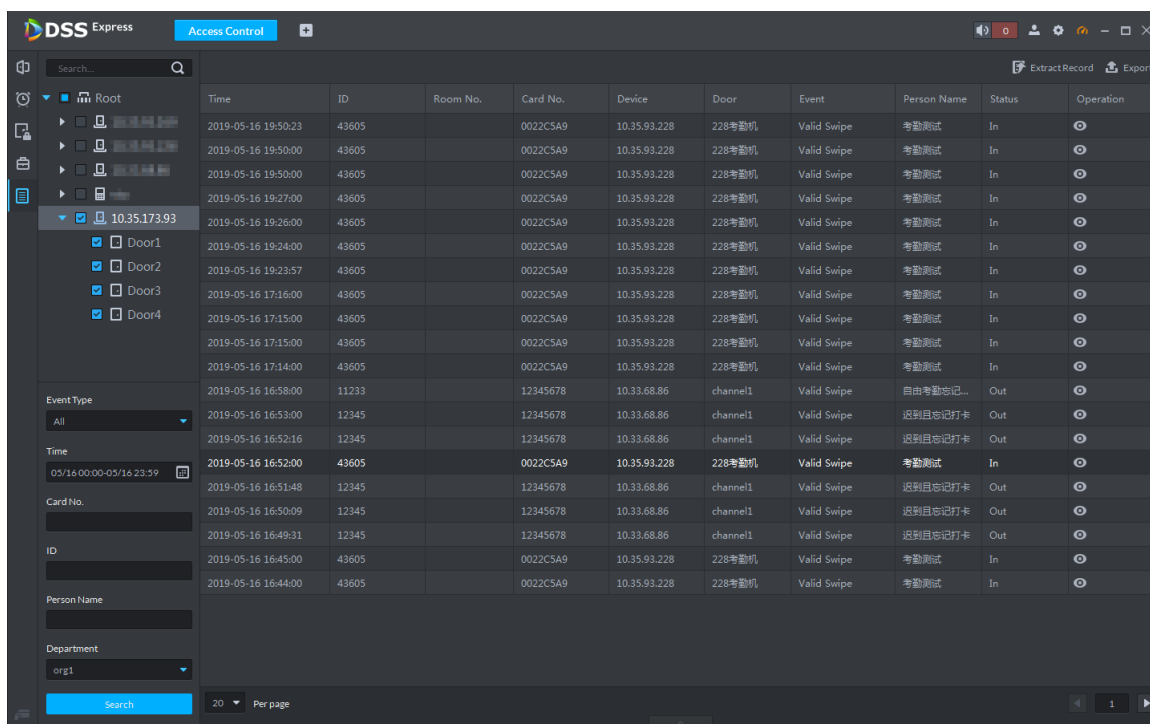
Figure 3-333 Enter AC log interface



Step 2 Set condition, click **Search**.

The system displays log info, see Figure 3-334.

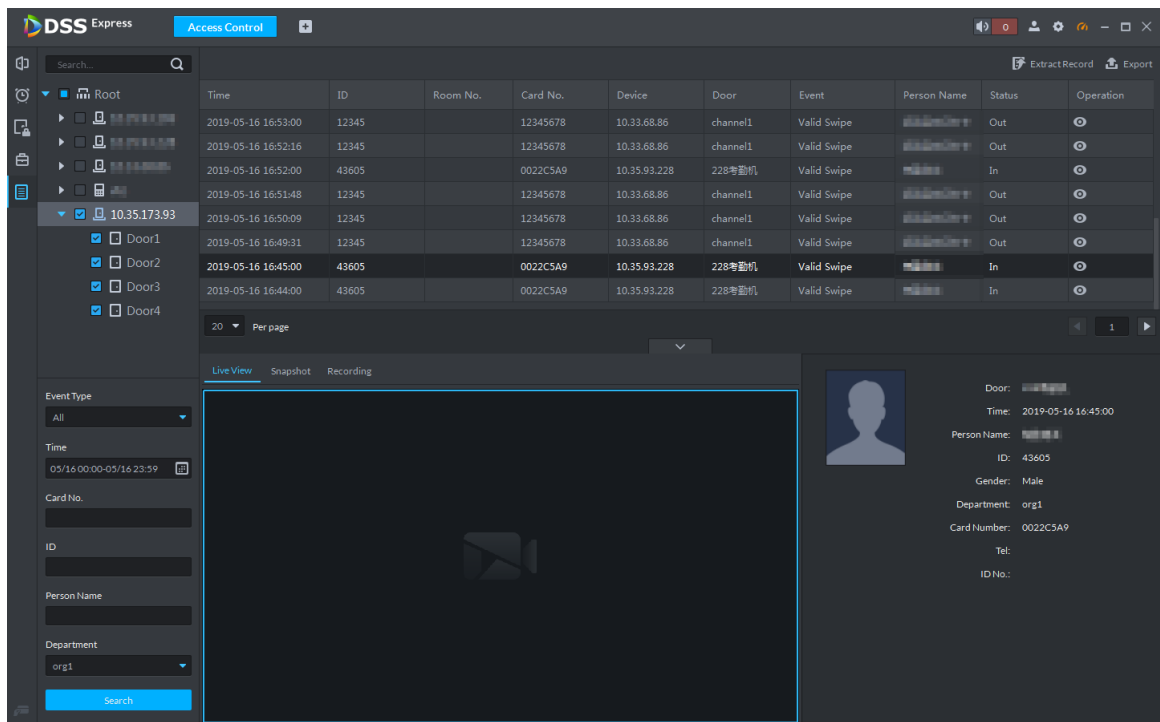
Figure 3-334 Search AC log



Step 3 Click

The system displays AC info and live view, snapshot and record of linked video channel. See Figure 3-335.

Figure 3-335 AC log details



Step 4 Click **Export** and save log to local according to system prompt.

3.13.9.2 Extracting Log during Device Offline

If device is offline during application, you can extract offline AC logs to platform.

Step 1 Enter AC log interface.

Supports following two methods.

- On **Access Control** interface, click .
- On **Access Control** interface, click  and enter console, click  and see Figure 3-333.

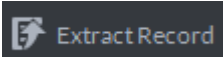
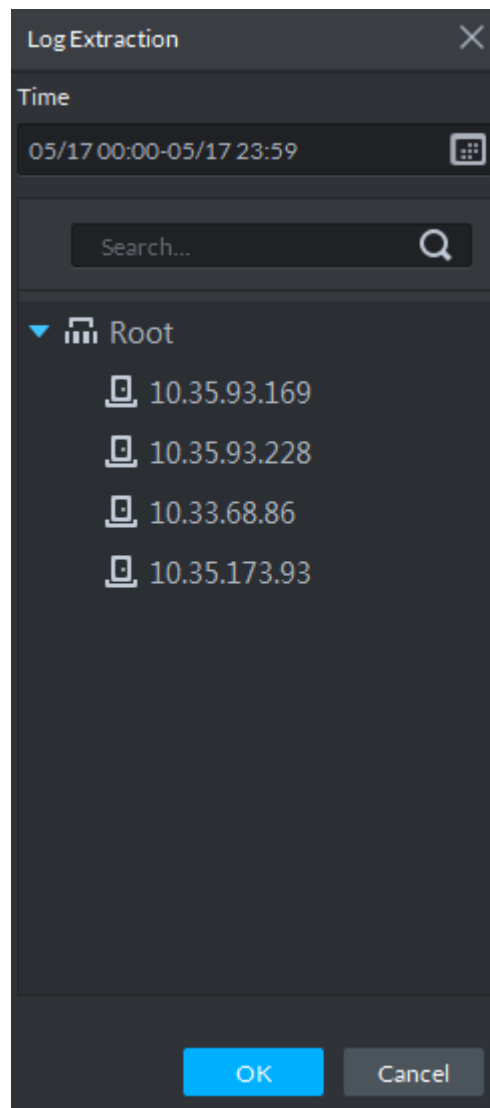
Step 2 Click  on upper right corner.

Figure 3-336 Extract logs during device offline



Step 3 Click  and set period.

Step 4 Click  and display AC devices, select channel.

Step 5 Click **OK**.
The system displays extracted logs.

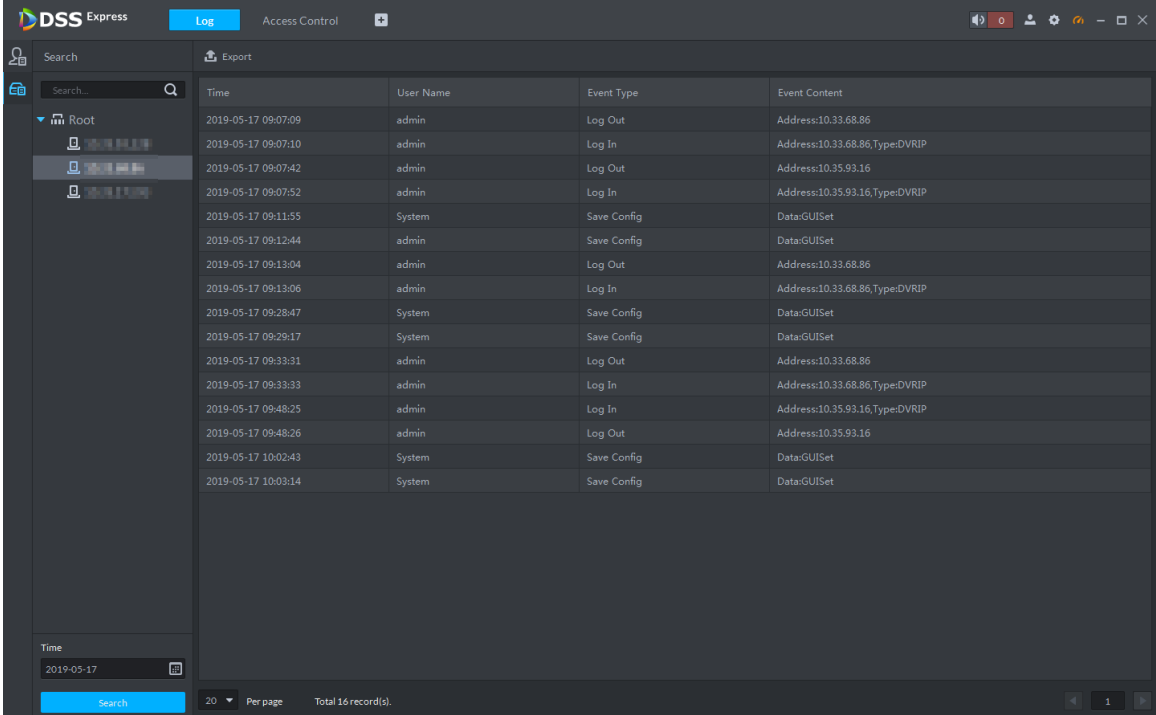
3.13.9.3 Searching Device Logs

You can search log info of AC device.

Step 1 On client homepage, click **Log**.
The system displays Log interface.

Step 2 Click .
The system displays **Device Log** interface, see Figure 3-337.

Figure 3-337 Device log



Time	User Name	Event Type	Event Content
2019-05-17 09:07:09	admin	Log Out	Address:10.33.68.86
2019-05-17 09:07:10	admin	Log In	Address:10.33.68.86,Type:DVRIP
2019-05-17 09:07:42	admin	Log Out	Address:10.35.93.16
2019-05-17 09:07:52	admin	Log In	Address:10.35.93.16,Type:DVRIP
2019-05-17 09:11:55	System	Save Config	Data:GUISet
2019-05-17 09:12:44	admin	Save Config	Data:GUISet
2019-05-17 09:13:04	admin	Log Out	Address:10.33.68.86
2019-05-17 09:13:06	admin	Log In	Address:10.33.68.86,Type:DVRIP
2019-05-17 09:28:47	System	Save Config	Data:GUISet
2019-05-17 09:29:17	System	Save Config	Data:GUISet
2019-05-17 09:33:31	admin	Log Out	Address:10.33.68.86
2019-05-17 09:33:33	admin	Log In	Address:10.33.68.86,Type:DVRIP
2019-05-17 09:48:25	admin	Log In	Address:10.35.93.16,Type:DVRIP
2019-05-17 09:48:26	admin	Log Out	Address:10.35.93.16
2019-05-17 10:02:43	System	Save Config	Data:GUISet
2019-05-17 10:03:14	System	Save Config	Data:GUISet

Step 3 Select AC device and time, click **Search**.
The system displays search results.

3.13.10 AC Device Maintenance

Support update or AC device reboot by platform. Please skip the chapter if you do not need to update or restart AC device.

3.13.10.1 Updating AC Device

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**.
The system displays **Config** interface.

Step 2 In left device tree, select AC device, click **Device Update** and see Figure 3-338.
The system displays **Device Update** interface, and version info of AC device. See Figure 3-339.

Figure 3-338 Enter device update interface

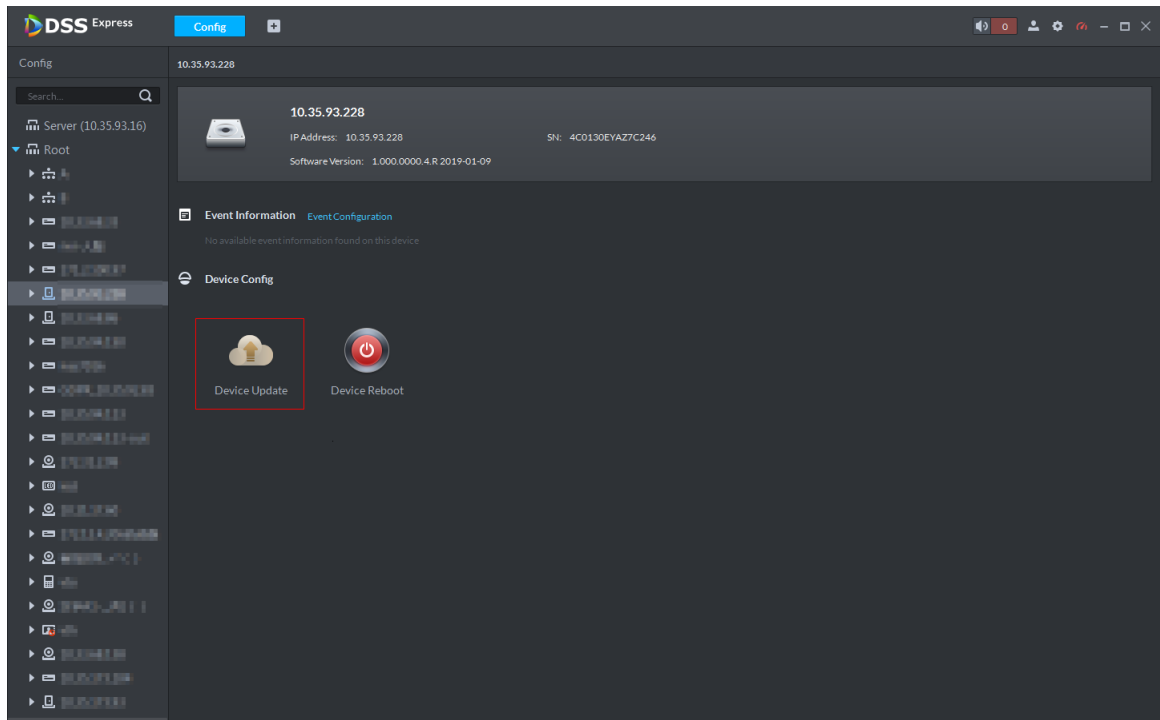
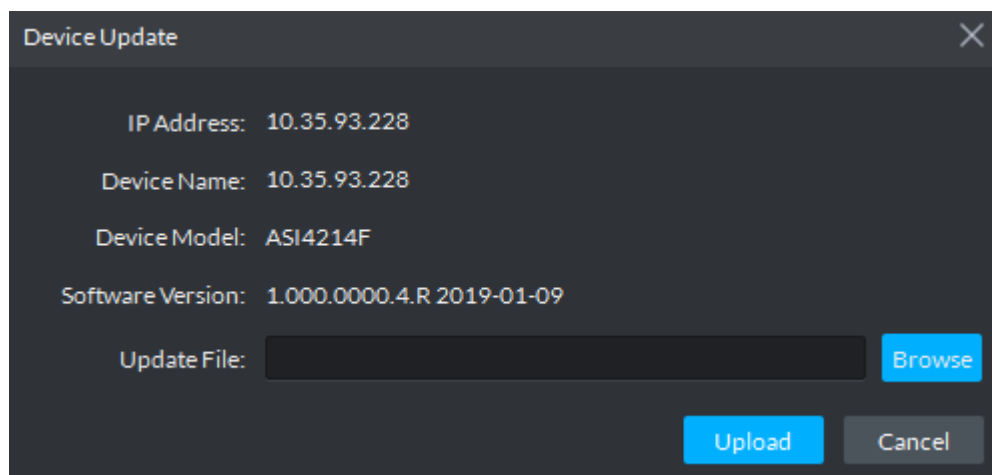


Figure 3-339 Device update



Step 3 Click **Browse** and select update file.

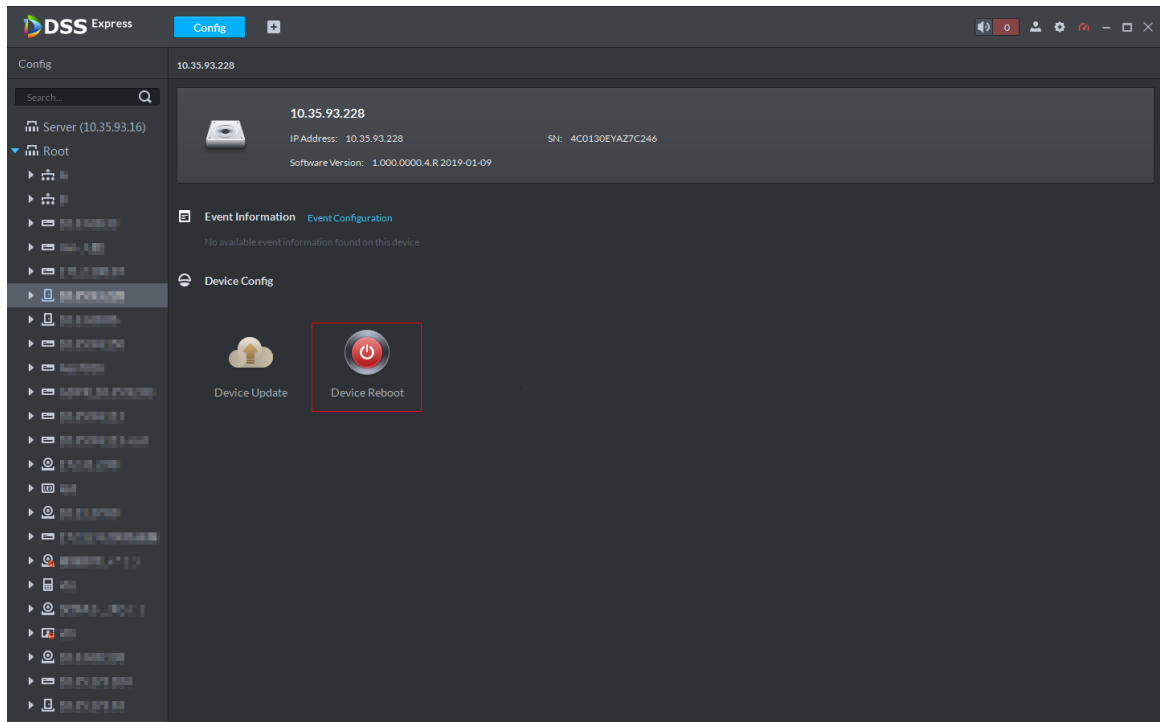
Step 4 Click **Upload** and update AC device.

3.13.10.2 Rebooting AC Device

Step 1 On client homepage, click **Config**.
The system displays **Config** interface.

Step 2 In left device tree, select AC device, click Device Reboot, and see Figure 3-340.
The system displays prompt box of rebooting device.

Figure 3-340 Enter device reboot



Step 3 Click **Yes** and reboot device.

3.14 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. The visitor management flow is shown in Figure 3-341.

Figure 3-341 Visitor flow



3.14.1 Adding AC Device

Add access control device. For more details, refer to **3.2.2.4 Adding Device**

3.14.2 Visitor Appointment

Record visitor info on platform.

Step 1 On client homepage, click **Visitor Management**.

The system displays **Visitor Management** interface.

Step 2 Click **Appointment Registration**.

The system displays interface of registration info, see Figure 3-342.

Figure 3-342 Appointment registration

Appointed Visit Details

Host Name: Host Company (Department):

Visitor Name: Visitor Company:

Credentials Type: Credential No.:

Identification Card:

Tel: Email Address:

Appointed Visit Time: Appointed End Visit Time:

Reason for Visit:

Remark:

Table:

Visitor Name	Card No.	Tel	Host Name	Host Compan...	Appointed Vi...	Visit Time	Status	Operation

Step 3 Enter visitor and some other info, click **OK** and complete appointment.
The platform displays appointment info, see Figure 3-343.



Click and skip to visit registration interface.

Figure 3-343 Appointed visitor info

Table:

Visitor Name	Card No.	Tel	Host Name	Host Company (Depar...	Appointed Visit Time	Visit Time	Status	Operation
ABC			123		2019-05-17 11:36:47	--	Appointed	
James			123	Green Life	2019-05-17 11:16:18	--	Appointed	
abc			123		2019-05-17 11:10:04	--	Appointed	

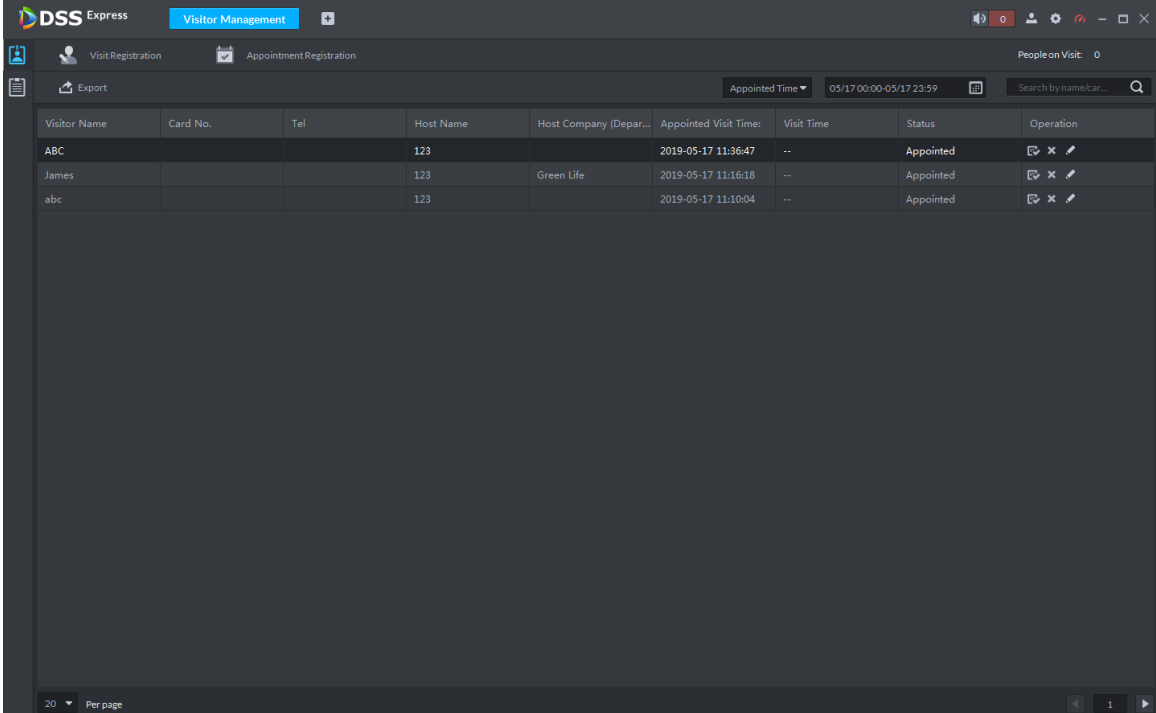
3.14.3 Visit Registration

When appointed visitor comes to visit, you need to confirm person info and grant access permission. On-site registration is supported when there is temporary visitor, and grant access permission. Visitor can have access by swiping card or face recognition.

Step 1 On **Visitor Management** interface, click .

The system displays **Visitor Management** interface. The interface displays appointed visitor info, see Figure 3-344.

Figure 3-344 Visitor management



Visitor Name	Card No.	Tel	Host Name	Host Company (Depart...	Appointed Visit Time	Visit Time	Status	Operation
ABC			123		2019-05-17 11:36:47	--	Appointed	  
James			123	Green Life	2019-05-17 11:16:18	--	Appointed	  
abc			123		2019-05-17 11:10:04	--	Appointed	  

Step 2 Enter visit registration info interface.

- If visitor is appointed.

Search visitor info, click . The system displays visitor registration details, see Figure 3-345.

- If visitor is not appointed.

Click **Visit Registration**, the system displays visitor registration detail interface. You need to enter info manually if there is no person info.

Figure 3-345 Visit details

Visitor Name	Card No.	Tel	Host Name	Host Compan...	Appointed Vi...	Visit Time	Status	Operation
ABC			123		2019-05-17 ...	--	Appointed	🔍 ✕ ✎
James			123	Green Life	2019-05-17 ...	--	Appointed	🔍 ✕ ✎
abc			123		2019-05-17 ...	--	Appointed	🔍 ✕ ✎

Host Name: 123		Host Company (Department):	
Visitor Name: ABC		Visitor Company:	
Credentials Type: Identification Card		Credential No.:	
Tel:		Email Address:	
Visit Time: 2019-05-17 11:47:52		Appointed End Visit Time: 2019-05-17 13:36:47	
Reason for Visit:			
Remark:			

Step 3 On Visit Detail interface, confirm visitor info or enter visitor info, see Figure 3-345.

Step 4 Click **Authorization Info** tab.

The system displays **Authorization Info** interface, see Figure 3-346.

Figure 3-346 Visitor authorization

Visitor Name	Card No.	Tel	Host Name	Host Compan...	Appointed Vi...	Visit Time	Status	Operation
ABC			123		2019-05-17 ...	--	Appointed	🔍 ✕ ✎
James			123	Green Life	2019-05-17 ...	--	Appointed	🔍 ✕ ✎
abc			123		2019-05-17 ...	--	Appointed	🔍 ✕ ✎

Card Add	
Face Snapshot	
Access right	

Step 5 Issue card for visitor.

You can issue card by entering card No. manually or 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 card No. requirement. For example, if you enter card number 8004, then the

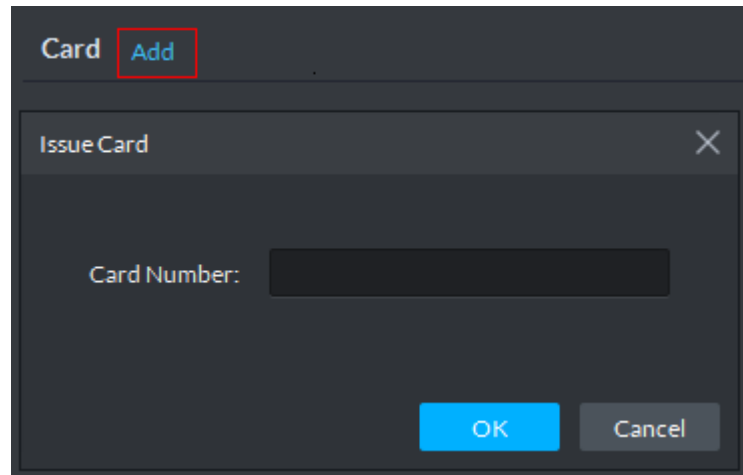
platform will change it to 00008004. If you enter card number 1000056821, then the platform will change it to 0000001000056821.

- Issue card by entering card No. manually

1) Click **Add** next to **Card**.

The system displays Issue Card interface, see Figure 3-347.

Figure 3-347 Add card



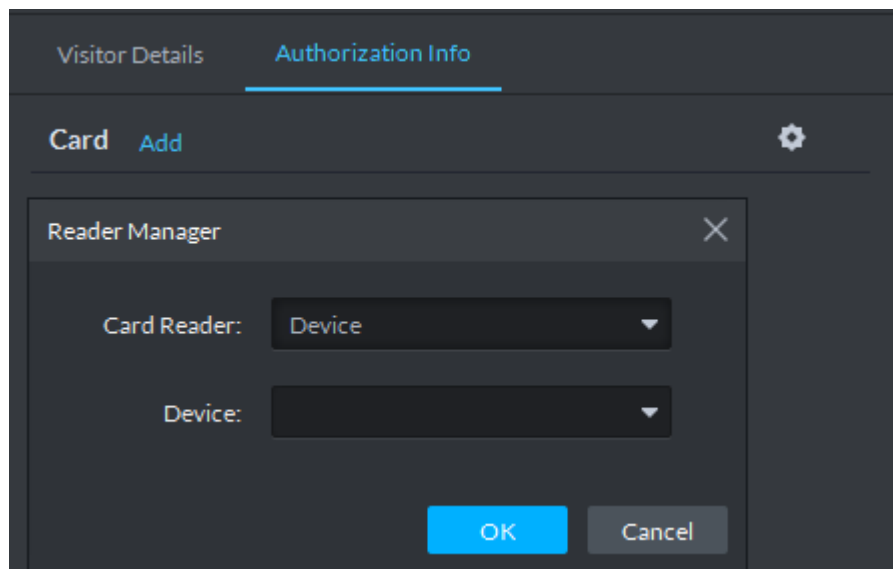
2) Enter card number, click **OK**, and card is issued.

- Issue card by reader

1) Click **Reader Manager**.

The system displays **Reader Manager** interface, see Figure 3-348.

Figure 3-348 Reader manager



2) Select card reader or device, click **OK**.

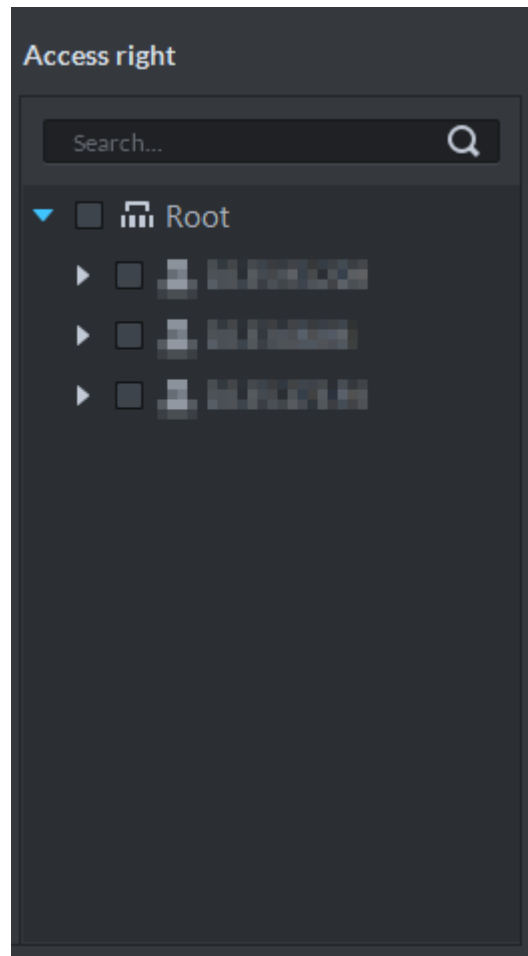
3) Swipe card on reader or device, and card is issued.

Step 6 Click **Snapshot**, and you can take face snapshot according to system prompt.

The face snapshot is used for face recognition and unlock door.

Step 7 In **Access Right** area, select AC channel that visitor can pass, see Figure 3-349.

Figure 3-349 Select channel

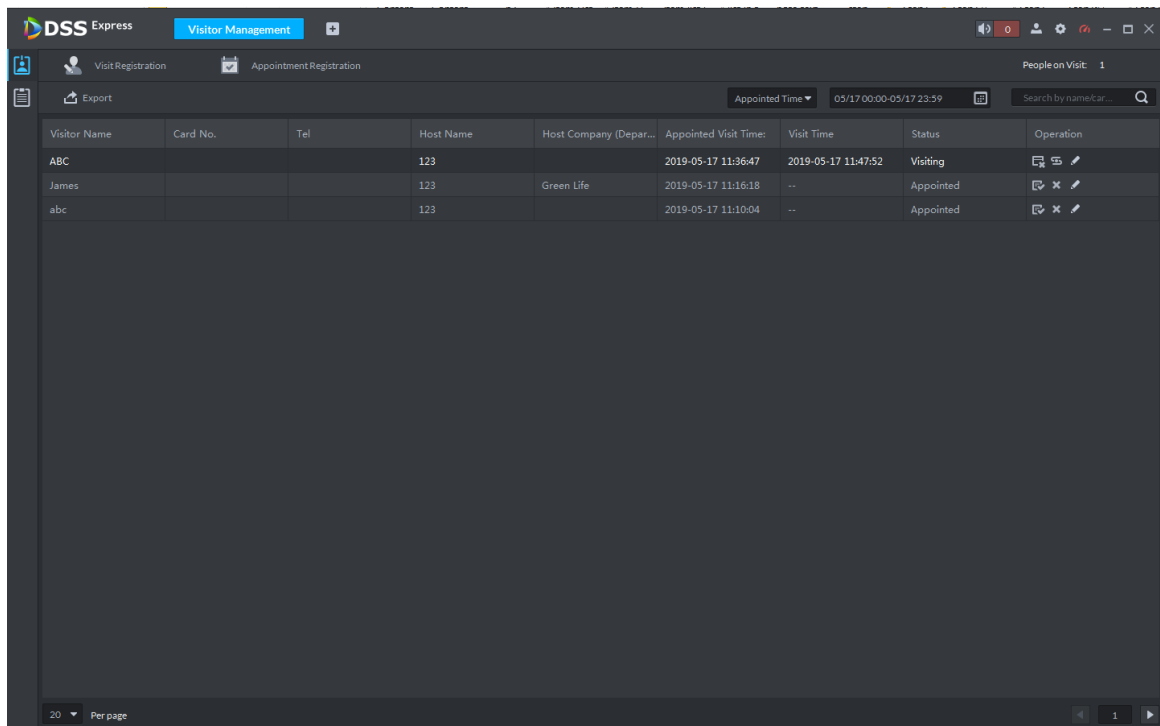


Step 8 Click **OK** and complete visitor registration, see Figure 3-350.



- Click  and skip to end visit interface.
- Click  and view visitor swiping card records.

Figure 3-350 Visit registration



3.14.4 End Visit Registration

When visitor leaves, close access permission.

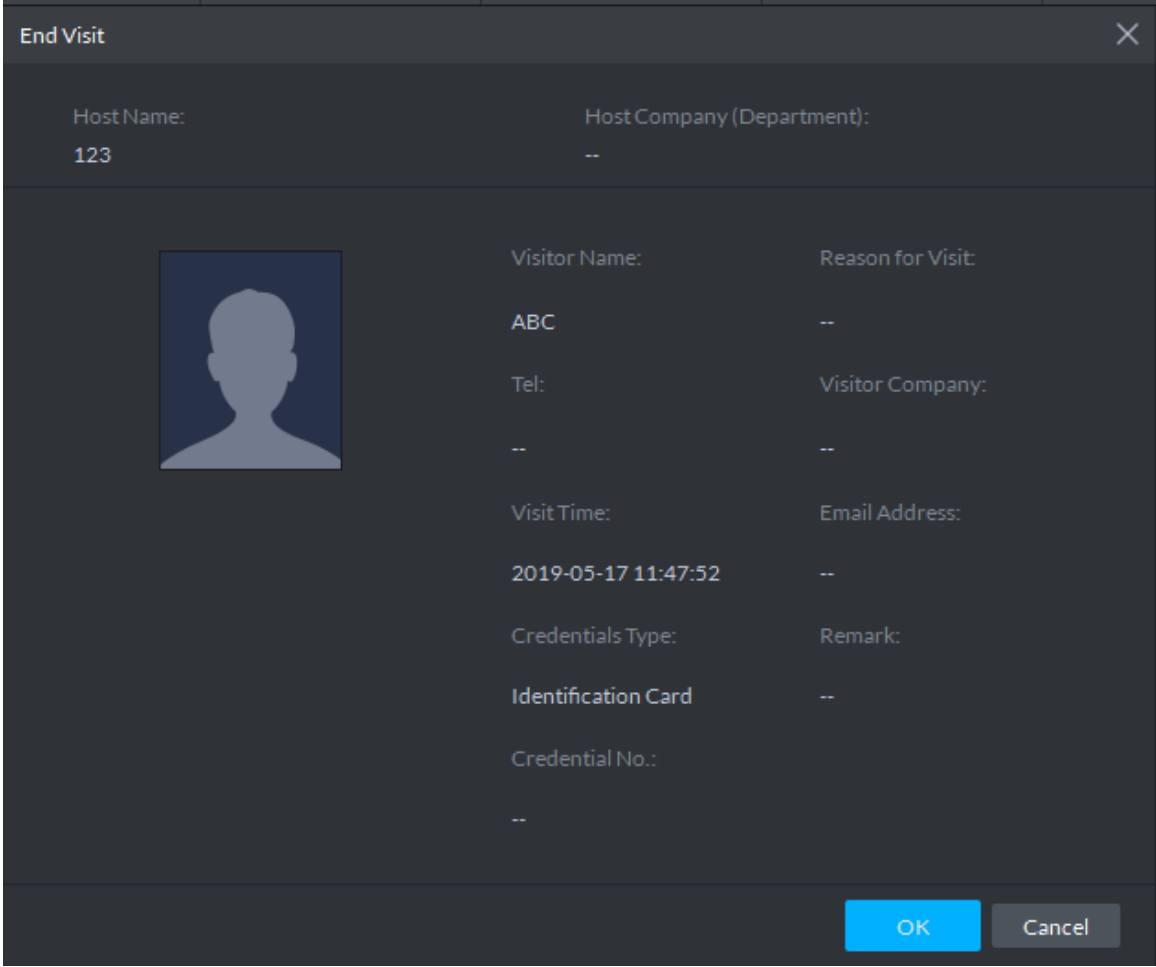
Step 1 On **Visitor Management** interface, click .

