



# General Surveillance Management Center DSS7016D-S2

User's Manual

V1.0.0

Zhejiang Dahua Vision Technology Co., Ltd

# Cybersecurity Recommendations

## **Mandatory actions to be taken towards cybersecurity**

### **1. Change Passwords and Use Strong Passwords:**

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

### **2. Update Firmware**

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

## **“Nice to have” recommendations to improve your network security**

### **1. Change Passwords Regularly**

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

### **2. Change Default HTTP and TCP Ports:**

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

### **3. Enable HTTPS/SSL:**

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

### **4. Enable IP Filter:**

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

### **5. Change ONVIF Password:**

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

### **6. Forward Only Ports You Need:**

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

### **7. Disable Auto-Login on DSS:**

Those using DSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

### **8. Use a Different Username and Password for DSS:**

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

#### **9. Limit Features of Guest Accounts:**

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

#### **10. UPnP:**

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

#### **11. SNMP:**

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

#### **12. Multicast:**

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

#### **13. Check the Log:**

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

#### **14. Physically Lock Down the Device:**

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

#### **15. Connect IP Cameras to the PoE Ports on the Back of an NVR:**

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

#### **16. Isolate NVR and IP Camera Network**

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

# Regulatory Information

## FCC Information



Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

### **FCC conditions:**

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

### **FCC compliance:**

This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the guide, may cause harmful interference to radio communication.

For class A device, these limits are designed to provide reasonable protection against harmful interference in a commercial environment. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

# 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.






## Applicable Models

DHI-DSS7016D-S2, DHI-DSS7016DR-S2, DSS7016D-S2 and DSS7016DR-S2

The corresponding software version is V1.000.0000000.0.R.

## Safety Instructions

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

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

No.	Version	Revision Content	Release Time
1	V1.0.0	First release	Sep.30th. 2018

## About the Manual

The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.

We are not liable for any loss caused by the operations that do not comply with the Manual.

The Manual would be updated according to the latest laws and regulations of related regions.

For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.

All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.

There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.

Upgrade the reader software or try other mainstream reader software if the 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

<b>Cybersecurity Recommendations .....</b>	<b>I</b>
<b>Regulatory Information.....</b>	<b>III</b>
<b>Foreword .....</b>	<b>IV</b>
<b>1 Overview.....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 Highlights .....	1
<b>2 Business Flow Chart.....</b>	<b>2</b>
<b>3 Configuring System Basic Info.....</b>	<b>3</b>
3.1 Logging in and Initializing Config System .....	3
3.2 Quick Guide .....	4
3.3 Segment Setup .....	9
3.4 Basic.....	10
3.4.1 Account Management.....	10
3.4.2 Maintenance .....	11
3.4.3 Time Setup.....	11
3.4.4 Route Setup.....	12
3.4.5 Ping Check.....	13
3.4.6 URL Detect .....	14
3.4.7 Log .....	15
3.5 Security Setup.....	15
3.5.1 SSH Connection Setup.....	15
3.5.2 HTTPS Setting.....	16
3.6 Self-check .....	17
3.7 System Upgrade .....	19
3.8 Advanced .....	20
3.8.1 Configuring Master/Slave .....	20
3.8.2 Configuring Hot Spare .....	21
<b>4 Manager Operations.....</b>	<b>24</b>
4.1 Initializing Password .....	24
4.2 Logging in Management .....	26
4.3 System Settings .....	27
4.3.1 Setting System Parameters.....	27
4.3.2 FTP .....	28
4.3.3 Setting Mail Server .....	29
4.4 Adding Organization.....	30
4.5 Adding Role and User .....	32
4.5.1 Adding User Role.....	32
4.5.2 Adding User .....	33
4.5.3 Setting Domain User.....	35
4.6 Adding Device .....	39
4.6.1 Adding Device Manually .....	39



4.6.2 Searching Added Device .....	42
4.6.3 Editing Device .....	43
4.6.4 Binding Resource .....	48
<b>4.7 Configuring Record Plan .....</b>	<b>50</b>
4.7.1 Configuring Storage Disk .....	50
4.7.2 Setting Disk Group Quota .....	52
4.7.3 Adding General Plan .....	54
4.7.4 Adding Backup Record Plan .....	56
4.7.5 Adding Time Template .....	58
<b>4.8 Configuring Event .....</b>	<b>60</b>
4.8.1 Configuring Alarm Source .....	60
4.8.2 Adding Alarm Scheme .....	61
<b>4.9 Configuring Map .....</b>	<b>70</b>
4.9.1 Editing Google Map .....	70
4.9.2 Adding Hot Zone .....	72
4.9.3 Marking Device .....	75
<b>4.10 Adding Video Wall .....</b>	<b>76</b>
<b>4.11 Configuring Face Recognition .....</b>	<b>78</b>
4.11.1 Creating Face Database .....	78
4.11.2 Arm Config .....	84
<b>4.12 Adding Vehicle Blacklist .....</b>	<b>87</b>
<b>4.13 System Maintenance .....</b>	<b>89</b>
4.13.1 Service Management .....	89
4.13.2 Backup and Restore .....	90
4.13.3 Log .....	96
4.13.4 System Dashboard .....	97
<b>5 Client Functions .....</b>	<b>104</b>
<b>5.1 Installation and Login of the Client .....</b>	<b>104</b>
5.1.1 PC Requirements .....	104
5.1.2 Download and Installation .....	104
5.1.3 Login Client .....	107
<b>5.2 Local Configuration .....</b>	<b>110</b>
<b>5.3 Video Preview .....</b>	<b>116</b>
5.3.1 Preparations .....	116
5.3.2 Real-Time Preview .....	117
5.3.3 PTZ .....	122
5.3.4 Smart Track .....	128
5.3.5 View Tour .....	131
5.3.6 Region of Interest (RoI) .....	133
<b>5.4 Record .....</b>	<b>134</b>
5.4.1 Preparations .....	134
5.4.2 Recording when Previewing .....	135
5.4.3 Playback .....	136
5.4.4 Download .....	141
<b>5.5 Event Center .....</b>	<b>145</b>
5.5.1 Preparations .....	145
5.5.2 Configuring Alarm Parameters .....	146

5.5.3 Searching and then Processing Real-Time Alarm .....	147
<b>5.6 Video Wall .....</b>	<b>151</b>
5.6.1 Preparations .....	151
5.6.2 Output to the Wall .....	152
5.6.3 Video Wall Plan.....	154
<b>5.7 Emap .....</b>	<b>157</b>
5.7.1 Preparations .....	157
5.7.2 Open Emap on the Real-Time Preview .....	158
5.7.3 Viewing Map .....	160
5.7.4 Alarm Flashing on the Map.....	162
<b>5.8 People Counting.....</b>	<b>164</b>
5.8.1 Preparations .....	164
5.8.2 People Counting Report .....	165
5.8.3 Viewing People Counting Statistics on Live View Interface .....	166
5.8.4 Heatmap .....	167
<b>5.9 Human Face Recognition .....</b>	<b>168</b>
5.9.1 Preparations .....	168
5.9.2 Real-Time Human Face Video .....	169
5.9.3 Searching Snapshot Images .....	171
5.9.4 Searching on the Snapshot Database.....	172
5.9.5 Statistics Report.....	174
<b>5.10 License Plate Recognition .....</b>	<b>176</b>
5.10.1 Preparations .....	176
5.10.2 Road Monitor .....	176
5.10.3 Searching Passed Vehicle.....	178
5.10.4 Vehicle Track .....	181
5.10.5 Monitor Place.....	184
<b>5.11 Time Synchronization.....</b>	<b>187</b>
5.11.1 Device Time Synchronization .....	187
5.11.2 Time Synchronization on the Client .....	188
<b>Appendix 1 Service Module Introduction .....</b>	<b>191</b>

## 1.1 Introduction



DSS general surveillance management center (Hereinafter referred to as “DSS Platform”) is a type of comprehensive monitoring management platform based on Linux system with powerful functions; it is installed with Linux DSS Pro software and able to meet the requirements of large and medium-sized projects via distributed extension performance. It supports max 2000 channels video access and expands max 15 3.5-inch hot swap harddrive as central storage. Equipped with advanced functions such as face recognition, LPR and people counting, it provides an integrated solution with high performance for customers.

## 1.2 Highlights

- High scalability
  - ◇ Supports distributed expansion system performance.
  - ◇ Supports IPSAN expansion center storage.
- High reliability
  - ◇ Supports dual hot spare, makes DSS system more stable.
  - ◇ Supports system data auto backup and manual backup, reduce loss caused by system crash.
- More open
  - ◇ Supports standard Onvif protocol connecting to third-party devices.
  - ◇ Open SDK, the third party platform can be connected via SDK.

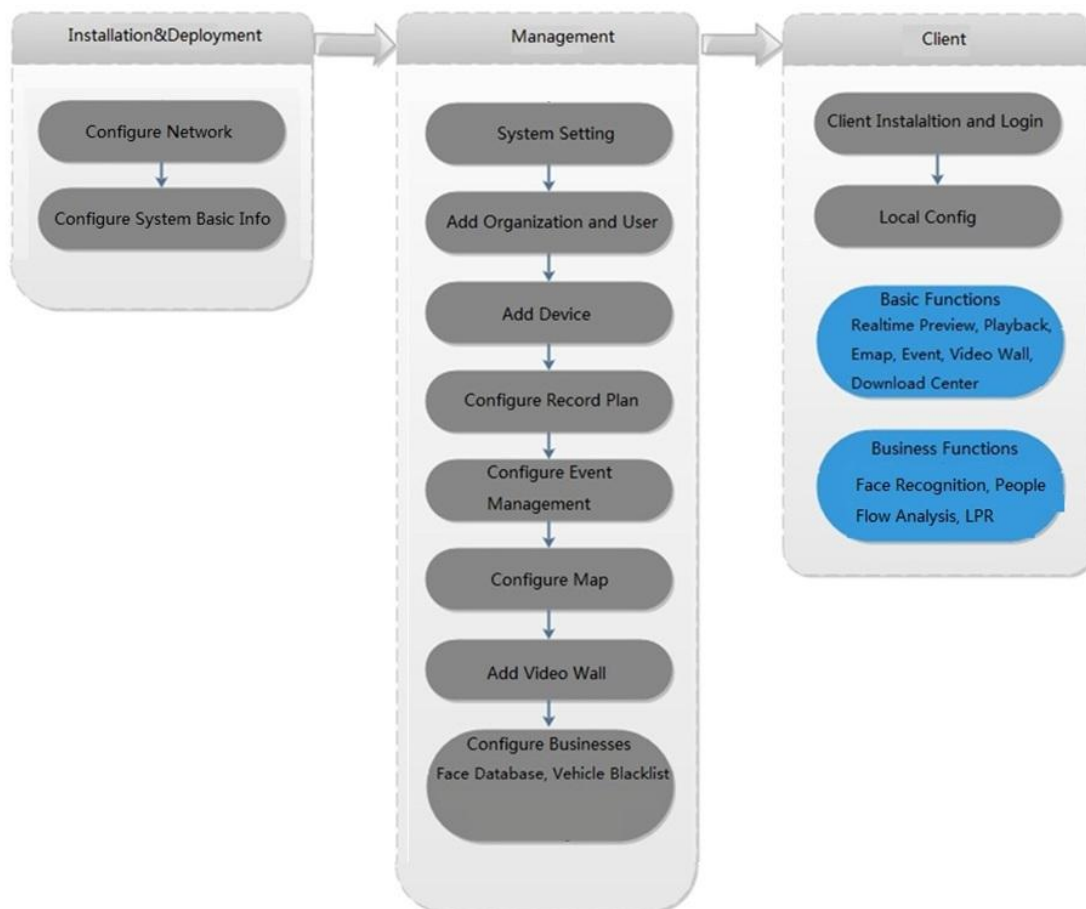
# 2 Business Flow Chart



In the business flow chart,  shading means config item,  shading means the exact application of business in the client.

The overall flow chart is shown in Figure 2-1.

Figure 2-1



# 3

## Configuring System Basic Info

The config system is used to quickly configure network parameters, basic parameters, safety parameters, hot standby etc. of general monitoring management center all-in-one device, as well as system upgrade and self-check.



Please make sure that the device installation and deployment has been completed before logging into the config system. For detailed deployment process, please refer to *DSS General Surveillance Management Center Applications and Deployment Guide* for more details.

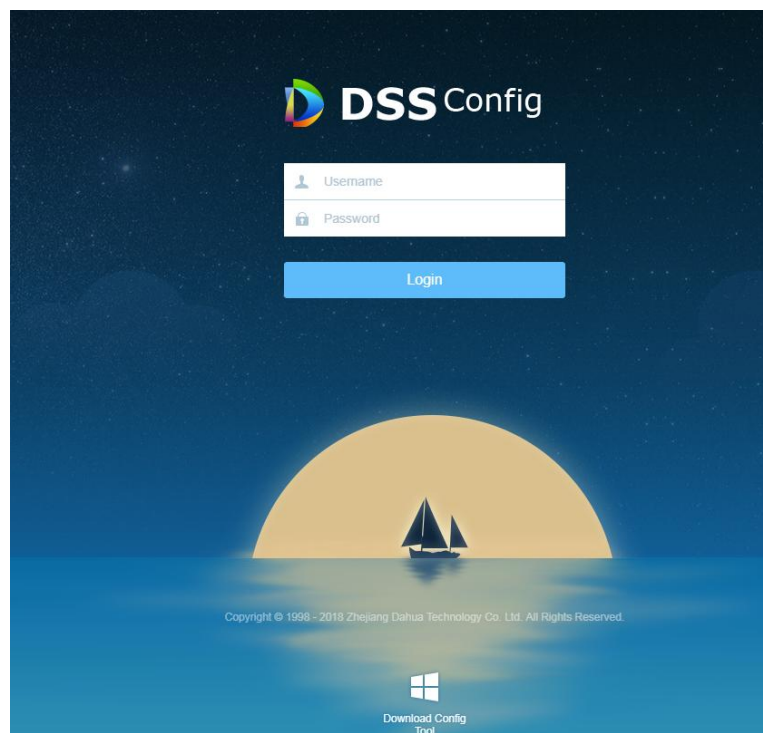
### 3.1 Logging in and Initializing Config System



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

**Step 1** Enter “DSS platform IP address/config” into the browser, press Enter button. The “Config System” interface is displayed. See Figure 3-1.

Figure 3-1



**Step 2** Enter user name and password (Default user name is admin, default password is 123456), click “Login”. The reset password interface is displayed. See Figure 3-2.

Figure 3-2

Reset Password

**Reset Password**

Old Password:

New Password:

Confirm:

**Security Question**

Security Question 1:  ▼

Answer:

Security Question 2:  ▼

Answer:

Security Question 3:  ▼

Answer:

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

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

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

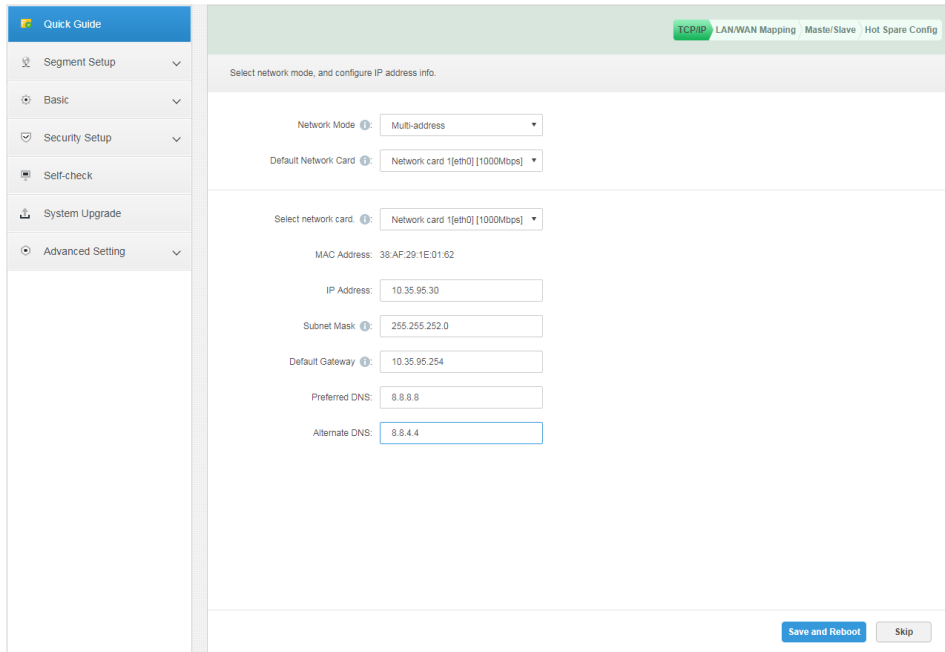
## 3.2 Quick Guide

Users can quickly configure the platform’s network, LAN/WAN network mapping and hot standby via quick guide.

**Step 1** Log in config system.

**Step 2** Click “Quick Guide”. The “Network Card Config” interface is displayed. See Figure 3-3.

Figure 3-3



**Step 3** Configure parameters of network card; please refer to Table 3-1 for more details.

Table 3-1

Parameter	Note
Network Mode	<ul style="list-style-type: none"> <li> <b>Multi-address</b>                      It is multi-network card mode, which can configure different network segments, realize multi network segment access and apply to the scenario with high requirements for network reliability. For example, configure double hot standby, it needs to use network card 2 to configure standby heartbeat IP; it can also be used in scenarios with iSCSI extended storage. The network port is planned as follows: network port 1 is used to service communication, network port 2 is reserved, and network port 3 and 4 are used for iSCSI storage.                 </li> <li> <b>Fault tolerance</b>                      Multiple network cards use one IP address, normally there is only one network card is working. When the working network card fails, a normal network card is automatically activated to ensure network smoothness.                 </li> <li> <b>Load Balance</b>                      Several network cards use one IP address, these network cards work together and share network load, provide network load capacity over the bandwidth of a single network card. When a network card becomes abnormal, the load is redistributed to other available network cards to provide network reliability.                 </li> </ul>

	<ul style="list-style-type: none"> <li>• Link aggregation</li> </ul> <p>Through network card binding and external communication, all the bound network ports participate in the work and share the network load. It can realize a network card forwarding greater than 1K stream; for example: 2 IP bound, another 2 multi-address, than there are 3 IP for the server, the bandwidth of bound IP is 2K and the other 2 is 1K; It can be applied to the scenario of pure forward code stream (Storage is not recommended).</p>
Add Bound Network Card	<p>It needs to set network card binding when network mode is set as fault tolerance, load balancing or link aggregation.</p> <p>Click “Add Bound Network Card”, select the network cards which need to be bound, users can set two bound network cards.</p>
Default Network Card	<p>Selects default network card, the network card will forward data package of non-adjacent network segment as default port (such as external network and public network)</p>
Select Network Card	<p>After selecting network card or binding network card, it will display the info of the network card or bound network card below.</p>
MAC Address	<p>It displays the MAC address of platform server.</p>
IP Address	<p>After selecting network card, you can set IP address, subnet mask, default gateway, preferred DNS server address and alternate DNS server address.</p>
Subnet Mask	
Default Gateway	
Preferred DNS	
Alternate DNS	

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

Step 5 After server restarts, use “DSS Platform IP Address/Config” to visit config system again.

The IP address has been configured.

Step 6 Click “Quick Guide” and click “Skip”.

The system will display the interface of “LAN/WAN Mapping”. See Figure 3-4.



Figure 3-4

The screenshot shows a configuration page for LAN/WAN Mapping. On the left is a navigation menu with options: Quick Guide, Segment Setup, Basic, Security Setup, Self-check, System Upgrade, and Advanced Setting. The main content area has a breadcrumb trail: TCP/IP > LAN/WAN Mapping > Master/Slave > Hot Spare Config. A note at the top states: "If the system visits WAN via internal and external mapping of router, then you need to fill in WAN address and port information. If no port mapping, then you do not need to change port setup. (The MQ ports of the internal and external networks need to be consistent.)".

Fields shown include:

- Local Address: 10.35.95.30
- WEB: 80
- Router Address: (empty)
- Service ports: CMS (9000), SS (9320), ARS (9500), MQ (61616), DMS (9200), ADS (9600), MGW (9090), MTS (9100), PES (9400), PTS (8081), WEB (80).

Buttons at the bottom include: Previous Step, Save and Next, and Skip.

**Step 7** Configure WAN address and port info; please refer to Table 3-2 for more details.

Table 3-2

Parameter	Note
IP Address	Sets the address of DSS platform.
Web Service Port	Default WEB service port is 80, it needs to use IP: Port to access WEB if it is not 80. For example, port 81; enter http://172.7.54.35:81/config to access config system.
Router Address	Sets WAN access IP address of router.
CMS	Center management service, which is responsible for registration and signaling scheduling of other services, it is 9010 by default.
SS	Storage playback service, which is in charge of video storage, query and playback, it is 9320 by default.
ARS	Active registration service, which is responsible for actively registering the device to monitor, log in and forward stream to MTS, it is 9500 by default.
MQ	MQ service, which is responsible for information interaction, it is 61616 by default.
DMS	Device management service, which is responsible for logging into the front-end encoder, receiving alarm, forwarding alarm and sending timing command, it is 9200 by default,
ADS	Alarm distribution service, which is responsible for sending alarm info to different objects according to the plan, it is 9600 by default.
MGW	Media gateway, which is responsible for sending MTS address to decoding device, it is 9090 by default.
WEB	Web application service, responsible for administrator config,

Parameter	Note
	providing web service interface, providing client embedded function, it is 801 by default.
MTS	Media distribution service, which is responsible for acquiring audio and video streams from front-end devices and distributing them to SS, client and decoder devices. It is 9100 by default.
PES	Power environment surveillance service, which is responsible for managing MCD (including POS, alarm host, radar, access control and so on), it is 9400 by default.
PTS	Picture transmission service, which is responsible for receiving, storing and forwarding ANPR pictures, it is 8081 by default.

**Step 8** Click “Save and Next”.

The “Server Mode” is displayed. See Figure 3-5 and Figure 3-6.

Figure 3-5

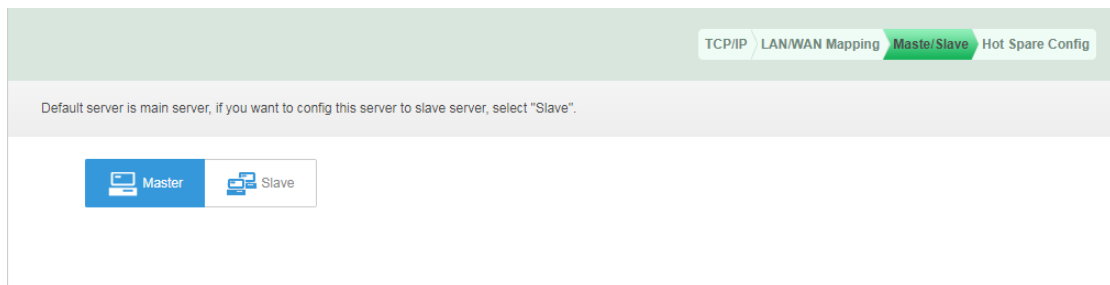
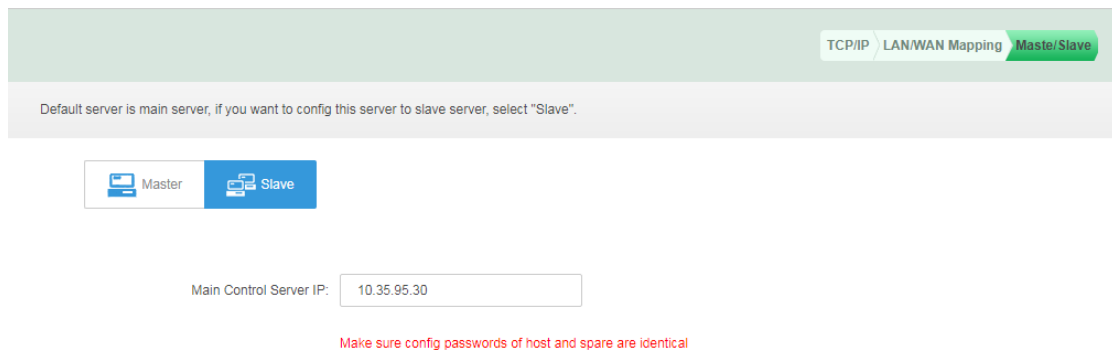


Figure 3-6



**Step 9** Configure server mode according to requirement, select “Master” or “Slave”.


**Step 10** Click “Save and Next”.

The system will display the interface of “Hot Spare”. See Figure 3-7.

Figure 3-7

**Step 11** It is to configure the parameters of hot spare server; please refer to Table 3-3 for more details

Table 3-3

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

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

### 3.3 Segment Setup

It is used to set network card and LAN/WAN mapping, please refer to “3.2 Quick Guide” for more details.

## 3.4 Basic

### 3.4.1 Account Management

It is to modify the login password of admin user.



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

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

The interface of “Manage Account” is displayed. See Figure 3-8.

Figure 3-8

Quick Guide

Segment Setup

Basic

> Manage Account

Maintenance

Time Setup

Route Setup

PING Check

URL Detect

Log

Security Setup

Self-check

System Upgrade

Advanced Setting

All services will restart after the new password is changed!

Old Username: admin

Old Password:

New Password:

Confirm:

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

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



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

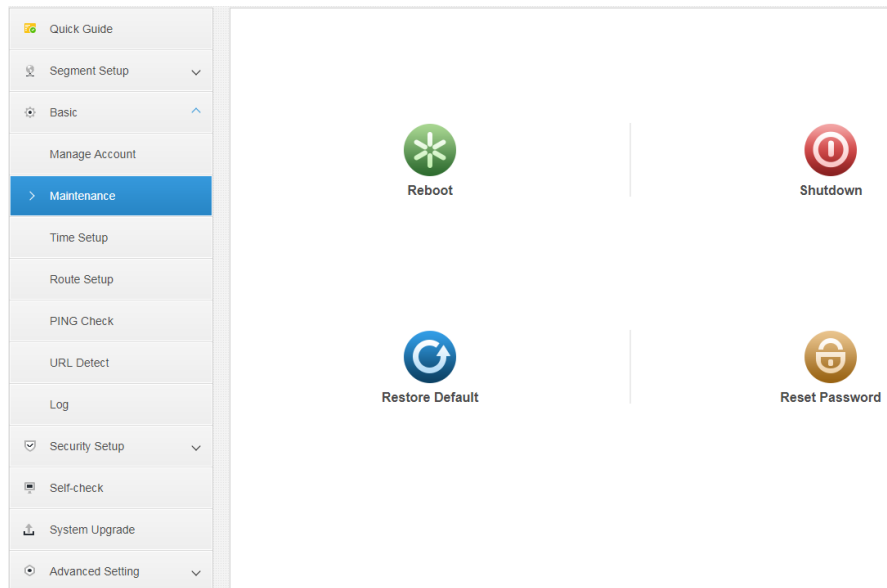
## 3.4.2 Maintenance

It is used to reboot device, shutdown and restore device to default status. It can also reset password.

**Step 1** Select “Basic > Maintenance”.

The “Maintenance” interface is displayed. See Figure 3-9.

Figure 3-9



**Step 2** Click relevant operation to realize corresponding functions.

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

## 3.4.3 Time Setup

It is to set the time zone and time of the server’s location.



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

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

The “Time Setup” interface is displayed. See Figure 3-10.

Figure 3-10

Configure time zone and time, you also can sync time via NTP server. When the servers or devices of different time zones sync time, it will only sync time, and original time zones of the servers and devices will not be changed.

DST:

Time Zone: (UTC)Monrovia, Reykjavik, Co...

Date/Time: 2018-08-26 08:56:50

NTP Setup:

NTP Server: 8.8.8.8

Update Period: 60 Minute(60-65535)

**Step 2** It is to configure time parameters, please refer to Table 3-4 for more details.

Table 3-4

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

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

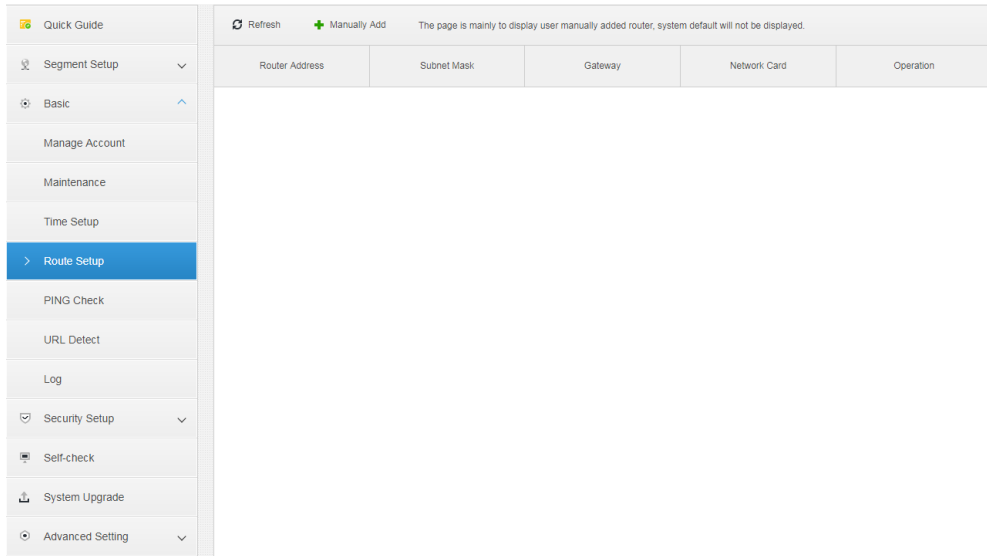
### 3.4.4 Route Setup

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

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

The “Route Setup” interface is displayed. See Figure 3-11.

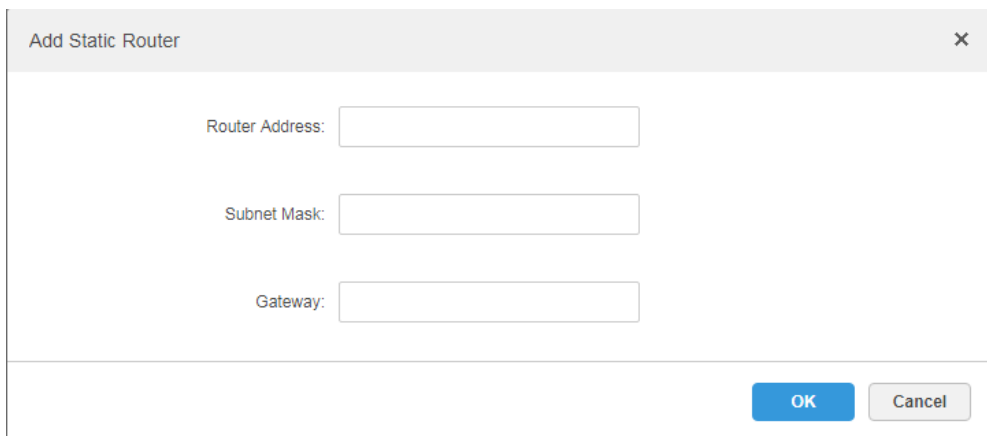
Figure 3-11



**Step 2** Click “Manually Add”.

The “Add Static Router” interface is displayed. See Figure 3-12.

Figure 3-12



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

**Step 4** Click “OK”.

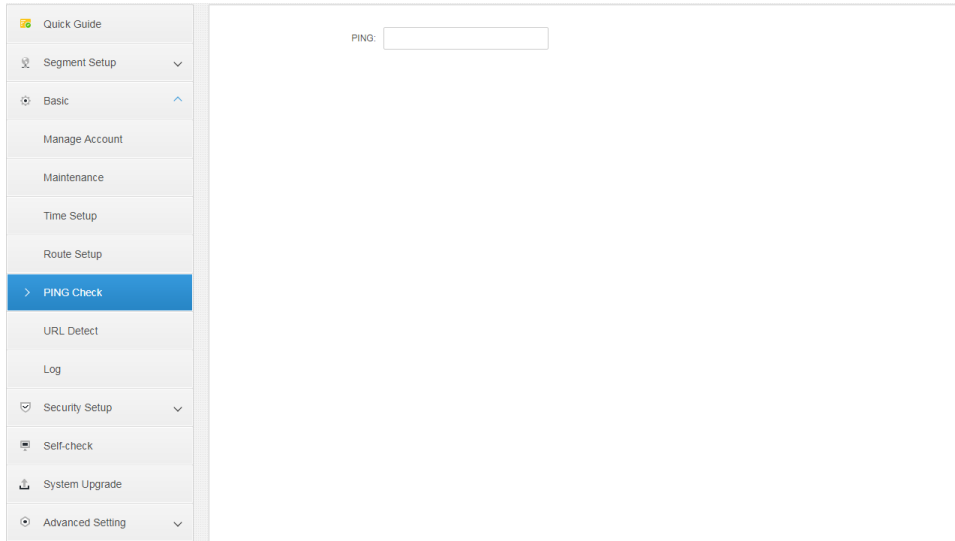
### 3.4.5 Ping Check

It is to check if the platform is interconnected with IP network.

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

The “Ping Check” interface is displayed. See Figure 3-13.

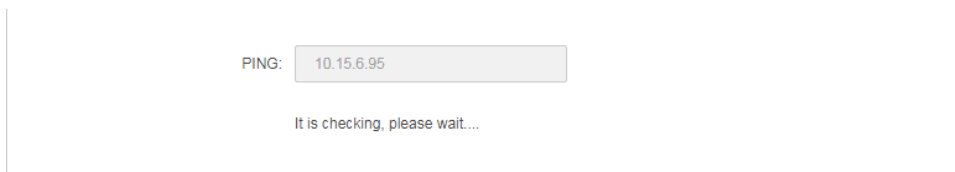
Figure 3-13



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

Then it starts to check if the platform and IP address are interconnected. See Figure 3-14.

Figure 3-14



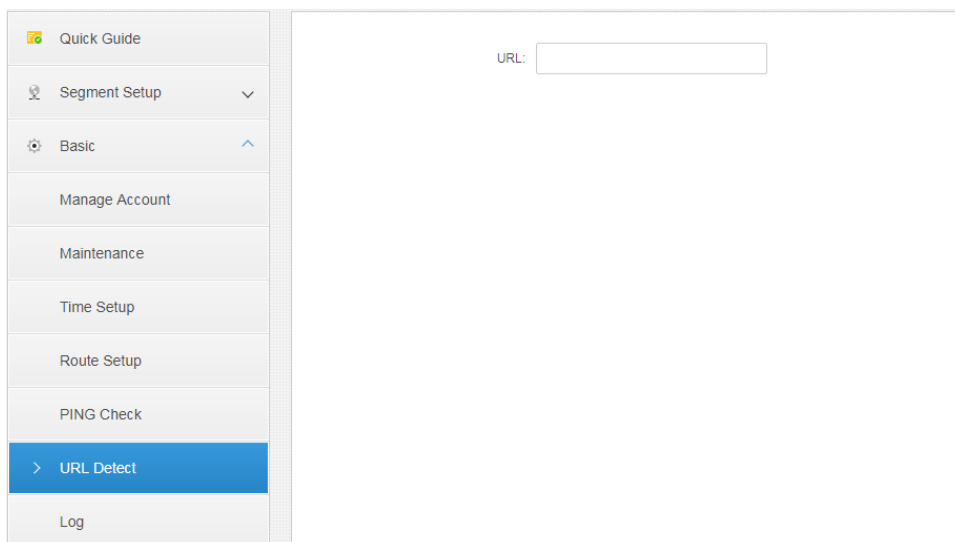
### 3.4.6 URL Detect

It is to test if the platform is interconnected with URL address network.

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

The interface of “URL Detect” is displayed. See Figure 3-15.

Figure 3-15



**Step 2** Enter URL address, click “Apply”.

Then it starts to detect if the platform is interconnected with the URL address.



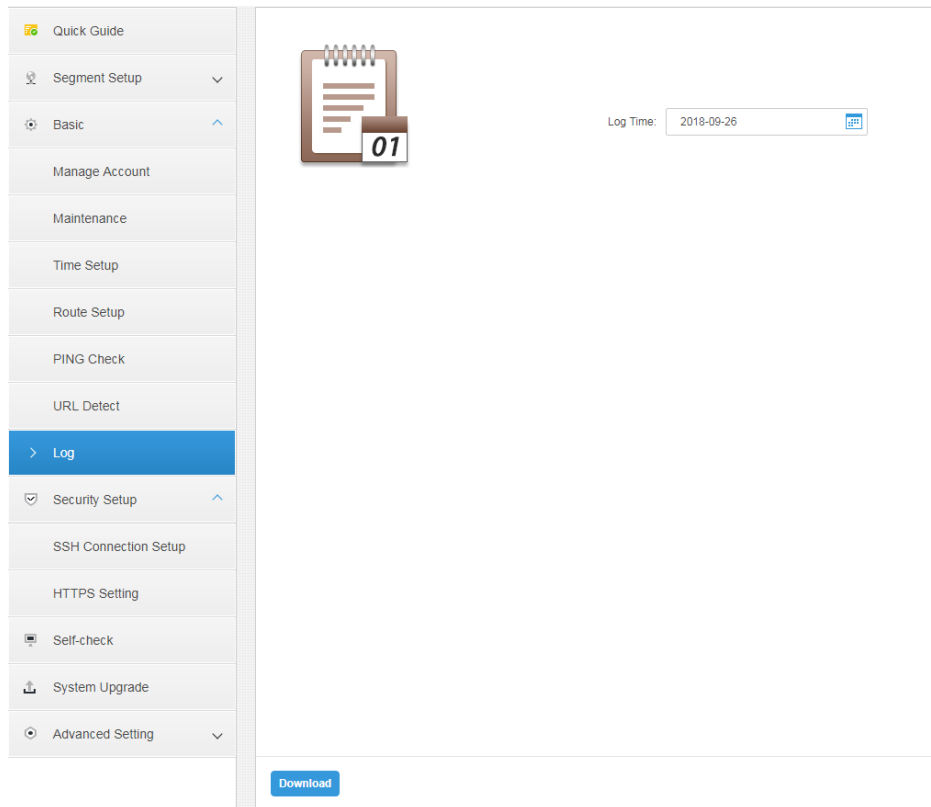
## 3.4.7 Log

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

**Step 1** Click “Log”.

The “Log” interface is displayed. See Figure 3-16

Figure 3-16



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

## 3.5 Security Setup

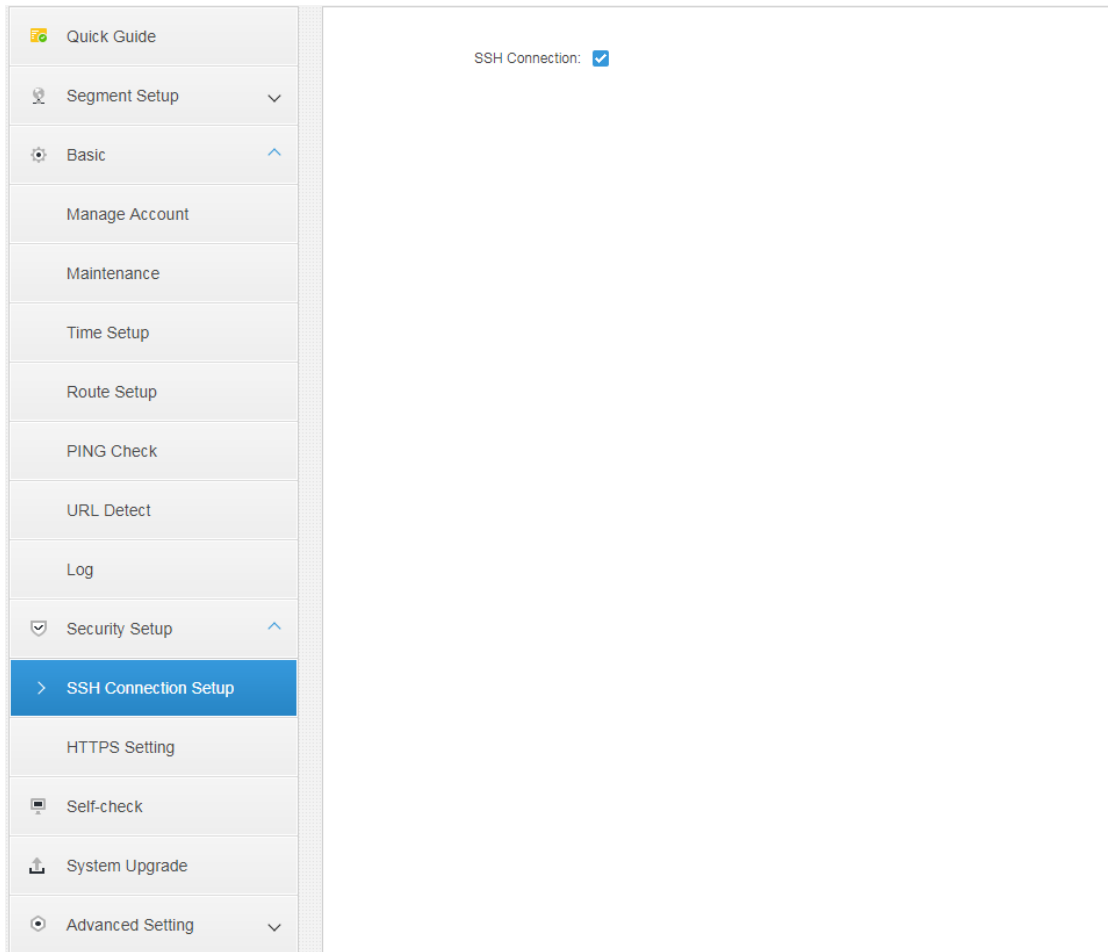
### 3.5.1 SSH Connection Setup

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

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

The interface of “SSH Connection Setup” is displayed. See Figure 3-17.

Figure 3-17



**Step 2** Select “SSH Connection”.

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

### 3.5.2 HTTPS Setting

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

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

The interface of “HTTPS Setting” is displayed. See Figure 3-18.

Figure 3-18

Port:

Import Certificate:

Password:

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



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

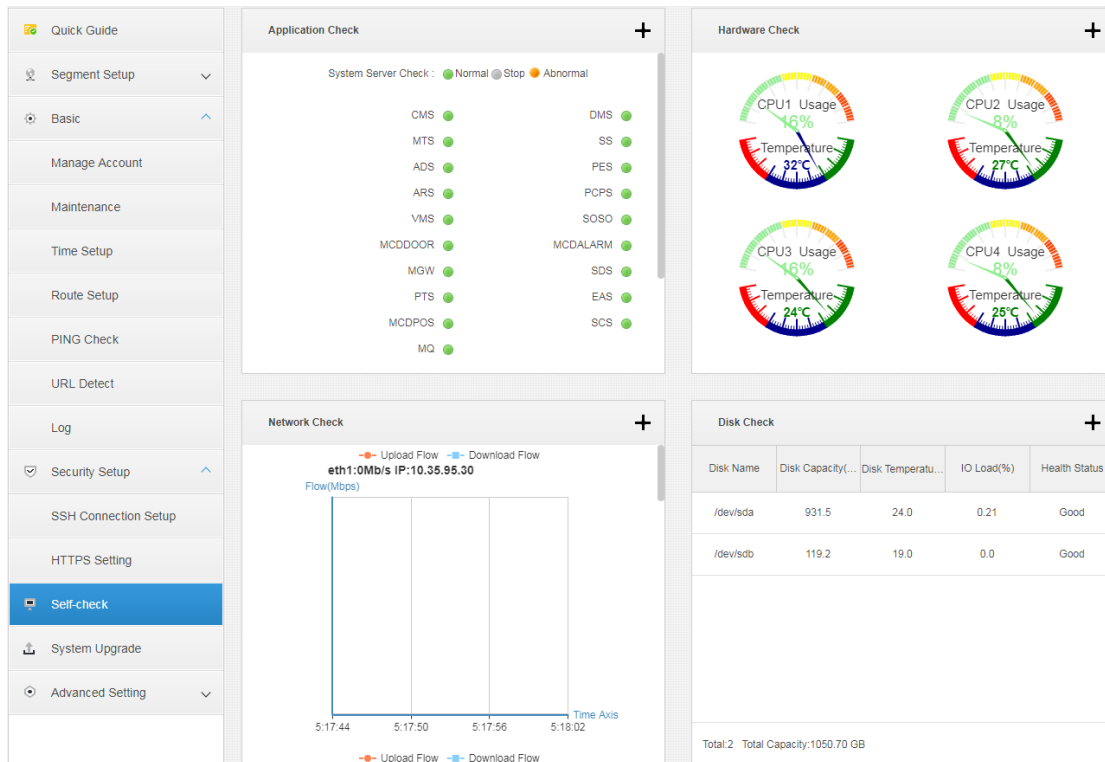
**Step 3** Click “Apply” to complete setting.

## 3.6 Self-check

It is to check the detection results of background application, CPU module, network and disk etc.

- Click “Self-check” and the system will display the interface of self-check result. See Figure 3-19.

Figure 3-19




Click the “+” on the upper right corner of each module or click the icon  on the top left corner of the interface, and then the detection result interface is displayed. See Figure 3-20, Figure 3-21, Figure 3-22 and Figure 3-23.

Figure 3-20

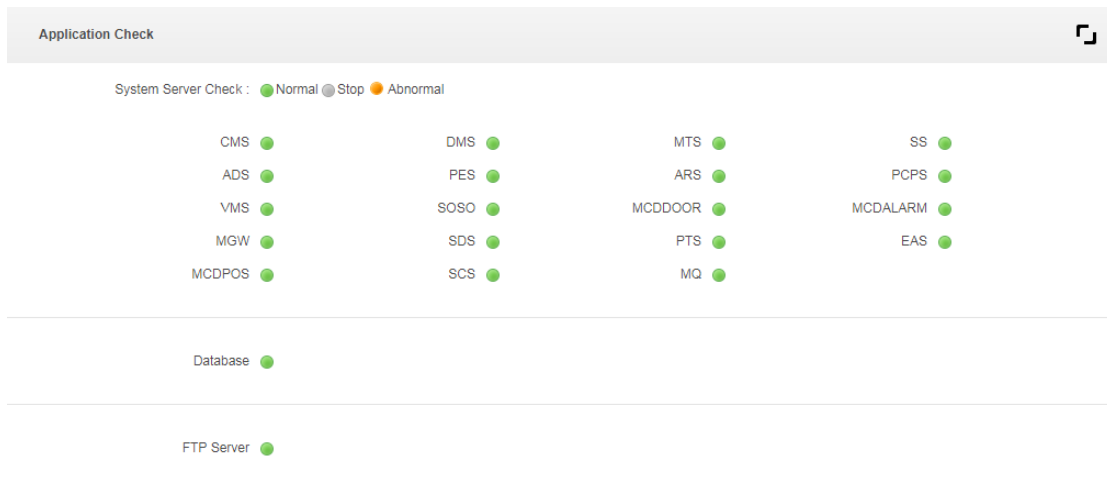


Figure 3-21

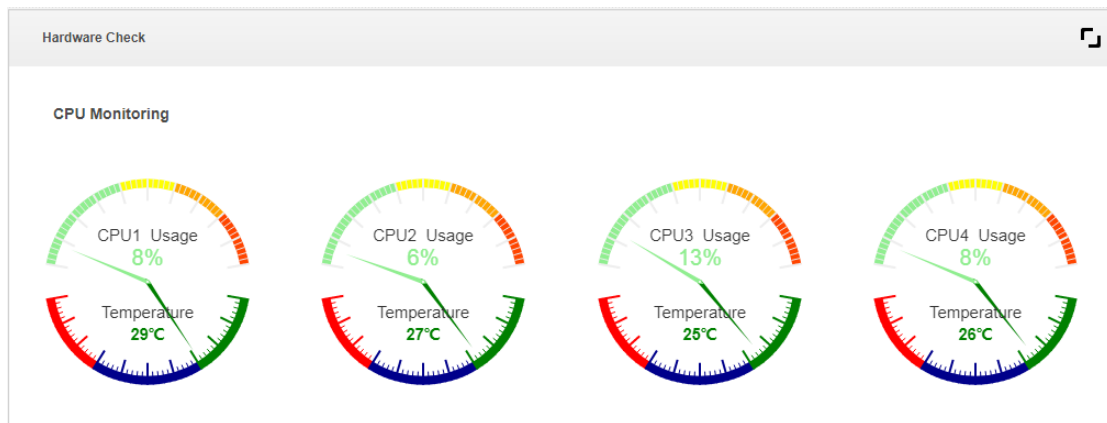


Figure 3-22

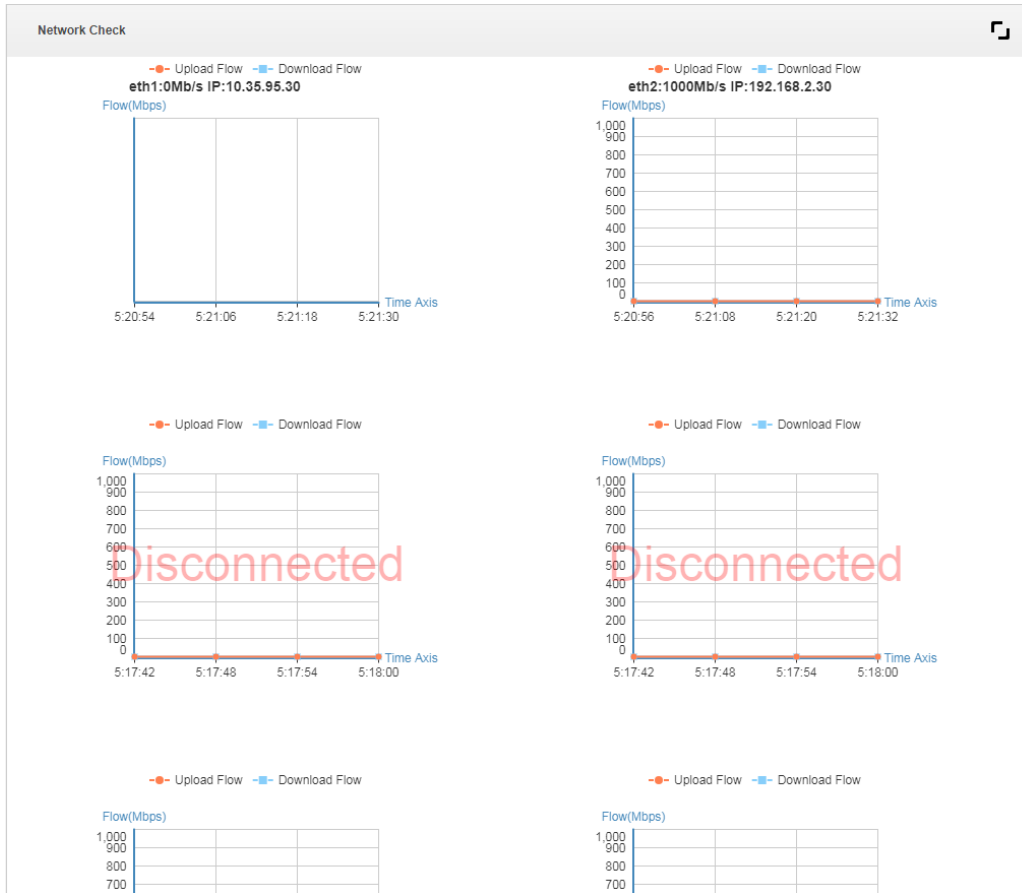


Figure 3-23

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

## 3.7 System Upgrade

The system supports upgrade via WEB one click, meanwhile it is compatible with upgrade tool and upgrade mode.



Users can choose Config Tool to upgrade system as well; it needs to pay attention to the following info.

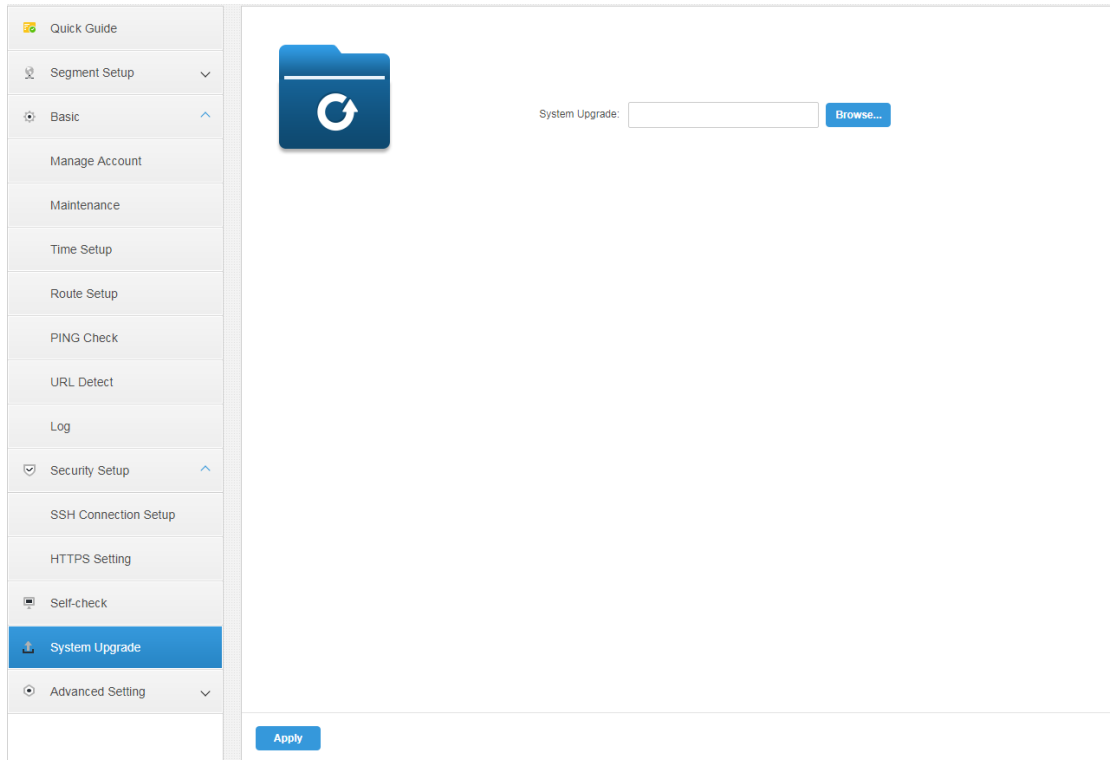
- When using Config Tool to upgrade, enter platform IP address, the username and password are the ones of login config system, and the port is 3800.
- Config Tool can be downloaded by clicking “Config Tool Download” on the login interface.

It is to take WEB one click upgrade as an example to introduce in the following chapter.

**Step 1** Click “System Upgrade”.

The system will display the upgrade interface. See Figure 3-24.

Figure 3-24



**Step 2** Click “Browse” and select upgrade package (.bin).

**Step 3** Click “Apply” and the system starts to upgrade.

## 3.8 Advanced

### 3.8.1 Configuring Master/Slave

Please set master and slave mode according to actual situation if it follows distributed deployment server.

**Step 1** Select “Advanced > Server Mode”.

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

The interface is shown in Figure 3-25 and Figure 3-26.

Figure 3-25

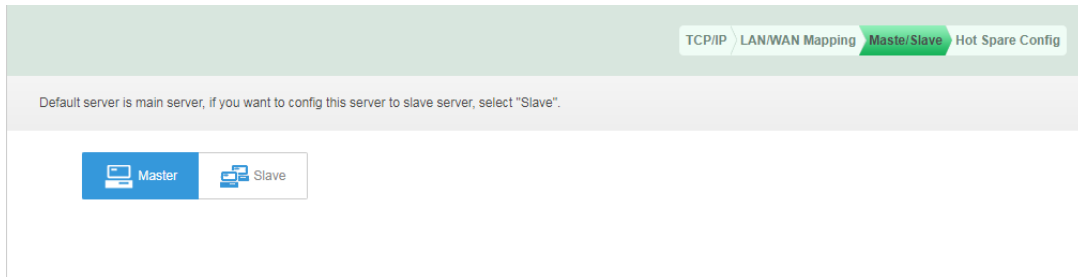
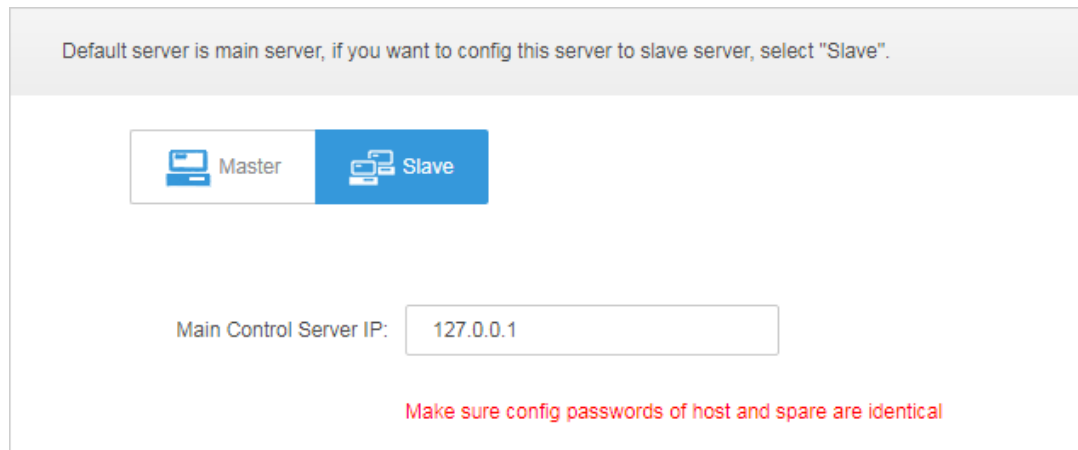


Figure 3-26



Step 3 Click “Apply”.

## 3.8.2 Configuring Hot Spare

Generally the application scene of dual hot spare is the central platform of surveillance, which cannot be stored as video. When one machine breaks down, the other machine will replace it.

### Preparation before Operation

- Physical Cable Connection

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

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

- Time Sync



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

- Attention

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

### **Operation Steps**

Step 1 Select “Advanced > Hot Spare”.

The “Hot Spare” interface is displayed. See Figure 3-27.



Figure 3-27

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

Virtual IP:

Mask:

Spare IP:

Spare beat IP:

Spare config username:


Spare config password:

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

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

**Step 2** It is to configure the parameters of hot spare server. Please refer to Table 3-5 for more details.

Table 3-5

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

**Step 3** Click “Execute Dual Host Spare” to enable the function of dual hot spare. Please click “Remove Hot Spare” if it needs to disable hot spare.

# 4 Manager Operations

It needs to use Internet Explorer 9 or higher version browser to log in DSS platform, or you can use Google Chrome and Firefox as well.

## 4.1 Initializing Password

Step 1 Enter platform IP address in the browser, press **【Enter】** .  
The system will display the login interface. See Figure 4-1.

Figure 4-1



Step 2 Enter username and password (default username is system, default password is 123456), click “Login”.



Please add the platform IP address into the browser’s trusted sites if it is your first time to log in the DSS manager.

If it is the first time to log in the system, the system will pop out the interface of modifying password. Users can continue to log in the system after modifying the password. The interface is show in Figure 4-2.

Figure 4-2

The screenshot shows a web interface titled "Change Password". At the top, there are two progress indicators: "1. Change Password" (highlighted in green) and "2. Security Question". Below this, the "Username" is set to "system". There are two input fields: "New Password:" and "Confirm:", both with a red asterisk indicating a required field. A blue "Next" button is located at the bottom right of the form area.

**Step 3** Enter “New Password” and “Confirm Password”, click “Next”.  
The interface is shown in Figure 4-3.

Figure 4-3

The screenshot shows the same "Change Password" interface, but now at step 2. The progress indicators are "1. Change Password" and "2. Security Question" (highlighted in green). There are three security questions, each with a dropdown menu and an "Answer" input field with a red asterisk. The questions are: "Who is your favorite athlete?", "Who is your favorite pop star?", and "What is your favorite flower in ...". At the bottom right, there are two buttons: a grey "Back" button and a blue "OK" button.

**Step 4** Click “OK” after setting security questions.  
The system will display the login interface.

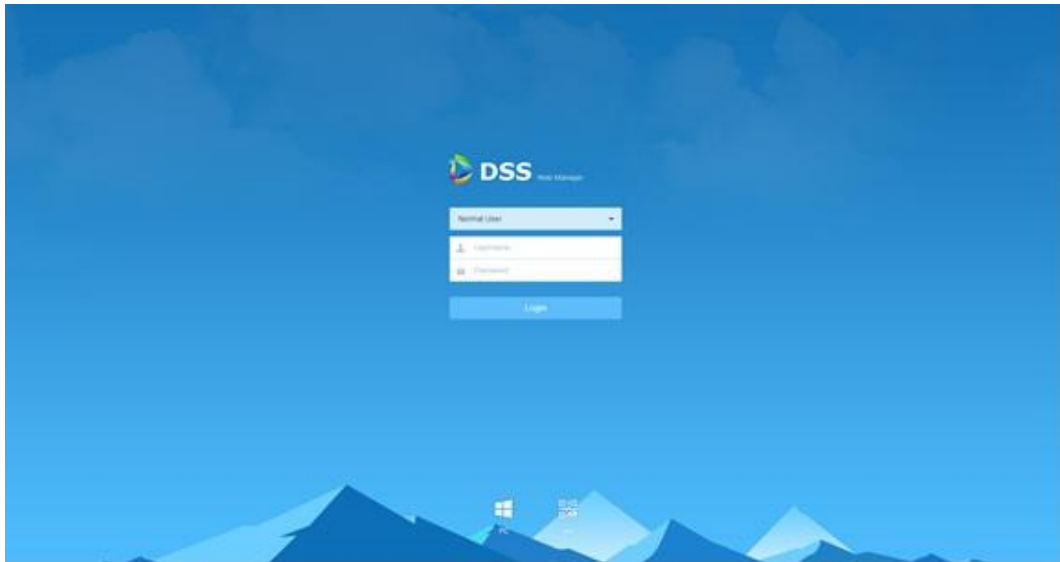
## 4.2 Logging in Management

It can log in the management end of platform server via browser, and realize remote config of relevant business by administrator.

**Step 1** Enter platform IP address in the browser, press **【Enter】** button.

The system displays the login interface. See Figure 4-4.

