General Surveillance Management Center

User’s Manual

V 1.0.1

Foreword

General

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

Safety Instructions

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

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

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	Version Number	Revision Content	Release Time

No.	Version	Version Number	Revision Content	Release Time
1	V1.0.0	-	First release	September 2018
2	V1.0.1	V1.001.0000000	● Added new functions such as RAID group config, personnel management, access control management, thermal, target detection, device config, entrance, attendance management and video intercom. ● Modified contents such as edit device, flow analysis, plate recognition. ● Deleted business function.	April 2019

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 dissemble 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

1 Overview

1.1 Introduction

DSS general surveillance management center (Hereinafter referred to as “DSS Platform”) is a type of video surveillance platform which is flexible, easily-extendable, highly-reliable and more professional. DSS platform is able to meet the requirements of large and medium-sized projects by distributed extension and cascade performance.

In addition to basic video surveillance business, DSS platform supports target detection and a series of AI functions, such as face recognition, license plate recognition and people counting. It can also expand functions like transportation, access control via value-added modules. These rich functions enable DSS platform to be widely used in chain supermarket, safe city, road traffic, medium and large-sized campus surveillance and some other scenarios.

1.2 Highlights

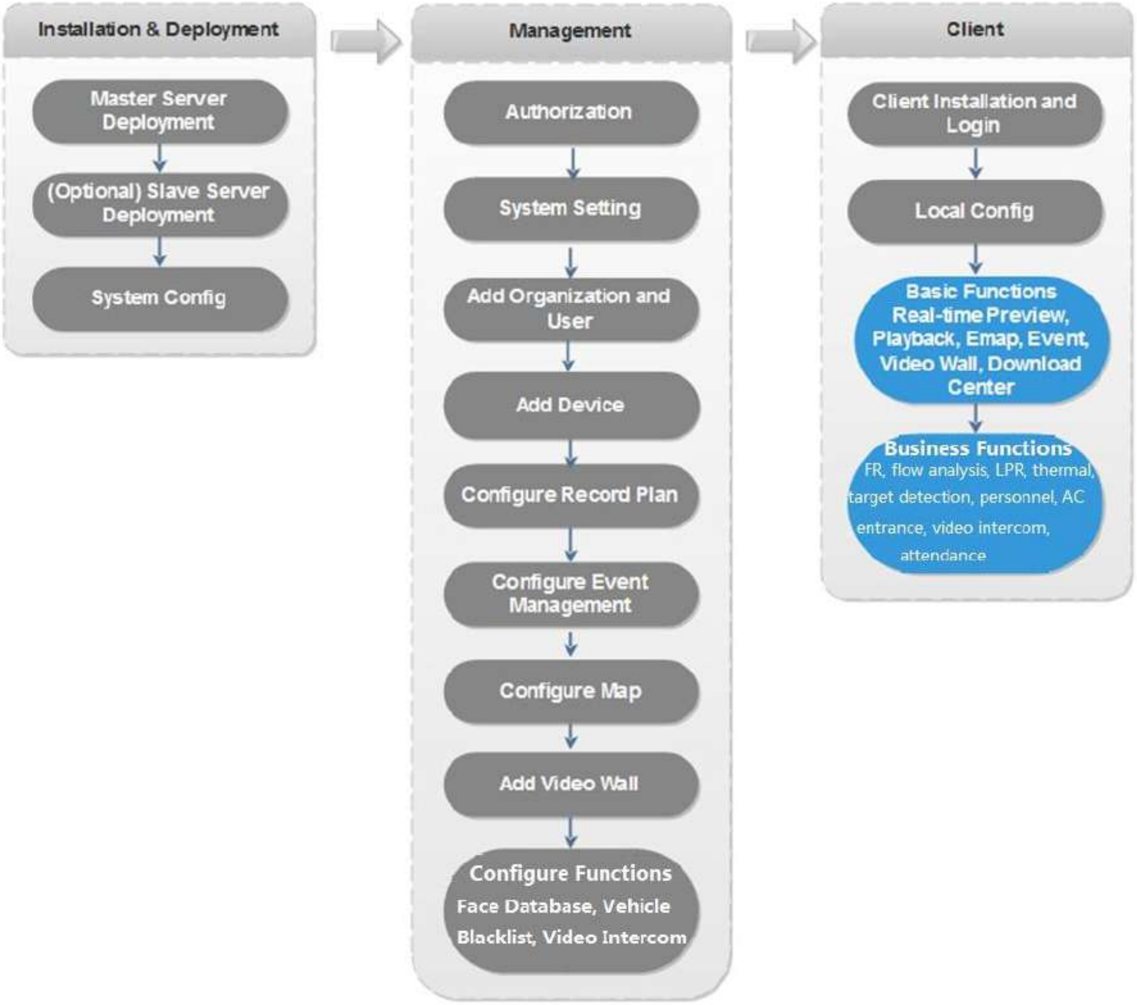
- Easily extendable
  - ◇ Supports extension system performance.
  - ◇ Supports cascading extension system performance.
  - ◇ Supports extending more dedicated function modules.
- More professional
  - ◇ Supports system operation and maintenance, easily acquire service, system, device, time and some other system info.
  - ◇ Separate Web manager; make management more convenient and professional.
  - ◇ Supports target detection, face recognition, plate recognition, people counting and other AI functions, access control, retail and transportation functions make DSS platform more powerful.
- Highly reliable
  - ◇ Supports dual hot standby, makes DSS platform system more stable.
  - ◇ Supports system data auto backup and manual backup, reduce loss caused by system crash.
- More open
  - ◇ Supports access over standard Onvif protocol and active registration.
  - ◇ 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 Flow chart


Installation & Deployment
Master Server Deployment
(Optional) Slave Server Deployment
System Config
Management
Authorization
System Setting
Add Organization and User
Add Device
Configure Record Plan
Configure Event Management
Configure Map
Add Video Wall
Configure Functions
Face Database, Vehicle Blacklist, Video Intercom
Client
Client Installation and Login
Local Config
Basic Functions
Real-time Preview, Playback, Emap, Event, Video Wall, Download Center
Business Functions
FR, flow analysis, LPR, thermal, target detection, personnel, AC entrance, video intercom, attendance

3 Configuring System Basic Info

The config system is used to quickly configure network parameters, basic parameters, safety parameters and hot standby. 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.

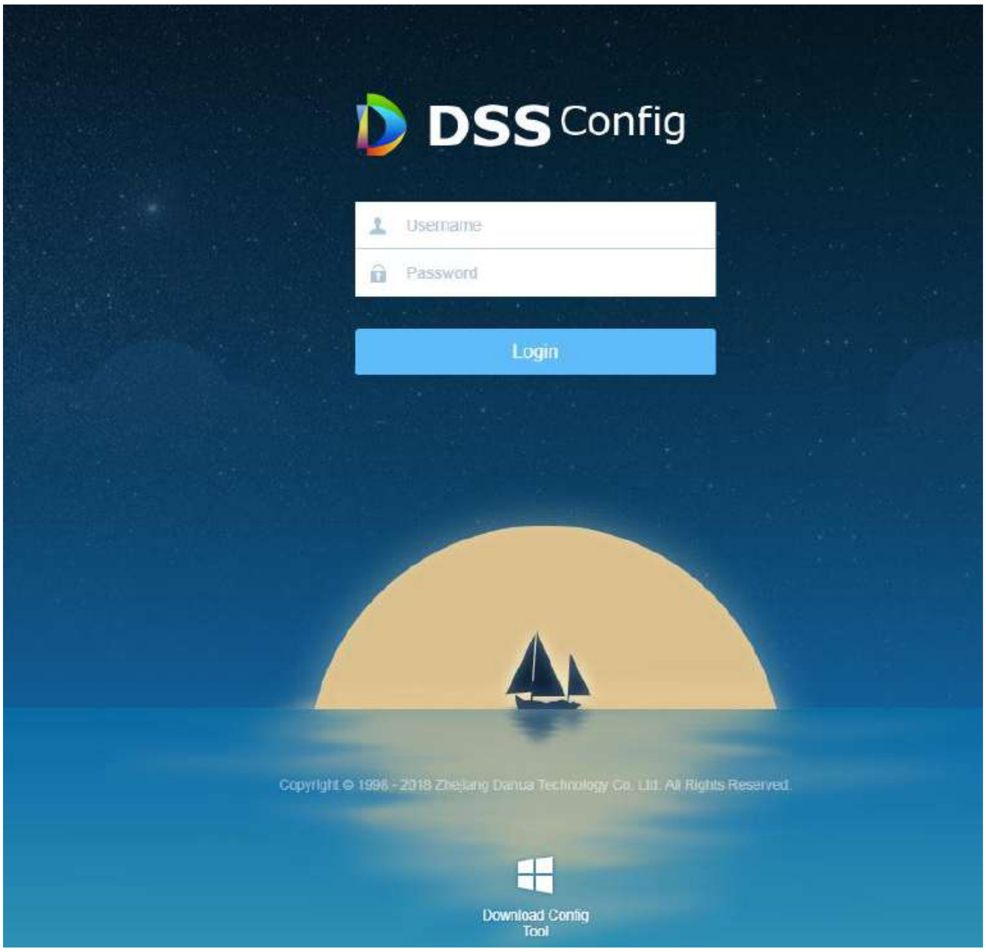
3.1 Login and Password Initialization

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

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

The **Config System** interface is displayed. See Figure 3-1.