The system displays **Visitor Management** interface.

Step 2 Search end visit person info, click .

The system displays **End Visit** interface, see Figure 3-351.

Figure 3-351 End visit

A dark-themed dialog box titled "End Visit" with a close button (X) in the top right corner. The dialog contains several fields for visitor information. On the left, there is a placeholder for a visitor photo. The fields are arranged in two columns. The first column includes "Host Name:" (value: 123), "Visitor Name:" (value: ABC), "Tel:" (value: --), "Visit Time:" (value: 2019-05-17 11:47:52), "Credentials Type:" (value: Identification Card), and "Credential No.:" (value: --). The second column includes "Host Company (Department):" (value: --), "Reason for Visit:" (value: --), "Visitor Company:" (value: --), "Email Address:" (value: --), and "Remark:" (value: --). At the bottom right, there are two buttons: "OK" (highlighted in blue) and "Cancel".

Field	Value
Host Name:	123
Host Company (Department):	--
Visitor Name:	ABC
Reason for Visit:	--
Tel:	--
Visitor Company:	--
Visit Time:	2019-05-17 11:47:52
Email Address:	--
Credentials Type:	Identification Card
Remark:	--
Credential No.:	--

Step 3 Click **OK** and close access permission.

If you issue card to visitor, make sure the card is returned when visitor leaves.

3.14.5 Searching Visit Record

You can set condition and search visit record, and view visitor details and card swiping records.

Step 1 On **Visitor Management** interface, click .

The system displays **Visit Record** interface, see Figure 3-352.

Figure 3-352 Visit record

The screenshot shows the 'Visitor Management' section of the DSS Express software. On the left, there is a sidebar with search filters: Visitor Name, Tel, Email, Card No. (with a gear icon), Credential No., Host Name, Host Company (Department), Visit Time (set to 05/24 00:00-05/24 23:59), and Type (set to Unlimited). A blue 'Search' button is at the bottom of the sidebar. The main area features a table with the following columns: Visitor Name, Card No., Tel, Host Name, Host Company (...), Appointed Visit (...), Visit Time, End Visit Time, Status, and Operation. The table is currently empty. At the bottom right, there is a pagination control showing '20 Per page' and a page number '1'.

Step 2 Set search condition, click **Search**.

The system displays results, see Figure 3-353.



Card number info supports clicking  to set card reader, and you can read by reader.

Figure 3-353 Search visit result

The screenshot shows the same 'Visitor Management' interface as Figure 3-352, but now with search results. The search filters on the left are the same, but the 'Visit Time' is now set to 05/16 00:00-05/16 23:59. The table now contains one row of data:

Visitor Name	Card No.	Tel	Host Name	Host Company (...)	Appointed Visit (...)	Visit Time	End Visit Time	Status	Operation
2			1		--	2019-05-16 14:...	2019-05-16 14:...	End Visit	

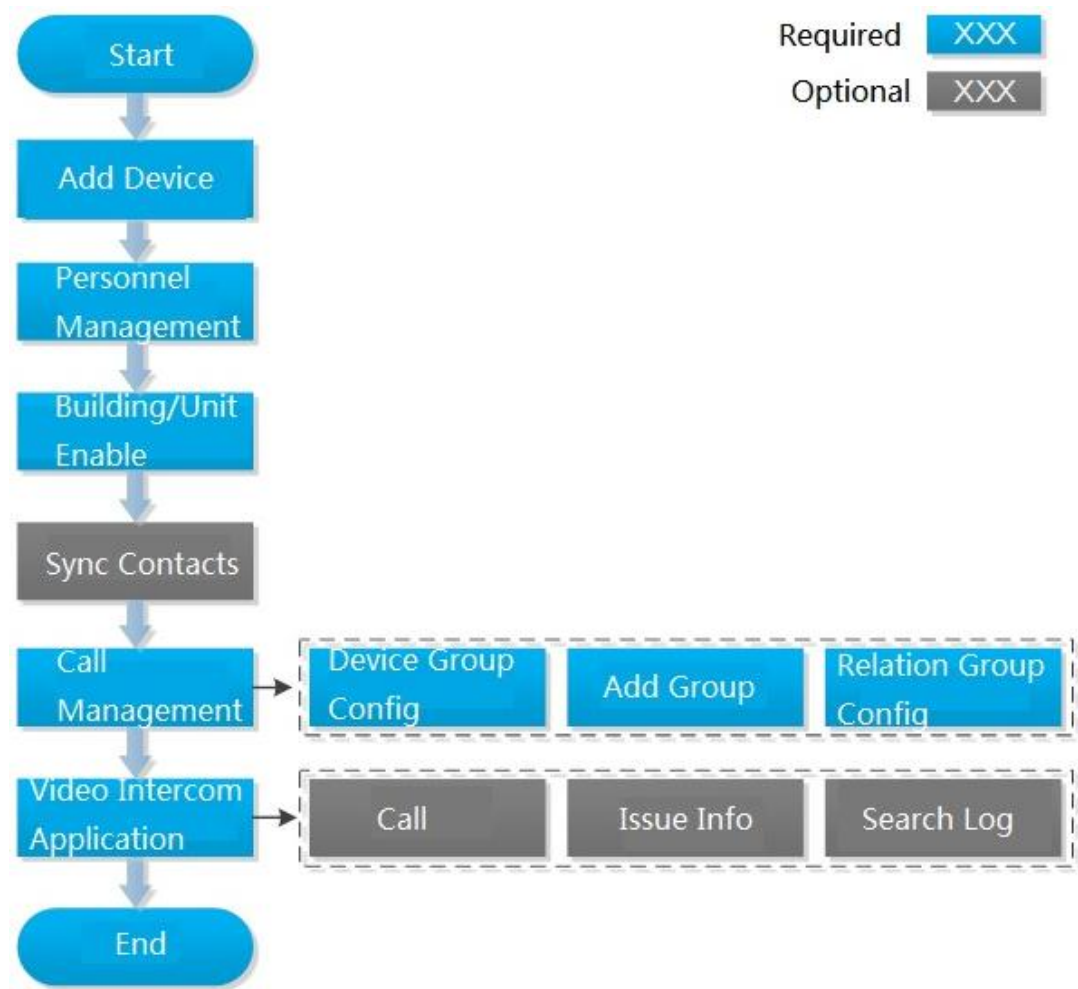
The pagination control at the bottom right still shows '20 Per page' and page number '1'.

Step 3 Click  and view visitor details and card swiping records.

3.15 Video Intercom

After integrating video talk module and adding video intercom device, you can realize device talk, realtime monitoring and issuing info. The video intercom operation flow is shown in Figure 3-354

Figure 3-354 Operation flow



Configure video intercom on platform, the device is required to be configured. For more details, refer to user manual.

3.15.1 Adding Video Intercom Device

Add video intercom devices such as unit VTO, VTH and fence VTO. For more details, see **3.2.2.4 Adding Device**

If you modify config when using device, the device will not actively push message to platform. You need to acquire device info manually from platform. For more details, see **3.2.2.5 Editing Device**

3.15.2 Personnel Management

For video intercom, you can add personnel by the module of personnel management. See **3.12 Personnel Management** for more details. Room number is required to be configured when adding personnel.

3.15.3 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”.

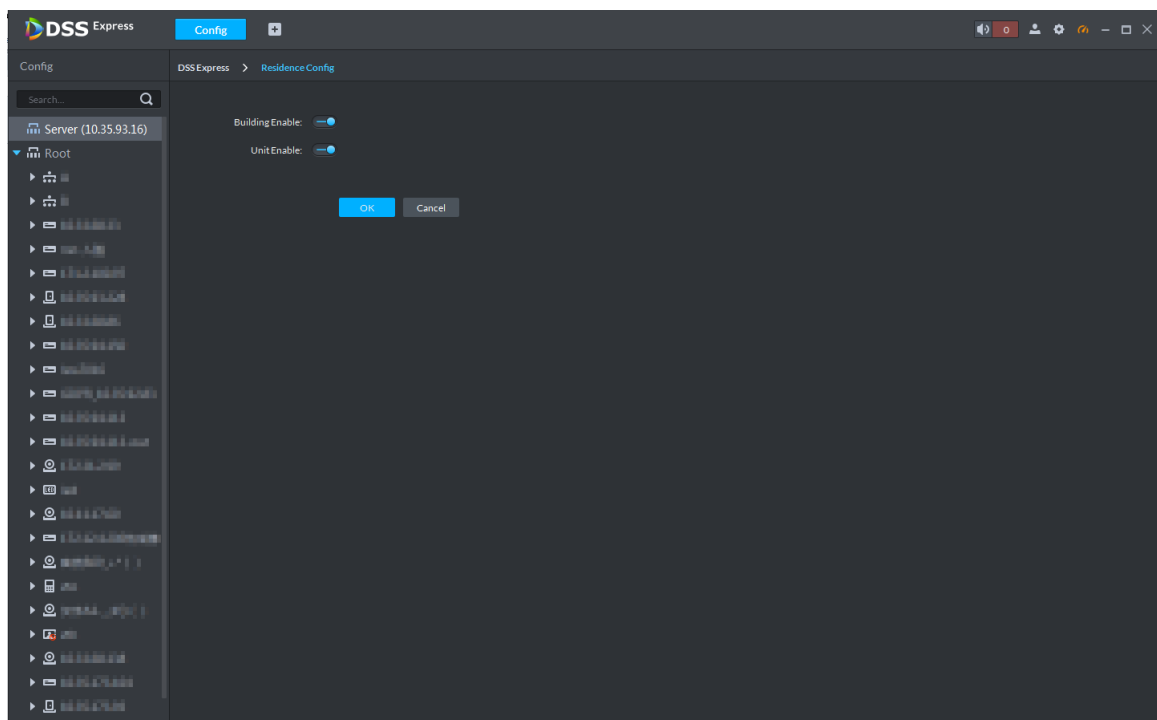
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Click **Residence Config**.

The system displays **Residence Config** interface. See Figure 3-355.

Figure 3-355



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 config.

3.15.4 Synchronizing Contacts

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

Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Select VTO from the device list, and click **Contacts**, see Figure 3-356.

The system displays **Release Contact** interface, see Figure 3-357.

Figure 3-356

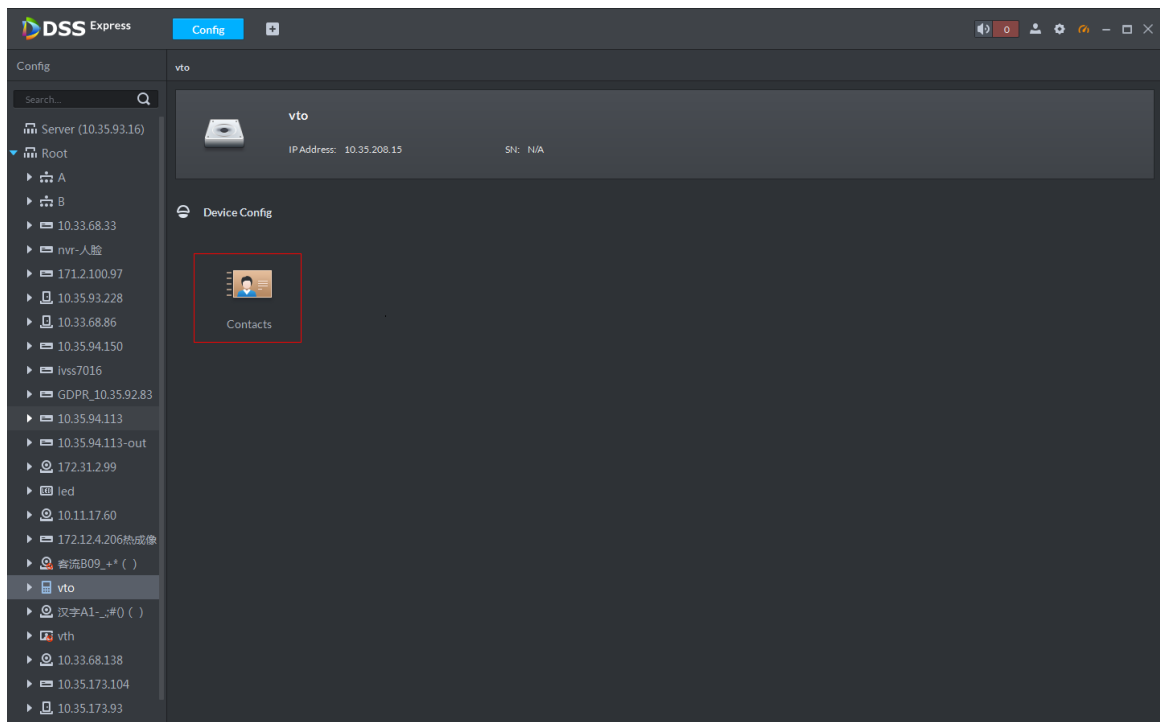
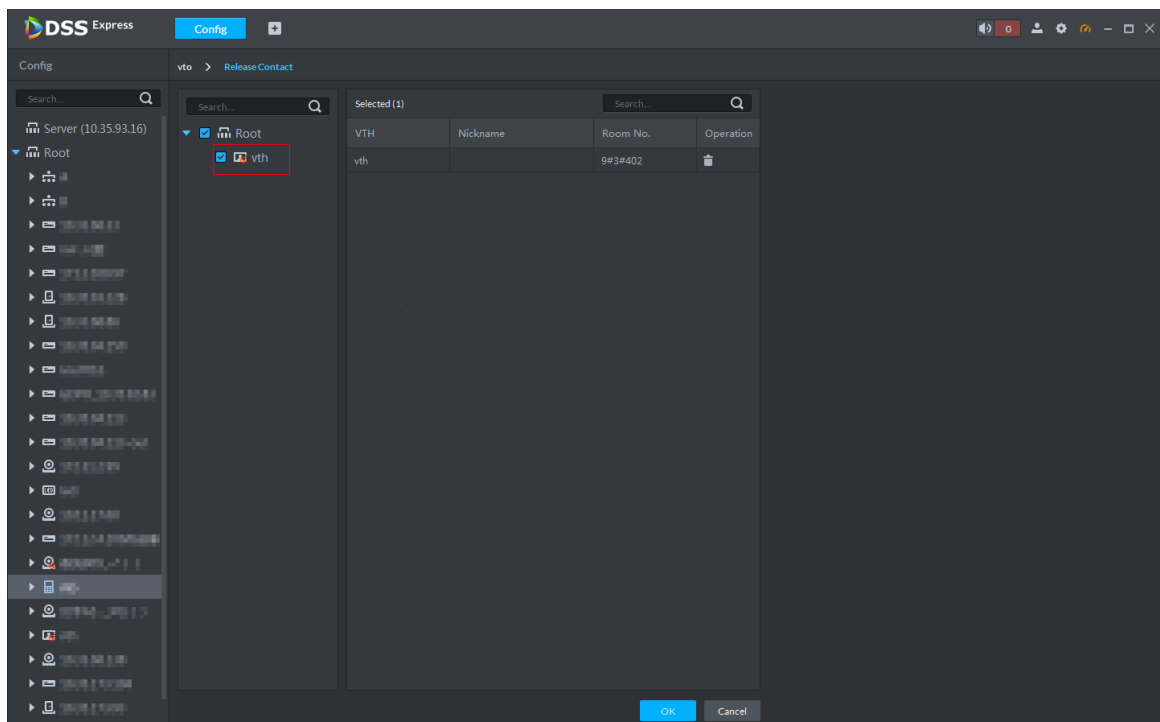


Figure 3-357 Release contact



Step 3 Select VTH, click **OK**.

You can view contacts on VTO screen or WEB interface after it is released.

3.15.5 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.

3.15.5.1 Device Group Config

It can realize mutual call only when VTO and VTH are added into the same device group. Pro will automatically generate corresponding device group when VTO, verifying VTO and fence station are added to Pro.

- Add VTO and automatically generate a device group, add VTH of the unit into the group, and realize mutual call between VTH and VTO within the group.
- Add verifying VTO and automatically generate a device group, add it to the group together with the VTH of the same room, and realize mutual call between VTH and verifying VTO within the group.
- Add fence station and automatically generate a device group, add all the VTH into the group. Realize mutual call between fence station and all the VTH.
- Add VTH, if the VTH is automatically connected to unit VTO, verifying VTO, fence station, and then it will be automatically added to the device group, and realize mutual call among unit VTO, verifying VTO or fence station.



Call between VTH is not restricted by device group; mutual call can be realized among VTH in different device groups.

3.15.5.2 Adding Management Group

Management group is to make groups for administrators, and realize relation binding of one to one, one to many or many to many. Administrators include Pro administrator and VTS. If there is default management group, VTS will be automatically added to management group when it is added.

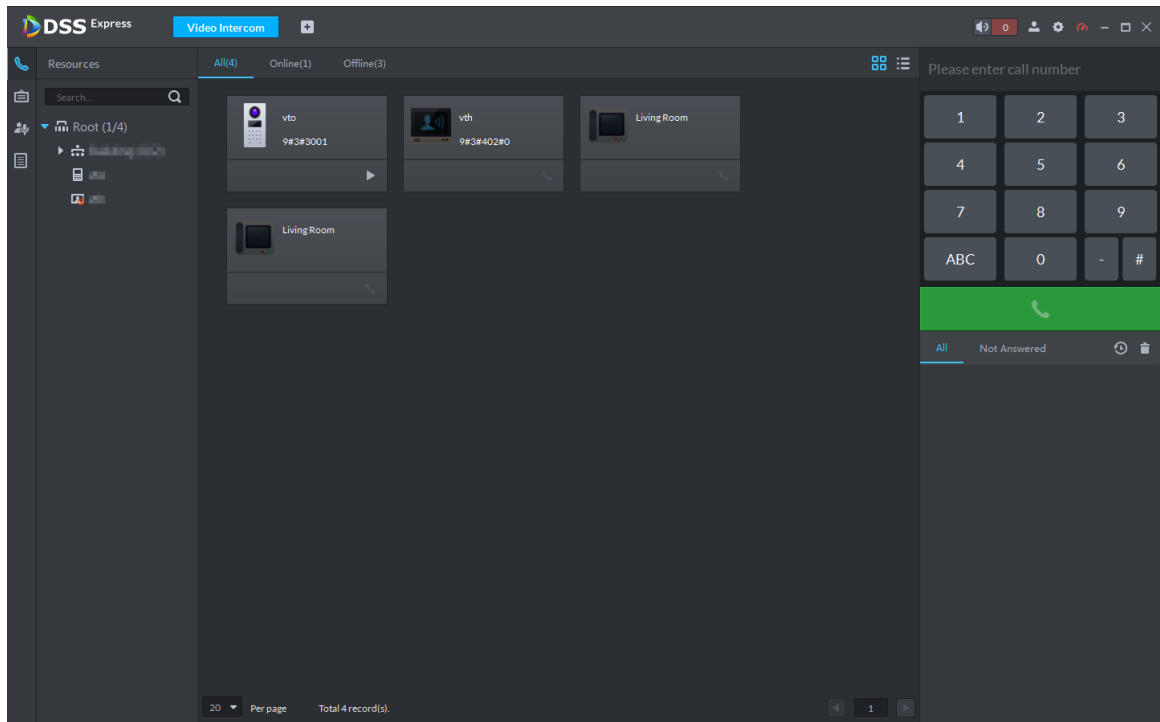


- Before configuring management group, it needs to create user, select video intercom menu permission and device permission, and add new users into management group.
- Use system user to configure group relation, need to switch to new user for login. If system logs onto many devices, then it cannot be used as administrator.

Step 1 On client homepage, click **Video Intercom**.

The system displays Video Intercom interface, see Figure 3-358.

Figure 3-358 Video intercom



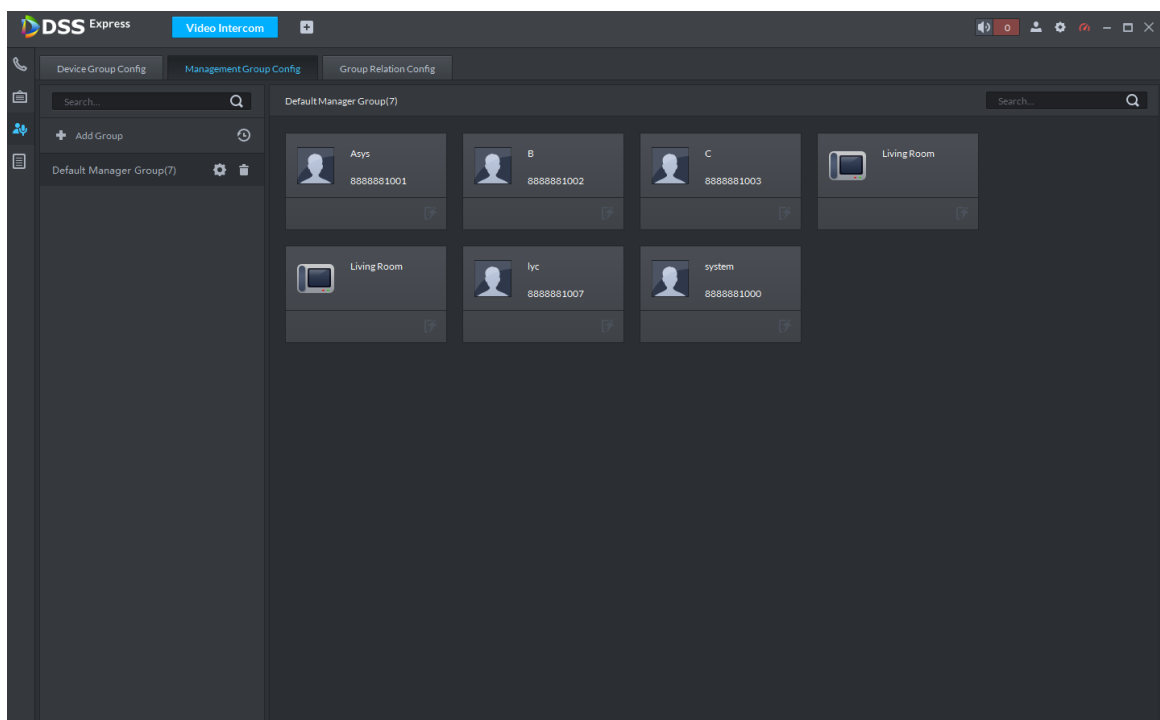
Step 2 Click .

The system displays the interface of **Call Management**.

Step 3 Click **Management Group Config**.

The system displays the interface of **Management Group Config**. See Figure 3-359.

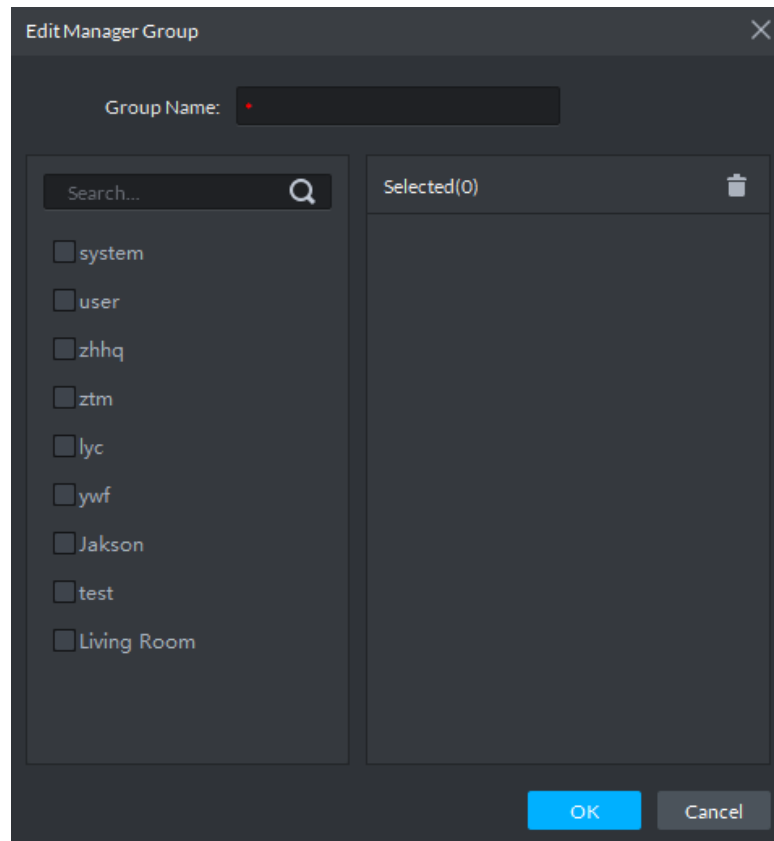
Figure 3-359 Call management



Step 4 Click **Add Group**.

The system displays the interface of **Edit Manager Group**. See Figure 3-360.

Figure 3-360 Manager group



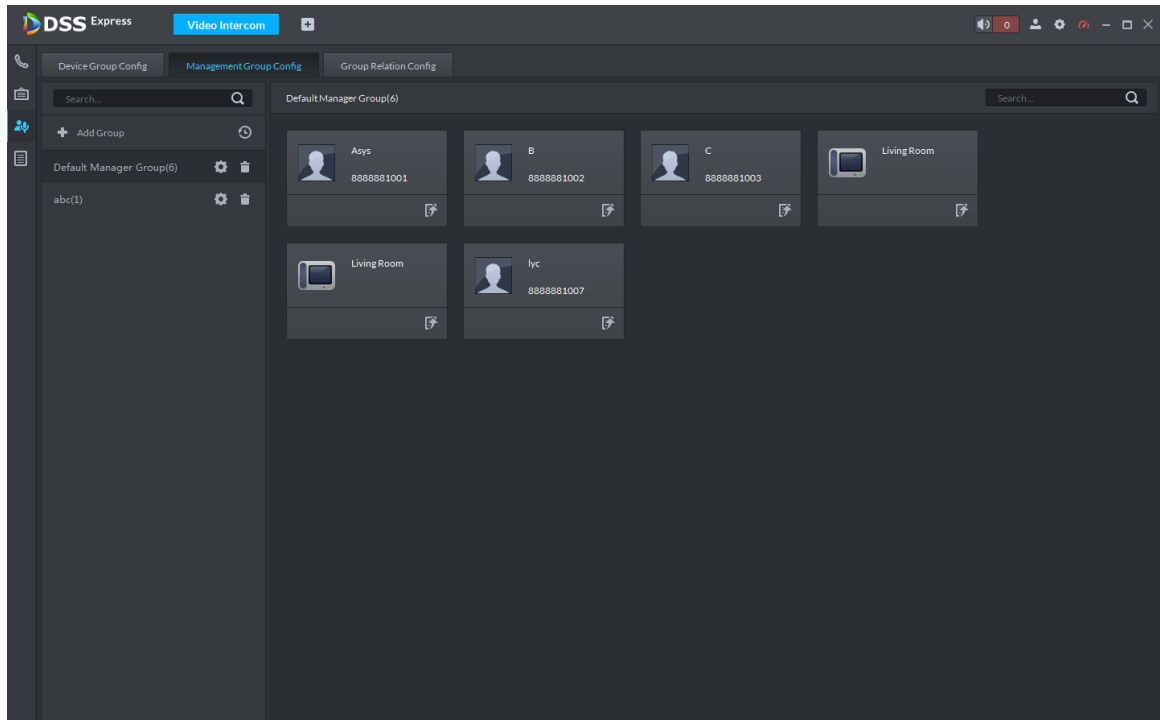
Step 5 Enter group name, select administrator account or VTS, and click **OK**.
The added management group is displayed in the list. See Figure 3-361.



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 3-361 Manager group



3.15.5.3 Group Relation Config

Relation group config 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.

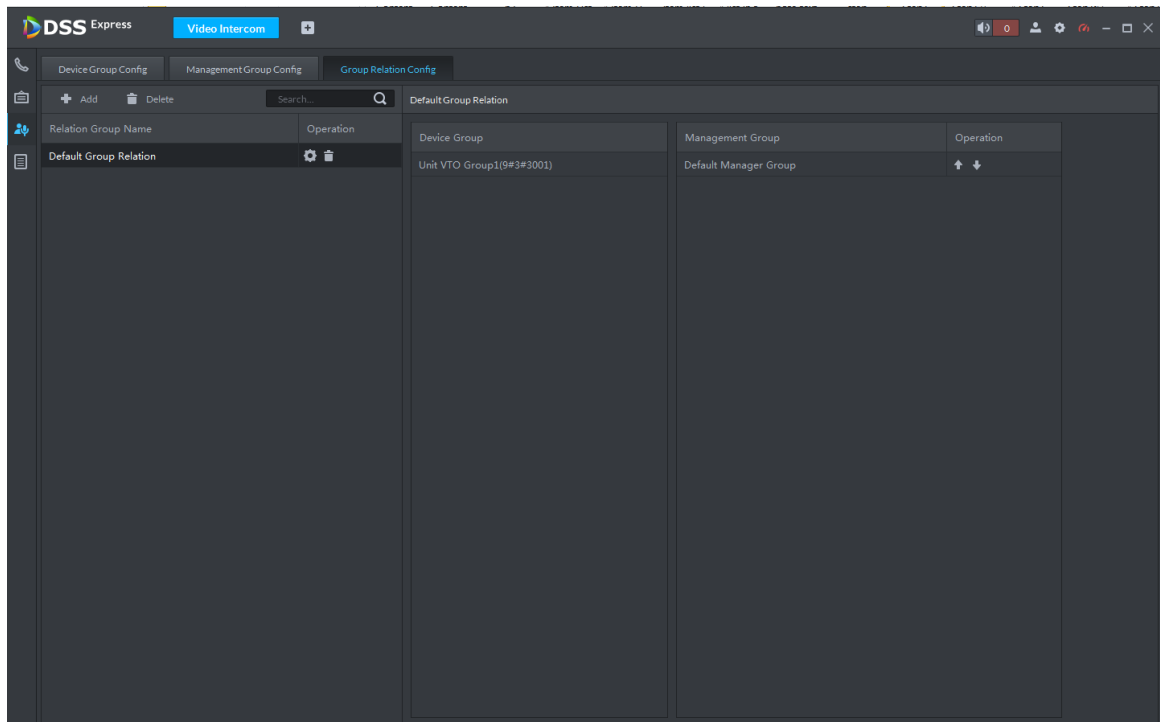
Step 1 Click  on the interface of **Video Intercom**.

The system displays the interface of **Relation Group Config**.

Step 2 Click the tab of **Relation Group Config**.

The system displays the interface of **Relation Group Config**. See Figure 3-362.

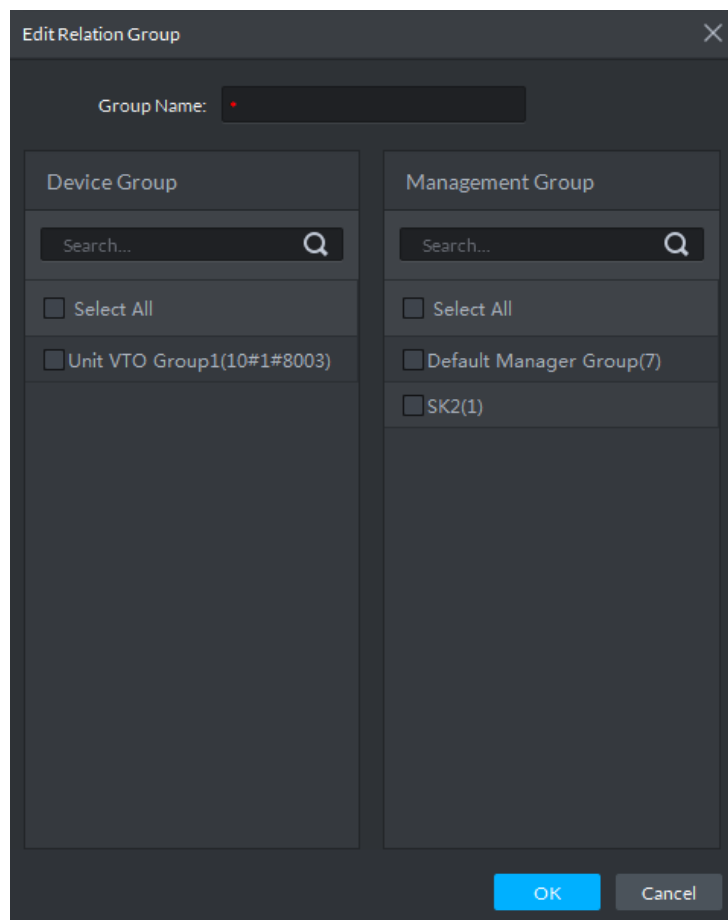
Figure 3-362 Group relation config



Step 3 Click **Add**.

The system displays the interface of **Edit Relation Group**. See Figure 3-363.

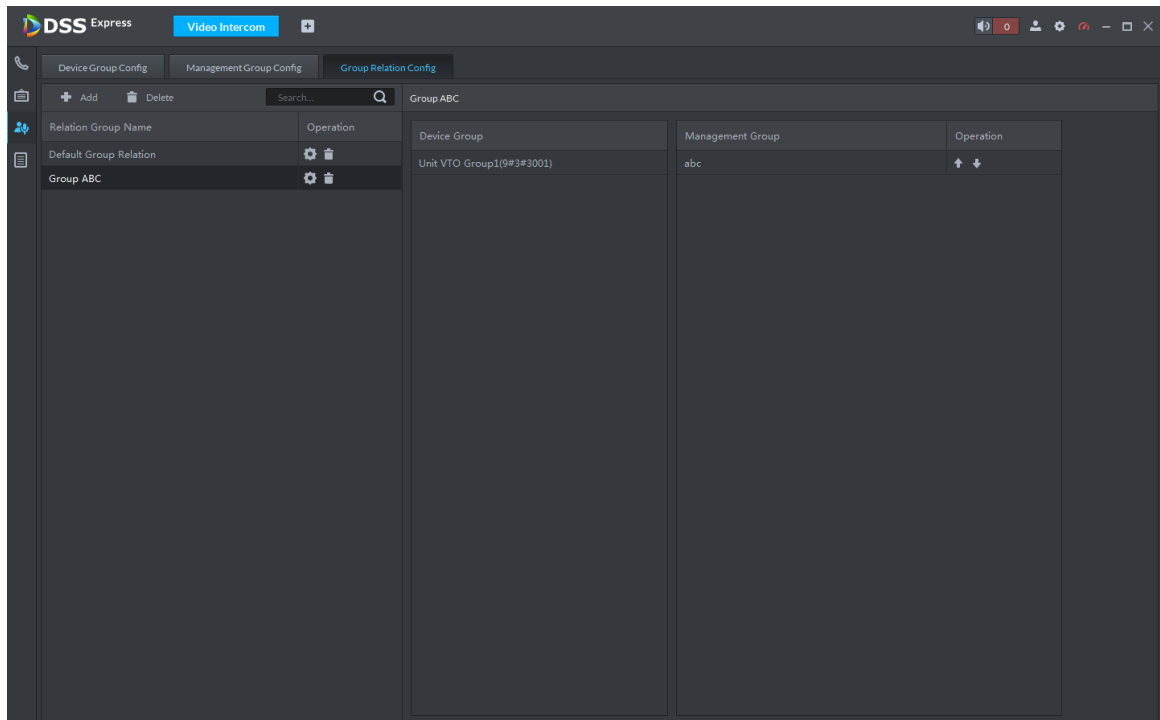
Figure 3-363 Edit relation group



Step 4 Enter name, select device group and management group, Click **OK**.

Added relation group is displayed in the list. See Figure 3-364. 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 3-364 Edit relation group



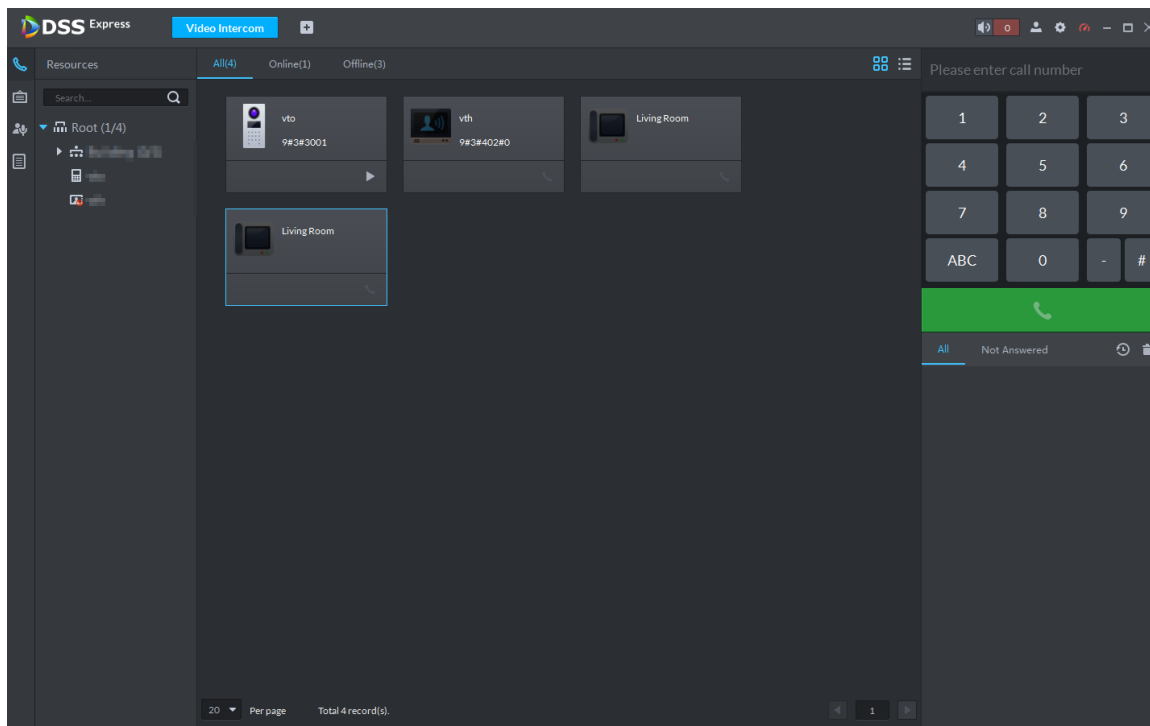
3.15.6 Video Intercom Application

3.15.6.1 Call Center

Step 1 Click  on the interface of **Video Intercom**.