Figure 4-4

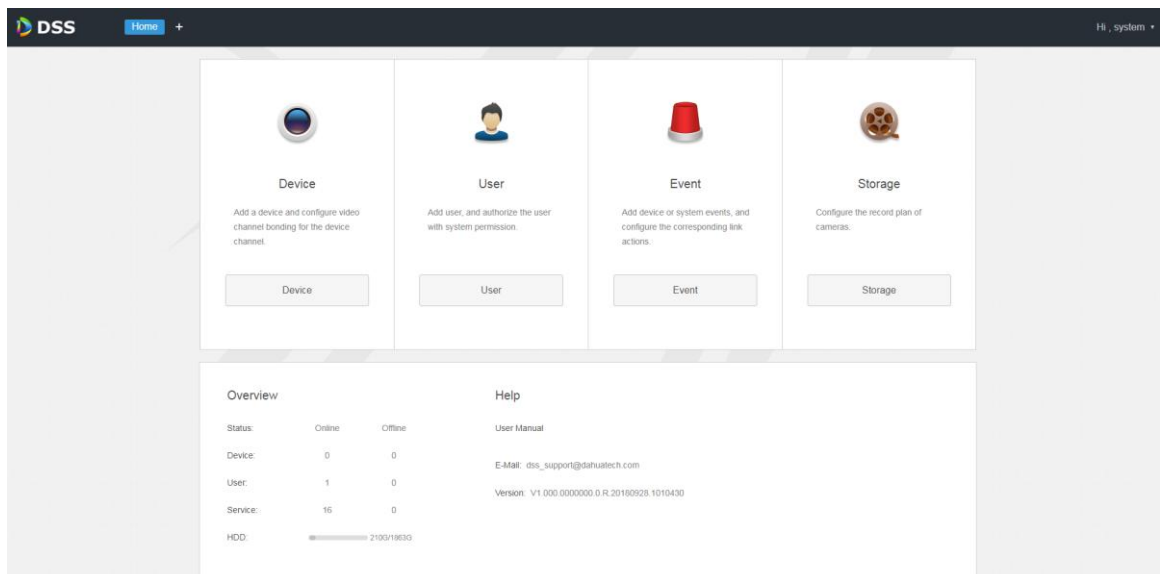


**Step 2** Enter username and password, click “Login”.


The default username is system; the password is the one which is set during initialization.

It will display the homepage after login. See Figure 4-5.

Figure 4-5



- Place the mouse on the username of top right corner, and then you can modify password or log out current user.

- The shortcut access of general modules is displayed on the top of interface, click  on the homepage to present all the modules and open new modules.
- Overview: It displays the online/offline status of device, user and service, and the usage proportion of hard drive.
- Help: Check user operation manual, platform version and so on.

## 4.3 System Settings

### 4.3.1 Setting System Parameters

It needs to configure system parameters when it is first time to log in DSS system, which is to make sure that the system runs normally.


Step 1 Click ; select “System Settings” in the interface of “New Tab”.

The system displays the interface. See Figure 4-6.

Figure 4-6

Table 4-1

Parameter		Note
Message Storage Time Setup	Log	Sets longest keep time of log, it is 30 days by default.
	Alarm info	Sets the longest keep time of alarm info, it is 30 days by default.
	GPS info	Sets the longest keep time of GPS info, it is 30 days by default.
	POS	Sets the longest keep time of POS info, it is 30 days by default.

Parameter		Note
	Heatmap	Sets the longest keep time of heat map info; it is 30 days by default.
FTP	LAN path	The FTP server LAN path where file is stored.
	WAN path	The FTP server Internet path where file is stored.
	Username/ password	Username and password used to log in FTP server.
Time Sync	Enable	Check it to enable the function of time sync.
	Start time	Sets start time of time sync.
	Sync Interval	The time of server shall prevail; synchronize the time of device and server. It is 2 hours by default, the system is based on the server time every 2 hours, and then it is to synchronize the time of both device and server.  <b>NOTE</b> The time between device and server is synchronized via SDK.
	Immediately	Click the button to start time sync immediately.
Mail Server	-	It is to set mail server IP, port, encryption type, username/password, sender, test recipient etc. It can select to send email to users when the administrator configures the alarm linkage and the client handles the alarm. At this moment, it needs to configure mail server first.
Activity Directory	-	Set domain info.
HTTPS	-	Enable HTTPS security verification.
POS End	-	After setting POS end mark, it will display on the location of POS receipts end.
Picture Storage Setup	Picture storage time	Sets the storage time of the picture, unit: day.
	Min Capacity	

Step 2 Configure corresponding parameters.


Step 3 Click 'Save'.

## 4.3.2 FTP

### 4.3.2.1 Use

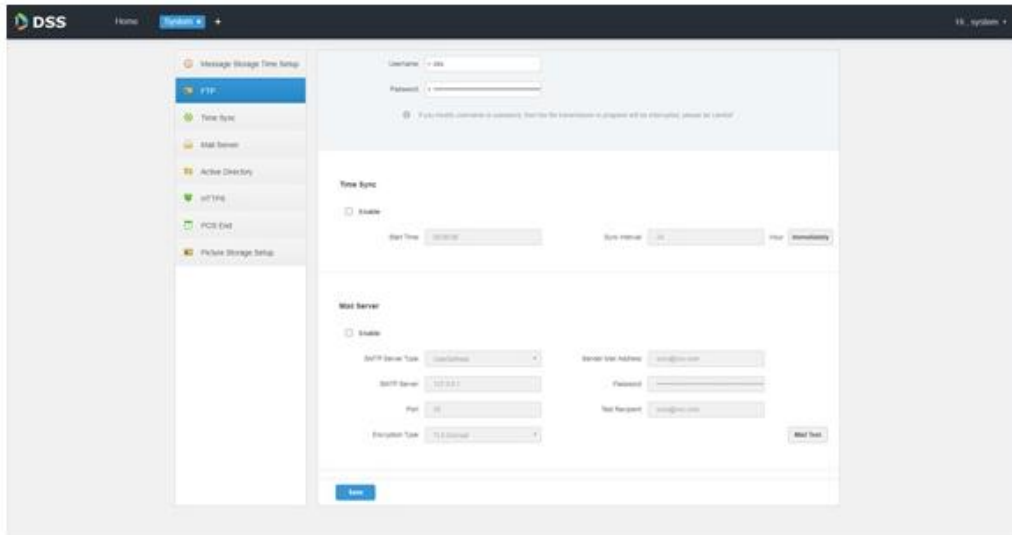
It is to enable FTP in the DSS server, which is mainly used to upload alarm capture to DSS platform. It can use built-in FTP of DSS system (Fail to support IP address modification), it can also configure the FTP server which is set up by users themselves.

## 4.3.2.2 Configuration Method

Step 1 Click , select “System” in the interface of “New Tab”.

Step 2 Click “FTP” and set FTP address, username and password.  
The interface is displayed. See Figure 4-7.

Figure 4-7



### NOTE

The item with \* has to be filled in, the standard format of FTP address is ftps://x.x.x.x, the system's own FTP address is the IP address of DSS server; both username and password are dss/dss by default.

Step 3 Click “Save” to save config.

You can use relevant tools to visit FTP address.

## 4.3.3 Setting Mail Server

### 4.3.3.1 Application Scenarios

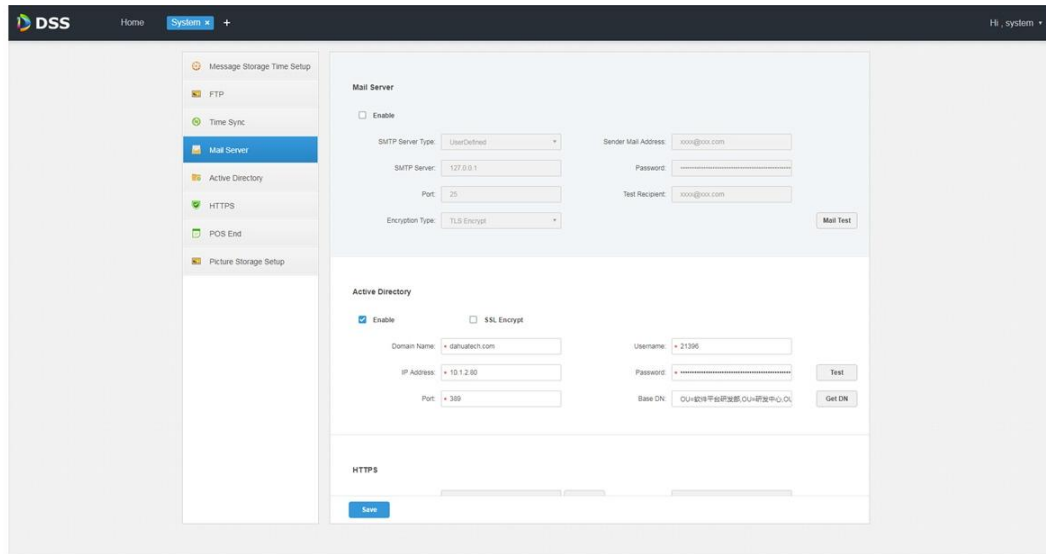
It can select to send mail to user when the administrator is configuring alarm linkage and client handling alarm, at this moment, it needs to configure mail server first.

### 4.3.3.2 Config Method

Step 1 Click  and select “System” on the interface of “New Tab”.

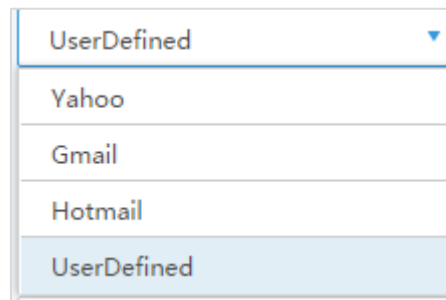
Step 2 Select the tab of “Mail Server”, check “Enable” to enable mail config. See Figure 4-8.

Figure 4-8




**Step 3** Select the type of mail server in the drop-down box. See Figure 4-9.

Figure 4-9



**Step 4** It is to set mail server IP, port, encryption type, username/password, sender and test recipient etc.

**Step 5** Click “Mail Test” to test if the config of mail server is valid. Test prompt will be received if the test is successful, and the test account will receive corresponding email.

**Step 6** Click  after the test is successful, and then it can save config info.

## 4.4 Adding Organization

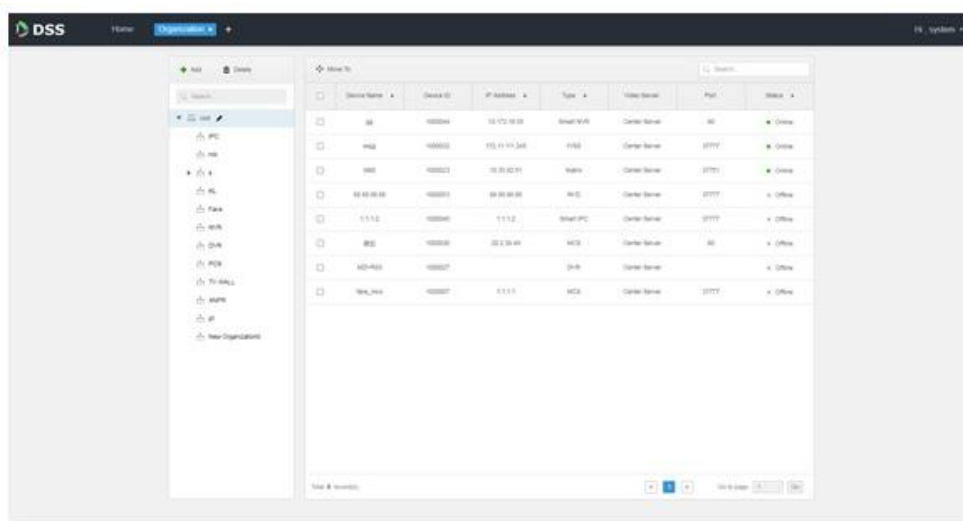
Adding organizations is to deploy the hierarchy of organization or device, which is to make it easy to manage. It doesn't have to add organizations, the added users or devices are classified to the default organization.

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

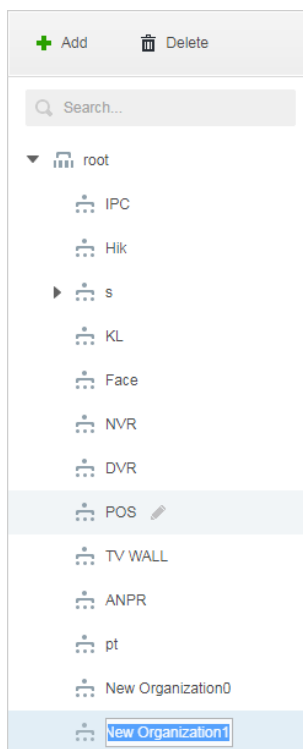
### Steps



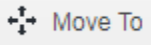


**Step 1** Click **+** and select “Organization” on the interface of “New Tab”.  
 The system displays the interface of organization. See Figure 4-10  
 Figure 4-10



**Step 2** Select root organization, click “Add”.  
 It is to add new organizations under the root organization. See Figure 4-11.  
 Figure 4-11



**Step 3** Enter organization name, press **【Enter】** button.

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

## 4.5 Adding Role and User

### 4.5.1 Adding User Role

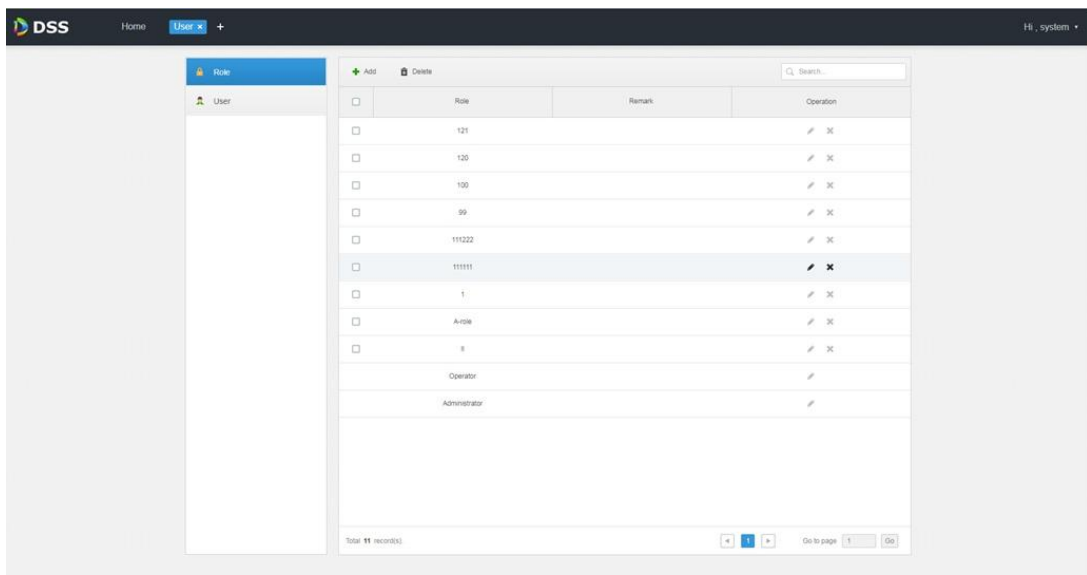
You can create user role and add user. The created user can log in both admin and client. Different user roles decide users to have different operation permissions.

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

Step 1 Click  and select “User” on the interface of “New Tab”.

The system displays the interface of user. See Figure 4-12.

Figure 4-12



Step 2 Click ‘Add’ under the “Role” tab.

The system pops out the interface of “Add Role”.

Step 3 Enter “Role Name”.



If it selects “Copy from” next to the “Role Name” and select some role in the drop-down Box, then it can copy the config info into the selected roles and realize quick config.

**Step 4** Select “Device Permission” and “Operation Permission”.  
The system will display the interface. See Figure 4-13.

Figure 4-13

The screenshot shows the 'Add Role' dialog box. It includes a 'Basic Info' section with 'Name' and 'Remark' fields, and a 'Copy from' dropdown. The 'Device Permissions' section is a tree view with categories like root, IPC, Hik, s, KL, Face, and NVR. The 'Control Permissions' section is a tree view with permissions like All Permissions, Control Permissions, Record, Record Lock, Record Tag, PTZ, Audio Talk, and Menu Permissions. The 'User' section is a table with a search bar and a list of users: Username, system, lmx, 21396, chenjie, and A. At the bottom right, there are 'OK' and 'Cancel' buttons.

 **Note**

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

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

## 4.5.2 Adding User

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

### Steps

**Step 1** Click “User” tab.

The system displays the interface. See Figure 4-14.

Figure 4-14

<input type="checkbox"/>	Username	Role	Status	User Type	Operation
<input type="checkbox"/>	ym	Administrator	● Online	Normal User	
<input type="checkbox"/>	asd		● Offline	Normal User	
<input type="checkbox"/>	77888111	Administrator	● Offline	Normal User	
<input type="checkbox"/>	778888	Administrator	● Offline	Normal User	
<input type="checkbox"/>	1		● Offline	Normal User	
<input type="checkbox"/>	ll	Administrator,II	● Offline	Normal User	
<input type="checkbox"/>	zhhq	Administrator	● Offline	Normal User	
<input type="checkbox"/>	testfx	Administrator,Operator,II	● Offline	Normal User	
<input type="checkbox"/>	A	A-role	● Offline	Normal User	
<input type="checkbox"/>	chenjie	Administrator	● Offline	Normal User	
<input type="checkbox"/>	21396	Administrator	● Offline	Domain User	
<input type="checkbox"/>	lrx	II	● Online	Normal User	
	system	Administrator,99,100,120,121	● Online	Normal User	

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

**Step 2** Click 'Add'.

The system will pop out the interface of "Adding User".

Figure 4-15

**Add User**

**Basic Info**

Username: \*   Password Expiry:

Password: \*  Email Address:

Confirm: \*  PTZ Control Permission: \* 5

MAC Address:  Remark:

**Role**

<input type="checkbox"/>	Role name
<input type="checkbox"/>	Administrator
<input type="checkbox"/>	Operator
<input type="checkbox"/>	II
<input type="checkbox"/>	A-role
<input type="checkbox"/>	1

**Device Permissions**

Search...

▼ root

**Control Permissions**

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

OK Cancel

**Step 3** Configure user info, select role below, and it will display device permission and operation permission of corresponding role on the right.

**NOTE**

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

**Step 4** Click “OK” to add the user.

## Operations

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

### 4.5.3 Setting Domain User

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

### 4.5.3.1 Application Scenario

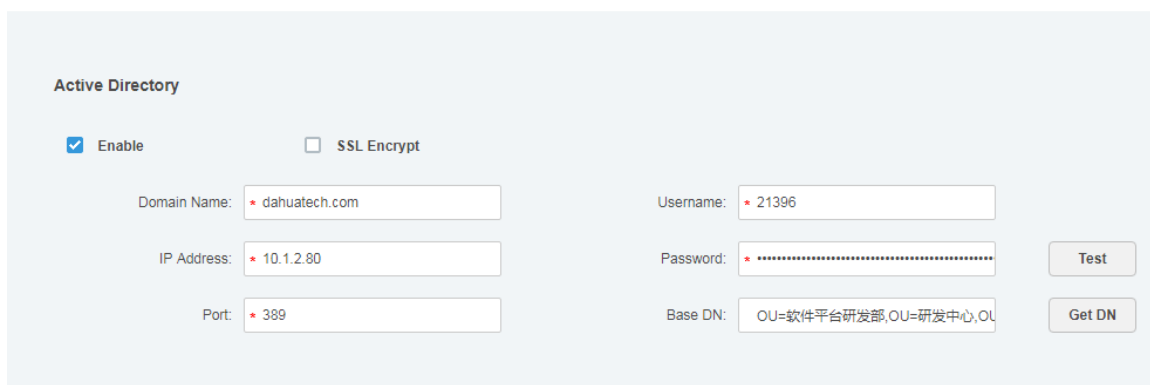
For the companies with domain information and want to use domain users as system login users, using domain user import can improve the convenience of project deployment.

### 4.5.3.2 Setting Domain Info

Step 1 Click  and select “System” on the interface of “New Tab”.

Step 2 Click the tab of “Active Directory” and configure domain info. See Figure 4-16.

Figure 4-16



Active Directory

Enable  SSL Encrypt

Domain Name: \* dahuatech.com Username: \* 21396

IP Address: \* 10.1.2.80 Password: \* .....

Port: \* 389 Base DN: OU=软件平台研发部,OU=研发中心,OU=

Test Get DN

Step 3 After setting domain info, click “Get DN” and it will acquire basic DN info automatically.

Step 4 After getting DN info, click “Test” to test if domain info is available.

Step 5 Click “Save” to save config.

It can import domain user on the interface of “User” after it prompted successfully.

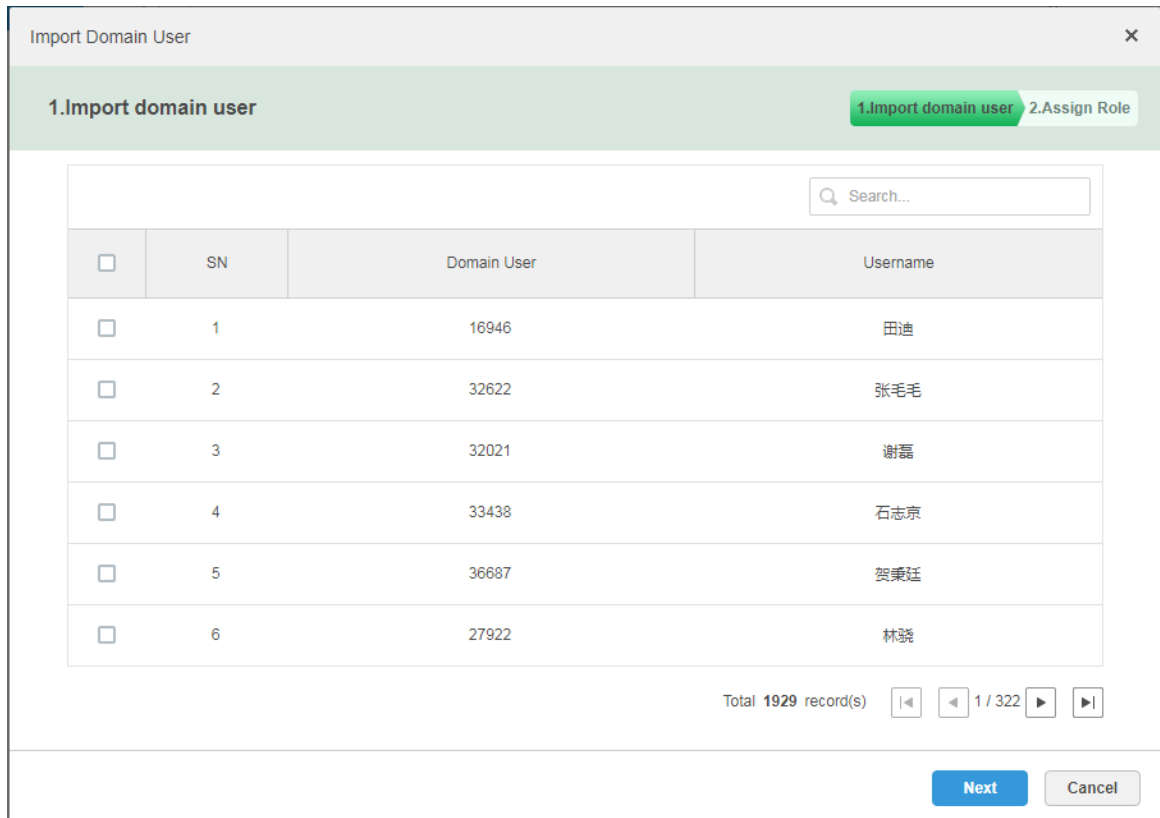
Please refer to the next chapter for more operation details.

### 4.5.3.3 Importing Domain User

Step 1 Click  and select “User” on the interface of “New Tab”.

Step 2 Select “User” tab, click “Import Domain User” on the right of the interface.  
The system will display the interface of “Import Domain User”. See Figure 4-17.

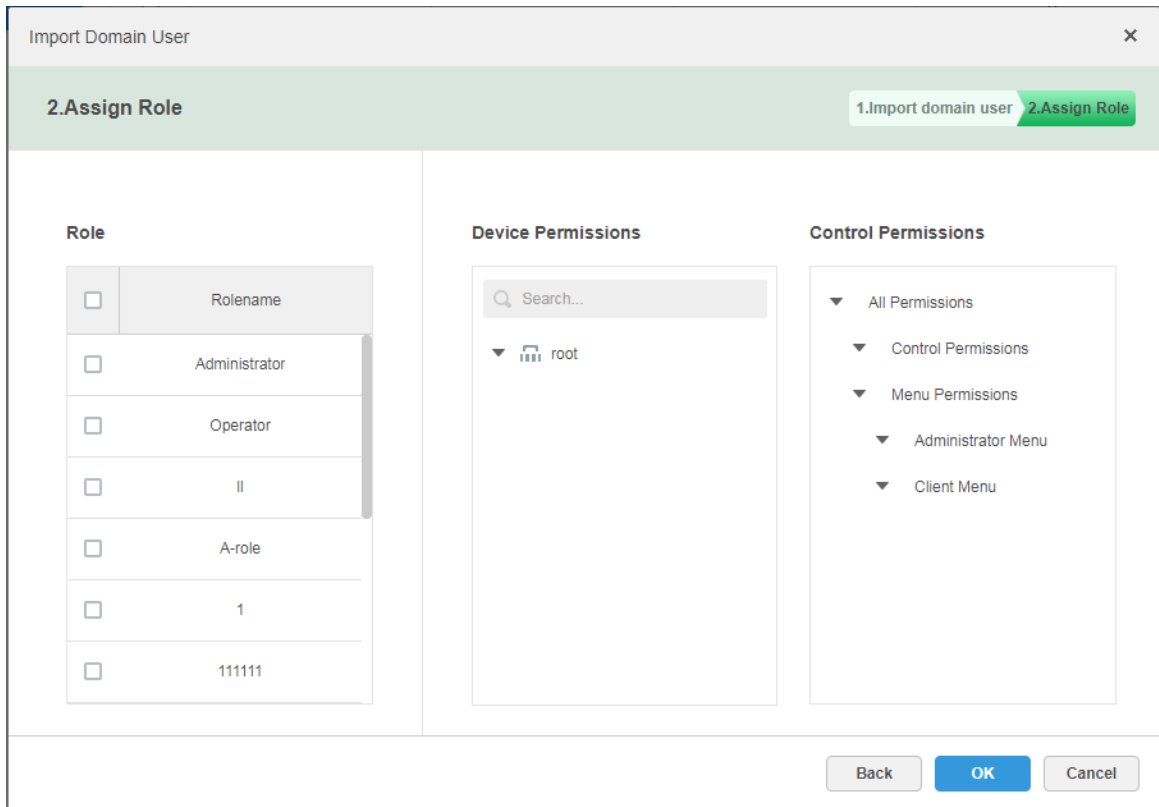
Figure 4-17



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

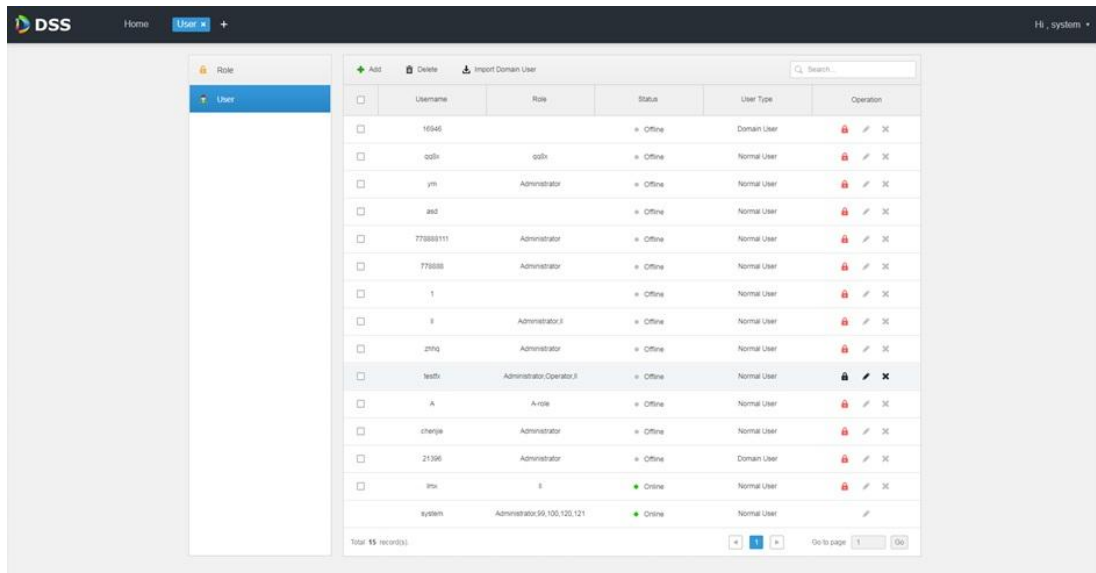
**Step 4** Click "Next".  
The system displays the interface of "Import Domain User". See Figure 4-18.

Figure 4-18



**Step 5** Select role for domain user, it displays corresponding device info and function permission info on the right of the interface, click “OK” after it is confirmed. Make sure domain user has been successfully imported in “User Info”. See Figure 4-19.

Figure 4-19



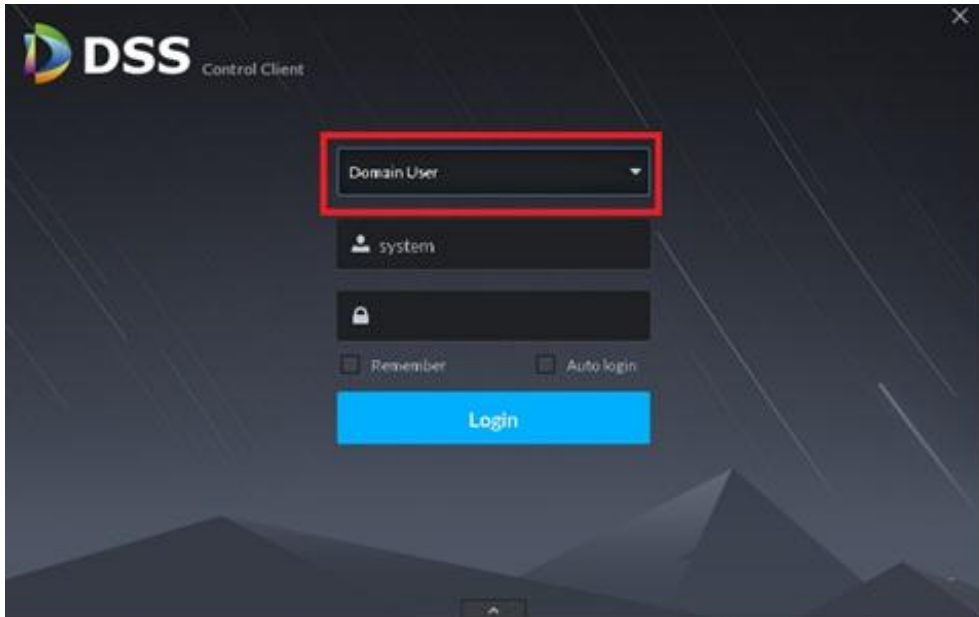
#### 4.5.3.4 Logging in Domain User

It can use domain user to log in client.

**Step 1** Select “Domain User” in the drop-down box of “User Type” on the client login interface. See Figure 4-20.



Figure 4-20



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

## 4.6 Adding Device

It can add different types of devices according to different business requirements.

### 4.6.1 Adding Device Manually

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

The system will display the interface of “Device”. See Figure 4-21.

Figure 4-21

The screenshot displays a network management interface. On the left, there is a sidebar with 'Device' and 'Bind Resource' options. The main area features a top toolbar with 'Connect', 'Refresh', 'Initialize Device', and 'Change IP' buttons. Below this is a table of initialized devices with columns for 'Init Status', 'IP Address', 'Type', 'Port', and 'MAC Address'. The table contains four rows, all with 'Initialized' status. Below the table is a section for adding and managing devices, including an 'Add' button, a search bar, and a dropdown menu for 'Org' set to 'root'. A second table lists various device types such as 'Encoder', 'Decoder', 'Video Wall', 'ANPR', 'Intelligent Device', 'Matrix', and 'POS'. This table has columns for 'Device ID', 'IP/Domain', 'Video Server', 'Device Name', 'Type', 'Org', 'Status', 'Offline Cause', and 'Operation'. It shows eight rows of devices, all with 'Offline' status and 'Network anomaly' as the cause. At the bottom, there is a pagination control showing 'Total 33 record(s)' and a 'Go to page' field set to '1'.

**Step 2** Click “Add”.

The interface is shown in Figure 4-22.

Figure 4-22

The screenshot shows a configuration window titled "Add All" with a close button (X) in the top right corner. Below the title bar, there are two tabs: "1. Login Information." (active) and "2. Device Information". The form contains the following fields:

- Protocol: Dahua
- Manufacturer: Dahua
- Add Type: IP Address
- Device Category: Encoder
- IP Address: \*
- Device Port: \* 37777
- User: \* admin
- Password: \*\*\*\*\*
- Org: root
- Video Server: Center Server

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

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

 **NOTE**

Select different "Protocol", it will configure different parameters, please refer to the interface for more details.

- When "Add Type" selects "IP Address", it enters device IP address.
- When "Add type" selects "Auto Register", it enters device auto register ID. It can only add encoder via auto register, the ID of auto register has to be in accordance with the registered ID configured at encoder.
- When "Add Type" selects "Domain Name", the options are from configured domain during deployment.

**Step 4** Click "Add".

The interface is shown in Figure 4-23.

Figure 4-23

Add All [X]

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

Device Name: \*

Type: DVR

Device SN:

Role: Administrator,Operator

Video Channel: \*

Alarm Input Channel:

Alarm Output Channel:

Back Continue to add OK

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

**Step 6** Click “OK”.

Please click “Continue to add” if it continues to add device.

## 4.6.2 Searching Added Device

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

**Step 1** Click  and select ‘device’ on the interface of “New Tab”.

**Step 2** Click “Search Again” above the “device” interface.

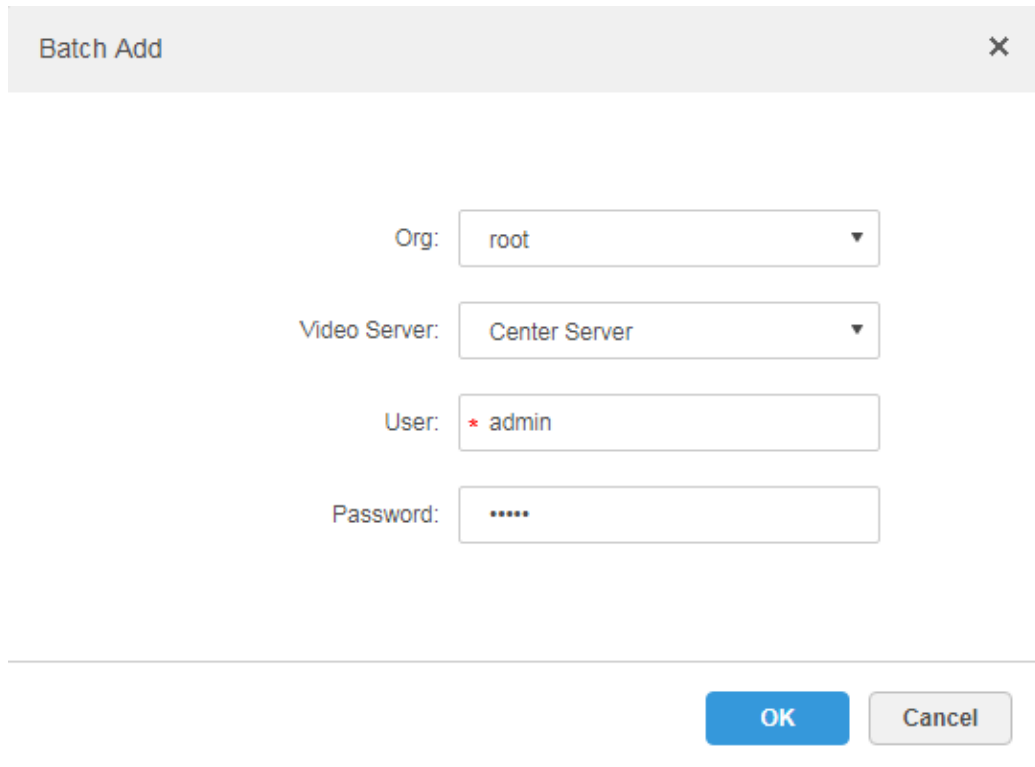
 **NOTE**

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

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

The system will pop out the interface of “Batch Add”. See Figure 4-24.

Figure 4-24



Batch Add

Org: root

Video Server: Center Server

User: \* admin

Password: \*\*\*\*\*

OK Cancel

- Step 4** Select “Organization” and “Video Server”, enter “User” and “Password”.  
“User” and “Password” are the username and password which are used to log in the device; both are “Admin” by default.
- Step 5** Click “OK”.  
The system will add the devices into corresponding organization.

### 4.6.3 Editing Device

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

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

**Step 2** Click the corresponding  of device list.

The system displays the interface of “Edit Device”. See Figure 4-25.

 **NOTE**

Click “Get Info” and the system will synchronize device info.

Figure 4-25

The screenshot shows the 'Edit Device' window with the 'Basic Info' tab selected. The 'Input Info' section contains the following fields: Protocol (Dahua), Manufacturer (Dahua), IP Address (88.88.88.88), User (admin), Device Port (37777), Password (masked), Video Server (Center Server), and Org (root). The 'Device Details' section contains Device Name (88.88.88.88), Device SN (empty), and Type (NVD). At the bottom, there are 'Get Info', 'OK', and 'Cancel' buttons.

**Step 3** It is to modify device basic info on the interface of “Basic Info”.

**Step 4** Click “Video Channel” tab, set the device channel name, channel function, camera type, SN, keyboard code and face function.

The interface is shown in Figure 4-26.

 **NOTE**

Different types of device have different interfaces of channel setting; please refer to the real interface for more details. See Figure 4-26, Figure 4-27, Figure 4-28 and Figure 4-29.

Figure 4-26

The screenshot shows the 'Edit Device' window with the 'Video Channel' tab selected. The 'Basic Info' section shows 'Channel Amount' set to 1. Below is a table with the following data:

Video Channel	Name	Function	Camera Type	SN	KeyBoard Code	Face Function
Decode Channel	* 88.88.88.1	Speed Dome				

At the bottom right, it says 'Total 1 record(s)' with navigation buttons. At the bottom, there are 'Get Info', 'OK', and 'Cancel' buttons.

Figure 4-27

The screenshot shows the 'Edit Device' window with the 'Video Channel' tab selected. The 'Basic Info' section shows 'Channel Amount' set to 1 and 'Stream Type' set to 'Sub Stream'. Below is a table with the following data:

Video Channel	Name	Function	Camera Type	SN	KeyBoard Code	Face Function
Alarm Input Channel	* 10.35.92.86	Fixed Camera				Face Detect...
Alarm Output Channel						

At the bottom right, it says 'Total 1 record(s)' with navigation buttons. At the bottom, there are 'Get Info', 'OK', and 'Cancel' buttons.

**NOTE**

It is to set video channel function according to the actual face recognition plan.

- Encoder has no need to set face function if face detection and recognition are realized by intelligent server.
- Face function shall be set as “Face Detection” if intelligent server realizes face recognition and encoder realizes face detection.
- Face function of encoder channel is set as “Face Recognition” if encoder realizes face detection and recognition.

Figure 4-28

Figure 4-28 shows the 'Edit Device' configuration window. The 'Basic Info' section includes 'Channel Amount' (1) and 'Stream Type' (Sub Strea...). The 'Video Channel' tab is selected, showing a table with columns: Name, Function, Camera Type, SN, People Counting, KeyBoard Code, and Face Function. A single record is listed with Name 'IPC\_80.8', Function 'Support ...', Camera Type 'Fixed C...', and Area Sta... The window also features 'Get Info', 'OK', and 'Cancel' buttons.

Figure 4-29

Figure 4-29 shows the 'Edit ANPR' configuration window. The 'Basic Info' section includes 'Channel Amount' (1) and 'Stream Type' (Sub Strea...). The 'Video Channel' tab is selected, showing a table with columns: Name, Camera Type, Type, Lane No., Direction, SN, Large Vehicle Speed Limit (Min/Max), and Small Vehicle Speed Limit (Min/Max). A single record is listed with Name 'II-91\_1', Camera Type 'Spee...', Type 'Video...', Lane No. 'Lane 1', and Direction 'E-W'. The window also features 'Get Info', 'OK', and 'Cancel' buttons.

**Step 5** Click the tab of “Alarm Input Channel”, configure channel name and alarm type of alarm input. See Figure 4-30.

**NOTE**

Please skip the step only when added devices need to be configured during alarm input.

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

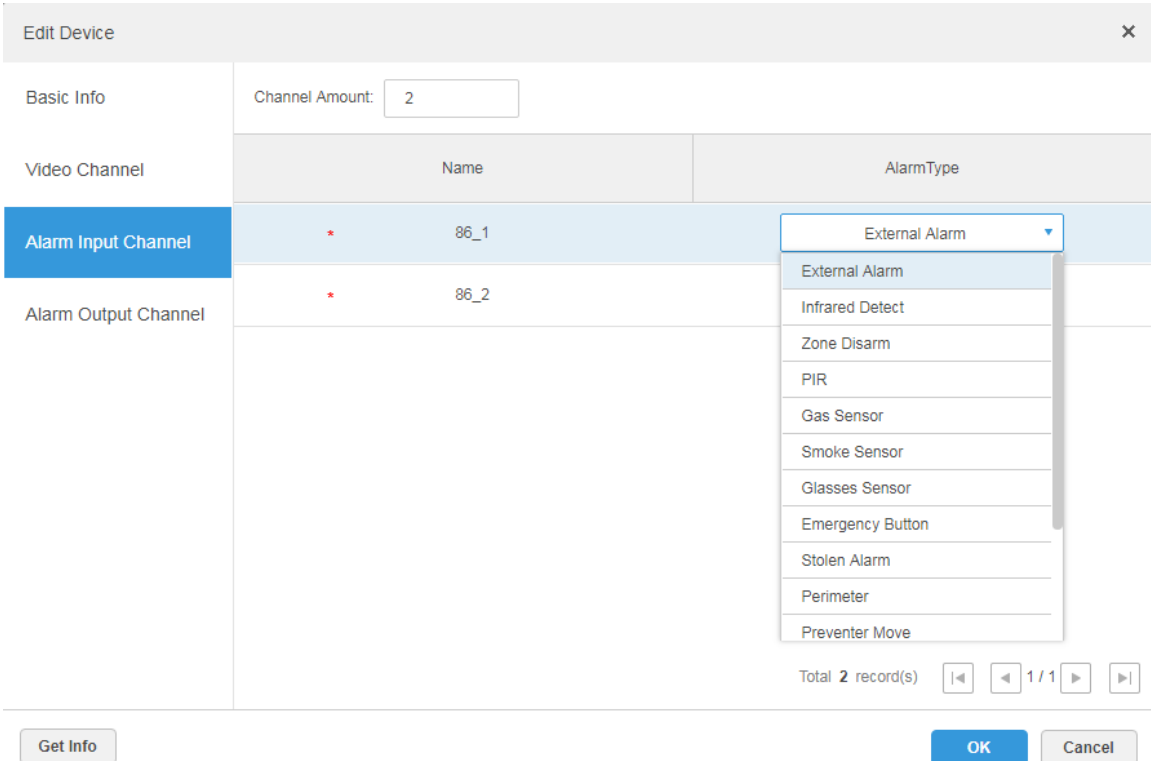


 NOTE

Custom alarm supports modification and deletion.

- If custom alarm type is used by alarm plan, then it is not allowed to be deleted but modified.
- It supports deletion if it is not used by alarm plan, after deletion, the alarm type of the alarm input channel configured with this alarm type is restored to the default value.
- When the name of the custom alarm type is modified, the history data remains the original name, while the new data adopts the modified name.
- The alarm input channel of alarm host is “Alarm Host Alarm” by default; the types of other alarm input channel are “External Alarm” by default.

Figure 4-30



The screenshot shows the 'Edit Device' configuration window. The 'Basic Info' section has a 'Channel Amount' of 2. The 'Alarm Input Channel' tab is active, displaying a table with two channels: 86\_1 and 86\_2. A dropdown menu is open for the 'AlarmType' of channel 86\_1, showing options like 'External Alarm', 'Infrared Detect', 'Zone Disarm', etc. The 'Alarm Output Channel' tab is also visible but not active.

Name	AlarmType
86_1	External Alarm
86_2	

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

Figure 4-31

The screenshot shows the 'Edit Device' configuration window. On the left sidebar, 'Alarm Output Channel' is selected. The main content area shows a table with two rows. The first row is 'Alarm Input Channel' with a name of '86\_1'. The second row is 'Alarm Output Channel' with a name of '86\_2'. Above the table, the 'Channel Amount' is set to 2. At the bottom right, there are navigation buttons and a 'Total 2 record(s)' indicator. At the bottom left, there is a 'Get Info' button. At the bottom right, there are 'OK' and 'Cancel' buttons.

	Name
Alarm Input Channel	86_1
Alarm Output Channel	86_2

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

## 4.6.4 Binding Resource

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

### Adding Resource Bind

**Step 1** Click “Resource Bind”.

The system displays the interface of “Resource Bind”. See Figure 4-32.

Figure 4-32

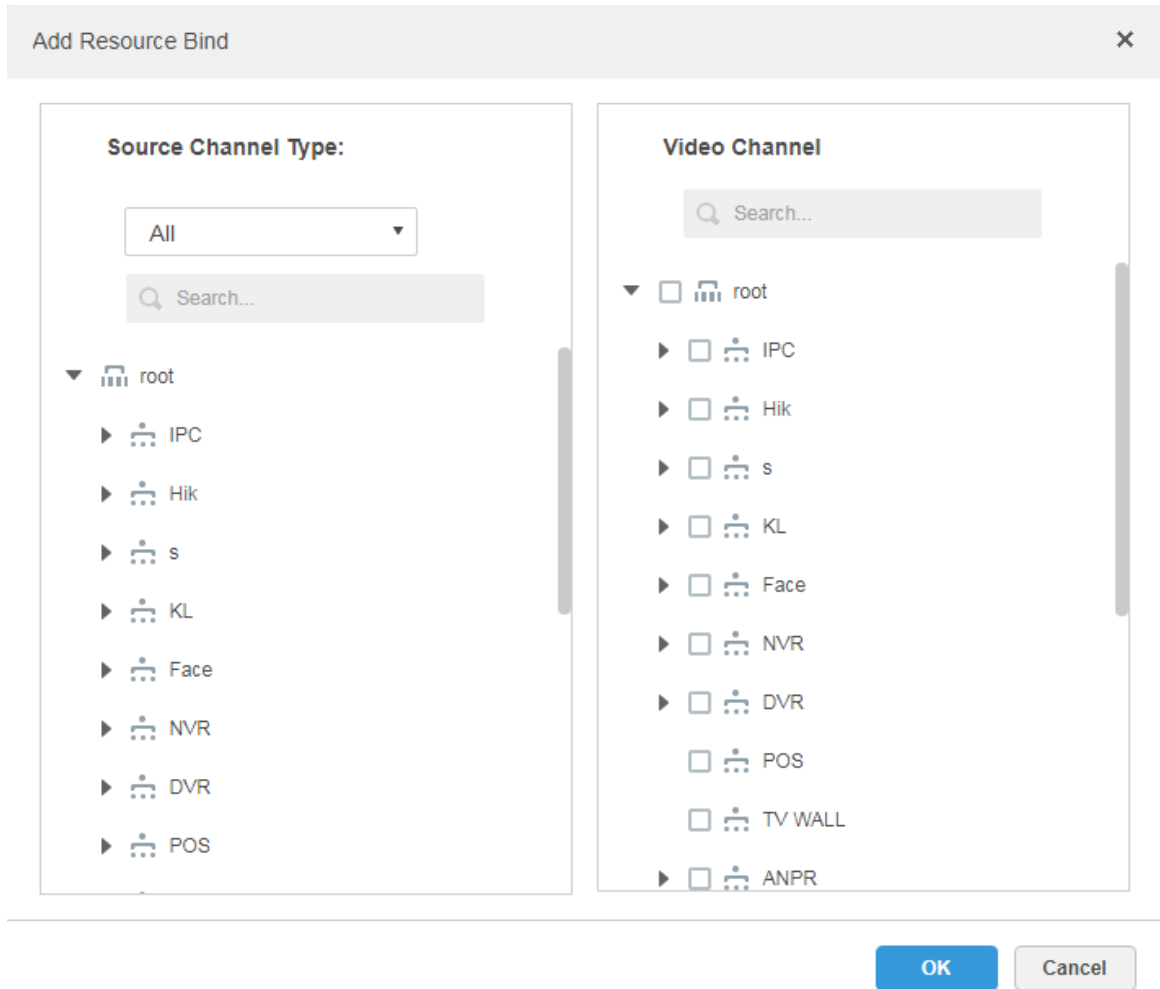
<input type="checkbox"/>	Org	Device Channel	Channel Type	Bound Channels	Operation
<input type="checkbox"/>	pt	通道4	Video Channel	通道4	
<input type="checkbox"/>	pt	IPC59htvm	Video Channel	IPC59htvm	
<input type="checkbox"/>	pt	IPC	Video Channel	IPC	
<input type="checkbox"/>	pt	CAM 1	Video Channel	CAM 1	
<input type="checkbox"/>	pt	CAM 1	Video Channel	CAM 1	
<input type="checkbox"/>	pt	IPC-22	Video Channel	IPC-22	
<input type="checkbox"/>	pt	通道4	Video Channel	通道4	
<input type="checkbox"/>	pt	IPC	Video Channel	IPC	
<input type="checkbox"/>	root	gg_64	Video Channel	gg_64	
<input type="checkbox"/>	root	gg_63	Video Channel	gg_63	
<input type="checkbox"/>	root	gg_62	Video Channel	gg_62	
<input type="checkbox"/>	root	gg_61	Video Channel	gg_61	
<input type="checkbox"/>	root	gg_60	Video Channel	gg_60	
<input type="checkbox"/>	root	gg_59	Video Channel	gg_59	
<input type="checkbox"/>	root	gg_58	Video Channel	gg_58	

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

**Step 2** Click “Add”.

The interface is shown in Figure 4-33.

Figure 4-33




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

## 4.7 Configuring Record Plan

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

### 4.7.1 Configuring Storage Disk

**Step 1** Click  and select “Record Plan” on the interface of “New Tab”.

The system displays the interface of “Record Plan”. See Figure 4-34.

Figure 4-34

<input type="checkbox"/>	Plan Name	Time Template	Position	Status	Operation
<input type="checkbox"/>	test1	All-Period Template	Store on Server	Enable	<input checked="" type="checkbox"/> ON
<input type="checkbox"/>	test	All-Period Template	Store on Server	Enable	<input checked="" type="checkbox"/> ON
<input type="checkbox"/>	putong	All-Period Template	Store on Server	Disable	<input type="checkbox"/> OFF

**Step 2** Click the tab of “Storage Config”.

The system displays the interface of “Storage Config”. See Figure 4-35.

Figure 4-35

<input type="checkbox"/>	Server Name	IP	Volume Name	Capacity(GB)	Free Capacity(GB)	Disk Type	Disk status	Operation
	Center Server	10.35.92.27	20-pic	50.00	49.97	Picture	Normal	
	Center Server	10.35.92.27	20-video	50.00	26.66	Video	Normal	
	Center Server	10.35.92.27	26-1	100.00	38.44	Video	Normal	
	Center Server	10.35.92.27	26-2	100.00	0.00	Video	Normal	
	Center Server	10.35.92.27	26-3	100.00	0.00	Video	Normal	
	Center Server	10.35.92.27	26-4	100.00	19.55	Video	Normal	
	Center Server	10.35.92.27	26-5	100.00	95.95	Picture	Normal	
	Center Server	10.35.92.27	4004-s2-1	300.00	250.67	Video	Normal	
	Center Server	10.35.92.27	4004-s2-2	300.00	299.97	Video	Normal	
	Center Server	192.168.4.108	e1	32.00	4.05	Video	Normal	
	Center Server	192.168.4.108	e10	80.00	0.00	Video	Normal	
	Center Server	192.168.4.108	e13	110.00	0.00	Video	Normal	
	Center Server	192.168.4.108	e15	110.00	0.00	Video	Normal	
	Center Server	192.168.4.108	e16	120.00	0.00	Picture	Normal	

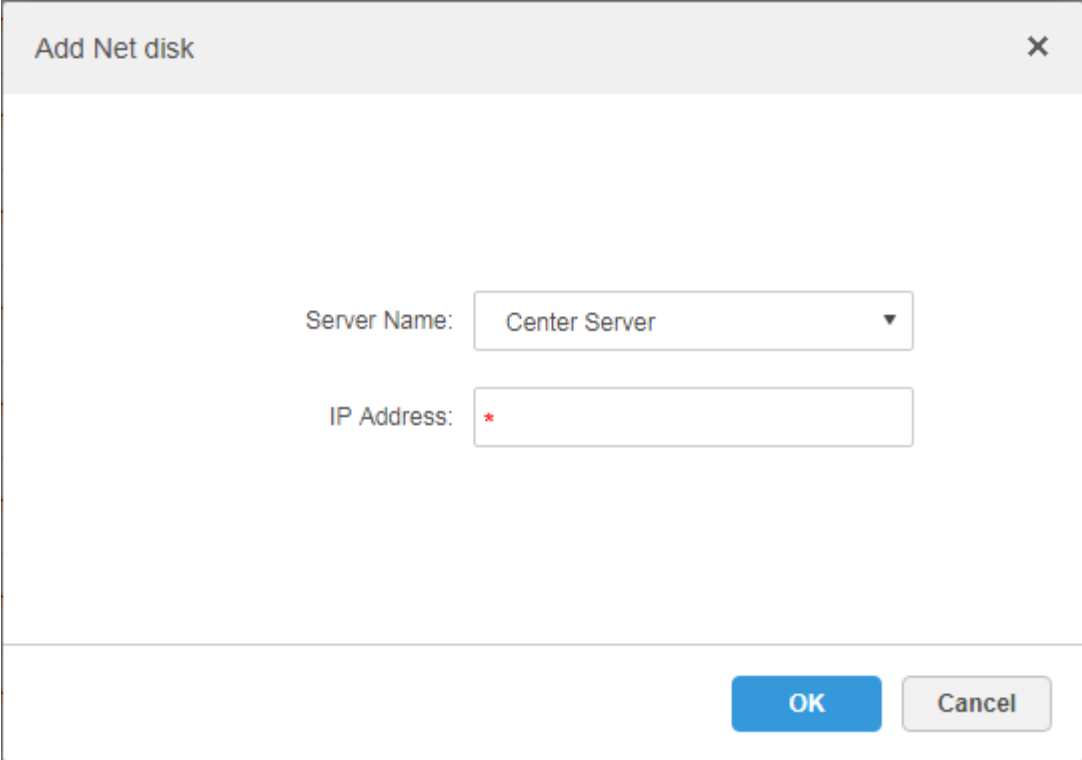
Total 60 record(s).

Go to page 1 Go

**Step 3** Click ‘Add’.


The interface is shown in Figure 4-36.

Figure 4-36



The screenshot shows a dialog box titled "Add Net disk". It has a close button (X) in the top right corner. The main area contains two input fields: "Server Name" with a dropdown menu currently showing "Center Server", and "IP Address" with a red asterisk indicating it is a required field. At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (grey).

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

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

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

**Step 7** Click “OK” in the prompt box to confirm formatting.  
You can check the results of disk formatting after formatting is completed; make sure both disk size and available space are correct.

## 4.7.2 Setting Disk Group Quota

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

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

The system will display the online status of server. See Figure 4-37.

Figure 4-37

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

**Step 2** Click next to the “Online” status server.  
The system will pop out the interface of “Edit Disk group”. See Figure 4-38.

Figure 4-38

Edit Disk Group ✕

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

Not Allocated			
<input type="checkbox"/>	Disk Name	Total Capacity(GB)	Used capacity (GB)
<input type="checkbox"/>	\\PhysicalDrive6	150	150
<input type="checkbox"/>	\\PhysicalDrive16	500	500

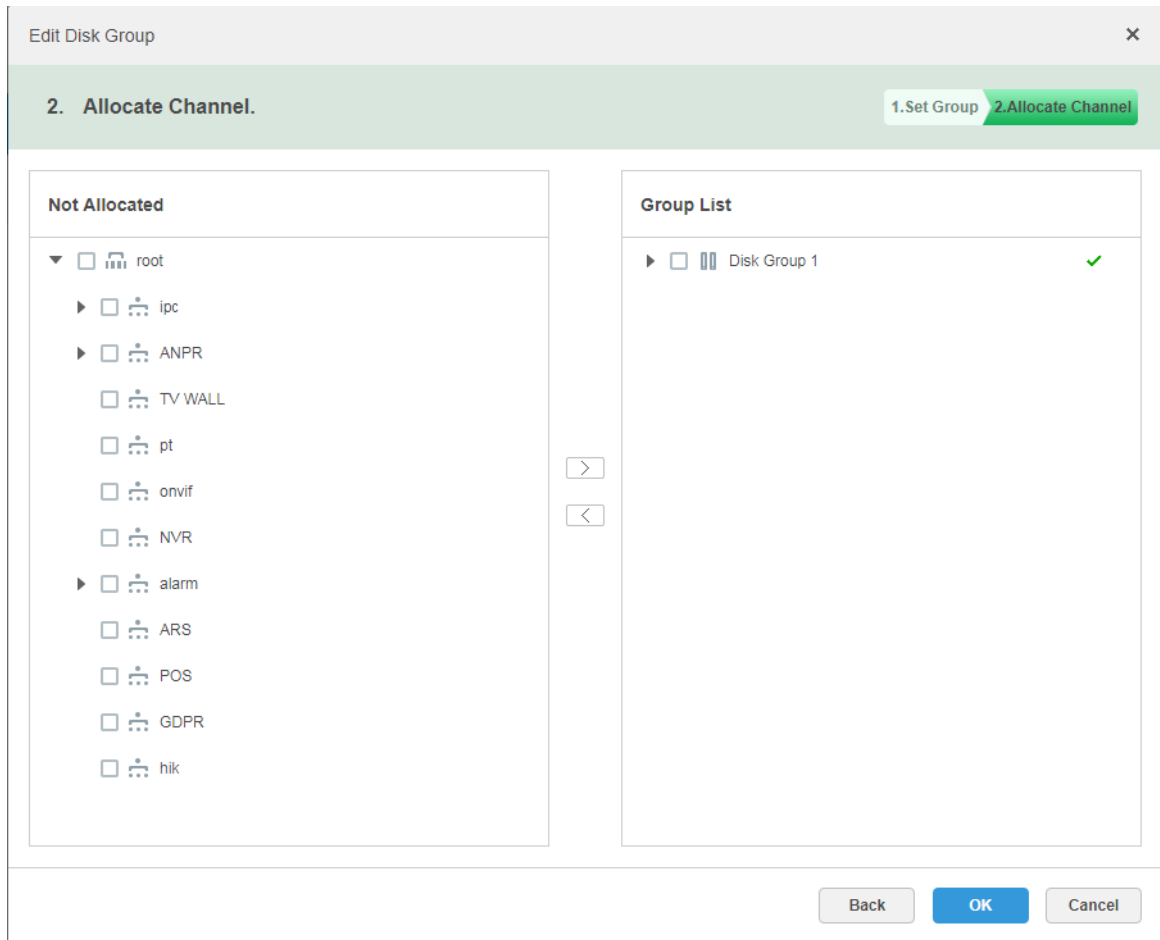
Group List			
<input type="checkbox"/>	Group Name	Total Capacity(GB)	Contain


**Next** **Cancel**

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

**Step 4** Click “Next” to distribute channels for disk group.  
The interface is shown in Figure 4-39.

Figure 4-39



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

**Step 6** Click "Done".

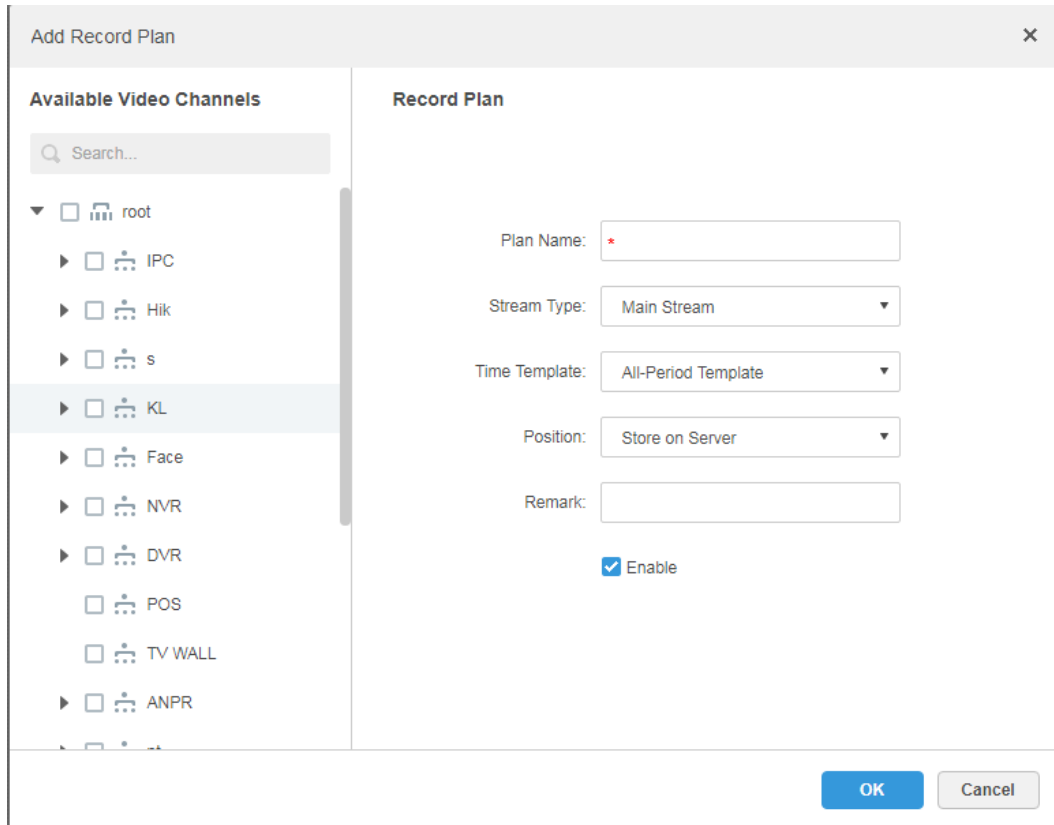
### 4.7.3 Adding General Plan

#### Steps

**Step 1** Click the tab of "Record Plan", click 'Add'. It is to add record plan. See Figure 4-40.



Figure 4-40



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

**NOTE**

- Stream type includes: Main stream, sub stream 1, sub stream 2.
- Time template can select the system default template or new template created by users, please refer to “4.7.5 Adding Time Template” for details of adding time template.
- Storage position can select server or recorder.