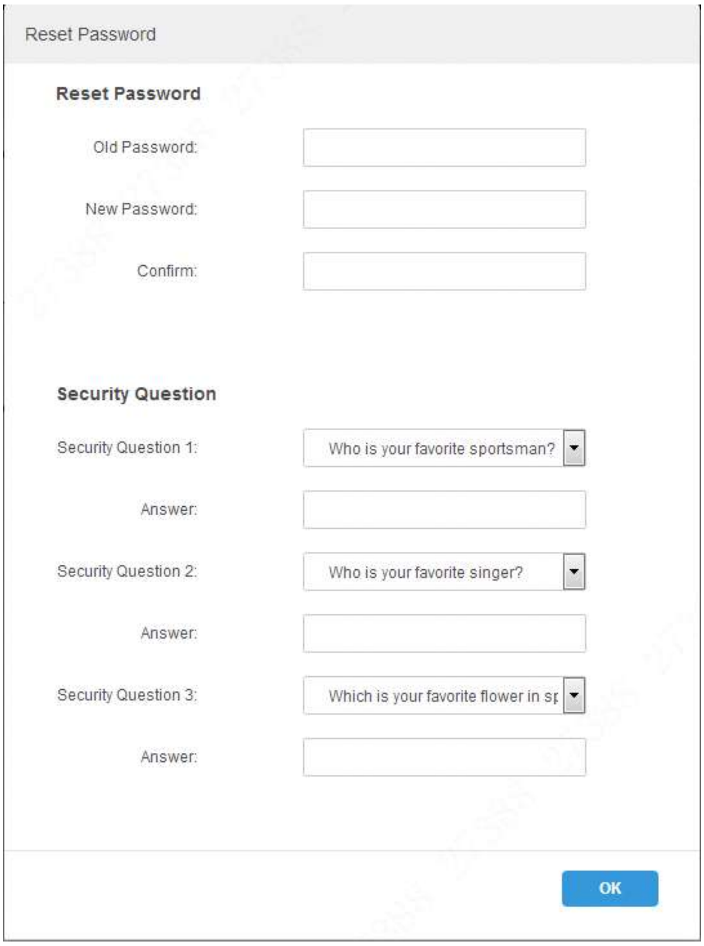
Figure 3-1 Log in config system



Copyright © 1998 - 2018 Zhejiang Dahua Technology Co., Ltd. All Rights Reserved.

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

Reset Password

Old Password:

New Password:

Confirm:

Security Question

Security Question 1: Who is your favorite sportsman?

Answer:

Security Question 2: Who is your favorite singer?

Answer:

Security Question 3: Which is your favorite flower in sp

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.

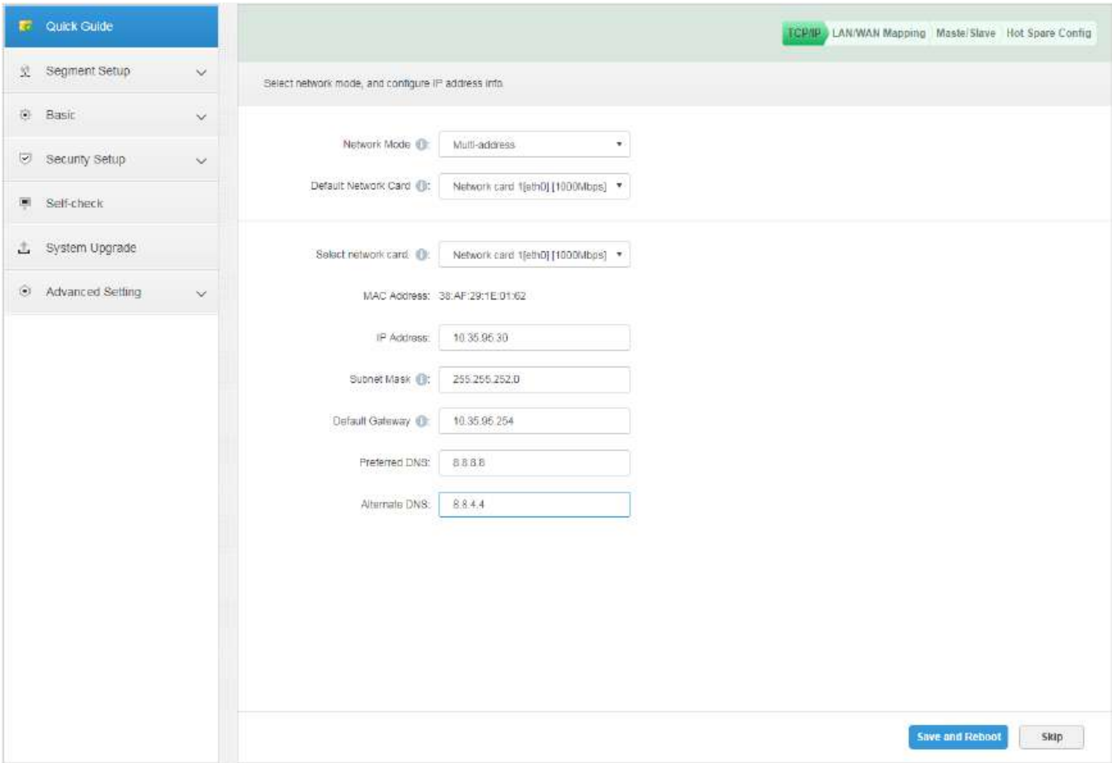
3.2 Quick Guide

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 Network card config



Select network mode, and configure IP address info.

Network Mode: Multi-address

Default Network Card: Network card 1[eth0] [1000Mbps]

Select network card: Network card 1[eth0] [1000Mbps]

MAC Address: 38:AF:29:1E:01:62

IP Address: 10.35.95.30

Subnet Mask: 255.255.252.0

Default Gateway: 10.35.95.254

Preferred DNS: 8.8.8.8

Alternate DNS: 8.8.4.4

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

Table 3-1 Network card parameter description

Parameter	Description
Network Mode	● Multi-address 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. ● Fault tolerance 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. ● Load Balance 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. ● Link aggregation 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).
Add Bound Network Card	It needs to set network card binding when network mode is set as fault tolerance, load balancing or link aggregation. Click “Add Bound Network Card”, select the network cards which need to be bound, users can set two bound network cards.
Default Network Card	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)
Select Network Card	After selecting network card or binding network card, it will display the info of the network card or bound network card below.
MAC Address	It displays the MAC address of platform server.
IP Address	After selecting network card, you can set IP address, subnet mask, default gateway, preferred DNS server address and alternate DNS server address.
Subnet Mask	
Default Gateway	
Preferred DNS	
Alternate DNS	

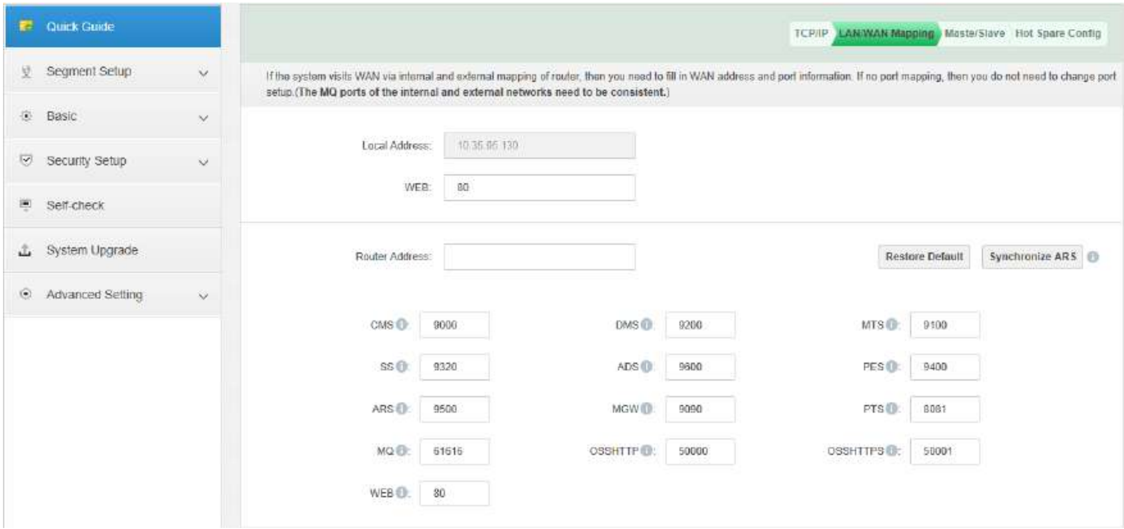
Step 4 Click **Save and Restart**, save network card config and restart server.