The system displays the interface of **Call Center**. See Figure 3-365.

Figure 3-365 Call center



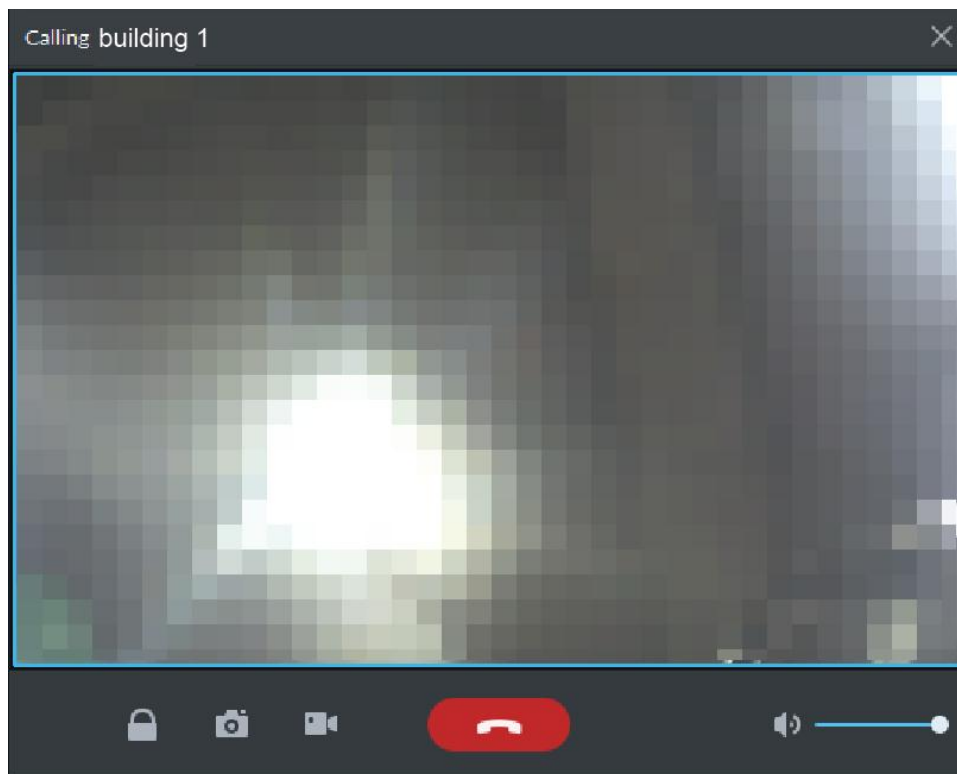
Step 2 You can call VTO and VTH on the interface of **Call Center**.

- Platform calls VTO

Select VTO in the device list; click corresponding  of VTO and call VTO. The system pops out call interface and realizes video talk. See Figure 3-366. Following operations are supported 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 **3.3.4 Setting Snapshot** for more details.
- ◇ , click the icon to start record, and 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 **3.3.5 Setting Recording Parameter** for more details.
- ◇ , click the icon to hang up.

Figure 3-366 Call VTO

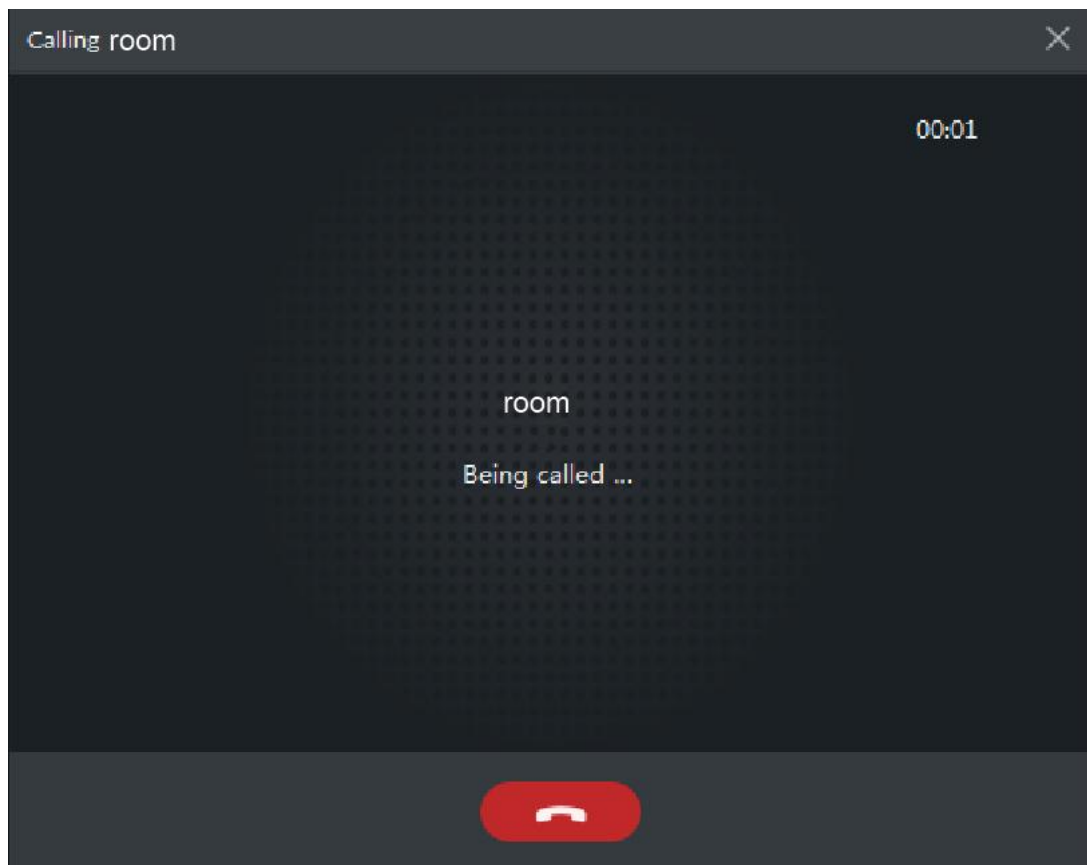


- Platform call VTH

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 3-367. There are two modes for answering the call.

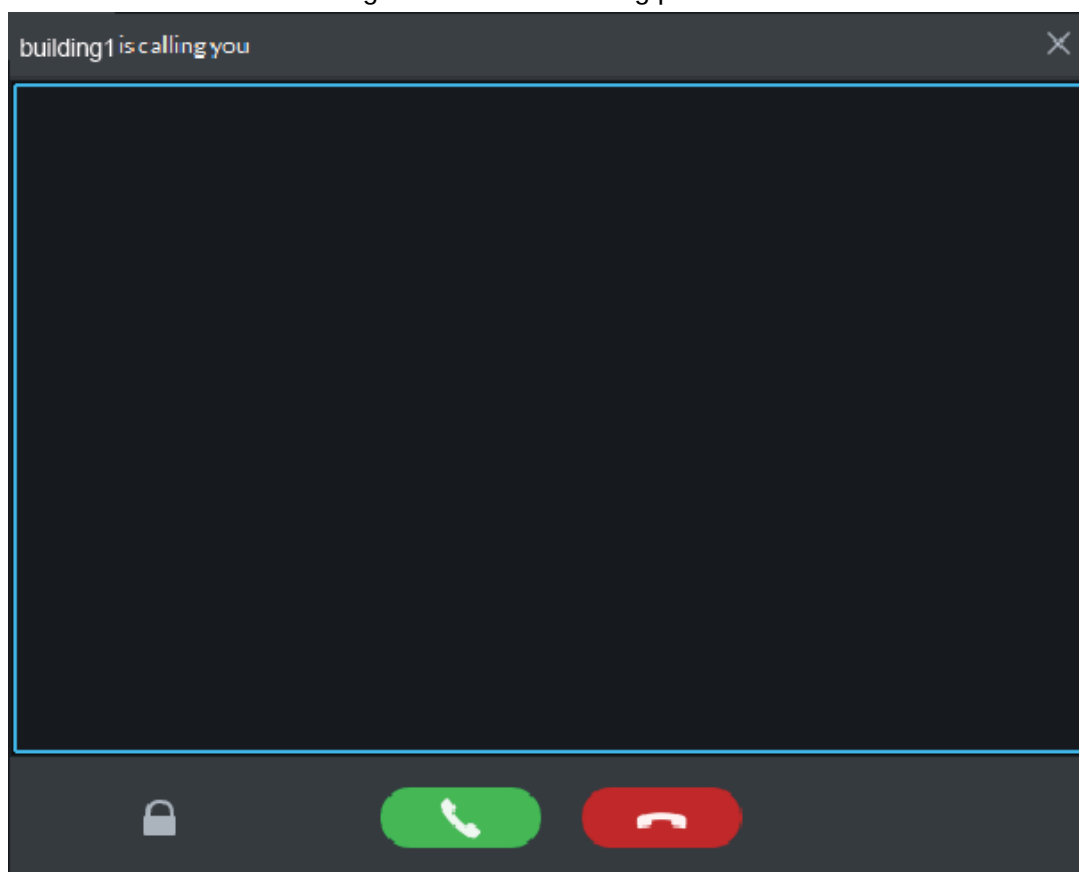
 - ◇ Answer by VTH, bidirectional talk between client and VTH. Press  to hang up when you answer the call.
 - ◇ If VTH fails to answer over 30s, busy or hang up directly, then it means the callee is busy.

Figure 3-367 Call VTH



- VTO calls platform
VTO calls platform, client pops up the dialog box of VTO calling. See Figure 3-368.
 - ◇ , 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 3-368 VTO calling platform

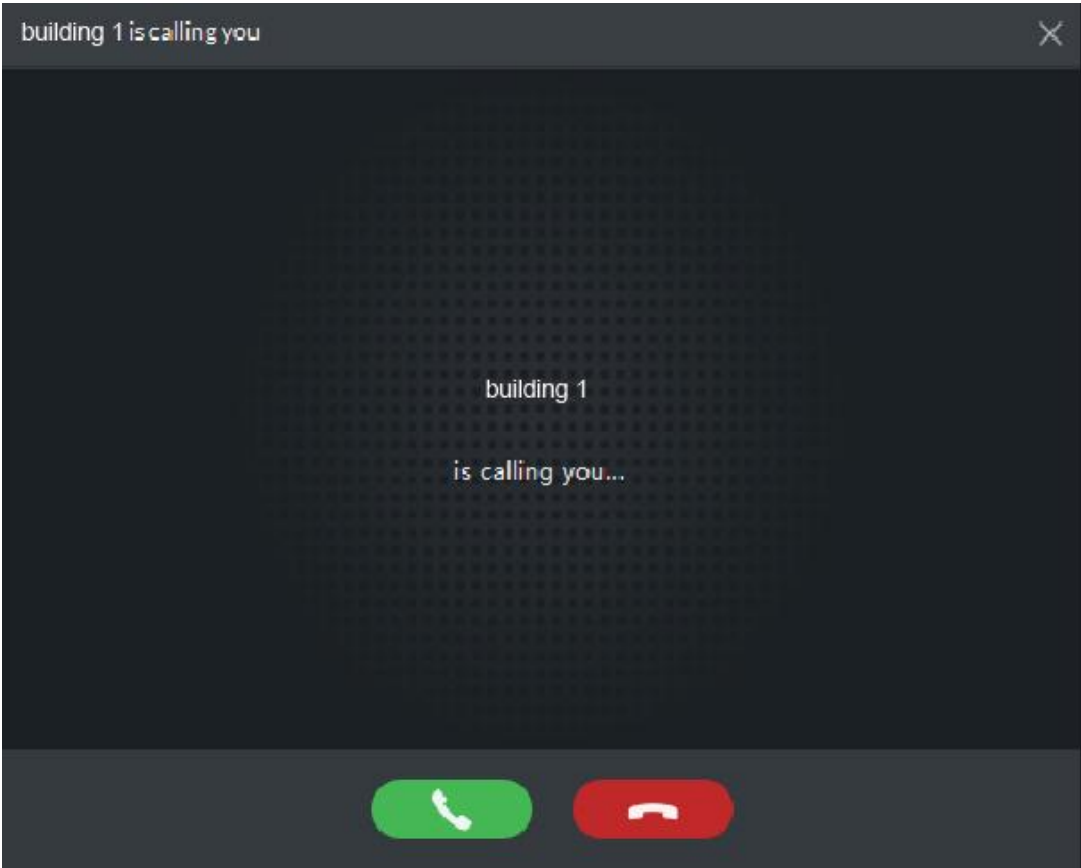


- VTH calls client

The client pops out the dialog box of VTH calling. See Figure 3-369. Click  and realize talk with VTH.

- ◇ , click the icon and answer VTO, realize mutual talk after connected.
- ◇ , click the icon and hang up.

Figure 3-369 VTH calling client



- Call via call record
All the call records are displayed in the **Call Record** in the lower right corner of the interface of **Video Intercom**. See Figure 3-370. Move the mouse to the record, click  and call back.

Figure 3-370 Call records

All	Not Answered		
	4#4#401#0	00:00	2018-07-02 13:57:28
	4#4#402#0	00:00	2018-07-02 13:56:55
	4#4#401#0 (2)	00:00	2018-07-02 13:56:44
	4#4#8001 (4)	00:06	2018-07-02 13:53:43
	4#4#402#0	00:00	2018-07-02 13:43:19

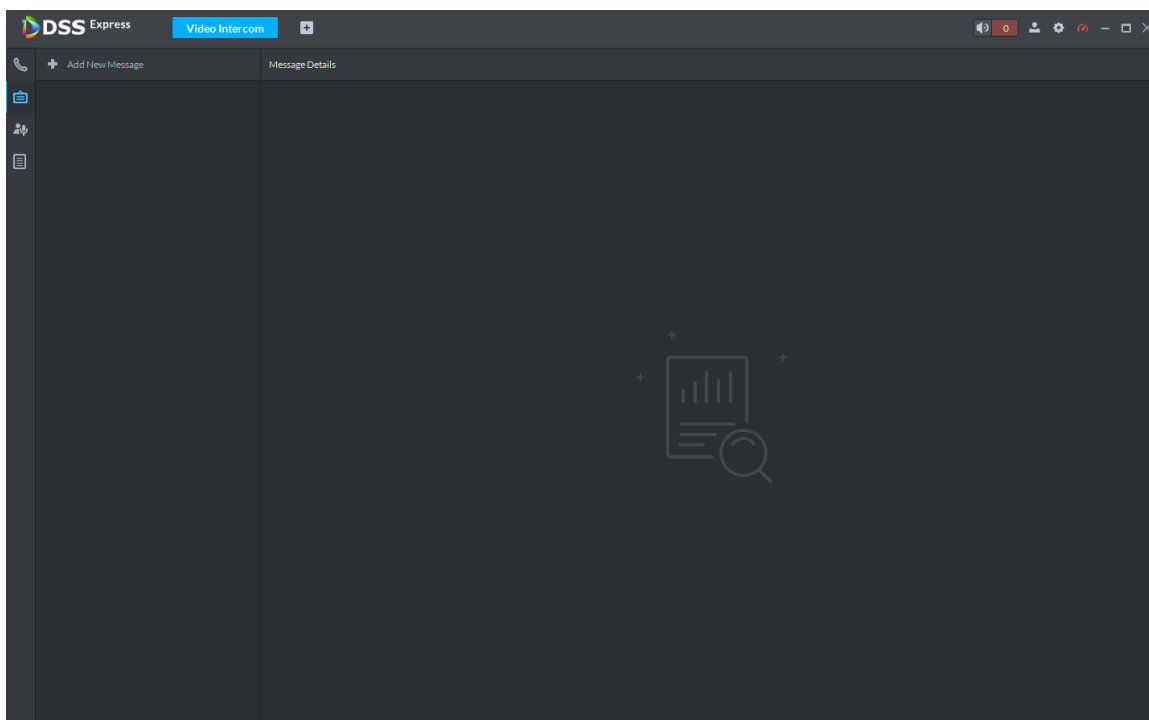
3.15.6.2 Releasing Info

The platform sends message to designated VTO.

Step 1 Click  on the interface of **Video Intercom**.

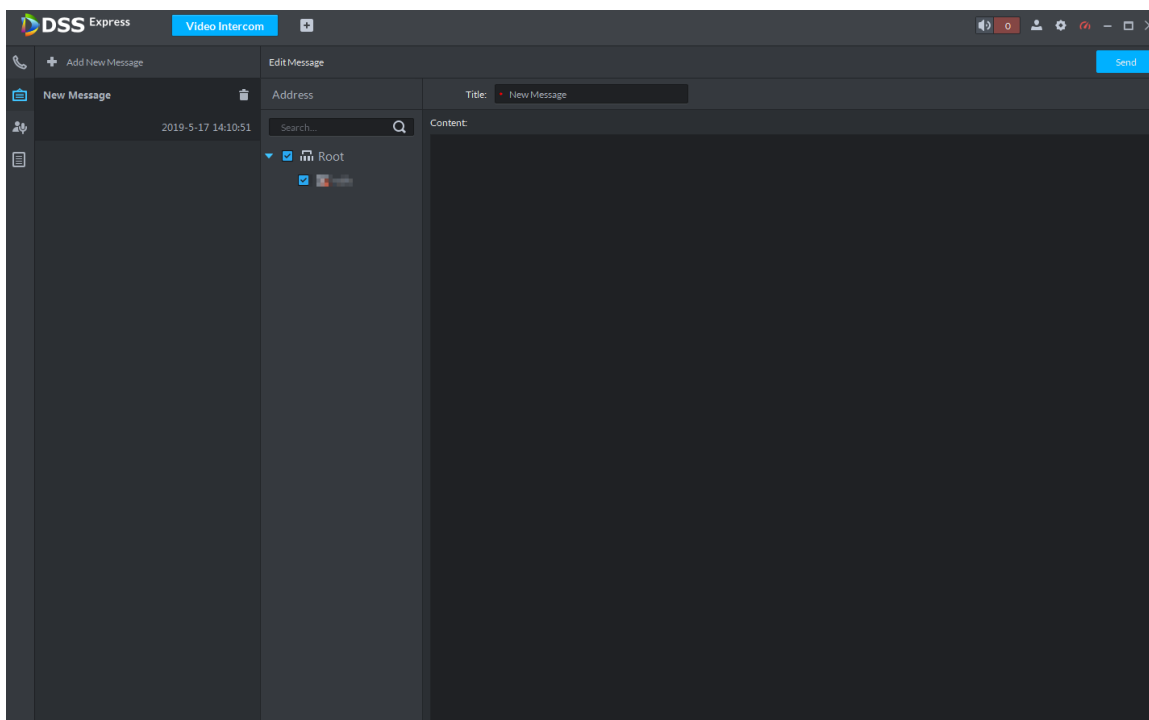
The system displays the interface of **Release Info**. See Figure 3-371.

Figure 3-371 Release info (1)



Step 2 Click **Add New Message**, select VTH and add release info. See Figure 3-372.

Figure 3-372 Release info (2)



Step 3 Click **Send**.

The VTH will receive the message after it is sent successfully.

3.15.6.3 Searching Video Intercom Log

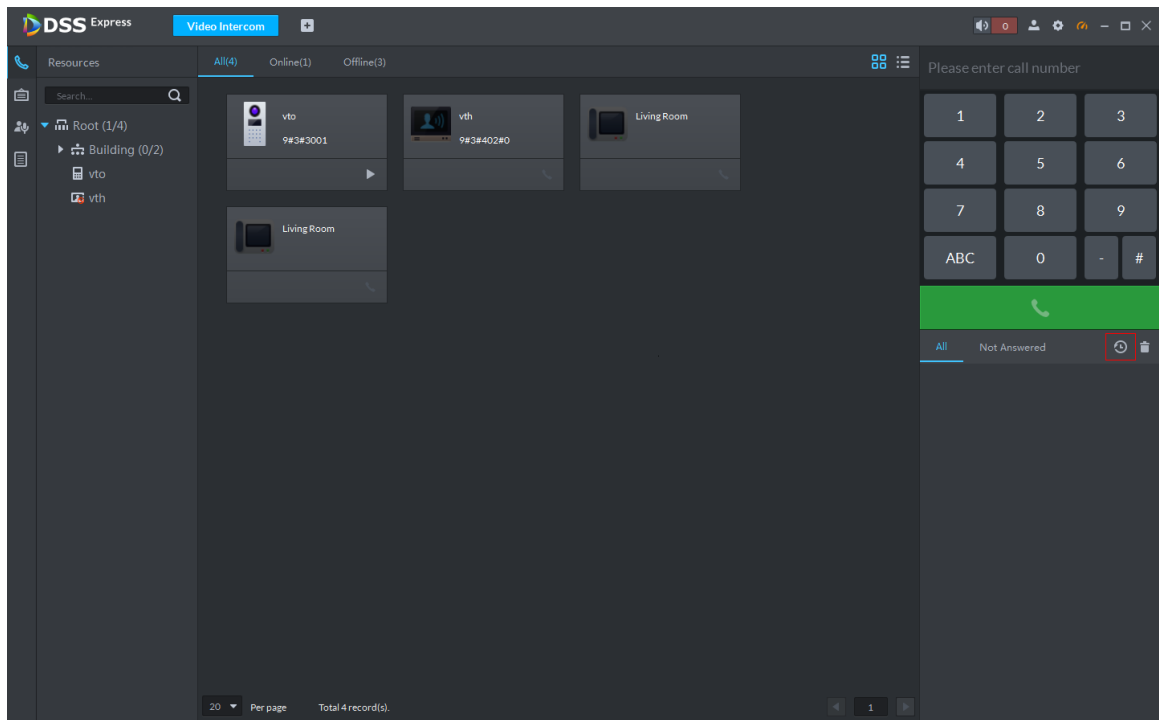
View log records and you can trace recorded calls.

Step 1 Enter the interface of video intercom log.

The system supports following two ways to enter.

- Click  on the interface of **Video Intercom**.
- Click  and enter console on the interface of **Video Intercom**. See Figure 3-373.

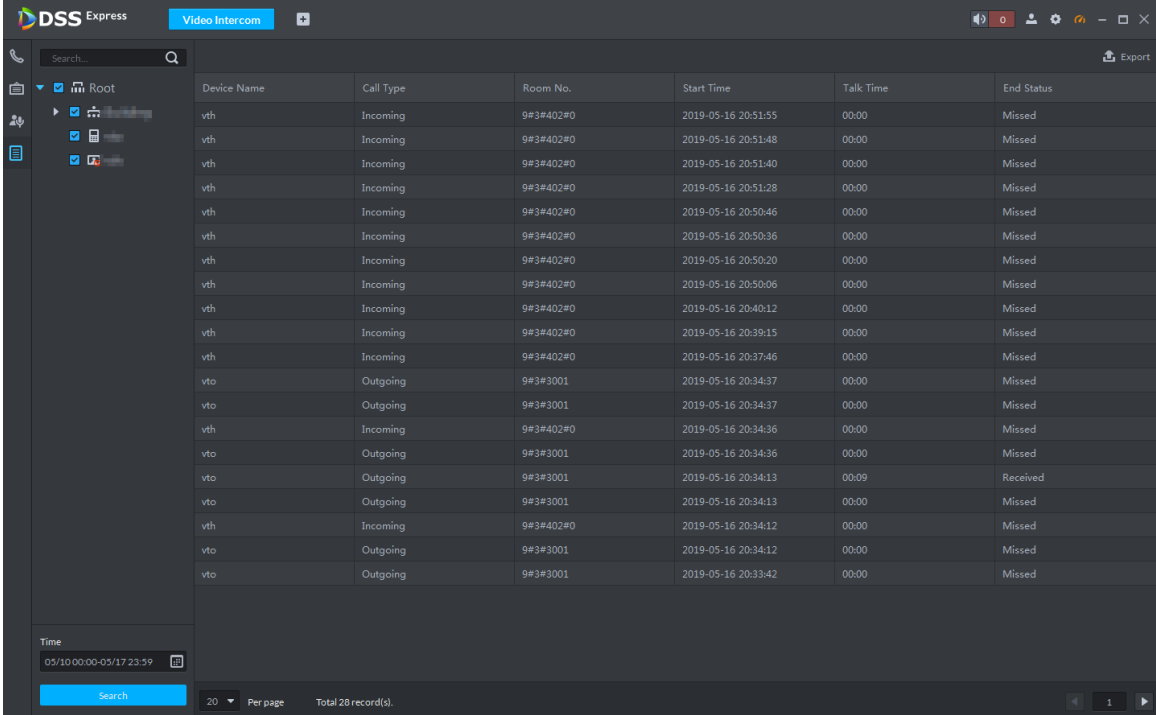
Figure 3-373 Enter log interface



Step 2 Set conditions, click **Search**.

The system displays the log info. See Figure 3-374

Figure 3-374 Search log



Device Name	Call Type	Room No.	Start Time	Talk Time	End Status
vth	Incoming	9#3#402#0	2019-05-16 20:51:55	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:51:48	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:51:40	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:51:28	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:50:46	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:50:36	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:50:20	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:50:06	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:40:12	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:39:15	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:37:46	00:00	Missed
vto	Outgoing	9#3#3001	2019-05-16 20:34:37	00:00	Missed
vto	Outgoing	9#3#3001	2019-05-16 20:34:37	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:34:36	00:00	Missed
vto	Outgoing	9#3#3001	2019-05-16 20:34:36	00:00	Missed
vto	Outgoing	9#3#3001	2019-05-16 20:34:13	00:09	Received
vto	Outgoing	9#3#3001	2019-05-16 20:34:13	00:00	Missed
vth	Incoming	9#3#402#0	2019-05-16 20:34:12	00:00	Missed
vto	Outgoing	9#3#3001	2019-05-16 20:34:12	00:00	Missed
vto	Outgoing	9#3#3001	2019-05-16 20:33:42	00:00	Missed

Step 3 Click **Export** and the logs will be saved locally according to system prompt.

3.16 Attendance Management

Add attendance device on platform, and you can manage and configure attendance, view attendance data on platform. The attendance operation flow is shown in Figure 3-375.

Figure 3-375 Attendance flow



3.16.1 Adding Attendance Device

Add access control or face attendance for attendance. For more details, see **3.2.2.4 Adding Device**

3.16.2 Personnel Management

Use the module of personnel management for attendance personnel. If you want to add person, see **3.12 Personnel Management**

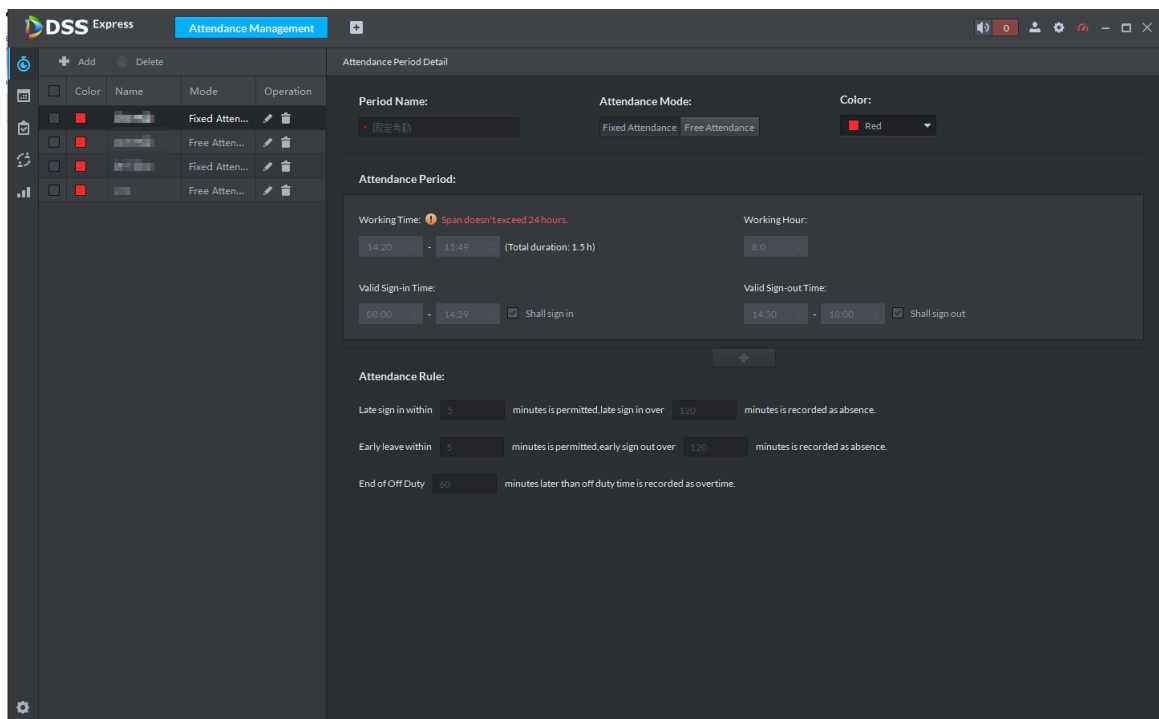
3.16.3 Setting Attendance Terminal

Make sure access control is used as attendance device, used to swipe card, record attendance info and upload attendance data.

Step 1 Click  and select **Attendance Management** on the interface of **Homepage**.

The system displays the interface of **Attendance Management**. See Figure 3-376.

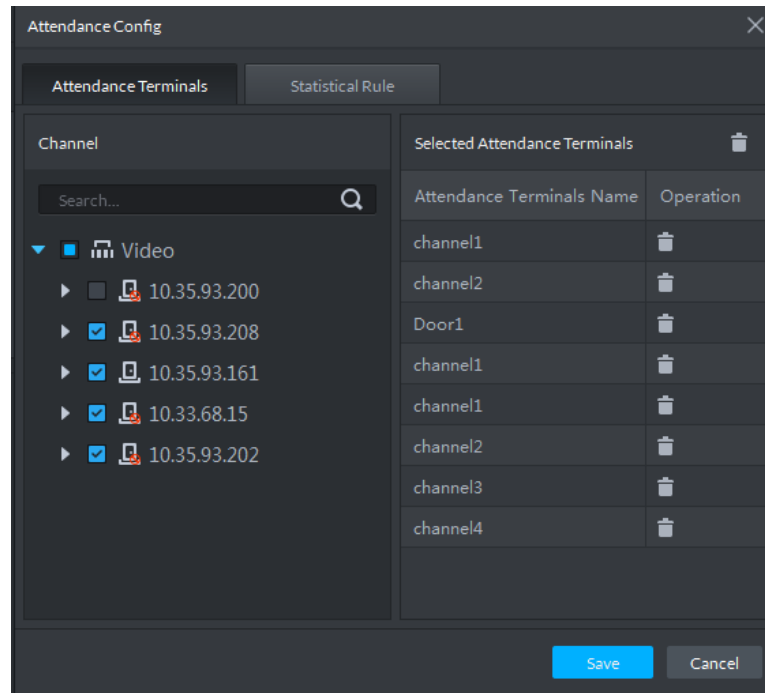
Figure 3-376 Attendance management



Step 2 Click  on the lower left corner of the interface, select **Attendance Terminal**.

The system displays the interface of **Attendance Terminal**. See Figure 3-377.

Figure 3-377 Attendance config



Step 3 Select access control channel from the left list, click **Save**.



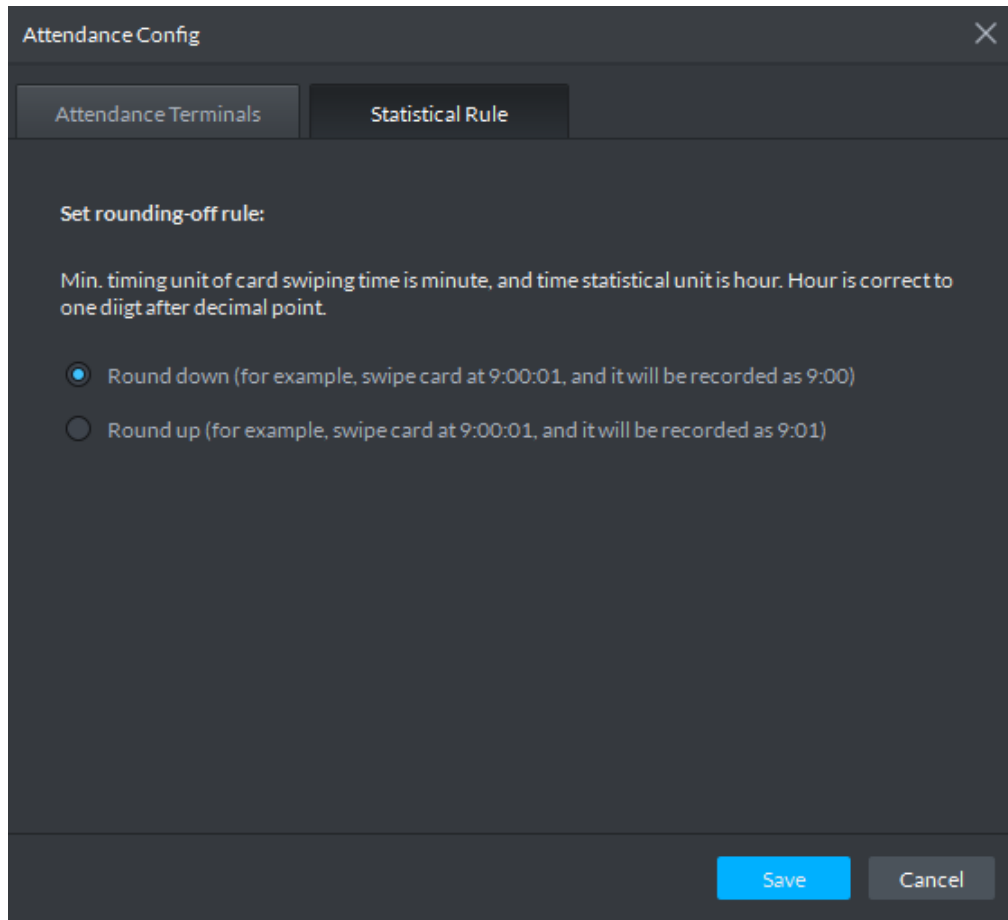
You can find needed device by search function, the system supports fast search.

3.16.4 Setting Statistics Rule

Minimum timing unit of swiping card is minute, the statistics rule of dealing with second is round up and round down. For example, swipe card at 09:00:01, if the rule is set as round down, then the time of swiping card is 09:00; if the rule is set as round up, then the time of swiping card is 09:01.

Step 1 Click  at the lower left corner on the interface of **Attendance Management**, select **Statistics Rule**. The interface of **Statistical Rule** is displayed. See Figure 3-378

Figure 3-378 Set statistics rule



Step 2 Select rule and click **Save**.

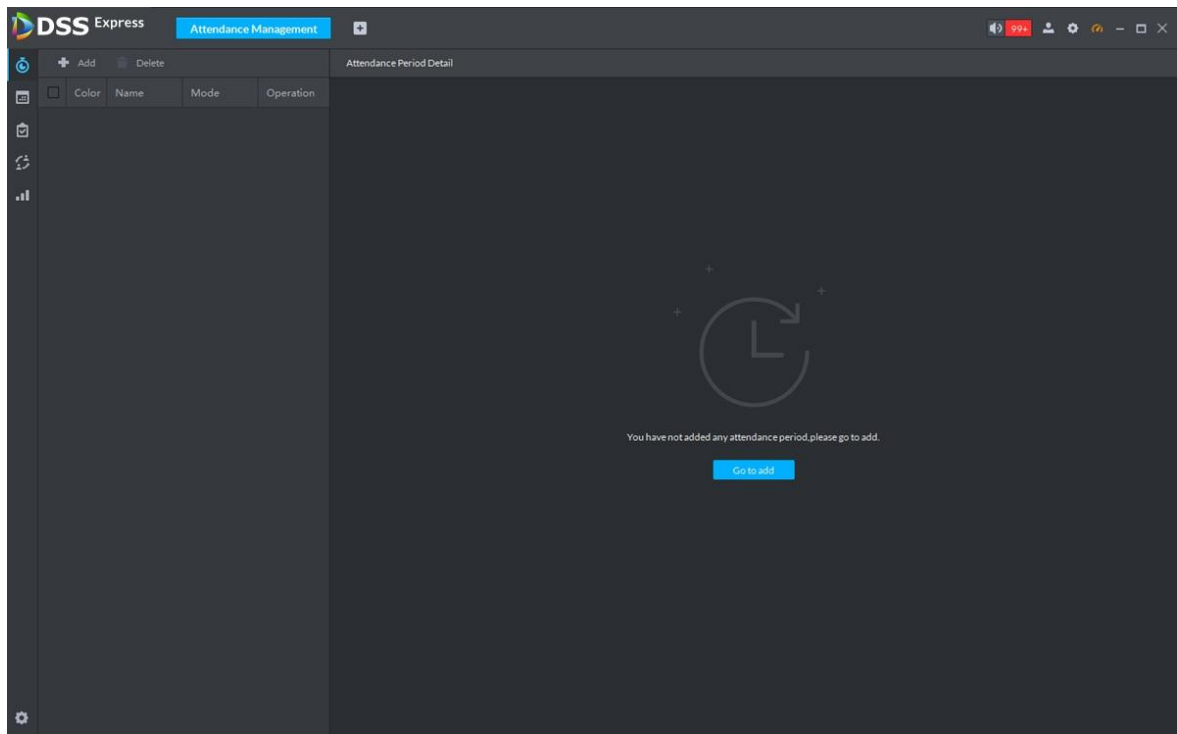
3.16.5 Setting Attendance Period

Set attendance period, which can be used as time evidence to judge if people attend, late or leave early.

Step 1 Click  on the interface of **Attendance Management**.

The interface of **Attendance Management** is displayed. See Figure 3-379.

Figure 3-379 Attendance period



Step 2 Click  on top left corner of the interface.

The new attendance period interface is displayed.

Step 3 Set parameters of attendance period.



The priority of rules set by Pro is higher than that of the device itself.

There are two types of attendance according to different attendance mode and different config.

- Fixed attendance requires you to sign in and sign out within the designated period. For config details, see Figure 3-380 and Figure 3-381. For parameter details, see Table 3-44.