**Step 3** Click “OK”.

## Operations

- Enable/disable general plan

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

- Edit General Plan

Click of corresponding plan to edit the general plan.

- Delete General Plan

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

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

## 4.7.4 Adding Backup Record Plan

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

### NOTE

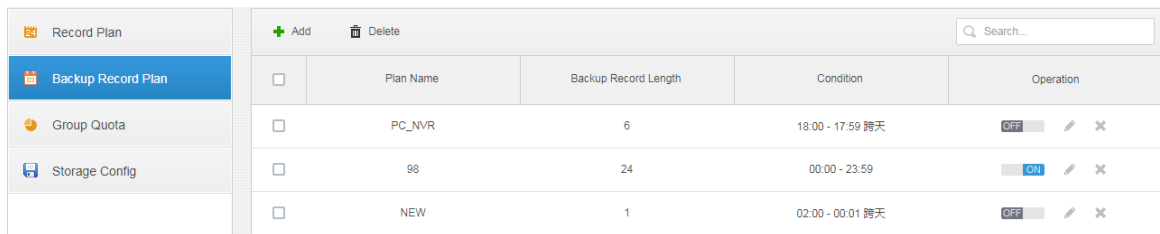
- Backup video comes for the local record of the camera.
- “Backup Condition” can select time and Wi-Fi. If it selects time, sets backup plan time, it will make backup record automatically after the time reaches; If it selects Wi-Fi, then it will make backup record automatically after the device is connected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







## Steps

**Step 1** Click the tab of “Backup Plan”.

The interface is shown in Figure 4-41.

Figure 4-41



<input type="checkbox"/>	Plan Name	Backup Record Length	Condition	Operation
<input type="checkbox"/>	PC_NVR	6	18:00 - 17:59 跨天	OFF  
<input type="checkbox"/>	99	24	00:00 - 23:59	ON  
<input type="checkbox"/>	NEW	1	02:00 - 00:01 跨天	OFF  

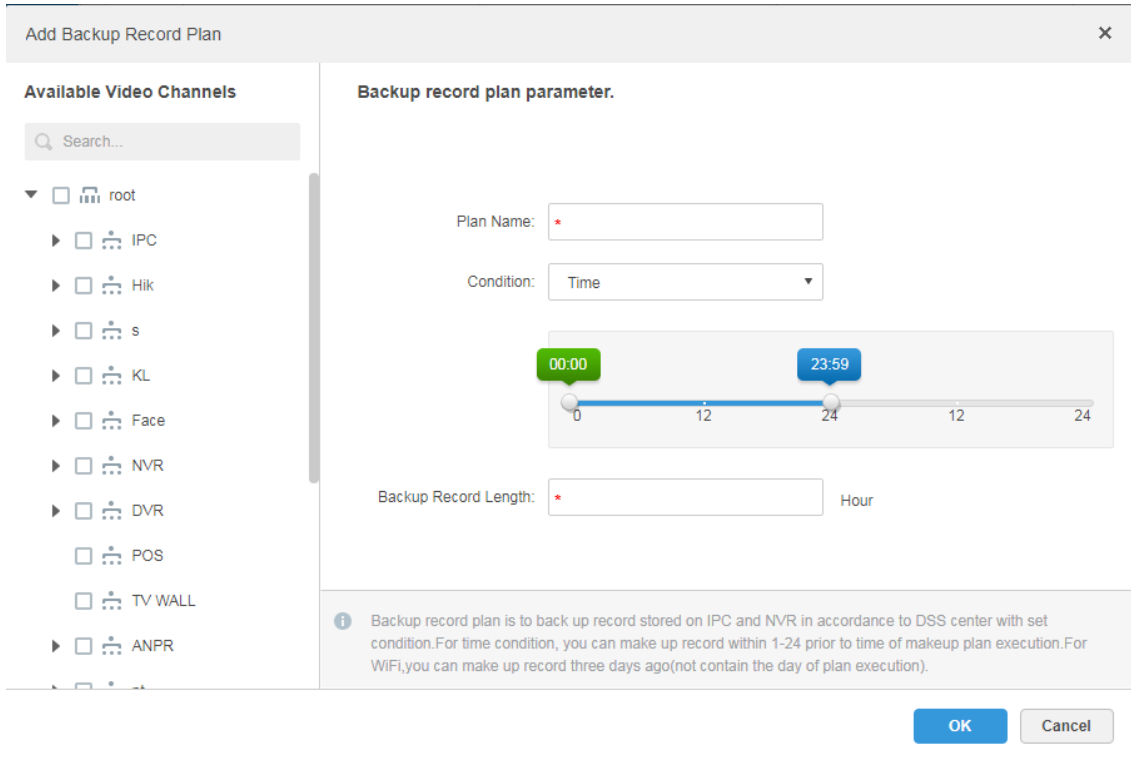
**Step 2** Click ‘Add’ to add backup plan.

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

**Step 4** Set backup conditions.

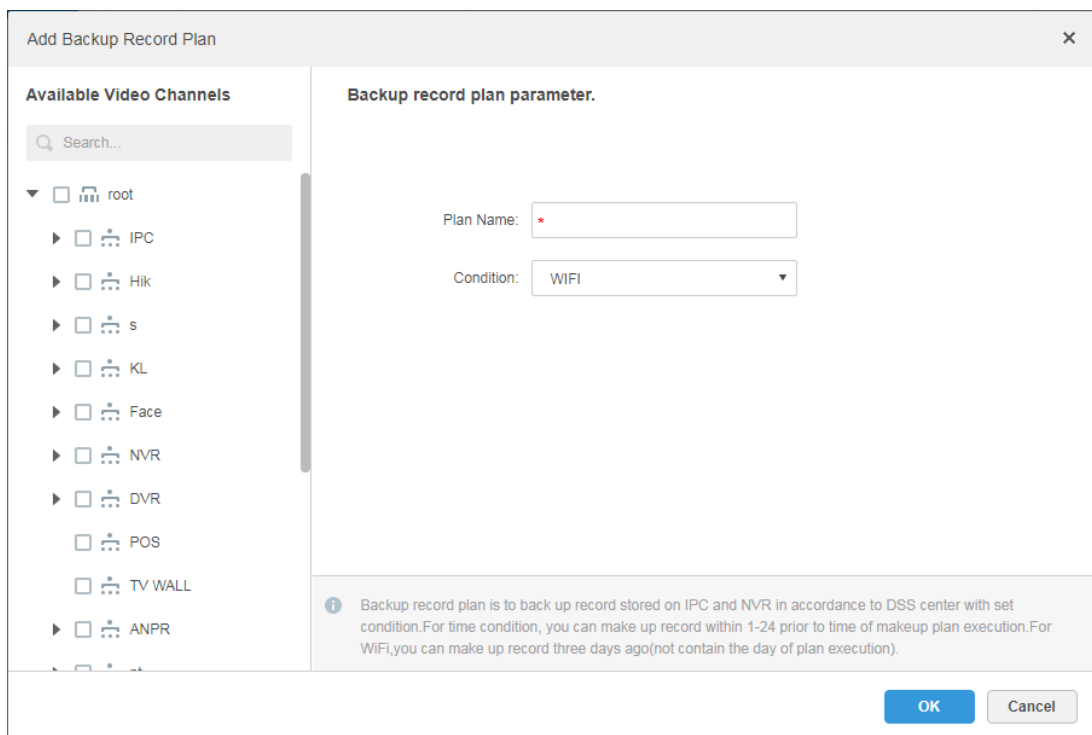
- Take time as condition.

Figure 4-42



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

Figure 4-43





- 1) Select "Wi-Fi" in the backup record condition.


- 2) Click “OK”.  
It will make backup record automatically when the network of backup device is switched to Wi-Fi.

## Operations

- Enable/Disable backup record plan.


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

- Edit backup record plan

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

- Delete backup record plan

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

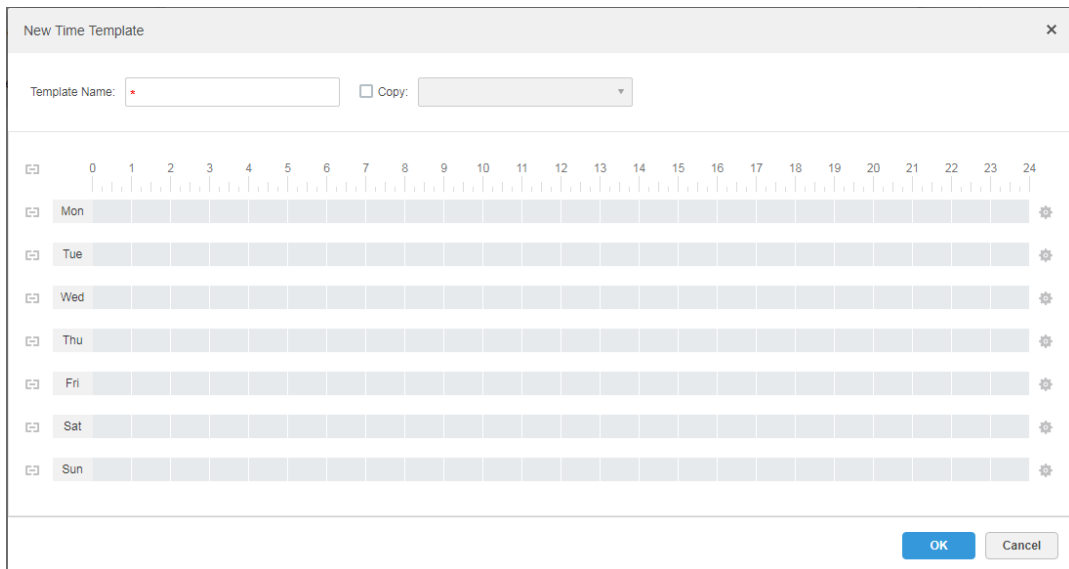
◇ Click the corresponding  of backup record plan, then you can delete the backup plan individually.

### 4.7.5 Adding Time Template

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

The system displays the interface of “New Time Template”. See Figure 4-44.

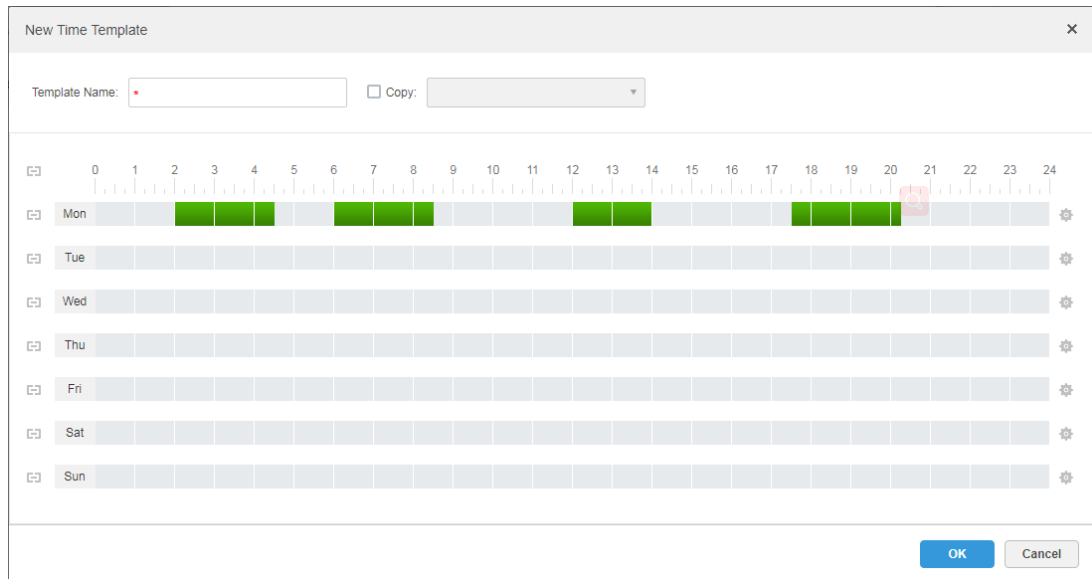
Figure 4-44



**Step 2** Sets template name and time period.

- Press the left button and drag it to draw time period on the time line. See Figure 4-45.

Figure 4-45




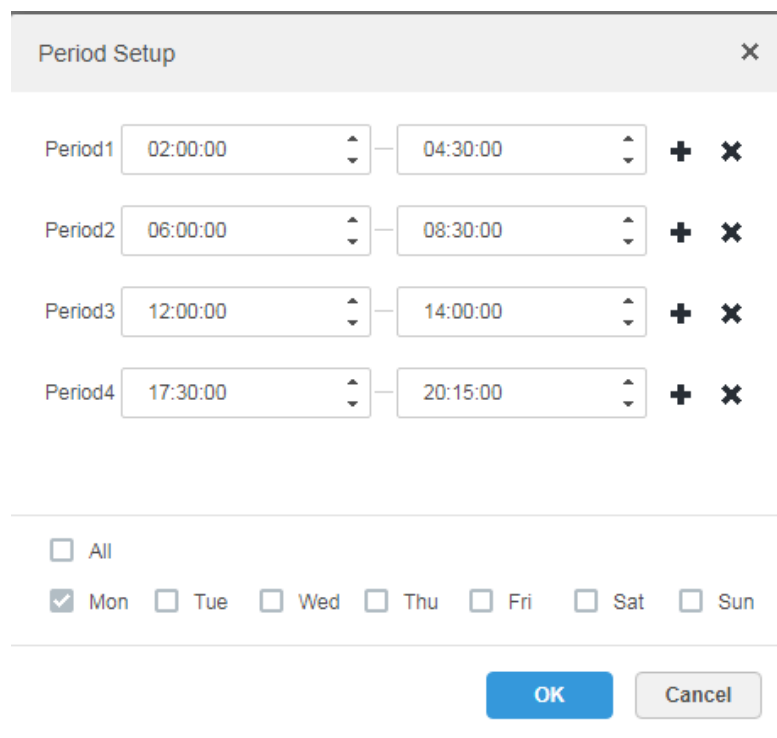
- Click the  of the corresponding day, set time period on the interface of “Period Setup”. See Figure 4-46.

Figure 4-46



 **NOTE**

It can set max 6 periods in one day.

**Step 3** Click “OK” to save time template.

 **NOTE**

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

## 4.8 Configuring Event


After configuring alarm plan on the management end, it supports displaying and handling corresponding report events on the client.

### 4.8.1 Configuring Alarm Source

Alarm source can be video channel, thermal channel and alarm input channel etc. Different encodes are configured with different alarm types, here it is to take IPC as an example to introduce.

#### NOTE

- Please make sure that IPC alarm input channel has connected to external alarm device before config, otherwise there will be no alarm being uploaded.
- Different devices need to configure different alarm types; it is based on the requirements of actual businesses. Please refer to user manual of each device for config of device end.

**Step 1** Log in WEB config interface of IPC, or click  next to IPC info line on the interface of “Device” of DSS management end.

**Step 2** Select “Setting > Alarm”.


The system displays the interface of “Alarm Setting”. See Figure 4-47.

Figure 4-47




**Step 3** Set alarm input info, click “OK”. Please refer to Table 4-2 for more details.

Table 4-2

Parameter	Note
Enable	Select check box; enable the selected alarm input channel.
Alarm Input	
Arm/Disarm Period	Set the time of alarm being reported to IPC.
Device Type	Select NO/NC; make sure it is in accordance with alarm device.
 NOTE	Other parameters need to be set according to actual requirements.

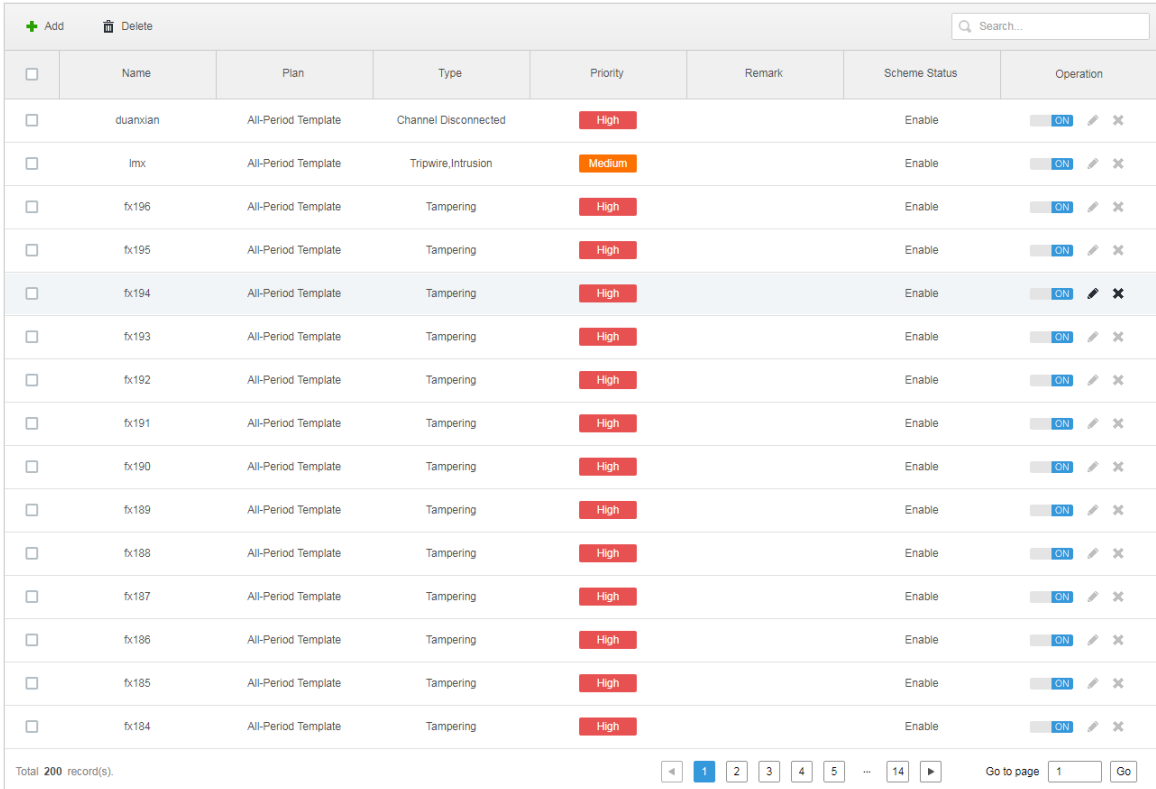
## 4.8.2 Adding Alarm Scheme































It is to set the reported events displayed on the DSS, it supports setting linkage record, email, capture, display on wall and so on, and set alarm period.

**Step 1** Click  on the management end; select ‘Event’ on the interface of ‘New Tab’.

The system displays the interface of ‘Event’. See Figure 4-48.

Figure 4-48



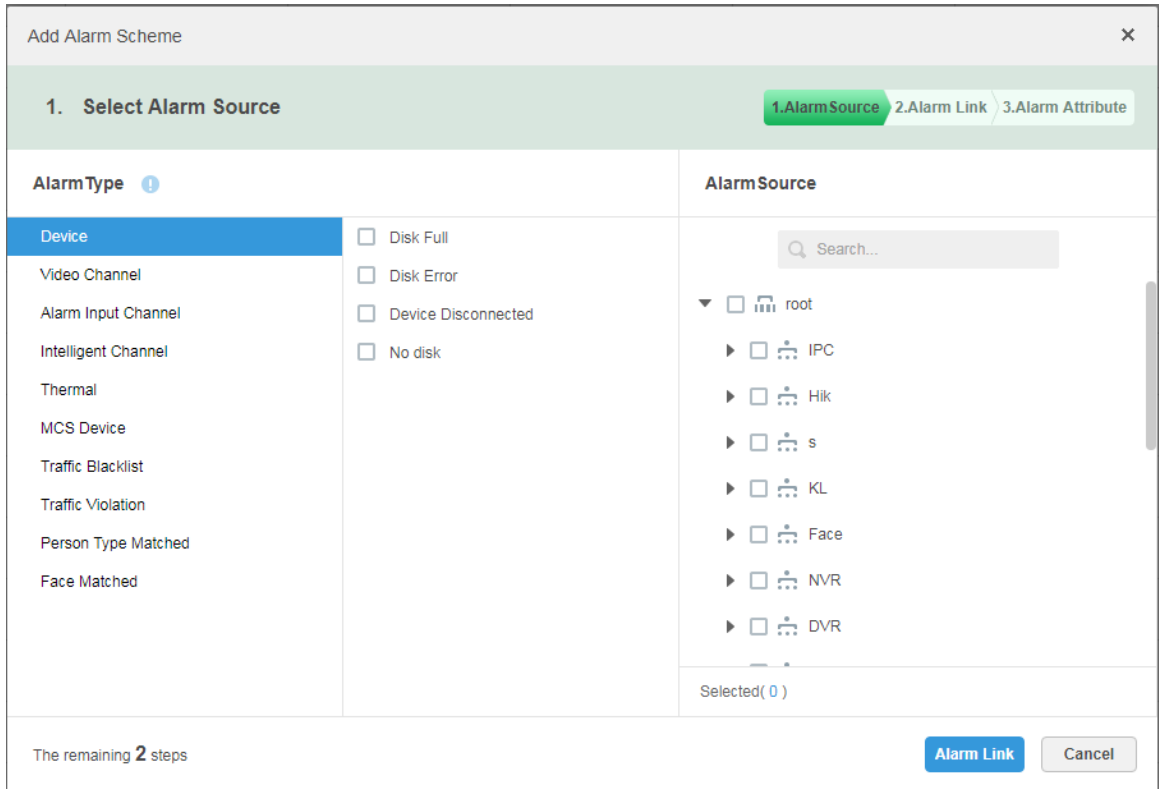
<input type="checkbox"/>	Name	Plan	Type	Priority	Remark	Scheme Status	Operation
<input type="checkbox"/>	duanxian	All-Period Template	Channel Disconnected	High		Enable	<input type="checkbox"/> ON  
<input type="checkbox"/>	lmx	All-Period Template	Tripwire Intrusion	Medium		Enable	<input type="checkbox"/>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

Total 200 record(s). 1 2 3 4 5 ... 14 Go to page

**Step 2** Click ‘Add’.

The system displays the interface of ‘Add Alarm Scheme’. See Figure 4-49.

Figure 4-49



**Step 3** Configure alarm source.

- 1) Select alarm type and alarm source.

 NOTE

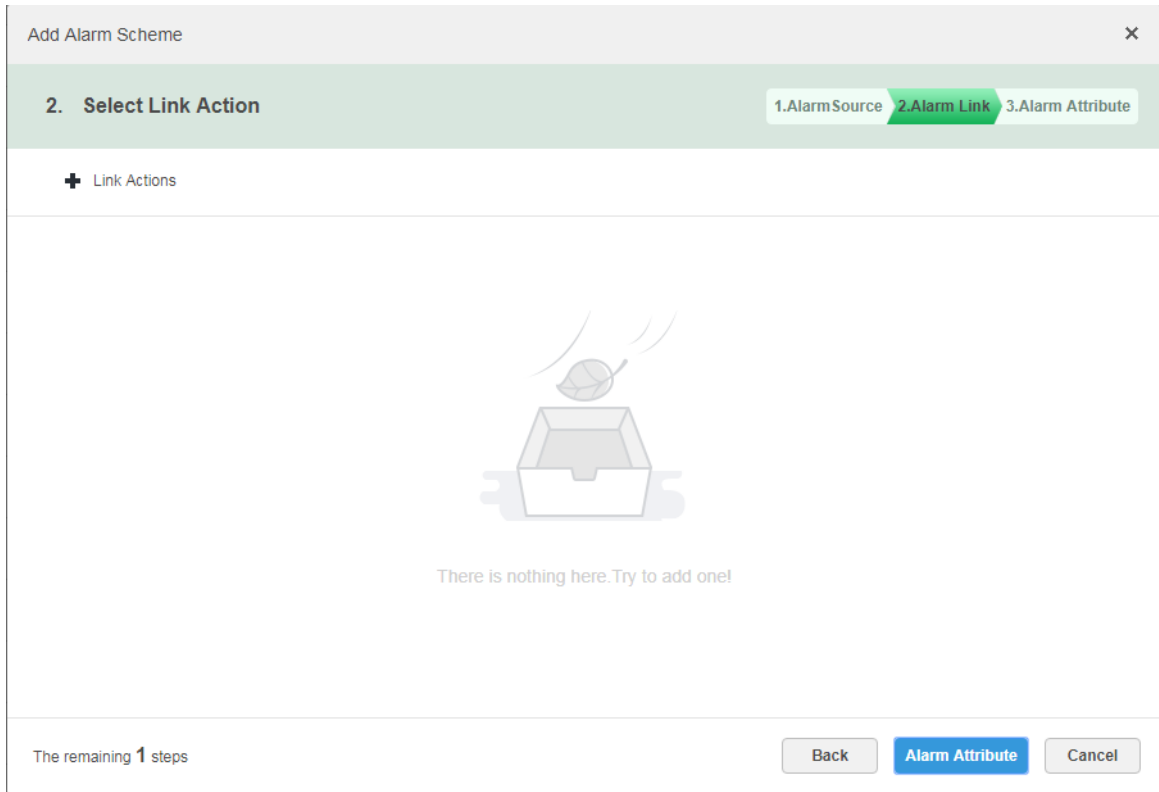
Alarm type selects "Alarm Input Channel", the alarm type is required to be the same as the one when editing encoding device.

- 2) Click "Alarm Link".

The system displays the interface of "Alarm Link". See Figure 4-50.



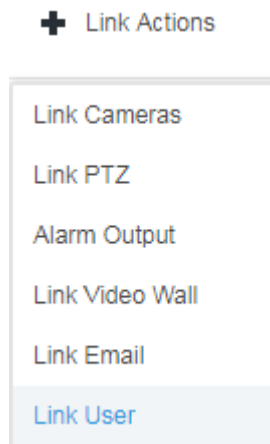
Figure 4-50



**Step 4** Configure alarm link.

- 1) Click **+**, the system pops out the window of link actions. See Figure 4-51.

Figure 4-51



- 2) Select link action, it supports several link actions.
  - ◇ Click "Link Cameras", set parameters. See Figure 4-52. Please refer to Table 4-3 for more details about parameters.

Figure 4-52

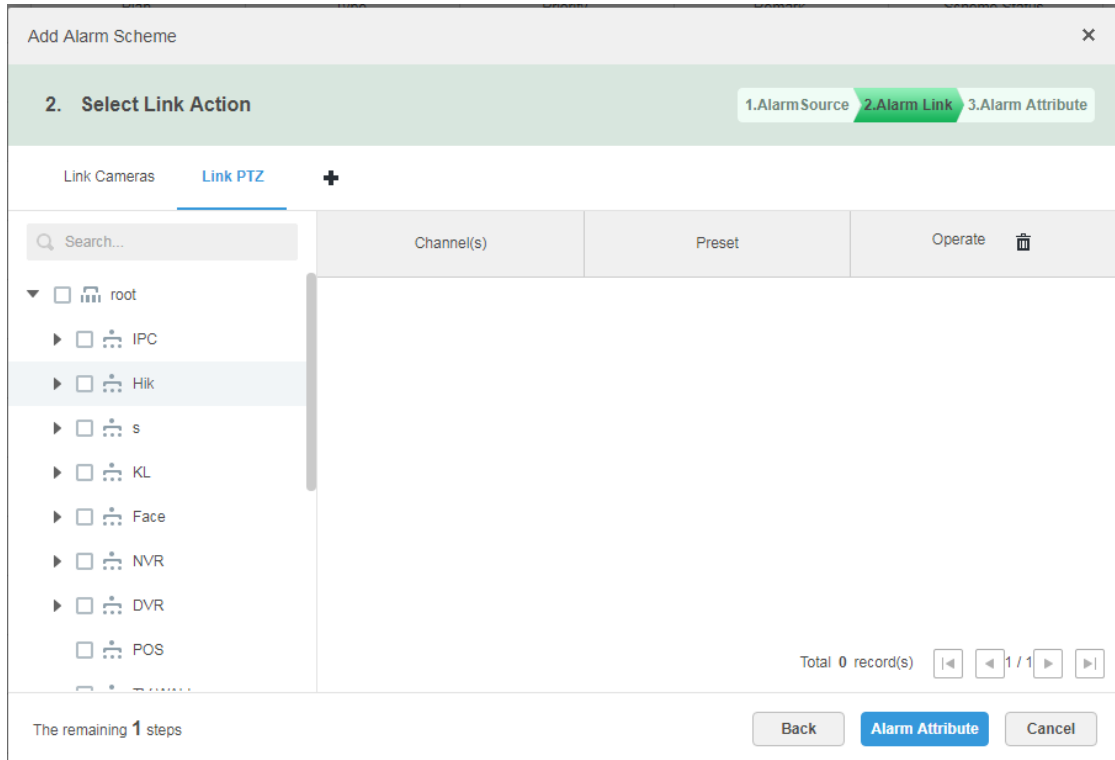
The screenshot shows a web interface for configuring an alarm scheme. The title is 'Add Alarm Scheme' with a close button. The current step is '2. Select Link Action', with progress indicators for '1. Alarm Source', '2. Alarm Link', and '3. Alarm Attribute'. Under 'Link Cameras', there are two radio buttons: 'Link Bind Camera' (selected) and 'Select Camera' (with an info icon). A 'Link bind camera prompt' explains that video channels bind themselves and source binding is configured on the device config page. Configuration fields include 'Position' (Store on Server), 'Stream Type' (Main Stream), 'Record Time' (input field with 's' suffix), and 'Prerecord Time' (input field with 's' suffix). Two checkboxes are present: 'Capture a picture of camera when alarm is triggered.' and 'Open camera video on client when alarm is triggered.'. At the bottom, there are 'Back', 'Alarm Attribute', and 'Cancel' buttons, and a note 'The remaining 1 steps'.

Table 4-3

Parameter	Note
<ul style="list-style-type: none"> <li><input checked="" type="radio"/> Link Bind Camera</li> <li><input type="radio"/> Select Camera <span style="color: blue;">!</span></li> </ul>	<ul style="list-style-type: none"> <li>● Link bind camera: Video channel has been bound with alarm source. It is to quickly configure scheme via resource binding of device management.</li> <li>● Select link camera: It needs link camera to manually select the alarm source.</li> </ul>
Position	If it is to set the position of storing video. It supports 3 options which are store on server, store on recorder and not stored respectively.
Stream	It is to set the stream type of recording video. Main stream and sub stream are clear but resource intensive.
Record Time	It is to set the length of video recording.
Prerecord Time	It is the recording time before setting link camera, the selected device is required to support record and it already exists in the device recording.
Capture picture when alarm is triggered.	Confirm if it captures camera picture.
Open camera video on client when alarm is triggered.	Confirm if it opens camera video window on the client during alarm.

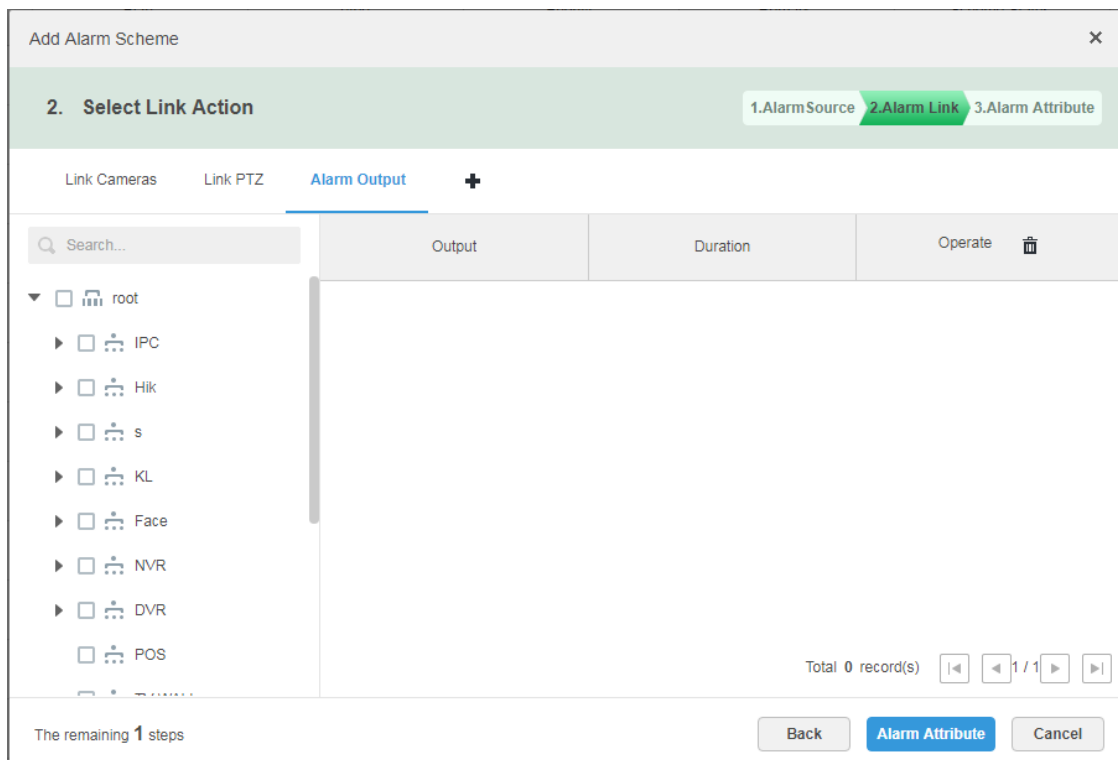
- ◇ Click "Link PTZ", select the channels which need PTZ to link device, set prerecord actions. See Figure 4-53.

Figure 4-53



- ◇ Click “Alarm Output”, select alarm output channel, set duration. See Figure 4-54.

Figure 4-54



- ◇ Click “Link Video Wall”, select link camera on the left of the interface, select video wall on the right of the interface. See Figure 4-55. Select “Link Bind Camera” and “Select Link Camera”, the interface will display differently,

please base on the actual display. Click “Video Wall Alarm Window Setup” to set duration and select the video channel which needs to be displayed on wall. See Figure 4-56.

Figure 4-55

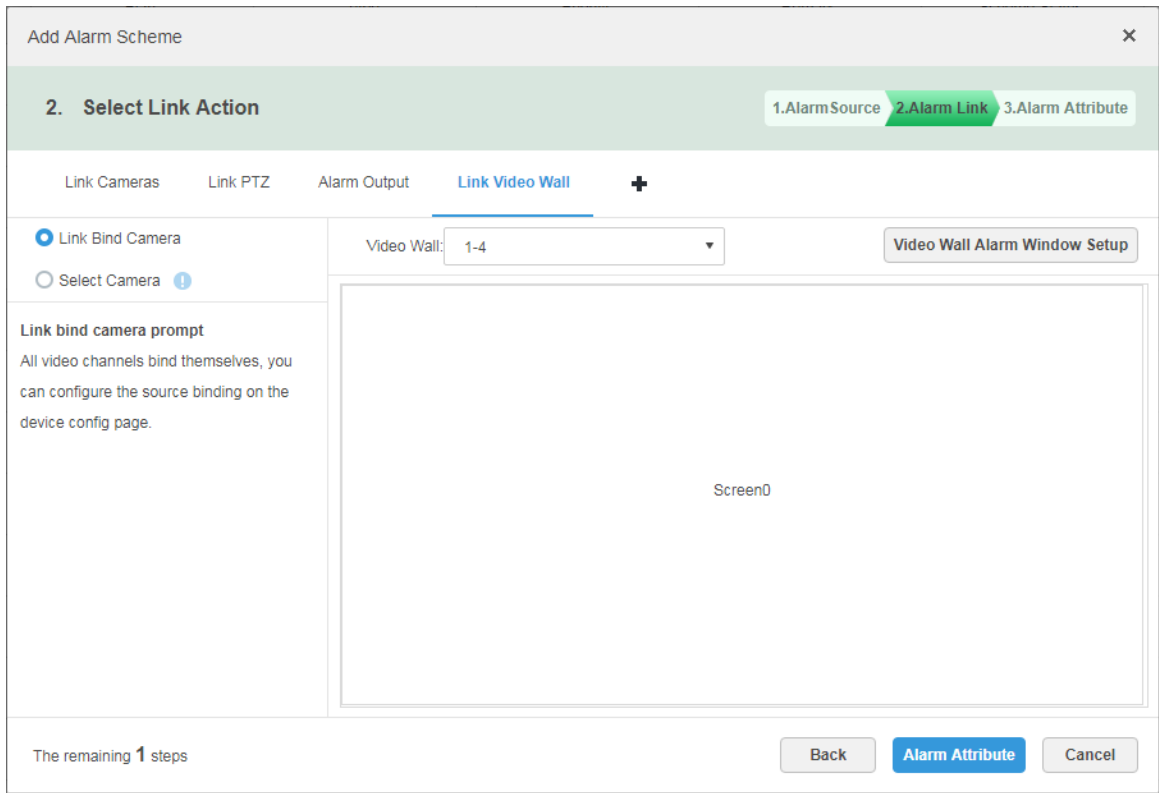
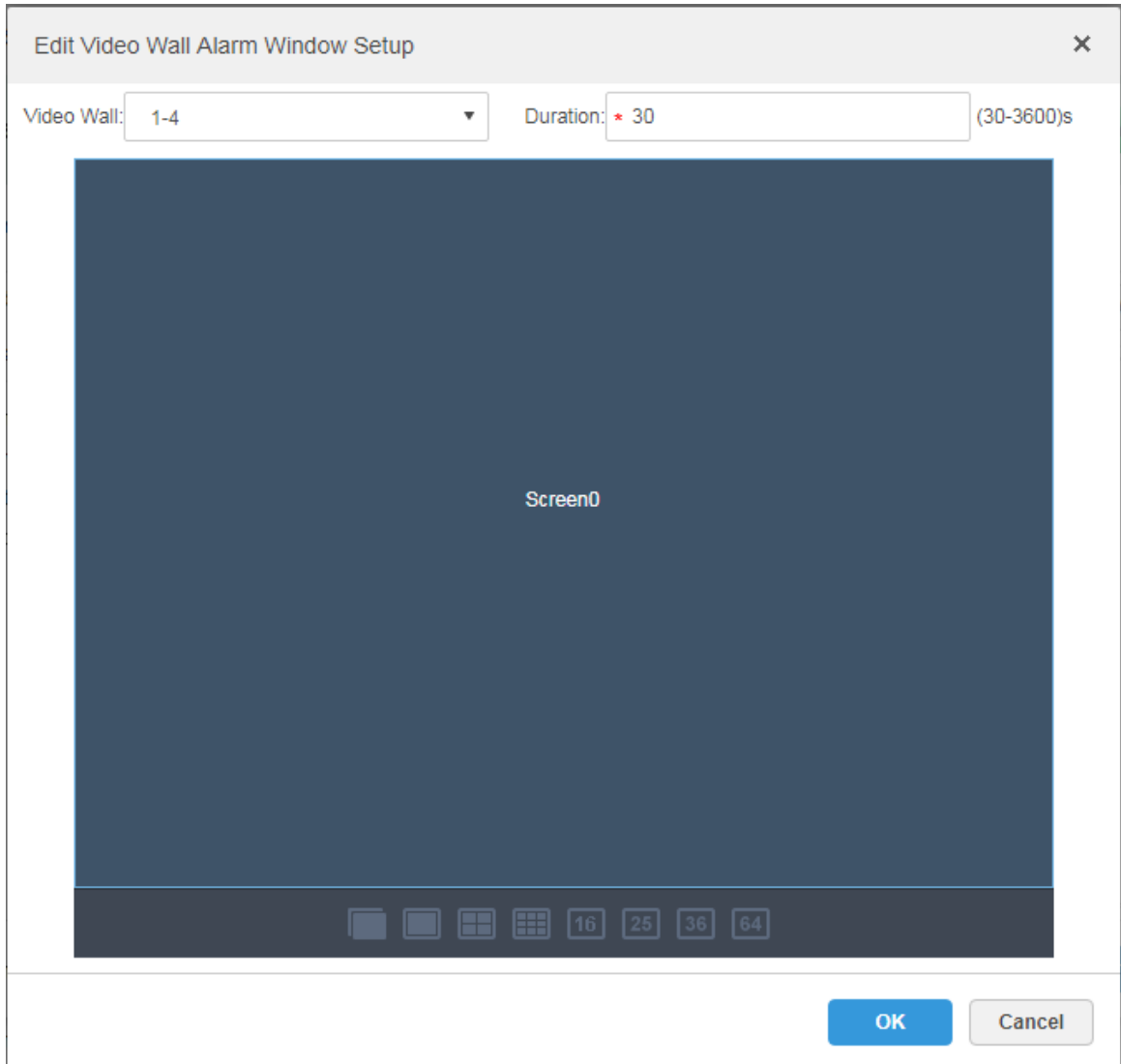


Figure 4-56



- ◇ Click “Link Email”, select email template and recipient. See Figure 4-57. The mail template can be configured, click the ▼ next to “Mail Template” and select “New Mail Template”, set new mail template. See Figure 4-58. Click “Alarm Time”, “Organization” and other buttons to insert buttons into “Email Theme” or “Email Content”.

Figure 4-57

Add Alarm Scheme [X]

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

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

Email Template: Default

Address: +

Subject: Event time Event source Event type

Send event image !

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

Time: Event time

Location: Org name

Event Source: Event source

The remaining 1 steps

Back Alarm Attribute Cancel

Figure 4-58

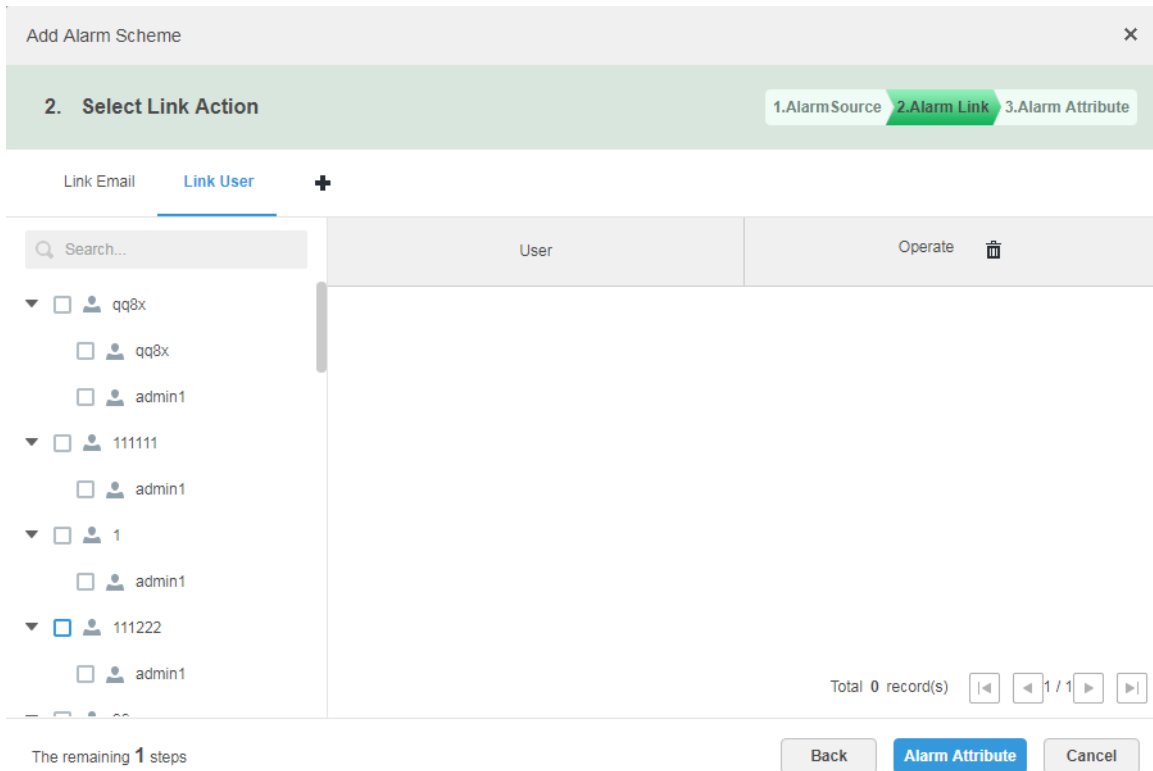
Add Alarm Scheme [X]

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

OK Cancel

◇ Click "User", select the users who need to be informed. See Figure 4-59.

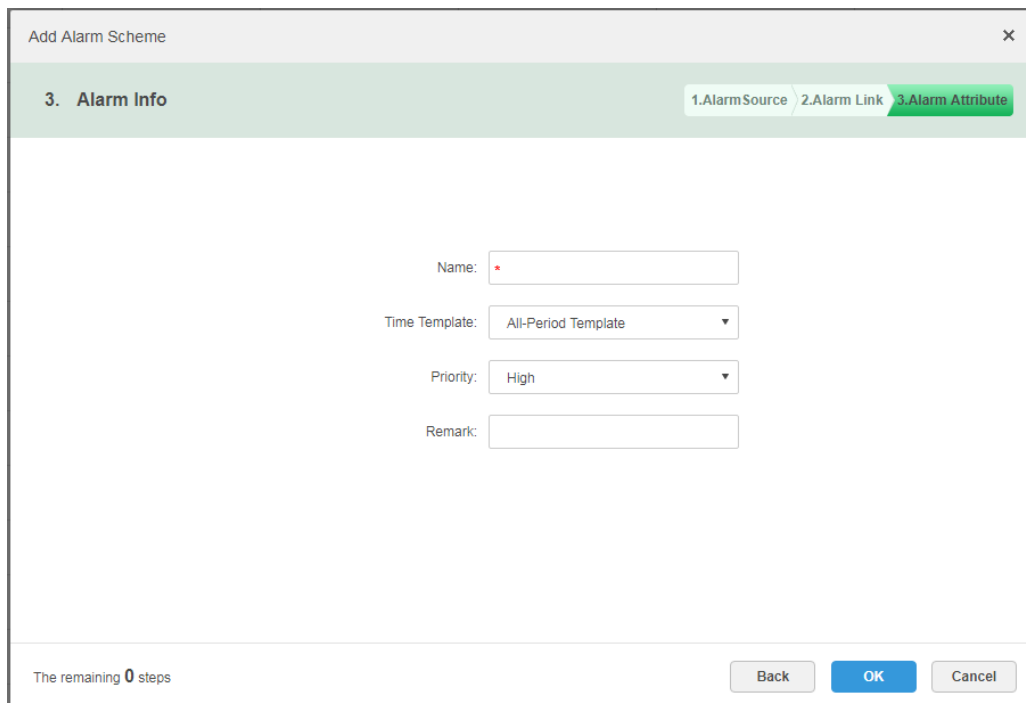
Figure 4-59



**Step 5** Click “Alarm Attribute”.

The system displays the interface of “Alarm Attribute”. See Figure 4-60.

Figure 4-60





**Step 6** Configure alarm attribute.

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


The system displays the added alarm scheme.

### Step 7 Enable/Disable Scheme.

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


## Operations

- Edit

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

- Delete

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

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

## 4.9 Configuring Map

Before using the electronic map function, you need to select the map category on the administrative side, including raster map, Google and Google offline map, and then drag the video device, alarm device and so on to the map on the DSS management side before you can use the map function on the client side. E-map supports alarm prompts, video viewing and video playback.

- Raster Map

A displayed picture, it is more suitable for indoor scenario. Place the camera in the fixed location indoors, such as parking lot (flat scene), people counting, retail and some other indoor scenarios. The server enables raster map by default.

- Google Online Map

Google online map, it needs network permission of accessing Google map to access the map client, it is to display the map of whole city via network and using the map info of Google online, it can zoom in and out, present the picture of magnificent city and it can be accurate to some spot in the city as well.

- Google Offline Map

Google offline map, deploy the offline map on other servers. The offline map can be accessed by accessing the client of the map and the server network of Google offline service.

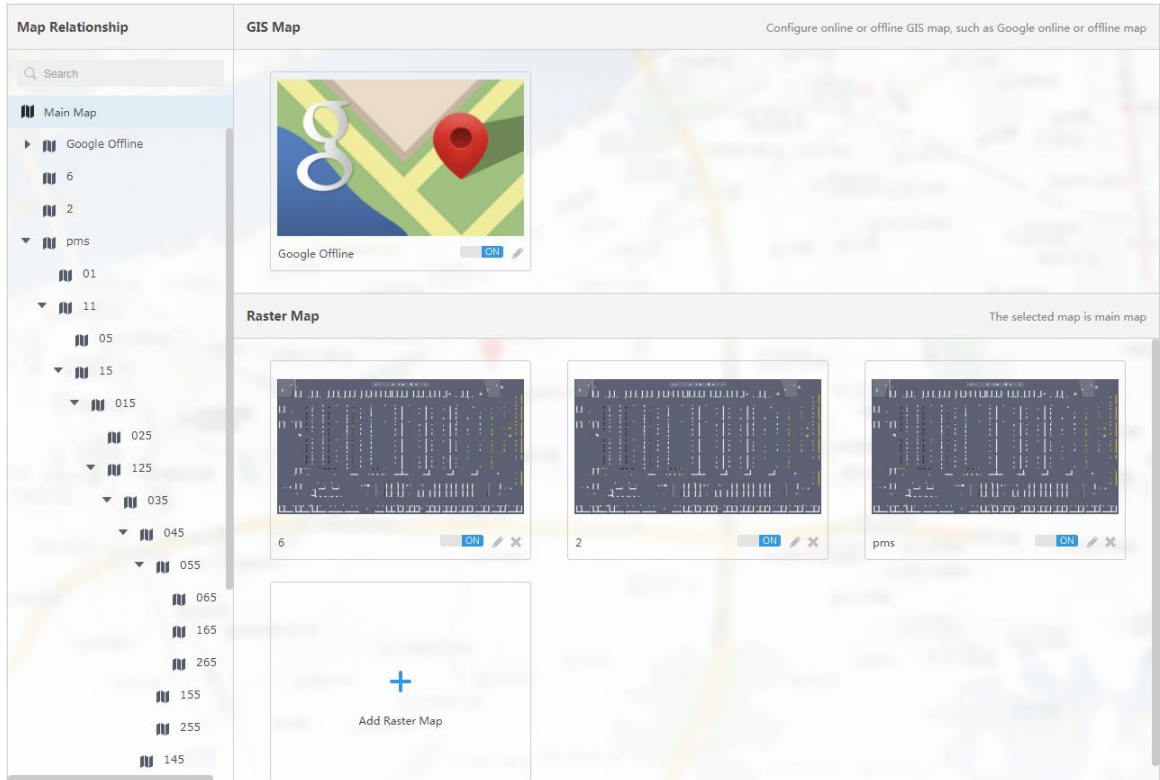
### 4.9.1 Editing Google Map

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

The system displays the map interface. See Figure 4-61.



Figure 4-61




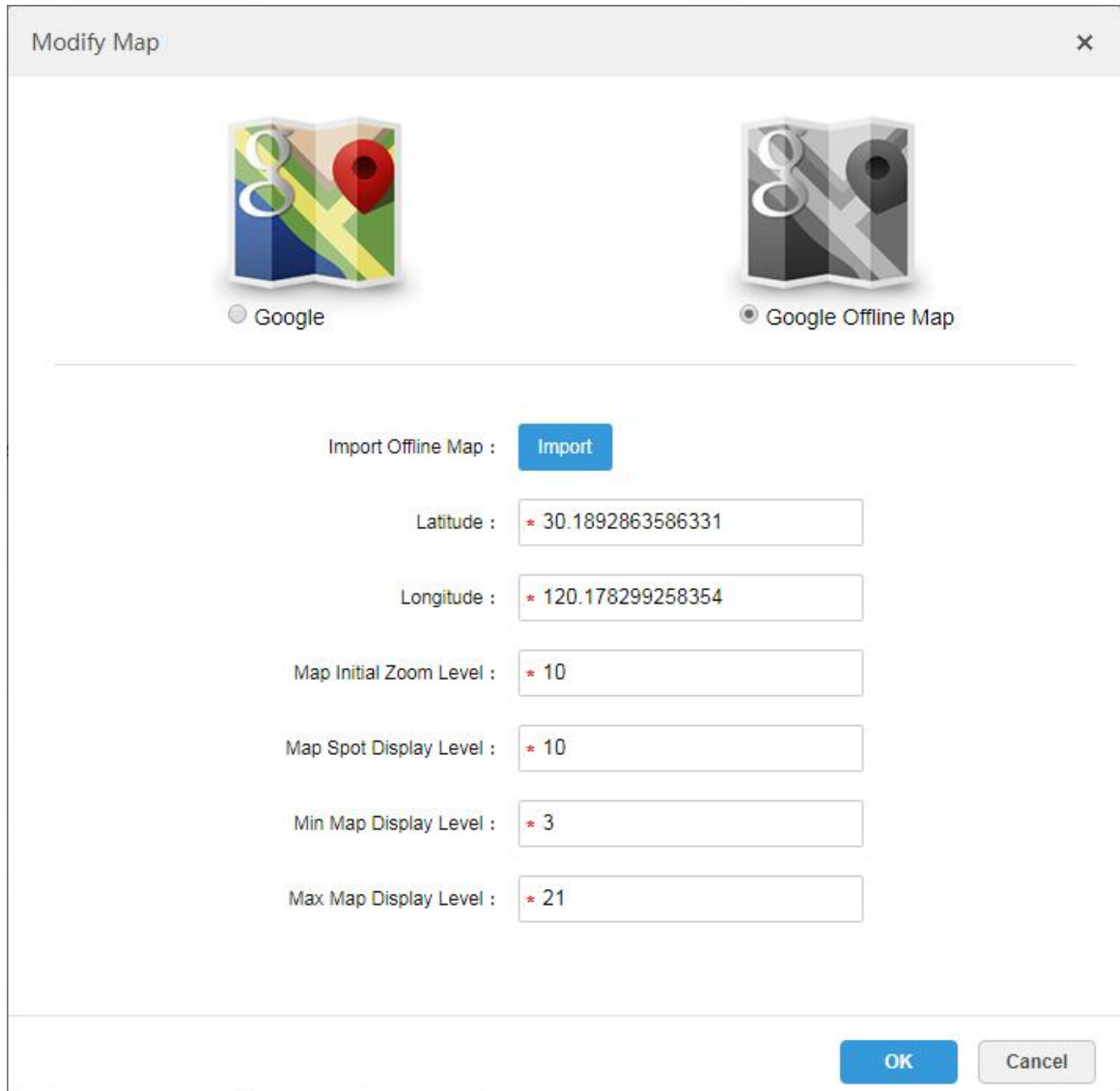
**Step 2** After click the  above the Google map.  
The system pops out the map config interface. See Figure 4-62.

Figure 4-62



- Google online map
  - 1) Select Google online map.
  - 2) Configure map info, click “OK”.
- Google offline map
  - 3) Select Google offline map.
  - 4) Click “Import” and import offline map.
  - 5) Configure map info, click “OK”.

## 4.9.2 Adding Hot Zone

It can add raster map as hot area, which is convenient for checking detailed scene picture. For example, it can be used in flat scene like parking lot.

Step 1 Click “Add Raster Map” on the “Map” interface.

The system pops out the interface of “New Main Map”. See Figure 4-63.

Figure 4-63

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

- Name:** A text input field with a red asterisk (\*) indicating it is a required field.
- Picture:** A text input field followed by a blue "Browse" button.
- Preview:** A large rectangular area containing a map icon (three vertical bars) and the text "Import raster map, support PNG, JPG, JPEG".
- Remark:** A text input field.

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

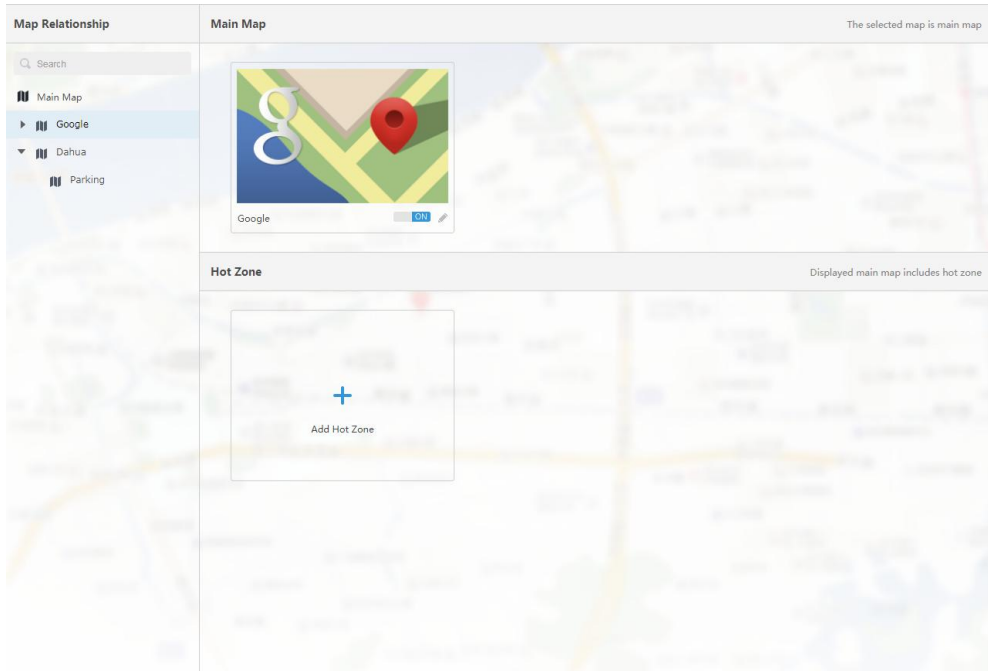
**Step 2** Enter "Name", select upload picture, click "OK".

You can continue to add several raster maps.

**Step 3** Add hot area.

- 1) Click the Google map or raster map on the left, it will display added hot zone module on the right. See Figure 4-64.

Figure 4-64



- 2) Click "Add Hot Area".  
The system displays the interface of "Add Hot zone". See Figure 4-65.

Figure 4-65

The image shows a dialog box titled 'Add Hot Zone' with a close button (X) in the top right corner. The form contains the following fields:

- Name:** A text input field with a red asterisk (\*) indicating it is required.
- Picture:** A text input field followed by a blue 'Browse' button.
- Preview:** A large rectangular area containing a gray map icon. Below this area, the text reads: 'Import raster map, support PNG, JPG, JPEG'.
- Remark:** A text input field.

At the bottom of the dialog, there are three buttons: 'OK' (blue), 'Next' (blue), and 'Cancel' (gray).

- 3) Enter hot zone name and upload picture, click "Next".
- 4) Drag icon and confirm hot zone location, and then click 'OK'.

## 4.9.3 Marking Device

**Step 1** Click the added main map on the navigation tree on the “Map” interface.

The system will display the map info. See Figure 4-66.

Figure 4-66

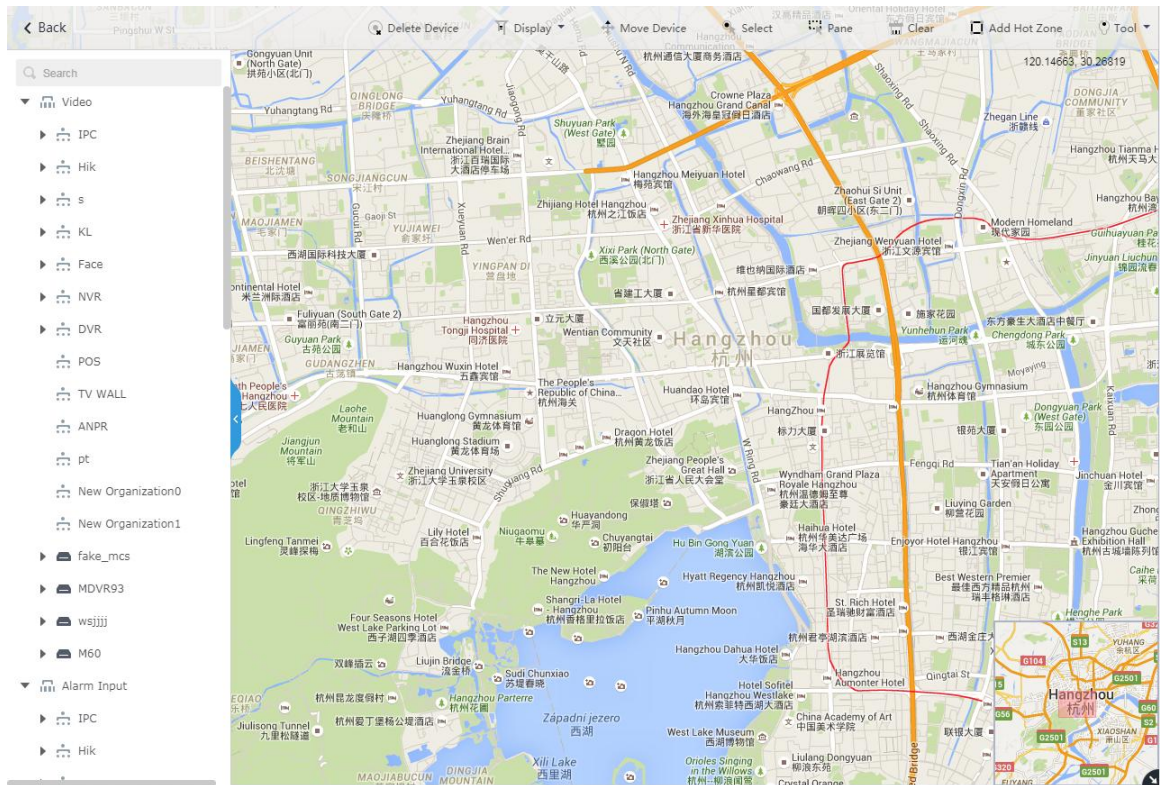


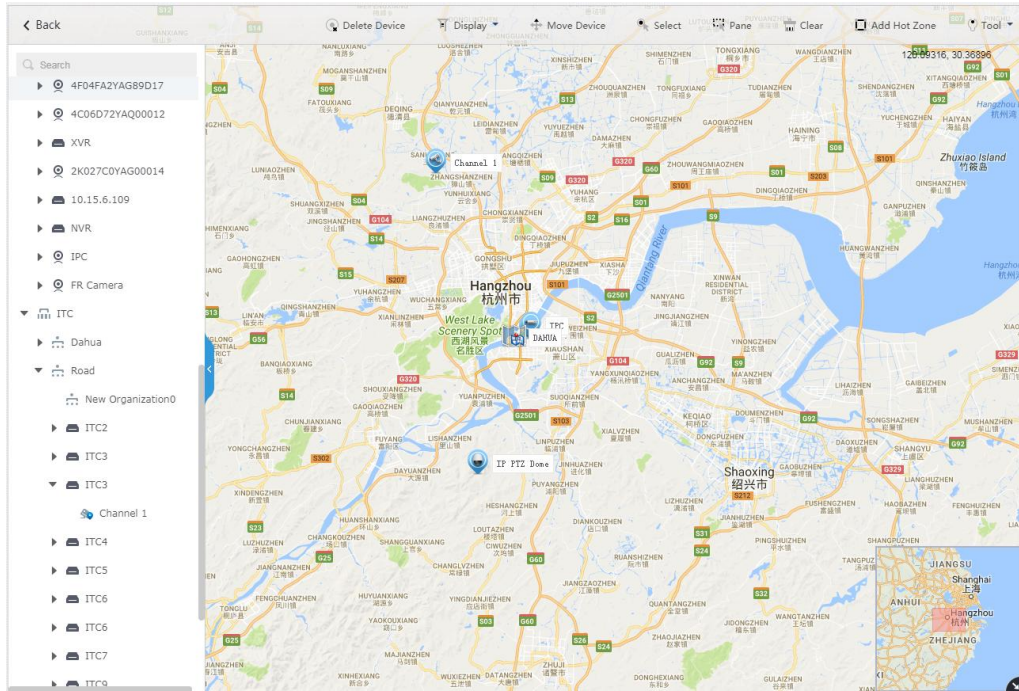
Table 4-4

Parameter	Note
Device Display	Filter and display video device, alarm input channel.
Delete Device	Click to move the device location on the map.
Select	Select device via clicking on it.
Pane	Select device via box selection.
Clear	Clear the boxing trace on the screen.
Add Hot Zone	Click “Add Hot Zone”, select location on the map and add hot zone map. After entering hot zone, it can also continue to add lower-level hot zone map. Click hot zone on the client map, the system will automatically link the map to the hot zone map.
Tool	Includes length, area, mark and reset. <ul style="list-style-type: none"> <li>Length: it is to measure the actual distance between two spots on the map.</li> <li>Area: It is to measure the actual area of the previous area on the map.</li> <li>Mark: It is to mark on the map.</li> <li>Reset: it is restored back the initial default location of the map.</li> </ul>

Others	<ul style="list-style-type: none"> <li>● Click hot zone, and it can modify the info of hot zone map.</li> <li>● Double click hot zone, the system will automatically skip to hot zone map, and then it can drag it into the channel on the hot zone map.</li> </ul>
--------	---


**Step 2** Drag the device channel from the left device tree to the corresponding location of the map. The interface is shown in Figure 4-67.