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

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

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

Figure 3-4 LAN/WAN mapping



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.**)

Local Address: 10.35.95.130

WEB: 80

Router Address:

CMS: 9000 DMS: 9200 MTS: 9100

SS: 9320 ADS: 9600 PES: 9400

ARS: 9500 MGW: 9090 PTS: 8081

MQ: 61616 OSSHTTP: 50000 OSSHTTPS: 50001

WEB: 80

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

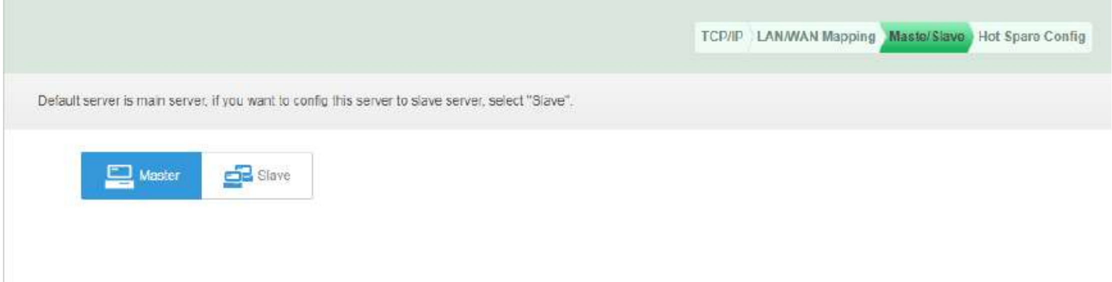
Table 3-2 Network card parameter description

Parameter	Description
IP Address	Sets the address of DSS platform.
Web Service Port	Default WEB service port is 80, it needs to use IP: Port to access WEB if it is not 80. For example, port 81; enter http://172.7.54.35:81/config to access config system.
Router Address	Sets WAN access IP address of router.
CMS	Center management service, which is responsible for registration and signaling scheduling of other services, it is 9010 by default.
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, 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.
OSSHTTP	Picture storage service, which is responsible for receiving, storing and forwarding general pictures, 50000 by default.
OSSHTTPS	Picture storage service which is safer than OSSHTTP, responsible for receiving, storing and forwarding general pictures, 50001 by default.

Step 8 Click **Save and Next**.

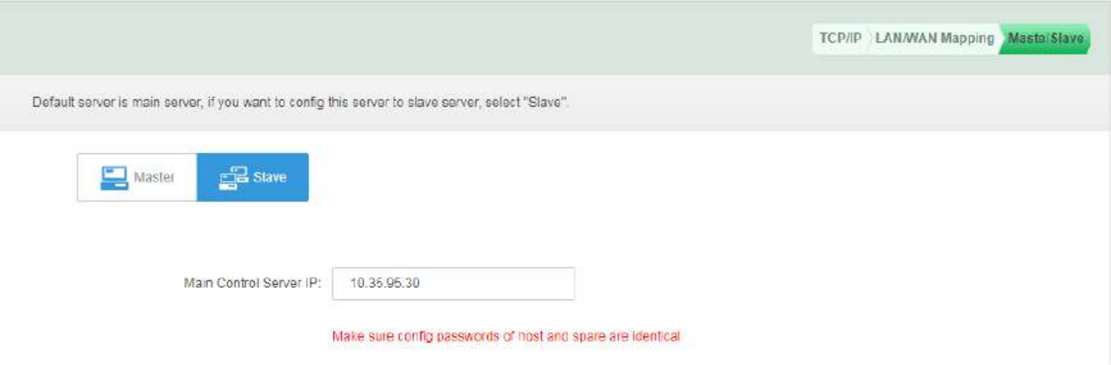
The **Server Mode** is displayed. See Figure 3-5 and Figure 3-6.

Figure 3-5 Server mode (Master)



Default server is main server, if you want to config this server to slave server, select "Slave".

Figure 3-6 Server mode (Slave)



Default server is main server, if you want to config this server to slave server, select "Slave".

Main Control Server IP: 10.35.95.30

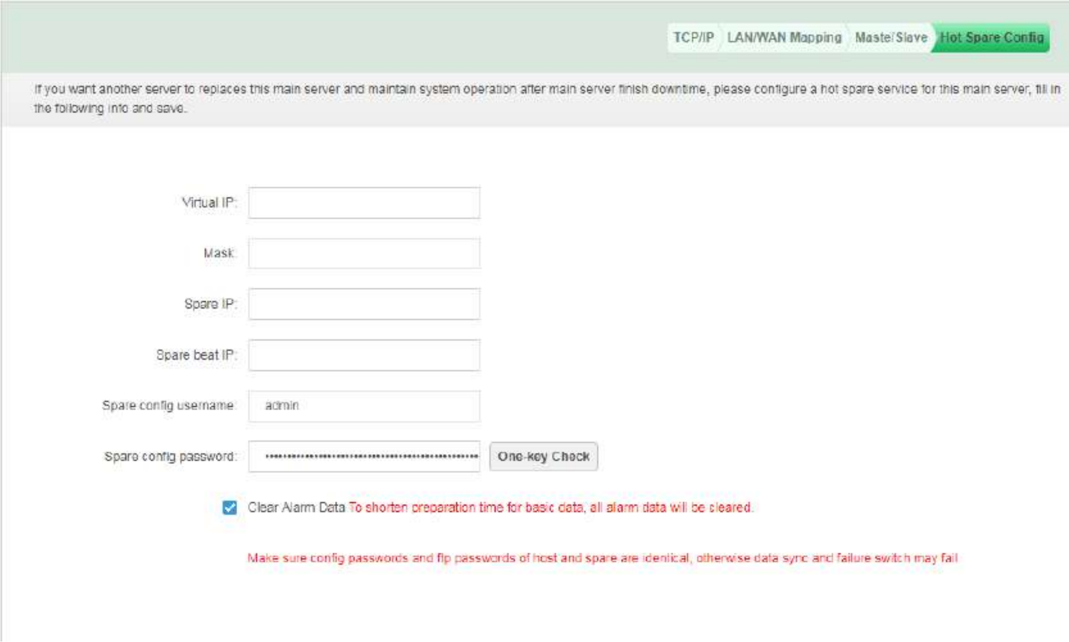
Make sure config passwords of host and spare are identical

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

Step 10 Click **Save and Next**.

The interface of **Hot Spare** is displayed. See Figure 3-7

Figure 3-7 Hot spare config



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

Virtual IP:

Mask:

Spare IP:

Spare beat IP:

Spare config username: admin

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

Table 3-3 Hot spare parameter description

Parameter	Description
Virtual IP	After setting virtual IP, then it can have access to platform via the virtual IP.