Figure 3-380 Attendance period detail (1)

The screenshot shows the 'Attendance Management' window in DSS Express. On the left is a sidebar with a list of attendance periods. The main area is titled 'Attendance Period Detail'. It contains the following sections:

- Period Name:** A text input field.
- Attendance Mode:** Two buttons: 'Fixed Attendance' (selected) and 'Free Attendance'.
- Color:** A dropdown menu showing 'Red'.
- Attendance Period:** A section with two rows of settings:
 - Working Time:** A warning icon and text 'Span doesn't exceed 24 hours'. Below it, a time range selector set to '09:00 - 17:00' with '(Total duration: 8.0 h)'.
 - Working Hour:** A numeric input set to '8.0'.
 - Valid Sign-in Time:** A time range selector set to '08:00 - 10:00' with a checkbox 'Shall sign in'.
 - Valid Sign-out Time:** A time range selector set to '16:00 - 18:00' with a checkbox 'Shall sign out'.
- Attendance Rule:** A section with three rows of settings:
 - Late sign in:** 'within 5 minutes is permitted, late sign in over 120 minutes is recorded as absence.'
 - Early leave:** 'within 5 minutes is permitted, early sign out over 120 minutes is recorded as absence.'
 - End of Off Duty:** '60 minutes later than off duty time is recorded as overtime.'

At the bottom right are 'Save' and 'Cancel' buttons.

Figure 3-381 Attendance period detail (2)

This screenshot shows the same 'Attendance Period Detail' form as Figure 3-380, but with two identical instances of the 'Attendance Period' settings section stacked vertically. The 'Valid Sign-out Time' checkbox 'Shall sign out' is checked in both instances. The 'Attendance Rule' section remains the same.

Table 3-44 Fixed attendance parameter description

Parameter	Description
Period name	Custom period name, used to recognize period, such as early shift and night shift.
Color	Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly recognize shift information.
Attendance mode	Set as Fixed Attendance .

Parameter	Description
Working time	Set corresponding working hour of period. Attendance time supports cross-day, but not exceeds 24 hours. One attendance period supports max two types of attendance time.  ● If attendance time needs to be split into twice, such as morning and afternoon, then it needs to click , set second working time and sign-in sign-out period. ● If you set two types of attendance time, then it needs to sign in and sign out according to the configured attendance time, which can be considered as normal attendance.
Working hour	Please fill in according to actual situation.
Valid sign-in time	If working time is set from 09:00-18:00, then valid sign-in time can be set as 08:00-10:00, valid sign-out time can be set as 16:00-18:00. Config rules are as follows: ● The start time of valid sign-in time is earlier than or equal to start working time (09:00), the end time of valid sign-in time should be later than start working time (09:00), earlier than start time of valid sign-out time. If there are several sign-in records within valid sign-in time, then the earliest record is considered as sign-in time.
Valid sign-out time	● The start time of valid sign-out time is later than the end time of valid sign-in time, earlier than end working time (18:00), the end sing-in time of valid sign-out time is later than or equal to end working time (18:00). If there are several sign-out records within valid sign-out time, then the earliest record is considered as sign-out time.
Shall sign in	If you set two working time, then the second working time can cancel sign in, you don't have to sign in when you work at the second working time, and the start time of working time can be used as sign-in time.
Shall sign out	If you set two working time, then the first working time can cancel sign in, you don't have to sign out when you finish work at the second working time, and the end time of working time can be used as sign-out time.
Work sign-in over _minutes recorded as late	Define the rules of late, absence and early leave. Suppose set Work sign-in over __minutes recorded as late as 5 minutes; Late sign-in over _minutes recorded as absence is set as 60 minutes; Off duty _ minutes in advance recorded as early leave is set as 10 minutes; Early leave exceeds_ minutes recorded as absebce is set as 30 minutes. Details are as follows.
Late sign-in over _minutes recorded as absence	

Parameter	Description
Off duty_ minutes in advance recorded as early leave	● Late When work sign-in is later than start time of working time, and 5 minutes< period ≤60 minutes, then it is recorded as late.
Early leave exceeds_ minutes recorded as absebce	● Early leave When off duty sign-out time is earlier than end time of working time, and 10 minutes< period ≤30 minutes, then it is recorded as early leave. ● Absence When work sign-in time is later than start time of working time, and period > 60 minutes, then it is recorded as absence. When off duty sign-out time is earlier than end time of working time, and period> 30 minutes, then it is recorded as absence.
Off duty sign-out over_ minutes recorded as overtime	Define overtime rule. Suppose Off duty sign-out over__minutes recorded as overtime is set as 120 minutes, off duty sign-out time is later than end time of working time, and period >120 minutes, then it is recorded as overtime, overtime period is Period – 120 minutes.

- Free Attendance, you are required to sign in and sign out within the specific period. See Figure 3-382. For parameter details, see Table 3-45.

Figure 3-382 Free attendance

The screenshot shows the 'Attendance Management' window in DSS Express. The 'Attendance Period Detail' panel is active, displaying the following configuration:

- Period Name:** (Empty text field)
- Attendance Mode:** 'Fixed Attendance' and 'Free Attendance' buttons are present; 'Free Attendance' is selected.
- Color:** A dropdown menu showing 'Red'.
- Attendance Rule:**
 - System:** 'Hour System' (selected)
 - Limit:** 'the final punch in time' (selected), with a time value of '08:00'.
 - Marked as:** 'Working Hour' (selected)
 - Final Punch out Time:** '23:59' (selected)
 - Overtime:** (Unchecked checkbox)
 - Odd In and Even Out:** (Unchecked checkbox, with a note: 'sign-in at odd number of swiping card, and sign-out at even number of swiping card')

At the bottom right, there are 'Save' and 'Cancel' buttons.

Table 3-45 Free attendance parameter description

Parameter	Description
Period name	Custom period name, used to recognize period, such as flexible attendance.
Attendance mode	Set as Free Attendance .

Parameter	Description
Color	Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly recognize shift information.
Hour system	Set how many hours you have to work a day. For example, if you set 8, then it means you are required to work 8 hours.
Final punch in time	Set if it restricts latest punch in time; sign in after restricted time is recorded as late.
Mark as_working hour	Fill in working hour according to actual situation.
Final punch out time	You are required to sign out before the designated time, otherwise no sign out is recorded.
Overtime	Working over__ hours is recorded as overtime. For example, working hour is 8 hours a day, and if you work overtime for 2.5 hours, then it is recorded as overtime, then you can set 10.5 here.
Work over_hours recorded as overtime	
Odd in even out	
Continuous twice card swiping interval≥_minutes	Swipe card at odd number is recorded as sign in. For example, the first card swiping is sign in. Swipe card at even number is recorded as sign out. For example, the second card swiping is sign out. It is recorded as twice punch card when the interval of continuous twice card swiping is bigger than the threshold.

Step 4 Click **Save** and save period config.



If attendance period is already applied to attendance shift, then before deleting attendance period, first enter the interface of **Attendance Shift**, modify attendance shift, and delete attendance period before removing application of the attendance period.

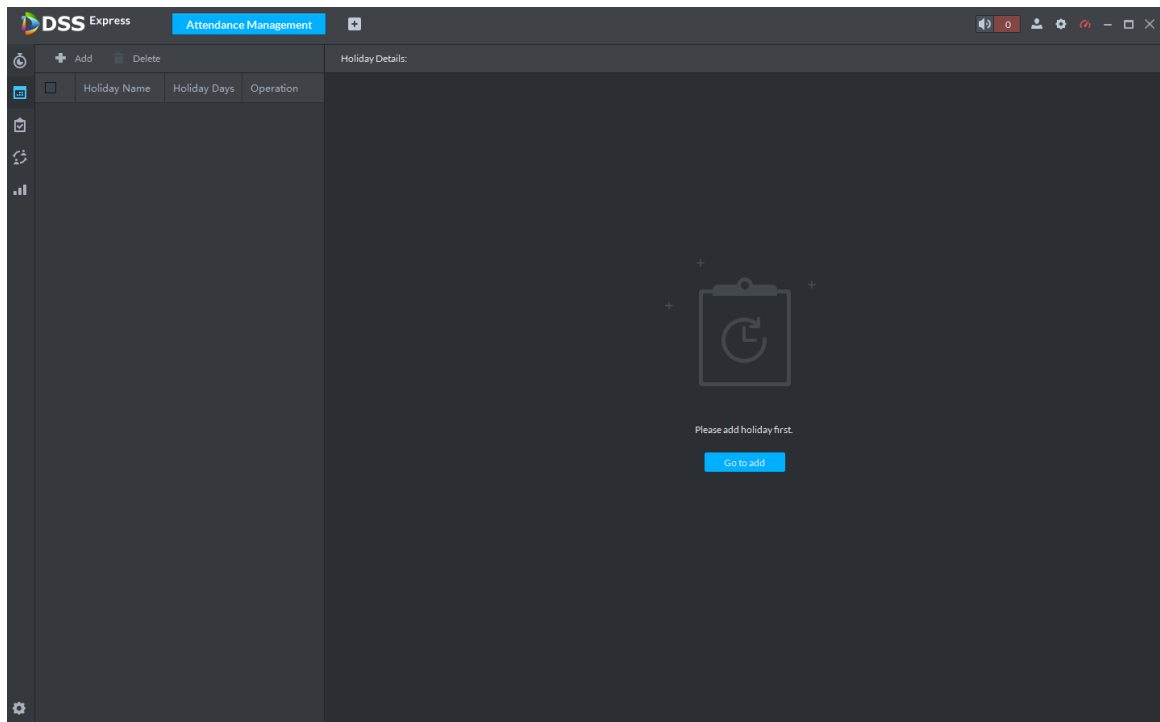
3.16.6 Setting Holiday

Set holiday time, used to judge overtime type during attendance statistics.

Step 1 Click  on the interface of **Attendance Management**.

The interface of **Holiday Management** is displayed. See Figure 3-383.

Figure 3-383 Holiday management



Step 2 Click  on the upper left corner of the interface.
The add holiday interface is displayed. See Figure 3-384.

Figure 3-384 Add holiday

Step 3 Set holiday details, three modes available. See Table 3-46 for more parameter details.

Table 3-46 Holiday mode description

Holiday mode	Description
Fixed Date	Set some specific date as holiday. For example, set June 7, 2019 (Dragon Boat Festival) as holiday, and lasts for 1 day, then set

Holiday mode	Description
	Start Date as June 7, 2019 and Holiday Days as 1.
Date Cycle	If the holiday is the fixed weekday of some week in some specific month, and it cycles according to year, which can be configured as data cycle. For example, if you want to set Mother's Day as holiday, and it lasts for 1 day, then you can set Start Date as the second Sunday in May, and Holiday Days as 1.
Year Cycle	If the holiday is fixed date and it cycles according to year, which can be configured as year cycle. For example, set New Year's Day as holiday, and it lasts for 1 day, then you can set Start Date as January 1 and Holiday Days as 1.

Step 4 Click **Save**.

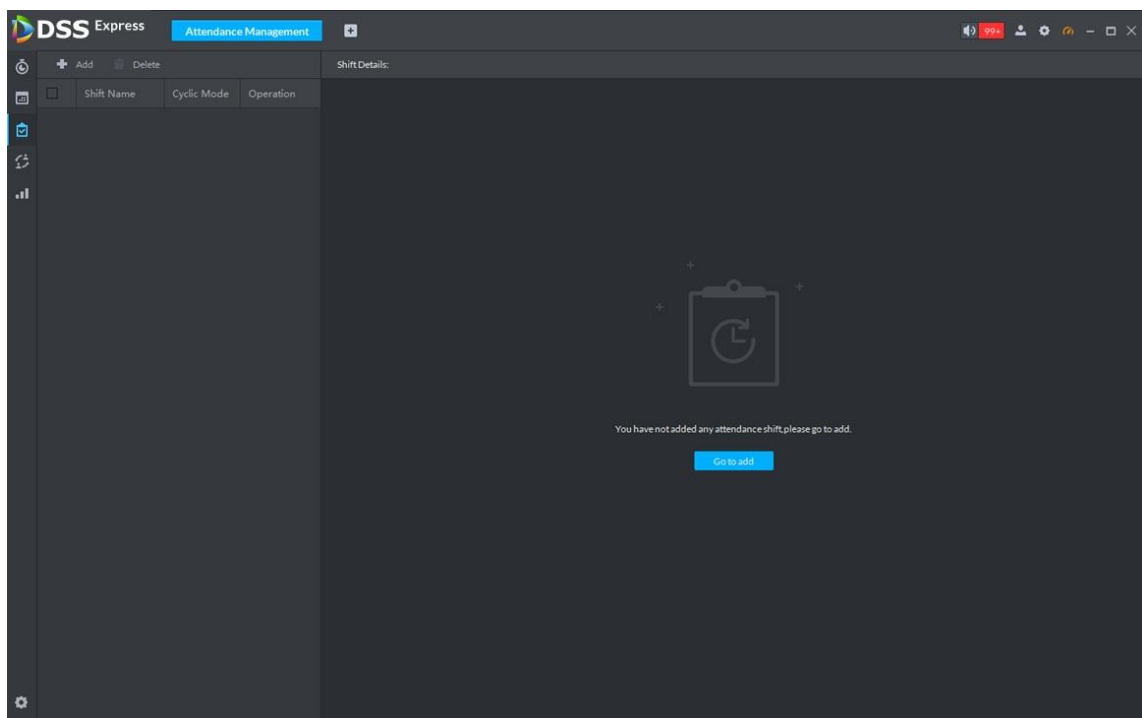
3.16.7 Setting Attendance Shift

Set attendance shift according to attendance period, used for department and personnel shift.

Step 1 Click  on the interface of **Attendance Management**.

The interface of **Attendance Shift** is displayed. See Figure 3-385.

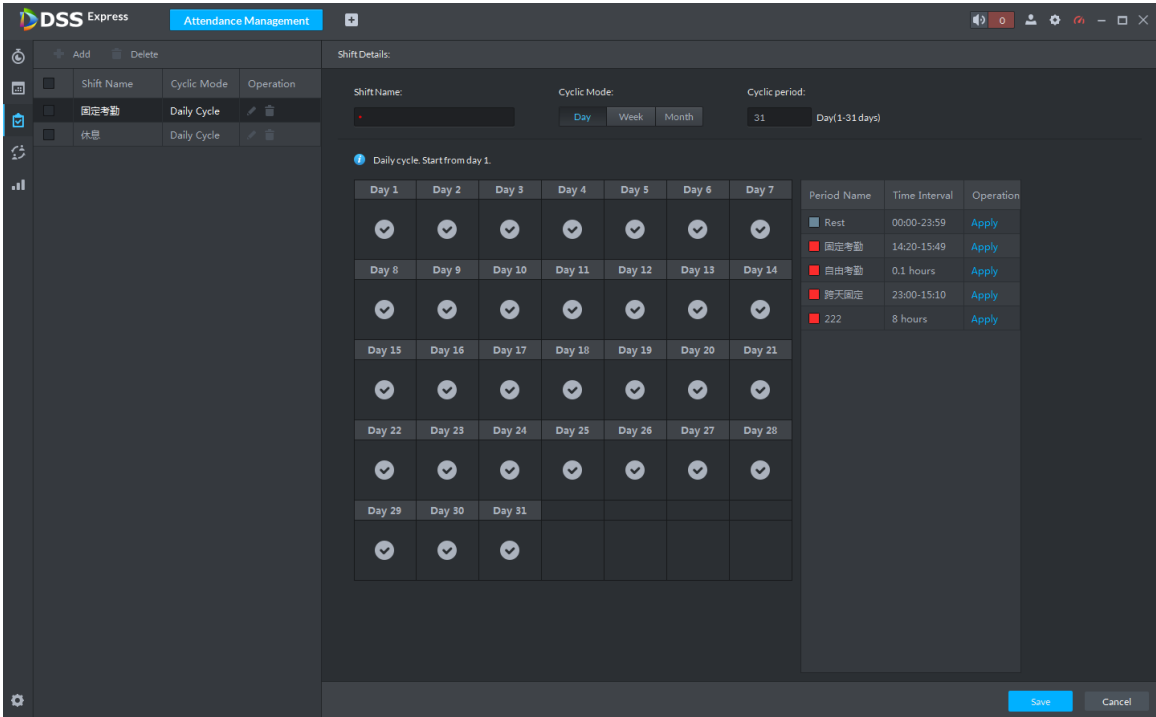
Figure 3-385 Attendance shift



Step 2 Click  on the top left corner of the interface.

The add attendance shift interface is displayed. See Figure 3-386.

Figure 3-386 Set attendance shift (1)



Step 3 Set shift details, select date, click Apply and arrange attendance period for date. See Figure 3-387. For parameter details, see Table 3-47.



Press the left mouse button and drag it on the date display area, you can select several dates quickly.  means that the date is selected.

Figure 3-387 Set attendance shift (2)

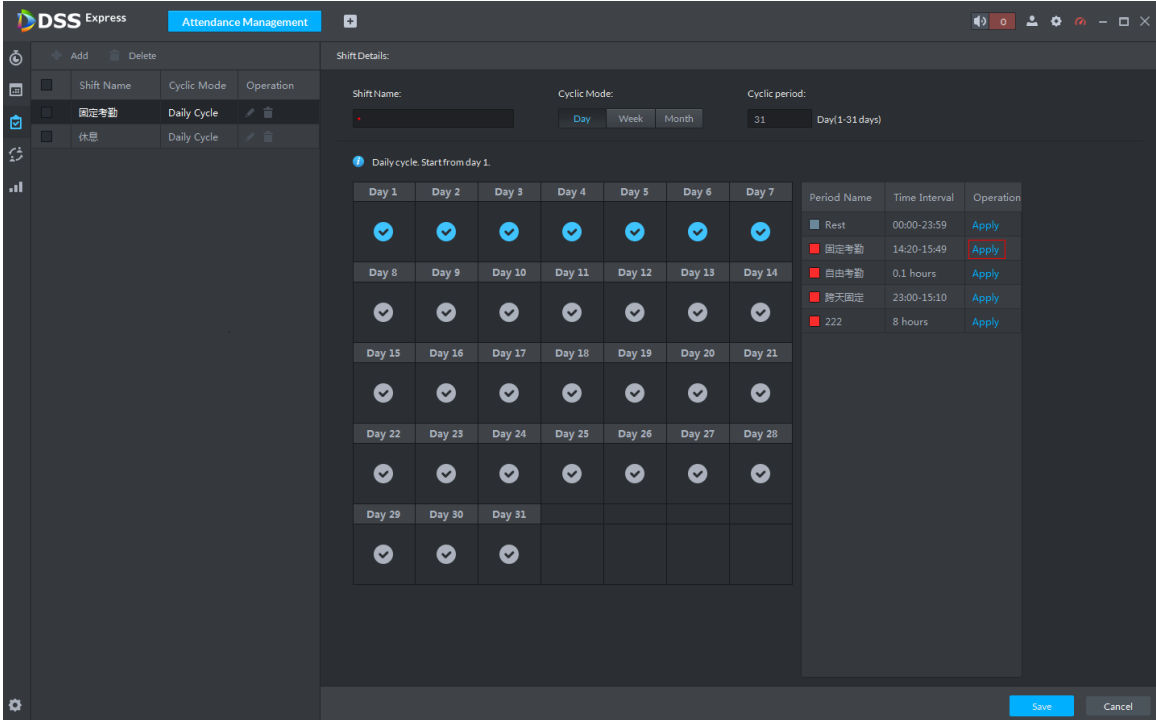


Table 3-47 Attendance shift parameter description

Parameter	Note
-----------	------

Parameter	Note
Shift name	Custom period name, used to recognize shift.
Cycle mode	Day: Start cycle from the first day, cycle period can be set as any number from 1 to 31 according to day. For example, if you set 2, then the cycle period is 2 days. Week: There are 7 days in a week by default, it starts cycle from Sunday, and so Sunday is required to be set as the first day. Cycle period can be set as any number from 1 to 4. For example, if you set 2, then 2 weeks can be a cycle period.
Cycle period	Month: There are 31 days in a month by default, it starts cycle from the current day (If the date does not exist, then it will be deleted during shift arrangement), cycle period can be set as any number from 1 to 3 according to month. For example, if you set 2, then 2 months can be a cycle period.

Step 4 Click **Save** to save shift config.



Delete in-use attendance shift: Enter the interface of **Personnel Shift Arrangement**, check if there are shifts need to be deleted for all personnel shifts, please delete after remove the relation.

3.16.8 Shift Management

Make shifts for personnel or department, meanwhile it makes temporary shift for personnel. The shift priority is temporary shift > holiday > personnel shift > department shift.

3.16.8.1 Personnel/Department Shift Arrangement

The operations over both personnel shift and department shift are similar, in this chapter; it takes personnel shift as an example to introduce config.

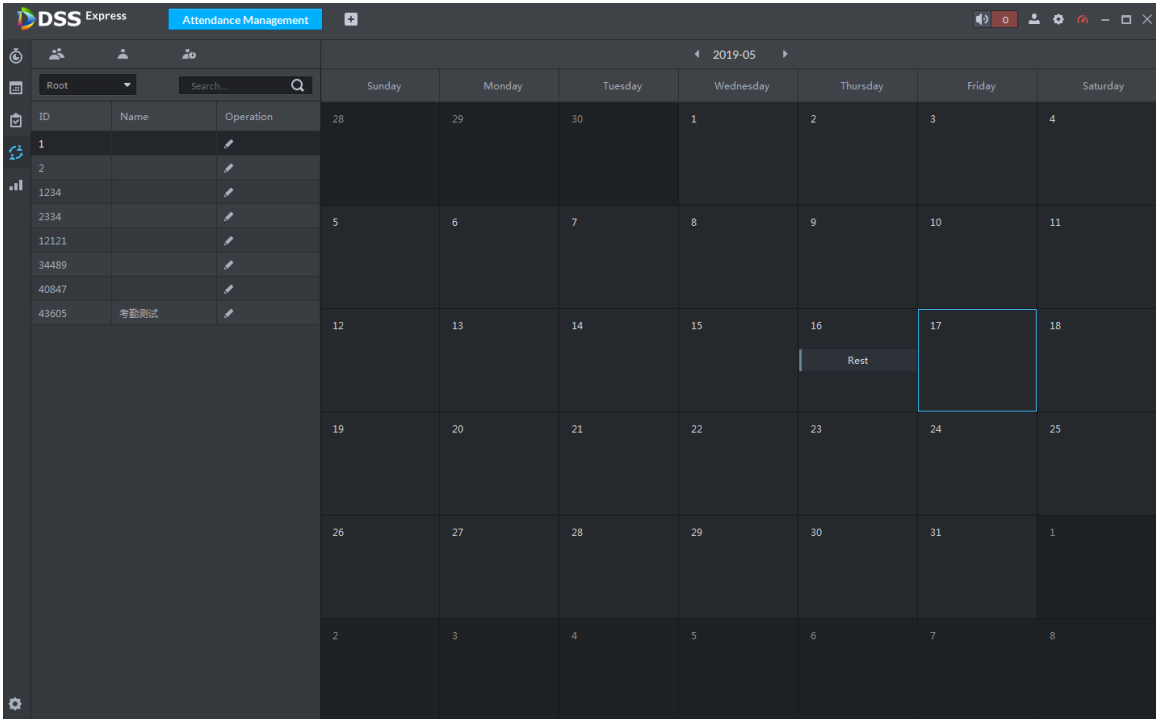


- If you configure department shift, then all the personnel of the department need to conform to the shift.
- If both personnel and department are configured with shift, then the latest personnel shift shall prevail. For example, after configuring the personnel shift, and the corresponding department is configured as well, then personnel shift is based on the latest department shift.
- If the department where new personnel belong is configured with shift, then the shift of new personnel should conform to department shift.

Step 1 Click  on the interface of **Attendance Management**.

The interface of **Personnel Shift Arrangement** is displayed. See Figure 3-388

Figure 3-388 Personnel shift arrangement



Step 2 Click  on the top left corner of the interface.

The interface of **Personnel Shift Arrangement** is displayed. See Figure 3-389.



- If you need to configure shift for department, click  on the top left corner and enter the interface of department shift arrangement. The following operation is the same as personnel shift arrangement.
- On the interface of personnel shift arrangement, select personnel and view the shift situation.
- Click  next to the personnel and you can view the shift details.

Figure 3-389 Personnel shift arrangement

Personnel Shift Arrangement

Root

Search...

	ID	Name
☐	123	
☐	33333	kuanggong
☐	36545	
☐	36546	
☐	44444	chidaotaotui
☐	55555	kuanggggg
☐	123456	ttt tt
☐	222222	zaotui
☐	1111111	chidao
☐	1243213	
☐	3333336	111 111

Select Shift

+ Add

🗑 Clean

Start Time	End Time	Shift	Operation
------------	----------	-------	-----------

Save

Cancel

Step 3 Select shift personnel, click  to add shift info. See Figure 3-390. For parameter details, see Table 3-48.

Figure 3-390 Select shift

Personnel Shift Arrangement

Root

Search...

	ID	Name
☒	123	
☒	33333	kuanggong
☒	36545	
☒	36546	
☐	44444	chidaotaotui
☐	55555	kuanggggg
☐	123456	ttt tt
☐	222222	zaotui
☐	1111111	chidao
☐	1243213	
☐	3333336	111 111

Select Shift

+ Add

🗑 Clean

Start Time	End Time	Shift	Operation
2019-03-28	2019-03-28		🗑

Save

Cancel

Table 3-48 Shift parameter description

Parameter	Note
Start time	Set start date and end date of personnel shift. Click the

Parameter	Note
End time	column of Start Time and display calendar, select date and time, and then click OK to complete date setting
Shift	Select needed shifts. Shift range means all the attendance shifts set in 3.16.7 Setting Attendance Shift

Step 4 Click **Save** to save personnel shift information.

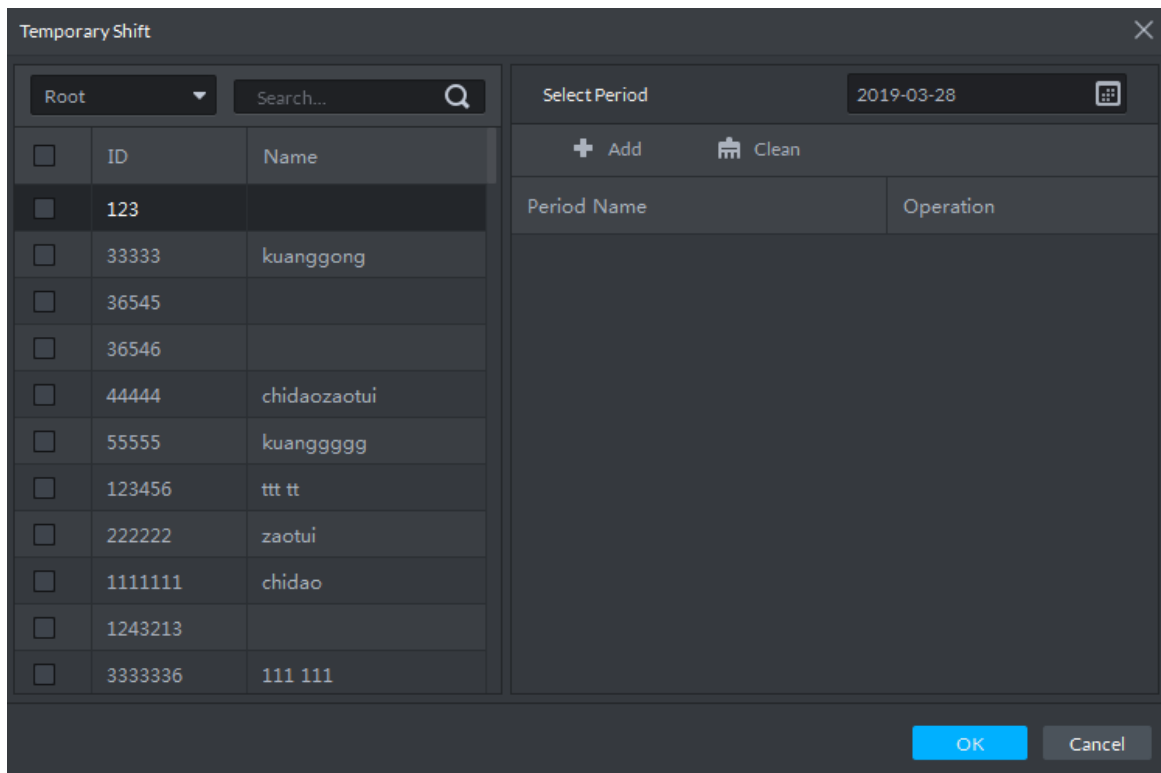
3.16.8.2 Temporary Shift

Temporary shift is needed when work changes temporarily.

Step 1 Click  on the interface of Attendance Management or select personnel on the right, double click date on the left.

The interface of Temporary Shift is displayed. See Figure 3-391.

Figure 3-391 Temporary shift



ID	Name
123	
33333	kuanggong
36545	
36546	
44444	chidaorzaotui
55555	kuanggggg
123456	ttt tt
222222	zaotui
1111111	chidao
1243213	
3333336	111 111

Step 2 Select personnel and date, click  and select temporary attendance period. See Figure 3-392. You can add max 2 attendance periods and 1 free attendance period.

Figure 3-392 Temporary shift

ID	Name
123	
33333	kuanggong
36545	
36546	
44444	chidaotaotui
55555	kuanggggg
123456	ttt tt
222222	zaotui
1111111	chidao
1243213	
3333336	111 111

Step 3 Click **OK** and save shift information.



Temporary shift can be deleted, right click the date which is configured with temporary shift, and delete temporary shift according to system prompt.

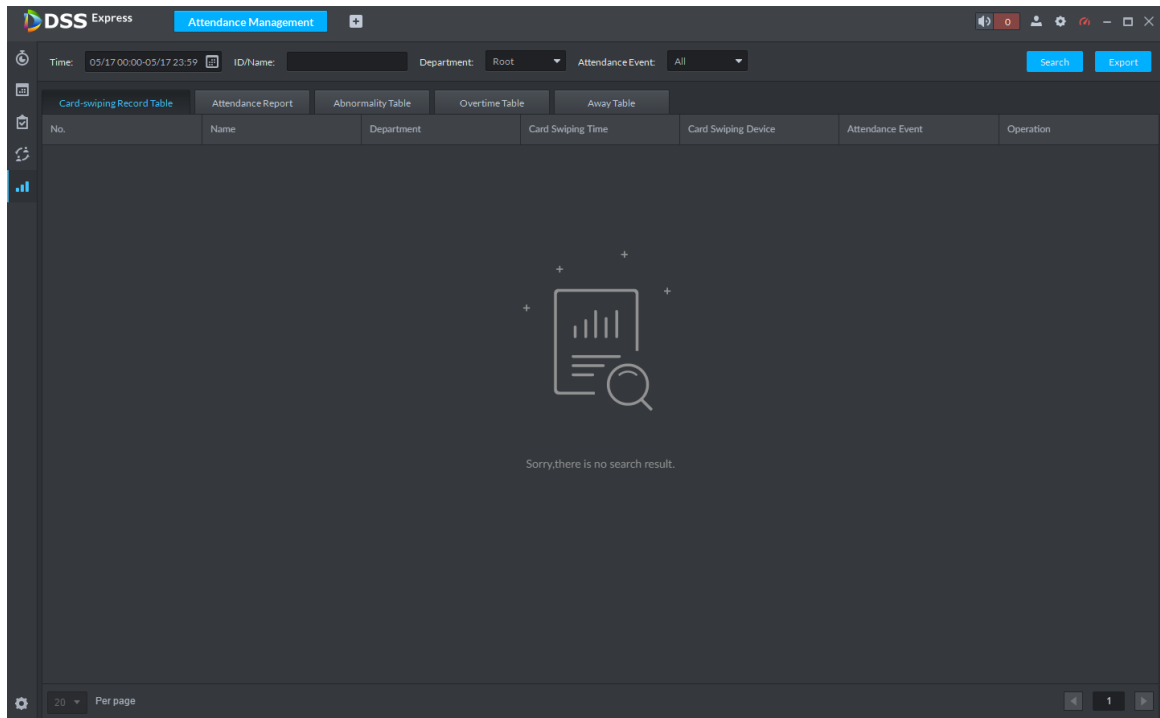
3.16.9 Viewing Attendance Report

View attendance data, displayed in the form of report, including card swiping record table, attendance report, abnormality table, overtime table and away table.

Step 1 Click  on the interface of **Attendance Management**.

The interface of **Attendance Report** is displayed. See Figure 3-393.

Figure 3-393 Attendance report



Step 2 Click corresponding tab, set search condition, click **Search**.

The search result is displayed, exported by excel and saved locally, it can export up to 10,000 records.

- Card swiping record table is shown in Figure 3-394. Click  and view more details of the person who swipes card.

Figure 3-394 Card-swiping record table

The screenshot shows the DSS Express Attendance Management interface with the 'Card-swiping Record Table' selected. The table displays a list of records with columns: 'No.', 'Name', 'Department', 'Card Swiping Time', 'Card Swiping Device', 'Attendance Event', and 'Operation'. The records are as follows:

No.	Name	Department	Card Swiping Time	Card Swiping Device	Attendance Event	Operation
43605	[icon]	org1	2019-05-16 19:50:55	10.35.93.228		
43605	[icon]	org1	2019-05-16 19:50:28	10.35.93.228		
43605	[icon]	org1	2019-05-16 19:50:23	10.35.93.228	Back	
43605	[icon]	org1	2019-05-16 19:27:35	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 19:26:32	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 19:24:38	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 19:23:57	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 17:16:40	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 17:16:40	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 17:15:42	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 17:15:42	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 17:15:38	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 17:15:38	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 17:14:29	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 17:14:29	10.35.93.228	Punch out	
11233	[icon]	org1	2019-05-16 16:58:59	10.33.68.86	Punch in	
12345	[icon]	org1	2019-05-16 16:53:05	10.33.68.86		
43605	[icon]	org1	2019-05-16 16:52:32	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 16:52:32	10.35.93.228	Punch out	
43605	[icon]	org1	2019-05-16 16:45:43	10.35.93.228	Punch out	

- See Figure 3-395 for attendance report.

Figure 3-395 Attendance report

The screenshot shows the 'Attendance Management' interface in DSS Express. The 'Attendance Report' tab is selected. The table displays attendance records for four dates in May 2019. The columns include Date, No., Name, Department, Sign-in Time, Sign-out Time, Week, Away Duration, Working Period, and Overtime Duration.

Date	No.	Name	Department	Sign-in Time	Sign-out Time	Week	Away Duration	Working Period	Overtime Duration
2019-05-16	43605	[REDACTED]	Root	14:29	14:44	Thursday	0.0 Hour(s)	0.3 Hour(s)	0.0 Hour(s)
2019-05-16	43605	[REDACTED]	org1	14:47	19:50	Thursday	4.8 Hour(s)	4.7 Hour(s)	4.5 Hour(s)
2019-05-16	34489	[REDACTED]	Root	16:09	16:09	Thursday	0.0 Hour(s)	0.0 Hour(s)	0.0 Hour(s)
2019-05-16	12345	[REDACTED]	org1	16:53		Thursday	0.0 Hour(s)	0.0 Hour(s)	0.0 Hour(s)
2019-05-16	11233	[REDACTED]	org1	16:58		Thursday	0.0 Hour(s)	0.0 Hour(s)	0.0 Hour(s)

- See Figure 3-396 for abnormality table.

Figure 3-396 Abnormity table

The screenshot shows the 'Attendance Management' interface in DSS Express. The 'Abnormality Table' tab is selected. The table displays abnormality records for one date in May 2019. The columns include Date, No., Name, Department, Sign-in Time, Sign-out Time, and Abnormal Type.

Date	No.	Name	Department	Sign-in Time	Sign-out Time	Abnormal Type
2019-05-16	43605	[REDACTED]	Root	14:29	14:44	Late and Leave Early

- See Figure 3-397 for overtime table.

Figure 3-397 Overtime table

Date	Name	No.	Department	Overtime Type	Overtime Duration
2019-05-16	[REDACTED]	43605	org1	General	4.5 Hour(s)

- See Figure 3-398 for away table.

Figure 3-398 Away table

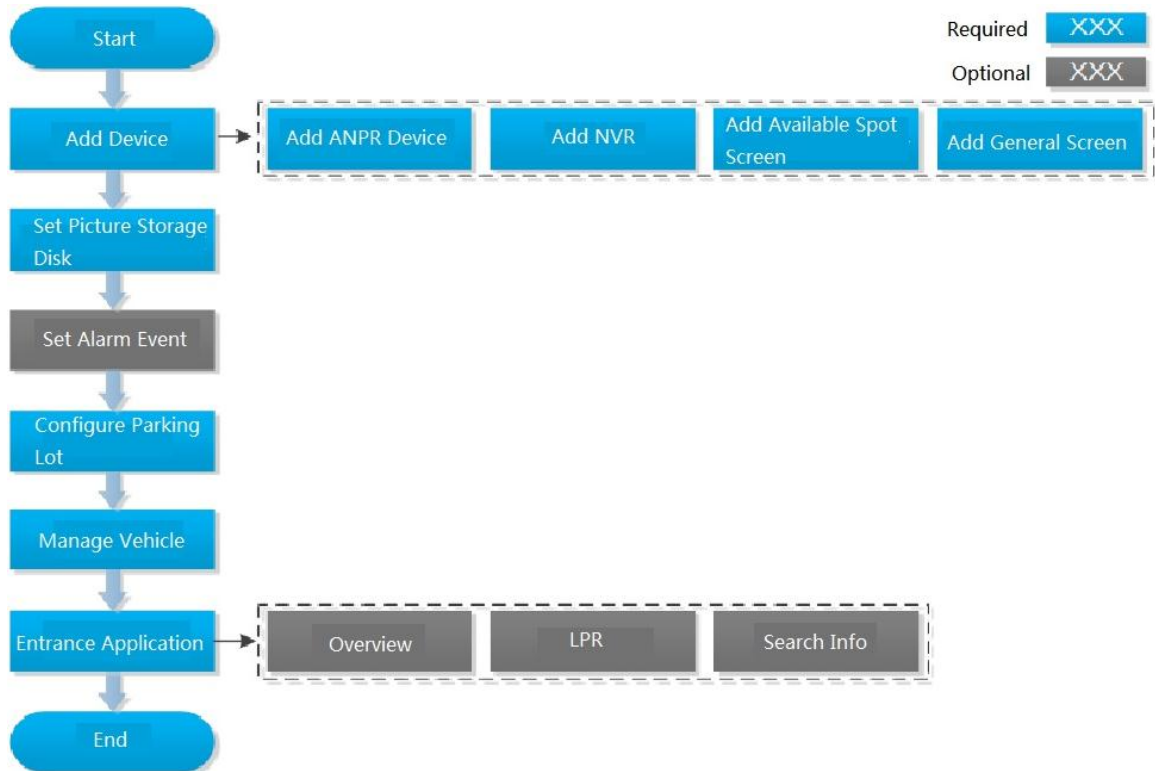
Date	No.	Name	Department	Card Number	Leave Time	Return Time	Away Duration
2019-05-16	43605	[REDACTED]	org1	0022C5A9	14:57	14:59	0.0 Hour(s)
2019-05-16	43605	[REDACTED]	org1	0022C5A9	14:55	14:56	0.0 Hour(s)
2019-05-16	43605	[REDACTED]	org1	0022C5A9	14:52	14:53	0.0 Hour(s)
2019-05-16	43605	[REDACTED]	Root	0022C5A9	14:50	14:51	0.0 Hour(s)
2019-05-16	43605	[REDACTED]	Root	0022C5A9	14:48	14:49	0.0 Hour(s)

3.17 Entrance

Integrate entrance module, realize entrance and exit recognition barrier unlock, remaining parking space info 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. The entrance operation flow is shown in Figure 3-399.