Figure 4-67



## 4.10 Adding Video Wall

It can refer to the content of the following chapter if you want to realize the business of displaying on wall.

**Step 1** Click  and select “Video Wall” on the interface of “New Tab”.

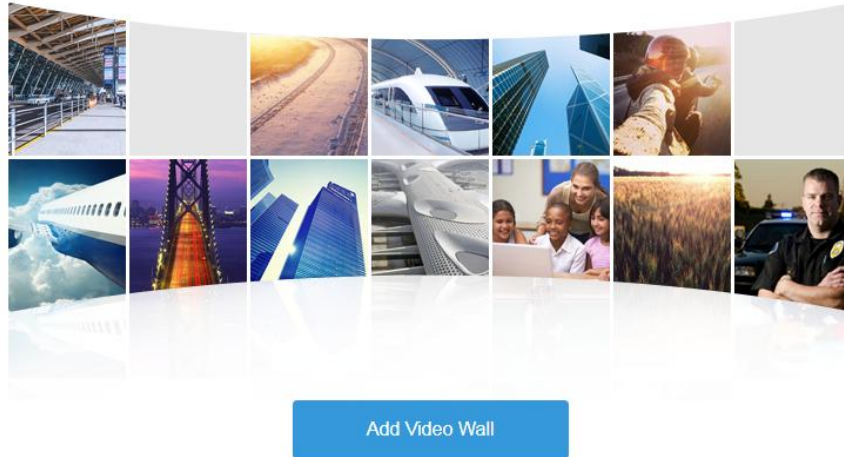
See Figure 4-68.



Figure 4-68

## Video Wall

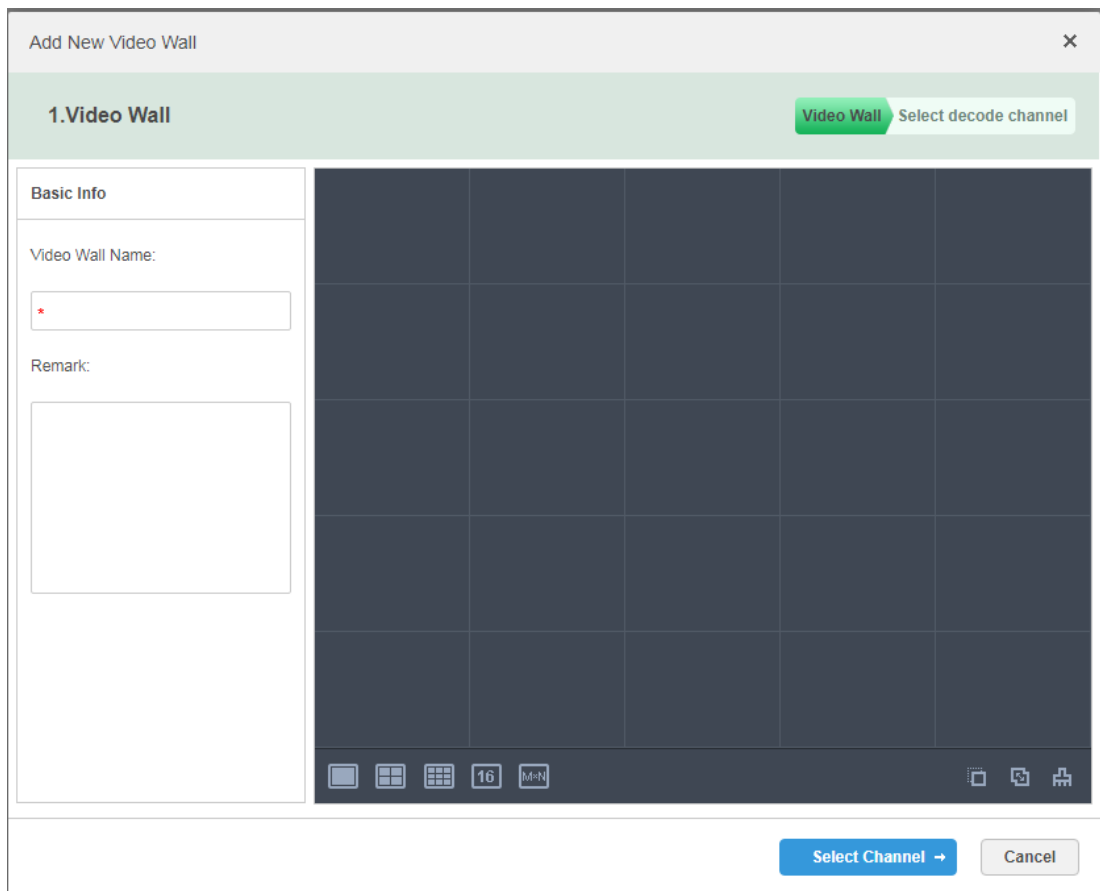
There is no video wall right now, please click the button to setup.



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

The system pops out the interface of "Add Video Wall". See Figure 4-69.

Figure 4-69

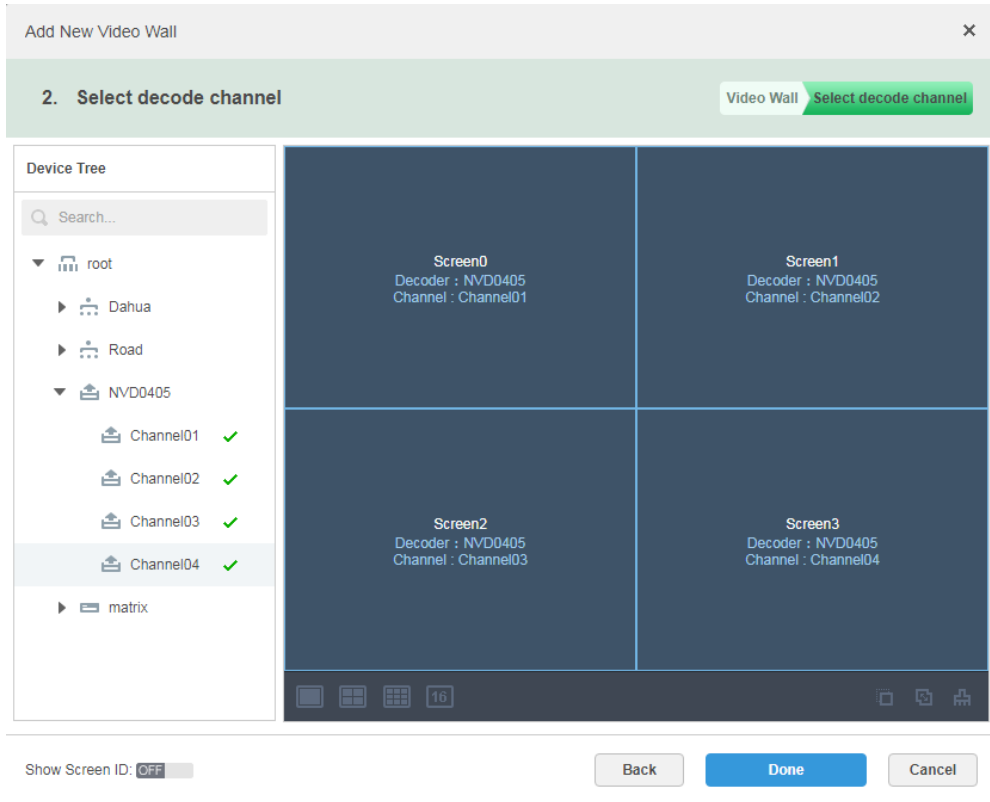


**Step 3** Enter "Video Wall Name", select window distribution.

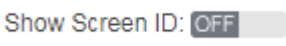
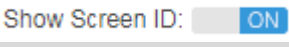
**Step 4** Click "Config Channel".

The system will display the interface of decoding channel. See Figure 4-70.

Figure 4-70



 **NOTE**

It can set if it displays ID in the screen,  means that the screen ID has been disabled; click the icon and it becomes , and then it means that screen ID has been enabled.

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

**Step 6** Click "Done".

## 4.11 Configuring Face Recognition

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

### 4.11.1 Creating Face Database

It supports creating staff library, managing the staff info in the library.

#### 4.11.1.1 Adding Face Library

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

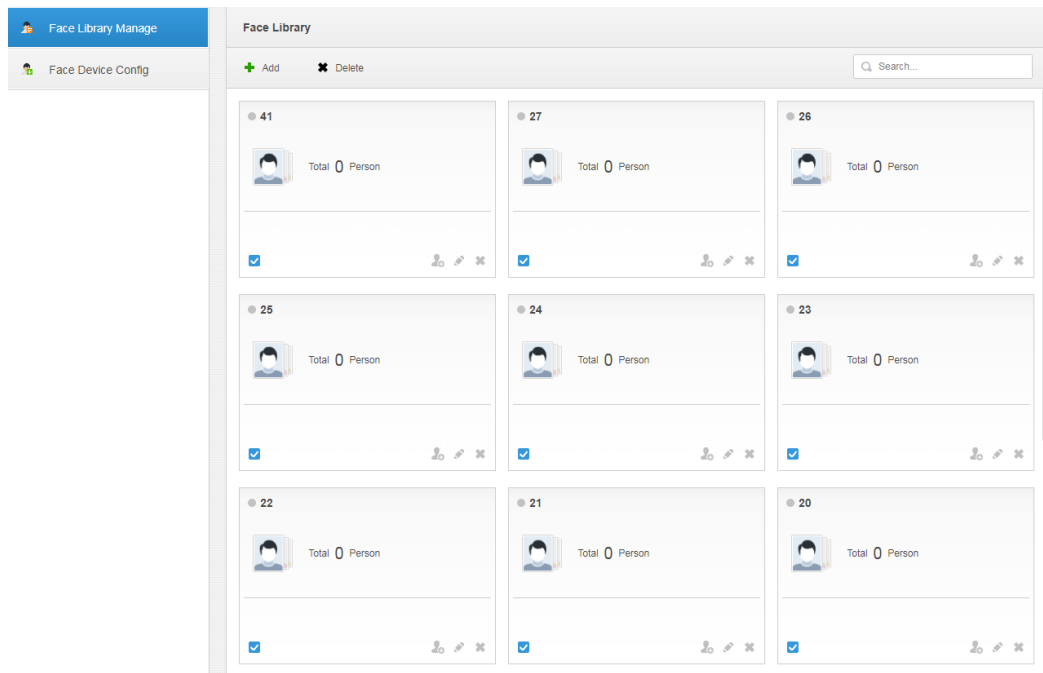


## Operation Steps

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

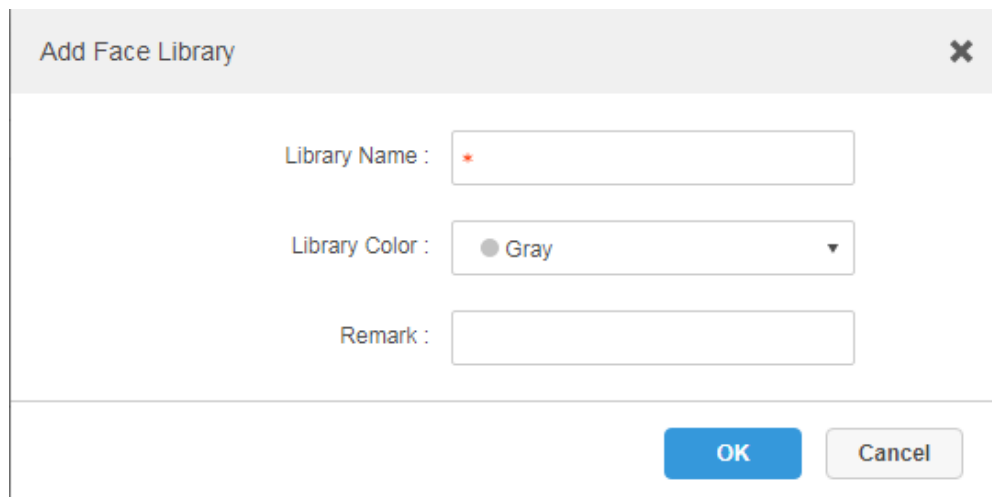
The system displays the interface of “Face Library”. See Figure 4-71.

Figure 4-71



**Step 2** Click ‘Add’.

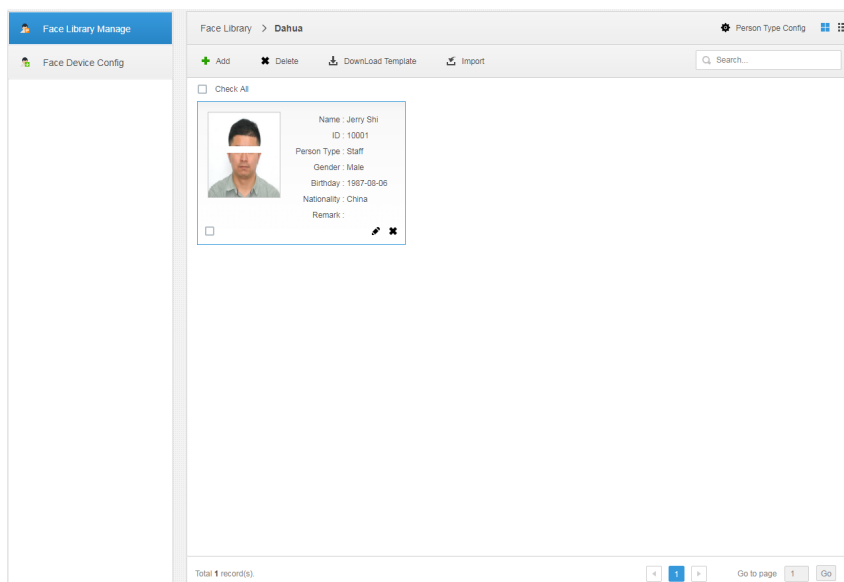
Figure 4-72

The screenshot shows the 'Add Face Library' dialog box. It has a title bar with a close button. The form contains three fields: 'Library Name' with a red asterisk indicating a required field, 'Library Color' with a dropdown menu currently set to 'Gray', and 'Remark' with an empty text area. At the bottom right, there are 'OK' and 'Cancel' buttons.




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

The interface is shown in Figure 4-73.

Figure 4-73



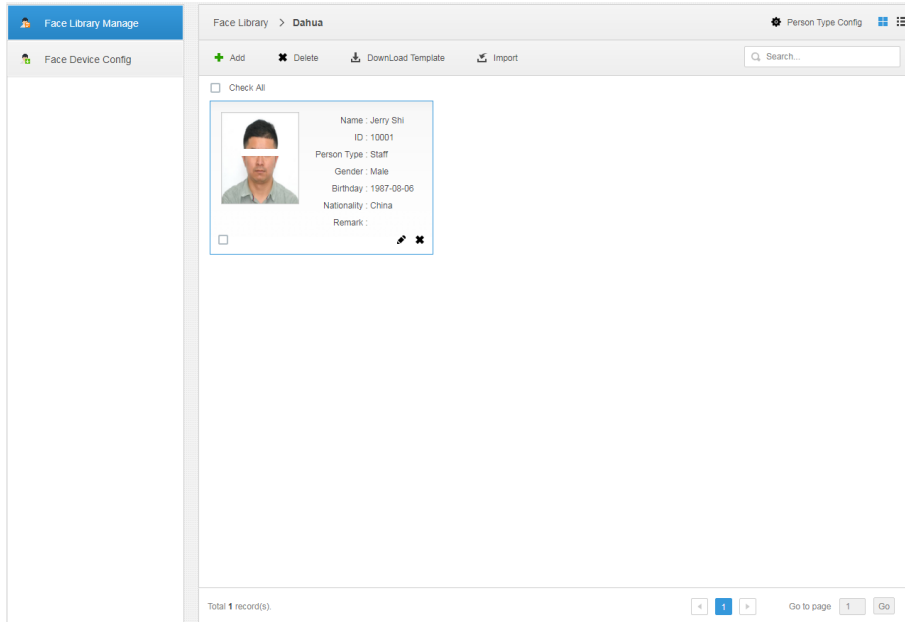
## Operations

- Search library  
Filter the library via face library type or keyword.
- Add face library  
Click  to add staff info. Please refer to “4.11.1.3 adding Staff Library Info”.
- Modify Staff Library  
Click  to modify library name and library description.
- Delete Staff Library  
Click  to delete face library only when there is no face info under the library.

### 4.11.1.2 Configuring person Type

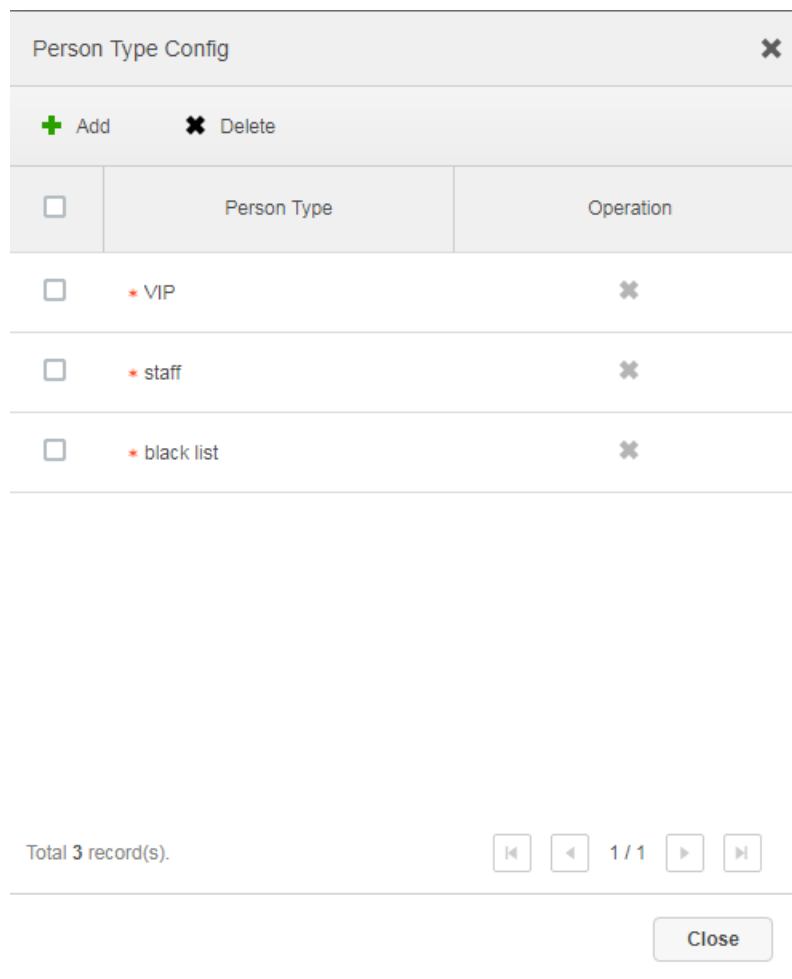
- Step 1 Click the face library which needs to be added with person on the interface of “Face Library Manage”.  
The interface is shown in Figure 4-74.

Figure 4-74



Step 2 Click “Person Type Config”. The interface is shown in Figure 4-75.

Figure 4-75



Step 3 Click ‘Add’ and enter type name in the column of “Person Type”.

Step 4 Click to disable the window.

### 4.11.1.3 Adding Face Library Info

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

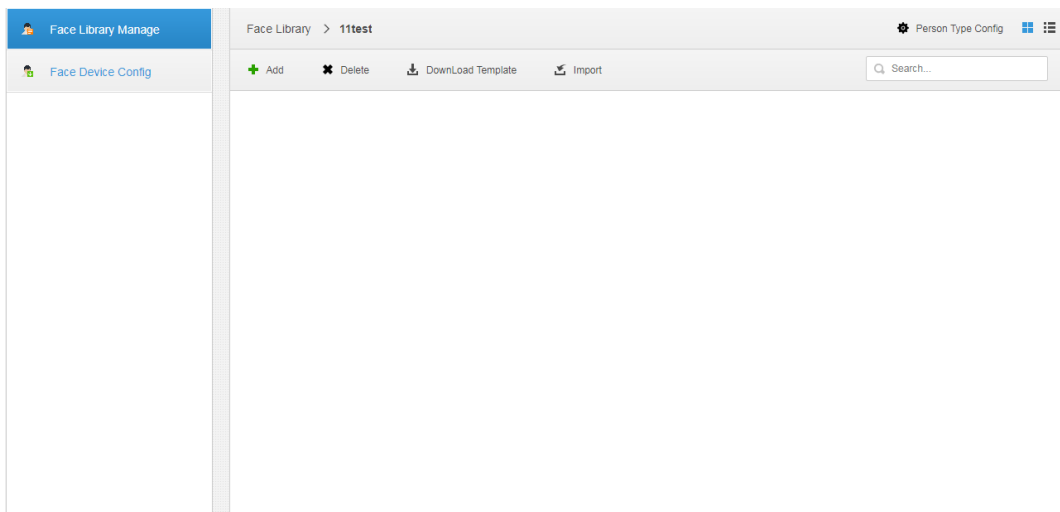
#### 4.11.1.3.1 Adding Individually

### Operation Steps

**Step 1** Enter the interface of adding person.

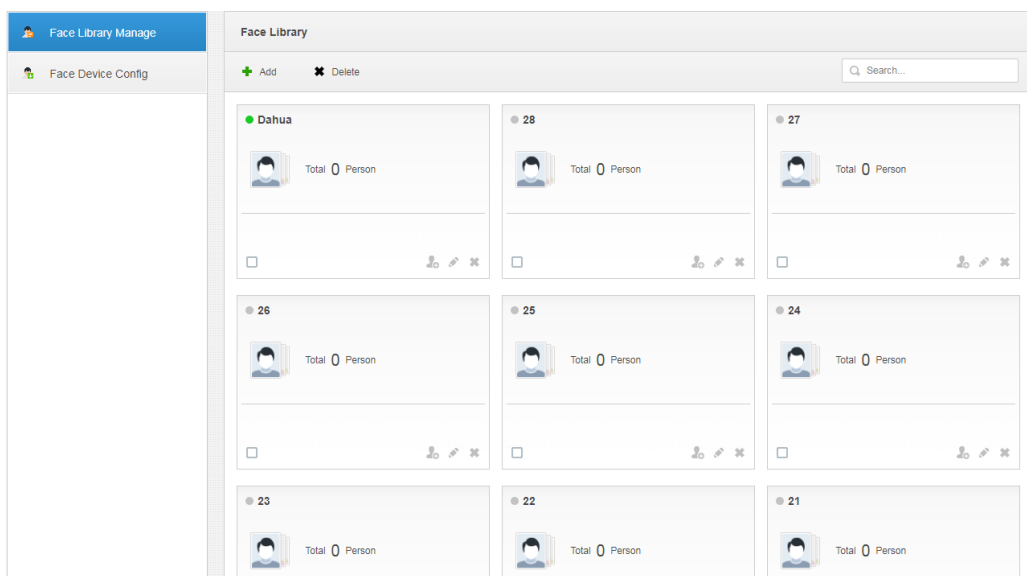
- Click the library which needs to be added with person on the interface of “Face Library Manage”. See Figure 4-76. Click “Add”.

Figure 4-76



- Click  on the card of person library, the interface is shown in Figure 4-77.

Figure 4-77



**Step 2** Enter person info.


**Step 3** Click profile photo and upload the picture.

**Step 4** Click “OK”.


Click “Continue to add” if it needs to add several persons, save person info and stay on the interface of “Add Person”, and then you can continue to add person info.

## Operations

- Query person

Enter key words into the query text box, press Enter or click  to query person.

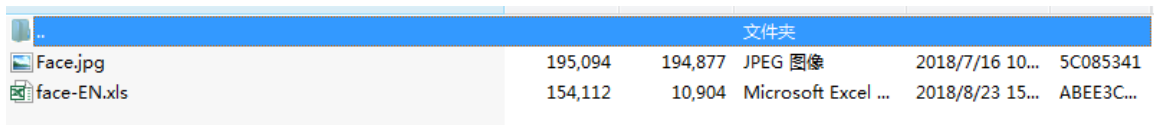
- Delete person

- ◇ Click  on person interface and then you can delete person individually.
- ◇ Select person, click ‘Delete’ to delete person in batches.

### 4.11.1.3.2 Batch Import

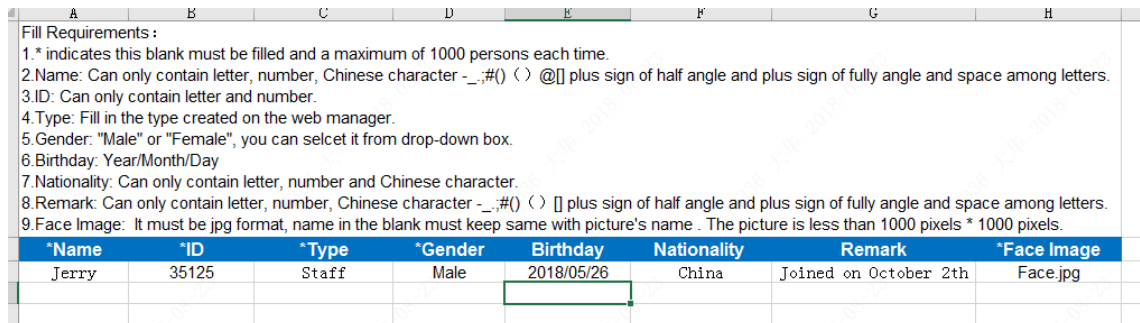
It needs to prepare person picture in advance if you want to import in batches, and compress it into zip RAR. RAR and excel style are shown in Figure 4-78 and Figure 4-79. Currently batch import supports max 1000 pictures at one time.

Figure 4-78



File Name	Size	Size	Format	Date	Code
Face.jpg	195,094	194,877	JPEG 图像	2018/7/16 10...	5C085341
face-EN.xls	154,112	10,904	Microsoft Excel ...	2018/8/23 15...	ABEE3C...

Figure 4-79



Fill Requirements :

- \* indicates this blank must be filled and a maximum of 1000 persons each time.
- Name: Can only contain letter, number, Chinese character -\_:#() ( ) @[] plus sign of half angle and plus sign of fully angle and space among letters.
- ID: Can only contain letter and number.
- Type: Fill in the type created on the web manager.
- Gender: "Male" or "Female", you can select it from drop-down box.
- Birthday: Year/Month/Day
- Nationality: Can only contain letter, number and Chinese character.
- Remark: Can only contain letter, number, Chinese character -\_:#() ( ) [] plus sign of half angle and plus sign of fully angle and space among letters.
- Face Image: It must be jpg format, name in the blank must keep same with picture's name. The picture is less than 1000 pixels \* 1000 pixels.

*Name	*ID	*Type	*Gender	Birthday	Nationality	Remark	*Face Image
Jerry	35125	Staff	Male	2018/05/26	China	Joined on October 2th	Face.jpg

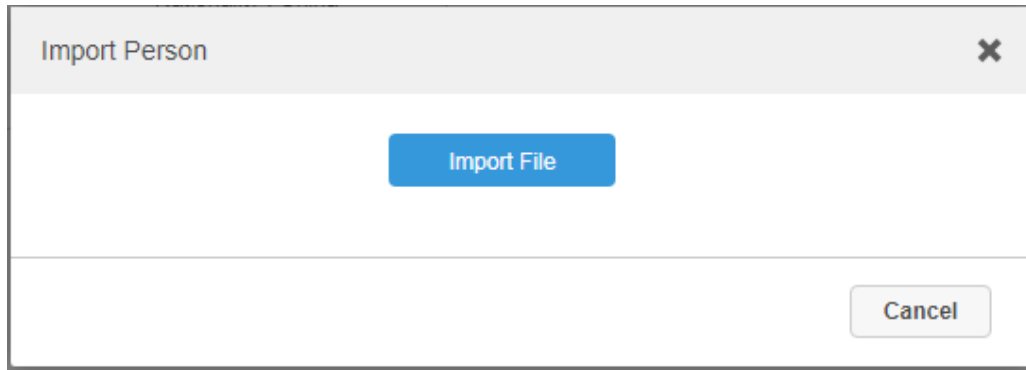
## Operation Steps

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

**Step 2** Click “Import”.

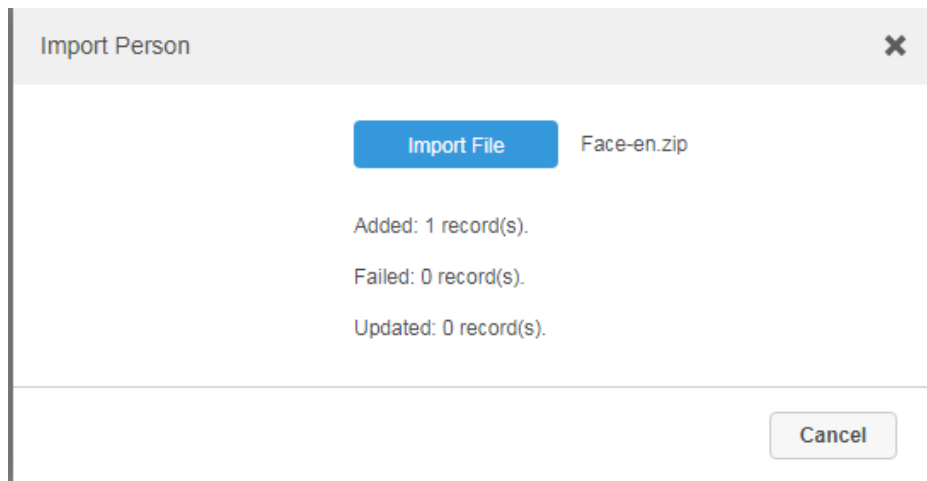
The system displays the interface of “Import Person”. See Figure 4-80.

Figure 4-80



**Step 3** Click “Import File” and upload compressed package according to prompt. The system will display import progress, it will display import info after import is completed. See Figure 4-81.

Figure 4-81



## Relevant Operations

Relevant operation is the same as that in “4.11.1.3.1 Add individually”.

## 4.11.2 Arm Config

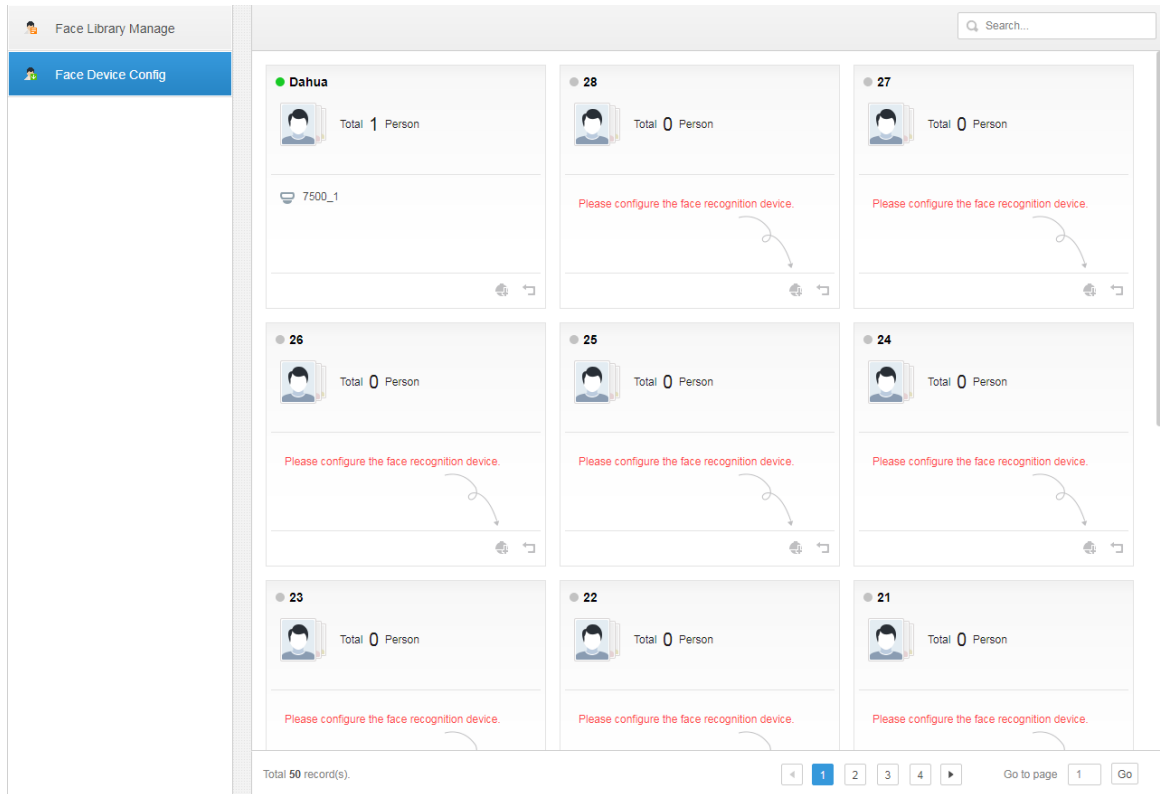
Arm means real-time comparison between capture image and face database image; it will trigger real-time alarm when the similarity reaches the value which has been set. It can make arm upon the face database where the person exists if it needs to take real-time surveillance over the designated person.

## Operation Steps

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

**Step 2** Click “Face Device Config” on the left of navigation bar. The system displays the interface of ‘Face Device Config’. See Figure 4-82.

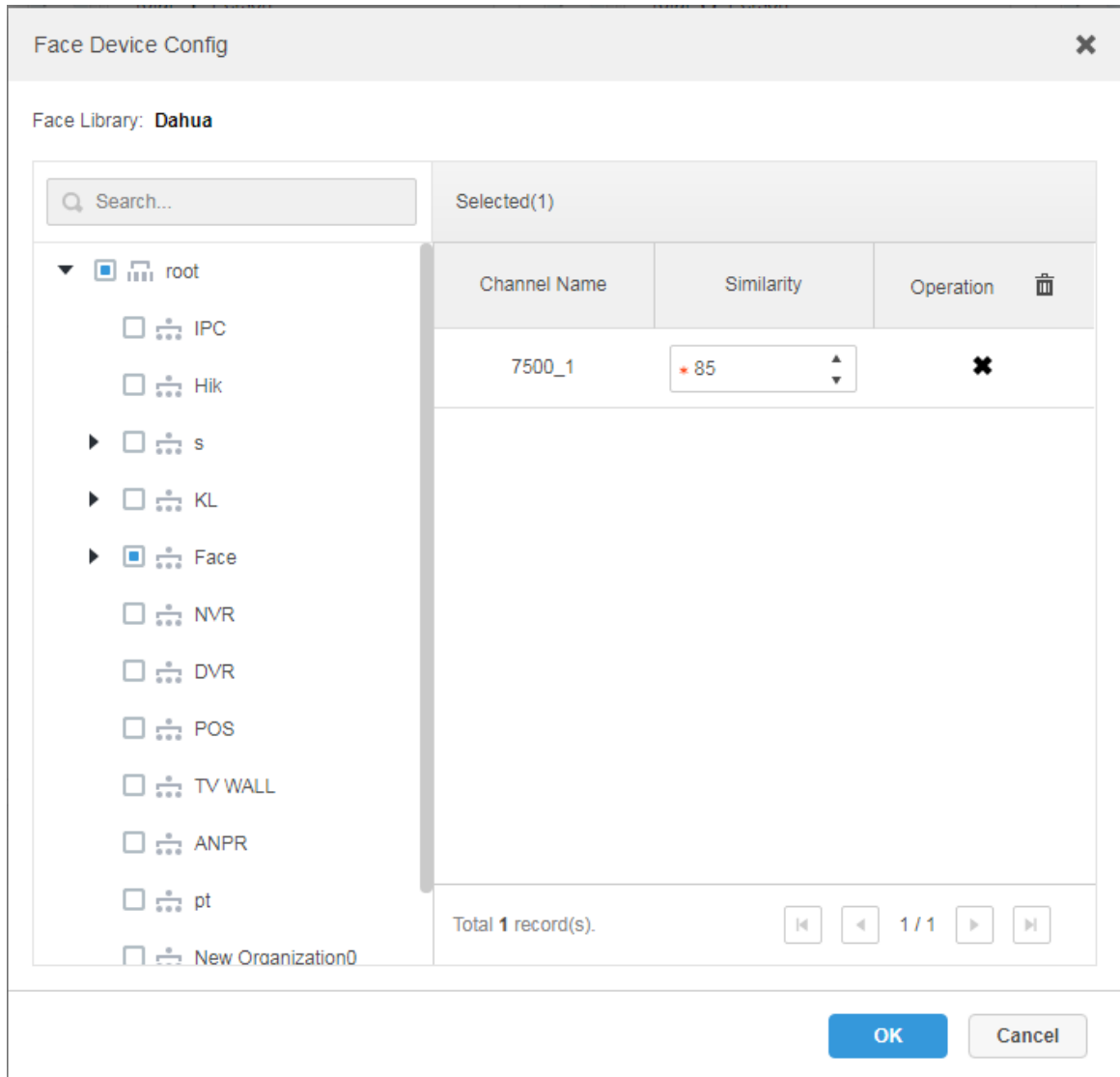
Figure 4-82



**Step 3** Click  to start arm.

The interface is shown in Figure 4-83.



Figure 4-83



Step 4 Select arm channel and set similarity.

Step 5 Click "OK" to complete arm.

## Relevant Operations

- Modify arm  
Arm has been implemented; click  and it can modify related device and similarity value on the arm interface.
- Disarm  
Click  on the interface of "Arm Manage" to disarm.



## 4.12 Adding Vehicle Blacklist

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

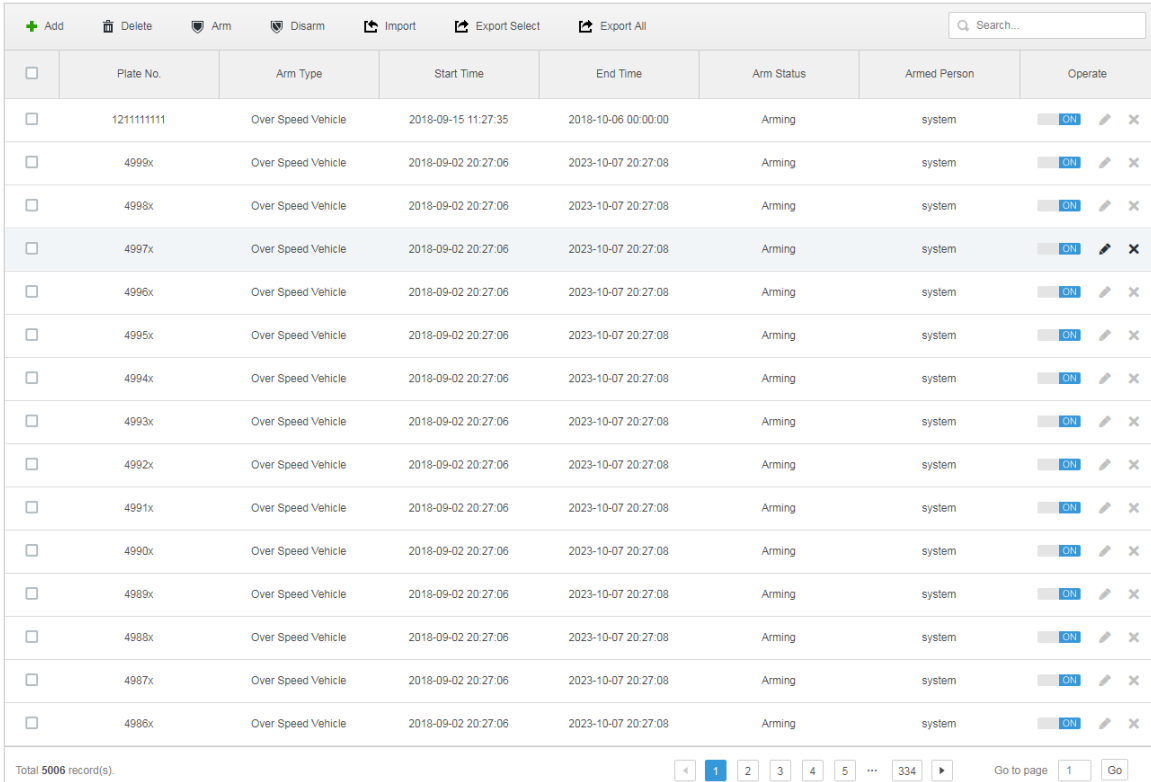
It can refer to the chapter when it needs to realize the business of road surveillance.































### Steps

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

The system displays the interface of “Vehicle Blacklist”. See Figure 4-84.

Figure 4-84



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

Total 5006 record(s).

Page navigation: 1 2 3 4 5 ... 334 Go to page 1 Go

**Step 2** Click ‘Add’.

The system displays the interface of “Add Arm”. See Figure 4-85.

Figure 4-85

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

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

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


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

**Step 4** Click "OK".


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

## Operations

- Modify vehicle blacklist

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

- Delete vehicle blacklist

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

- Arm/Disarm

Select vehicle arm info, click 'Arm" to arm the vehicle; Click 'Disarm" to disarm the vehicle.

- Import

Click "Import" and it can import vehicle arm info according to template.

 **NOTE**

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

- Export

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

## 4.13 System Maintenance

### 4.13.1 Service Management


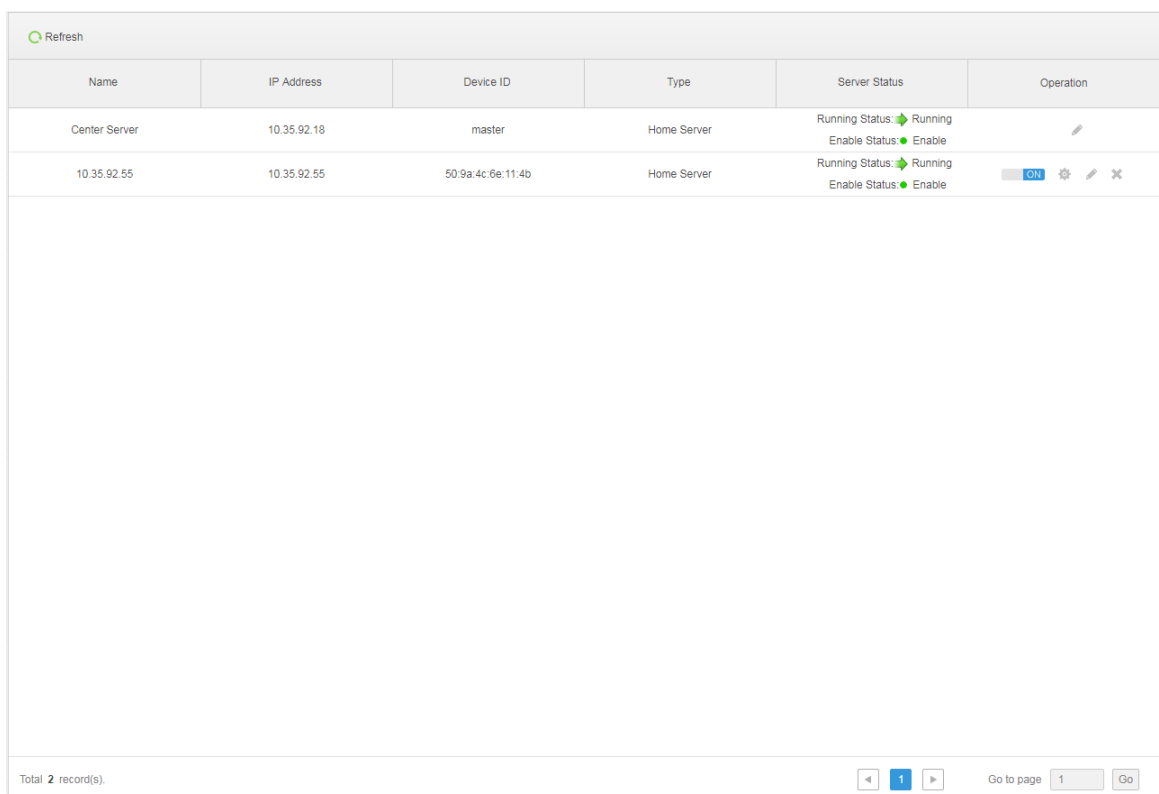









Click  and select "Service Management" on the interface of "New Tab", which is shown in Figure 4-86.

Figure 4-86





Name	IP Address	Device ID	Type	Server Status	Operation
Center Server	10.35.92.18	master	Home Server	Running Status:  Running Enable Status:  Enable	
10.35.92.55	10.35.92.55	50.9a.4c.6e:11:4b	Home Server	Running Status:  Running Enable Status:  Enable	 ON   

Total 2 record(s).

Go to page 1 Go

- Click  and edit the server info.

-  Means the server is not enabled; click it and the icon becomes , which means it has enabled the server.

- Click  to distribute the server type.

- Click  to delete the server info.

## 4.13.2 Backup and Restore

DSS management end supports backing up configured info and save it to local PC, meanwhile it supports restoring system via backup file, which is convenient for system maintenance and guarantee system security.


### NOTE

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

### 4.13.2.1 System Backup

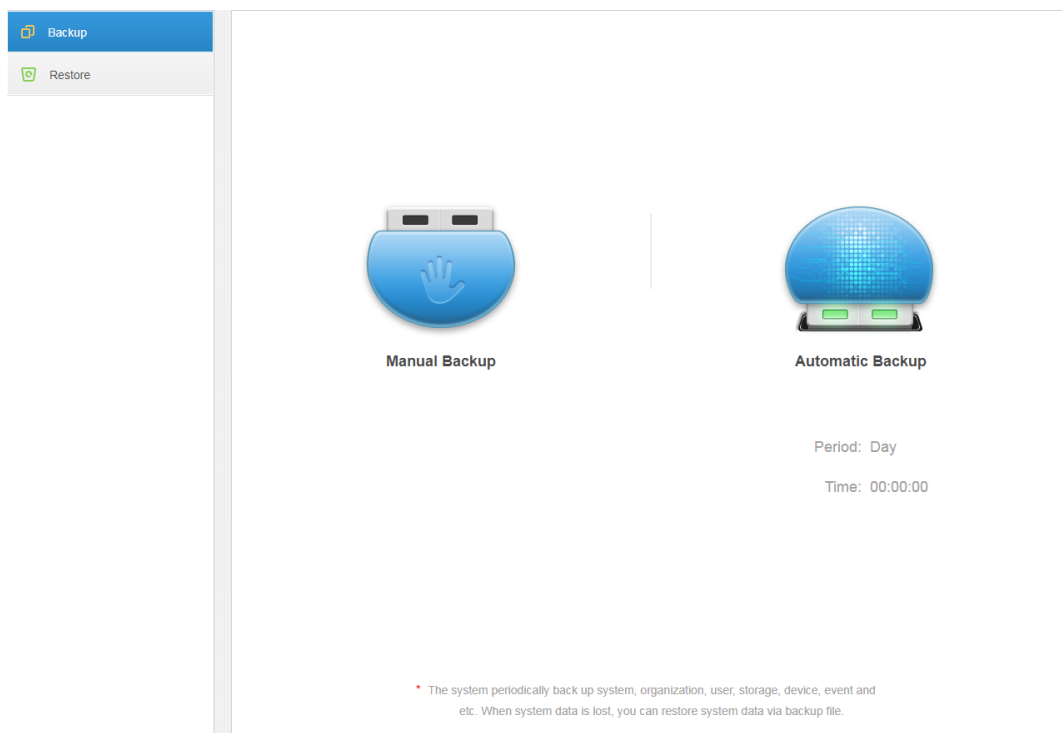
In order to guarantee the security of user data, DSS PROFESSIONAL system provides data backup function. The backup includes manual backup and automatic backup.

#### Manual Backup

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

The system displays the interface of “Backup”. See Figure 4-87.

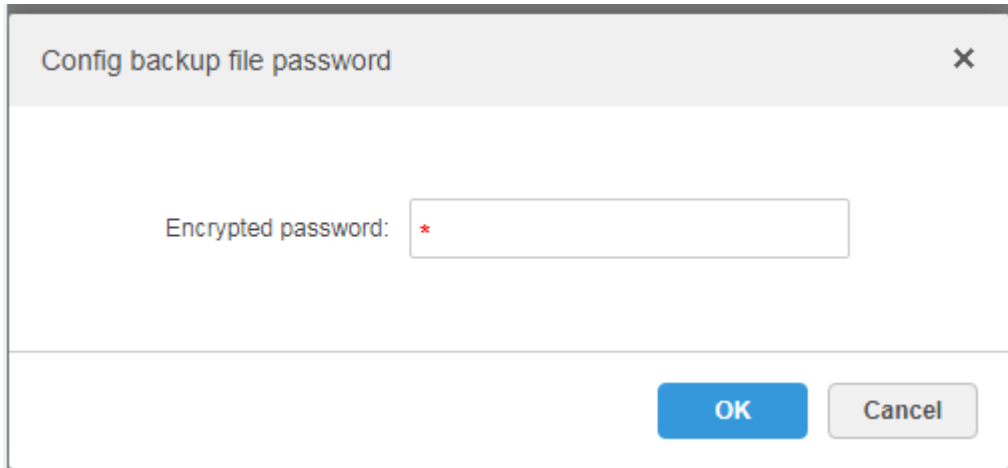
Figure 4-87



**Step 2** Click “Manual Backup”.

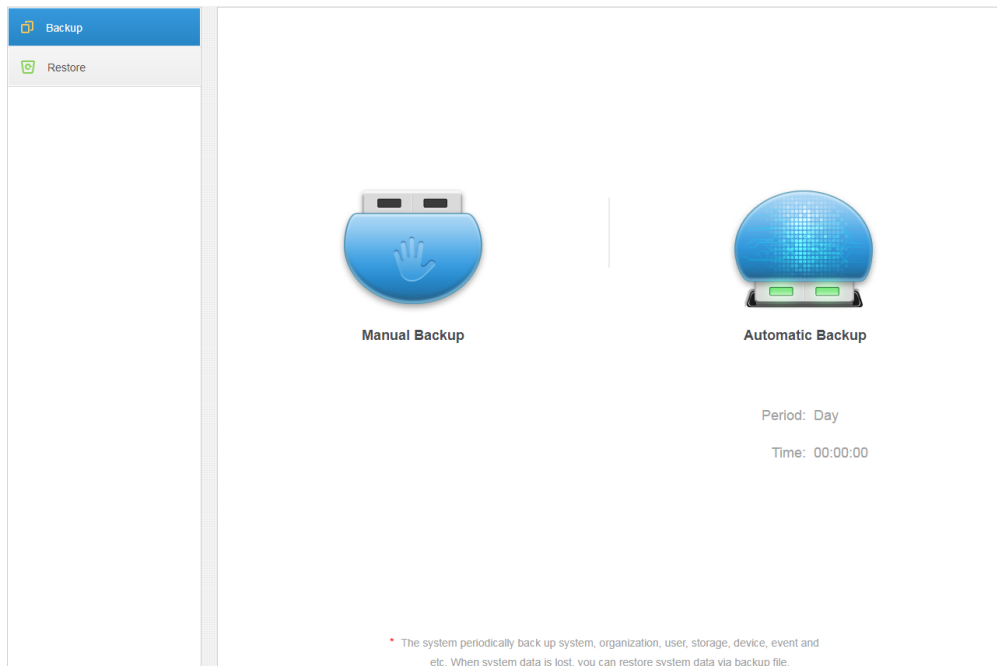
The system displays the interface which is shown in Figure 4-88.

Figure 4-88




- Step 3** Enter encrypted password, click “OK”.  
The backup result is displayed in Figure 4-89.

Figure 4-89



## Automatic Backup

- Step 1** Click  and select “Backup and Restore” on the interface of “New Tab”.

- Step 2** Click “Auto Backup”.

The system pops out the interface of “Auto Backup”. See Figure 4-90.

Figure 4-90

Automatic Backup

Backup Path: Automatically backup to the server.

Period: Day

Time: 00:00:00

Encrypted password: \*

OK Cancel

**Step 3** Select backup period, it includes: never, day, week, and month. See Figure 4-91.

Figure 4-91

Day

Never

Day

Week

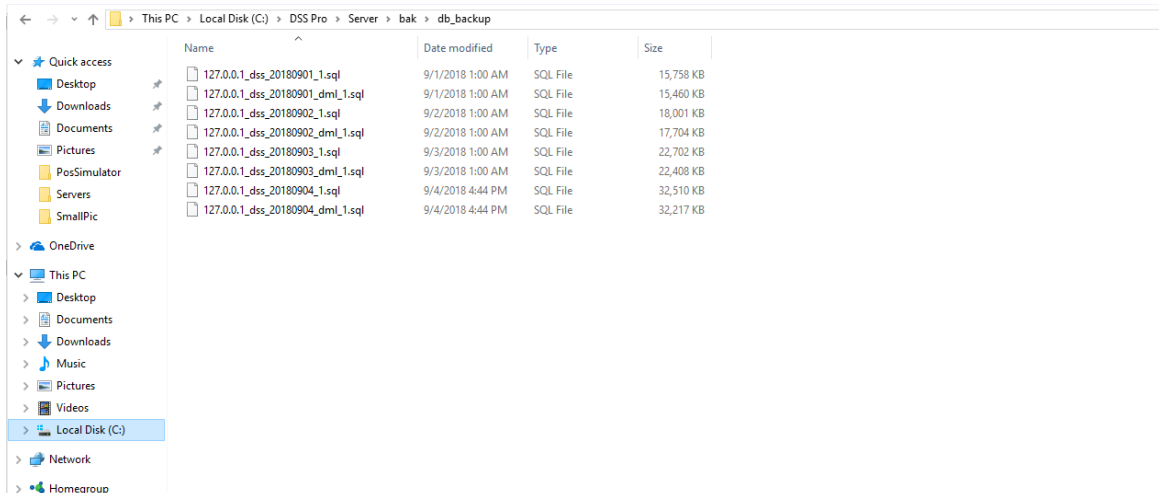
Month

**Step 4** Click “Ok” to save config.

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

**Step 5** Check the auto-backup file on the server, the default backup path is -Servers-bak-db\_backup. See Figure 4-92.

Figure 4-92



### 4.13.2.2 System Restore

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



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

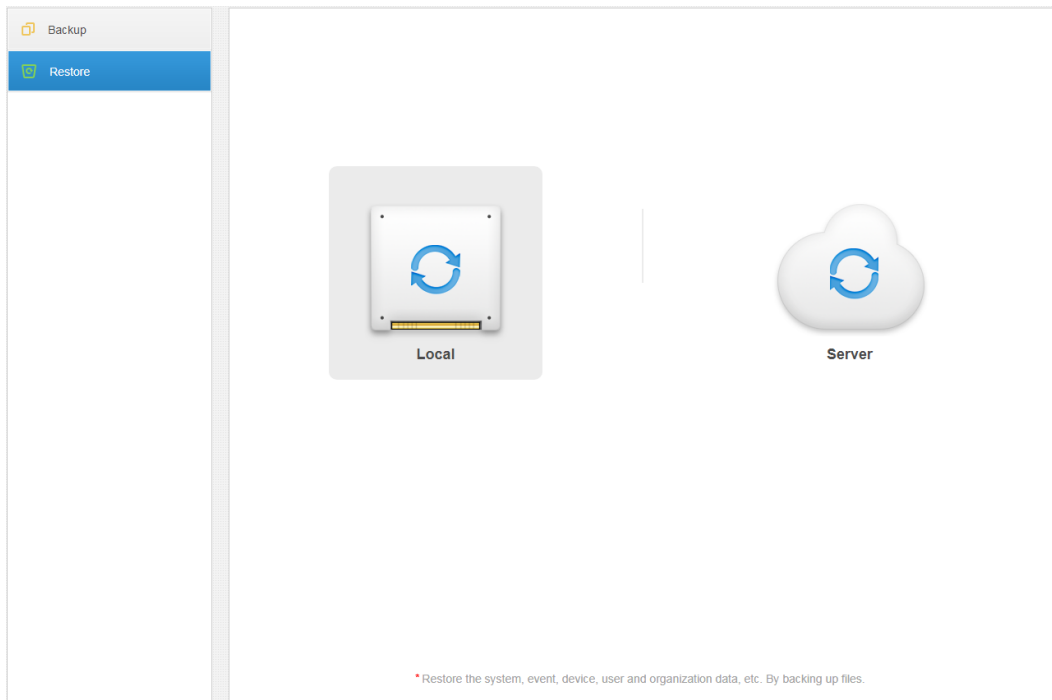
### Local

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

**Step 1** Select "Restore" tab.

The system enters the interface of "System Restore". See Figure 4-93.

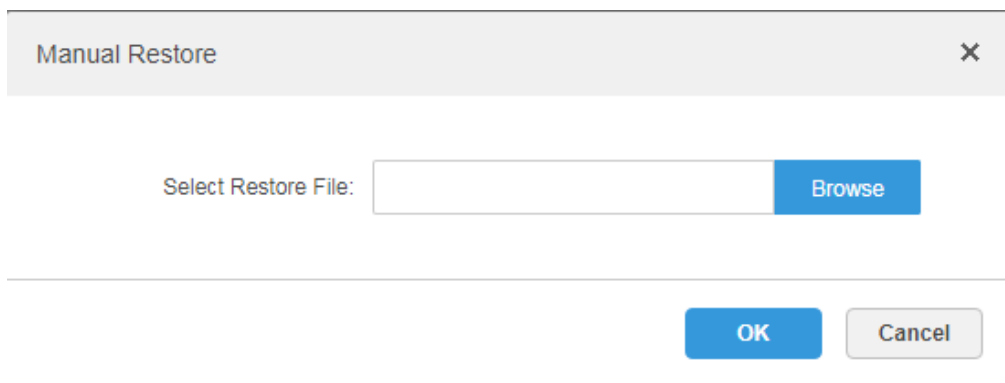
Figure 4-93



**Step 2** Click “Local”.

The interface is shown in Figure 4-94.

Figure 4-94

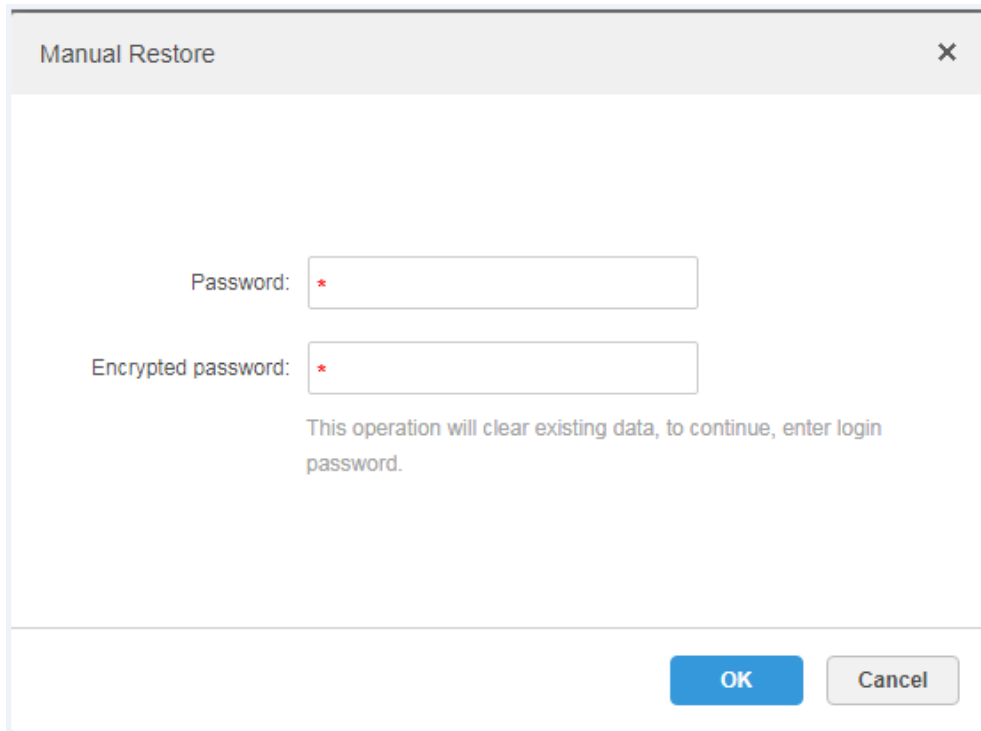


**Step 3** Click “Browse”, select file and then click “OK”.

**Step 4** Enter administrator “Login Password” and backup file “Encrypted Password”. See Figure 4-95.



Figure 4-95



The image shows a dialog box titled "Manual Restore" with a close button (X) in the top right corner. Inside the dialog, there are two input fields: "Password:" and "Encrypted password:", each followed by a red asterisk and a text box. Below these fields is a warning message: "This operation will clear existing data, to continue, enter login password." At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (grey).