Mask	It is in accordance with the mask of network port 1.
Spare Business IP	IP address of spare server network port 1.
Spare Beat IP	IP address of spare server network port 2.
Spare Config System Username	It is the login username and password of spare server config system. 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.
Spare Config System Password	
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

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

3.4 Basic

3.4.1 Manage Account

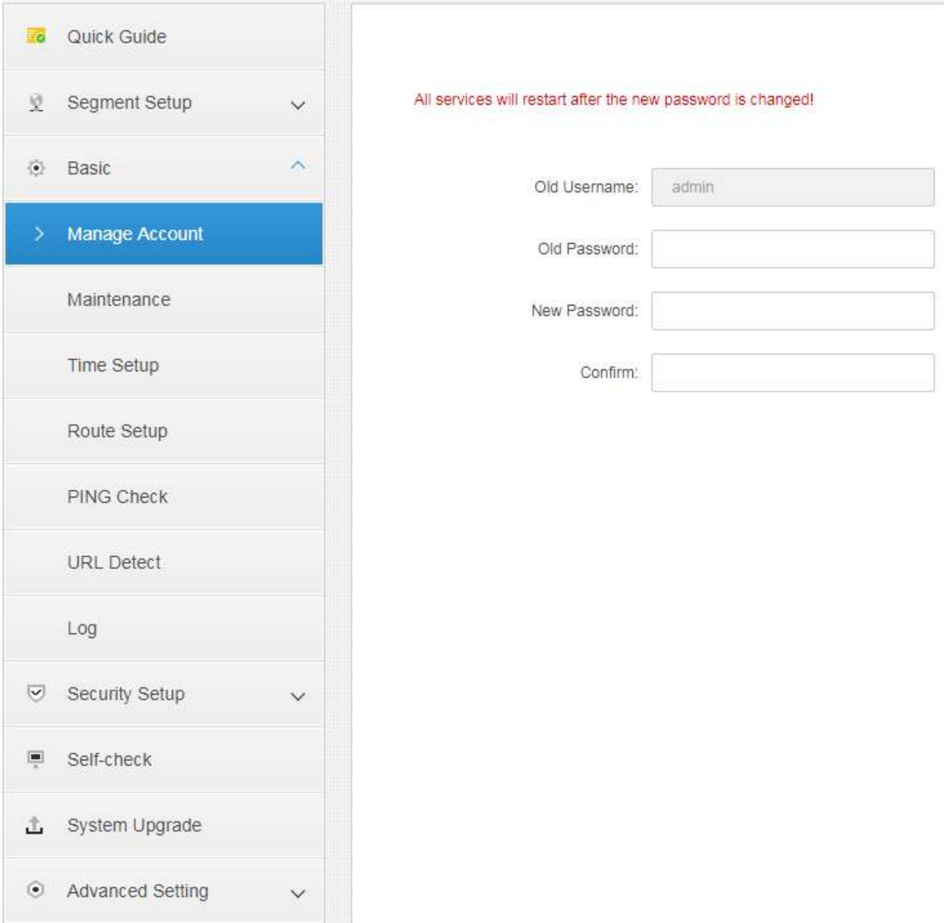
You can modify the login password of admin user.

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

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

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

Figure 3-8 Manage account



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.

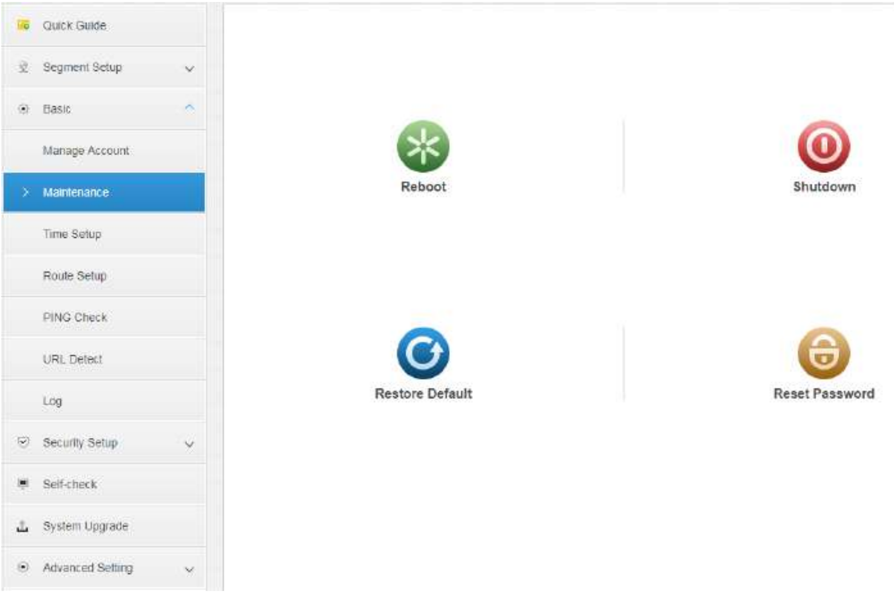
3.4.2 Maintenance

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

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

The **Maintenance** interface is displayed. See Figure 3-9.

Figure 3-9 Maintenance



Step 2 Click relevant operation to realize corresponding functions.

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

3.4.3 Time Setup

Set time zone and time where the server is located.

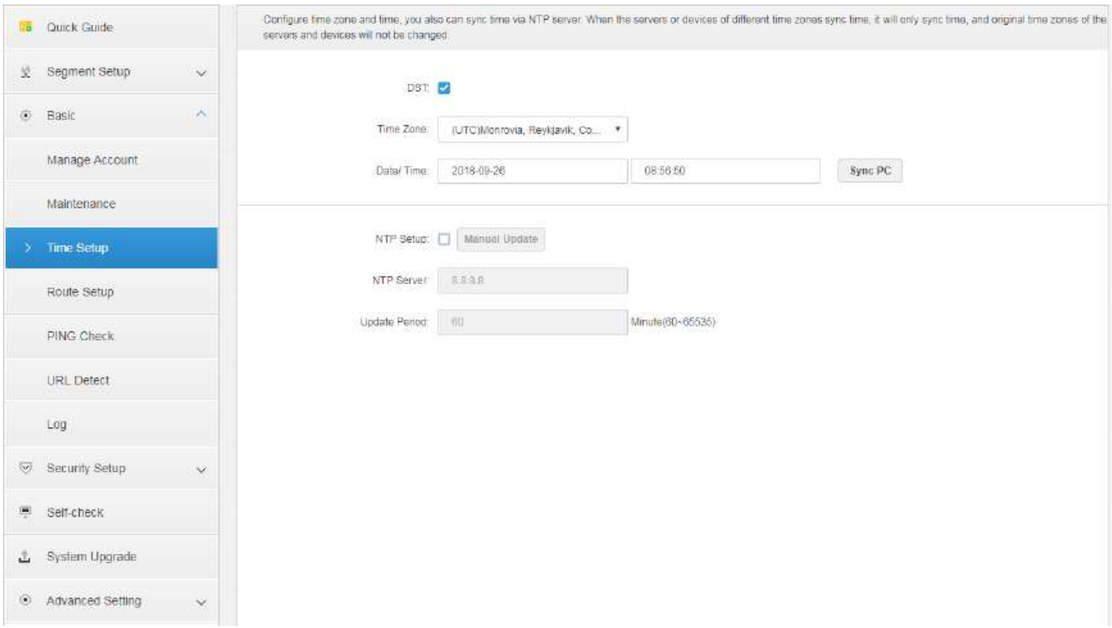
⚠

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

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

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

Figure 3-10 Time setup



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...

Data/ Time: 2018-09-26 08:56:50 Sync PC

NTP Setup: □ Manual Update

NTP Server: 8.8.8.8

Update Period: 60 Minute(60~65535)

Step 2 Configure time parameter. Refer to Table 3-4 for more details.

Table 3-4

Parameter	Description
DST	After selecting **DST**, it enables DST function.
Time Zone	Selects the time zone where the device is located.
Date/Time	The system provides two methods to set data and time. ● Click display box to select data and time. ● Click **Sync PC** and it synchronizes system time to local PC time.
Sync PC	
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.