Figure 3-399 Entrance operation flow



3.17.1 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.

3.17.1.1 Adding ANPR Camera

ANPR device is used to recognize license plate and vehicle info.



- 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 **3.2.2.4 Adding Device**
Modify device type.

- 1) On the **Device** interface of Web, click  of added ANPR device. See Figure 3-400. The device displays the interface of Edit Device. See Figure 3-401.

Figure 3-400 Enter ANPR device

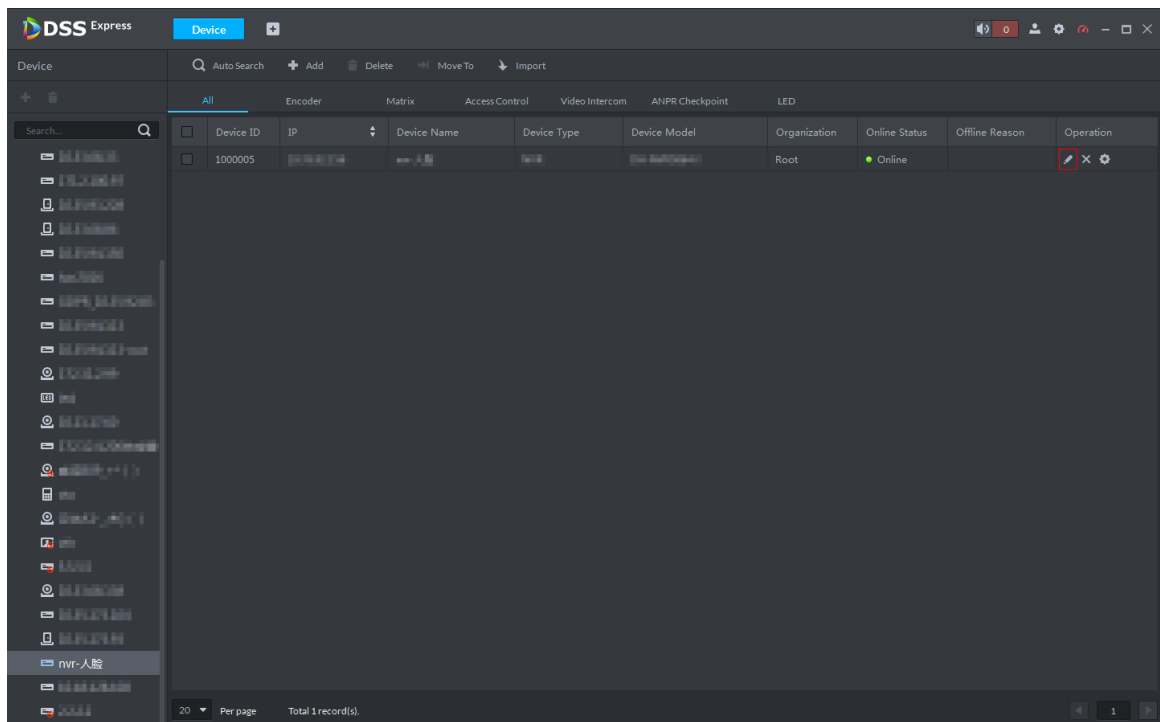
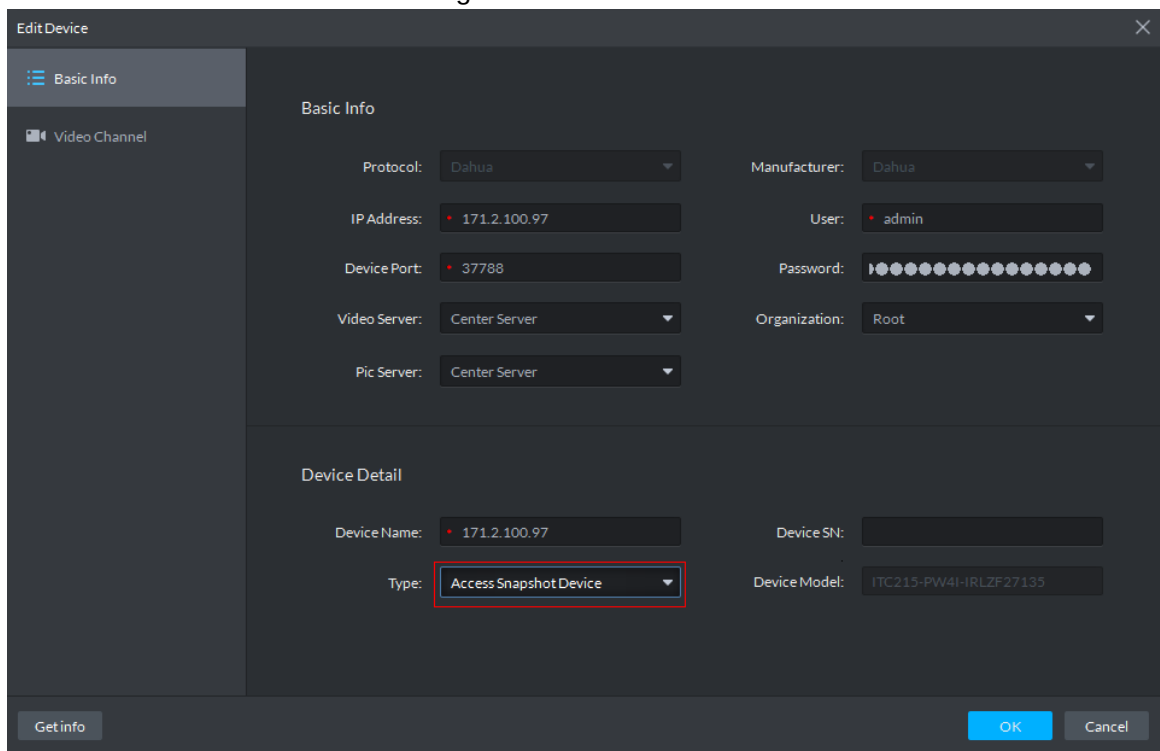


Figure 3-401 Edit device



- 2) Set Type as Access Snapshot Device.
- 3) Click OK and complete config.

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) On client homepage, click **Config**.
The system displays **Config** interface.

- 2) In left device tree, select access control channel, click **Bind Resource**, and see Figure 3-402.

Figure 3-402 Enter resource bind interface

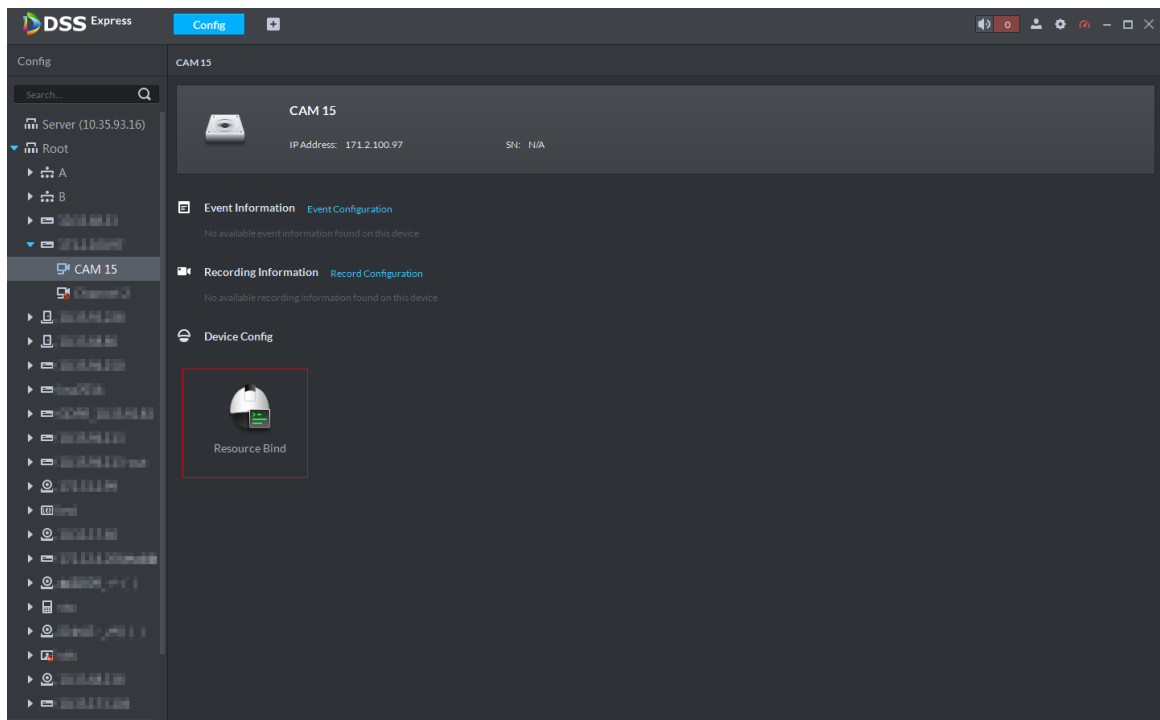
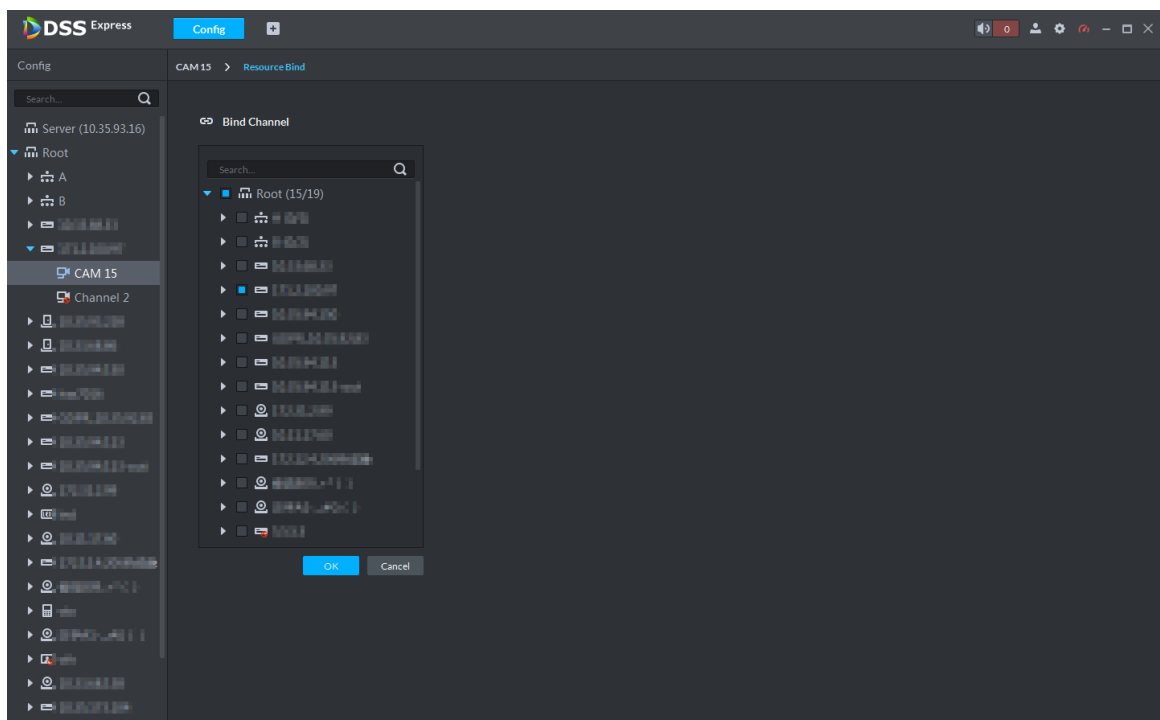


Figure 3-403 Resource bind



- 3) Select bound panoramic camera.
- 4) Click **OK** and complete config.

3.17.1.2 Adding NVR

NVR is used to connect ANPR and DSS Express, 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 **3.2.2.4 Adding Device**.

Step 2 Modify device capacity set.

- 1) Click  of added NVR on the **Device** interface on Web. See Figure 3-404.

The system displays the interface of **Edit Device**. See Figure 3-405.

Figure 3-404 Enter encoder edit interface

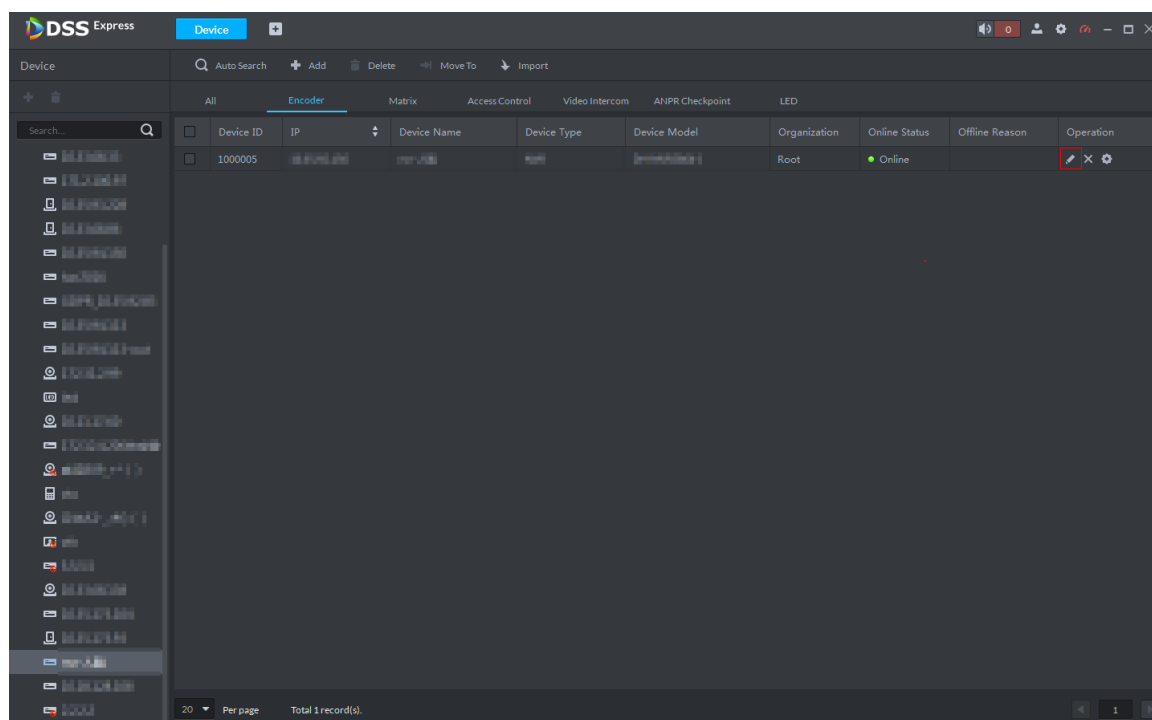
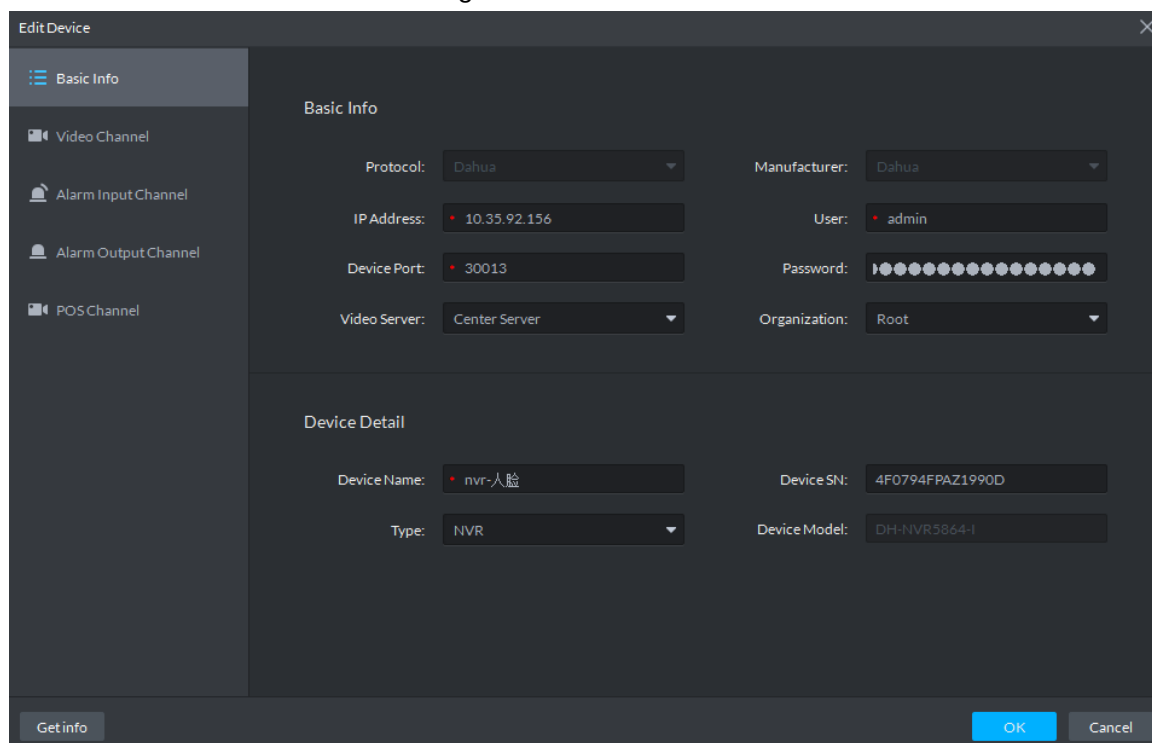


Figure 3-405 Edit device



- 2) Click the tab of **Video Channel**, set **Features** as **Access Snapshot**. See Figure 3-406.

The feature of all the bound ANPR device channel is set as **Access Snapshot**.

Figure 3-406 Modify features

Name	Camera Type	Features	SN	KeyBoard Code
[Name]	[Camera Type]	Access Snapshot		
[Name]	[Camera Type]	Access Snapshot		
[Name]	[Camera Type]	Access Snapshot		
[Name]	[Camera Type]	Access Snapshot		
[Name]	[Camera Type]	Access Snapshot		
[Name]	[Camera Type]	Access Snapshot		
[Name]	[Camera Type]	Access Snapshot		

- 3) Click **OK** and complete config.

3.17.1.3 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. Currently the supported brands of remaining parking screen include Dahua and Jiuzhou.



- 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 **3.2.2.4 Adding Device**.

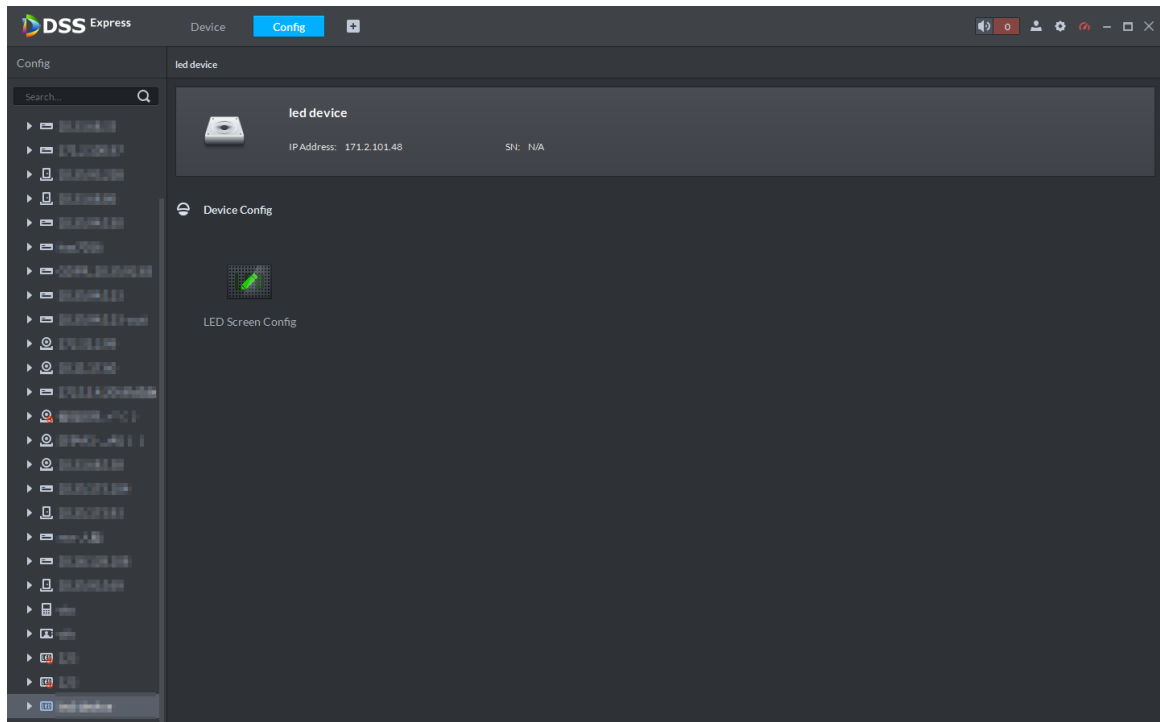
Step 2 On client homepage, click **Config**.

The system displays **Config** interface.

Step 3 Select remaining parking screen from left device list.

The system displays **LED Screen Config** button. See Figure 3-407.

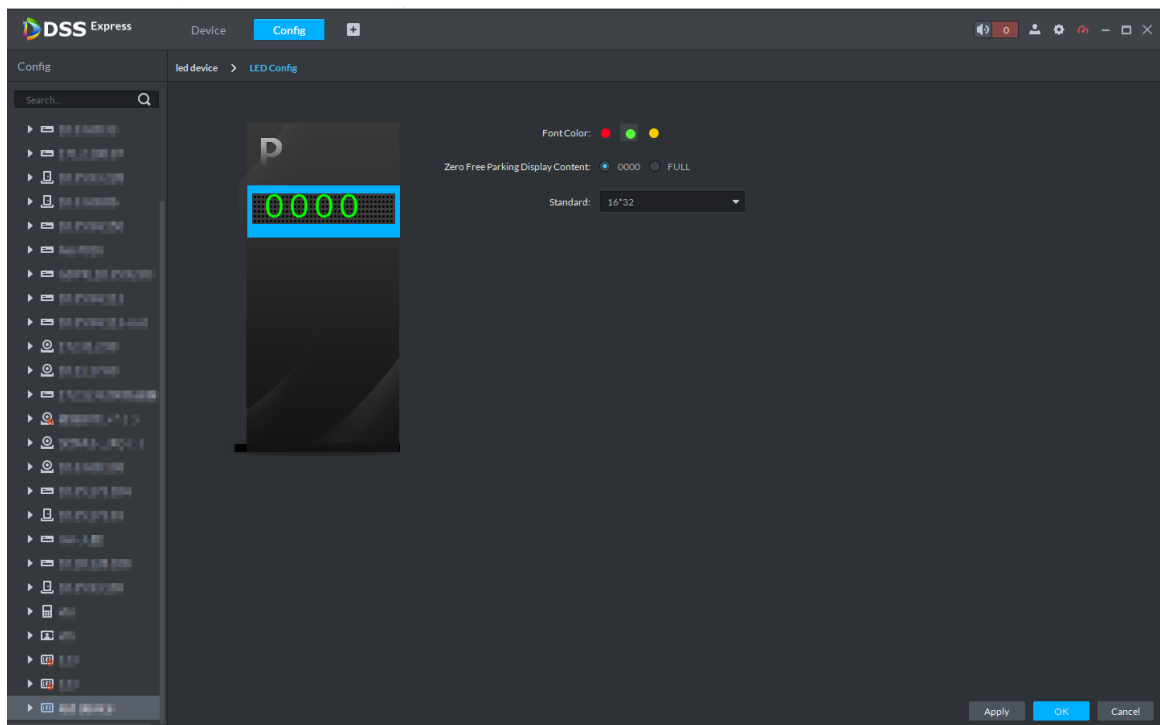
Figure 3-407 LED screen config



Step 4 Click **LED Screen Config**.

The system displays **LED Config** interface, see Figure 3-408.

Figure 3-408 LED config



Step 5 You can set **Font Color** and **Zero Free Parking Display Content**. See Figure 3-408. 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.

Step 6 Click **OK** to complete config.

3.17.1.4 Adding Common Screen

Add common screen and display vehicle info. Currently the platform supports Jezetek common screen.



- Please make sure common screen is configured before adding, such as modifying IP address.
- Common screen is categorized as **LED Device**.

Step 1 Add common screen, for more details. See **3.2.2.4 Adding Device**.

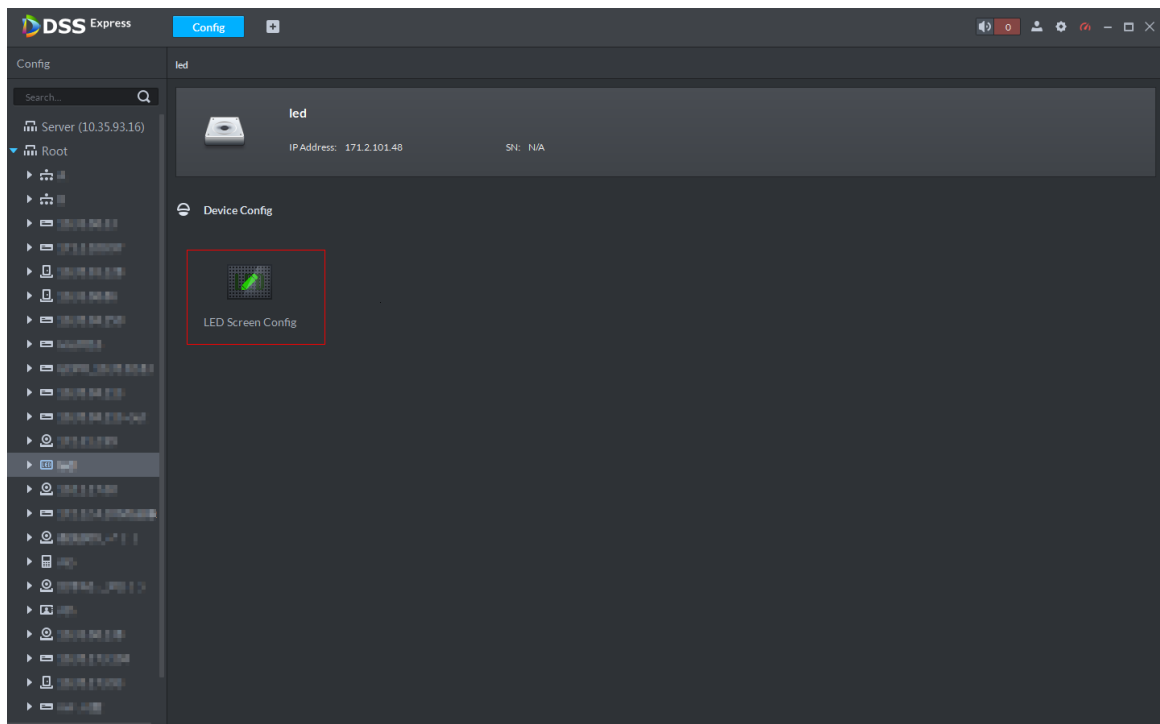
Step 2 On client homepage, click **Config**.

The system displays **Config** interface.

Step 3 Select common screen from left device list.

The system displays the button of **LED Screen Config**.

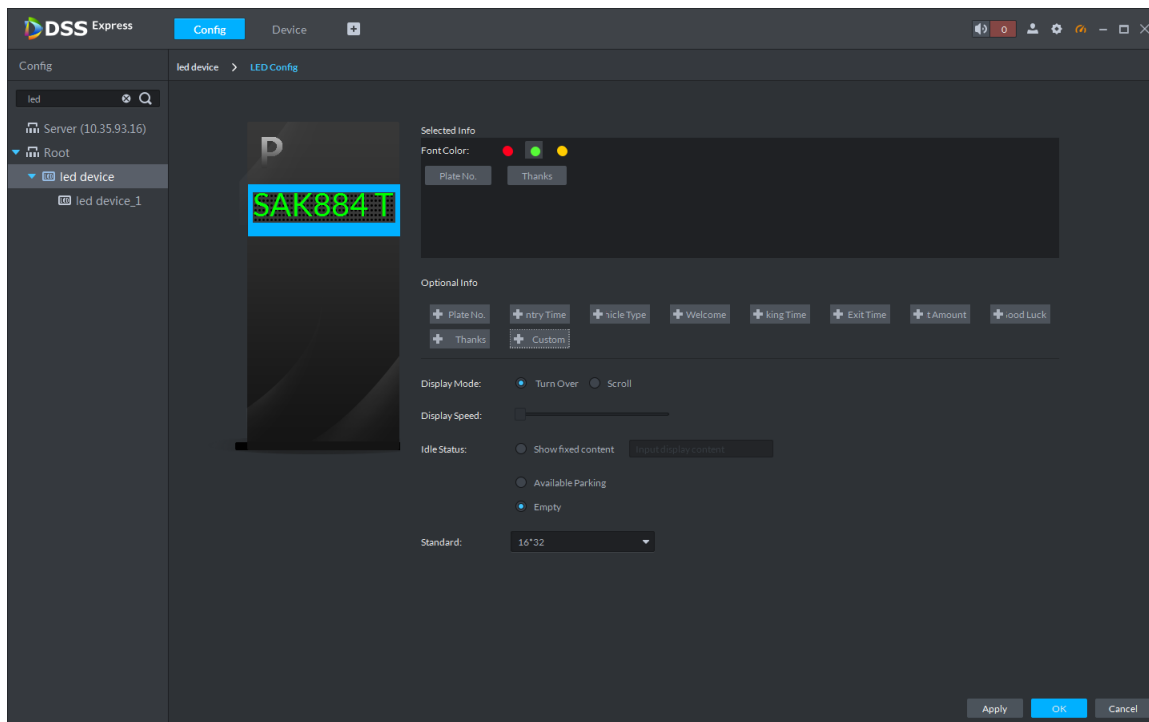
Figure 3-409



Step 4 Click **LED Screen Config**.

The system displays **LED Screen Config** interface, see Figure 3-410.

Figure 3-410 LED config



Step 5 Set font color and info content, select display mode, display speed and show fixed content during idle status.

Step 6 Click **OK** and complete config.

3.17.2 Setting Picture Storage Disk

Configure local storage disk, you must reserve an ANPR picture disk to store ANPR snapshots, otherwise, snapshots cannot be stored or displayed. For more details, see **3.2.1.4 Setting Storage Space**.

3.17.3 Setting Alarm Event

This chapter introduces entrance alarm, for more alarm events and details, refer to **3.2.4 Setting Alarm Event**. Entrance alarms include following types.

- **LPR (License plate recognition)**
After license plate is recognized by ANPR, reported to platform by NVR, the platform triggers alarm, and extract video before and after license plate recognition, saved into platform. The default video duration is 20s, 10s before and 10s after alarm is triggered.
- **Blocked list alarm**
The platform supports marking some plate number as blocked list vehicle, meanwhile, compare the recognized plate number with blocked plated number, if it is the blocked plated number, then alarm is triggered.

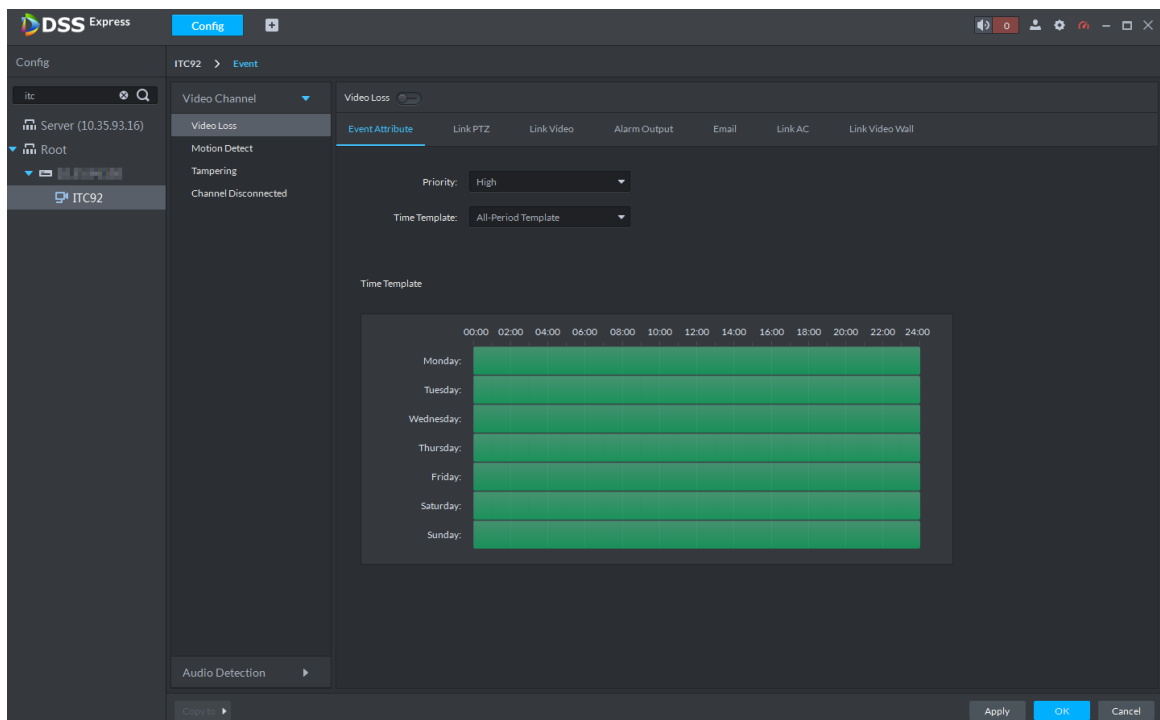


If you want to mark some plate number as blocked plate number, see **3.17.5 Vehicle Management**

- **Parking timeout**
The parking duration exceeds the threshold, and then alarm is triggered.

Set alarm events, see Figure 3-411.

Figure 3-411 Alarm event



3.17.4 Configuring Parking Lot

Generally one parking lot is considered as an area. Parking lot config 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.

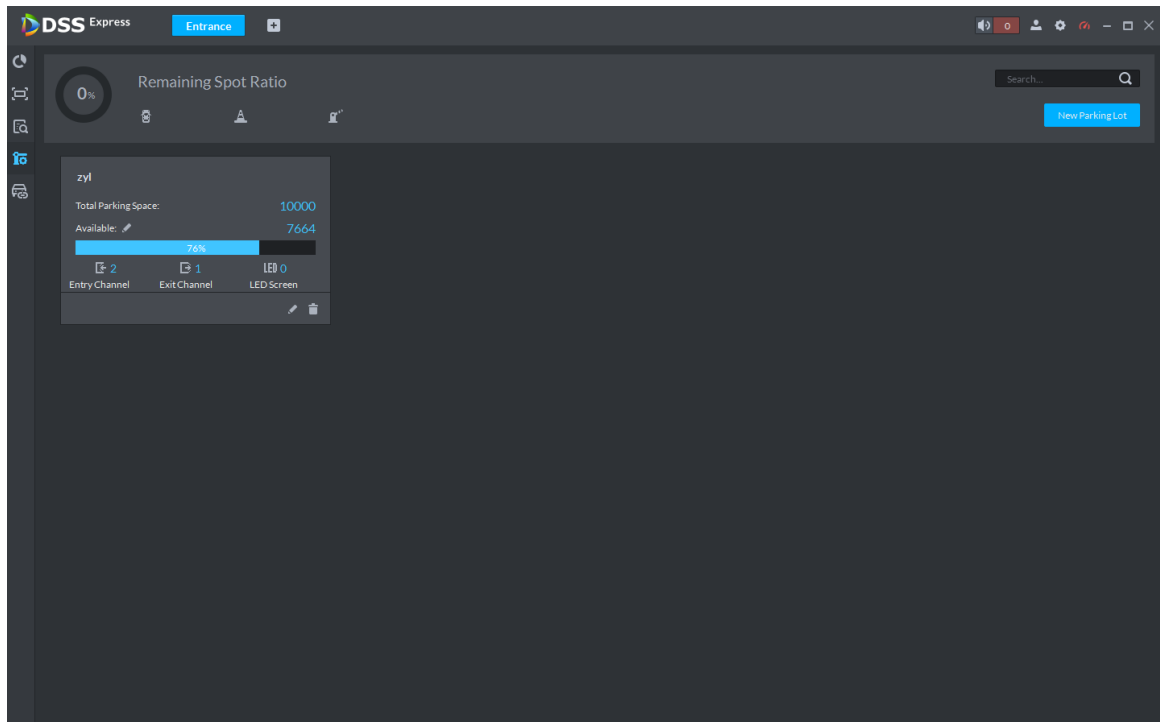
Step 1 On client homepage, click **Entrance**.