Step 5 Click "OK".

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

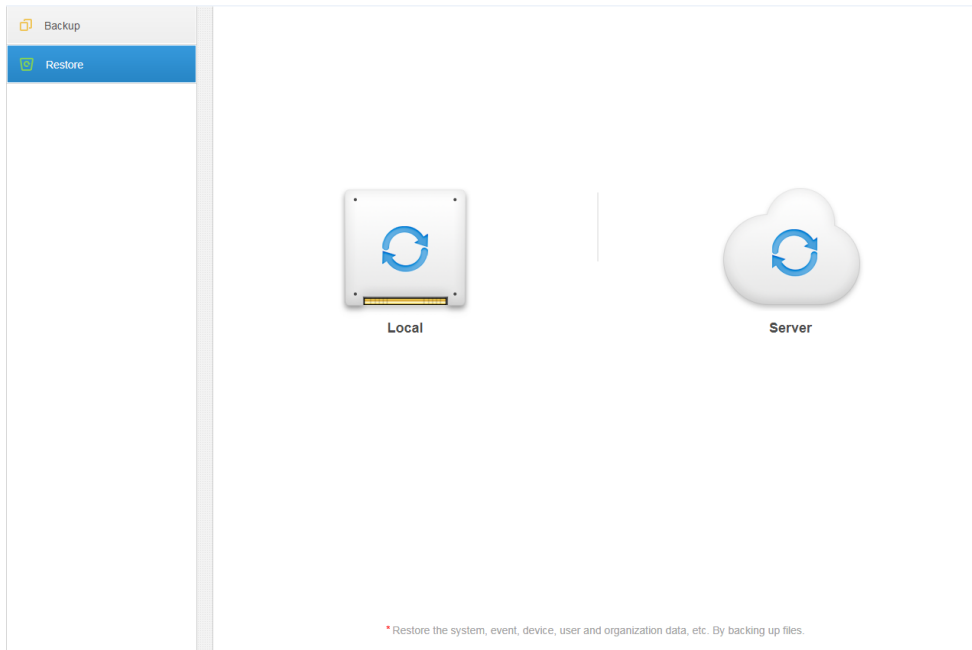
## Server


It selects to restore the data from the backup file on the server side. The precondition is that it needs to enable the auto backup function, the server end backs up the database according to the set period and from backup file.

Step 1 Select "Restore" tab.

The system enters the interface of "System Restore". See Figure 4-96.

Figure 4-96



**Step 2** Click 'Server' and click  from the list and select the file which needs to be restored.

**Step 3** Enter admin password, click "OK" and restore.

The system will restart after the data is successfully restored.

### 4.13.3 Log

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

Take "Management Configuring Log" for an example.

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

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

The system displays query results; it will display the total records on the lower left corner. See Figure 4-97.

Figure 4-97

Time	Username	Event Type	Event Contents	IP
2018-09-04 16:48:43	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:48:20	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:47:29	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:46:50	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:45:45	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:45:17	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:44:57	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:44:15	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:43:37	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:43:25	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:42:32	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:42:23	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:42:12	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:41:50	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52

Total 288 record(s).

Navigation: 1 2 3 4 5 ... 21 Go to page 1 Go

**Step 3** Click “Export” and export log info.

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

**Step 5** Check log final record results. See Figure 4-98.

Figure 4-98

Time	Username	Event Type	Event Contents	IP
2018-09-04 16:48:43	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:48:20	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:47:29	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:46:50	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:45:45	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:45:17	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52
2018-09-04 16:44:57	system	Preview	Request Main Stream video of IPC channel.	10.18.121.52

### 4.13.4 System Dashboard

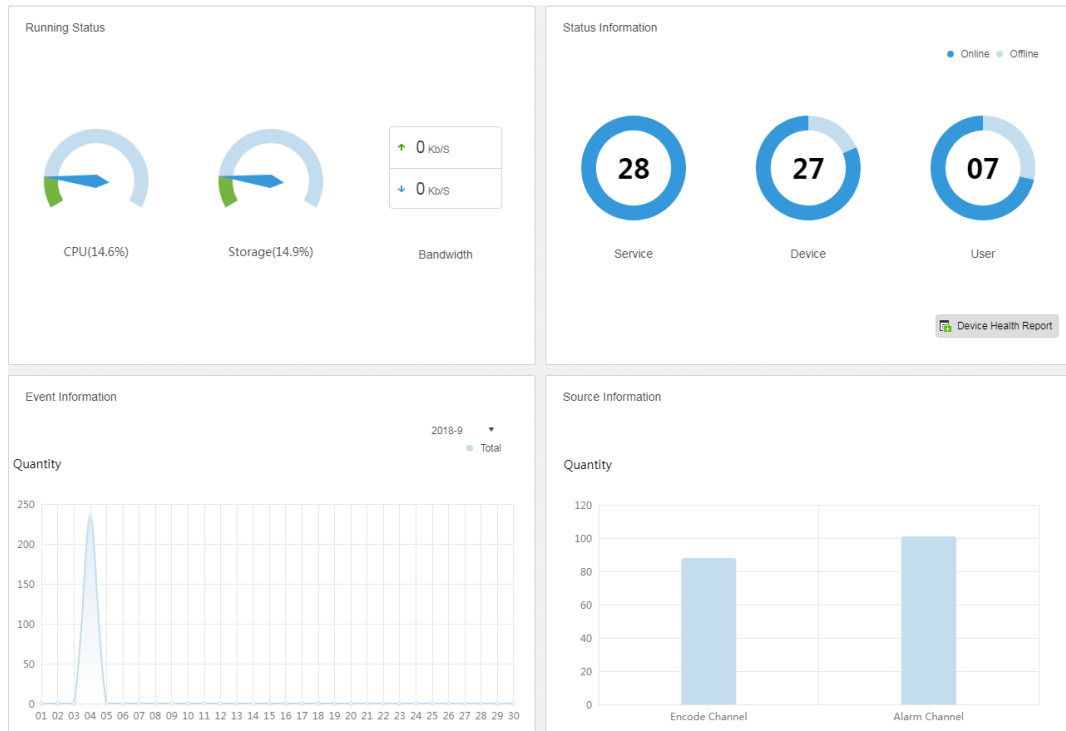
DSS management end supports function of inquiring system operation and maintenance statistics, which is to know the system running situation in time.

### 4.13.4.1 Overview

**Step 1** Click  and select “System Dashboard” on the interface of “New Tab”.

The system displays the interface of “Dashboard”. See Figure 4-99.

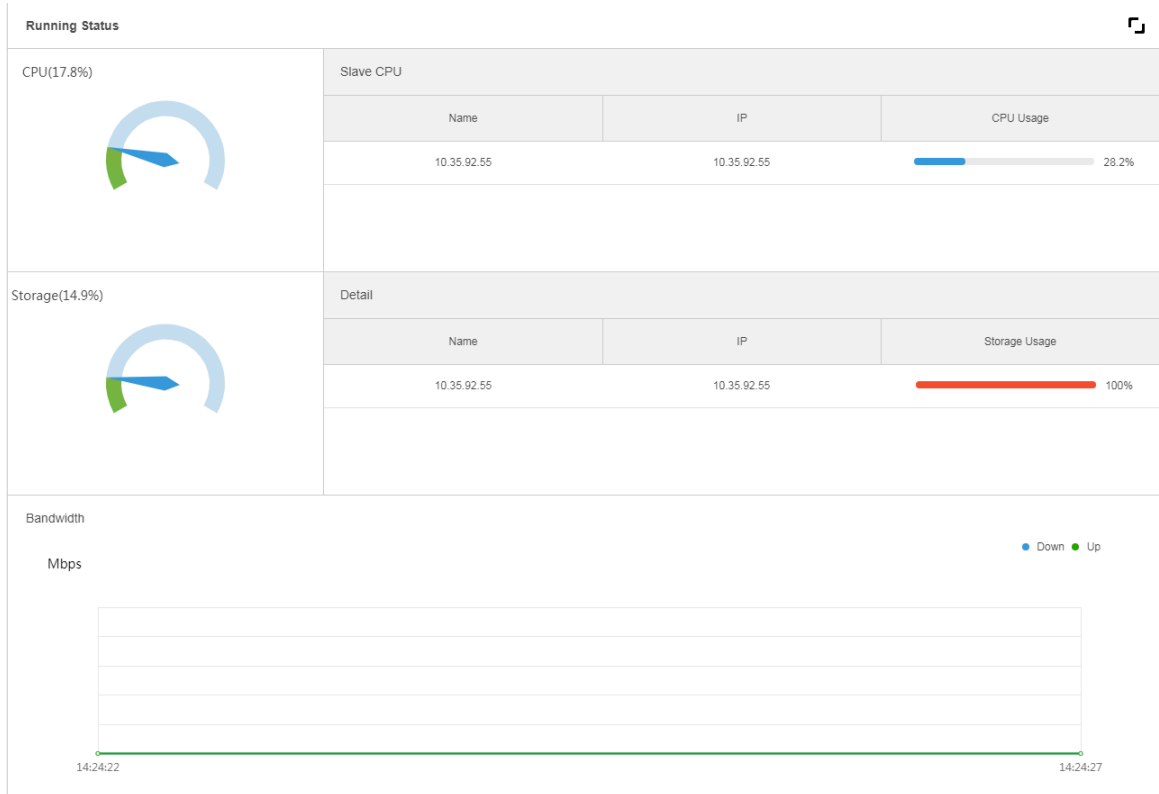
Figure 4-99



### 4.13.4.2 Running Status

Check CPU, storage, bandwidth and so on; click “Running Status” or the icon below to jump to the detail interface. See Figure 4-100.

Figure 4-100



### 4.13.4.3 Status Information

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

### Service Status Information


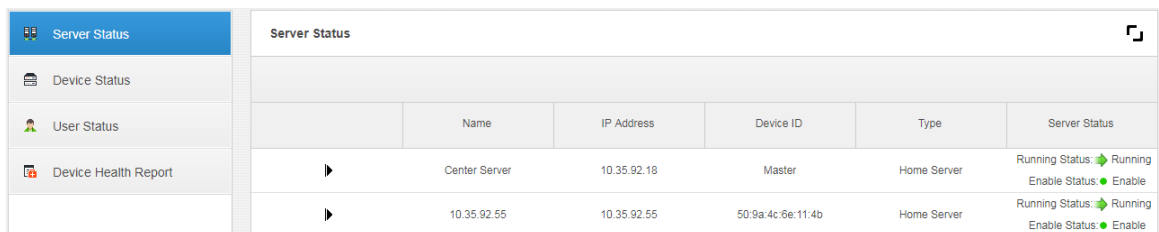
Click  on the “Service Status” interface, and then the interface displays service details. See Figure 4-101.

Figure 4-101



### Device Status Information

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

The system will display device real-time status by default. See Figure 4-102.

Figure 4-102

The screenshot shows a web interface for monitoring device status. On the left is a sidebar with navigation options: Server Status, Device Status (selected), User Status, and Device Health Report. The main area is titled 'Device Status' and has tabs for 'Real Time' and 'History'. Below the tabs is a search bar and an 'Export' button. A table lists 27 devices, all with a status of 'Online'. The table columns are Device ID, Status, Device Name, Org, and IP/Domain. The device 'GDPR-83' is highlighted in blue. At the bottom, there is a pagination control showing 'Total 27 record(s)', page numbers 1 and 2, and a 'Go to page' field with the number 1.

Device ID	Status	Device Name	Org	IP/Domain
1000029	Online	八目	root	10.35.160.142
1000027	Online	ipc-77	test	10.35.106.77
1000025	Online	onvif hik	onvif	172.7.57.16
1000024	Online	hik-ipc	ipc	172.7.57.16
1000023	Online	ipc-121	test	10.35.92.121
1000021	Online	双目睿流	KL	10.35.92.84
1000020	Online	GDPR-83	GDPR	10.35.92.83
1000018	Online	ARS-NVR-83	ARS	10.35.92.83
1000016	Online	onvif 84	onvif	10.35.92.84
1000015	Online	10.11.16.122	KL	10.11.16.122
1000014	Online	10.11.16.121	KL	10.11.16.121
1000012	Online	atal-5	alarm	10.8.70.57
1000011	Online	onvif ipc-21	onvif	10.35.92.21
1000010	Online	10.35.92.29	NVR	10.35.92.29

**Step 2** Check device status.

- Click the “Real Time” tab on the device status information interface, check device realtime status info.
- Click the “History” tab on the device status information interface, check device history status info. See Figure 4-103.

Figure 4-103

Time	Status	Device Name	Org Name	IP/Domain
2017-04-08 11:51:45	● Online	172.10.1.202	root	172.10.1.202
2017-04-08 11:51:45	● Online	37779	root	172.10.1.201
2017-04-08 11:51:45	● Online	37778	root	172.10.1.201
2017-04-08 11:51:44	● Online	37777	root	172.10.1.201
2017-04-08 11:51:17	● Online	172.10.1.202	root	172.10.1.202
2017-04-08 11:51:17	● Online	37779	root	172.10.1.201
2017-04-08 11:51:17	● Online	37778	root	172.10.1.201
2017-04-08 11:51:16	● Online	37777	root	172.10.1.201
2017-04-07 01:23:22	● Online	172.10.1.202	root	172.10.1.202
2017-04-07 01:19:19	● Offline	172.10.1.202	root	172.10.1.202
2017-04-07 01:19:16	● Offline	172.10.1.202	root	172.10.1.202
2017-04-06 11:46:04	● Online	172.10.1.202	root	172.10.1.202
2017-04-06 11:42:36	● Offline	172.10.1.202	root	172.10.1.202
2017-04-06 11:42:33	● Offline	172.10.1.202	root	172.10.1.202

**Step 3** Click “Export”

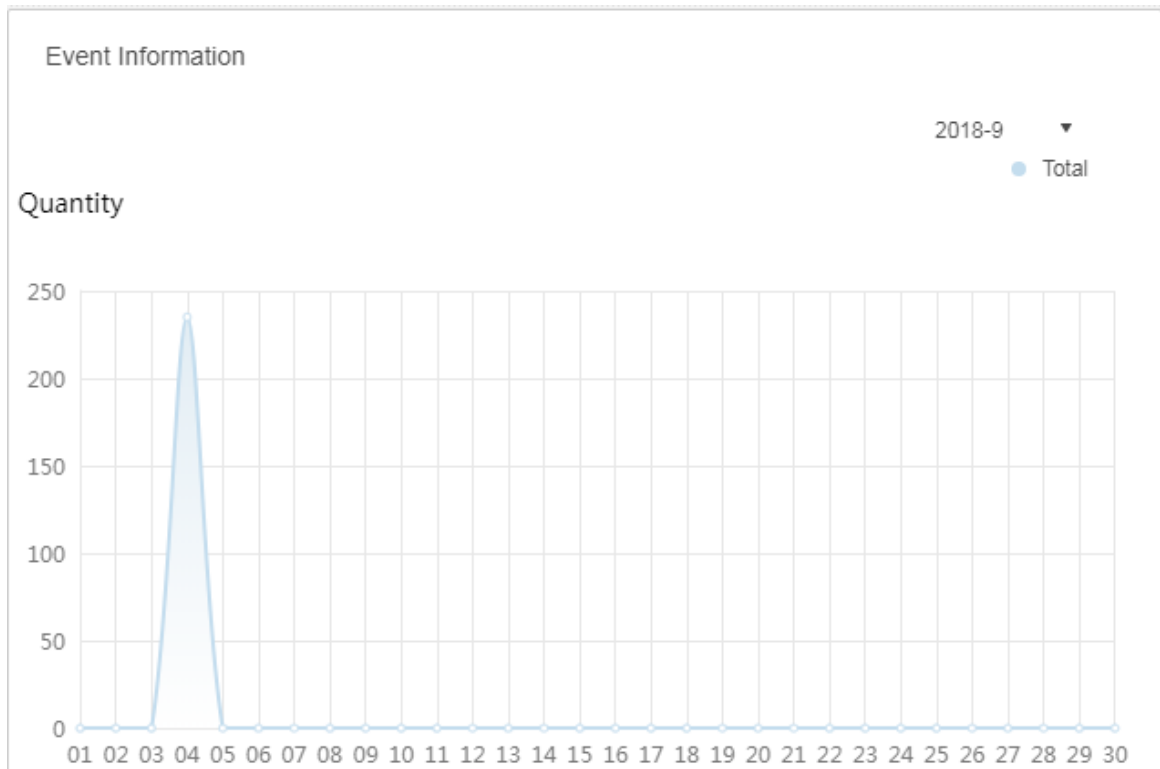
It exports device realtime status information (PDF format).

Click “User Status”, “Device Health Report” tab to check corresponding details.

### 4.13.4.4 Event Information

It is to check total number of alarm events and processed events according to month. See Figure 4-104.

Figure 4-104



#### 4.13.4.5 Source Information

It is to check the statistics of encoding channel and alarm channel, click “Source Information” or the icon below to jump to the detailed interface.

- Check video channel details. See Figure 4-105.



Figure 4-105

Name	Device	Org	SN	Camera Type
10.35.92.10IPC	10.35.92.10	KL		Fixed Camera
ONVIF协议_大华_FE_1	LL-91	ANPR		Fixed Camera
37722_1	37722	ANPR		Speed Dome
10.35.92.11IPC	10.35.92.11	KL		Fixed Camera
37723_1	37723	ANPR		Speed Dome
Slot04-01	M70-E	TV WALL		Speed Dome
Slot04-02	M70-E	TV WALL		Speed Dome
Slot04-03	M70-E	TV WALL		Speed Dome
Slot04-04	M70-E	TV WALL		Speed Dome
Slot06-01	M70-E	TV WALL		Speed Dome
Slot06-02	M70-E	TV WALL		Speed Dome
Slot06-03	M70-E	TV WALL		Speed Dome
Slot06-04	M70-E	TV WALL		Speed Dome
10.35.164.140_1	M70-E	TV WALL		Speed Dome

Total 89 record(s).

Navigation: < 1 2 3 4 5 6 7 > Go to page 1 Go

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

# 5 Client Functions

## NOTE

The client includes PC and cellphone App. Here we use operation on the PC to continue.

## 5.1 Installation and Login of the Client

### 5.1.1 PC Requirements

To install the DSS Client, the PC shall meet the requirements as shown in Table 5-1.

Table 5-1

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


### 5.1.2 Download and Installation

#### 5.1.2.1 Installation on PC

Step 1 Input IP address of DSS on the browser and then click **【Enter】** button.  
The Login interface is displayed. See Figure 5-1.

Figure 5-1



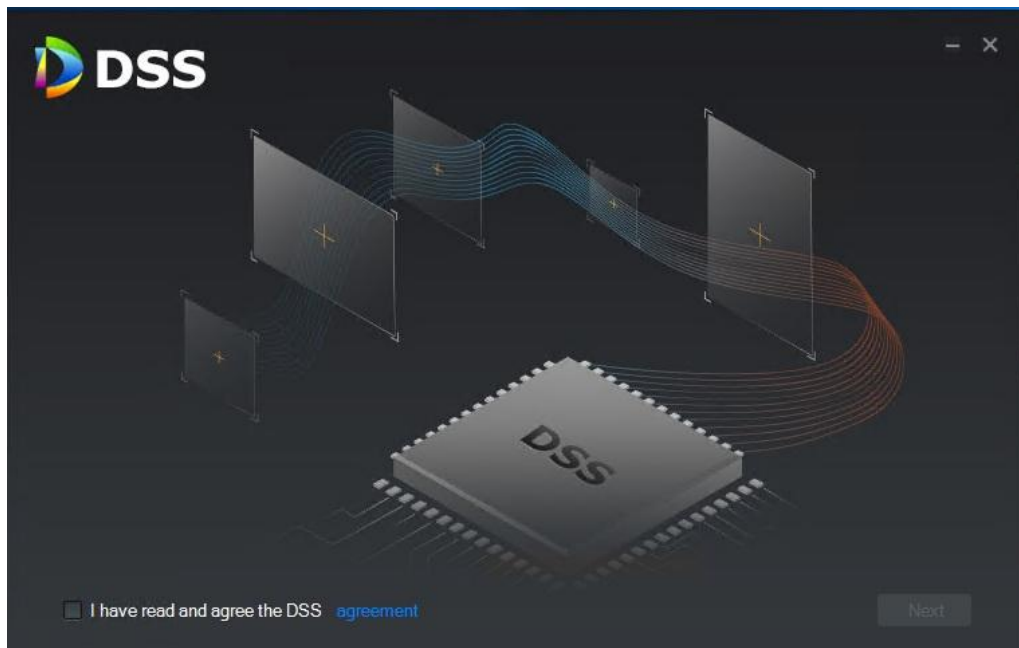
Step 2 Click  to download the client.

System pops up the “File Downloads” dialogue box.

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

Step 4 Double click the client installation applications to install.

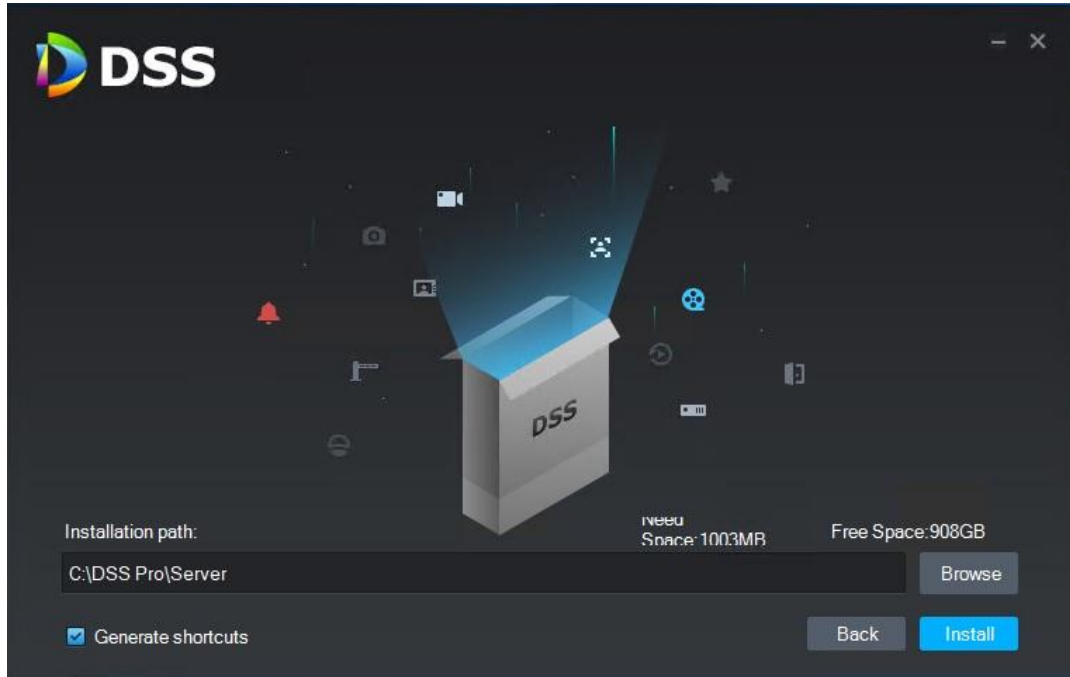
Figure 5-2



Step 5 Check the box to agree DSS agreement and then click Next to continue.

Step 6 Select installation path. See Figure 5-3.

Figure 5-3



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

System displays installation process. It takes 3 to 5 minutes to complete. Please be patient. The complete interface is shown as in Figure 5-4.

Figure 5-4



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

### 5.1.2.2 Cellphone App

Step 1 Input IP address of DSS on the browser and then click **【Enter】** button.


Step 2 Click  to view cellphone App QR code. Now it supports iOS and Android.


Figure 5-5



Step 3 Scan the QR code and then download the cellphone App.

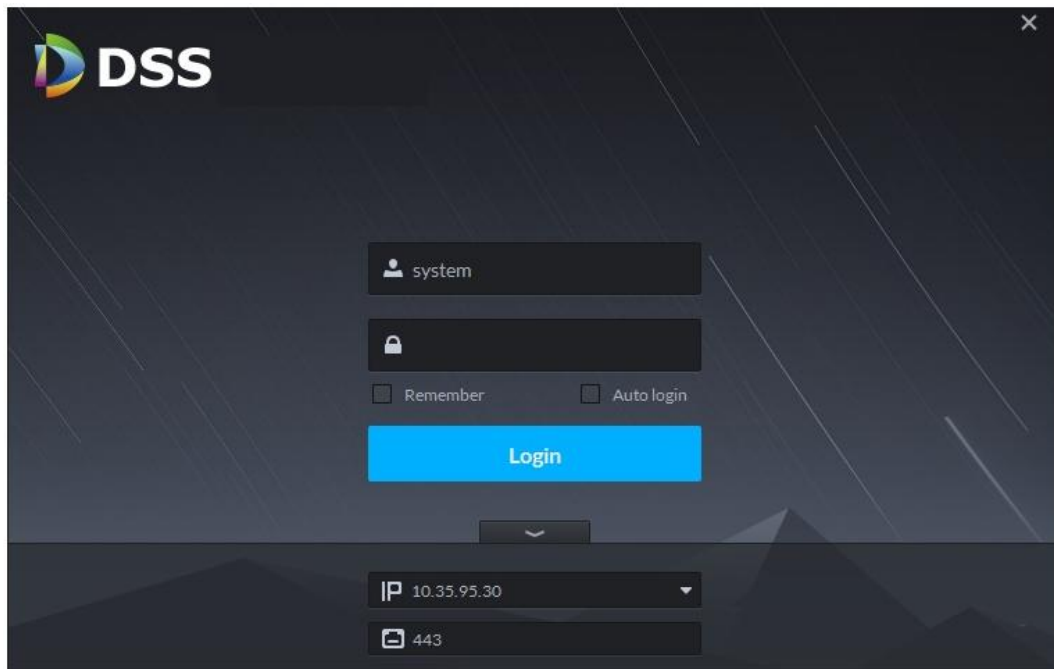
### 5.1.3 Login Client




Step 1 Double click icon  on the desktop.

The client login interface is displayed. See Figure 5-6.

Figure 5-6



**Step 2** Enter “User Name” and “Password”.

**Step 3** Click  and set server IP address and port number.

“Server IP” means the IP address of the DSS platform Manager, while “Port” is “443” by default.

**Step 4** Click “Login”.

The system displays the interface of “Homepage” by default. See Figure 5-7.

Figure 5-7

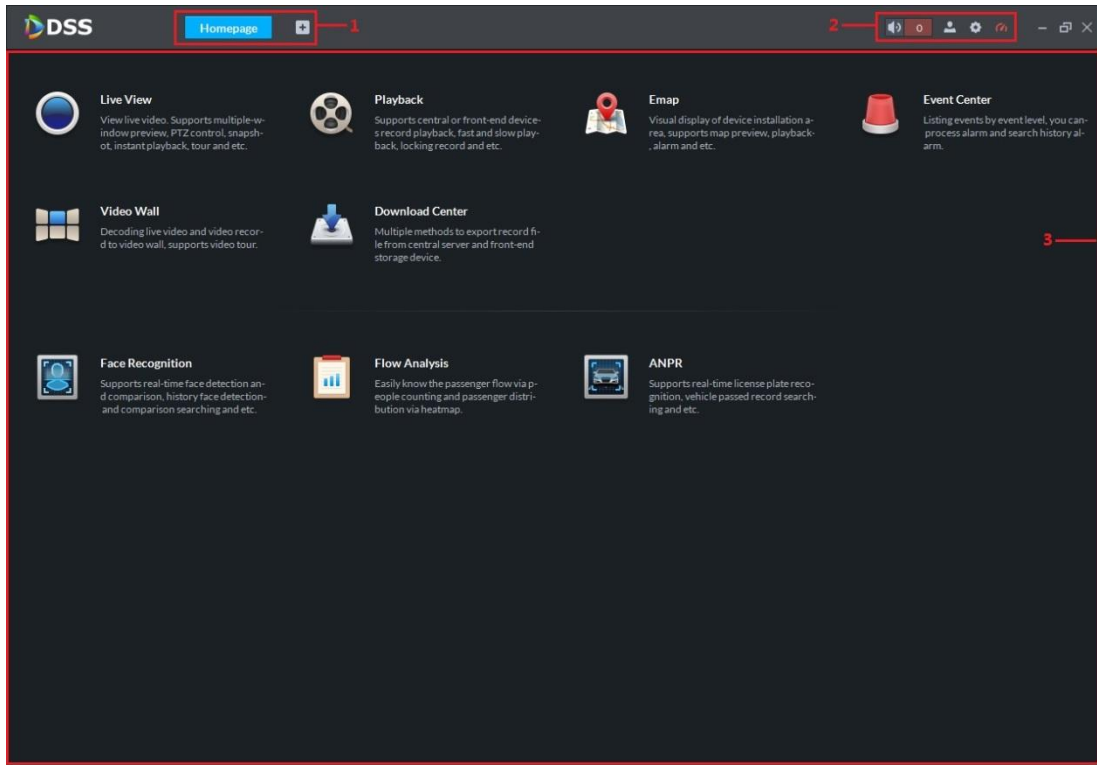







Table 5-2

SN	Name	Function
1	Tab	It displays all valid tab. Click  to open the desired module.

SN	Name	Function
2	System operation pane	<p>Refer to the following contents for icon definition.</p> <ul style="list-style-type: none"> <li>● : Open/close alarm audio.</li> <li>● : It displays alarm amount. Click an alarm; you can go to Event center interface.</li> <li>● : User information: click the icon and then select the corresponding function, you can login platform manager, modify password, lock client, view help file, and logout user. <ul style="list-style-type: none"> <li>◇ Select platform IP address, system goes to platform manager login interface.</li> <li>◇ Select Modify password, you can change user password.</li> <li>◇ Select Lock Client, it is to lock the system, you cannot operate on the client. Input the login password again to unlock.</li> <li>◇ Select About, it is to view version information, released date.</li> <li>◇ Select Logout, it is to logout the system. System goes back to the client login interface.</li> </ul> </li> <li>● : Local config. It is to set general, video, playback, snapshot, record, alarm shortcut settings. Refer to chapter 5.2 Local configuration for detailed information.</li> <li>● : It is to view system status. It includes network status, CPU status, and memory status.</li> </ul>
3	Operation pane	It is to operate the functions.

## 5.2 Local Configuration

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


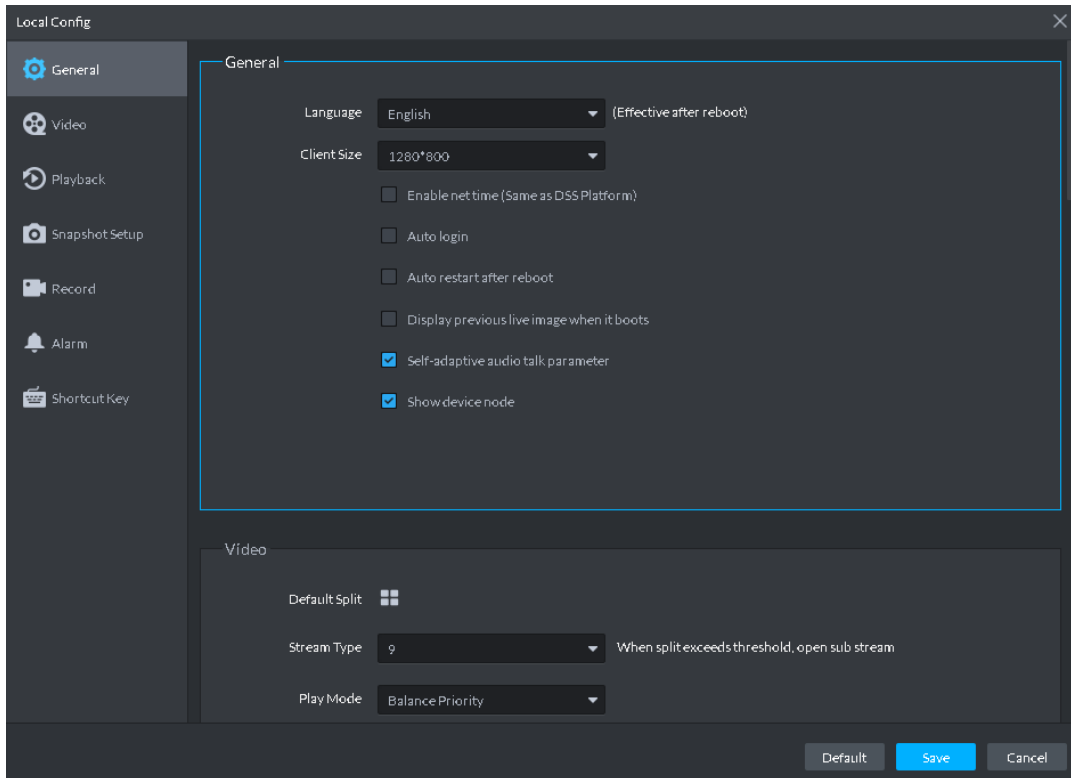
Step 1 Click  at the top right corner on the Homepage.  
The General interface is displayed. See Figure 5-8.



Figure 5-8



Step 2 Refer to Table 5-3 to set parameters.

Table 5-3

Parameters	Note
Language	Choose the language for the interface. It includes Simplified Chinese, English, etc.
Client size	It is to set client display size.
Enable net time	If checked, the client starts to synchronize network time with the server. It is to complete time synchronization.
Auto Login	If checked, auto login is allowed when Client starts running.
Auto Reboot	If checked, auto reboot of the Client is allowed when the PC power is on.
Display Previous live Image when it boots	If checked, system displays the last Live video automatically after rebooting the client.
Self-adaptive Audio Talk Parameter	If checked, the system will adapt to “Sampling Frequency”, “Sampling Bit”, and “Audio Format” to the device automatically during audio talk.

Parameters	Note
Show Device Node	Check the box, system displays device node.

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

The Video interface is shown as in Figure 5-9. Refer to Table 5-4 to set parameters.

Figure 5-9

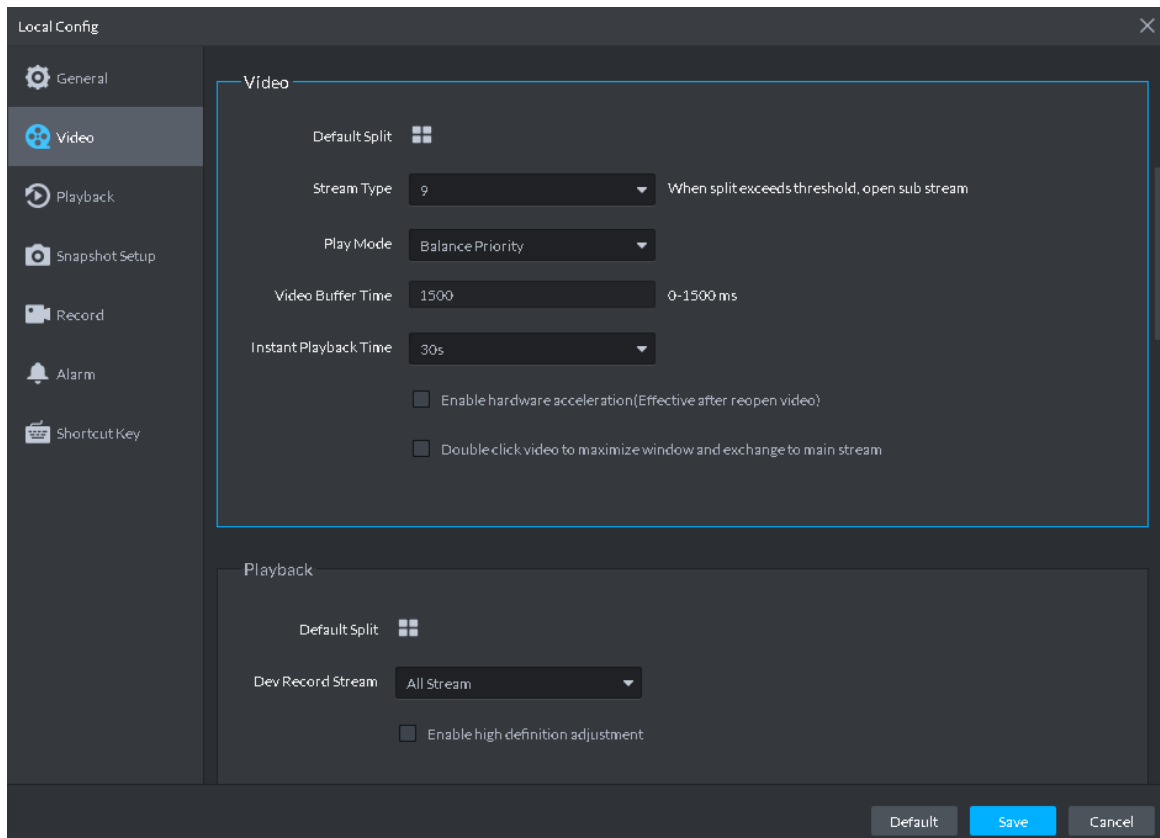


Table 5-4

Parameters	Note
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	It is to 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.

Parameters	Note
Enable hardware acceleration (effective after reopen the video)	Check the box to enable the function. It is to use hardware module to enhance acceleration features.
Double click video to maximize window and exchange to main stream	Check the box to enable the function.

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

The playback interface is shown as in Figure 5-10. Refer to Table 5-5 to set parameters.

Figure 5-10

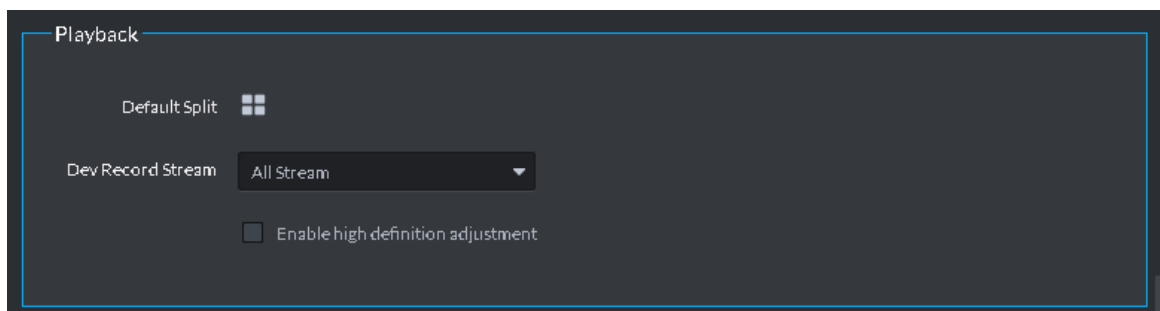


Table 5-5

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

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

The Snapshot interface is shown as in Figure 5-11. Refer to Table 5-6 to set parameters.

Figure 5-11

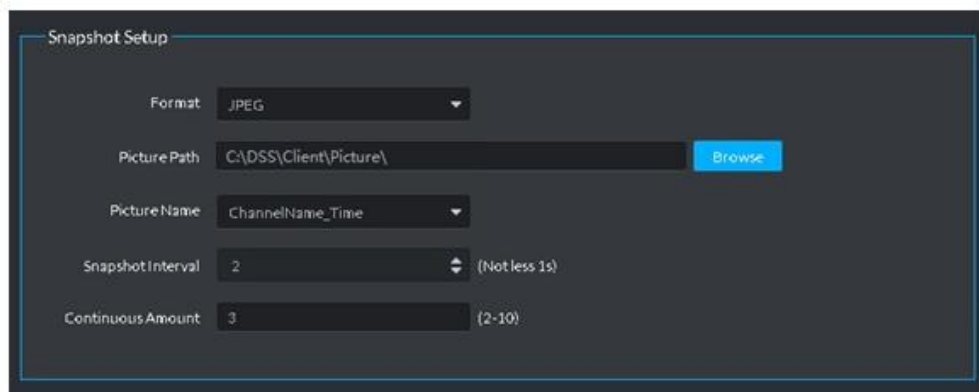


Table 5-6

Parameters	Note
Format	It is to set snapshot image format.

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

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

The Record interface is shown as in Figure 5-12. Refer to Table 5-7 to set parameters.

Figure 5-12

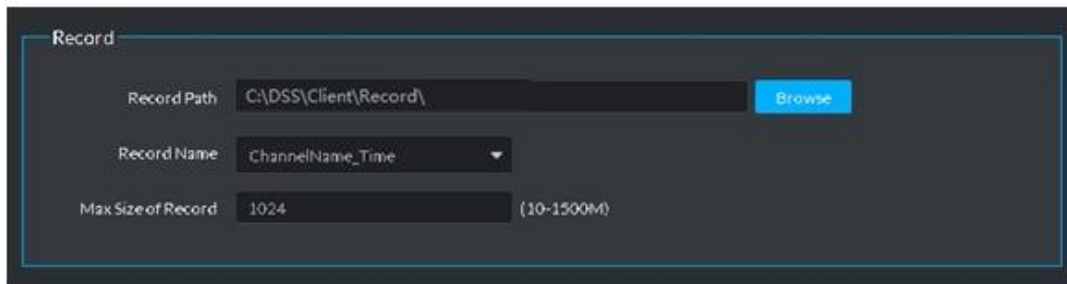


Table 5-7

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

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

The Alarm interface is shown as in Figure 5-13. Refer to Table 5-8 to set parameters.

Figure 5-13

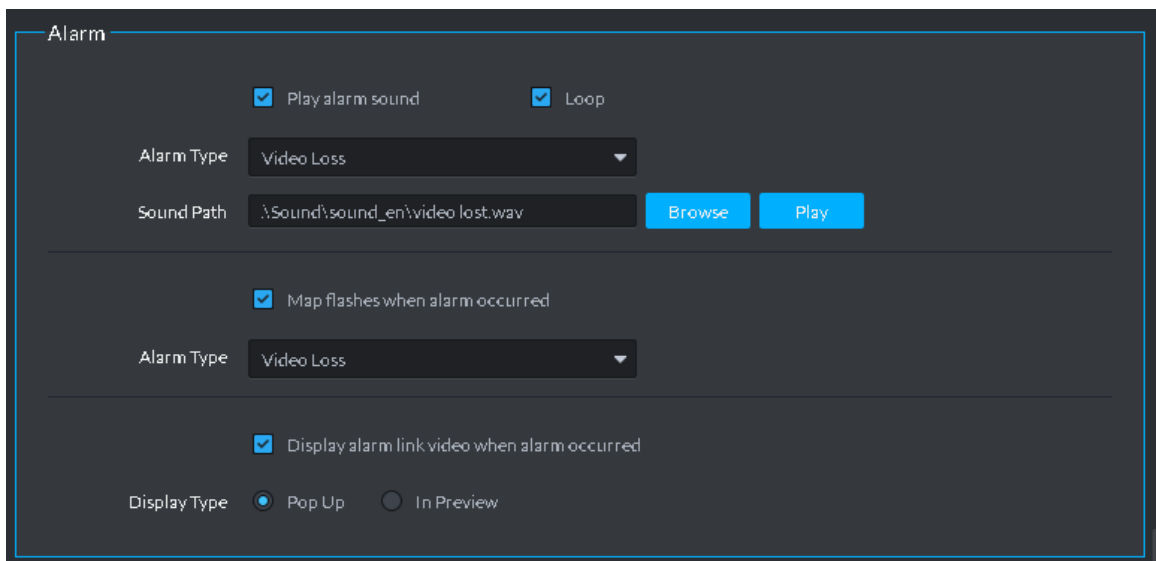




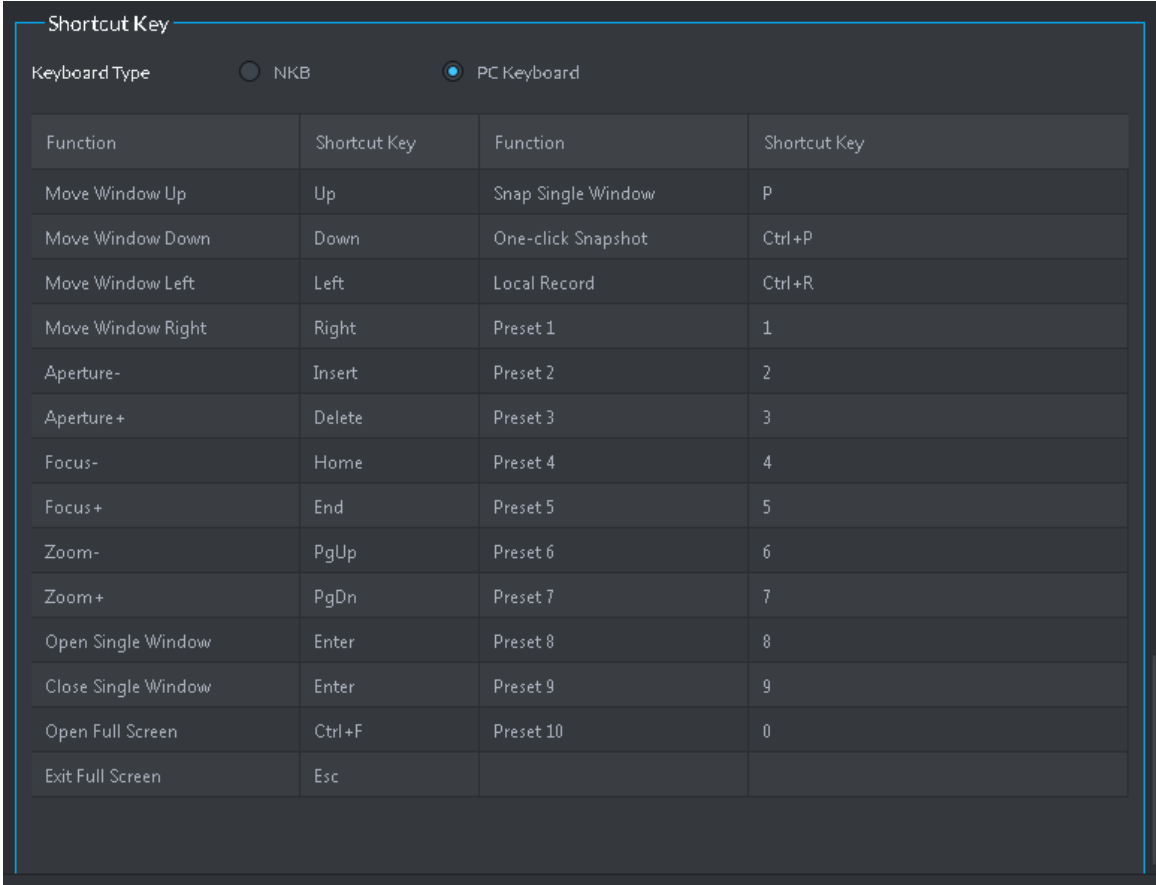
Table 5-8

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.  <b>NOTE</b> This item is only valid when Play alarm sound function is enabled.
Alarm type	It is to set alarm type. System can play sound when corresponding alarm occurs.  <b>NOTE</b> 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 map 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.

**Step 8** Click Shortcut key to set parameters.

The Shortcut key interface is shown as in Figure 5-14.

Figure 5-14



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

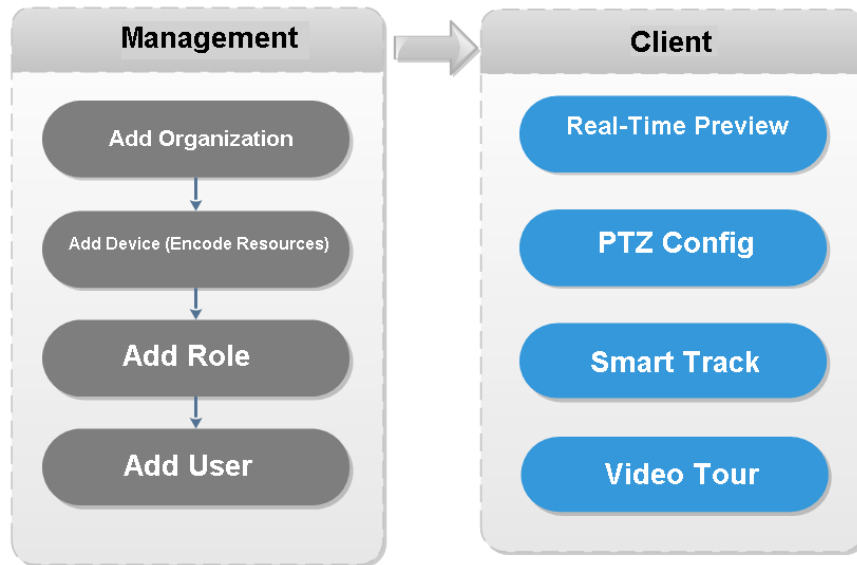
Step 9 Click Save.

## 5.3 Video Preview

### 5.3.1 Preparations

Before the operation, refer to chapter 4.6 Adding device to add decode device on the manager. Refer to Figure 5-15 for video preview flows information.

Figure 5-15



## 5.3.2 Real-Time Preview

### 5.3.2.1 Real-Time Video Preview

Click **+** and then on the New tab interface, select Live View, system displays Live view interface by default.


Select channel from the device list on the left side of the Live view interface, and double click or drag it to video window. If you double click device, then all channels of the device will be opened.

Real-time monitoring interface is displayed in the video window. See Figure 5-16. Refer to Table 5-9 to set parameters.


Figure 5-16



Table 5-9

SN	Name	Function
1	Favorites and Device Tree Search	<ul style="list-style-type: none"> <li>From Local config&gt; 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.</li> <li>Search is supported by input device name or channel name in <input type="text" value="Search.."/> here.</li> <li>★: Add, Delete or Rename Favorite. Favorite Tour supported.</li> </ul>
2	POS	It is to open POS and its corresponding video channel on the Live view interface.
3	Map Resource	Map can be opened in preview window, both GIS map and Raster map.
4	View	<ul style="list-style-type: none"> <li>Live video window can be saved as View. Three-level directory is adopted for view, with level one as root node, level two for group and level three for view. Video Tour is supported from root node and group node, with tour intervals selected from 10s, 30s, 1min, 2min, 5min and 10min. Maximum of 100 views can be created.</li> </ul>
5	PTZ	More info about PTZ of PTZ camera, refer to chapter 5.3.3 PTZ".
6	Save view	Click  to save current video window as a view.



SN	Name	Function
7	Display mode	<ul style="list-style-type: none"> <li>Aspect ratio of the video window, selected from two modes for video play: actual scale and fit in window.</li> </ul>
8	Window Split Mode	<ul style="list-style-type: none"> <li>Select from modes among 1 to 64 to set window split mode, or click  to define split mode.</li> </ul>
9	Full Screen	<ul style="list-style-type: none"> <li>Switch the video window to “full screen” mode. To exit “full screen”, press the Esc key, or right click to select “exit full screen”.</li> </ul>
10	Bit Stream and Quick Start	<p>It is to display encode format, bit stream information and quick start.</p> <p>Refer to chapter 5.3.2.3 Window Shortcut Menu for detailed information.</p>

### 5.3.2.2 Right –Click Shortcut Menu

On the Preview video window, right click mouse, the interface is shown as in Figure 5-17. Refer to Table 5-10 to set parameters.

Figure 5-17

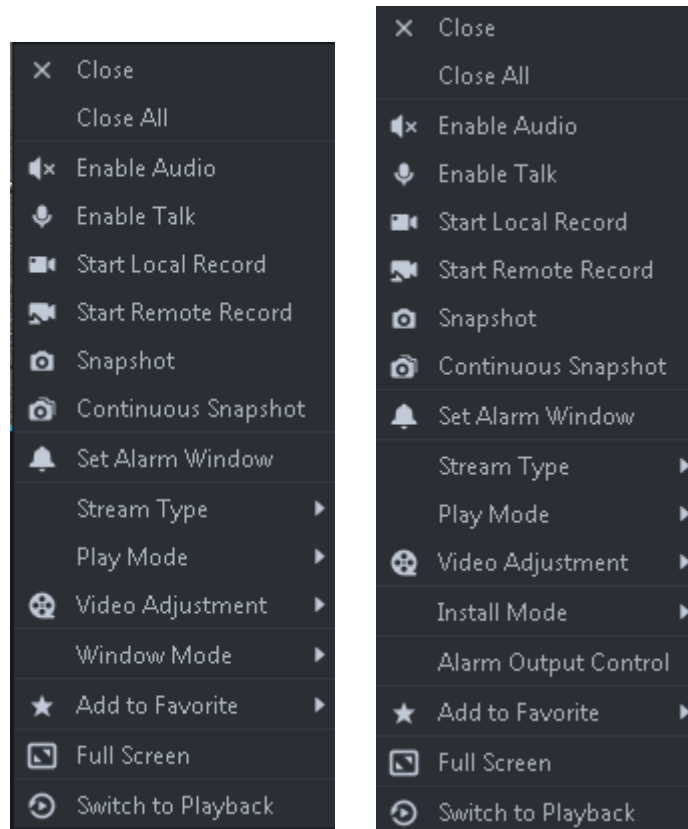









Table 5-10

Parameters	Note
Close Video	Close active video window.
Close All Videos	Close all video windows.

Parameters	Note
Audio Enable	Same as  , to enable or disable camera audio.
Audio Talk Enable	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.
Switch Bit Stream	Switch among “Main stream”, “Sub stream” and “Third stream”.  <b>NOTE</b> 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.
Installation mode	 <b>Note</b> 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	 <b>Note</b> For fisheye camera only It refers to current video display mode (system supports original video mode by default.). System supports following display modes according to different installation mode. <ul style="list-style-type: none"> <li>● Ceiling mount: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8.</li> <li>● Wall mount: 1P, 1P+3, 1P+4, 1P+8.</li> <li>● Ground mount: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8.</li> </ul>
Split mode	It supports 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.

Parameters	Note
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.

### 5.3.2.3 Window Shortcut Menu

Move the mouse to the video window, you can see the shortcut menu at the top right. See Figure 5-18. Refer to Table 5-11 for detailed information.

Figure 5-18

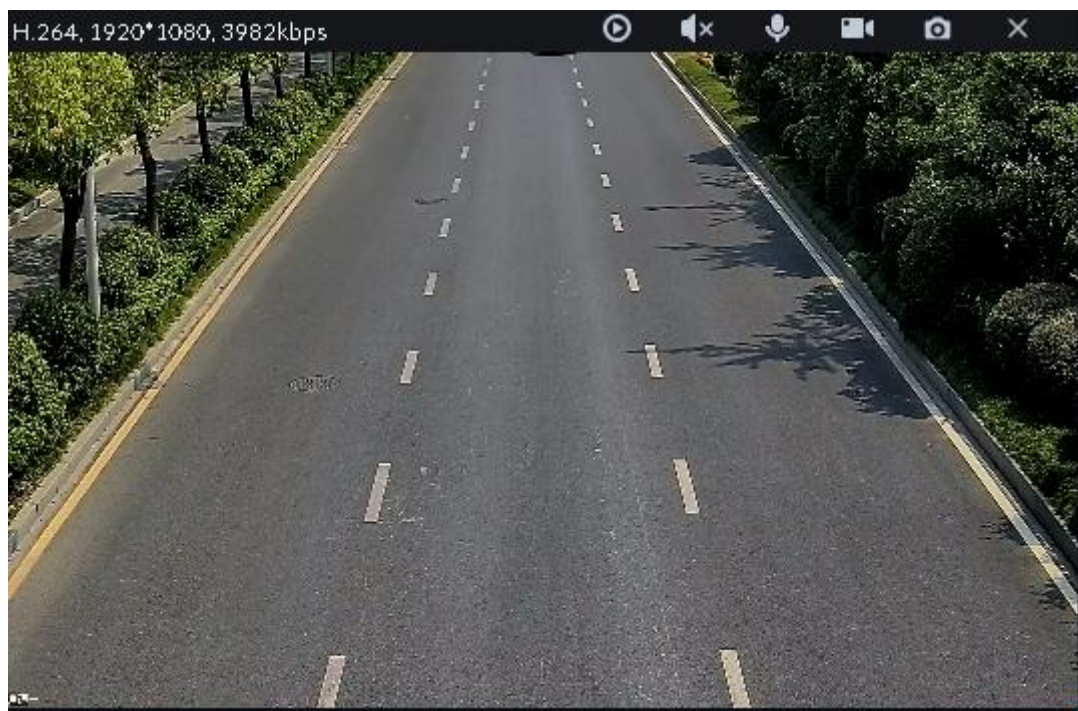


Table 5-11

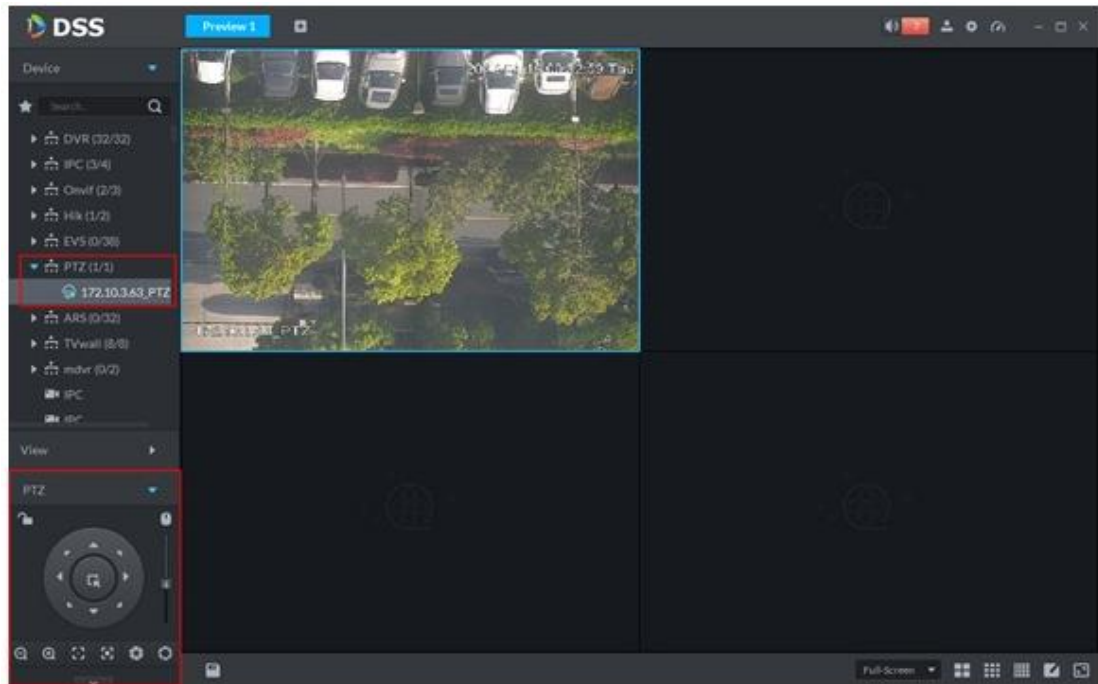
Icon	Name	Note
	Instant playback	Open/close instant playback. Go to Local config>General to set instant playback time. Make sure there is a record on the platform or the device.
	Audio	Open/close audio.
	Audio talk	Open/close bidirectional talk.
	Local record	Click it, system begins record local file 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.
	Close	Click to close video.

## 5.3.3 PTZ

### 5.3.3.1 PTZ Operation Pane

**Step 1** On Preview interface, open video from the PTZ camera, you can see PTZ operation pane on the left. See Figure 5-19.

Figure 5-19




**Step 2** Click  at the bottom of the interface to operate. See Figure 5-20.

Figure 5-20

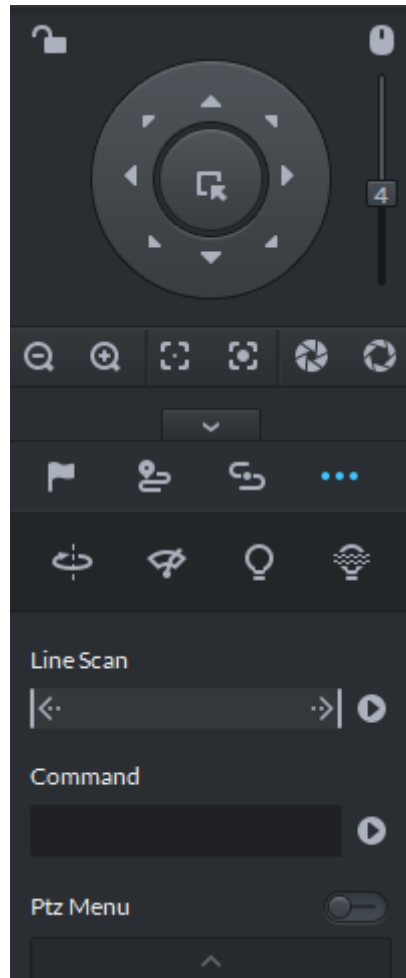










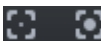




Table 5-12

Parameters	Note
	<p>Click  to lock the current PTZ. Locked status shows as .</p> <p>Control over PTZ varies depending on user level.</p> <ul style="list-style-type: none"> <li>• When user of low level locks PTZ, user of high level can unlock and enable the PTZ by clicking .</li> <li>• When user of high level locks PTZ, user of low level can't unlock the PTZ, unless PTZ automatically unlock itself.</li> <li>• Users of the same level can unlock PTZ locked by each other.</li> </ul> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>• Default time for automatically unlocking PTZ is 30s.</li> </ul>
	<ul style="list-style-type: none"> <li>• Control speed dome with mouse.</li> </ul>
Direction Key	<ul style="list-style-type: none"> <li>• Set rotation direction of PTZ, eight directions are available in total: up, down, left, right, upper left, upper right, lower left and lower right.</li> </ul>


Parameters	Note
	<ul style="list-style-type: none"> <li>• 3D Location and Partially Zoom In (for Speed Dome PTZ), to zoom in or zoom out the selected area.</li> </ul> <p> <b>Note</b></p> <p>This function can be controlled with mouse only.</p>
	From top to the bottom to adjust rotation speed of PTZ, to set the step size chosen from 1 to 8.
	<ul style="list-style-type: none"> <li>• Zoom, to control zoom operation of speed dome.</li> </ul>
	<ul style="list-style-type: none"> <li>• Focus, to adjust focus.</li> </ul>
	<ul style="list-style-type: none"> <li>• Aperture, to adjust brightness.</li> </ul>
	It is to set preset, tour, pattern, scan, rotation, wiper, light, IR light function, etc. Refer to chapter 5.3.3.2 PTZ settings for more information.