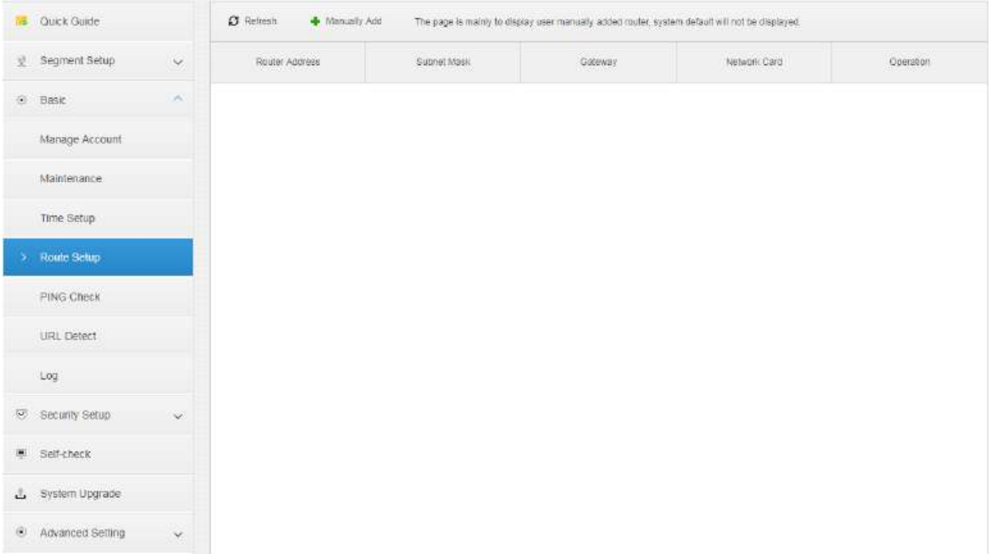
3.4.4 Route Setup

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 Route setup



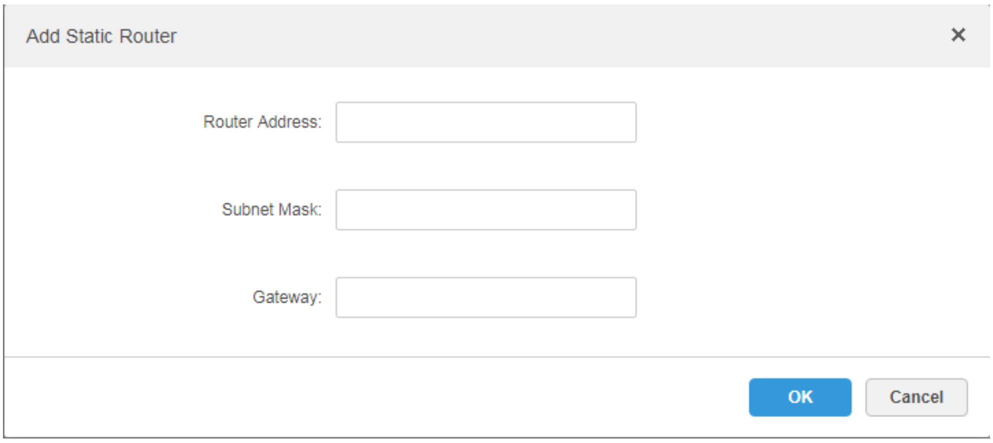
The page is mainly to display user manually added router, system default will not be displayed.

Router Address	Subnet Mask	Gateway	Network Card	Operation

Step 2 Click **Manually Add**.

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

Figure 3-12 Add statistic router



Add Static Router

Router Address:

Subnet Mask:

Gateway:

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

Step 4 Click **OK**.

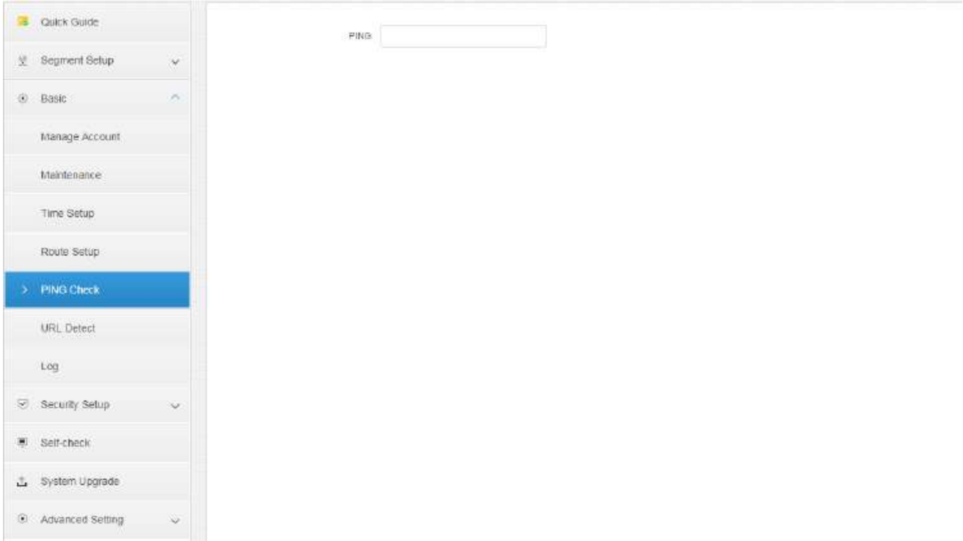
3.4.5 Ping Check

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.

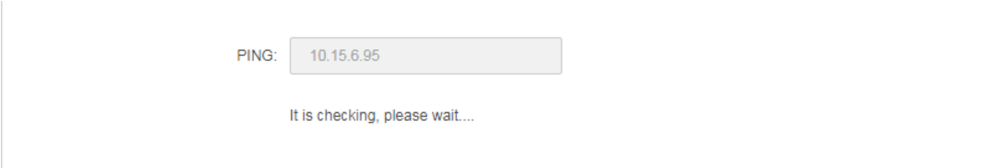
Figure 3-13 PING check



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

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

Figure 3-14 IP



PING: 10.15.6.95

It is checking, please wait....