The system displays the interface of **Entrance**.

Step 2 Click .

The system displays the interface of **Parking Lot Config**. See Figure 3-412.

Figure 3-412 Parking lot info



Step 3 Add parking lot.

- 1) Click New Parking Lot.

The system displays interface of new parking lot, see Figure 3-413.

Figure 3-413 Add parking lot

- 2) Configure parking lot info. For more parameter details, see Table 3-49.

Table 3-49 Parking lot info

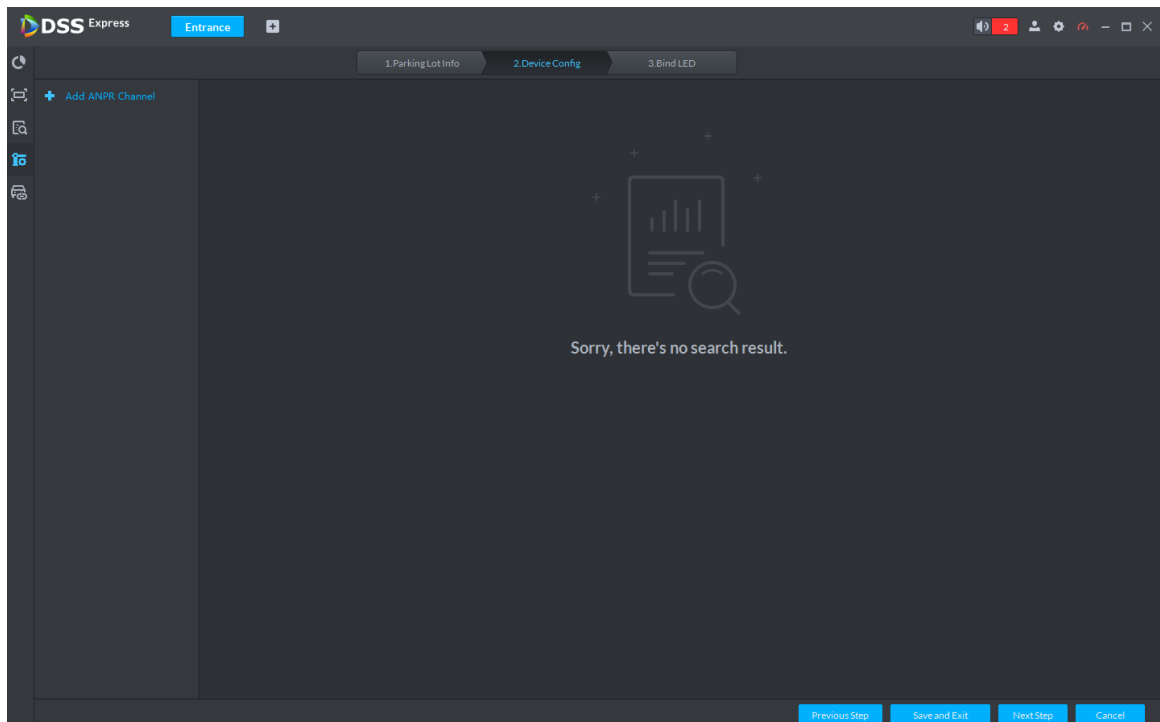
Parameter		Description
Parking	Name	Parking lot name, used to recognize different areas.

Parameter		Description
Lot Info	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: - All-period template: 00:00 to 24:00 daily. - Weekday template: 00:00 to 24:00 Mon to Fri - Weekend template: 00:00 to 24:00 Sat and Sun
	Zero residual space	Release option when remaining space is zero. - No entry. Any vehicle is not allowed to enter. - All Any vehicle is allowed to enter. - Whitelist Whitelist vehicles include several vehicle types, such as no group, general and VIP. Only three types of vehicle above are allowed to enter when remaining space is zero. - VIP Only VIP vehicle is allowed to enter when remaining space is zero.  Vehicle type should be set during vehicle management.
	Visitor auto release	Those which are not registered on DSS Express 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.
	Alarm timeout	Vehicle enters parking lot and stays longer than threshold, alarm is triggered.
Exit Release	Visitor auto release	Those which are not registered on DSS Express 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.

3) Click **Next**.

The system displays the interface of **Device Config**. See Figure 3-414

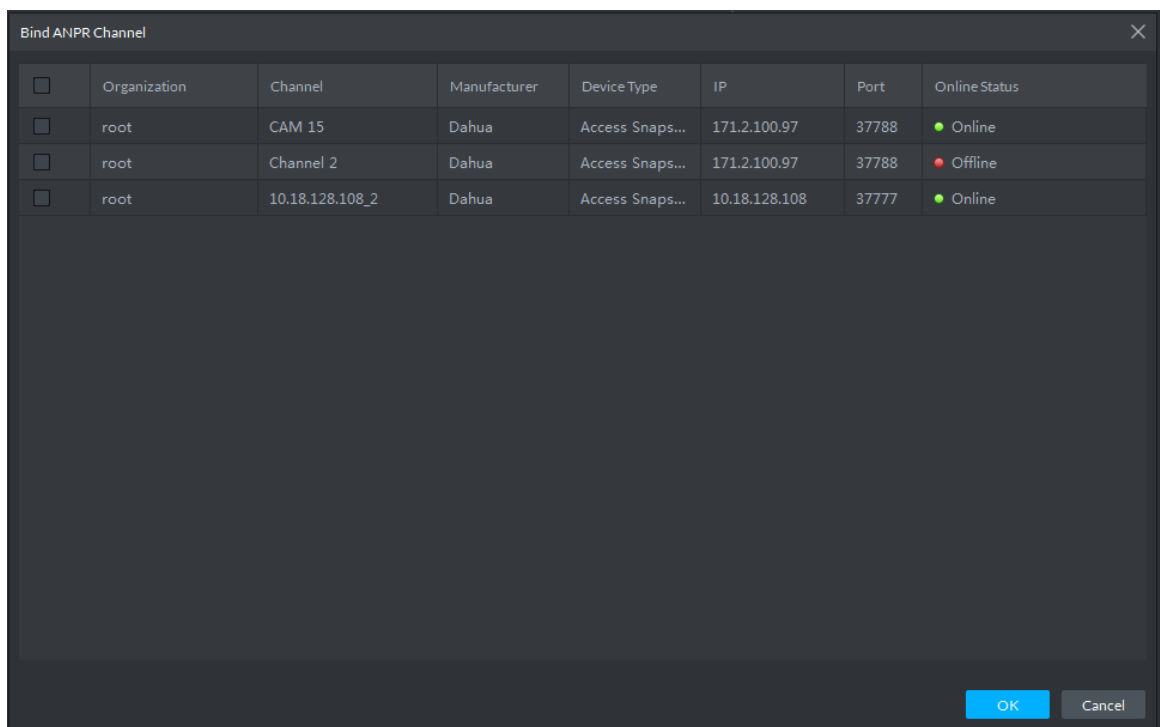
Figure 3-414 Device config



Step 4 Add 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. See Figure 3-415.

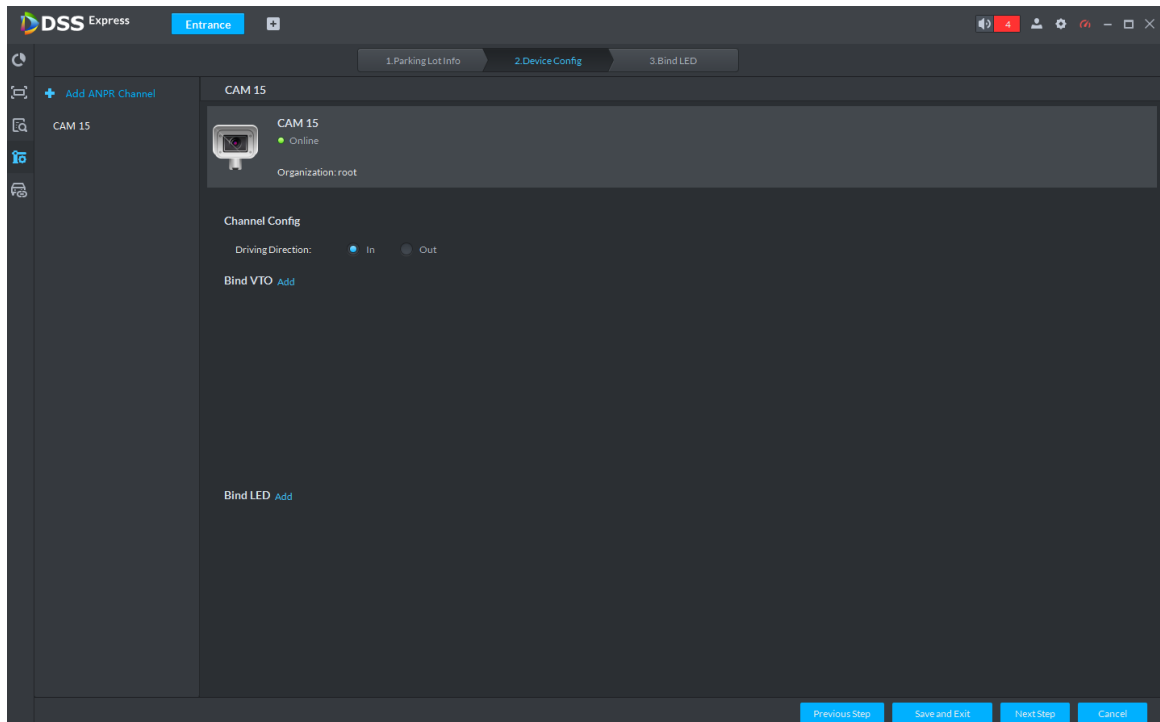
Figure 3-415 Add ANPR device



- 2) Click **OK**.

The system displays the information of added ANPR device. See Figure 3-416.

Figure 3-416 ANPR device info



- 3) Select ANPR device from device list in sequence, and set corresponding driving direction. Default driving direction is **In**.

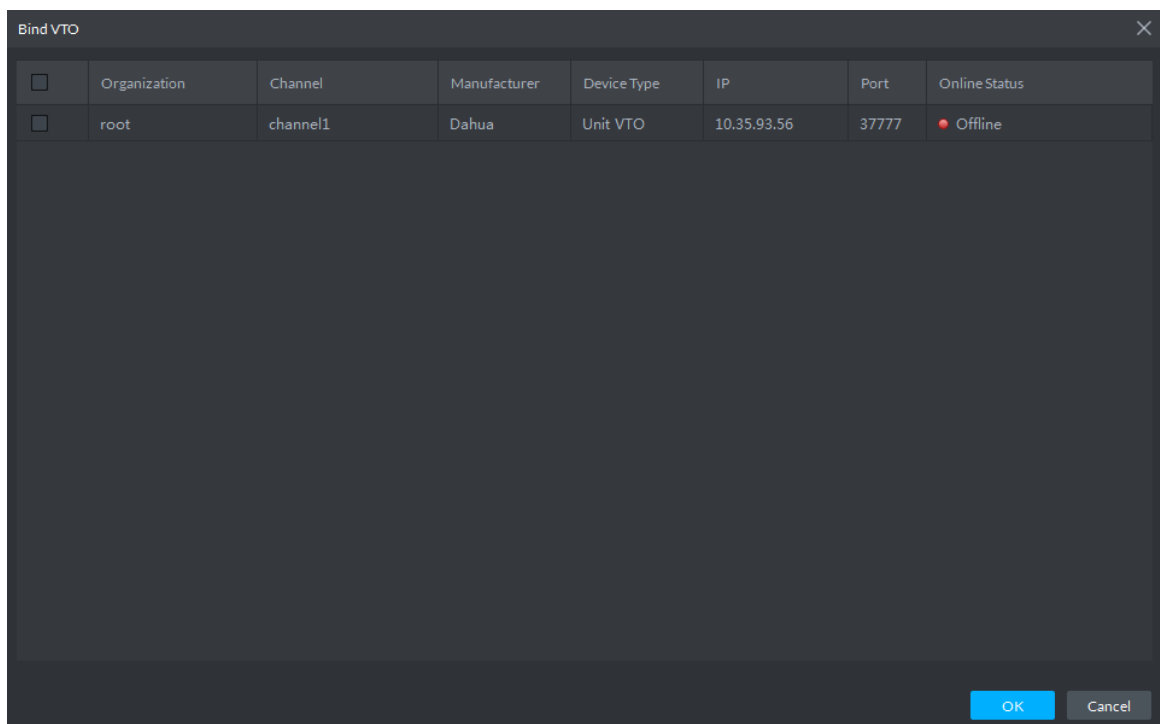
Step 5 Bind VTO device.

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**.

The system displays the interface of **Bind VTO**. See Figure 3-417.

Figure 3-417 VTO device info



- 2) Select the VTO that is deployed next to barrier, and click OK.

The interface displays the VTO information.

Step 6 Click **Next**.

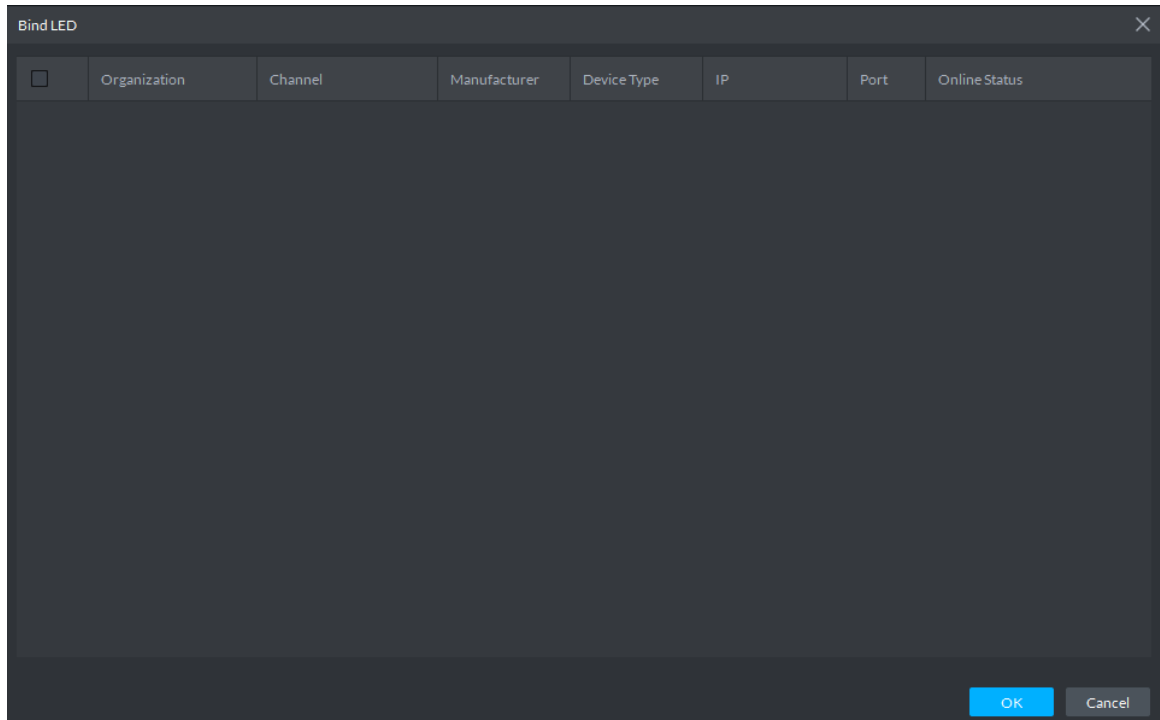
The system displays Bind LED.

Step 7 Add LED.

1) Click **Add LED**.

The system displays the interface of **Bind LED**. See Figure 3-418.

Figure 3-418 LED device info



2) Select all the LED of the parking lot and click **OK**.

The system displays the information of LED.

3.17.5 Vehicle Management

Vehicle info 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 info from personnel management module.

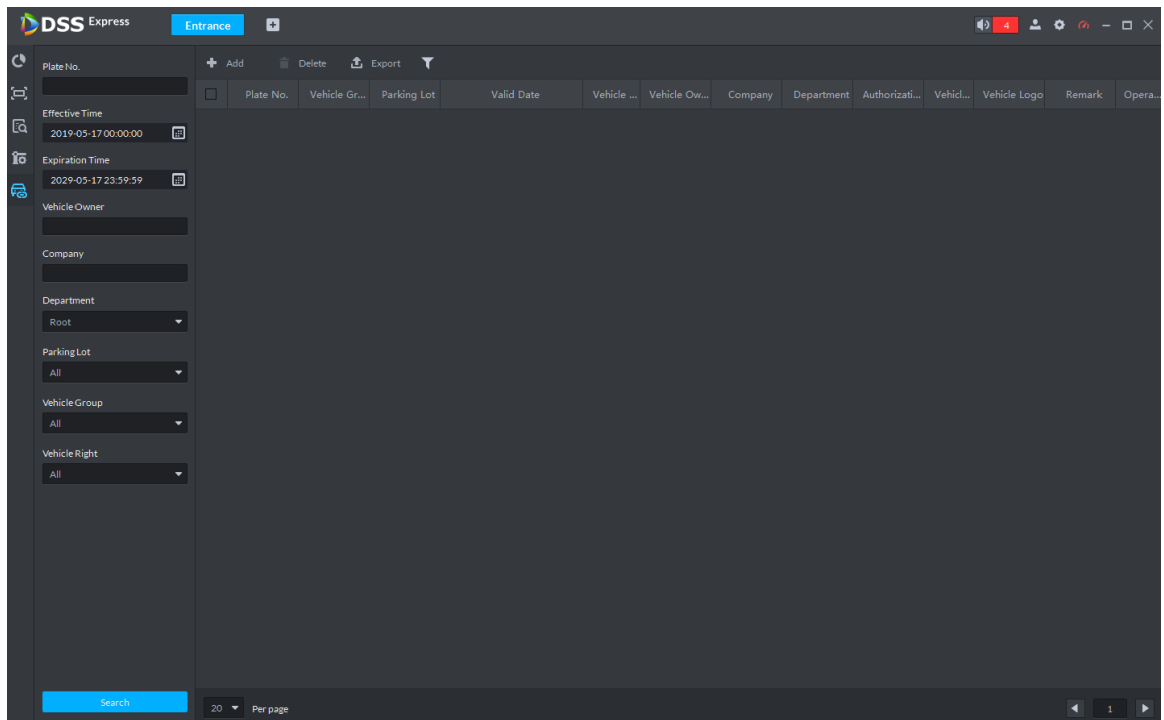
Step 1 Click  on the interface of **Entrance**.

The system displays the interface of Vehicle Management. See Figure 3-419.



You can set search condition, click **Search** and the system displays vehicle info including vehicle information added on personnel management module.

Figure 3-419 Vehicle management



Step 2 Click **Add**.

The system displays the interface of **Add**. See Figure 3-420.

Figure 3-420 Add vehicle

Step 3 Click the tab of **Vehicle Info** and add vehicle info, click **Next** and the system displays the interface of **Personnel Info**. Refer to Figure 3-421. Refer to Table 3-50 for parameter details.

Figure 3-421 Personnel info

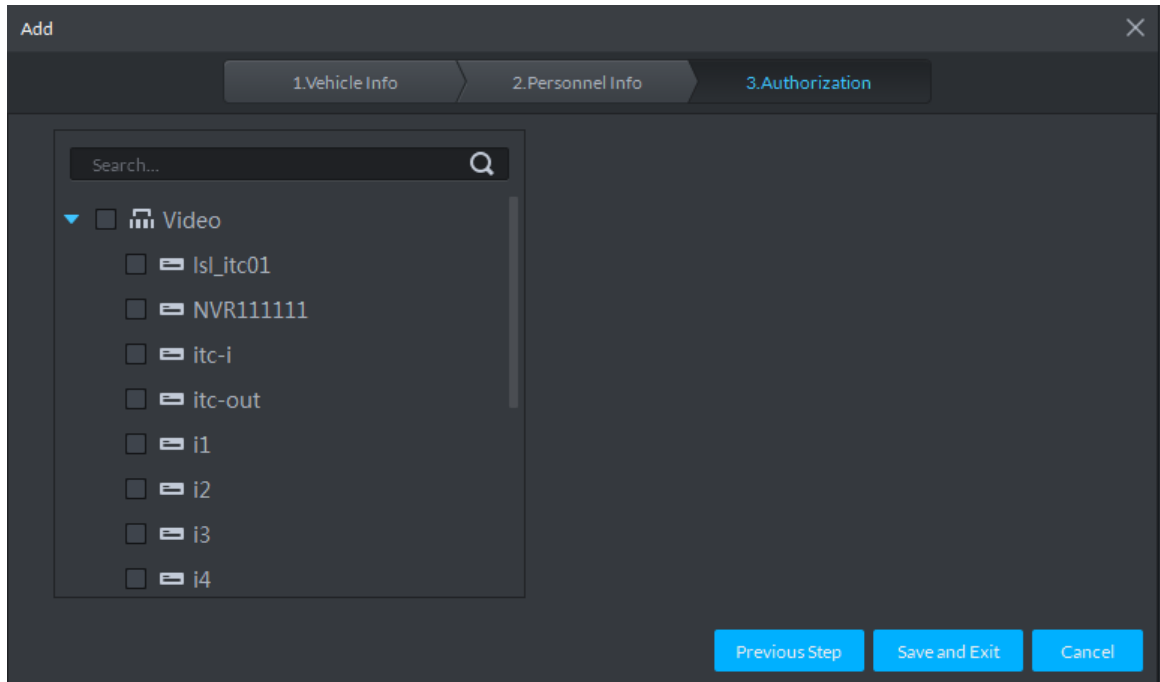
Table 3-50 Vehicle info

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 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 info, click **Next**.

The system displays the Authorization interface. See Figure 3-422.

Figure 3-422 Authentication



Step 5 Select all the ANPR devices that allow entrance and exit of the parking lot, click **Save and Exit**. Synchronize vehicle info to corresponding ANPR device, and make sure the ANPR device can make judgment if it has to release the vehicle even if ANPR device is disconnected to platform.

3.17.6 Entrance Application

3.17.6.1 Overview

View the free parking ratio of current parking area; make statistics over realtime quantity and on-site vehicle quantity, view quantity of entrance and exit vehicle within some period.

Click  on the Entrance interface. The system displays the interface of Overview. See Figure 3-423. Refer to Table 3-51 for parameter details.

Figure 3-423 Overview



Table 3-51 Vehicle info overview

SN	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.

SN	Description
5	Display following data. - 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.
6	Auto refresh overview info every 5 minutes. Click Refresh to sync realtime data.

3.17.6.2 License Plate Recognition

Click  on the **Entrance** interface. The system displays the interface of **License Plate Recognition**. See Figure 3-424. Refer to Table 3-52 for more parameter details.

Figure 3-424 LPR

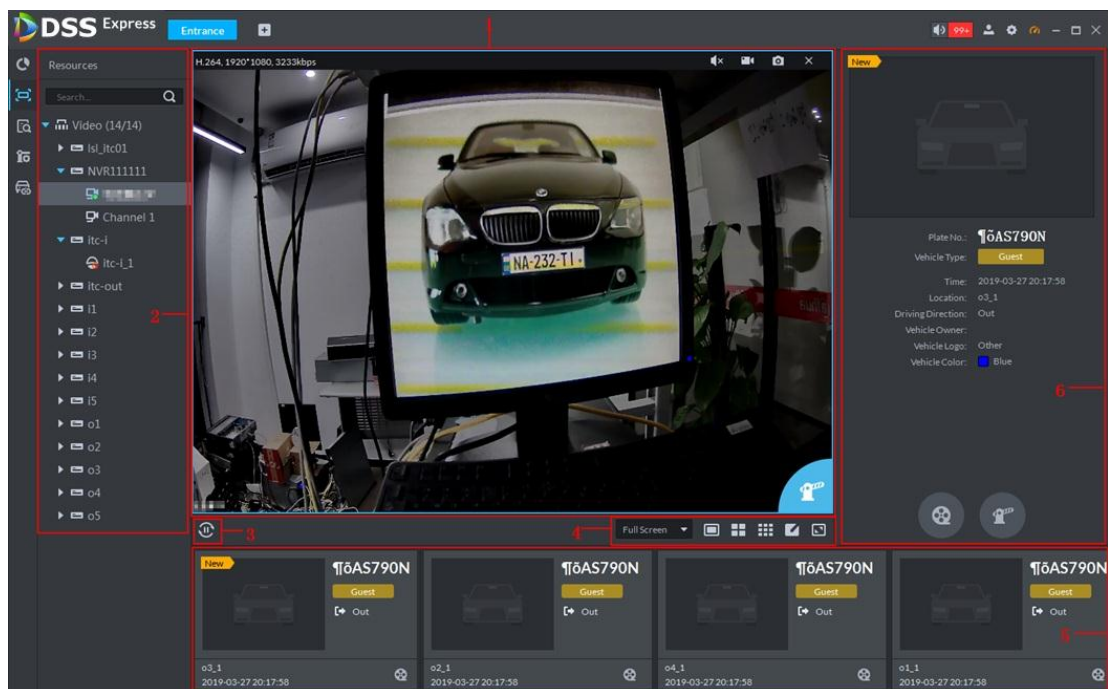
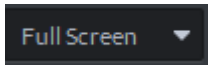


Table 3-52 LPR interface description

SN	Description
----	-------------

SN	Description
1	Realtime 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 realtime 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 info. Click  and the icon becomes  , the interface will update realtime ANPR recognition info.
4	, set height and width ratio of video window, it plays video by two modes which are original scale and full screen. , used to set image split mode, which includes 1 split, 4 splits and 9 splits, or click  and customize split mode. , switch video window to Full Screen mode. If you want to exit Full Screen, you can also press ESC button or right click to select Exit Full Screen.
5	Display latest 4 snapshots of LPR. More details as follows. - Double click and display snapshot details, vehicle info, snapshot panoramic picture and vehicle matting. - Click  and view video of linked channel.
6	Display license plate snapshot and vehicle which need to be released manually. More operation as follows. - Click  and unlock barrier to release vehicle. - Click  and view video of linked channel.

3.17.6.3 Info Query

Search accessed vehicle, on-site vehicle and snapshot record.

Step 1 Click  on the **Entrance** interface.

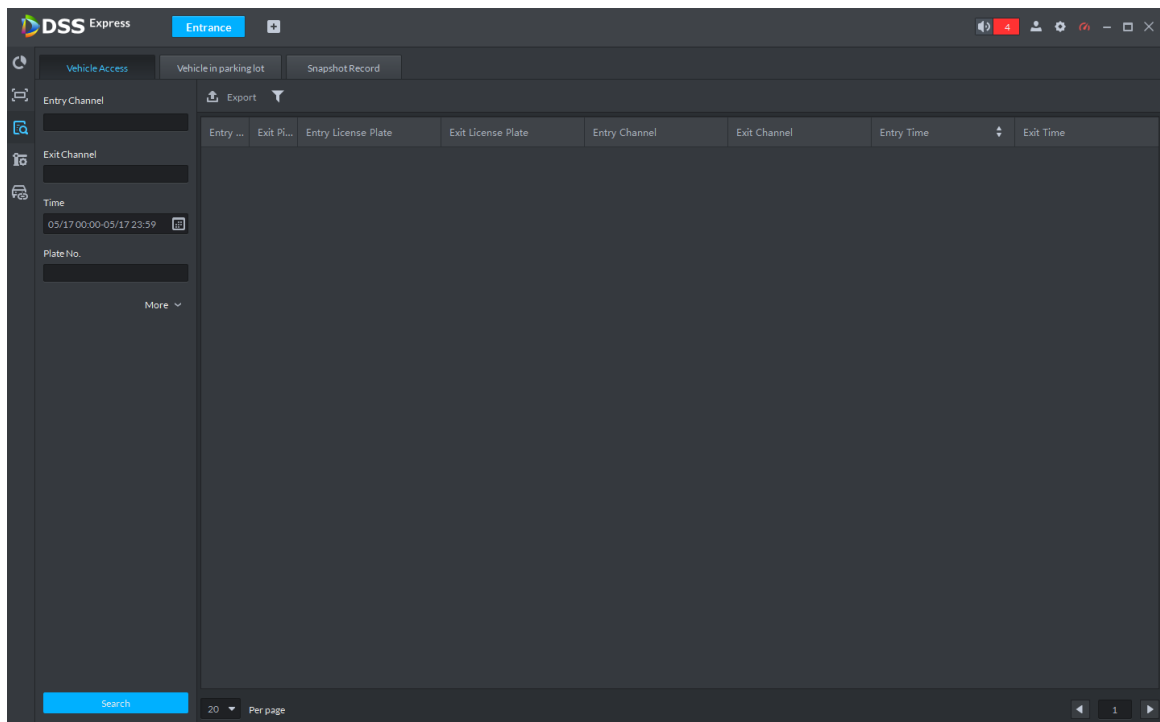
The system displays the interface of **Info Query**.

Step 2 Search vehicle in and out information.

1) Click the tab of **Vehicle Access**.

The system displays the interface of **Vehicle Access**. See Figure 3-425.

Figure 3-425 Vehicle access



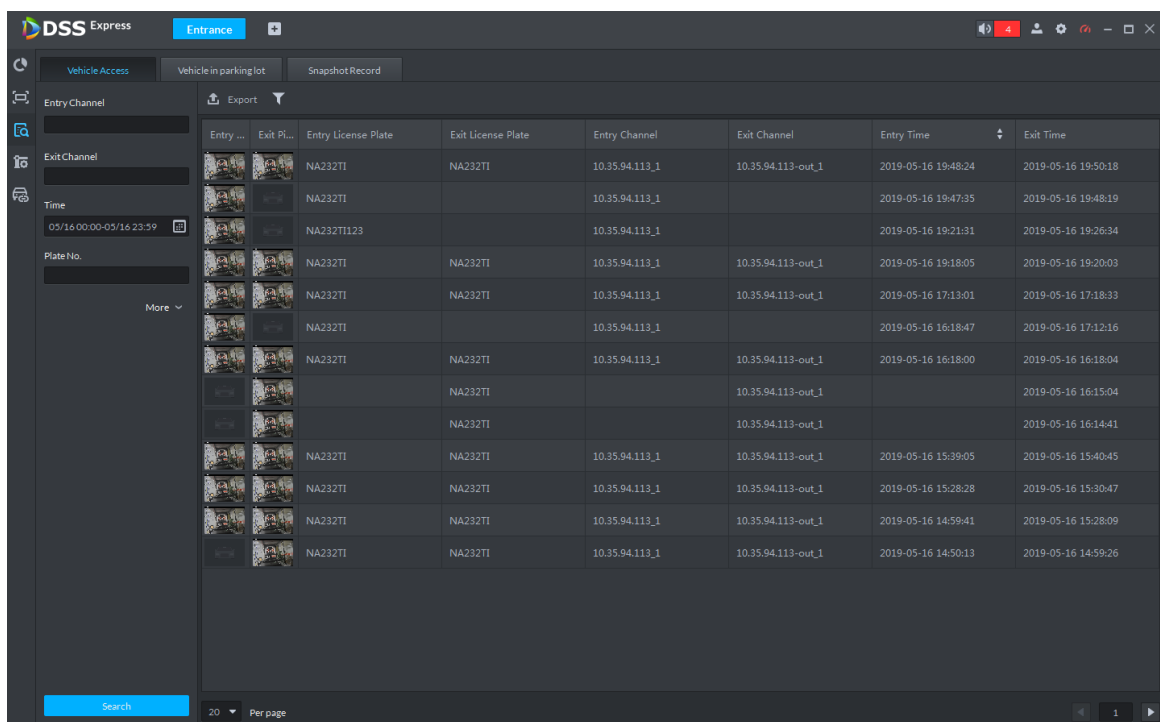
- 2) Set search condition, click Search.

The system displays search results. See Figure 3-426.



Click **More** and you can search by vehicle owner, department and vehicle type etc.

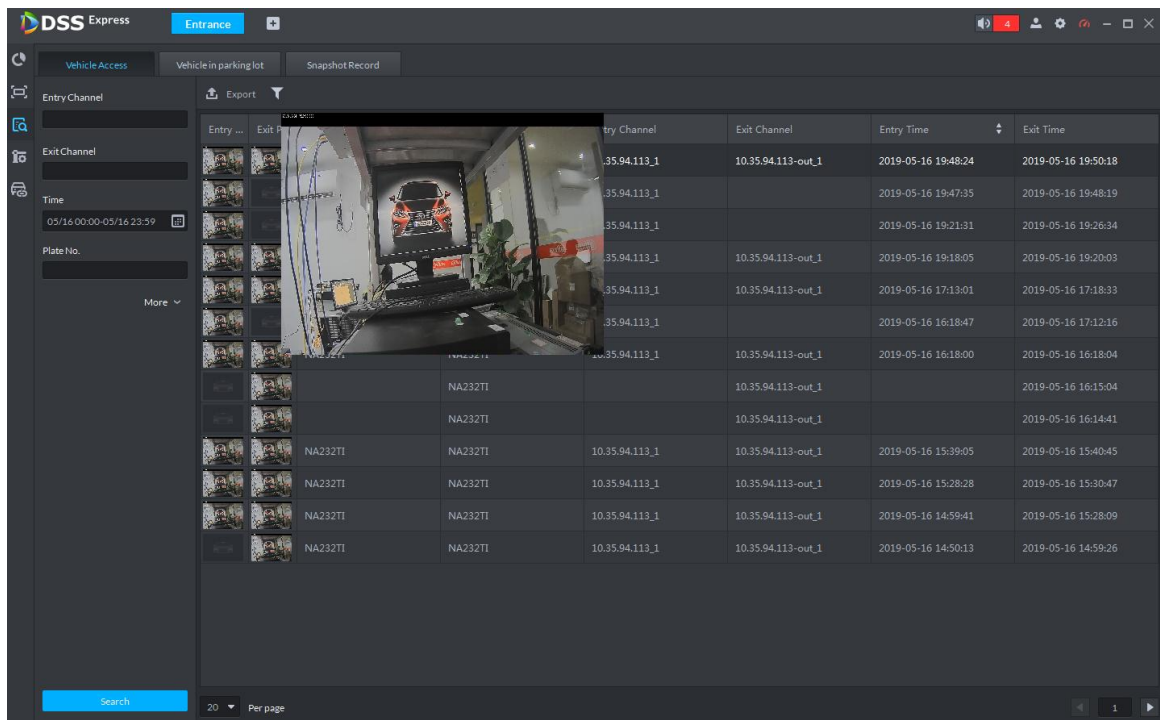
Figure 3-426 Vehicle access info



- 3) 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. See Figure 3-427.

Figure 3-427 Big vehicle picture



- ◇ Double click the record, and detailed info is displayed on the right of interface. See Figure 3-428. Double click the picture in the Info, display big picture, drag green box and the big picture will be displayed in the lower right corner. See Figure 3-429. Click **Edit** to modify vehicle info, click **OK** to save config. Click **Video** to view linked video.