## 5.3.3.2 PTZ Settings


### 5.3.3.2.1 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.


### 5.3.3.2.2 Configuring Tour

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


 **Note**

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

Step 1 Click .

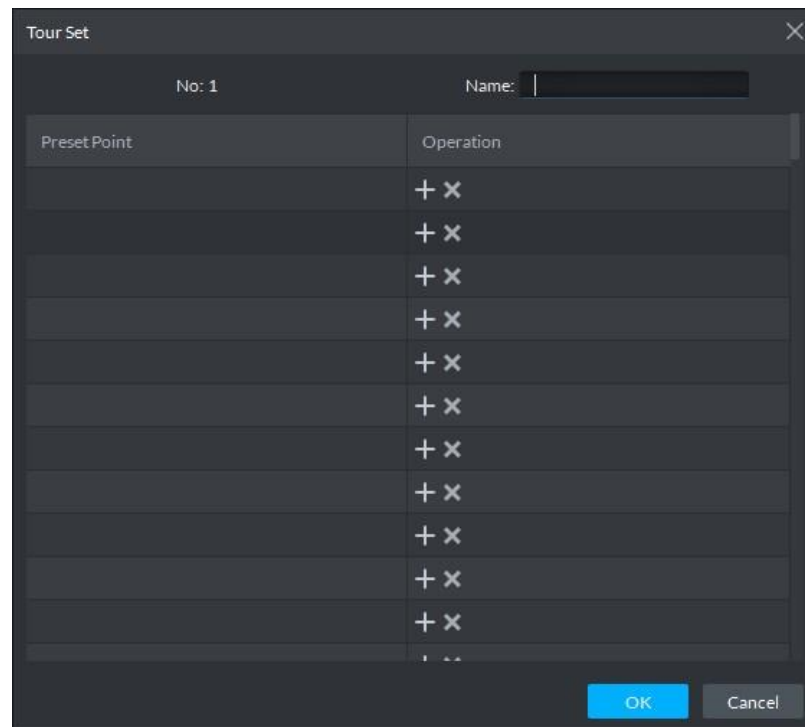
Step 2 Place mouse over 1 and click .

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 5-21.

Figure 5-21




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

**Step 5** Click “OK”.


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


### 5.3.3.2.3 Pattern

Pattern is equivalent to a record process.

**Step 1** Click .


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


**Step 3** Click  to complete pattern setup.


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

### 5.3.3.2.4 Configuring Scan




**Step 1** Click .

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

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




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

### 5.3.3.2.5 Start/stop rotation

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




### 5.3.3.2.6 Start/stop wiper

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




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

### 5.3.3.2.7 Start/stop light

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

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

### 5.3.3.2.8 Start/stop IR light

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

### 5.3.3.2.9 Configuring customized commands

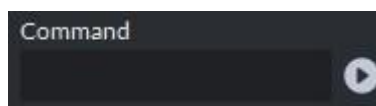
#### NOTE

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 5-22.

Figure 5-22



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

### 5.3.3.2.10 PTZ Menu

Step 1 Click .

The PTZ menu is shown as in Figure 5-23.



Figure 5-23

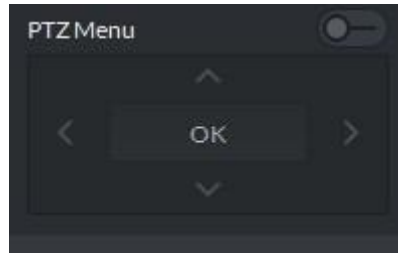








Table 5-13

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. <ul style="list-style-type: none"> <li>• If the main menu has the sub-menu, click OK to enter the sub-menu.</li> <li>• Move the cursor to Back and then click OK to go to go back to the previous menu.</li> <li>• Move the cursor to Exit and then click OK to exit the menu.</li> </ul>

Step 2 Click OK.

The monitor window displays main menu. See Figure 5-24.

Figure 5-24

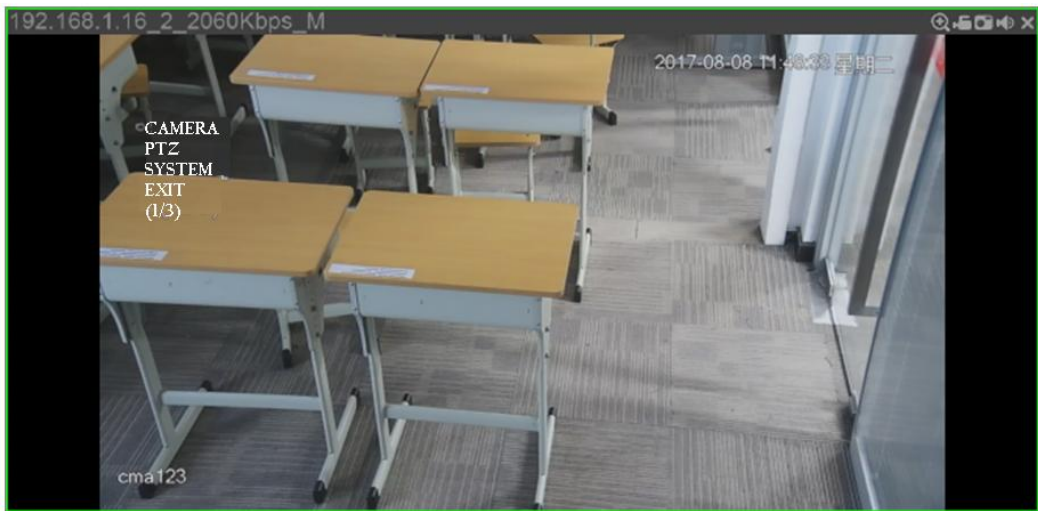


Table 5-14

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

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

### 5.3.4 Smart Track

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

#### 5.3.4.1 Preparations


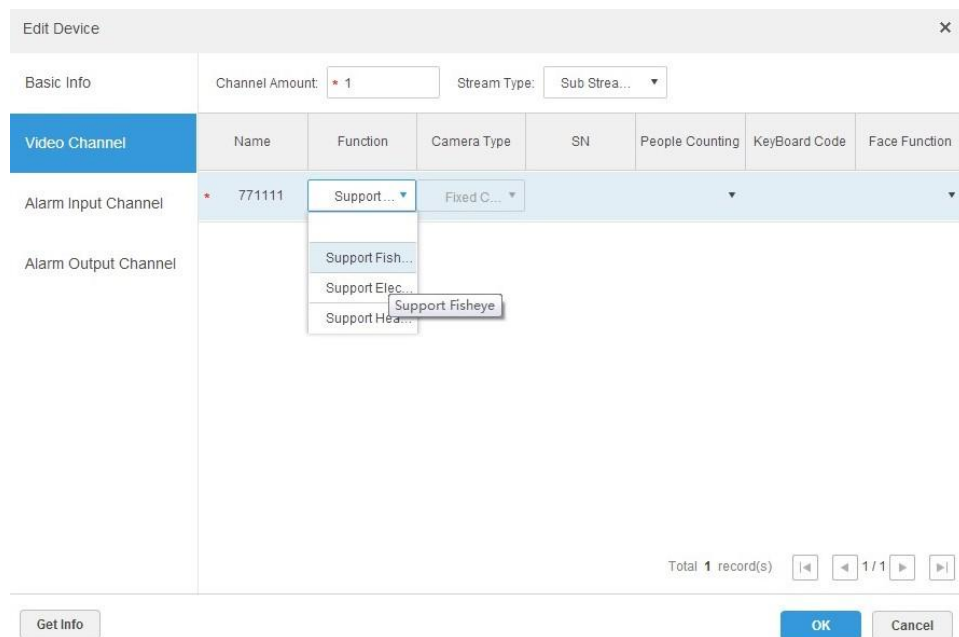
- Before operating smart track, go to Device manager to add fisheye device and PTZ camera first. Refer to chapter 4.6 Adding device for detailed information.
- After device is added, click , and select fisheye and general speed dome.

Figure 5-25



#### 5.3.4.2 Adding Smart Track Settings

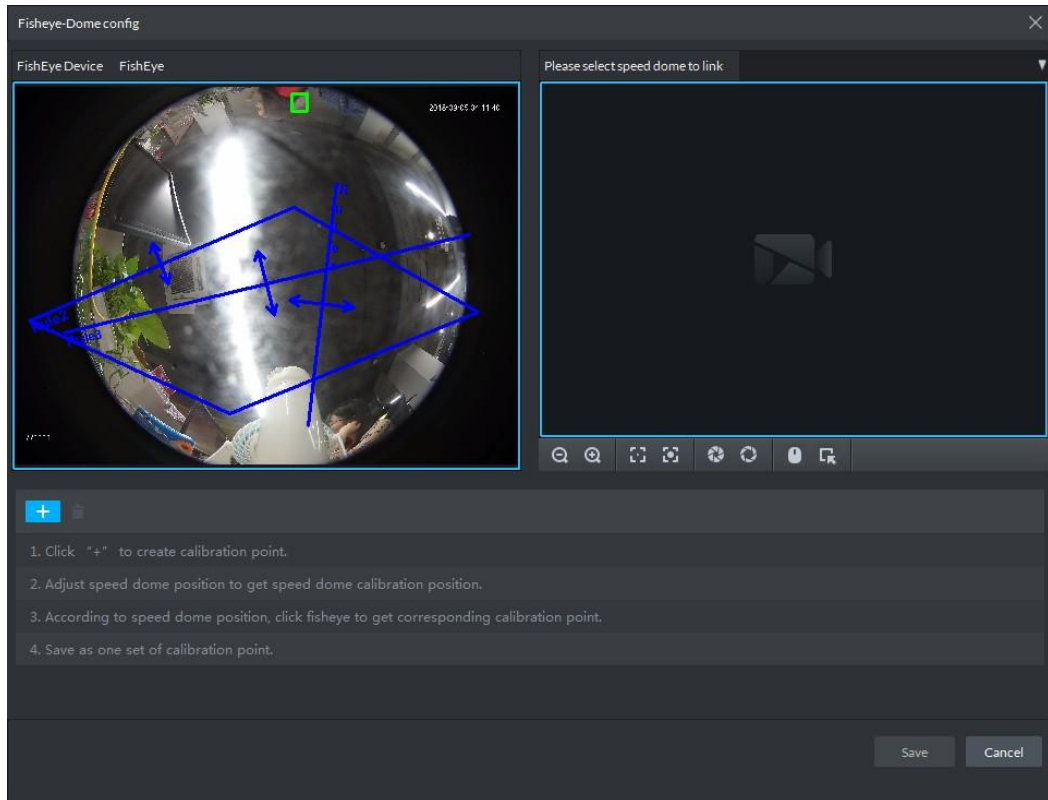
**Step 1** Select the fisheye device on the device tree and then right click to select Smart track.

 **NOTE**

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 5-26.

Figure 5-26



**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.


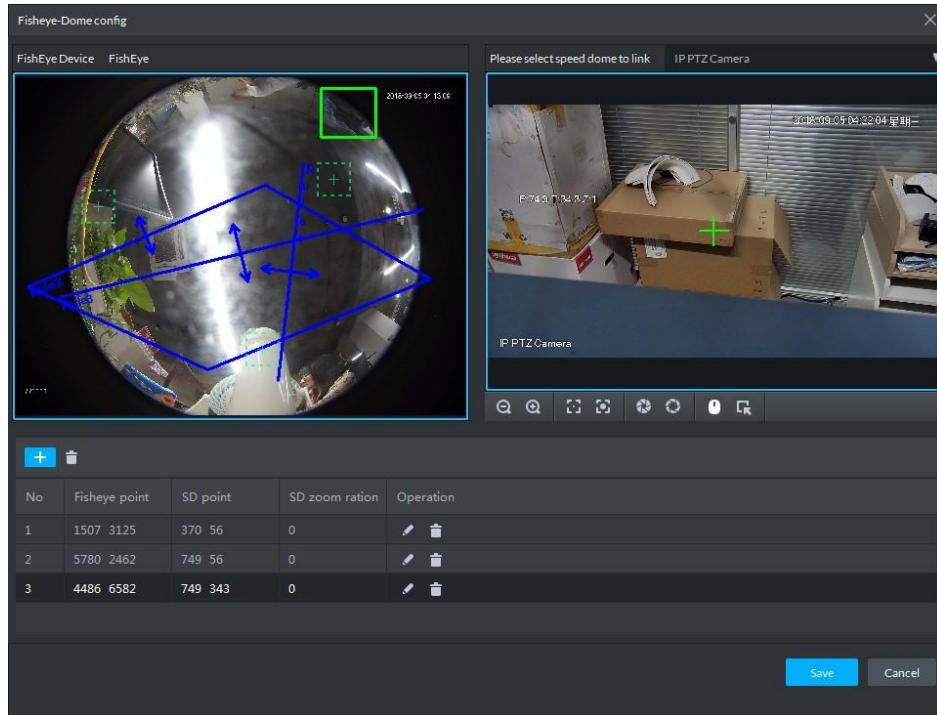
Click  on the general PTZ camera to find the position. Adjust the PTZ camera to find the position and move the PTZ to the center position (The green cross on the image). See Figure 5-27.

Figure 5-27



**NOTE**

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

**Step 4** Click to save the calibration point.

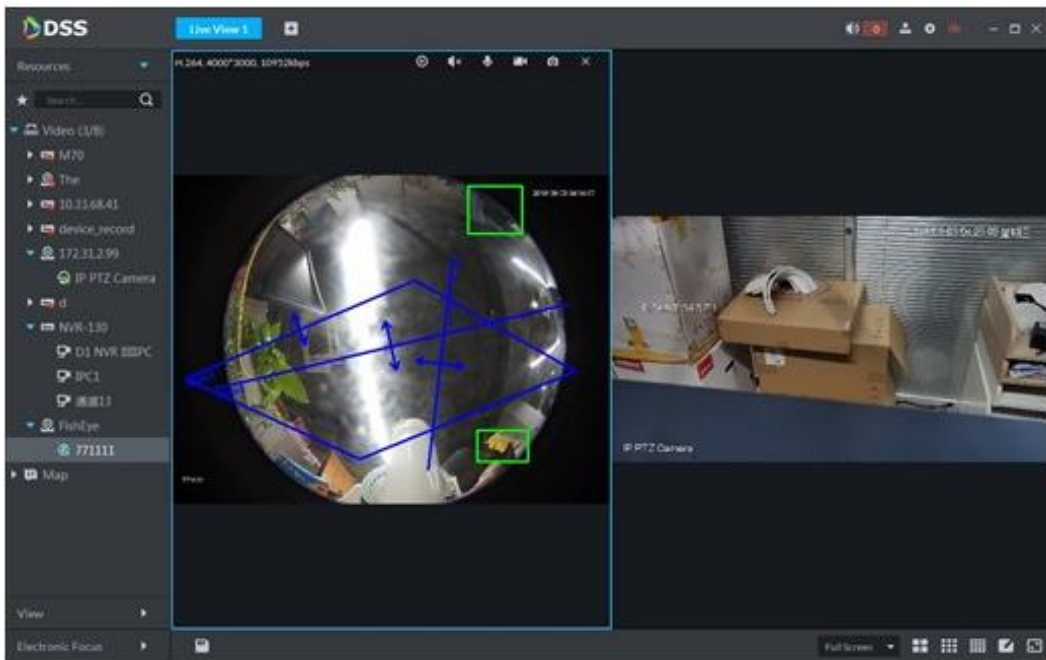
Refer to above steps to add at least three calibration points. These three points shall not be on the same straight line.

**Step 5** Click Save.

### 5.3.4.3 Enable Smark Track Function

**Step 1** Select the fisheye device on the device tree and then right click to select Smart track. See Figure 5-28.

Figure 5-28



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


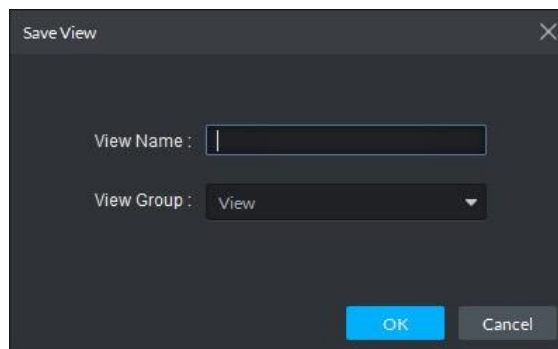
**Step 3** Click , system pops up Save View box. See Figure 5-29.

Figure 5-29



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

### 5.3.5 View Tour

**Step 1** On the “Live View” interface, double click a channel on the left side to open the video.


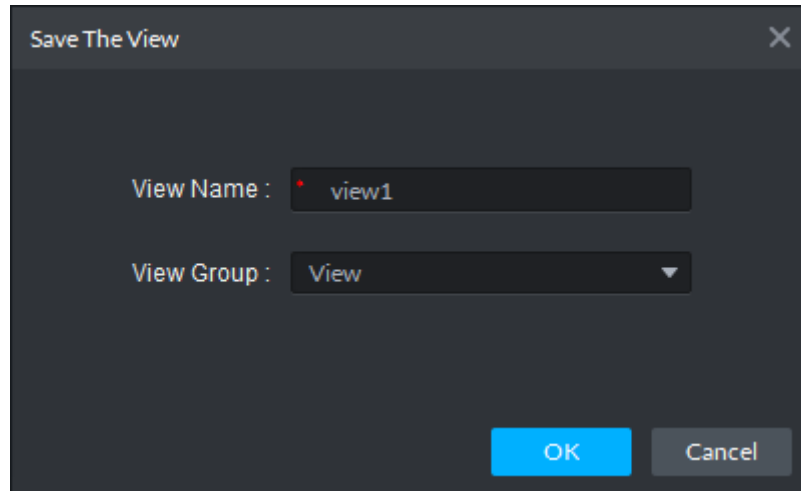
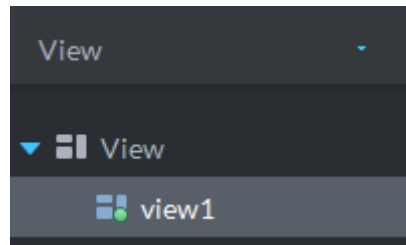
**Step 2** Click  in the lower part, system pops up “Save the View” dialogue box. See Figure 5-30.

Figure 5-30



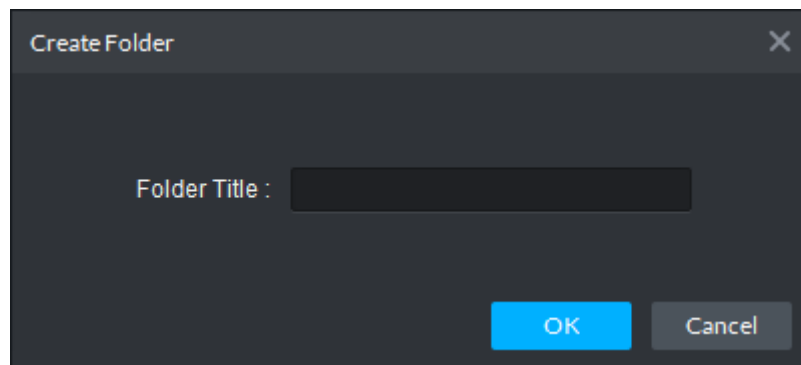
**Step 3** Input "View Name", select "View Group", and click "OK".  
Check the added view under View tab on the left. See Figure 5-31.

Figure 5-31



**Step 4** Right click View and then select New directory.  
Create folder dialogue box is displayed. See Figure 5-32.

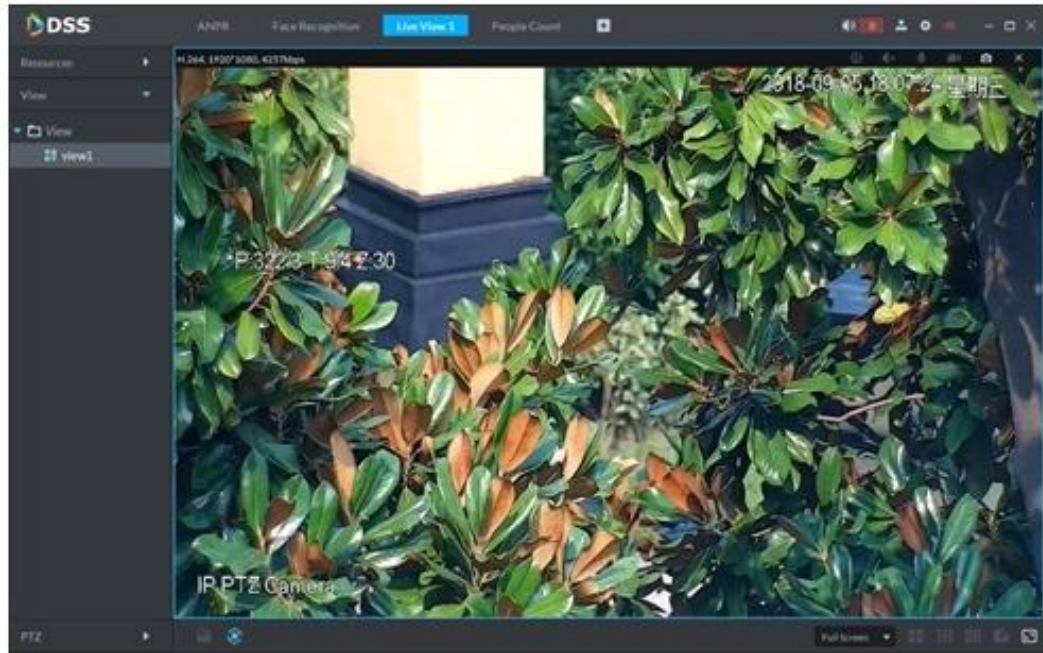
Figure 5-32



**Step 5** Input "Folder Title" and click "OK".  
**Step 6** Right click View to select Tour interval, for example, 10s.  
a View Tour will be initiated at intervals of 10s. See Figure 5-33.

Click  to stop Tour.

Figure 5-33

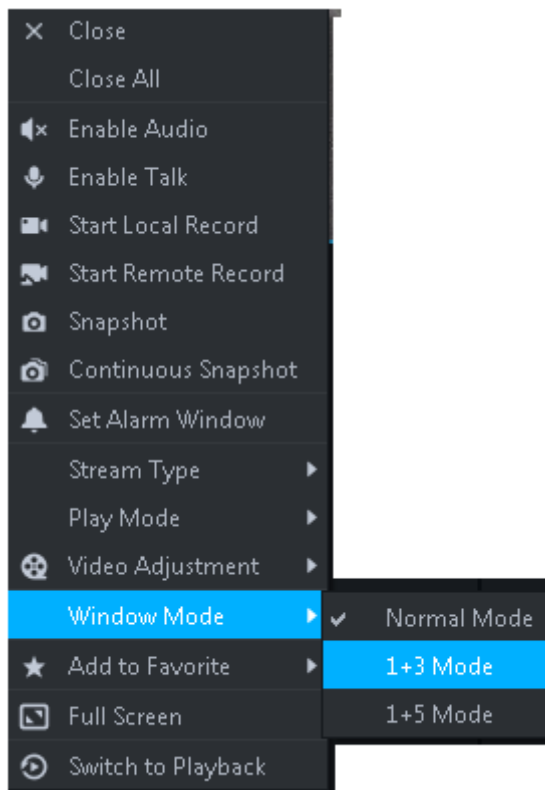


### 5.3.6 Region of Interest (RoI)

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

Right click to select “Screen Mode” in the live view window. See Figure 5-34.

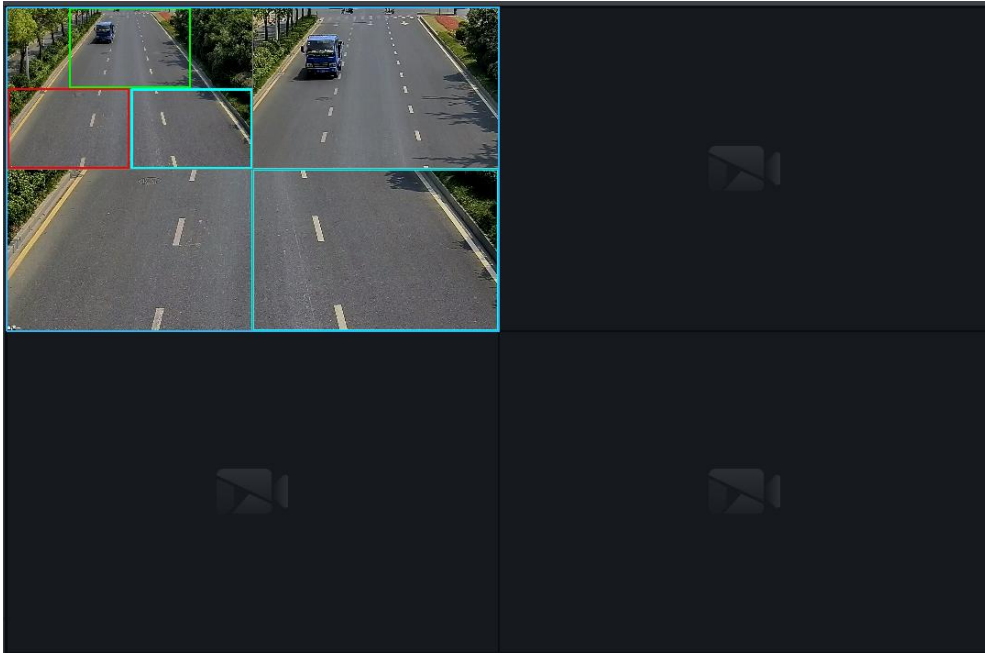
Figure 5-34



For example, select 1+3 mode. See Figure 5-35.



Figure 5-35



## 5.4 Record

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

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

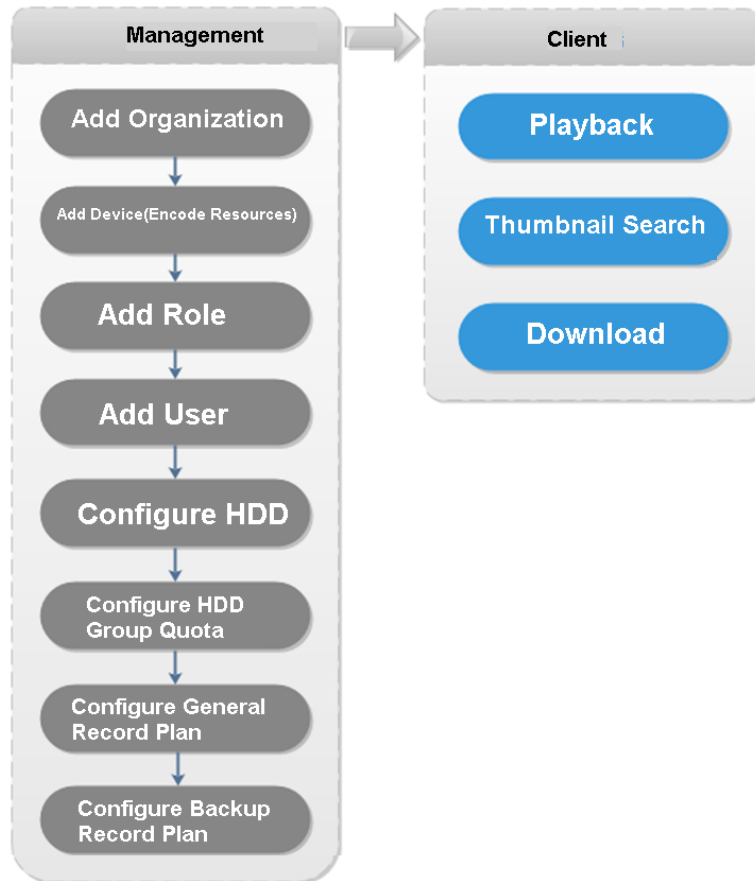
### 5.4.1 Preparations

Make sure you have set record schedule on the manager. Contact the admin or refer to chapter 4.7 Configuring Record Schedule for detailed information.

Refer to Figure 5-36 for Playback flows information.



Figure 5-36



## 5.4.2 Recording when Previewing

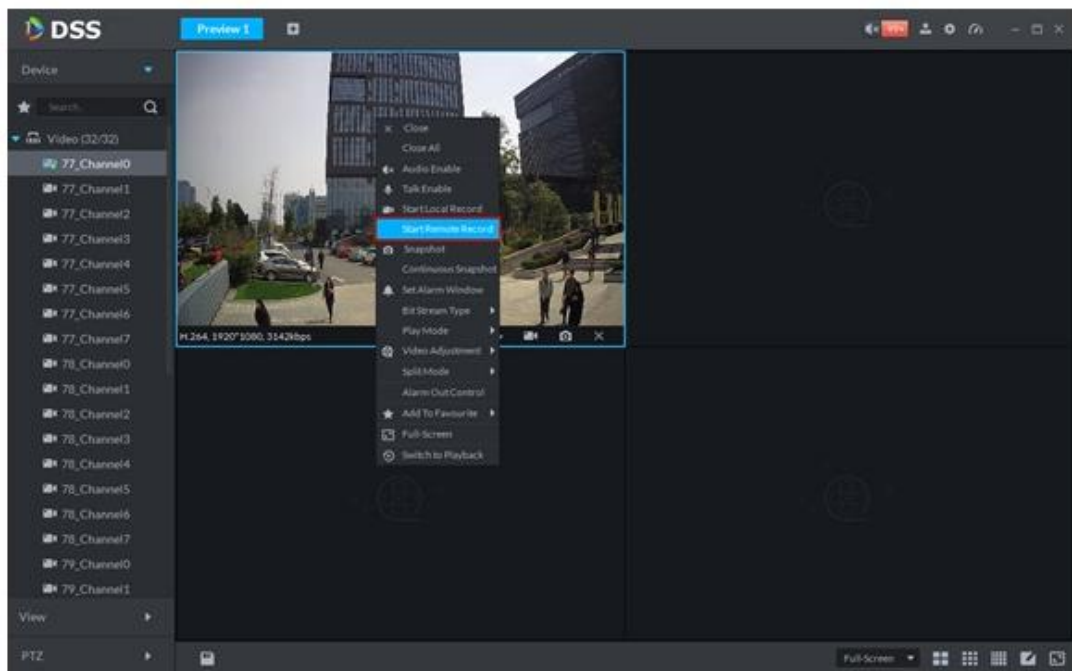
Open video in the preview window of the Client, then you can start center record of the channel from the right-click menu, provided that the center storage disk has been configured and the channel is not configured with a central storage plan.

Step 1 On Preview window, click the corresponding channel of the device tree on the left.

Step 2 Right click the window, and select "Start Remote Record"

See Figure 5-37.

Figure 5-37




 **NOTE**

- Stop remote record: Select the window that is remotely recording and then right click mouse to select Stop remote record.
- Once current channel has the record at the same time, the preview window overlays record status.

## 5.4.3 Playback

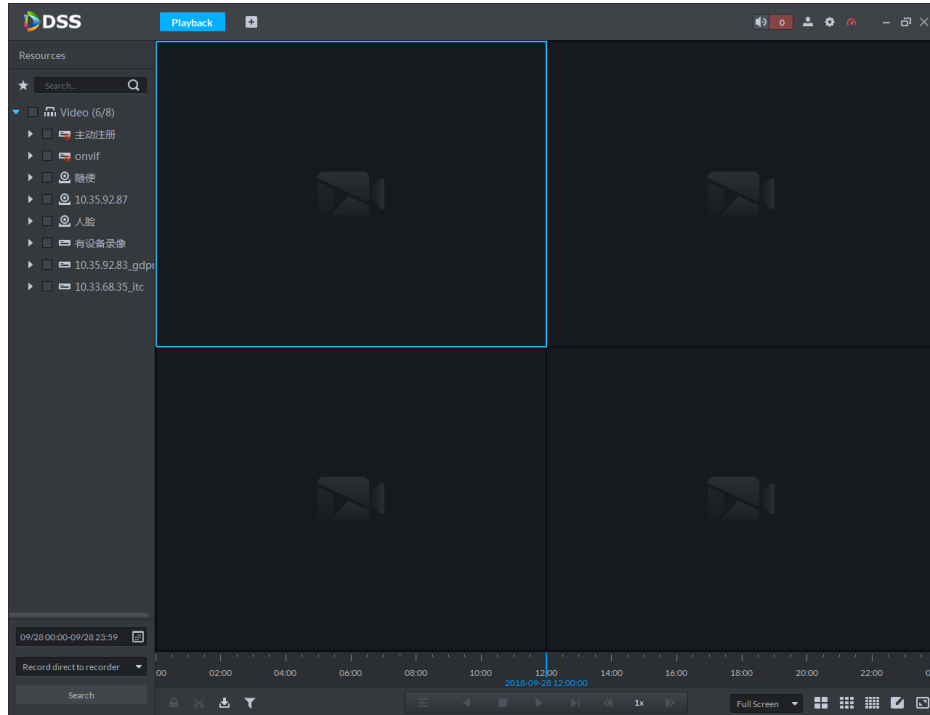
### 5.4.3.1 Search Record

It is to search record of today, specified date or specified period.

Step 1 Click , on the new tab interface select Playback.


The Playback interface displayed. See Figure 5-38.

Figure 5-38



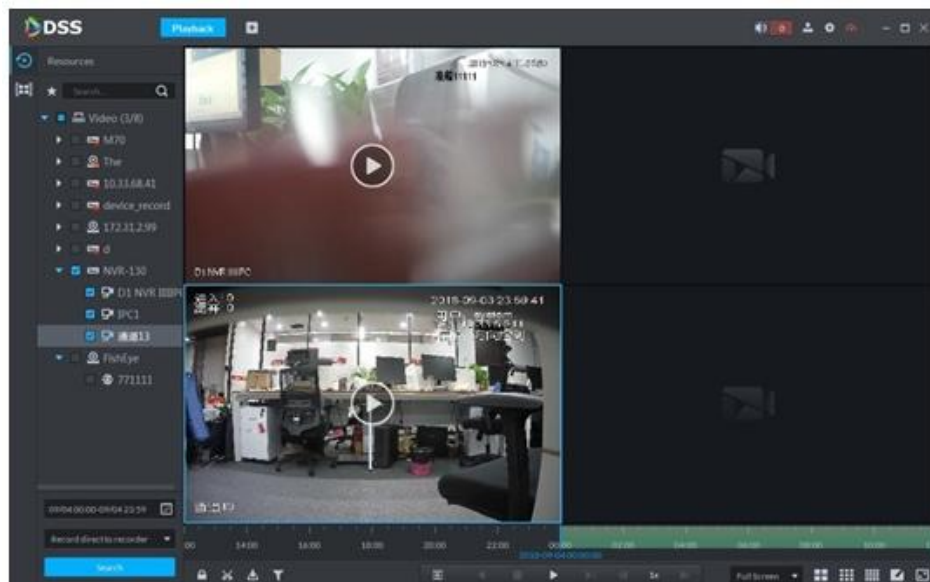
**Step 2** Select a channel on the device tree.

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

**Step 4** Select a video window that has the record and then click .

Corresponding window begins playback the record of current channel. See Figure 5-39.

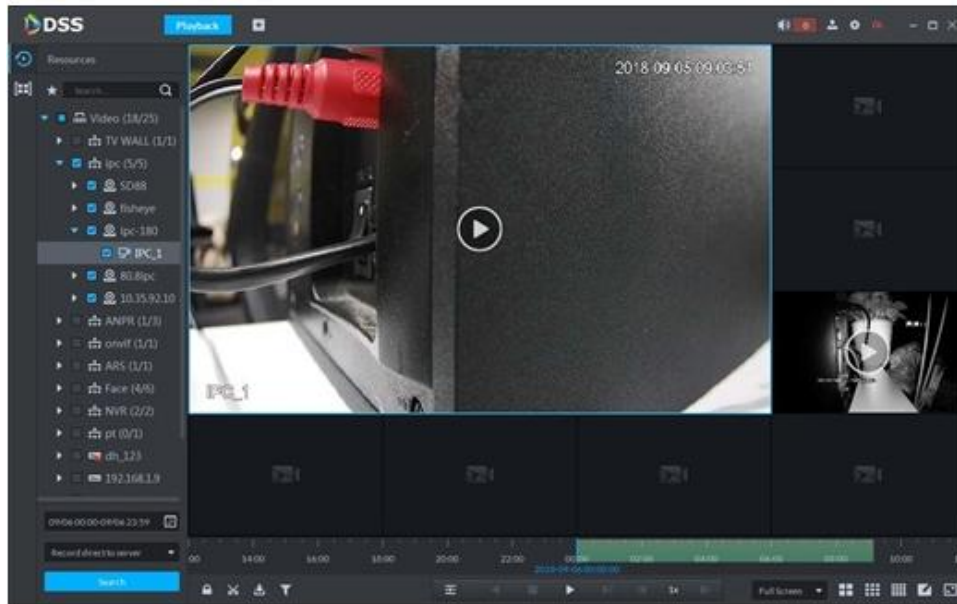
Figure 5-39



### 5.4.3.2 Record Type Filter

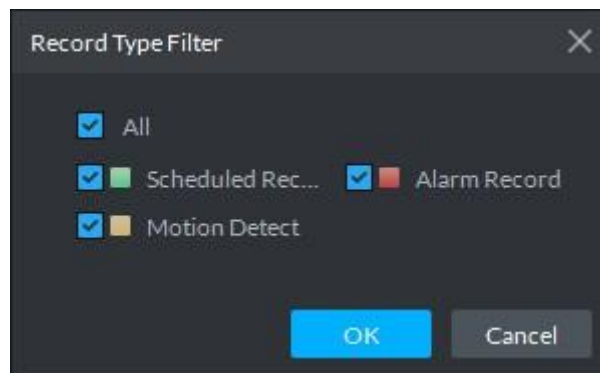
**Step 1** On Playback interface, click . See Figure 5-40.

Figure 5-40



System pops up Record type filter interface. See Figure 5-41.

Figure 5-41



**Step 2** Select a record type (or types) and then click OK.

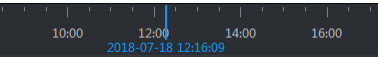
The record type includes schedule record, alarm record, motion detect record.

### 5.4.3.3 Record Control

Refer to Table 5-15 for buttons at the bottom of record playback interface and the description

Table 5-15


Icon	Note
	It is to lock record
	It is to cut record
	It is to download record
	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.

Icon	Note
	During playback, you can drag time progress bar to play back record at the specific time.

### 5.4.3.4 Lock Record

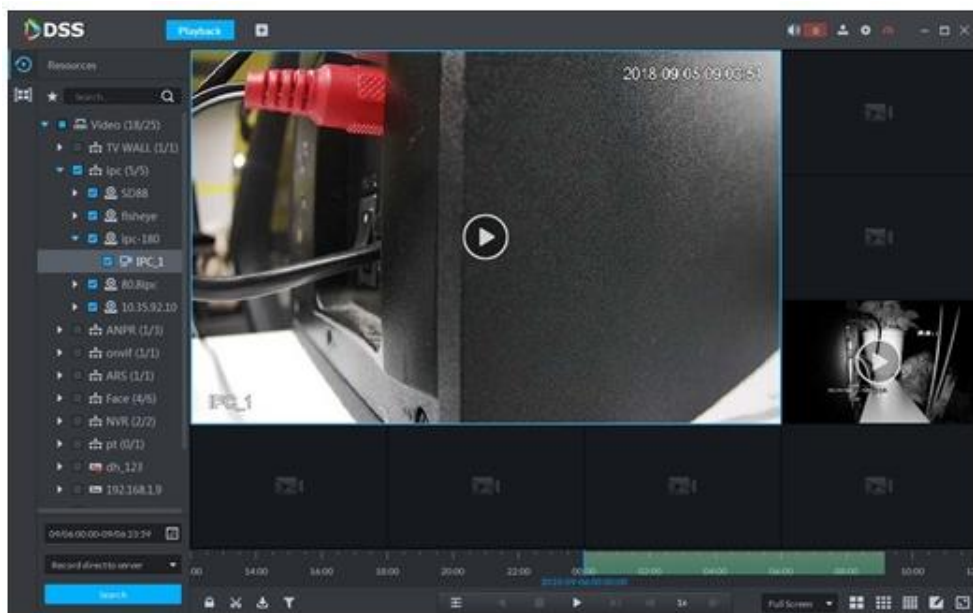
#### NOTE

You can only lock center records stored on the server

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

Move the mouse to the timeline. See Figure 5-42.

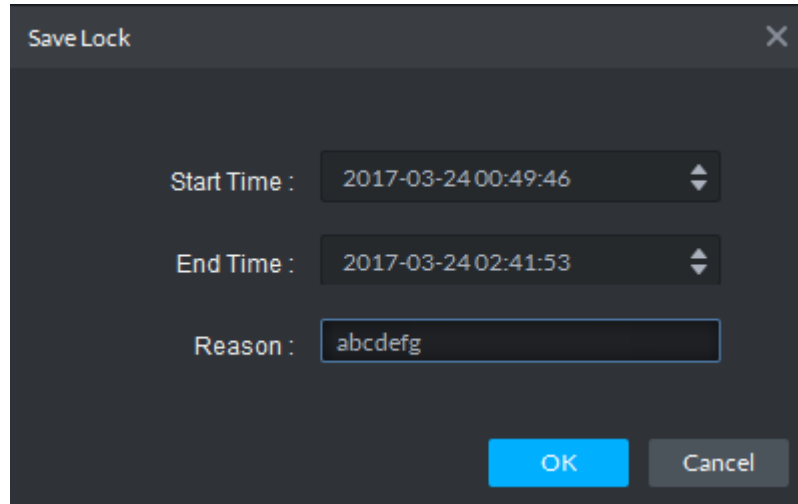
Figure 5-42



**Step 2** Click the time progress bar to select lock start time, then drag mouse, and then click to select end time.

System pops up “Save Lock Record” dialogue box. See Figure 5-43.


Figure 5-43



Step 3 Click OK.

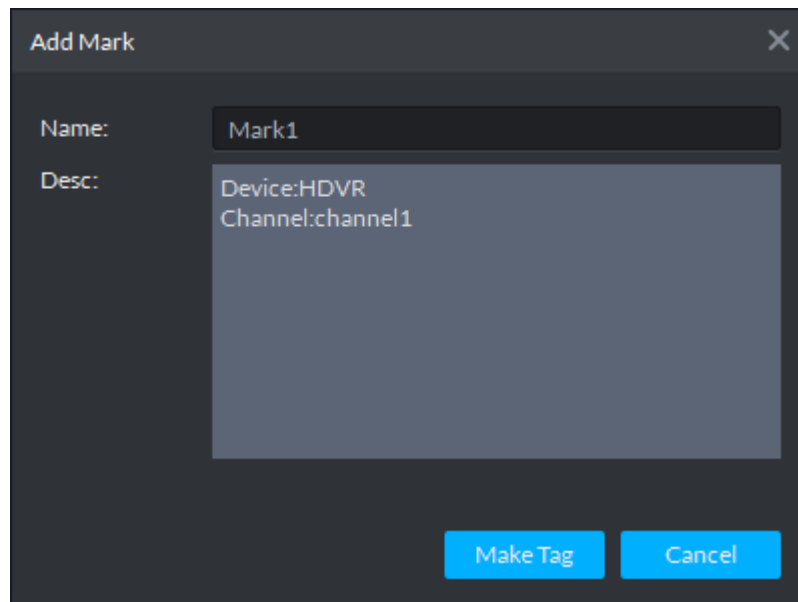
### 5.4.3.5 Add Mark

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

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


System pops up Add mark interface. See Figure 5-44.

Figure 5-44



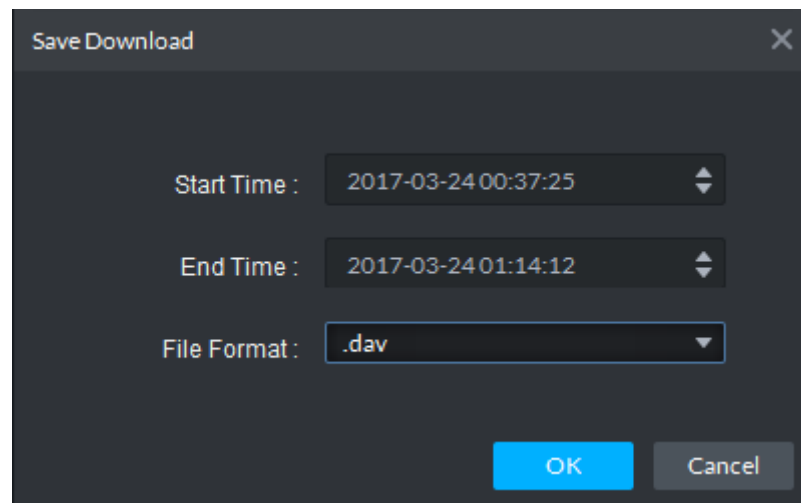
Step 2 Input “Name” and “Description”, then click “Make Tag”.  
System prompts “Tag Creation Successful”.

### 5.4.3.6 Clip Record

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

Step 2 During the timeline, click to start clip and then drag the mouse, click to stop clip. The Save download interface is displayed. See Figure 5-45.

Figure 5-45



Step 3 Set file format and then click OK.



## 5.4.4 Download

Go to the Download center of the DSS client to download the corresponding records. You can download by the timeline, by selection or download marked file.

### 5.4.4.1 Timeline

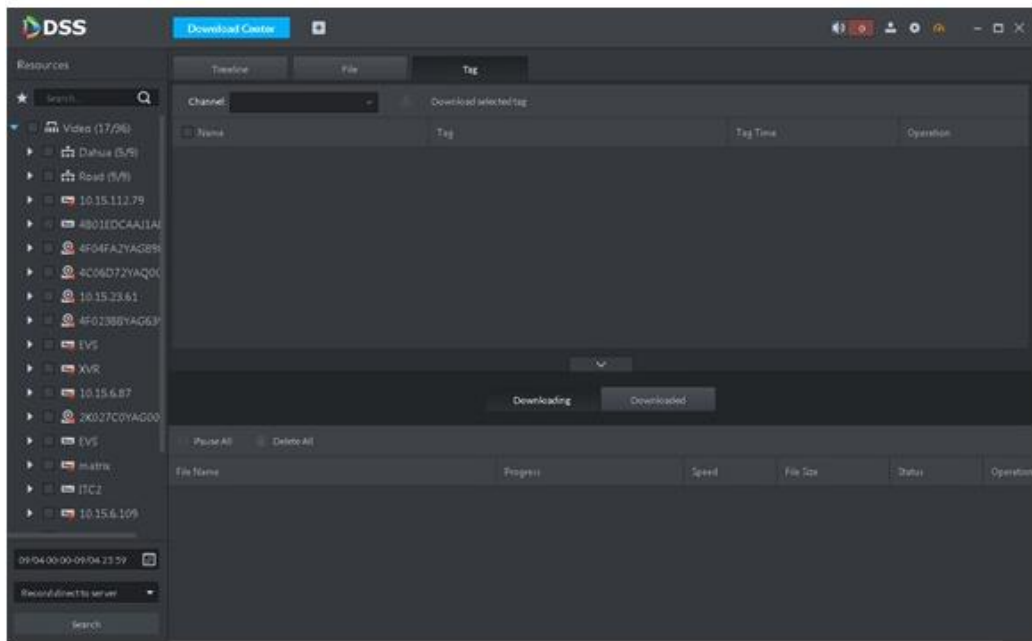
Step 1 Go to Download center.

There are two ways to go to the download center.

- Click  at the bottom of the Playback.
- Click , on the New tab interface, select Download center.

The Download interface is displayed. See Figure 5-46.

Figure 5-46

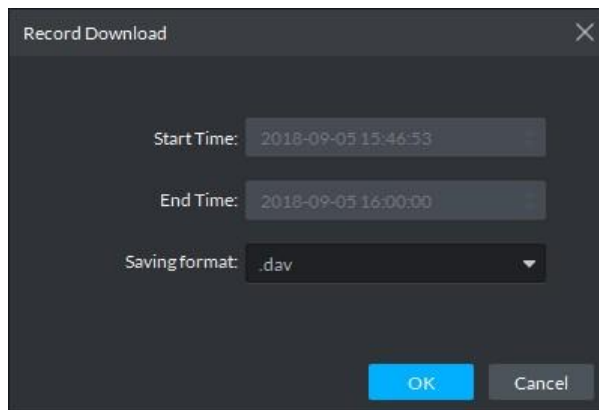


**Step 2** Click Timeline.

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

**Step 4** Select the period on the timeline, system pops up download dialogue box. See Figure 5-47.

Figure 5-47

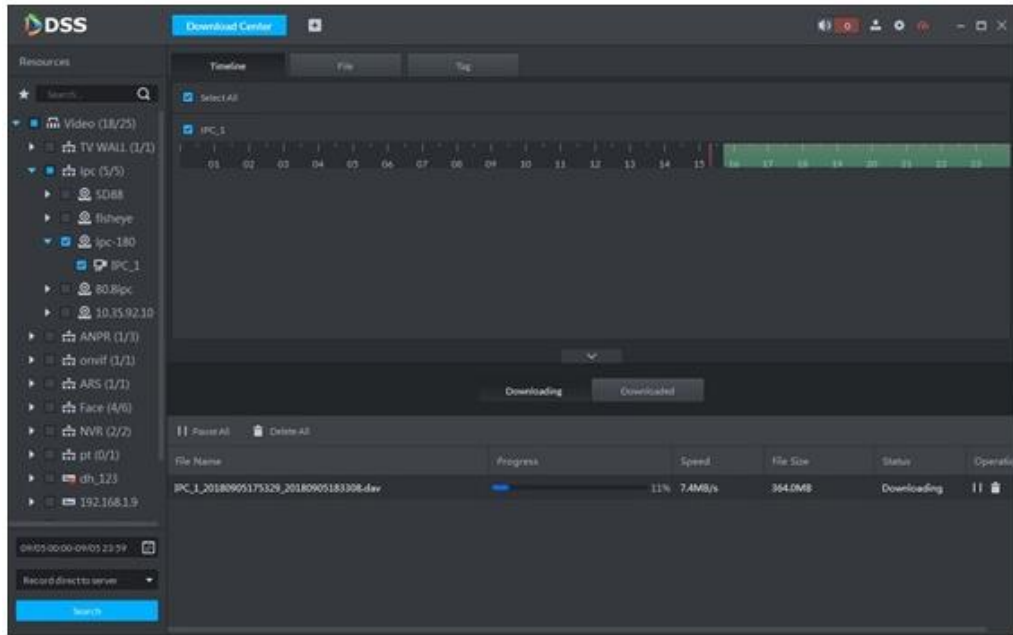


**Step 5** Set file format and then click OK.

You can view the download process at the bottom of the interface. See Figure 5-48.

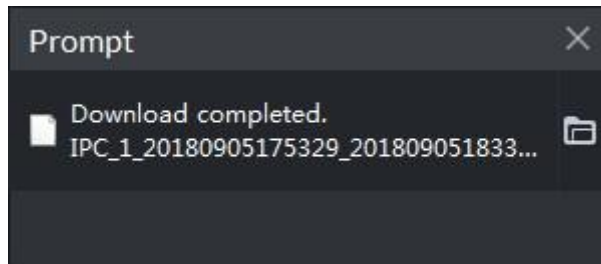


Figure 5-48



System pops up the following dialogue box once the download is complete. See Figure 5-49.

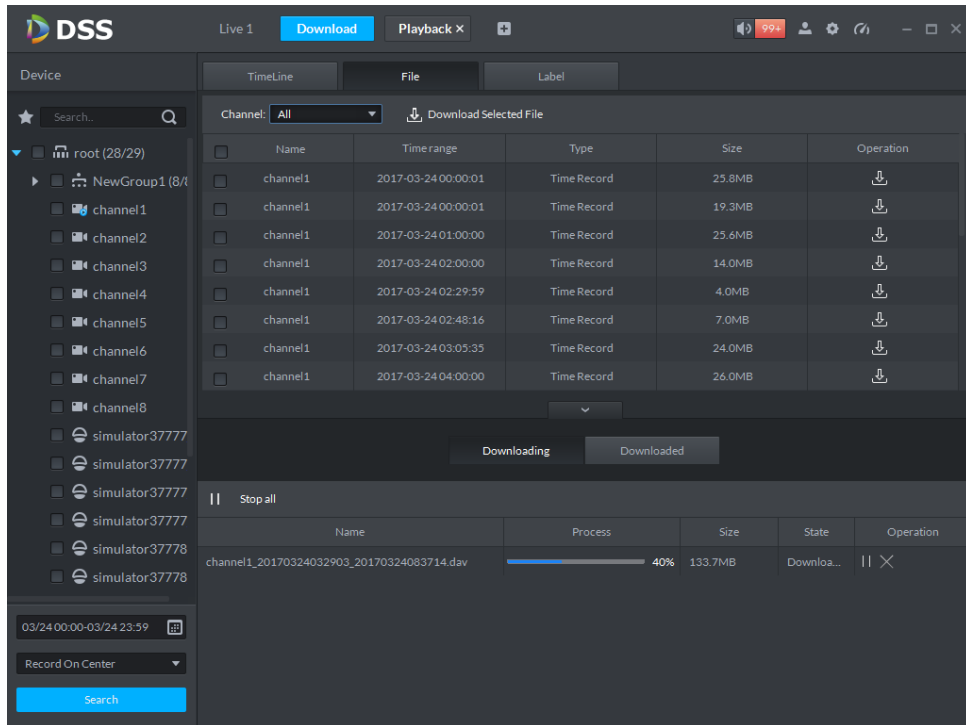
Figure 5-49




#### 5.4.4.2 File List

- Step 1 On Download interface, click File tab.  
System displays record files. See Figure 5-50.

Figure 5-50

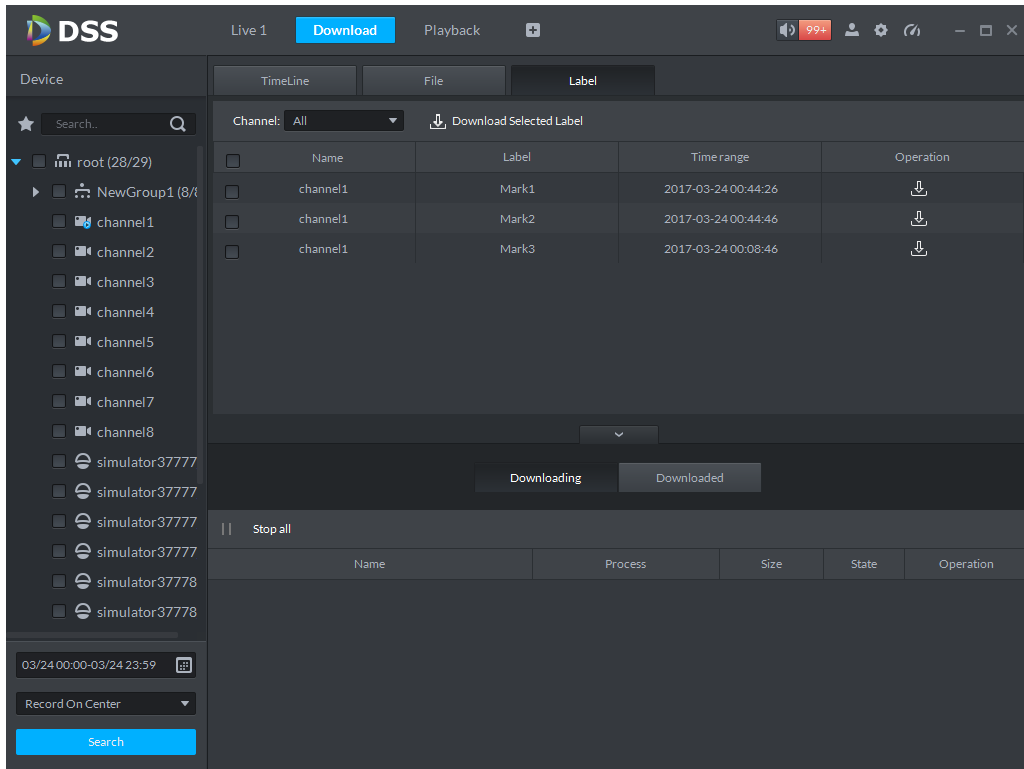



**Step 2** Directly click  in the record file list, or check multiple files and click “Download Selected Files”  
System displays download process at the bottom of the interface. System pops up dialogue box once the download is complete.

### 5.4.4.3 Label

**Step 1** On Download interface click Label tab.  
System displays marked record files. See Figure 5-51.

Figure 5-51



**Step 2** Directly click  in the record file list, or check multiple files and click “Download Selected Files”  
System displays download process at the bottom of the interface. System pops up dialogue box once the download is complete.

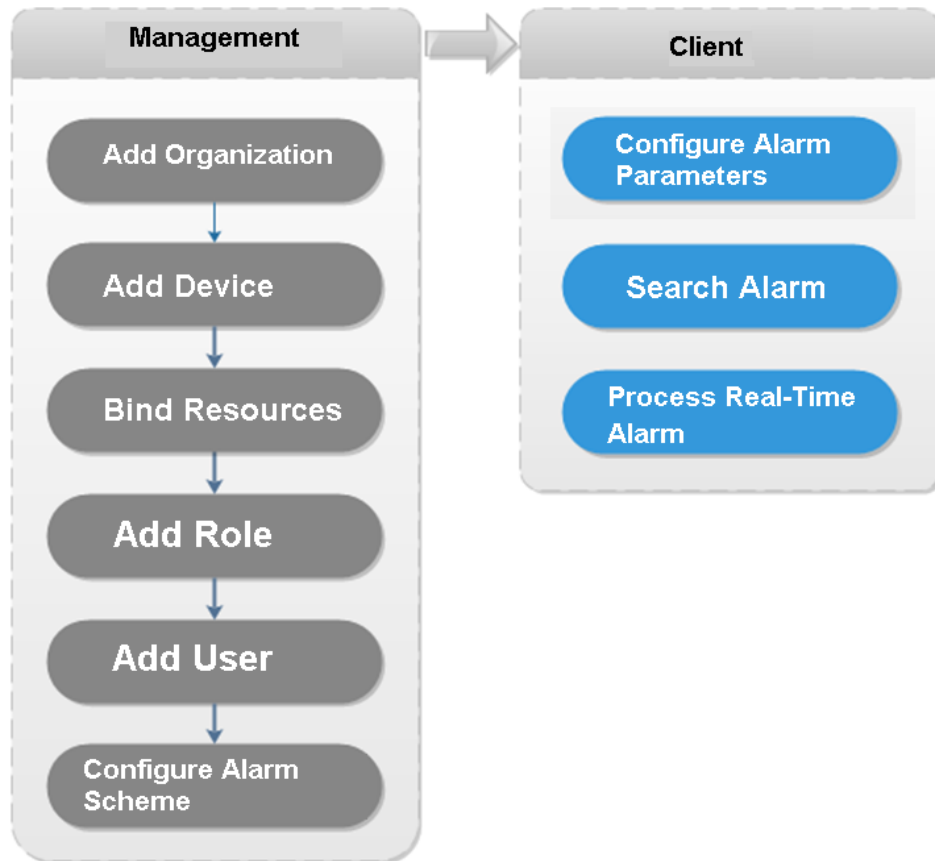
## 5.5 Event Center

### 5.5.1 Preparations

- Make sure you have added corresponding devices on the manager. Refer to chapter 4.6 Adding device for detailed information.
- You have completed event management settings on the manager. Refer to chapter 4.8 Configuring Event for detailed information.

Refer to Figure 5-52 for event management flows.

Figure 5-52



## 5.5.2 Configuring Alarm Parameters

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


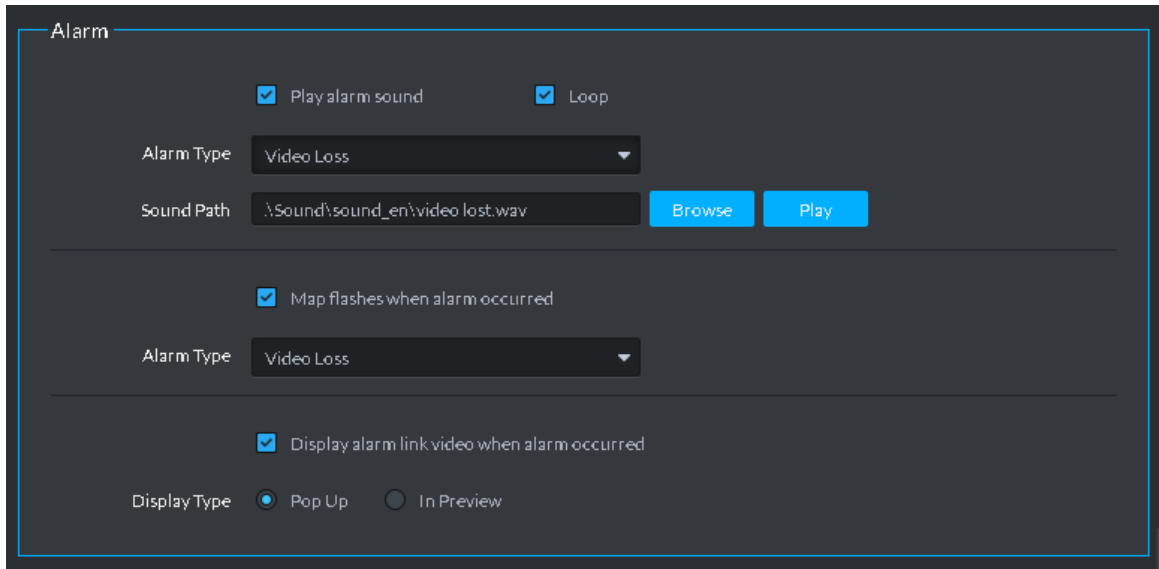
**Step 1** Click  at the top right corner, from General>Alarm, the interface is shown as below. See Figure 5-53.