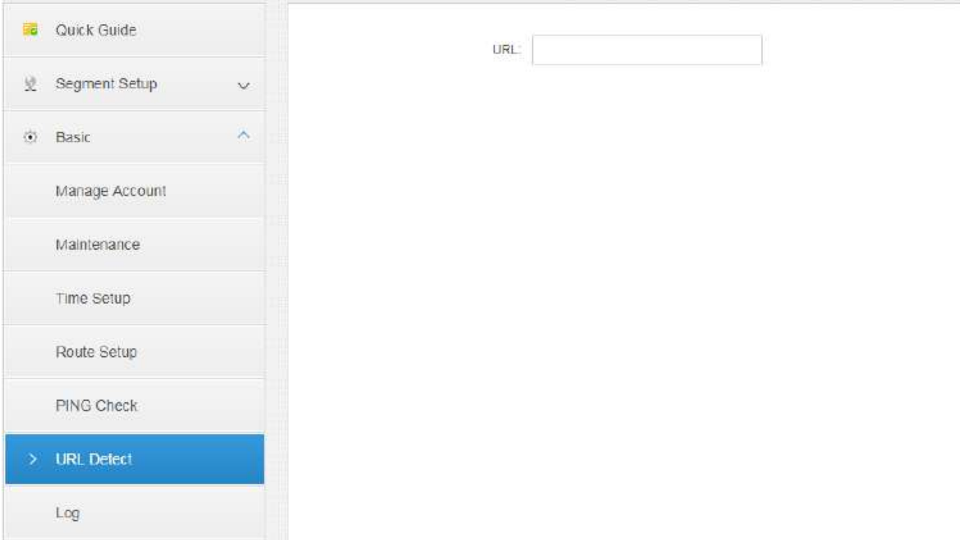
3.4.6 URL Detect

Detect 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 URL detection



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

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

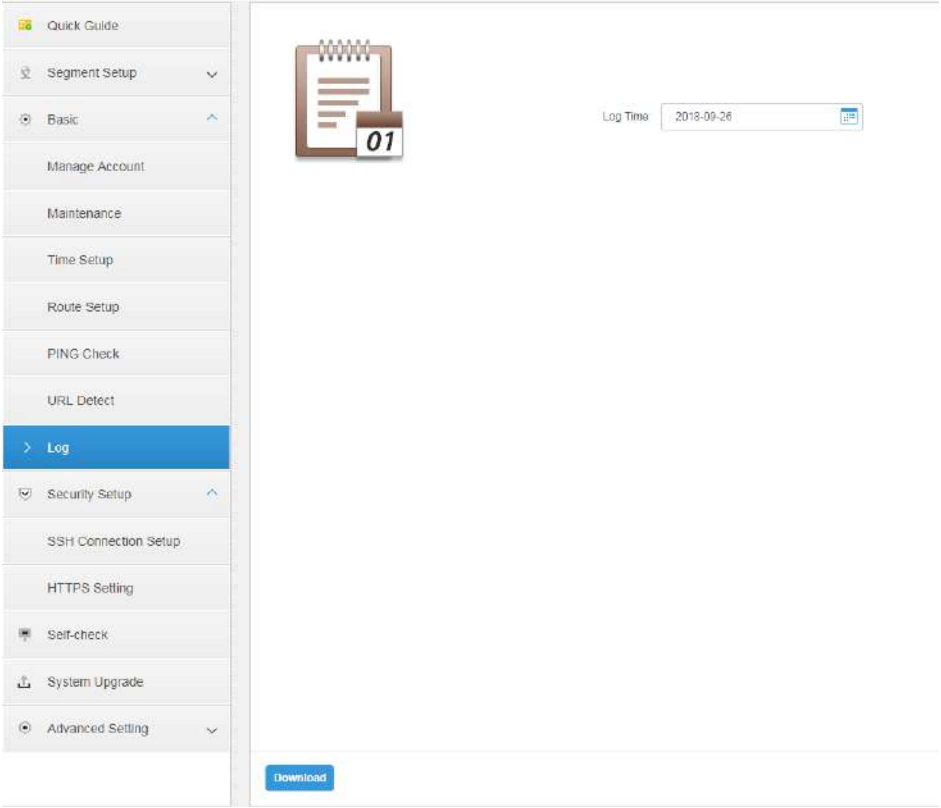
3.4.7 Log

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 Log



Log Time 2018-09-26

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

3.5 Security Setup

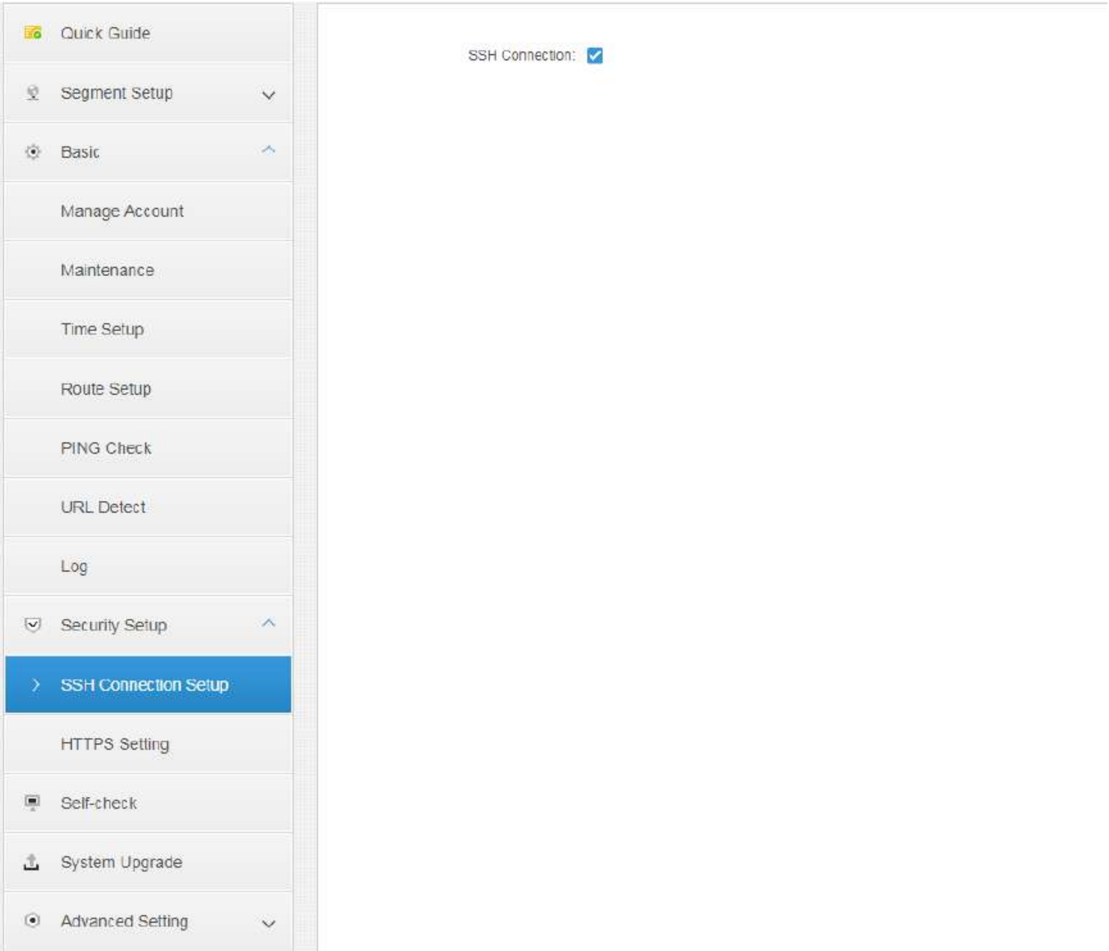
3.5.1 SSH Connection Setup

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 SSH connection



SSH Connection: ☑

Step 2 Select **SSH Connection**.

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

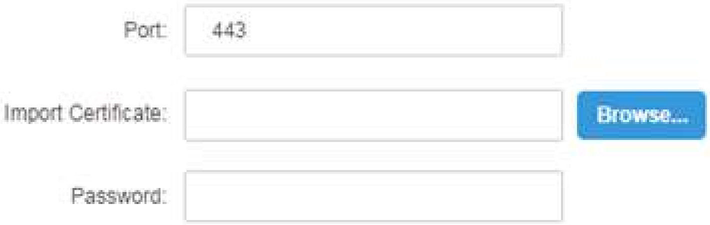
3.5.2 HTTPS Setting

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 Configure HTTPS



Port: 443

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.

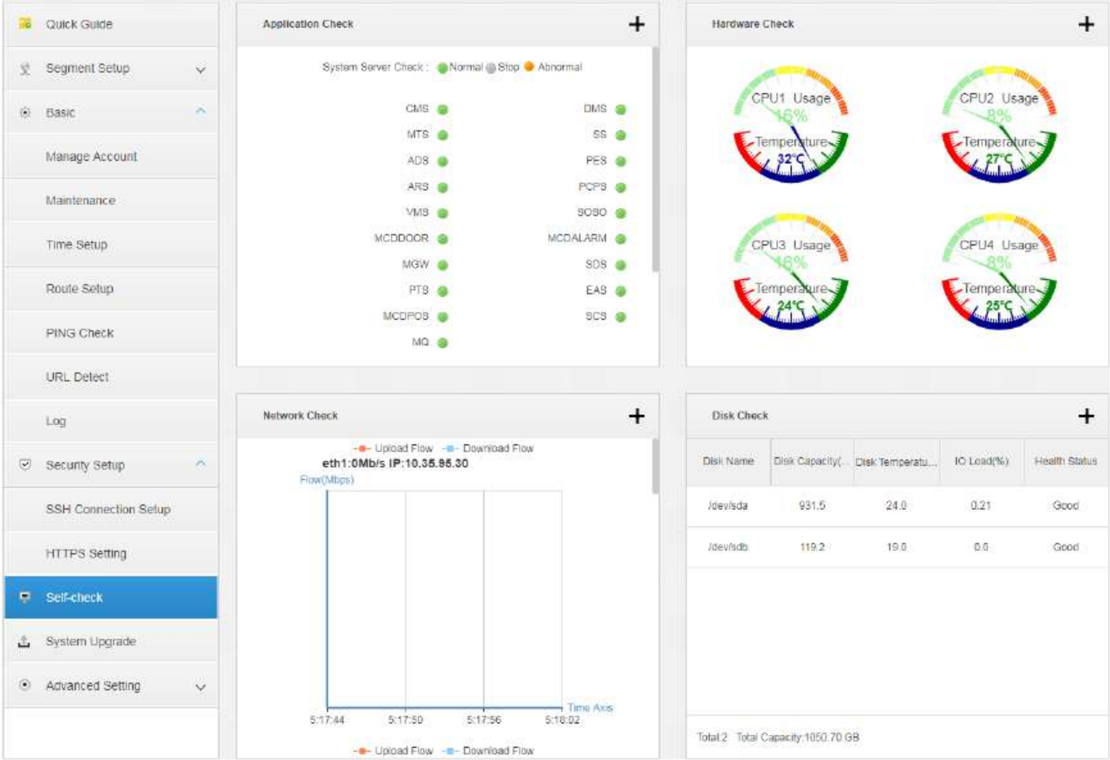
Step 3 Click **Apply** to complete setting.