Figure 3-428 Vehicle details (1)

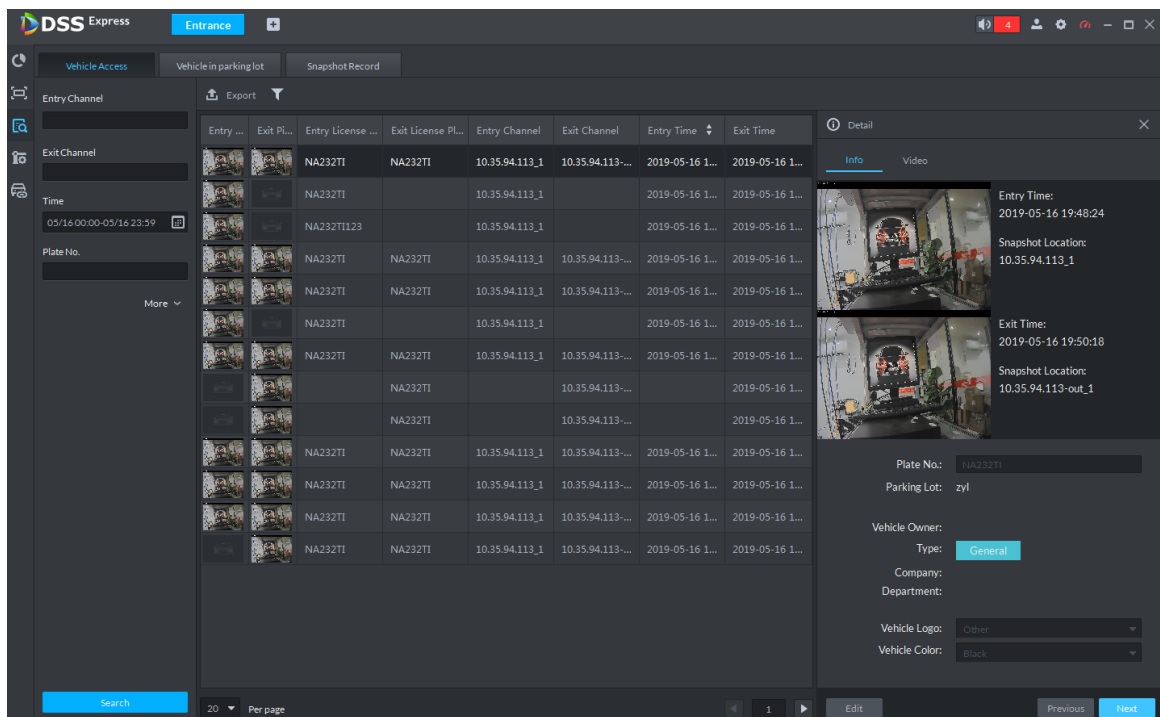
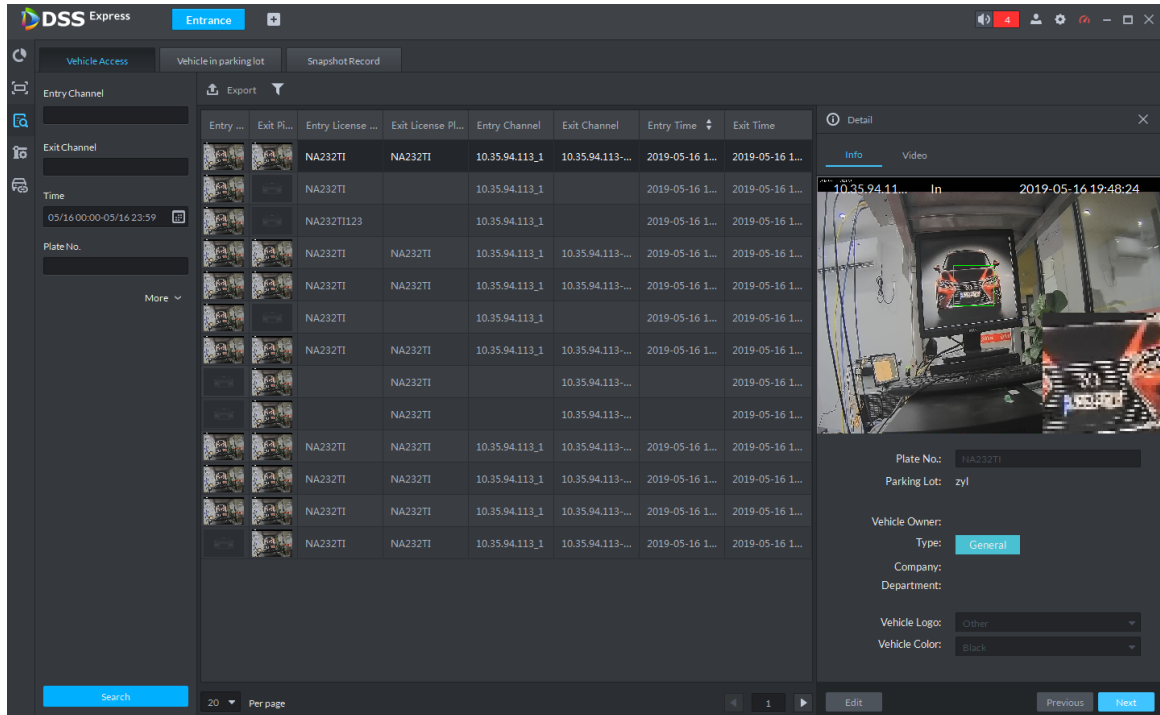


Figure 3-429 Vehicle details (2)



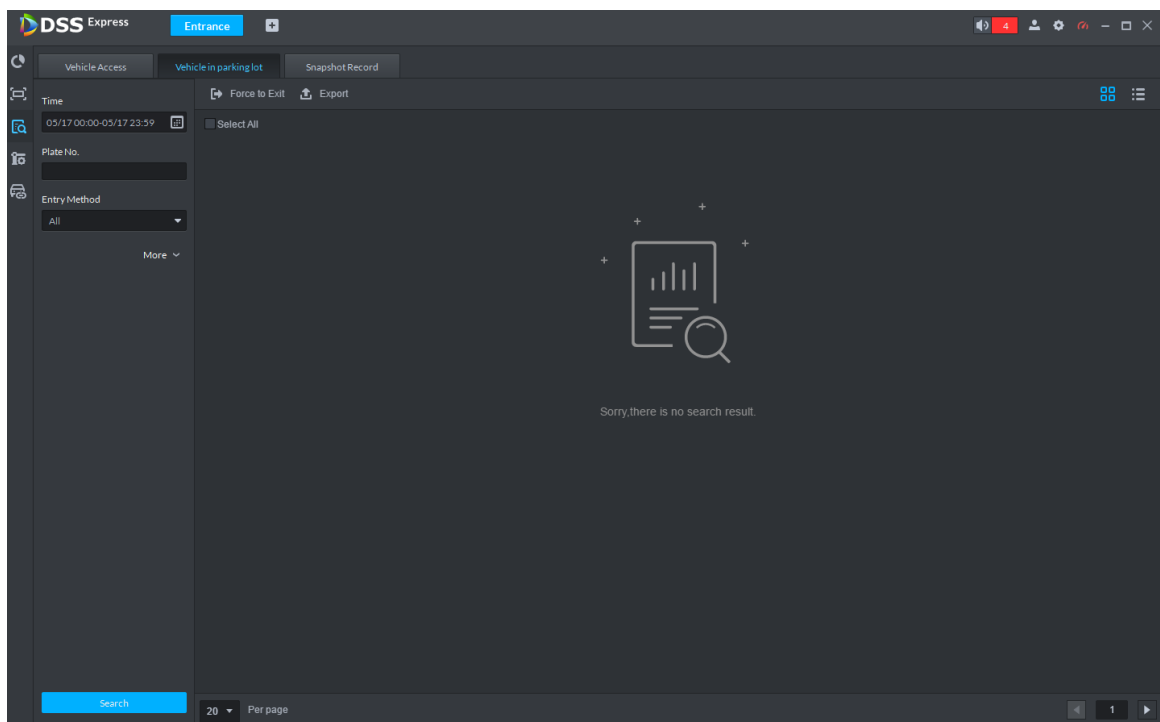
- ◇ Export info. Click **Export** to export all the searched vehicle access info.
- ◇ Set info display item. Click and select display item.
- ◇ Click **Next** and display next info detail. Click **Previous** and display previous info detail.

Step 3 Search on-site vehicle.

- 1) Click the tab of Vehicle in parking lot.

The system displays the interface of **Vehicle in Parking Lot**. See Figure 3-430.

Figure 3-430 Vehicle in parking lot



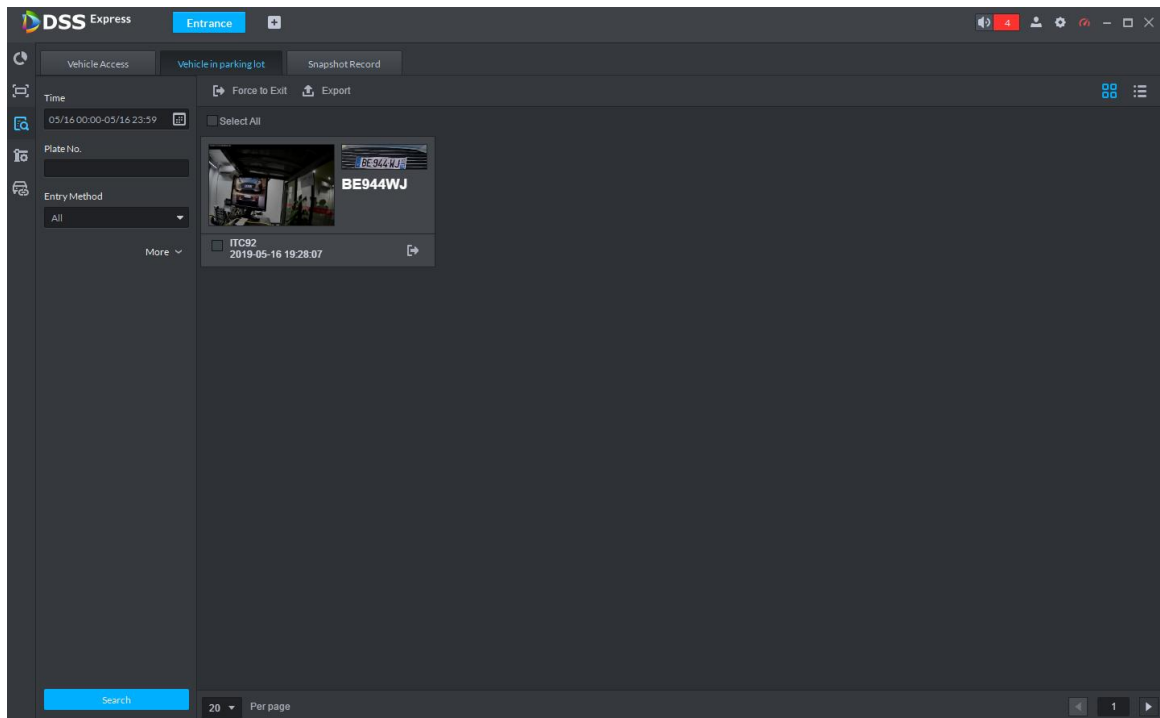
- 2) Set search condition, Click **Search**.

The system displays the search results. See Figure 3-431.



Click **More** and you can search info via vehicle owner, department and vehicle type etc.

Figure 3-431 Vehicle in parking lot info



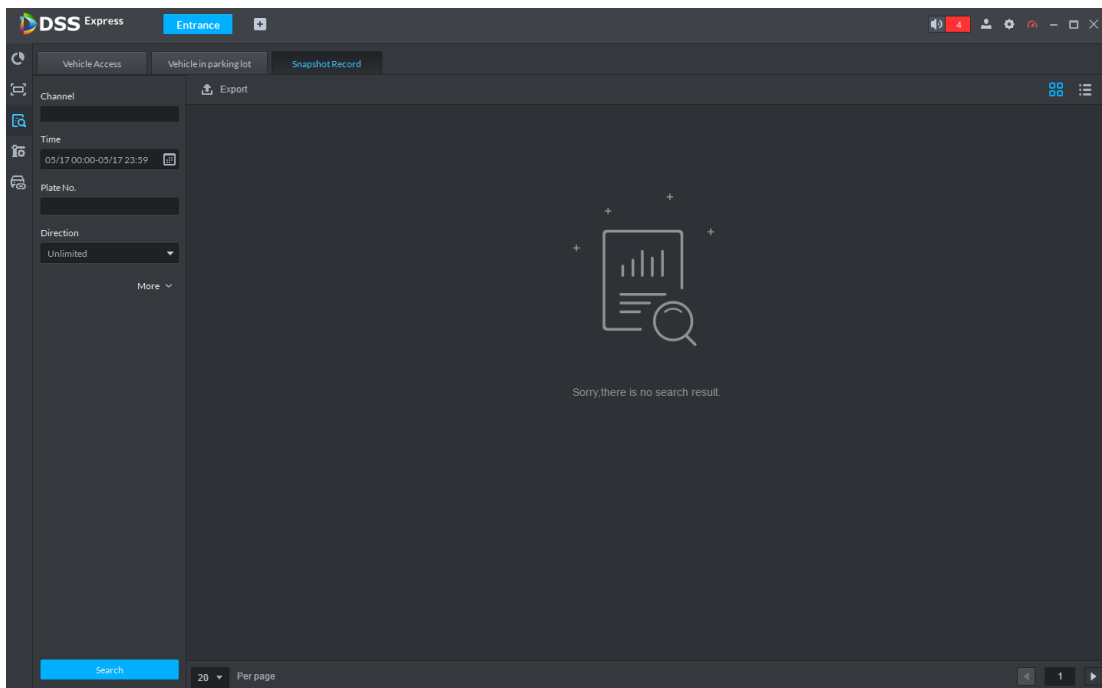
- 3) Related operations of vehicle in and out are as follows.
 - ◇ If the vehicle is confirmed not to be in the area, then click to select information (several items supported), and click **Force to Exit** or . Make sure the vehicle exits by Pro.
 - ◇ Export information. Click **Export** and export all the information of on-site vehicles that can be searched.
 - ◇ Set info display item. Click  and select display item.
 - ◇ Click view mode () or list mode () to select different display mode.

Step 4 Search Snapshot Record

- 1) Click the tab of **Snapshot Record**.

The system displays the interface of **Snapshot Record**. See Figure 3-432.

Figure 3-432 Snapshot record



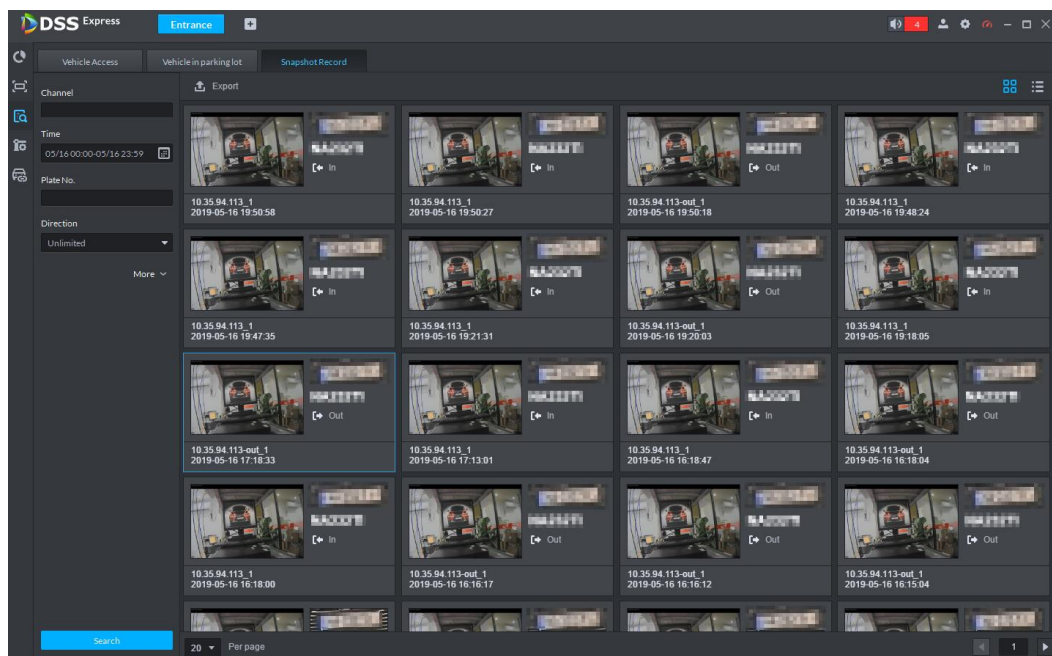
- 2) Set search condition, click **Search**.

The system displays search results. See Figure 3-433.



Click **More** and you can search info via vehicle owner, department and vehicle type etc.

Figure 3-433 Snapshot record info



- 3) Related operations of vehicle snapshot are as follows.

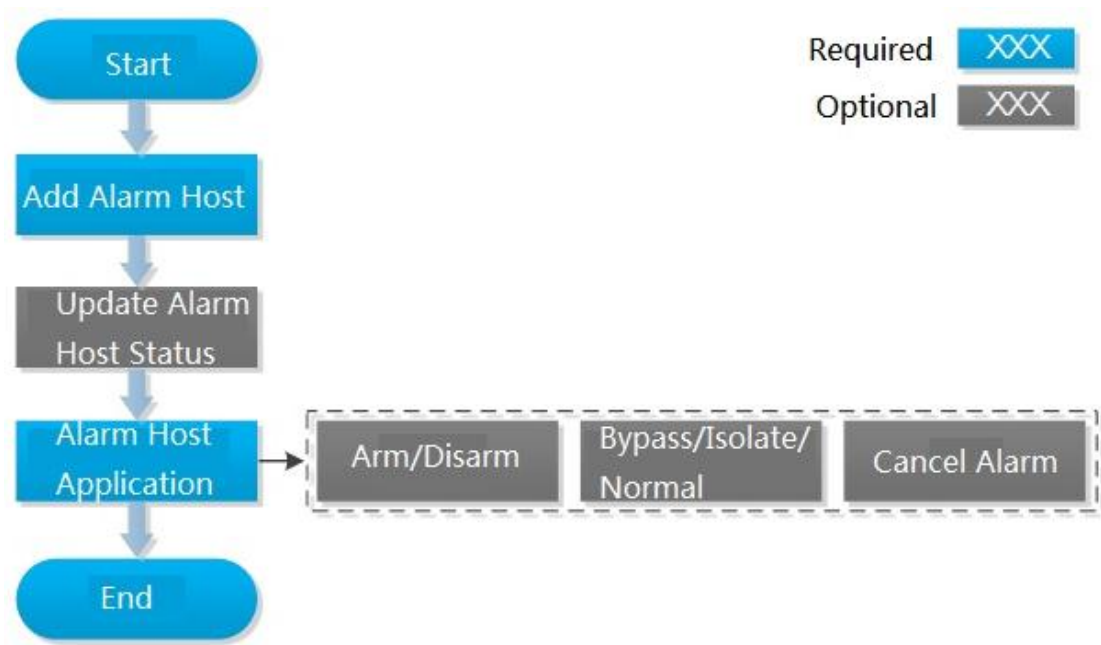
- ◇ Export info. Click **Export** to export all the info of on-site vehicles that can be searched.
- ◇ Click view mode () or list mode () and select different display modes.

3.18 Alarm Host

After adding alarm host to platform, you can manage and configure alarm zone and sub system.

The alarm host operation flow is shown in Figure 3-434.

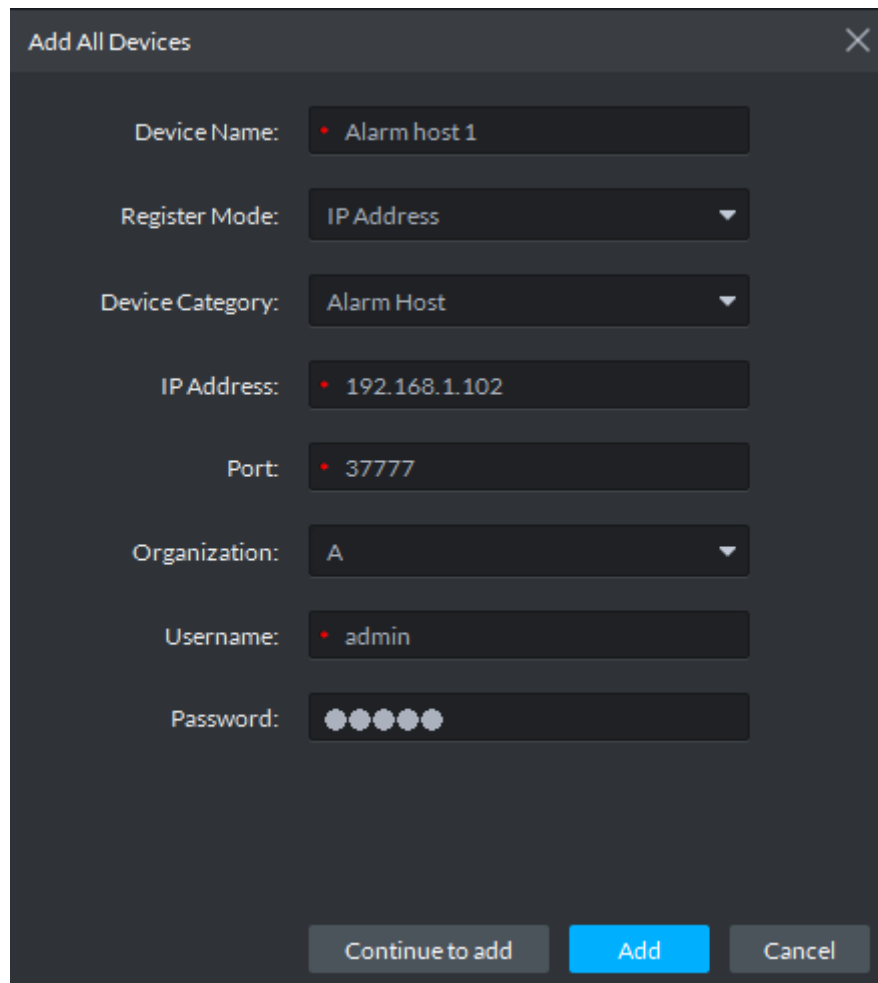
Figure 3-434 Alarm host management flow



3.18.1 Adding Alarm Host

Step 1 Add alarm host, set **Device Category** as **Alarm Host**, and see Figure 3-435. For more details, see **3.2.2.4 Adding Device**

Figure 3-435 Add alarm host



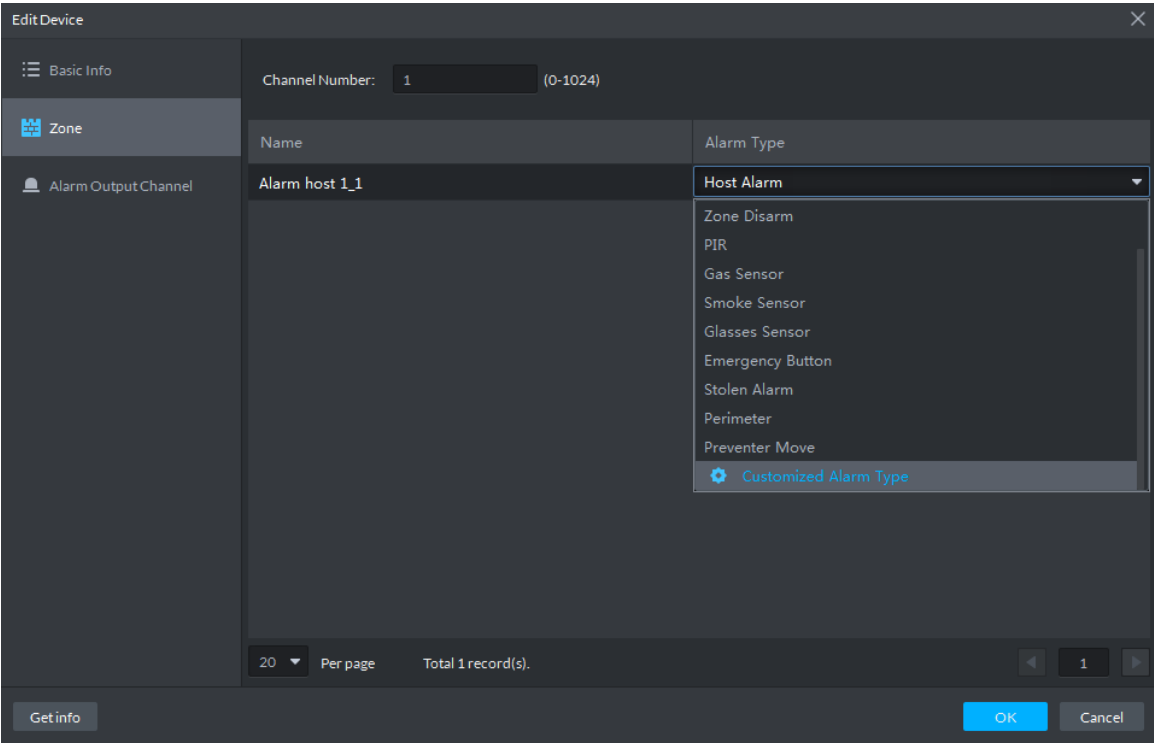
The screenshot shows a dark-themed dialog box titled "Add All Devices" with a close button (X) in the top right corner. The dialog contains several input fields for configuring a device:

- Device Name:** A text input field containing "Alarm host 1".
- Register Mode:** A dropdown menu currently showing "IP Address".
- Device Category:** A dropdown menu currently showing "Alarm Host".
- IP Address:** A text input field containing "192.168.1.102".
- Port:** A text input field containing "37777".
- Organization:** A dropdown menu currently showing "A".
- Username:** A text input field containing "admin".
- Password:** A password input field represented by five dots.

At the bottom of the dialog, there are three buttons: "Continue to add" (disabled), "Add" (highlighted in blue), and "Cancel" (disabled).

Step 2 Modify device zone info. For example, zone is connected to smoke sensor, then select **Alarm Type** as **Smoke Sensor**, see Figure 3-436. Alarm type supports custom, you can select **Customized Alarm Type** from the **Alarm Type** box, and set the alarm type you need, used to quickly recognize alarm. After config, on event config interface, corresponding alarm input can configure corresponding alarm event.

Figure 3-436 Modify zone



3.18.2 Entering Alarm Controller Interface

Click  and select Alarm Controller on the client homepage, the system displays Alarm Controller interface, see Figure 3-437.

Figure 3-437 Alarm controller interface

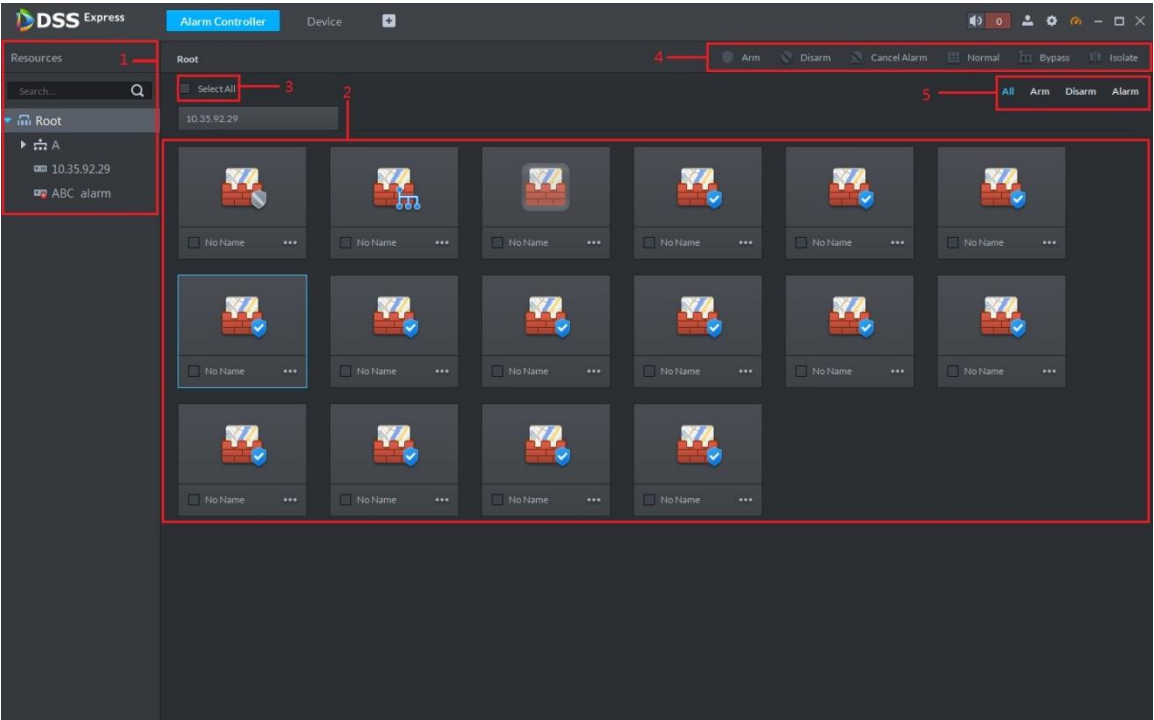


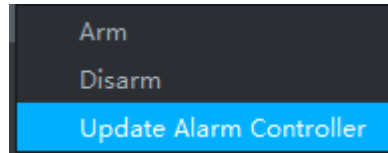
Table 3-53 Alarm controller interface description

No.	Name	Description
1	Device list	Display all alarm controller devices and subsystems under device. Icon status of subsystem , no zone under subsystem. , zone exists under subsystem  The subsystem and zone info displayed on platform can be acquired from device; the platform does not support config.
2	Subsystem and zone list	If you select alarm controller device from the left device list, display subsystem under alarm controller and zones not added to subsystem; if you select subsystem from left device list, then the platform displays zones under subsystem. The description of icon status is shown as follows. - Zone status icon  , arm.  , disarm.  , bypass.  , isolate. - Subsystem status icon  , 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.

3.18.3 Updating Alarm Controller Status

In the device tree area, right click the alarm controller that needs to be updated, select **Update Alarm Controller**, and see Figure 3-438. The platform synchronizes status of alarm controller.

Figure 3-438 Update alarm controller



3.18.4 Alarm Controller Application

3.18.4.1 Arm/Disarm

After armed, the alarm controller makes response upon the alarm signal from zone; You can disarm the zone and controller will not upload alarm message.

3.18.4.1.1 Global Arm/Disarm

Globally arm or disarm all zones under alarm controller.

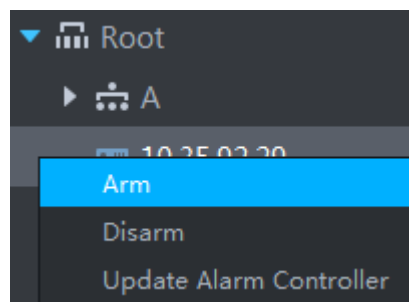
Arm

In device tree area, right click the alarm controller that needs to be armed globally, select **Arm**, and see Figure 3-439.



Arm fails when alarm input exists in zone. Please disarm if you continue to arm, clear alarms in each zone, zone with alarm input exists in bypass, and then arm again.

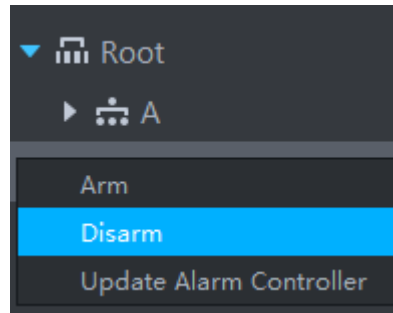
Figure 3-439 Global arm



Disarm

In device tree area, right click the alarm controller that needs to be disarmed globally, select **Disarm**, and see Figure 3-440.

Figure 3-440 Global disarm



3.18.4.1.2 Arm/Disarm Zone or Subsystem

Arm or disarm single zone.

Arm



- Arm fails when alarm input exists in zone. Please disarm if you continue to arm, clear alarms in each zone, zone with alarm input exists in bypass, and then arm again.
- If subsystem has no zone, then you cannot arm or disarm subsystem.

You can arm by following two methods

- Click the zone you want to arm or  of corresponding subsystem, select **Arm**, see Figure 3-441 and Figure 3-442.

Figure 3-441 Arm zone

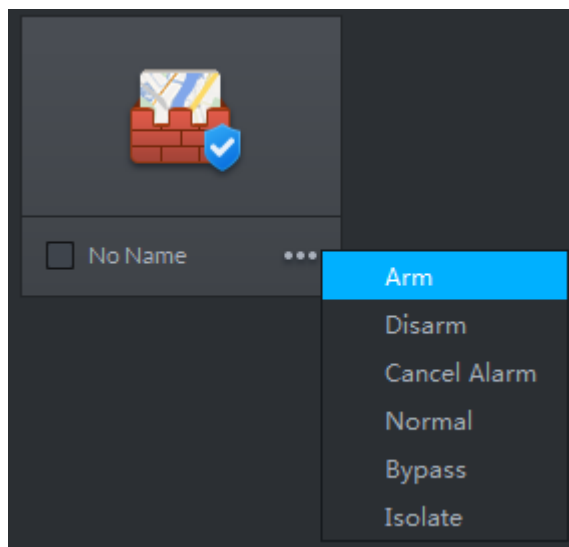
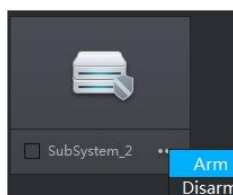
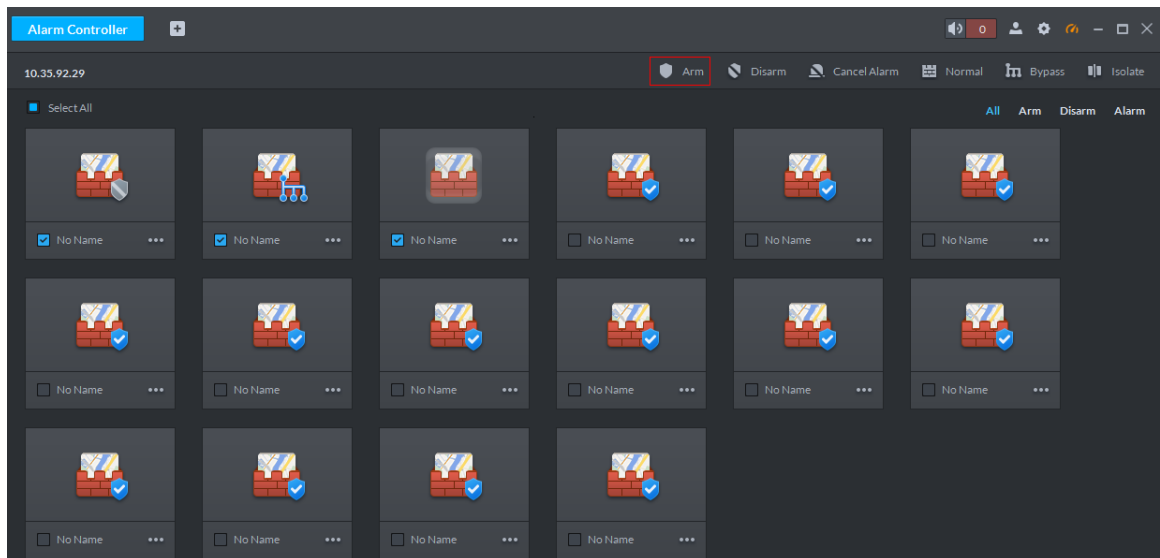


Figure 3-442 Arm subsystem



- Select the zone or subsystem you want to arm (multiple choice supported), click **Arm** on top of the interface, and see Figure 3-443.

Figure 3-443 Arm



Disarm

Supports disarm by following two methods.

- Click the zone you want to disarm or  of corresponding subsystem, select **Disarm**, see Figure 3-444 and Figure 3-445.

Figure 3-444 Disarm zone

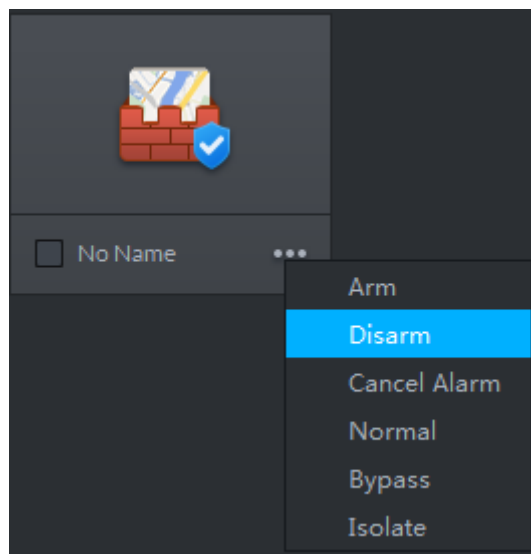
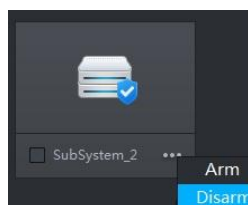
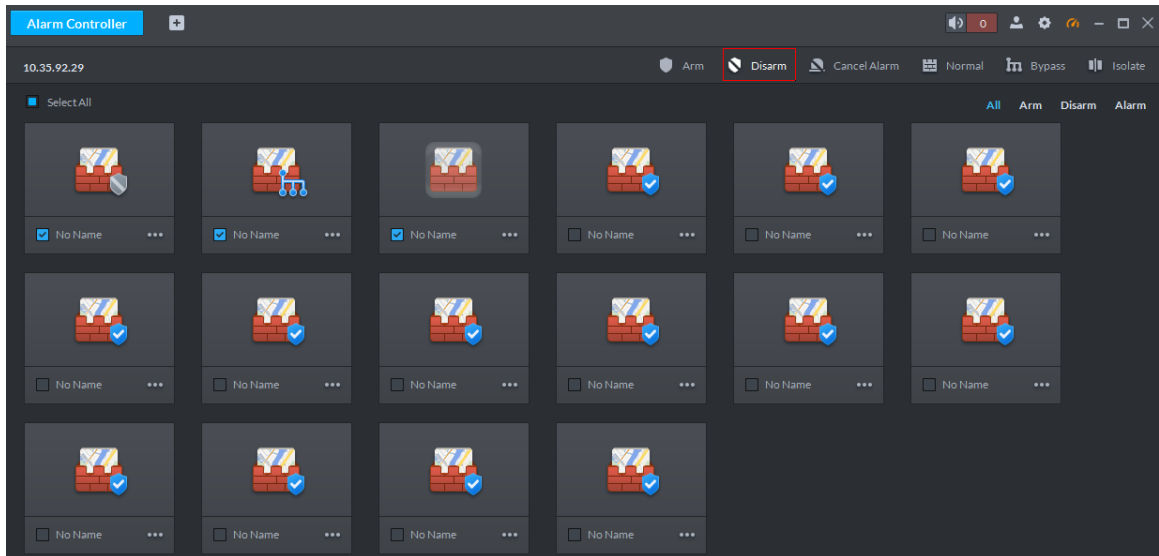


Figure 3-445 Disarm subsystem



- Select the zone or subsystem you want to disarm (multiple choice supported), click **Disarm** on top of the interface, and see Figure 3-446.

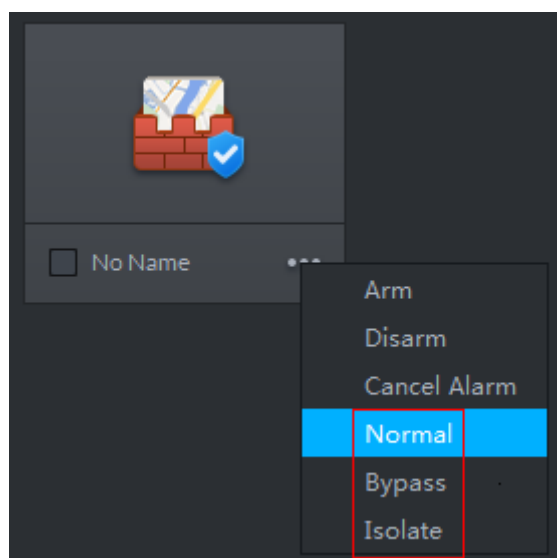
Figure 3-446 Disarm



3.18.4.2 Bypass/Isolate/Normal

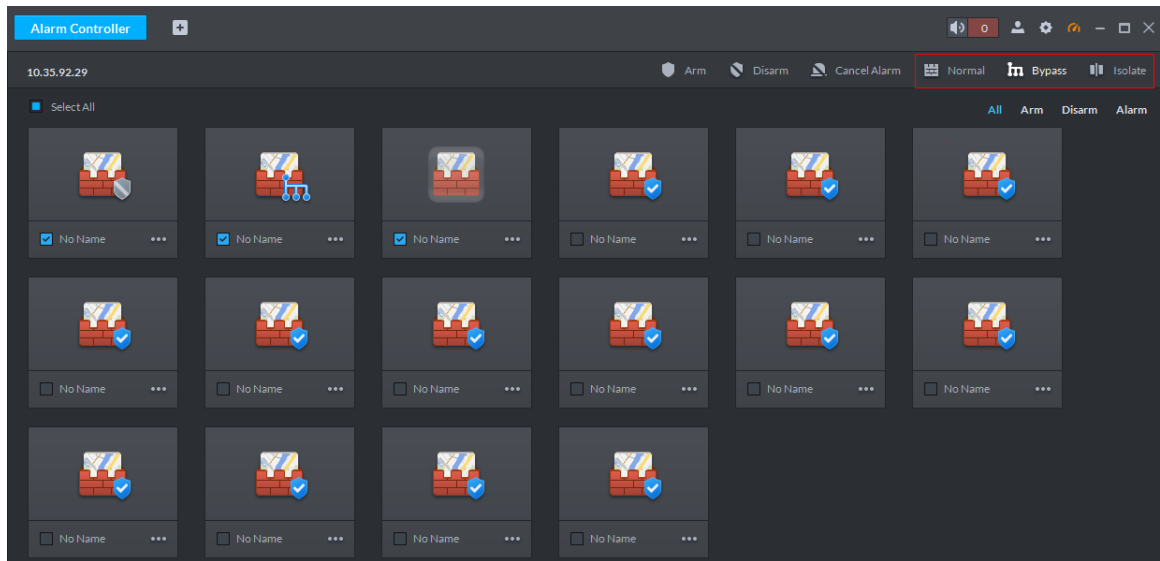
- Bypass zone, the alarm controller still monitors external detector and make records, but not forward to users. If you want to arm the bypassed zone, please disarm the zone into non-bypass and arm again.
 - Isolate zone, the alarm controller still monitors external detector and make records, but not forward to users. When the zone is disabled or you want to disarm and arm again, the isolated zone is still disabled.
 - Normal zone, the zone can trigger alarm normally when it is armed.
- Two ways to operate over the zone.
- Click  of the zone that needs to be bypassed, isolated or recovered to normal, select operation and see Figure 3-447.