Figure 5-53



**Step 2** Set alarm parameters and then click Save.  
Refer to Table 5-16 for detailed information.

Table 5-16

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

### 5.5.3 Searching and then Processing Real-Time Alarm


**NOTE**

The customized alarm supports modification and deletion.

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

### 5.5.3.1 Processing Real-Time Alarm

#### Steps

**Step 1** Click , on the New tab interface select Event center.  
Enter Event center interface.


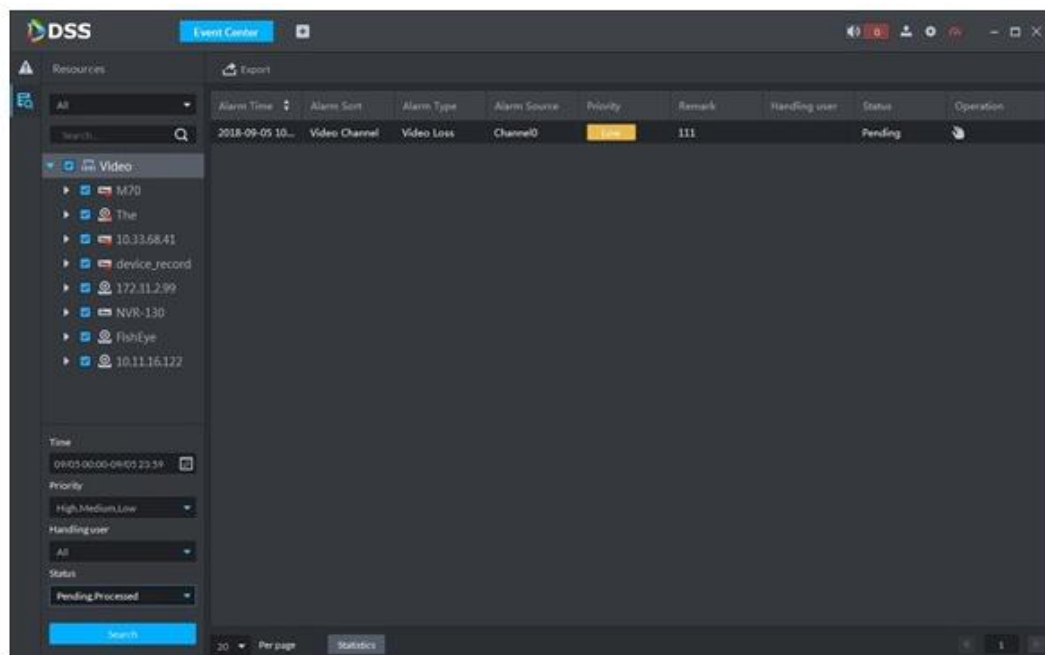


**Step 2** Click  on the left navigation bar.  
System displays alarm processing interface. See Figure 5-54.

Figure 5-54



#### NOTE

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

**Step 3** Click  of an alarm item.

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


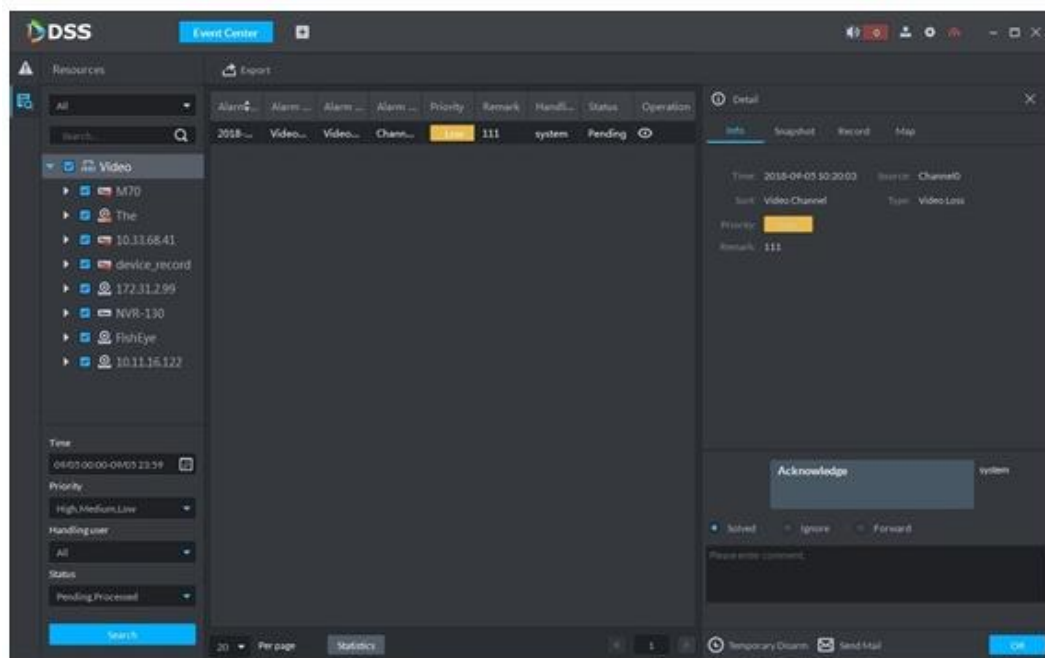
**Step 4** Click  to view details and process the alarm. See Figure 5-55.

Figure 5-55



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

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

 **NOTE**

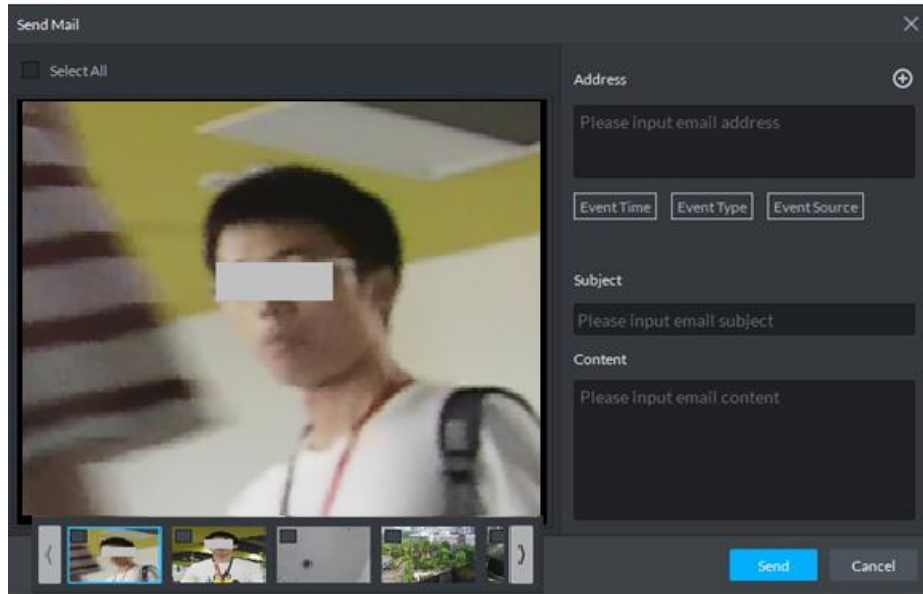
When you are selecting Forward, you can select other user on the dialogue box. It is to send current event to specified user to process.

**Step 7** Click OK.

## Operations


- Disarm temporarily: Click disarm temporarily, and then set disarm time on the pop-up window. Click OK.
- Send email: Click Send email, and then set email information on the pop-up window. Click Send, the interface is shown as below. See Figure 5-56.

Figure 5-56



### 5.5.3.2 Searching Alarm Record

#### Steps

**Step 1** Click , on the New tab interface select Event center.  
Enter Event center interface.


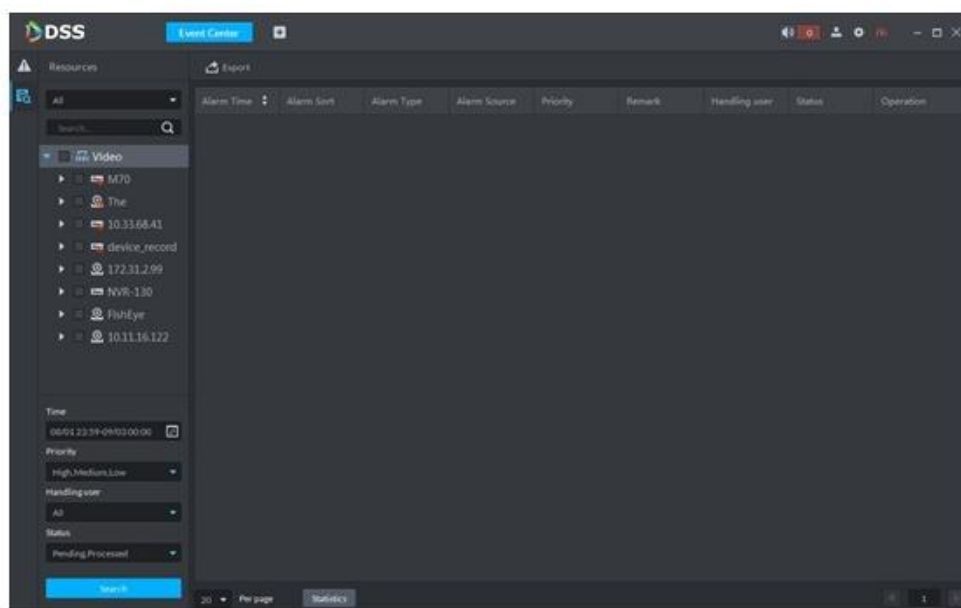
**Step 2** Click  on the left navigation bar.  
System displays search interface. See Figure 5-57.

Figure 5-57



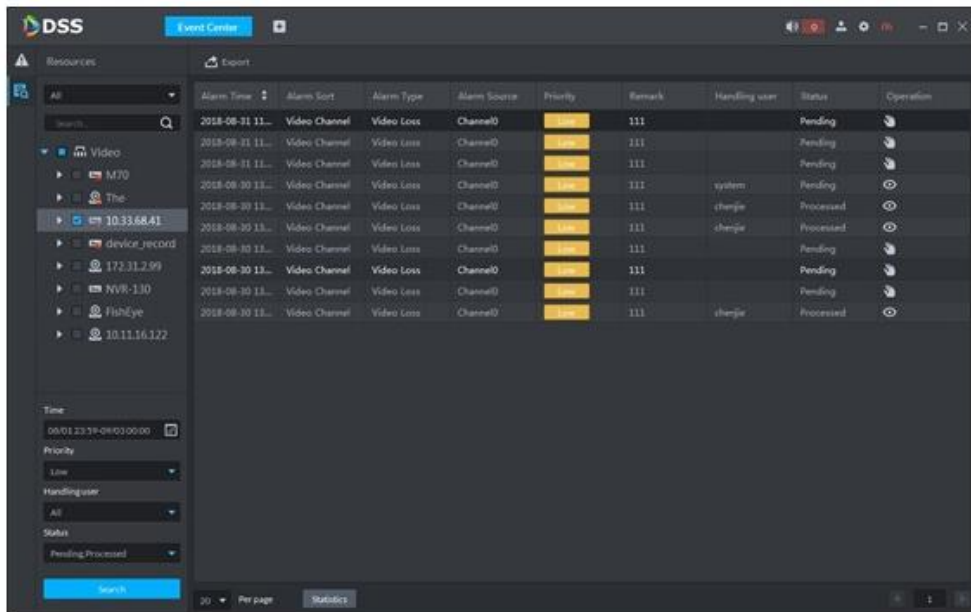
**Step 3** Select device channel, search time, alarm level, user or alarm status.





**Step 4** Click Search.

System displays corresponding alarm information. See Figure 5-58.

Figure 5-58



## Operations

- Select amount on per page, it is to set displayed alarm message amount each time.
- Click Statistics, it is to display the total alarm message amount of corresponding device.
- Click Export, it is to export device alarm message.
- Click  to claim alarm, click  to process alarm. Refer to chapter 5.5.3.1 Processing Real-Time Alarm for detailed information.

## 5.6 Video Wall

### 5.6.1 Preparations

It is to view the video on the video wall on the client. It needs to complete the following settings.

- Adding corresponding device: It includes decoder, encoder or matrix device. Refer to chapter 4.6 Adding device for detailed information.
- Refer to chapter 4.10 Adding Video Wall to add the video wall first.

Refer to Figure 5-59 for video wall flows.

Figure 5-59



## 5.6.2 Output to the Wall


Step 1 Click , on the New tab interface select Video wall, system displays Video wall interface. See Figure 5-60.

Figure 5-60

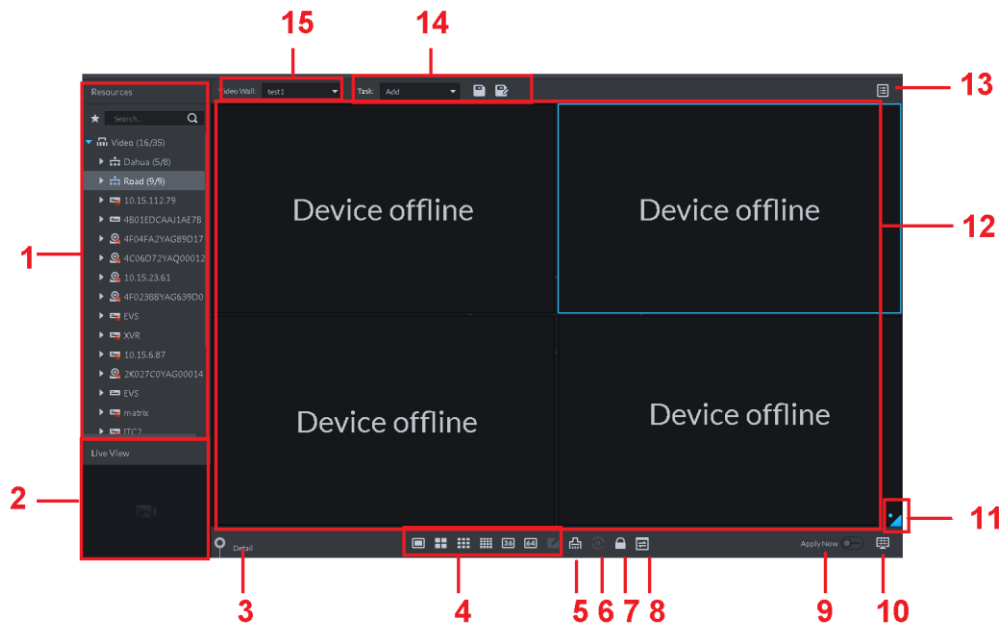


Table 5-17

SN	Name	Function
1	Device tree	<p>From Local config&gt; 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.</p> <p>Click  to view the channels on the favorites folder.</p> <p>Search is supported by input device name or channel name in <input type="text" value="Search.."/> here.</p>
2	Preview	View channel video.
3	Detailed information	<p>Click to view the screen, window, and channel bound information.</p> <ul style="list-style-type: none"> <li>Click  to preview the video at the bottom left pane. It is to check current channel is what you want or not.</li> <li>Click  to adjust sequence.</li> <li>Click  to delete the video channel that adds to current window.</li> <li>Click Stay time column or click , it is to modify signal interval on current channel when tour.</li> <li>Click Stream column or , it is to modify video bit stream.</li> </ul>
4	Window split	It is to set window split mode.
5	Clear	It is to clear information on all screens.
6	Start/stop all tours	Start or stop all tours.

SN	Name	Function
7	Lock window	Click to lock the window. You cannot operate on the locked window.
8	Display layout	It is to view current layout.
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	It is to schedule task and tour task. Refer to chapter 5.6.3 Video wall plan for detailed information.
14	Task management pane	It is to add, save delete task.
15	Video wall selection	It is to select a video wall to configure.

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


**Step 3** Double click the video channel or drag the video channel to the window.  
The window displays “Bound one video source”

 **NOTE**

- Input device name or channel name to search.
- One window can bind several video channels at the same time.

**Step 4** Click  to output the video to the wall.

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

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

Right click mouse and then select Stop all tour, or click  to stop all tour.

## 5.6.3 Video Wall Plan

### 5.6.3.1 Configuring Schedule plan

After set schedule plan, you can play video file on the video wall at the specified time.

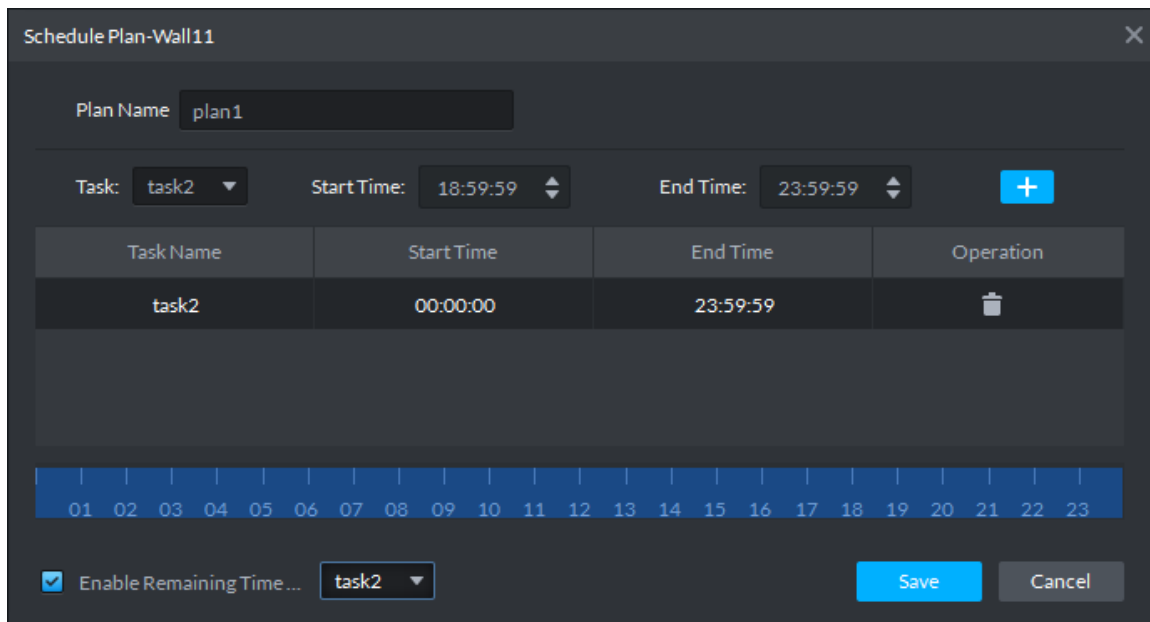
#### Steps

Step 1 On the Video Wall interface, click  at the top right corner.


Step 2 Select .

Enter Schedule plan interface. See Figure 5-61.

Figure 5-61



Step 3 Input the plan name.

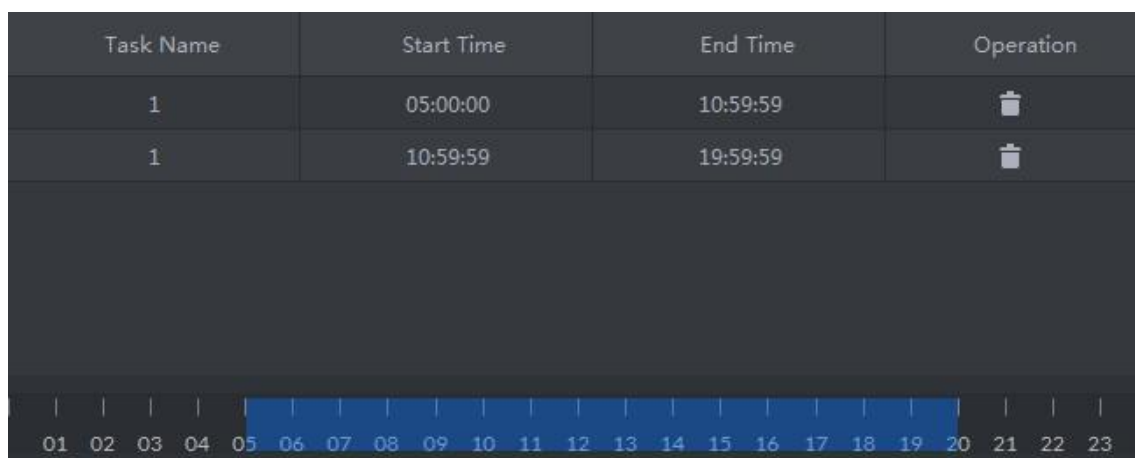
Step 4 Select a video task, and then set start time and end time, click .

The list displays detailed plan information. The specified period on the timeline is highlighted as blue. See Figure 5-62.

 **NOTE**

Check the Enable remaining time schedule function and set the task. The video wall displays corresponding video if it is not in the scheduled plan period.

Figure 5-62





Step 5 Click Save

Enter Video wall interface.

Step 6 Click  to start the plan.


## Operations

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

### 5.6.3.2 Configuring Tour Plan

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

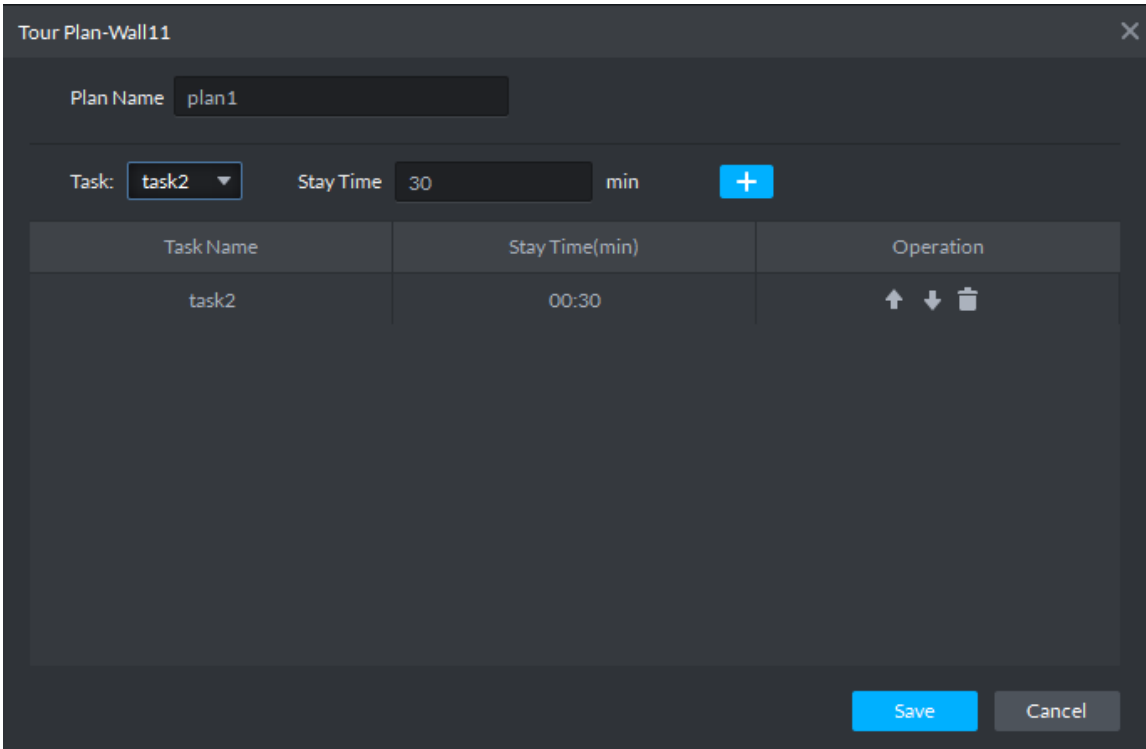
## Steps

Step 1 On the Video Wall interface, click  at the top right corner.

Step 2 Click .


Enter Tour plan interface. See Figure 5-63.

Figure 5-63



Task Name	Stay Time(min)	Operation
task2	00:30	↑ ↓ 🗑️

Step 3 Input task name.

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

The list displays tour information. See Figure 5-64.

 **NOTE**










Click   to adjust task sequence, click  to delete task.

Figure 5-64



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

**Step 5** Click Save.

Enter Video wall plan interface.

**Step 6** Click  to start the plan.

## Operations

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

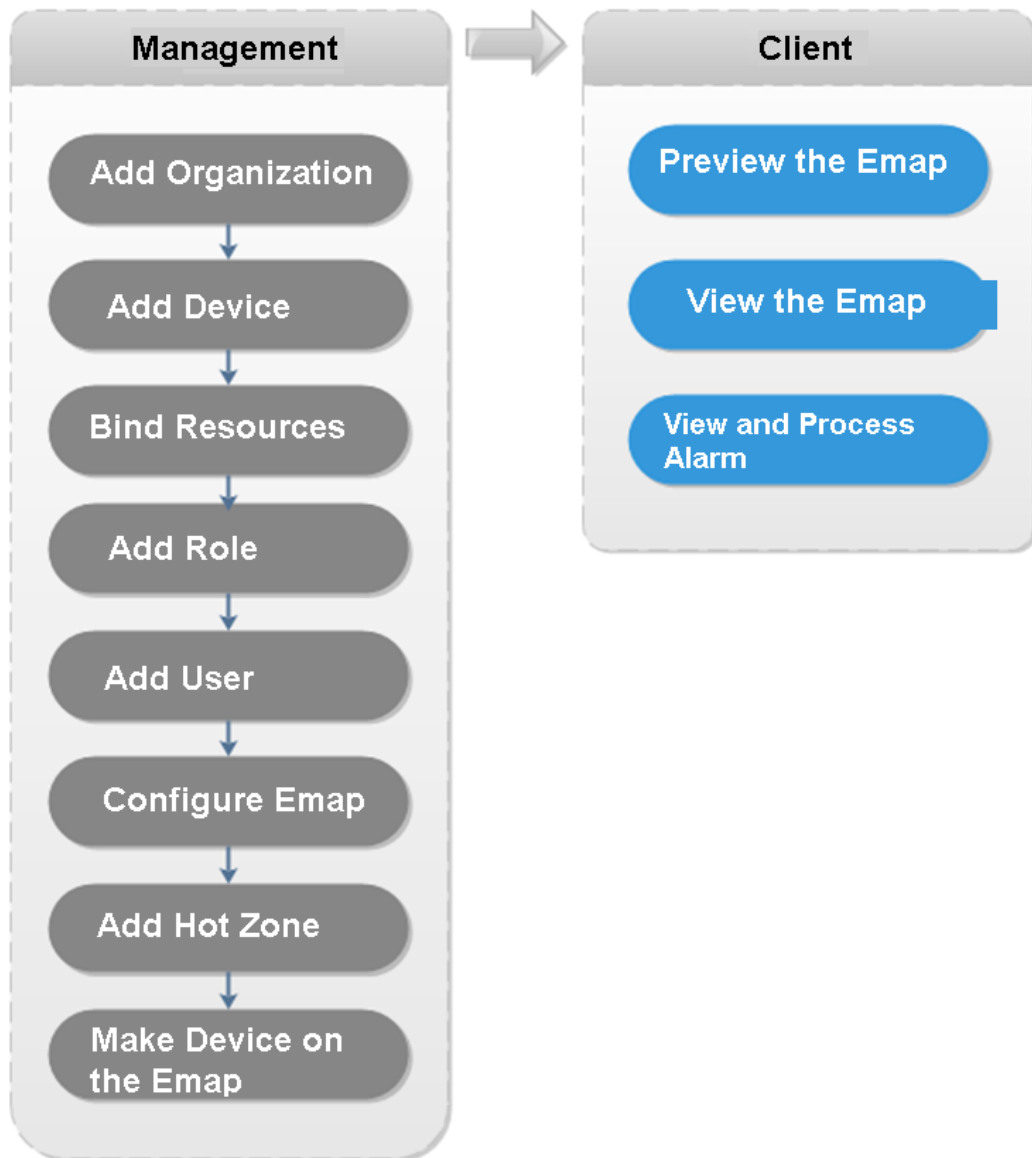
## 5.7 Emap

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

### 5.7.1 Preparations

Refer to chapter 4.9 Configuring Emap to add emap and hot zone on the platform manager and mark the device on the map. Refer to Figure 5-65 for flows information.

Figure 5-65

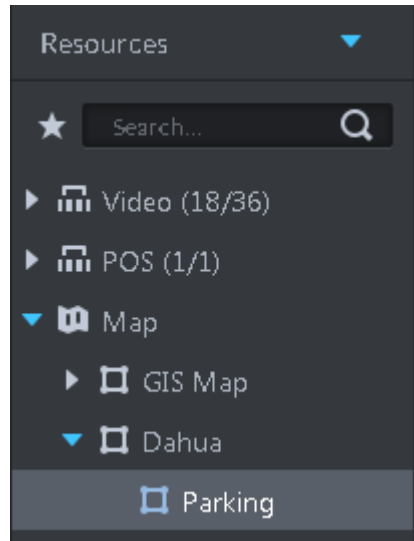


## 5.7.2 Open Emap on the Real-Time Preview

- Step 1 On the Live view interface, click the Map at the bottom of the device tree on the left. System displays map and hotspot map on the manager. See Figure 5-66.



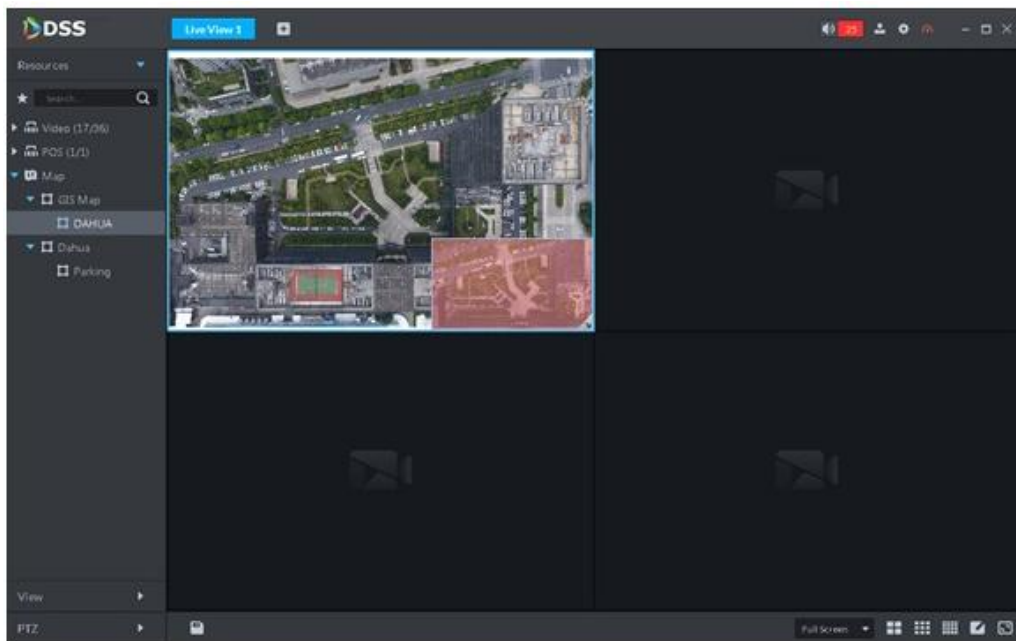
Figure 5-66



**Step 2** Double click the map; you can view the map and the added devices.

On the map, you can record real-time video, playback record file, cancel alarm, etc. See Figure 5-67.

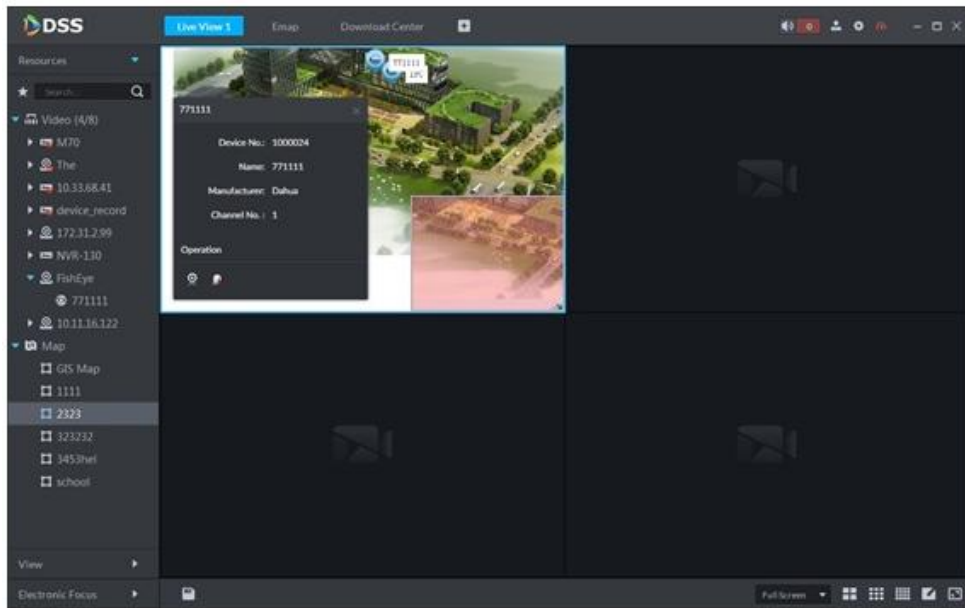
Figure 5-67



**Step 3** Click the marked channel.

System displays channel information. See Figure 5-68.

Figure 5-68




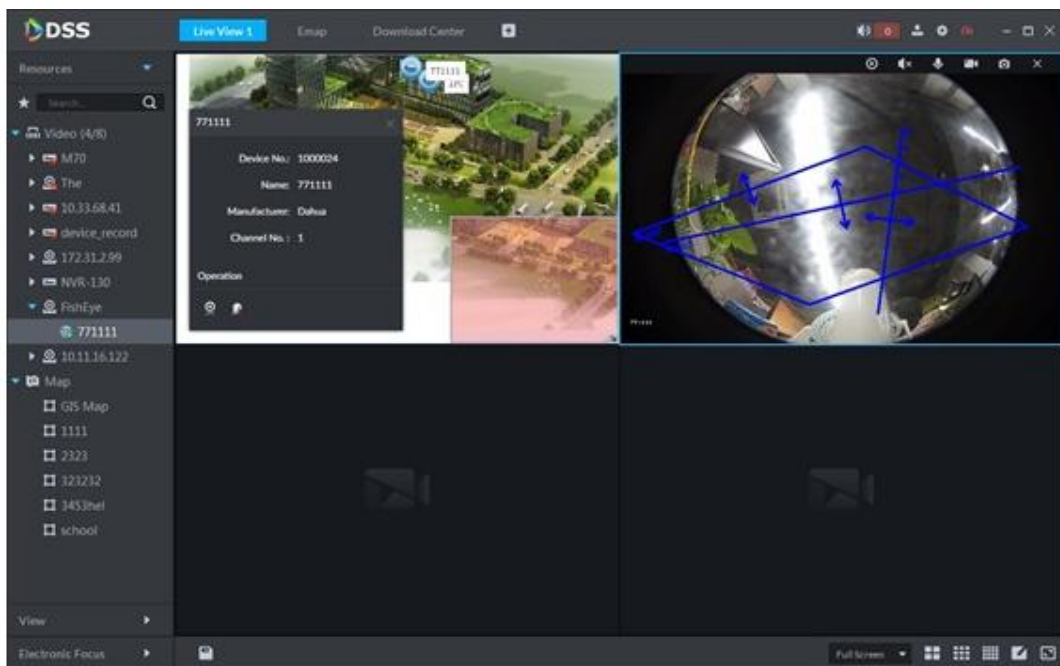

**Step 4** Click  to playback real-time video on the window. See Figure 5-69.

Figure 5-69



### 5.7.3 Viewing Map

It is to display the map setting on the manager. The e-map and the raster map are not the same. Here we use Google map to continue.

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

**Step 2** Select Google map or raster map.  
Enter Emap interface. See Figure 5-70.

Figure 5-70

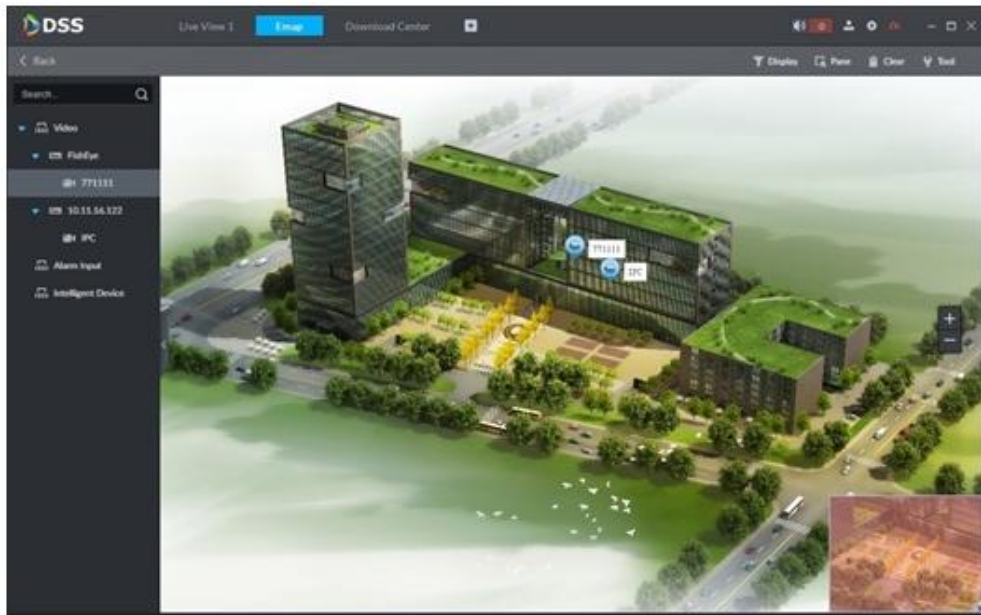


Table 5-18

SN	Name	Note
1	Display device	It is filter to display video device, alarm input channel.
2	Use frame to select	Use frame to select a device.
3	Clear data on the screen	Clear selection track on the screen.
4	Tools	It includes mark, reset, and video relay. <ul style="list-style-type: none"> <li>● Mark: It is to give a mark on the map.</li> <li>● Reset: The map restores default position.</li> <li>● Video relay: This function is null right now.</li> </ul>




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

**Step 4** Click the channel on the map.

System displays device SN, channel name, manufacture, channel information, etc. See Figure 5-71.

Figure 5-71



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

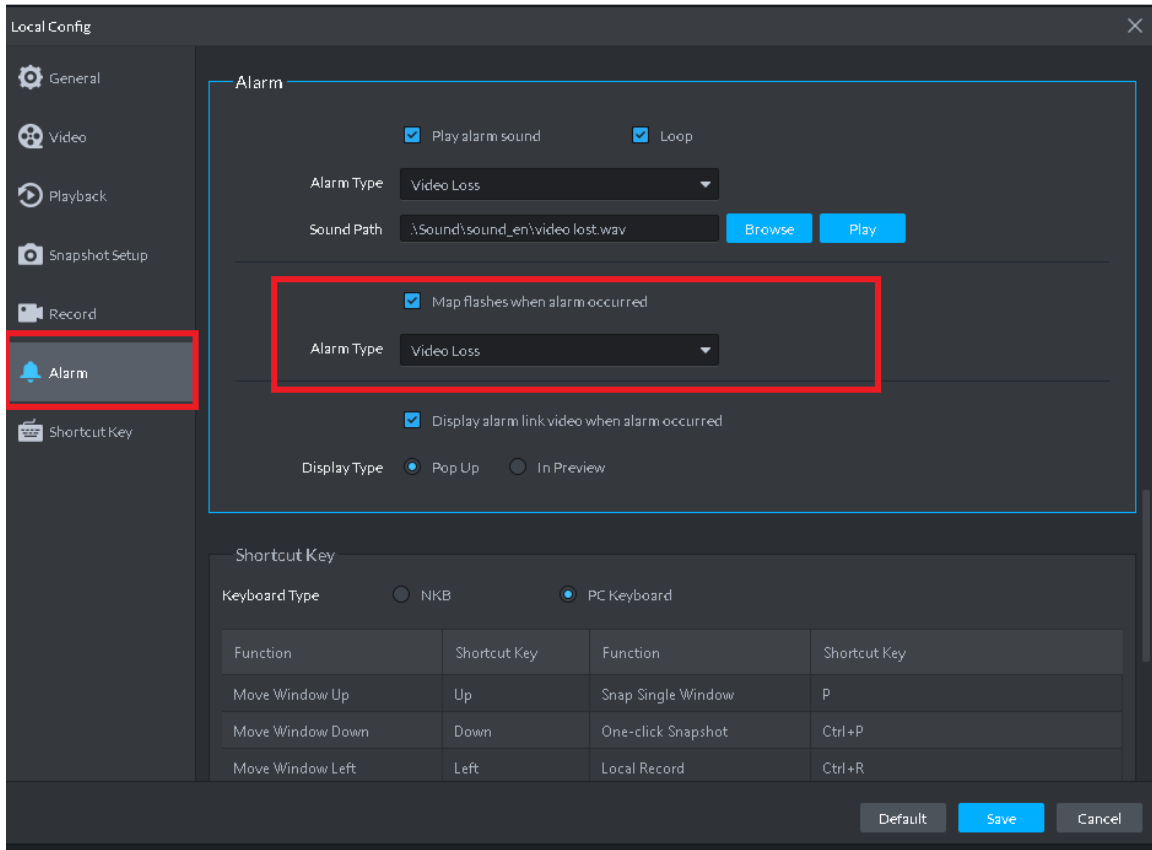
## 5.7.4 Alarm Flashing on the Map

### 5.7.4.1 Configuring Alarm Flashing on the Client

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

Step 2 Click Alarm tab, select “Map flashes when an alarm occurs” and then set alarm type from the dropdown list. See Figure 5-72.

Figure 5-72



**Step 3** Click Save.

### 5.7.4.2 Client Triggering Alarm

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

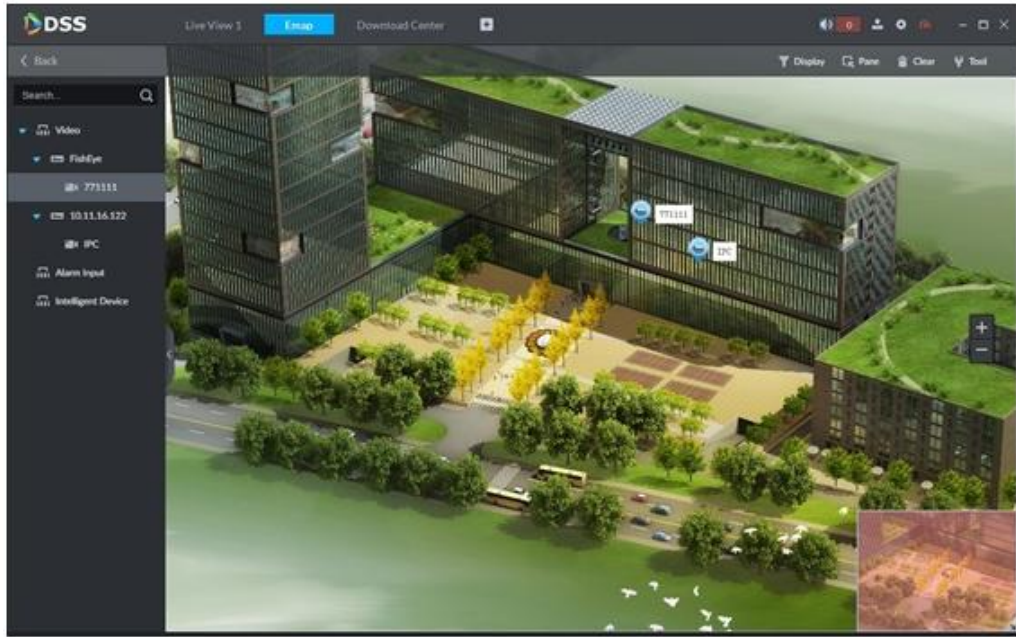
Enter Map interface.

**Step 2** Click to go to Google map or Raster map.

Here we use raster map to continue.

**Step 3** The channel is flashing when an alarm occurs. See Figure 5-73.

Figure 5-73



## 5.8 People Counting

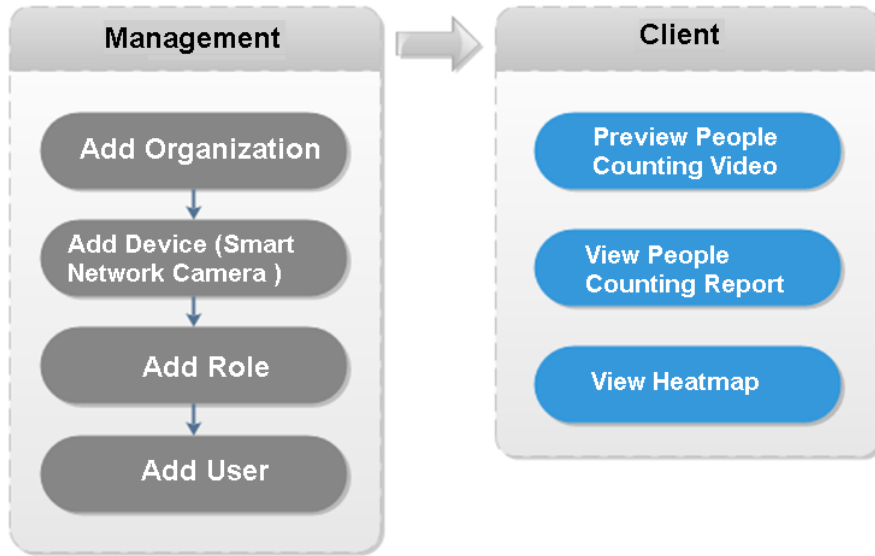
System supports people counting and heatmap function.

### 5.8.1 Preparations


- Refer to chapter 4.6 Adding Device to register the smart network camera that supports people counting function on the client.
- Refer to the network camera user's manual to set camera intelligent rules.

Refer to Figure 5-74 for flows information.

Figure 5-74

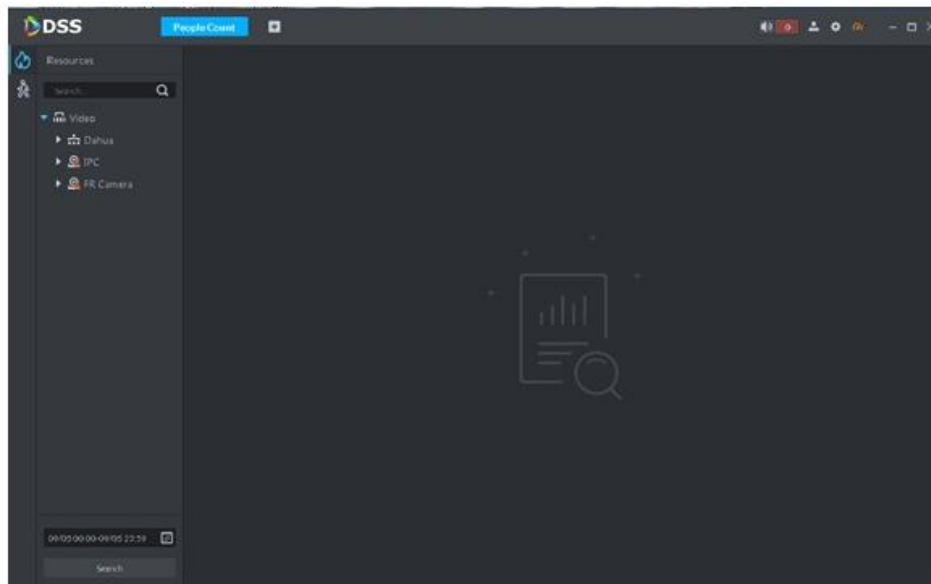


## 5.8.2 People Counting Report

Step 1 Click , on the New tab interface select People Count.

Enter People counting interface. See Figure 5-75.

Figure 5-75




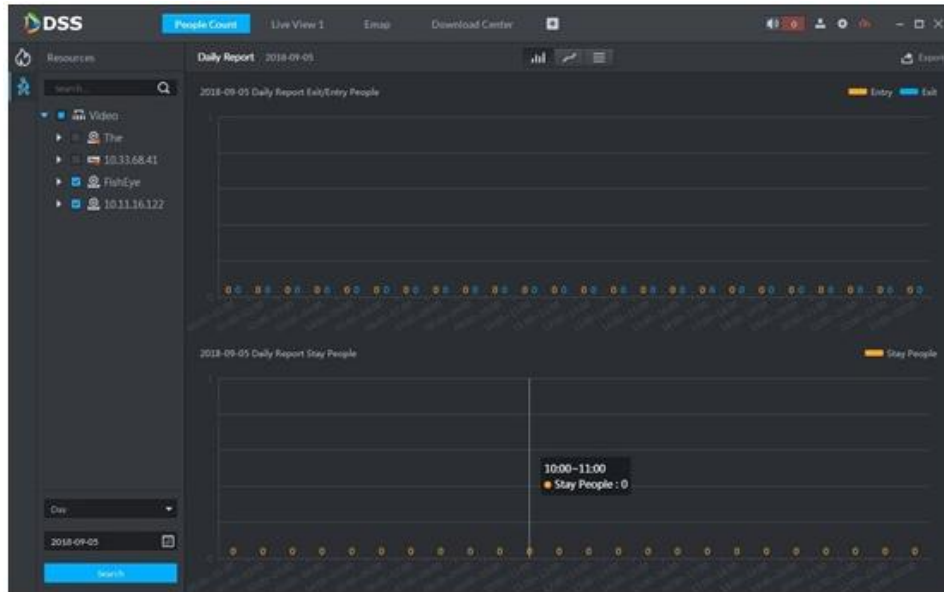
Step 2 Click  on the left and then select a channel, select the report type, statistics time, and then click Search. It is to search people counting report. See Figure 5-76.

Figure 5-76

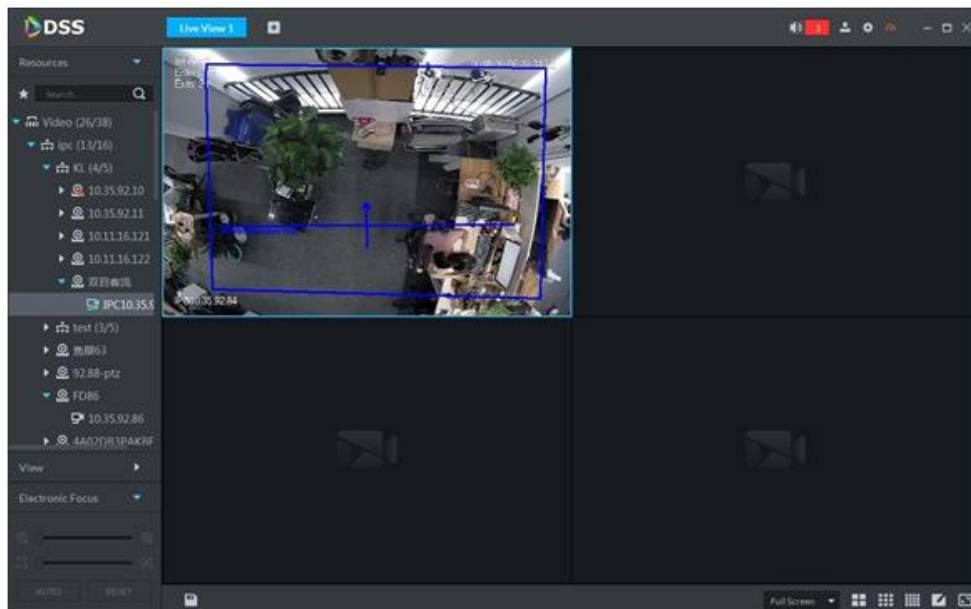


Or you can click  to view line chart, or list.

### 5.8.3 Viewing People Counting Statistics on Live View Interface

On Live View interface, you can view the video of the smart network camera, and view the statistics people amount at the top left corner. See Figure 5-77.

Figure 5-77



Entry/exit count is shown at the top left corner. See Figure 5-78.



Figure 5-78



## 5.8.4 Heatmap

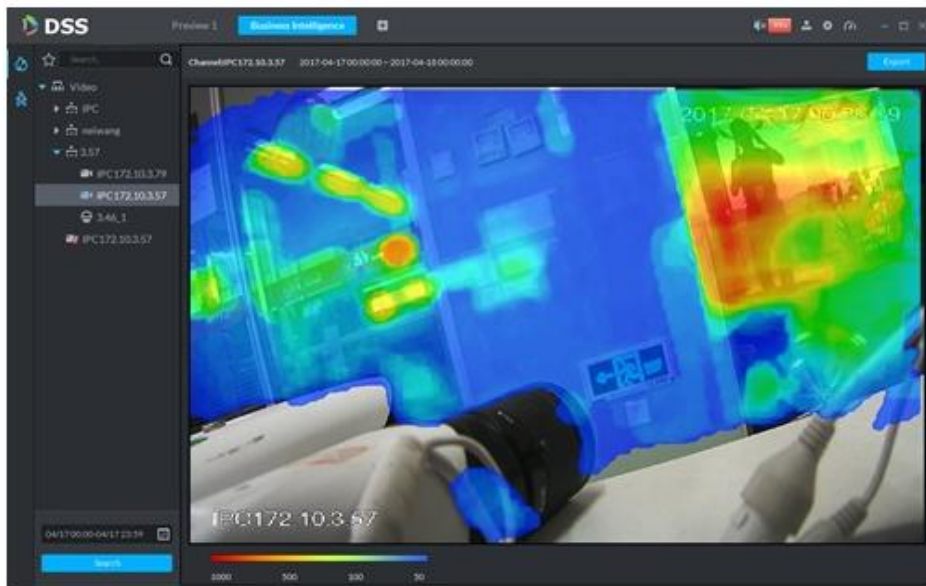
Step 1 Click  tab.

Step 2 Select a channel to show heat map, and select time, click Search  
System displays heatmap interface. See Figure 5-79.

### NOTE

The device sends heat map data to platform on a real-time basis. Starting when device is added to platform, you can search heat map data uploaded. Unit of search is week (interval between start time and end time cannot exceed 1 week).

Figure 5-79



Step 3 Click Export at the top right corner, you can export heat map in bmp format.

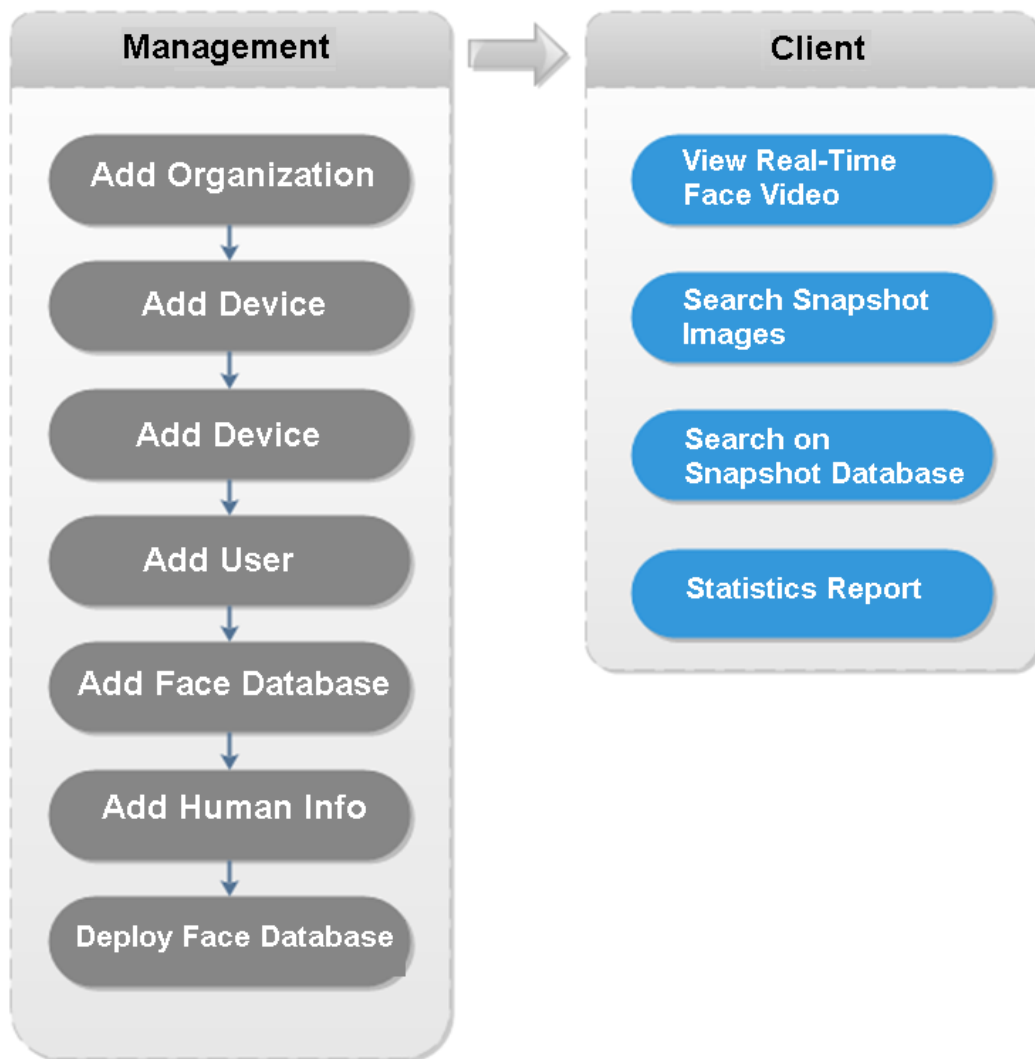
## 5.9 Human Face Recognition

### 5.9.1 Preparations

- Refer to chapter 4.11.1 Creating face database to create human face database on the manager.
- Refer to chapter 4.11.2 Configuring arm to arm human face database on the platform manager.


Refer to Figure 5-80 for flows information.

Figure 5-80



## 5.9.2 Real-Time Human Face Video

Human face recognition function is applied to real-time video and snapshot human face image.

**Step 1** Click , on the New tab interface select Face recognition.

**Step 2** Click .

System displays real-time video. See Figure 5-81.

Figure 5-81

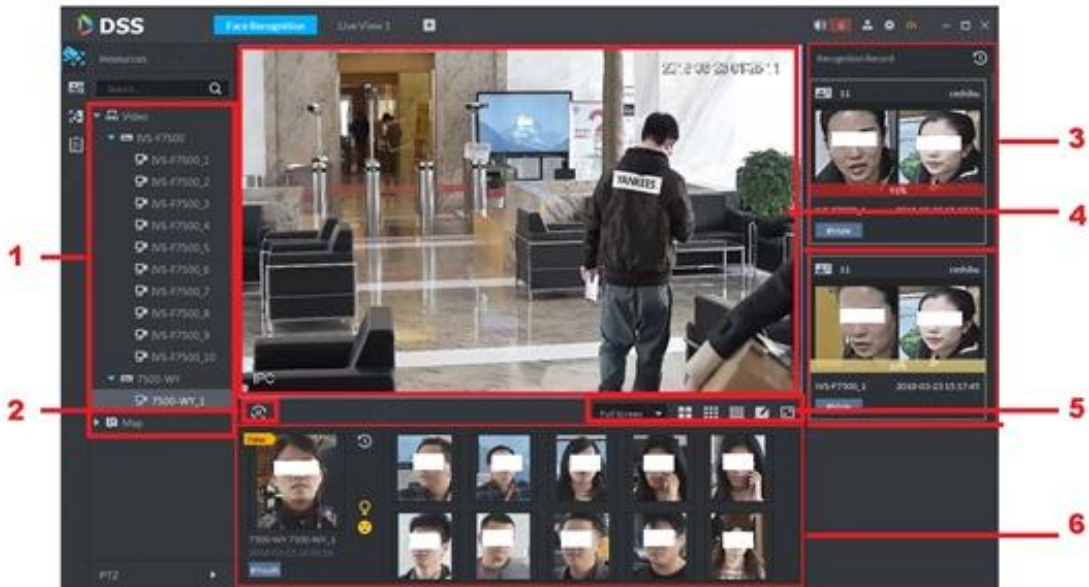


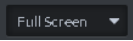




Table 5-19

SN	Name	Note
1	Device tree	It is to display device information.
2	Pause refresh/start refresh	<ul style="list-style-type: none"> <li>: When this icon is on the interface, the snapshot display pane does not refresh human face snapshot image. Click the icon, system displays real-time face image.</li> <li>: When this icon is on the interface, the snapshot display pane refresh human face snapshot image. Click the icon, system refreshes human face snapshot image.</li> </ul>
3	Recognition history record	It is to display the snapshot human face image of the video.
4	Monitor window	It is to display channel preview video. In multiple-window display mode, double click the window to switch to 1-window display mode. Double click the window again to restore original mode.
5	 Image display rate	<ul style="list-style-type: none"> <li>There are two modes: full screen, original scale. The full screen refers to one window at the full screen.</li> </ul>
	 Window split switch	It is to display switched window amount. System supports customized settings.
	 Full screen display	The system displays window at full screen.
6	Snapshot human face image display pane	It is to display snapshot human face image.

Step 3 Enable video preview.

- Select a monitor window (white frame means it is the checked window). Double click a channel or record file to enable real-time surveillance.
  - Drag the channel or the video file to the monitor window.
- It is to enable video preview interface. See Figure 5-82.

Figure 5-82



**Step 4** Double click snapshot human image.

System displays human detailed information interface.

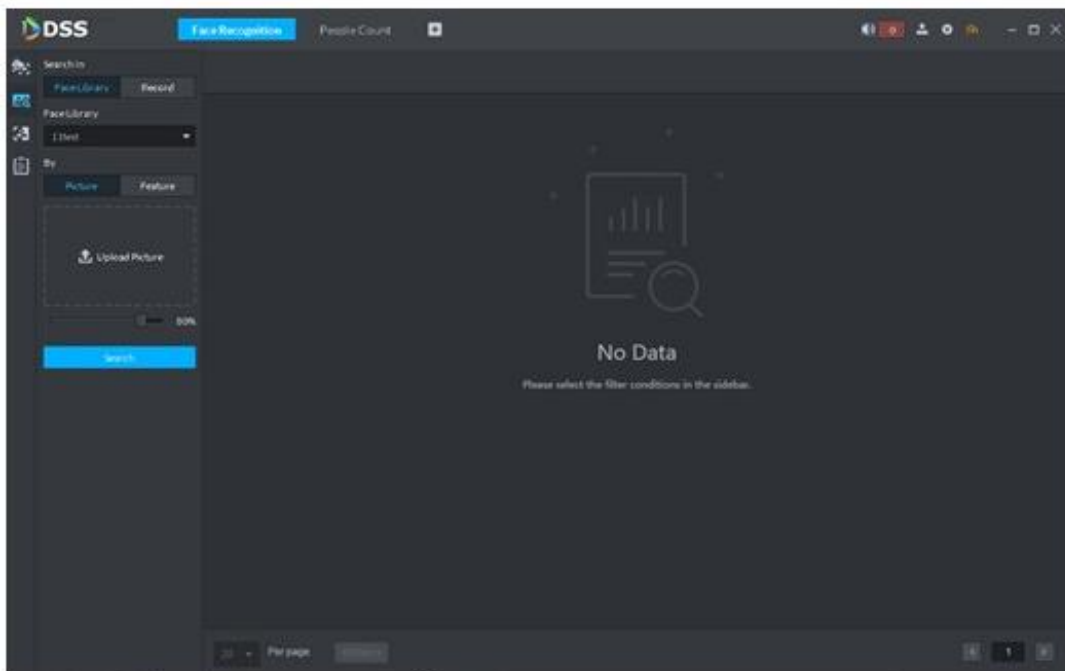
### 5.9.3 Searching Snapshot Images

The human face recognition function can search the specified person from the human face database or the snapshot image database. Or you can use the image to search the corresponding person.