3.6 Self-check

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

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

Figure 3-19 System self-check



Quick Guide
Segment Setup
Basic
Manage Account
Maintenance
Time Setup
Route Setup
PING Check
URL Detect
Log
Security Setup
SSH Connection Setup
HTTPS Setting
Self-check
System Upgrade
Advanced Setting

Application Check +

System Server Check : ● Normal ● Stop ● Abnormal

CMS ● DMS ●
MTS ● SS ●
ADS ● PES ●
ARS ● PCPS ●
VMS ● SOSO ●
MCDDOOR ● MCDALARM ●
MGW ● SDS ●
PTS ● EAS ●
MCDPOS ● SCS ●
MQ ●

Hardware Check +

Network Check +

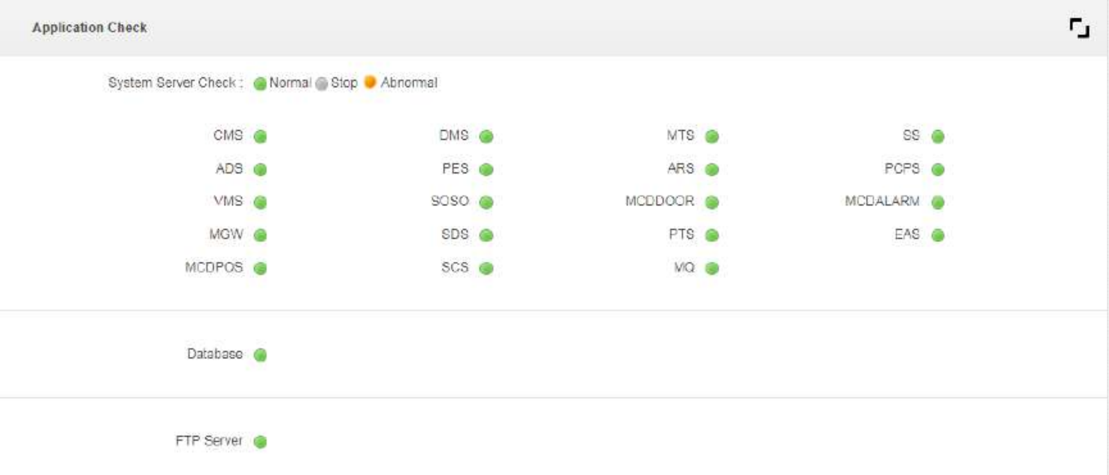
Disk Check +

Disk Name	Disk Capacity(...	Disk Temperatu...	IO Load(%)	Health Status
/dev/sda	931.5	24.0	0.21	Good
/dev/sdb	119.2	19.0	0.0	Good

Total:2 Total Capacity:1050.70 GB

- 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 Application check result



Application Check

System Server Check : ● Normal ● Stop ● Abnormal

CMS ● DMS ● MTS ● SS ●
ADS ● PES ● ARS ● PCPS ●
VMS ● SOSO ● MCDDOOR ● MCDALARM ●
MGW ● SDS ● PTS ● EAS ●
MCDPOS ● SCS ● MQ ●

Database ●

FTP Server ●

Figure 3-21 CPU check result

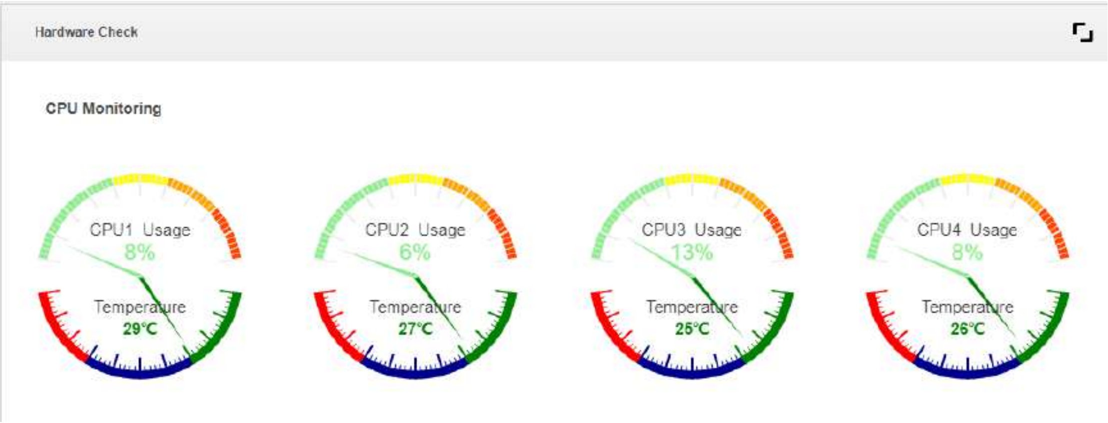


Figure 3-22 Network detection result

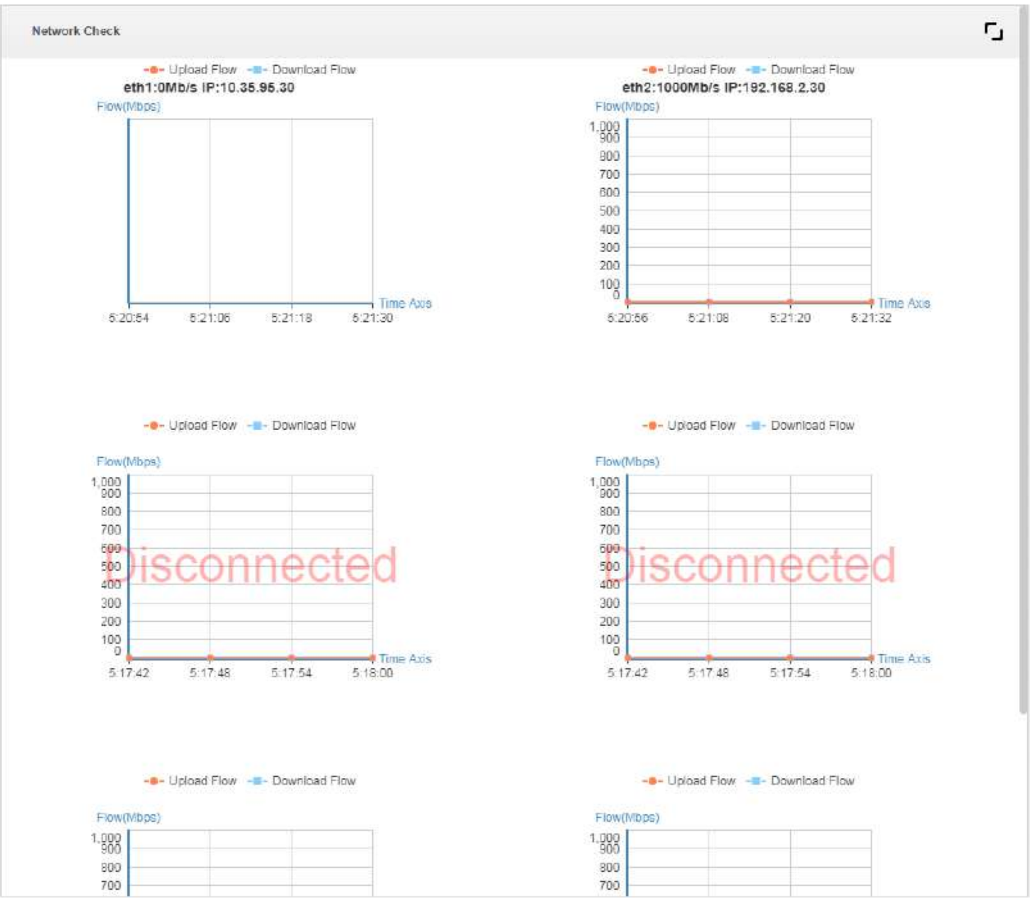
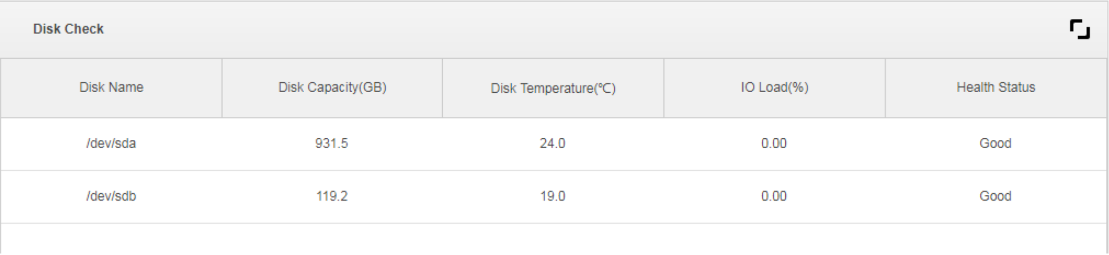