Figure 3-447 Bypass/isolate zone (1)



- Select the zone that needs to be bypassed, isolated or recovered normal (multiple choice supported), click the operation buttons on top of the interface, see Figure 3-448.

Figure 3-448 Bypass/isolate zone (2)

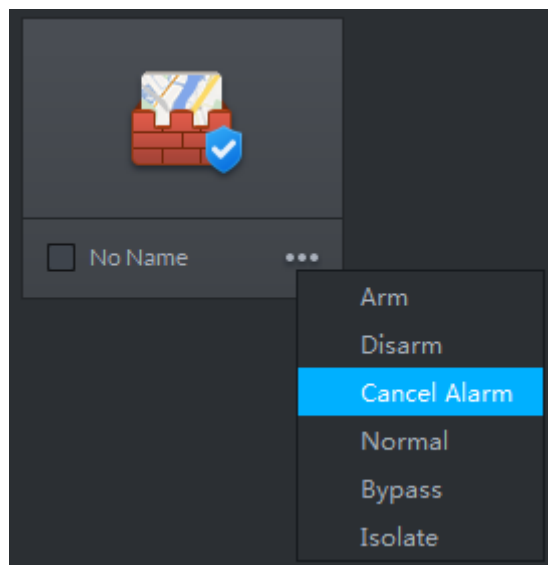


3.18.4.3 Cancel Alarm

You remove alarm by **Cancel Alarm** when alarm is triggered.

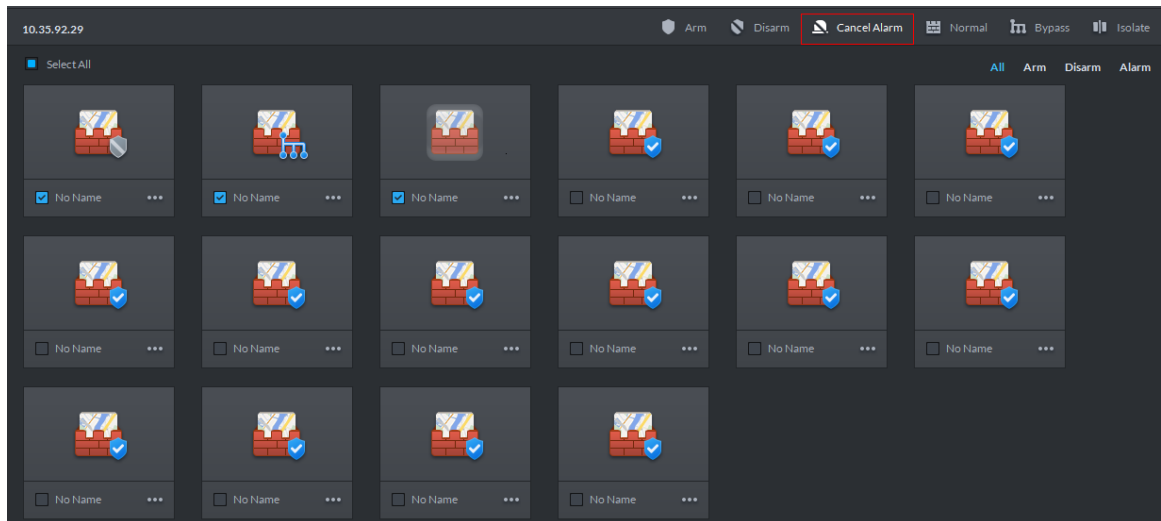
- Click the zone you want to cancel alarm, select **Cancel Alarm** and see Figure 3-449.

Figure 3-449 Cancel alarm



- Select the zone you want to cancel alarm (multiple choices supported), click **Cancel Alarm** on top of the interface and see Figure 3-450.

Figure 3-450 Cancel alarm (2)



4 Maintenance Guide

The chapter introduces daily maintenance, and make sure the platform runs safely and normally.

4.1 Backup and Restore

4.1.1 Backup

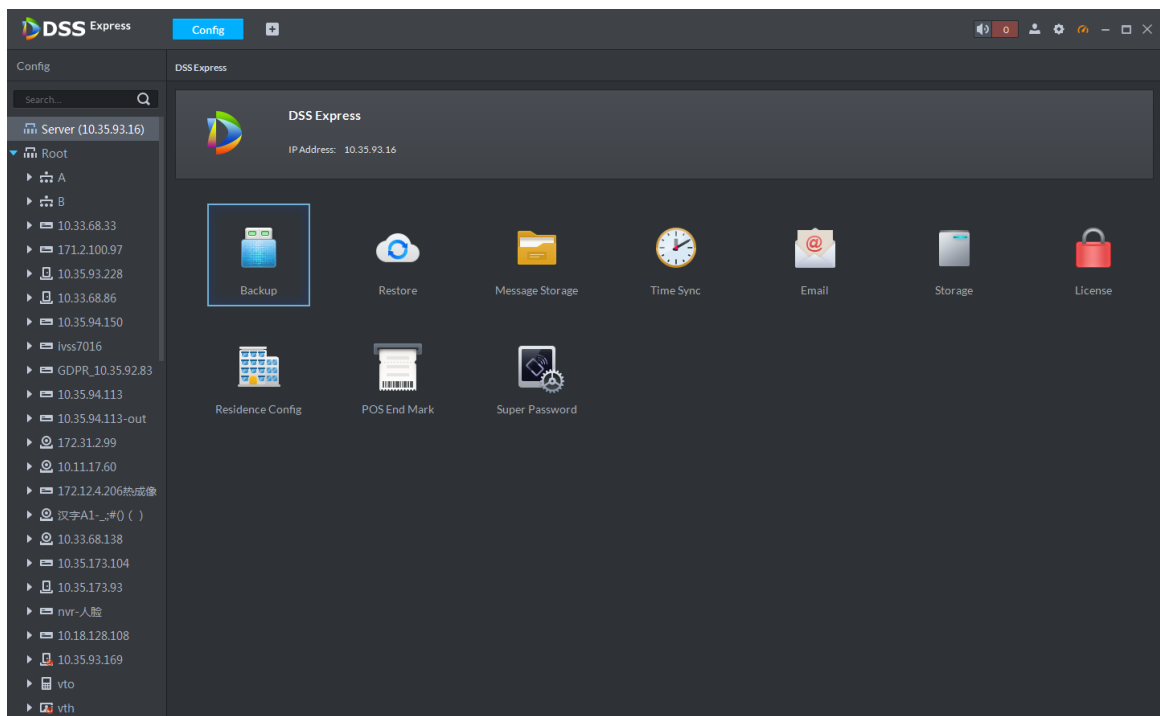
To guarantee data security, the platform provides data backup function; backup mode includes auto backup and manual backup. You are recommended to enable auto backup for regular data backup.

4.1.1.1 Auto Backup

Step 1 On client homepage, click **Config**.

The system displays **Config** interface, see Figure 4-1.

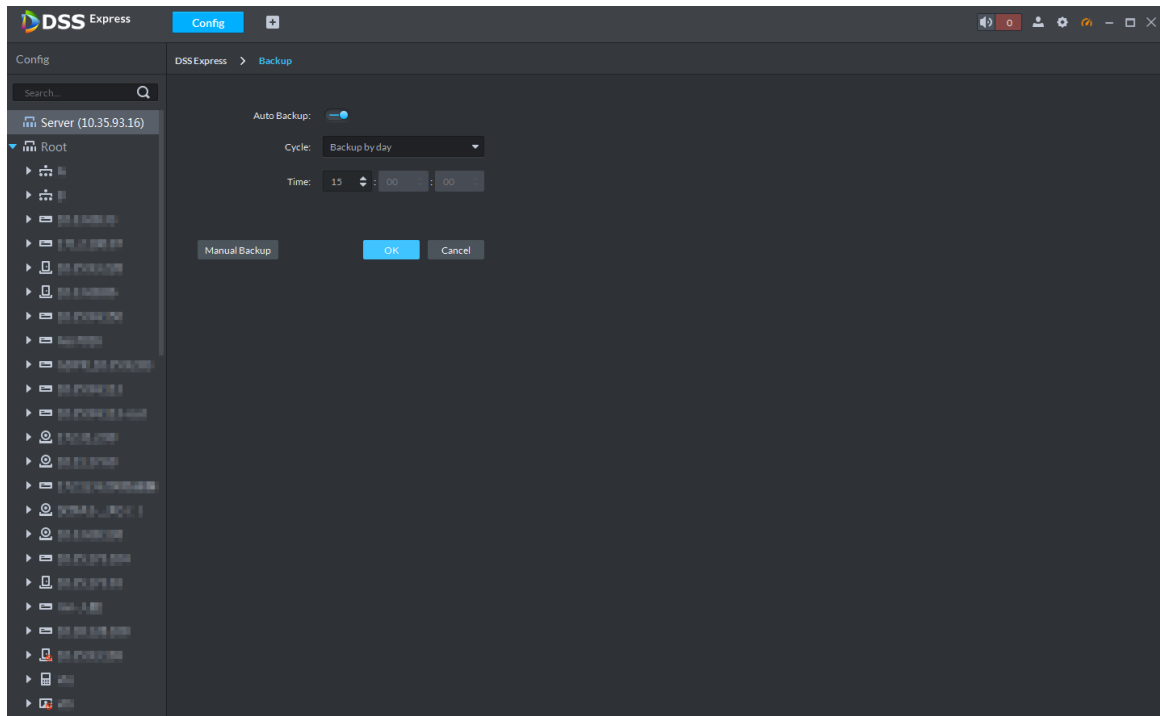
Figure 4-1 Config



Step 2 Click **Backup**.

The system displays **Backup** interface, see Figure 4-2.

Figure 4-2 Backup



Step 3 Click  next to Auto Backup.

The icon becomes , and auto back is enabled.

Step 4 Set **Cycle** and **Time**, click **OK**.

The system pops out the interface of **Set Backup File Password**.



You can select any whole hour between 3:00 and 23:00 to implement backup.

Step 5 Enter file password, click **OK**.

- File password, used to guarantee backup data file security, you need to enter password for verification if you want to open or restore backup file.
- Backup file is stored under server installation path, which is “..\Server\WEBCLIENT\webclient\apache-tomcat\tmp\systemBackup”.

4.1.1.2 Manual Backup

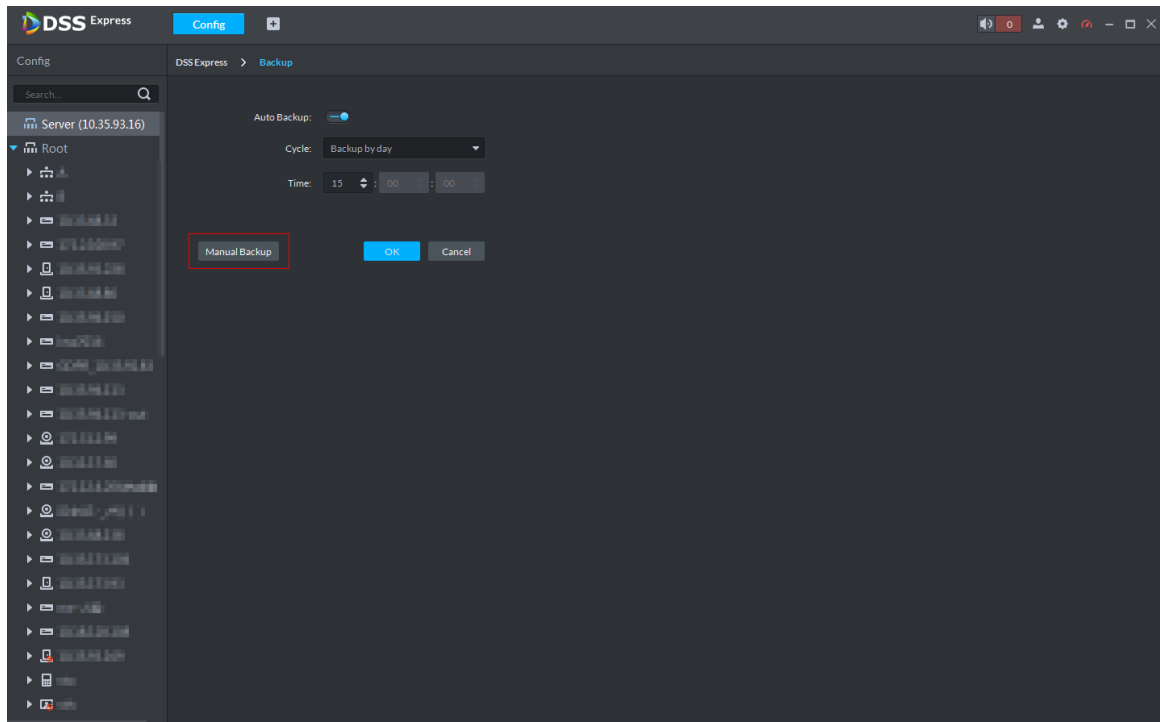
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Click **Backup**.

The system displays **Backup** interface, see Figure 4-3.

Figure 4-3 Backup



Step 3 Click Manual Backup.

The system pops up the interface of **Set Backup File Password**

Step 4 Enter file password, click **OK**.

- File password, used to guarantee backup data file security, you need to enter password for verification if you want to open or restore backup file.
- Backup file is stored under server installation path, which is “..\Server\WEBCLIENT\webclient\apache-tomcat\tmp\systemBackup”.

4.1.2 Restore

You can restore the system and data back to the latest backup time during database exception. The system can be quickly recovered and lower user loss.



Other users cannot operate the system when restoring the database. The data information will change after being restored, please operate with care.

4.1.2.1 Restoring Local File

Local file restoration is to restore manually backup file to server.

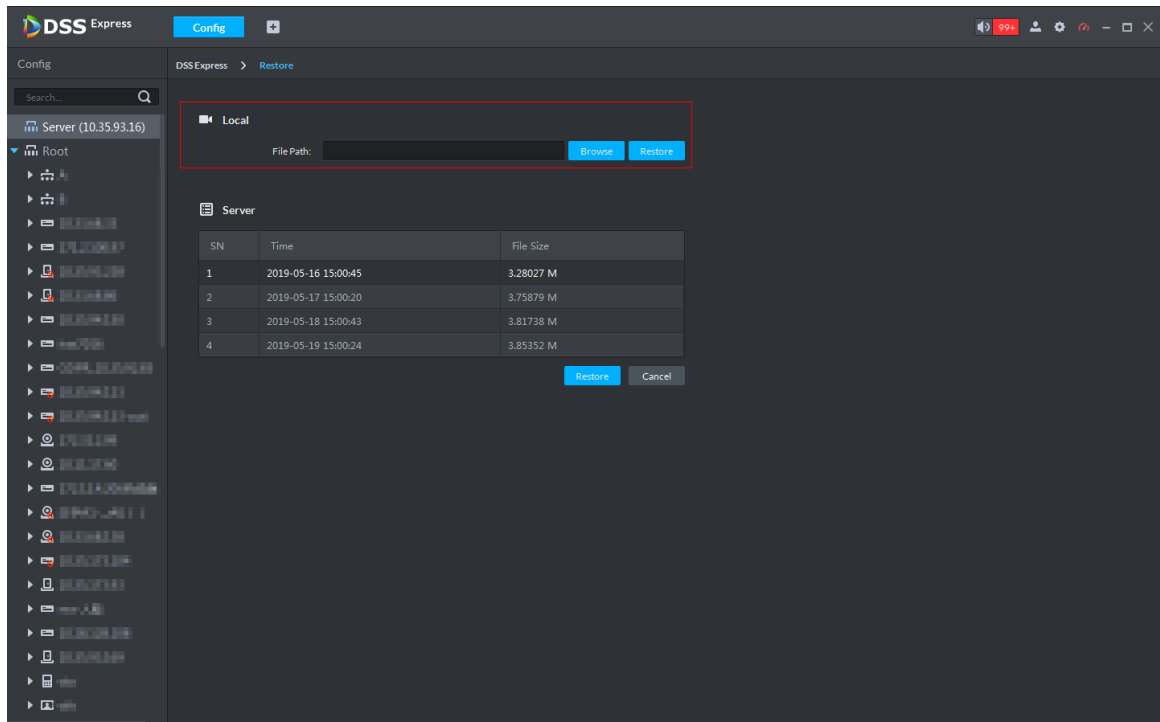
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Click **Restore**.

The system displays **Restore** interface, see Figure 4-4.

Figure 4-4 Local



Step 3 Click **Browse** and select backup data file.

Step 4 Click **Restore**.

The system pops out **Restore** box.

Step 5 Enter administrator login password and file password, click **OK**.

The system displays restoration progress, and the system will prompt restored successfully on the lower right corner.

4.1.2.2 Restoring Server File

Restore data from backup file of server, the backup file on server is automatically backed up from system.

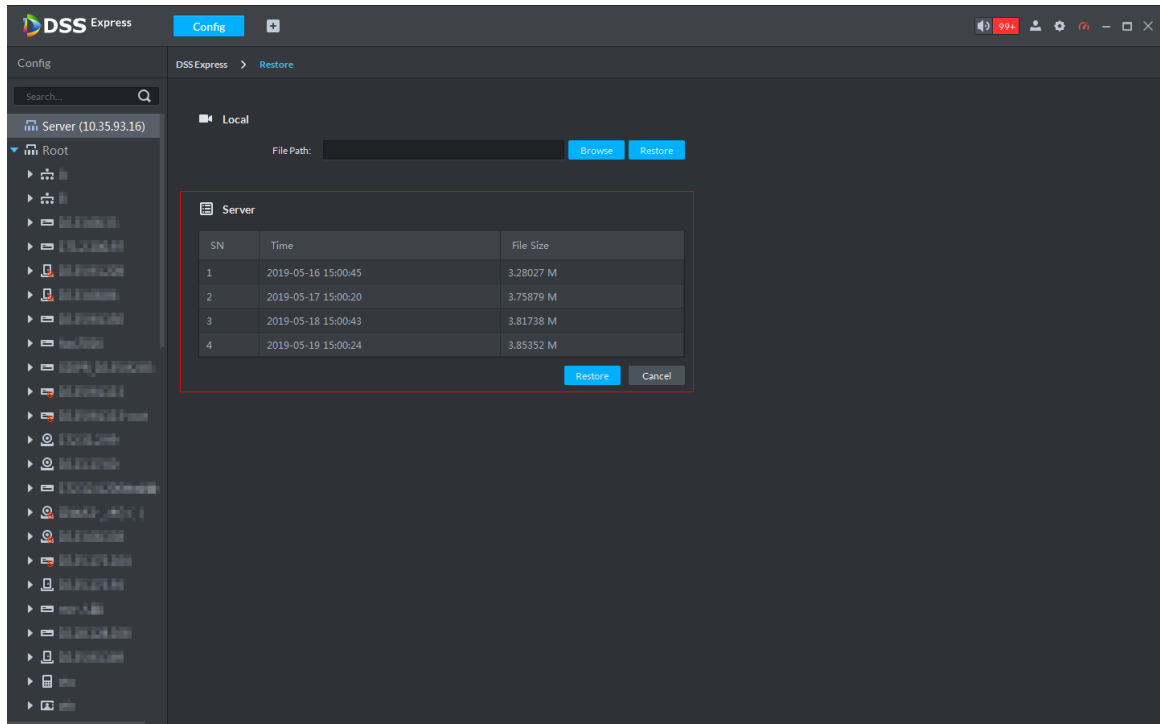
Step 1 On client homepage, click **Config**.

The system displays **Config** interface.

Step 2 Click **Restore**.

The system displays **Restore** interface, see Figure 4-5.

Figure 4-5 Restore server file



Step 3 Select backup file from server, click **Restore**.

The system pops out prompt box.

Step 4 Enter administrator login password and file password, click **OK**.

The system displays restoration progress; the system will prompt restored successfully on lower right corner.

4.2 Update

If the platform version is too low, you can install new software version and update. Please make sure you have acquired the new program, otherwise, please contact technical support for it.



- Program name includes version number and date, please check before installation.
- Update will not cause data and config loss.
- If you modify SC service port of platform before update, when the program is updated to version 1.000.0000003, SC service port will be reset to default. Please modify port number after update is completed, make sure the the port number of platform is in accordance with that of the device.

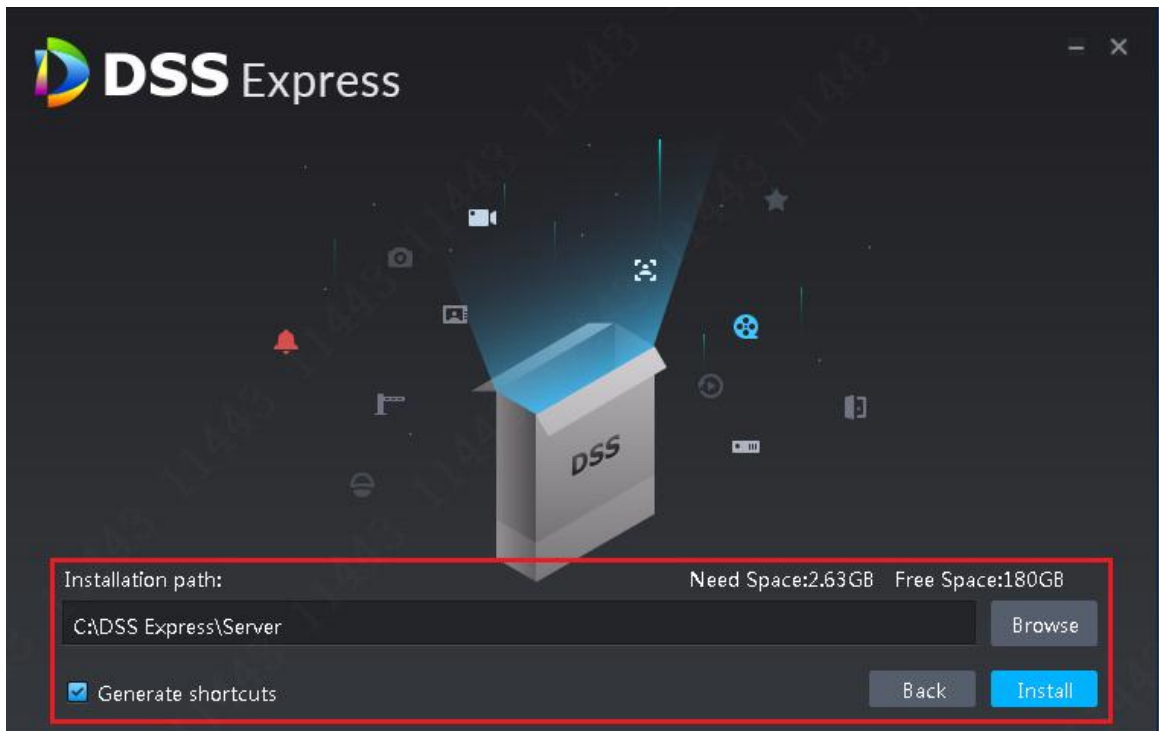
Double click installation program, install according to system prompt. For more installation requirement, please see **2.2 Installing Program (Update)**

Figure 4-6 Confirm agreement



Step 1 Select **I have read and agree the DSS agreement**, click **Next**.
The installation path interface is displayed. See Figure 4-7.

Figure 4-7 Select installation path



Step 2 Click **Browse** and select installation path, click **Install**.
The system displays installation progress, the whole installation needs 5-10 minutes.
See Figure 4-8 after installation is completed. The server starts automatically after installation.



- The system automatically detects the available space of path after the installation path is selected, if available space is less than needed for system installation, then the icon **Install** becomes gray, and installation cannot be implemented.
- Do not select **Generate Shortcuts** if it is not necessary.
- If port conflict exists, the system will prompt conflicted port during installation. Open DSS Express Server and modify port after installation is completed. See **2.3.2 Modifying Service Port** for more details.

Figure 4-8 Installation completed



4.3 Log

In log module, you can view operator log and access control device log.

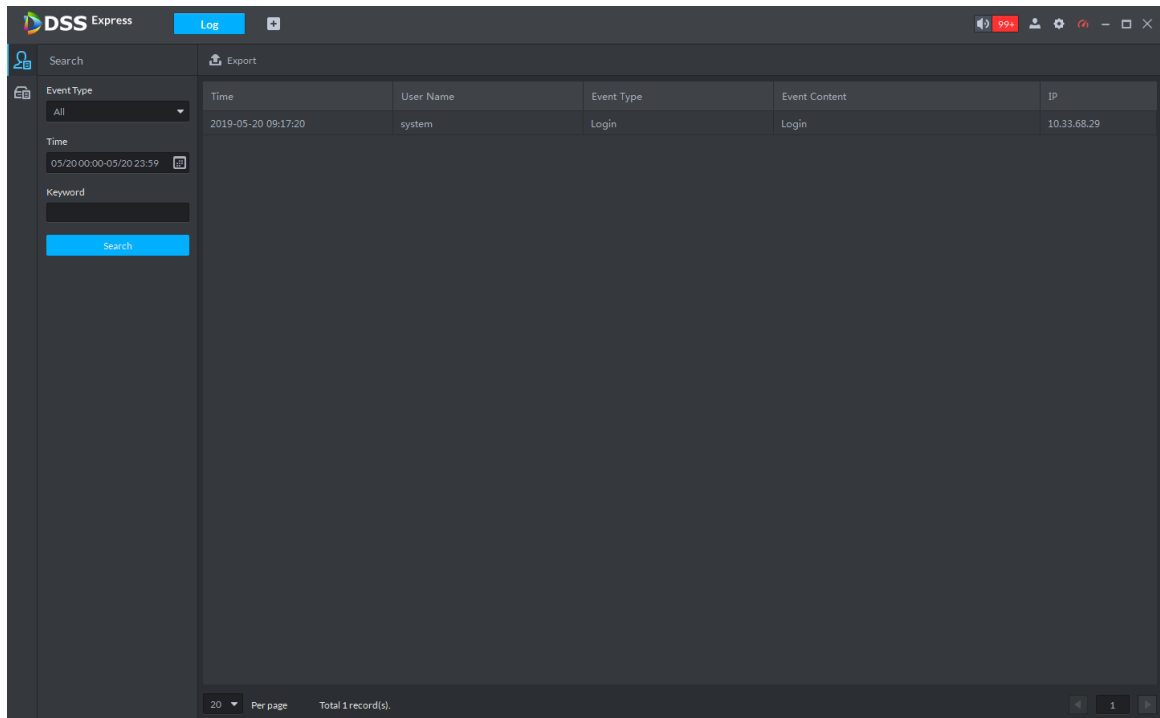
Step 1 On client homepage, click **Log**.

The system displays **Log** interface.

Step 2 Click .

The system displays **Operator Log** interface, see Figure 4-9.

Figure 4-9 Operation log



Step 3 Select event type and enter keyword, click **Search**.
The system displays results.

4.4 Password Maintenance

4.4.1 Changing Password

To make sure the account is safe, you are recommended to change login password regularly.

Step 1 After logging in client, click  on top right corner of the interface, select **Change Password**.

The system displays **Change Password** interface, see Figure 4-10.

Figure 4-10 Change password

The dialog box is titled 'Change Password' with a close button (X) in the top right corner. It contains three input fields: 'Old Password:', 'New Password:', and 'Confirm Password:'. Each field has a red dot icon on the right side, indicating password strength. At the bottom right, there are two buttons: 'OK' (highlighted in blue) and 'Cancel'.

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

4.4.2 Resetting Password

When users forget password, you can reset a new password.

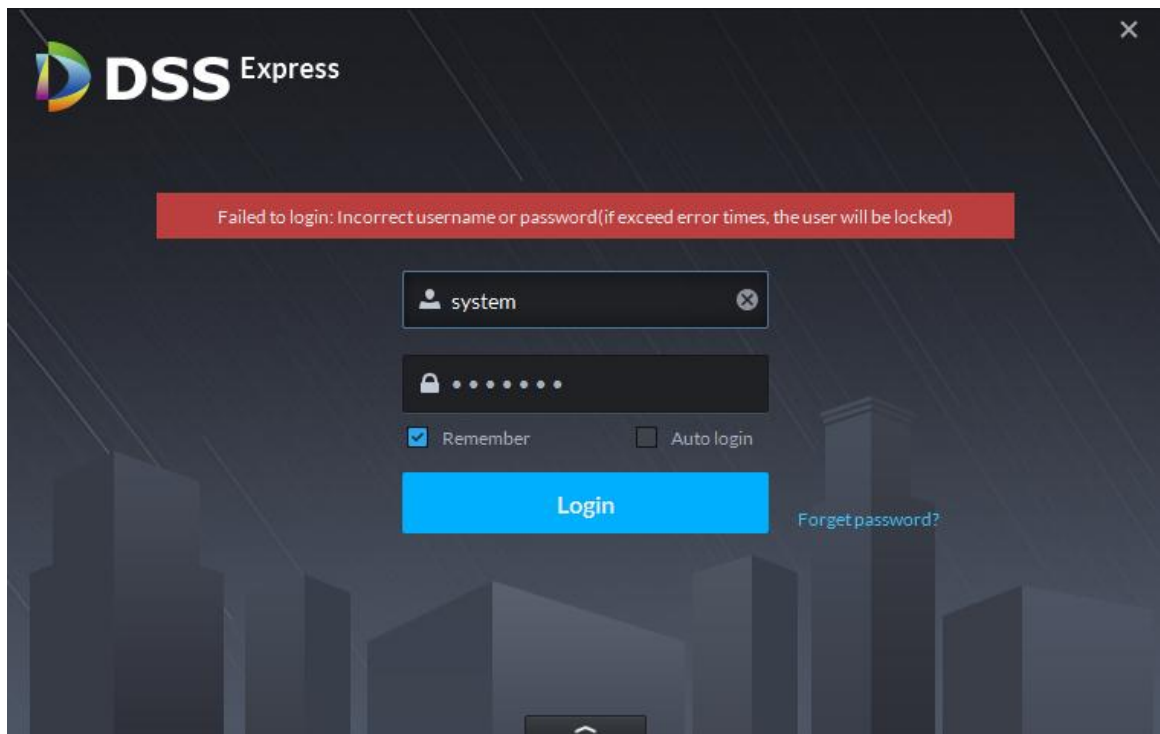
System User Password Reset

When system user forgets password, you can reset password by answering security question.

Step 1 Users forget password when logging in client, enter wrong password to log in client.

The login interface displays **Forget Password**, see Figure 4-11.

Figure 4-11 Forget password



Step 2 Click **Forget Password**.

The system displays **Security Question** interface, see Figure 4-12.

Figure 4-12 Security question

The interface is titled "Security Question" and has a close button (X) in the top right corner. It features two tabs: "1.Secure question" (active) and "2.Set password". Below the tabs, there are three questions, each with an "Answer:" label and a text input field:

- Question 1: Who is your favorite athlete?
- Question 2: Who is your favorite pop star?
- Question 3: What is your favorite flower in spring?

A "Next Step" button is located at the bottom right of the form.

Step 3 Enter answers to three questions, click **Next Step**.

The system displays **Set Password** interface.

Step 4 Enter new password, click **OK** and password is reset.

Non-system User Password Reset

When non-system user forgets password, you can only let system user set new password.

Step 1 On client homepage, click **User**.

The system displays **User** interface, see Figure 4-13.

Figure 4-13 User

The interface is titled "DSS Express" and has a "User" tab. It displays a list of roles and users on the left sidebar, including "Admin(1/4)", "system", "Asys", "dxh", "lyc", "Advanced User(0/1)", and "Normal User(0/1)". The main area shows the "Admin" role selected, with fields for "Role Name" and "Remark". Below this, there are two panels: "Device Permissions" and "Control Permissions". The "Device Permissions" panel shows a tree structure starting with "Root". The "Control Permissions" panel shows a list of permissions, including "All Permissions", "Control Permissions", "Playback video", "PTZ Control", "Voice Intercom", "Lock Record", "Record tag", "Menu Permissions", "Device", "Live View", "User", "Record Playback", "Emap", "Video Wall", "Config", "Download Center", "Event Center", and "Video Wall Config".

Step 2 Select the user you want to reset password, click .

The system displays the interface of modifying user info, see Figure 4-14.

Figure 4-14 Modify user info

The screenshot displays the 'DSS Express' application window with the 'User' tab selected. The left sidebar shows a tree view of roles and users, with 'C' under 'Normal User(0/1)' selected. The main area is titled 'Edit C' and contains two sections: 'Basic Info' and 'Device Permissions'.

Basic Info

- Username: C
- Password: [masked]
- Confirm Password: [masked]
- MAC Address: [masked]
- Password Expiry: 2019-05-20
- Email Address: [empty]
- Remark: [empty]

Device Permissions

- Root: [checked]
- Control Permissions: [checked]
- Menu Permissions: [checked]

The bottom right corner has 'OK' and 'Cancel' buttons.

Step 3 Enter password and confirm password, click **OK** and password is changed.

Appendix 1 Service Module Introduction

Service Name	Function Description	Port	Protocol Type
DSS_WEB (Center Management Service)	Center management service is to manage each service and provide accessing port.	H HTTP: 80 HTTPS: 443 CMS: 9000	TCP
DSS_MQ (Message Queue Service)	Message queue service is to transfer messages between the platforms.	61616	TCP
DSS_DMS (Device Management Service)	Device management service is to register front-end encoder, receive alarm, transfer alarm and send out sync time command.	9200	TCP
DSS_MTS (Media Transmission Service)	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
DSS_SS (Storage Service)	Storage service is to storage/search/playback record.	9320	TCP
DSS_VMS (Video Matrix Service)	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
DSS_MGW (Media Gateway Service)	Media gateway service is to send out MTS service to the decoder.	9090	TCP
DSS_PCPS (ProxyList control Proxy Service)	Login Onvif device and then get the stream and transfer the data to MTS.	SIP: 5060 REGISTER: 9550	UDP TCP

DSS_ADS (Alarm Dispatch Service)	Alarm dispatch service is to send out alarm information to different objects according to the plans.	9600	TCP
DSS_SOSO (Device Search Service)	Search devices by adding IP address	12366	TCP
DSS_SC (Video Intercom Service)	Video intercom SIP service	SIP: 5080 RTP: 554	TCP
DSS_MCDDOOR (Access Control Service)	Access control device accessed to service, interacted with access control device.	Not fixed, do not need to be mapped to the outside.	TCP

Appendix 2 Shortcut Key List

Function	Shortcut Key	Function	Shortcut Key
Wnd Move up	Up	Snap Single Wnd	P
Wnd Move down	Down	Snap pic	Ctrl+P
Wnd Move Left	Left	Local Record	Ctrl+R
Wnd Move Right	Right	Lock	Ctrl+L
Aperture-	Insert	PreSet1	1
Aperture+	Delete	PreSet2	2
Focus-	Home	PreSet3	3
Focus+	End	PreSet4	4
Wiper	PgUp	PreSet5	5
Light	PgDn	PreSet6	6
Open Single Wnd	L	PreSet7	7
Close Single Wnd	L	PreSet8	8
Open Full Screen	Ctrl+F	PreSet9	9
Close Full Screen	ESC	PreSet10	10

Appendix 3 Deleting Videos on Central Server

If you want to delete 1000001\$0 record period [2018-07-08 10:00:00 2018-07-08 10:30:00], do the following steps.

Step 1 Log in central server.

Step 2 Enter...\DSS Express\Server\SS directory, drag **.CQFSTools.exe list** file to cmd input

window, find disk uuid.

The disk info is displayed as follows:

[[Disk List]]

[Disk Path] [Target (Size) (Portal) (slot)]

D:\730c4deedd9f4f7786d49ab9e7802a7a.cqd

D:\730c4deedd9f4f7786d49ab9e7802a7a.cqd (10.00GB) () (-1)

11:32:57.355 TID 584188 [INFO] cmd[cmd.exe /c "getmac /FO

list >cqfs_tmp_584188.txt.tmp & type cqfs_tmp_584188.txt.tmp >cqf

[[CQFS List]]

[Disk Path] [CQFS UUID (Service Type) (Allocation Type)]

D:\730c4deedd9f4f7786d49ab9e7802a7a.cqd

{1bdb9a6e-41a6-4058-87ef-d944f630edf1} (1) (0)

Step 3 Search streamed.

Use tool to connect to platform database, and implement the following SQL, the searched ID field is streamed.

SELECT ID FROM adm_record_stream where DEVICE_CODE= device No. and CHANNEL_SEQ = channel No.

Step 4 Implement the command of deleClip.

.CQFSTools.exe deleteClip <streamID> <beginTS> <endTS> <diskUUID>

Appendix 4 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.