**Step 1** On the Face recognition interface, click .

Enter Search face library interface. See Figure 5-83.

Figure 5-83



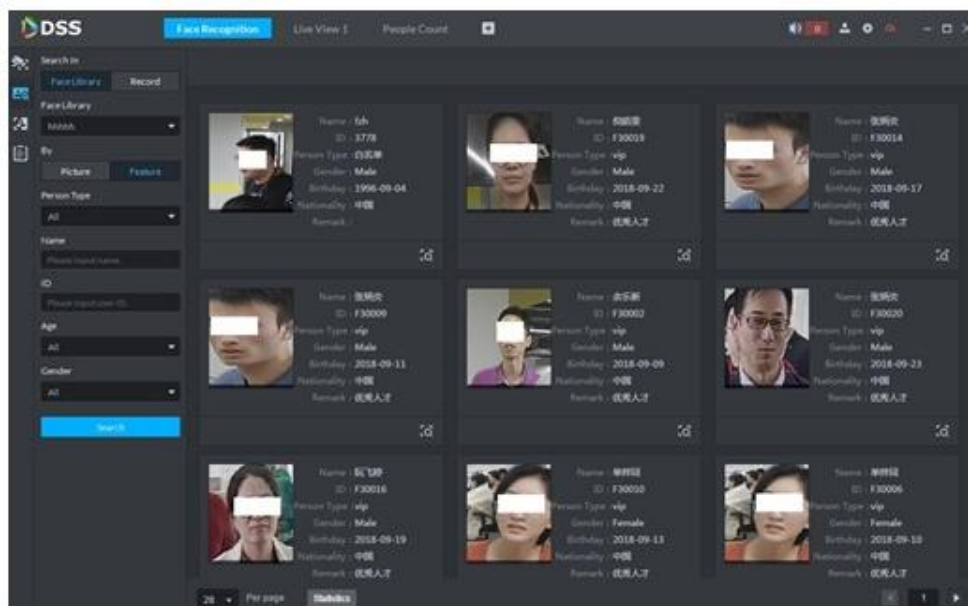
**Step 2** Set search criteria.

- You can search on human face database or records.
- Select a human face database already exists.
- The search criteria can be Picture or Feature.

**Step 3** Click Search.


The search interface is displayed. See Figure 5-84.

Figure 5-84



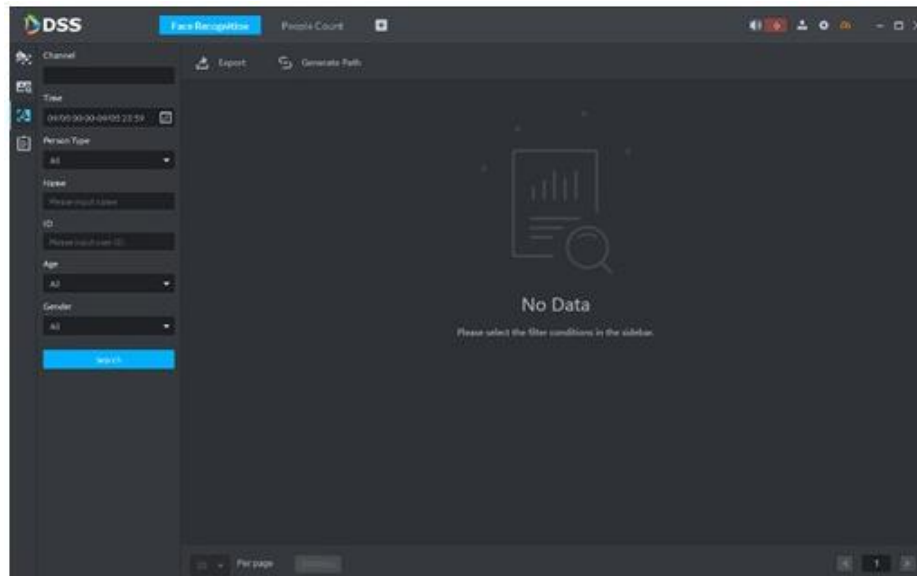
## 5.9.4 Searching on the Snapshot Database

The human face recognition function can search images of specified period or search the image on the image database.

Step 1 On Face recognition interface, click .

The snapshot database search interface is displayed. See Figure 5-85.

Figure 5-85



Step 2 Set search criteria.

System supports search by channel, time, human face features, name, ID, age, gender, etc.

Step 3 Click Search.

Step 4 Double click the search result

System displays human information. See Figure 5-86. There is no image on the left if you do not upload image when setting search criteria. Refer to Table 5-20 for detailed operation information.



Figure 5-86

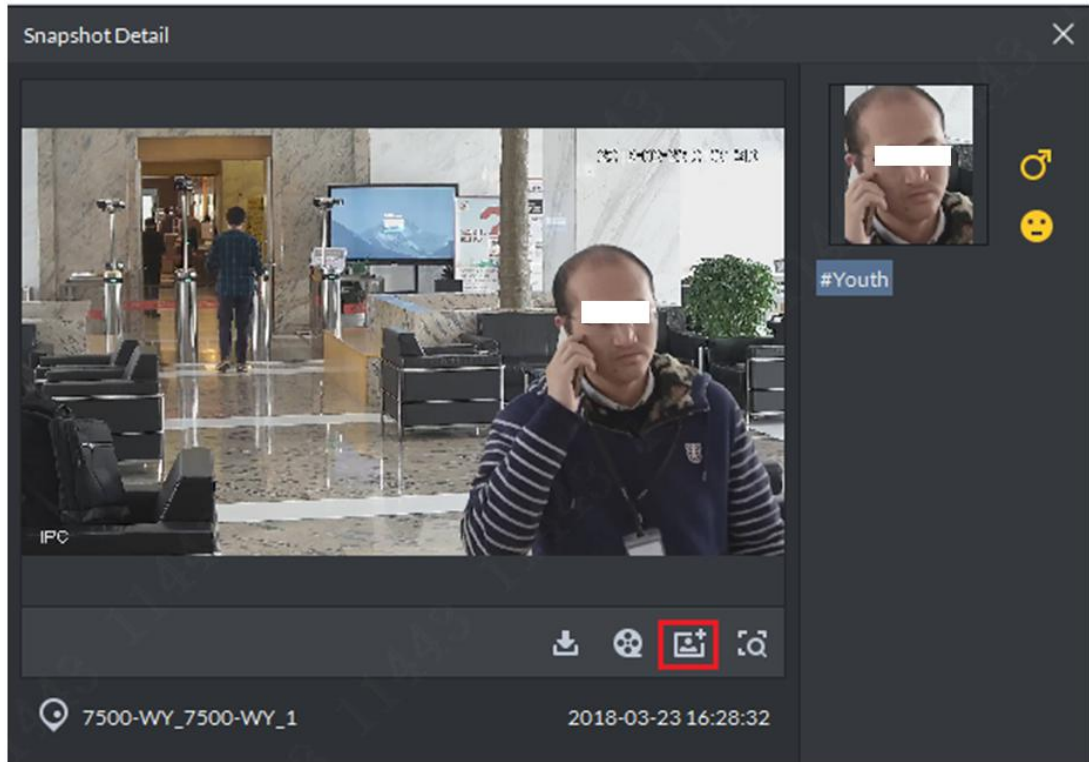






Table 5-20

Operation	Note
Download Record	Click  , it is to save RAR file on the specified path. The .RAR file contains the human face snapshot image and snapshot panorama images.
Playback record	Click  to playback the 15-seconds video record before and after the snapshot.
Add person	It is to add the snapshot person to the database. 1. Click  , system displays View interface. 2. Set person information and then click OK.
Search record	You can use the snapshot image to search on the registration database. 1. Click  , system goes to human face search interface with the snapshot image. 3. Click Search, system displays search result.

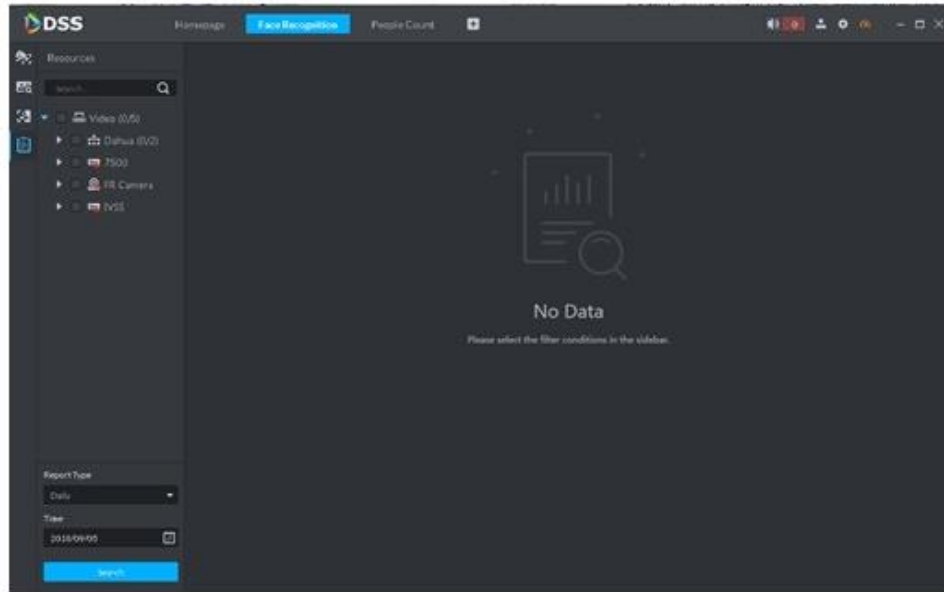
## 5.9.5 Statistics Report

Step 1 On Face recognition interface, click .

Enter Registration database search interface. See Figure 5-87.



Figure 5-87



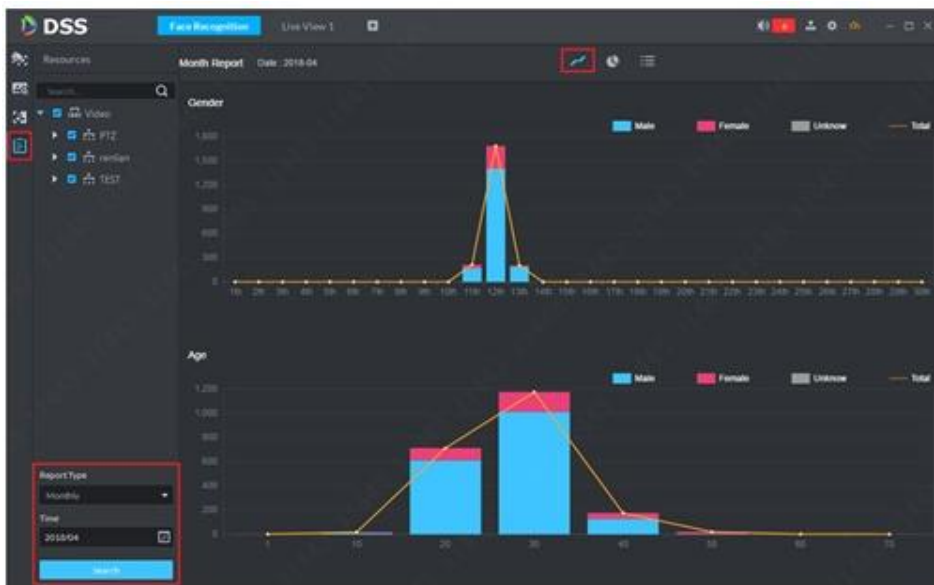
**Step 2** Set search criteria.



Set video channel, report type and time.

**Step 3** Click Search.

The statistics search result is displayed. See Figure 5-88.

Figure 5-88



- System displays results by line chart.
- Click  to display by pie chart.
- Click  to display by list.
- Click Export, it is to export statistics result to .pdf file.

## 5.10 License Plate Recognition

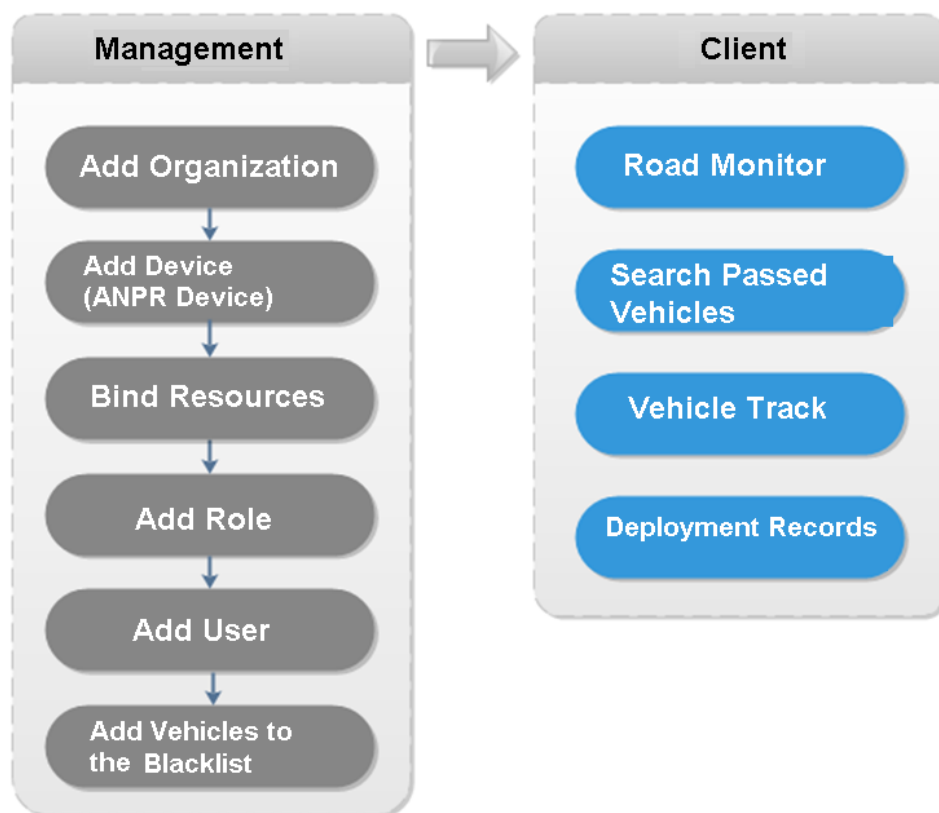
The platform integrates vehicle module. It can search passed vehicles and search violation records and alarm.

### 5.10.1 Preparations

- Refer to chapter 4.6 Adding device to add ANR device on the platform manager.
- Refer to chapter 4.12 Adding vehicle blacklist to add vehicle blacklist on the platform manager.


Refer to Figure 5-89 for flows of license plate recognition.

Figure 5-89



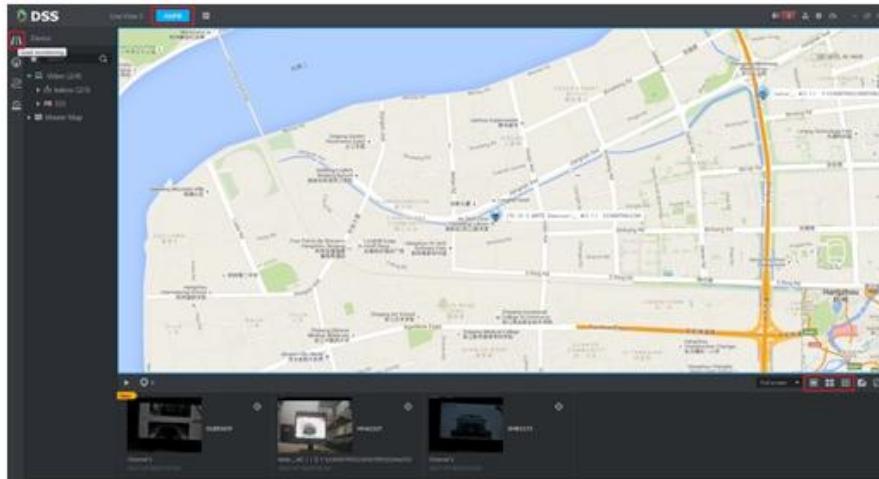
### 5.10.2 Road Monitor


**Step 1** Click , on the New tab interface select ANPR.

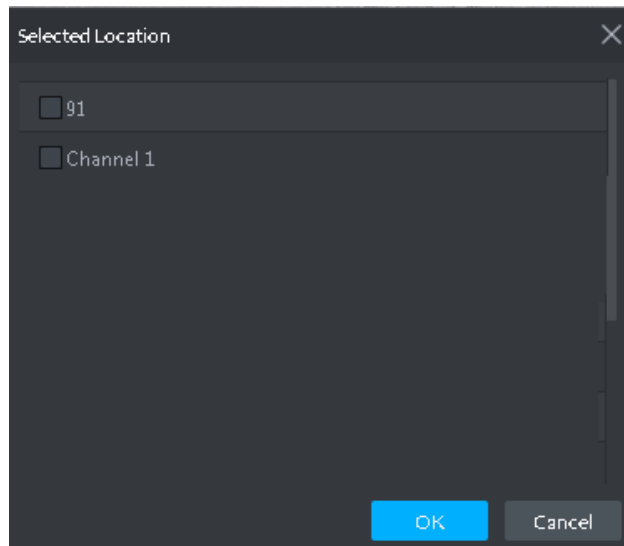
**Step 2** Click , system displays road monitor interface.

System displays emap in 1-window by default. You can manually switch window amount. See Figure 5-90.

Figure 5-90

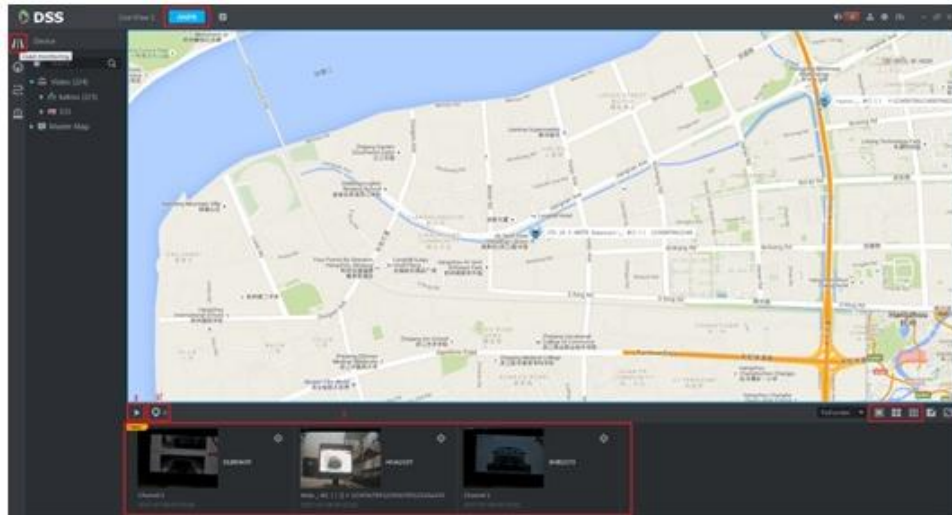


**Step 3** Click  to select the ANPR channel. See Figure 5-91.  
Figure 5-91



**Step 4** Select ANPR device and then click OK.  
System displays the selected channel amount and the latest passing vehicle image on the rolling pane. See Figure 5-92.


Figure 5-92



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

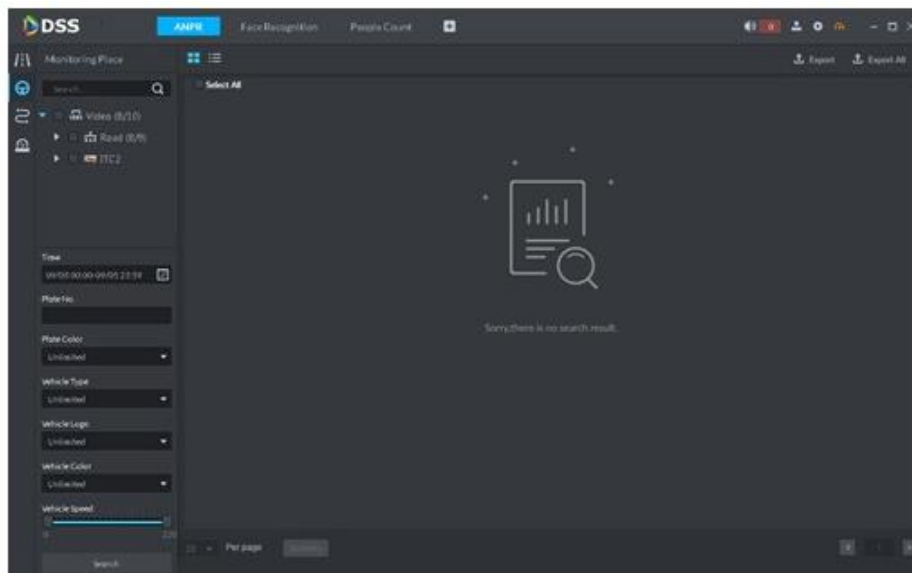
### 5.10.3 Searching Passed Vehicle

It is to search passing vehicle.

**Step 1** Click .

Enter Passed vehicle interface. See Figure 5-93.

Figure 5-93

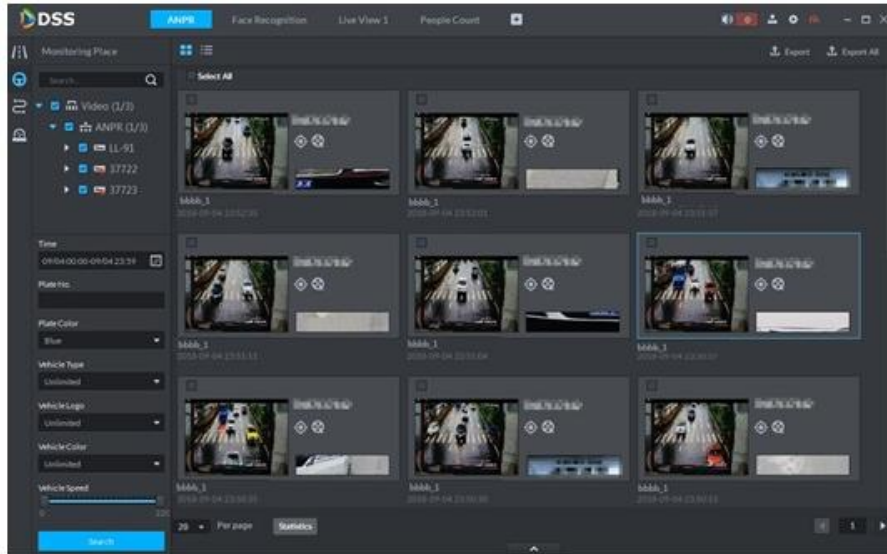


**Step 2** Select video channel and search criteria. It includes time, plate number, plate color, plate type, vehicle logo, vehicle body color and lane.

**Step 3** Click Search.

System displays search result. See Figure 5-94.

Figure 5-94



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 5-95. Move the cursor to the middle to select the specified zone, you can zoom in it. See Figure 5-96.

Figure 5-95

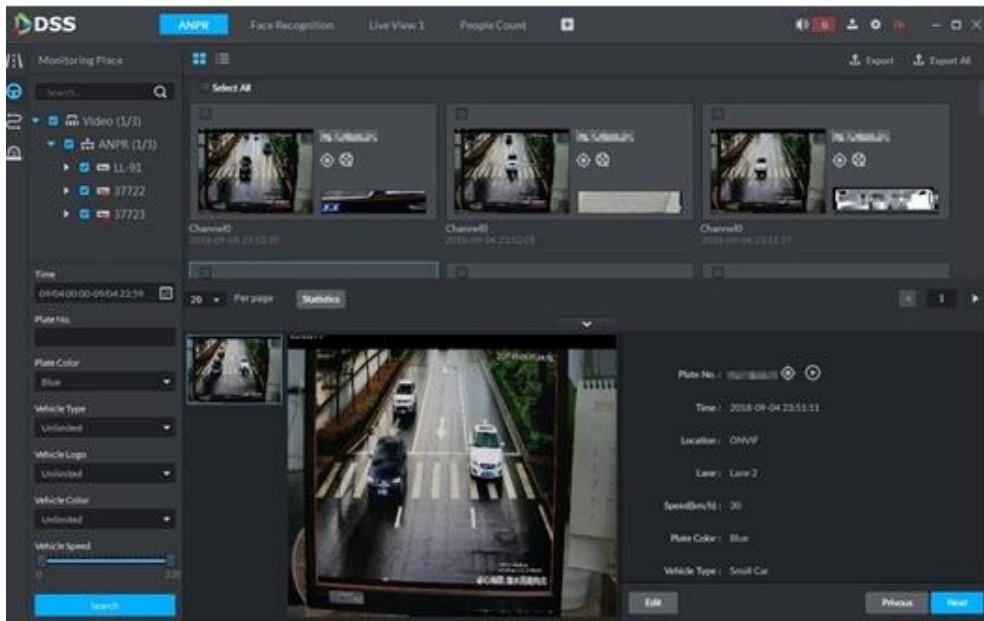
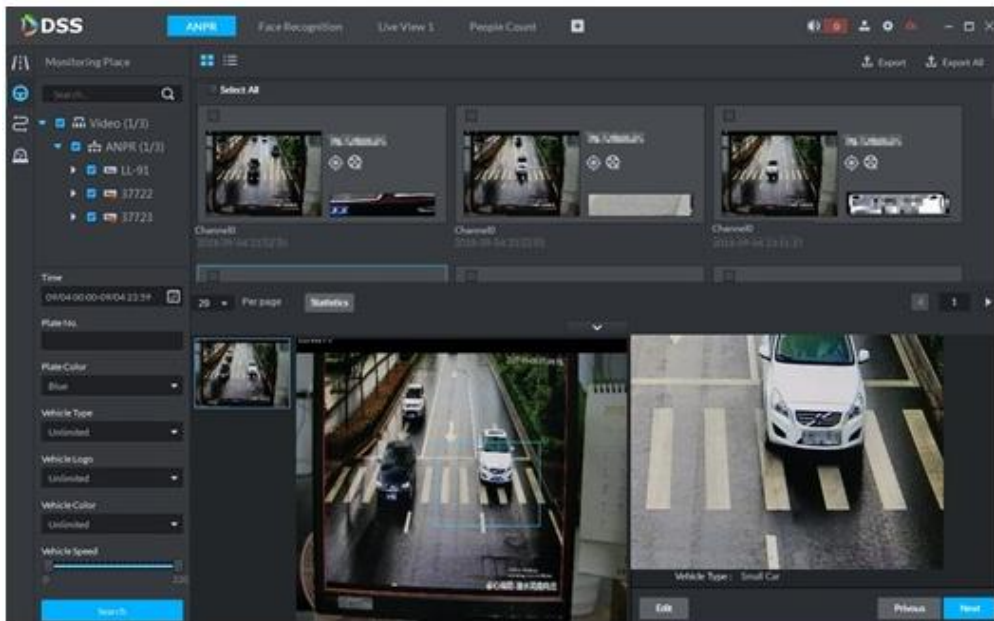


Figure 5-96




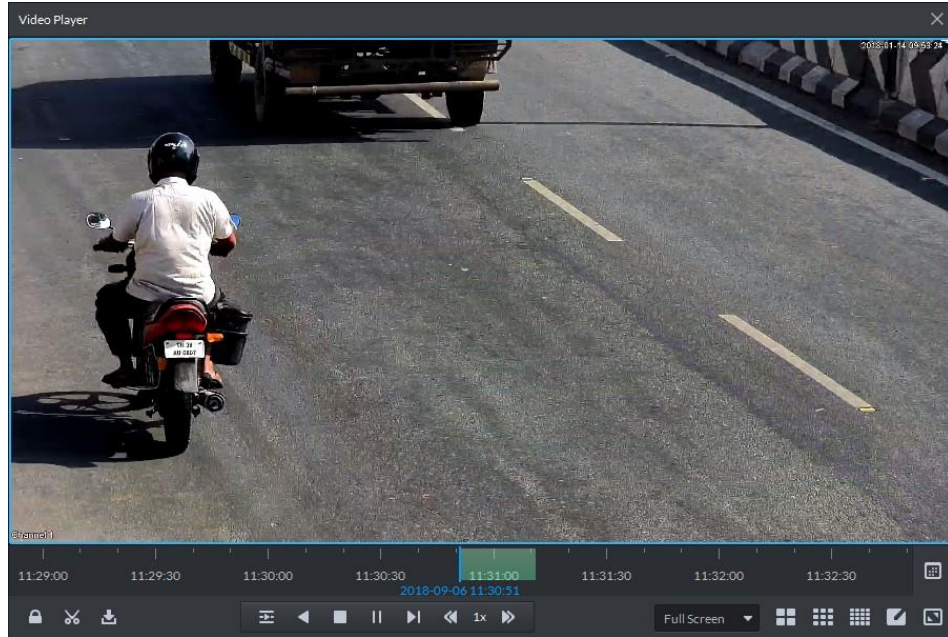

- Click  to playback the 15-second video before and after the vehicle passed time. See Figure 5-97. The video file is total 30 seconds. It is to display the 15-second video before and after the vehicle passed.

Figure 5-97



- Click  to view the vehicle running track. Refer to chapter 5.10.4 Vehicle Track for detailed information.
- Export: Select the passed vehicle information and then click Export. It is to export selected passed vehicle. Click Export all, it is to export all searched passed vehicle information.

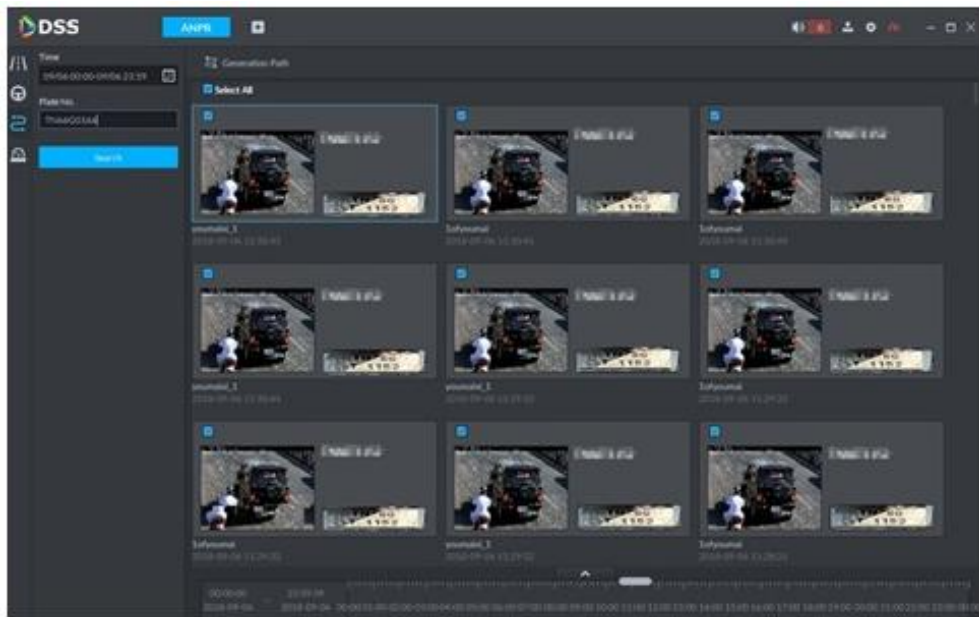
## 5.10.4 Vehicle Track

Step 1 Click , system displays Road monitor interface.

Step 2 Select time and then input plate number. Click Search.  
Enter Vehicle track search result. See Figure 5-98.



Figure 5-98



Refer to the operations listed below.


- Select the snapshot image and then click  or double click the image, you can view snapshot vehicle detailed information. See Figure 5-99. Move the cursor to the middle to select the specified zone, you can zoom in it. See Figure 5-100.



Figure 5-99

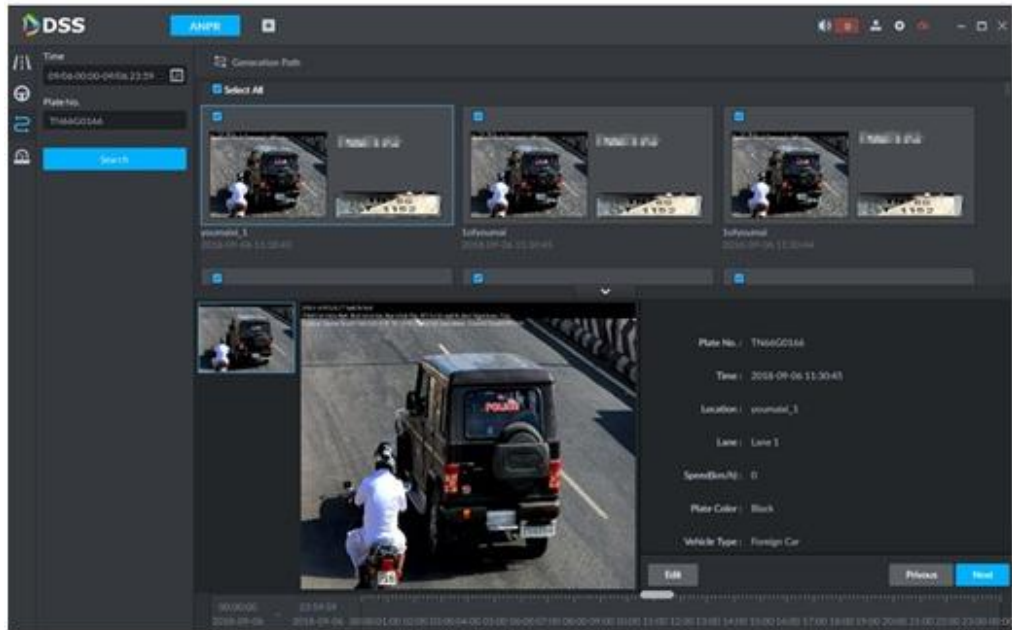
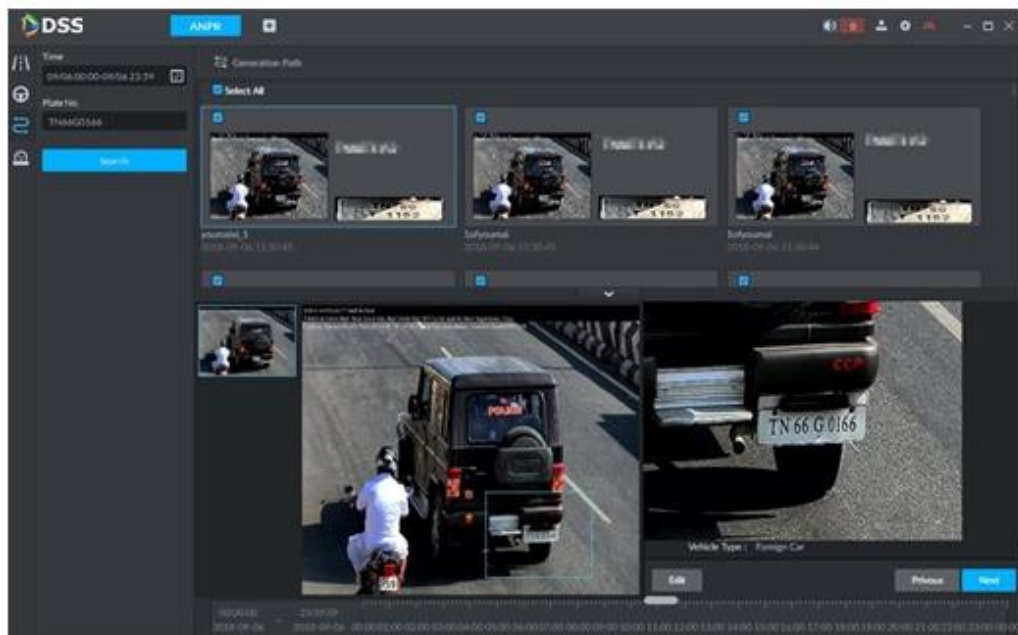
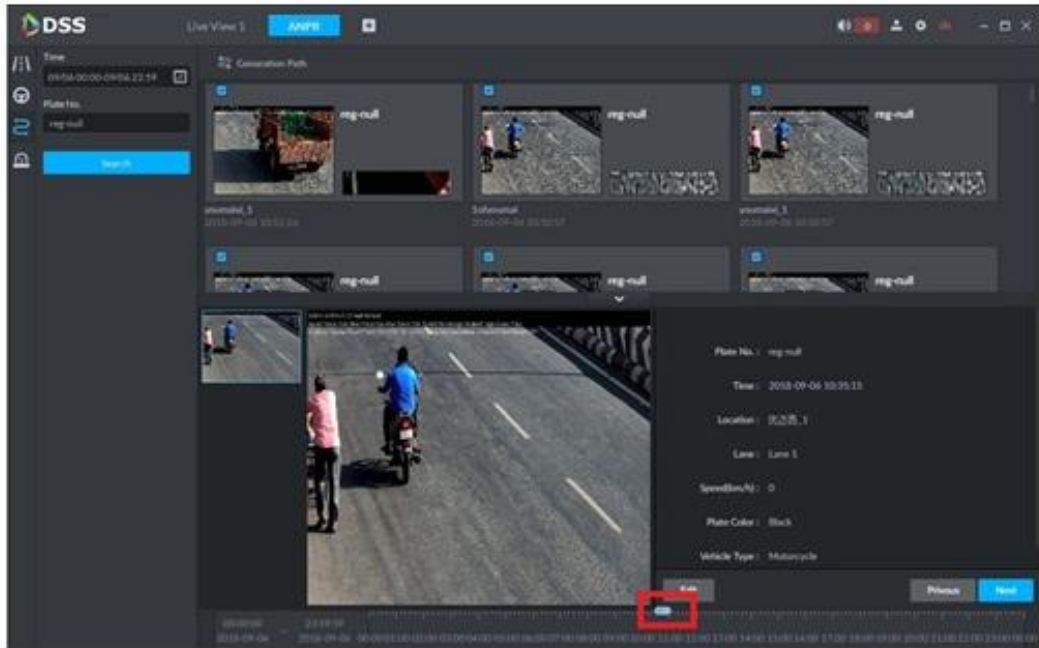


Figure 5-100



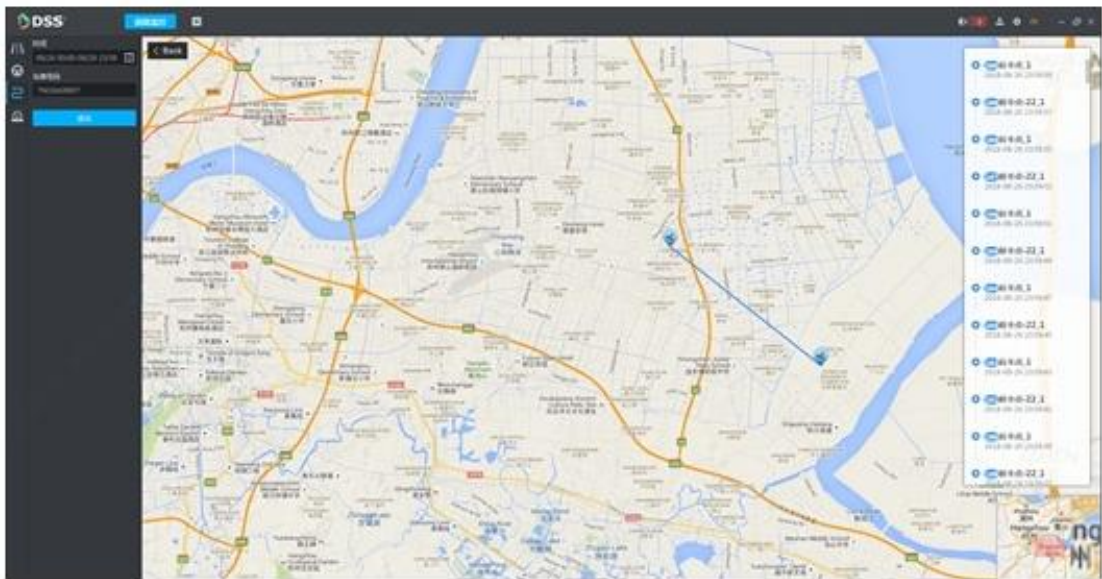
- Click Edit, it is to edit vehicle basic information.
- Click Previous or Next to view the previous or the next search item.
- Click the timeline that has the records, you can view the vehicle information of the specified time. See Figure 5-101.

Figure 5-101




- Select the snapshot image and then click the Generation path (track), you can view the vehicle track on the map. See Figure 5-102.

Figure 5-102



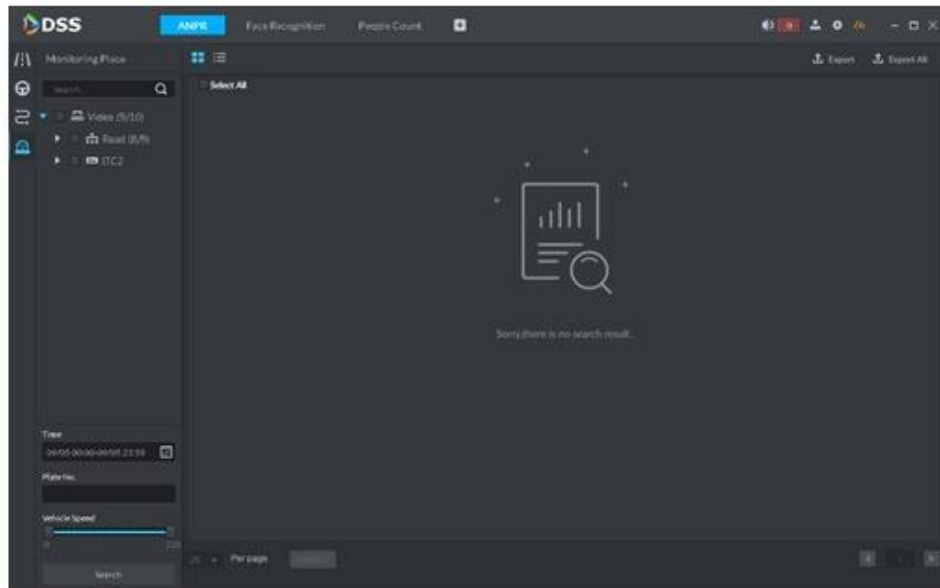
## 5.10.5 Monitor Place

It is to view and confirm the alarm information.

Step 1 Click .

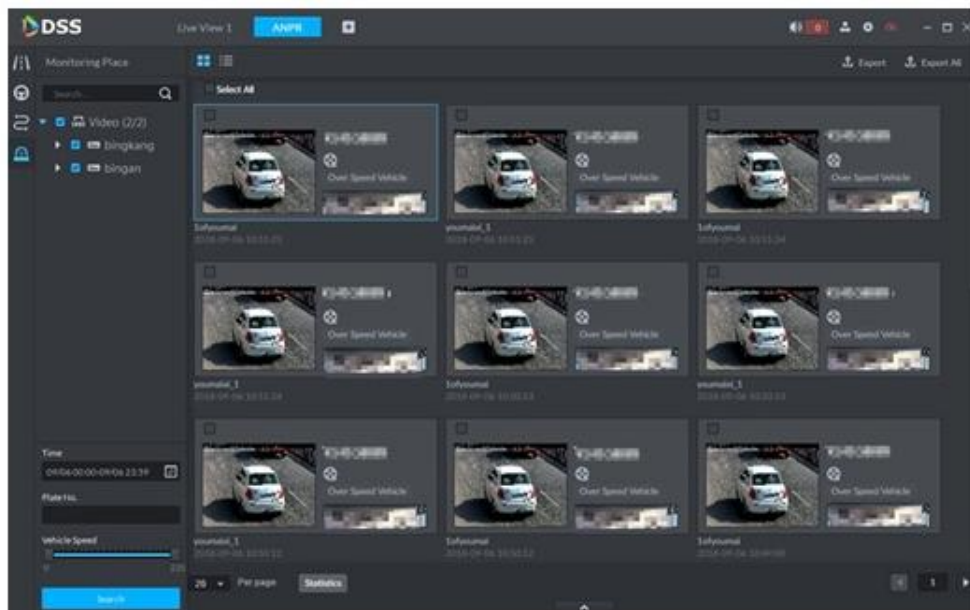
Enter Monitor place interface. See Figure 5-103.

Figure 5-103



**Step 2** Select device channel, and then set time, plate number, speed. Click Search. System displays search result. See Figure 5-104.

Figure 5-104



For the monitor record, you can view vehicle detailed information, corresponding video, edit vehicle information. Refer to the operations listed below.




- Click View mode (  ) or List mode (  ), it is to select different display mode.
- Select the snapshot image and then click  or double click the image, you can view snapshot vehicle detailed information. See Figure 5-105. Move the cursor to the middle to select the specified zone, you can zoom in it. See Figure 5-100.

Figure 5-105

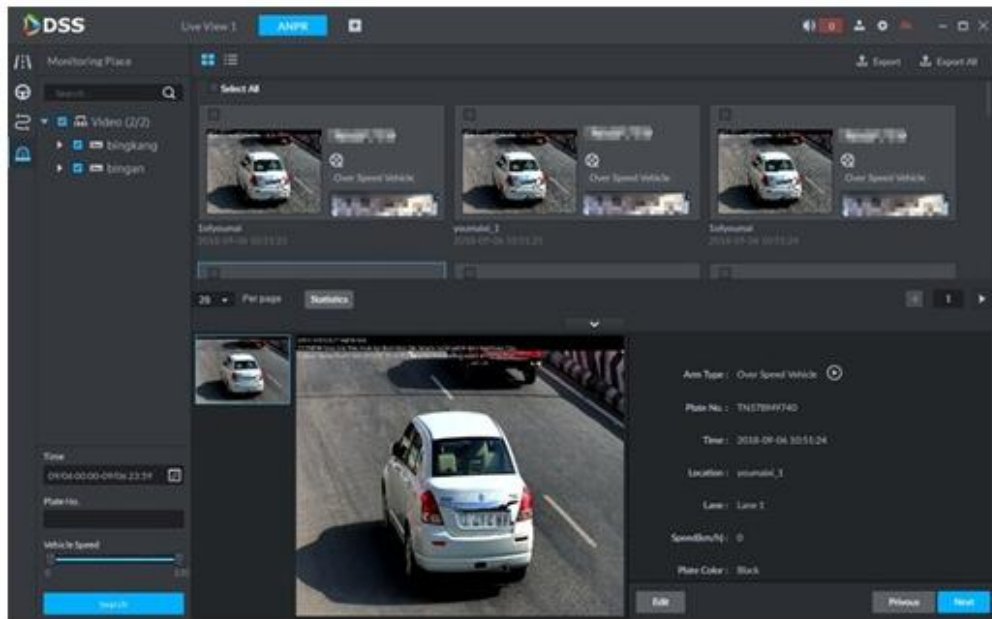
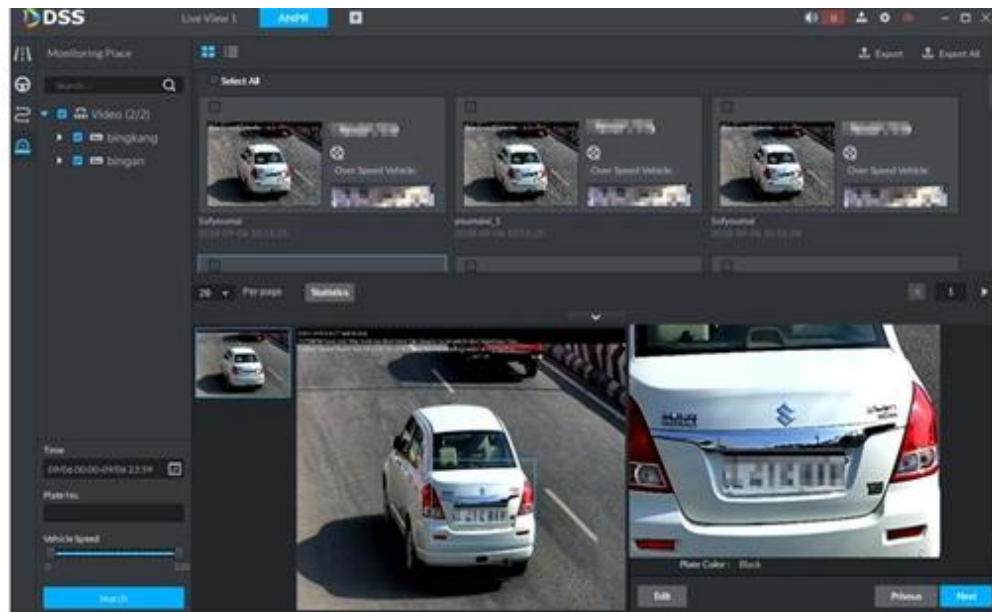


Figure 5-106




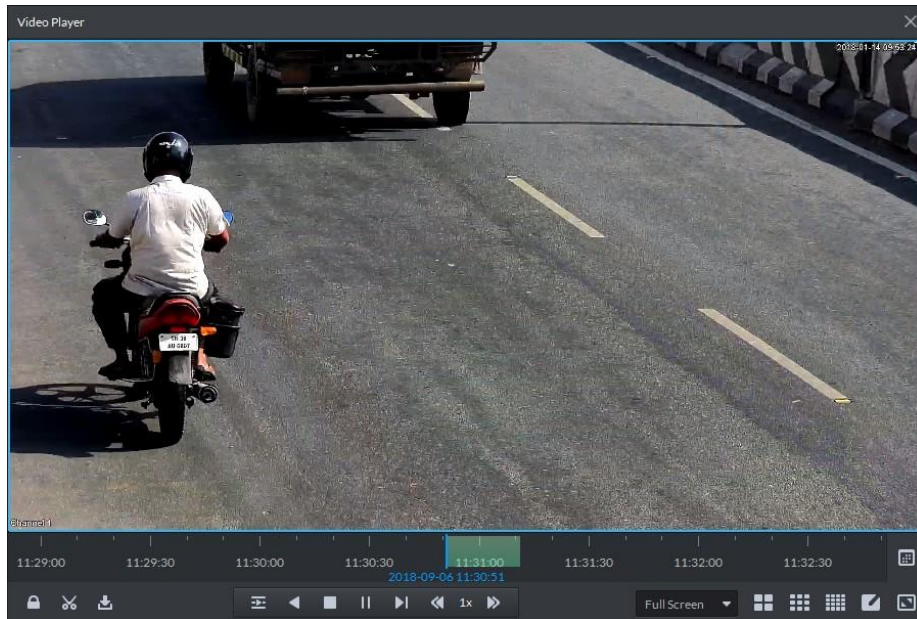

- Click  to playback the 15-second video before and after the vehicle passed time. See Figure 5-107. The video file is total 30 seconds. It is to display the 15-second video before and after the vehicle passed.



Figure 5-107



- Click  to view the vehicle running track. Refer to chapter 5.10.4 Vehicle Track for detailed information.
- Export: Select the passed vehicle information and then click Export. It is to export selected monitor position information. Click Export all, it is to export all monitor position information.

## 5.11 Time Synchronization

### 5.11.1 Device Time Synchronization

Device time synchronization is to synchronize front-end device time with platform server. The platform server time is the basic time. DSS platform supports devices of Dahua, and ONVIF protocol to synchronize time. It supports auto time synchronization function and manual time synchronization function. The auto time synchronization refers to synchronize time with the server at the specified interval and time. Manual time synchronization is to start time synchronization manually, system responds immediately and then execute time synchronization.

#### 5.11.1.1 Auto Sync Time

Step 1 Click  and then on the New tab interface select System settings.

Step 2 Click Time Sync and then check the box to enable the function. Set time synchronization parameters. See Figure 5-108.

Figure 5-108

Time Sync

Enable

Start Time: \* 00:00:00

Sync Interval: \* 24

Hour: Immediately

**Step 3** Click Save to save configuration information.

### 5.11.1.2 Manual Sync Time

**Step 1** Click  and then on the New tab interface select System settings.

**Step 2** Click Immediately box. See Figure 5-109.

Figure 5-109

Time Sync

Enable

Start Time: \* 00:00:00

Sync Interval: \* 24


Hour: Immediately

## 5.11.2 Time Synchronization on the Client

Time synchronization on the client is to synchronize client installed PC's time with platform server. The platform server time is the basic time. It supports auto time synchronization function and manual time synchronization function. The auto time synchronization refers to server starts time synchronization at the specified interval and time. Manual time synchronization is to start time synchronization manually, system responds immediately and then execute time synchronization.

### 5.11.2.1 Auto Sync Time

**Step 1** Login DSS client.

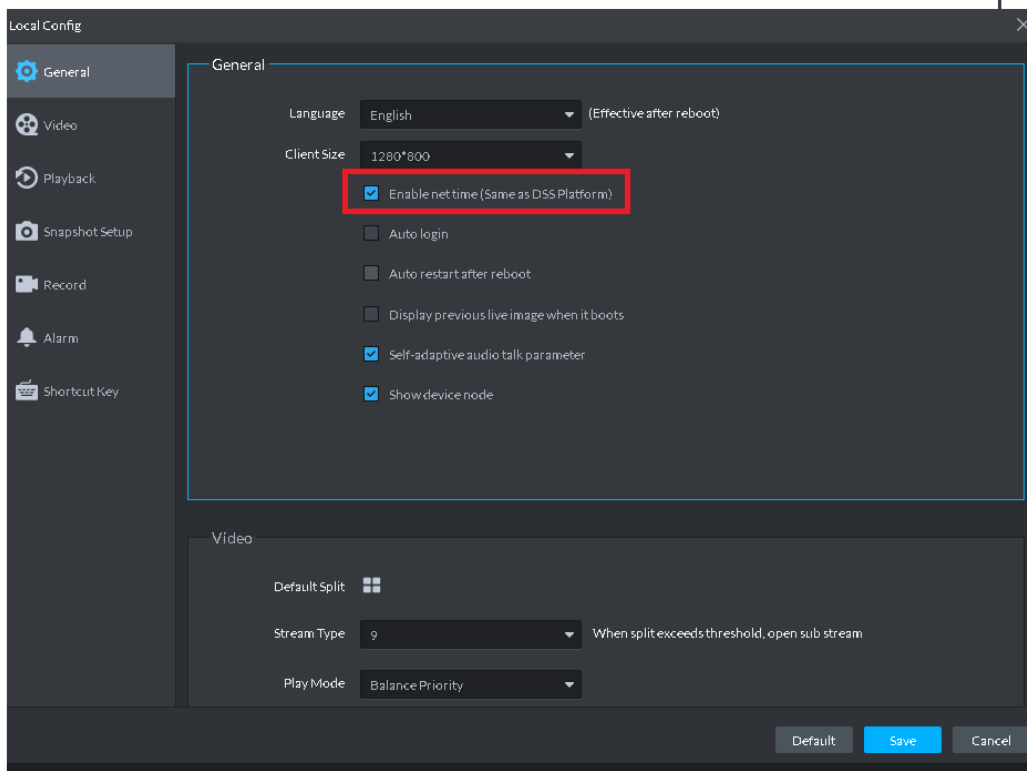
**Step 2** Click  at the top right corner. Enter Local config interface.

**Step 3** Click General tab and then enable client time sync function. Click Save. See Figure 5-110.

#### NOTE

After you enabled time sync function on the General interface, client begins the request to the server immediately. It is to complete the time synchronization.

Figure 5-110

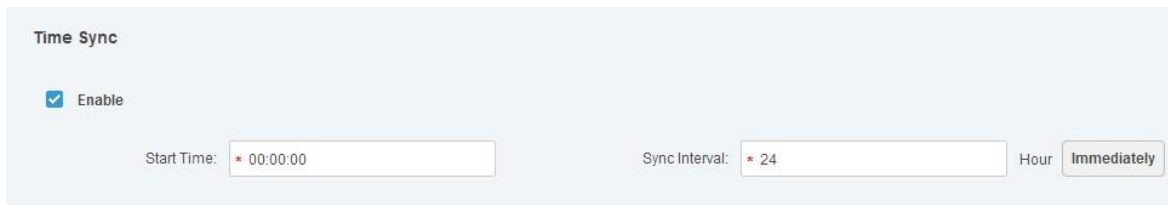


**Step 4** Click Save.

**Step 5** Login DSS manager, and then on the New tab interface select System settings.

**Step 6** Click Time sync and then check the box to enable the function. See time sync parameters. See Figure 5-111.


Figure 5-111



**Step 7** Click Save to save configuration information.

### 5.11.2.2 Manual Time Sync

**Step 1** Login DSS client.

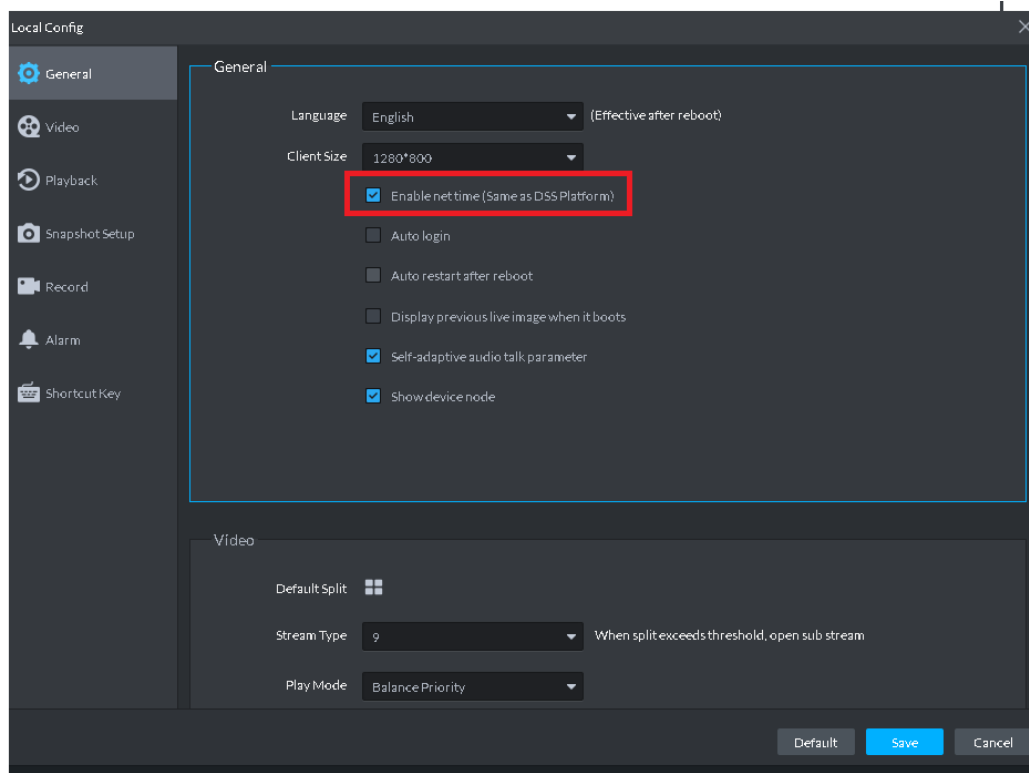
**Step 2** Click  at the top right corner. Enter Local config interface.

**Step 3** Click General tab and then enable client time sync function. Click Save. See Figure 5-112.

#### **NOTE**

After you enabled time sync function on the General interface, client begins the request to the server immediately. It is to complete the time synchronization.

Figure 5-112

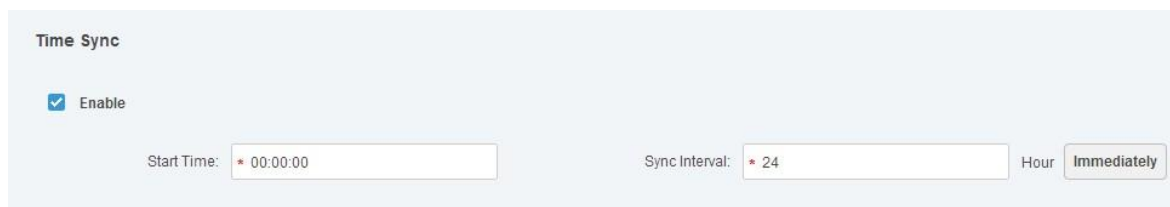


**Step 4** Click Save.

**Step 5** Login DSS manager, and then on the New tab interface select System settings.

**Step 6** Click Immediately box. See Figure 5-113.

Figure 5-113





## Appendix 1 Service Module Introduction

Service Name	Service Name	Function Description	Port	Protocol Type
Center Management Service	DSS_WEB	Center management service is to manage each service and provide accessing port.	HTTPS: 443	TCP
Message Queue Service	DSS_MQ	Message queue service is to transfer messages between the platforms.	61616	TCP
DMS (Device Management Service)	DSS_DMS	Device management service is to register front-end encoder, receive alarm, transfer alarm and send out sync time command.	9200	TCP
MTS (Media Transmission Service )	DSS_MTS	Media transmission service is to get the audio/video bit stream from the front-end device and then transfer these data to the SS, client and decoder.	9100	TCP
SS (Storage Service)	DSS_SS	Storage service is to storage/search/playback record.	9320	TCP
VMS (Video Matrix Service)	DSS_VMS	Video matrix service is to login the the decoder and send out task to the decoder to output to the TV wall.	Not fixed, do not need to be mapped to the outside.	TCP
MGW (Media Gateway Service)	DSS_MGW	Media gateway service is to send out MTS service to the decoder.	9090	TCP
ARS (Auto Register Service)	DSS_ARS	Auto register service is to listen, login, or get bit streams to send to MTS.	9500	TCP
PCPS (ProxyList control Proxy Service)	DSS_PCPS	ProxyList control Proxy Service is to login Hikvision device, Onvif device, and then get the stream and transfer the data to MTS.	5060 14509	UDP TCP

ADS (Alarm Dispatch Service)	DSS_ADS	Alarm dispatch service is to send out alarm information to different objects according to the plans.	9600	TCP
------------------------------------	---------	---	------	-----