Figure 3-23 Disk detection result


Disk Check

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

3.7 Advanced Setting

3.7.1 Configuring Master/Slave

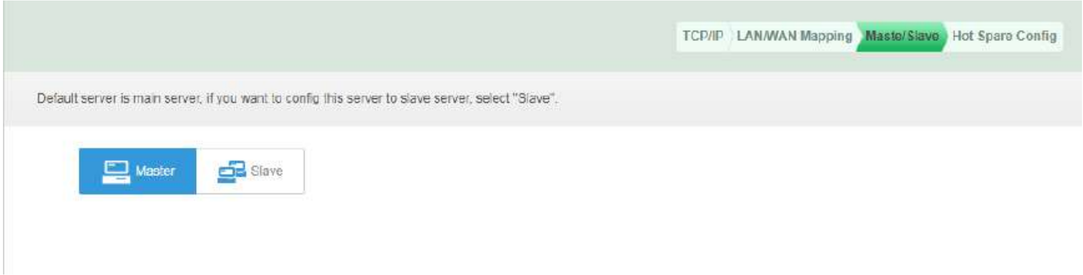
If the server is deployed by distribution, then you can set master and slave mode according to actual situation.

Step 1 Select **Advanced Setting** > **Server Mode**.

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

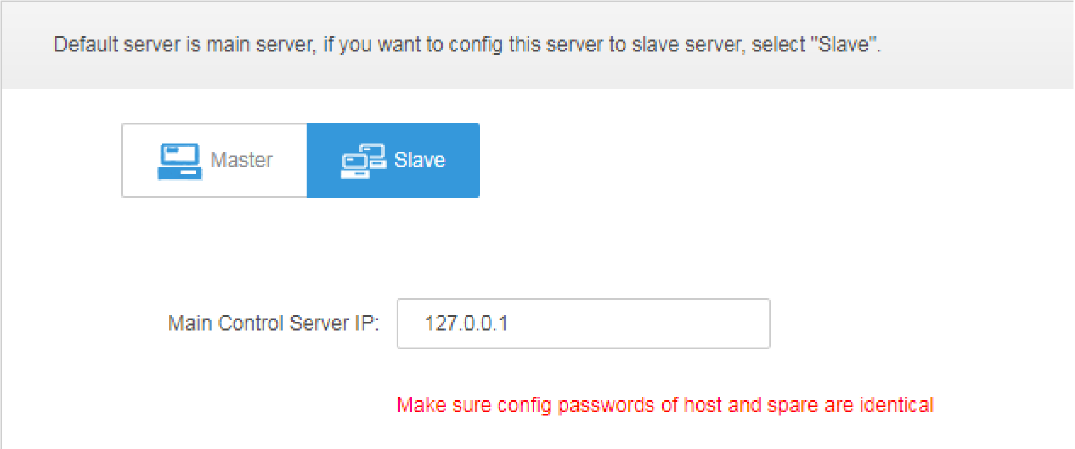
The interface is shown in Figure 3-24 and Figure 3-25

Figure 3-24 Configure server mode (master)



Default server is main server, if you want to config this server to slave server, select "Slave".

Figure 3-25 Configure server mode (slave)



Default server is main server, if you want to config this server to slave server, select "Slave".

Main Control Server IP: 127.0.0.1

Make sure config passwords of host and spare are identical

Step 3 Click **Apply**.

3.7.2 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.

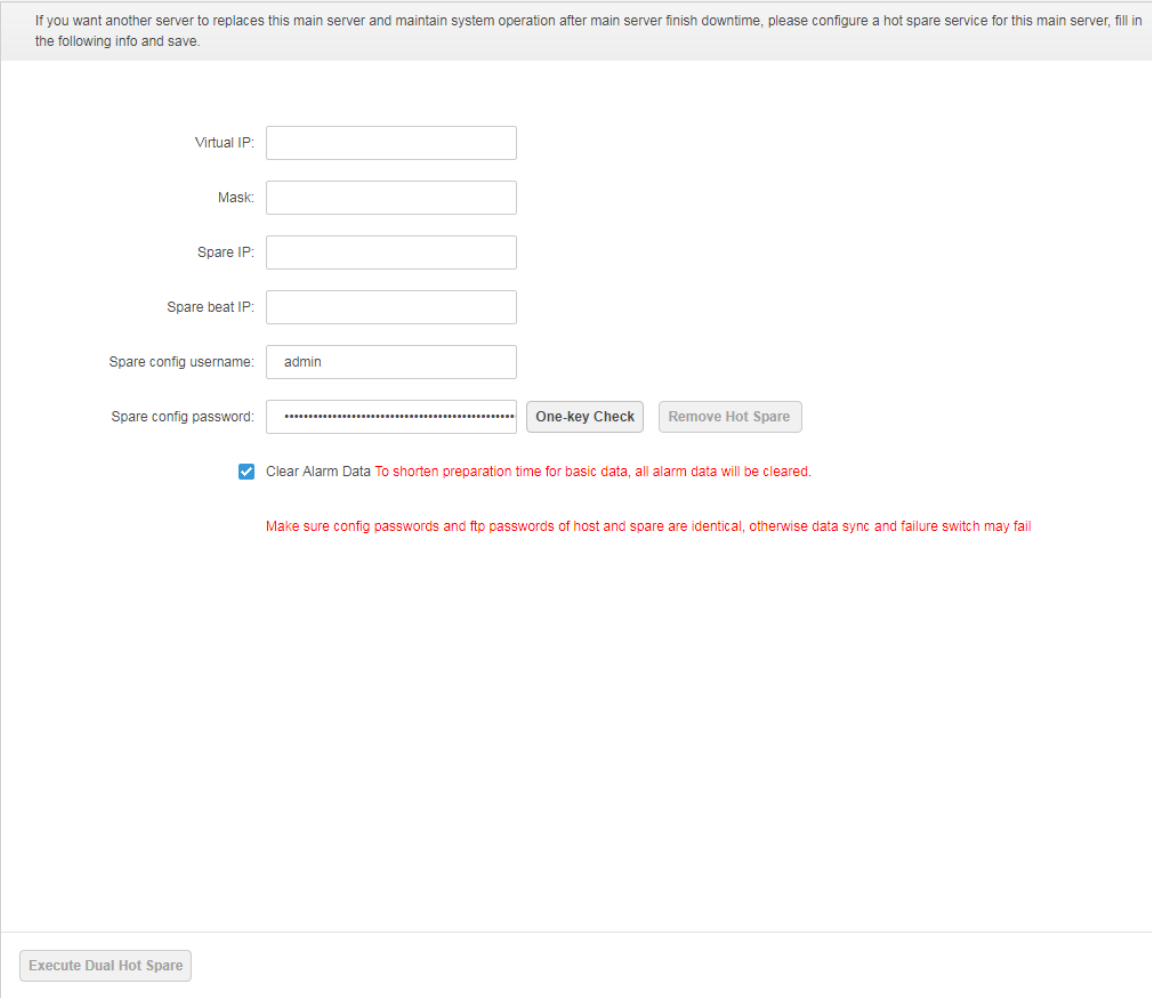
- Attention
  - Dual hot spare needs to use one virtual IP address, which is VIP (Virtual IP) .The VIP is chosen to, allocate an unused IP address in the business network. After the configuration is completed, the IP addresses of two DSSs do not need to log in, it only needs to log in VIP.
  - If dual 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 3-26.

Figure 3-26 Hot spare



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

Virtual IP:

Mask:

Spare IP:

Spare beat IP:

Spare config username: admin

Spare config password: ••

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

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

Step 2 Configure the parameters of hot spare server. Please refer to Table 3-5 for more details.

Table 3-5 Hot spare parameter description

Parameter	Description
Virtual IP	After setting virtual IP, then it can have access to platform via the virtual IP.
Mask	It is in accordance with the mask of network port 1.
Spare Business IP	IP address of spare server network port 1.
Spare Beat IP	IP address of spare server network port 2.
Spare Config System Username	It is the login username and password of spare server config system. 📖 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.
Spare Config System Password	
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

DSS7016 Manager (hereinafter referred to as Manager) supports configuring system information, user information and record plan. It is recommended to use Google Chrome 40 and later version, Firefox 40 and later version to log in manager.

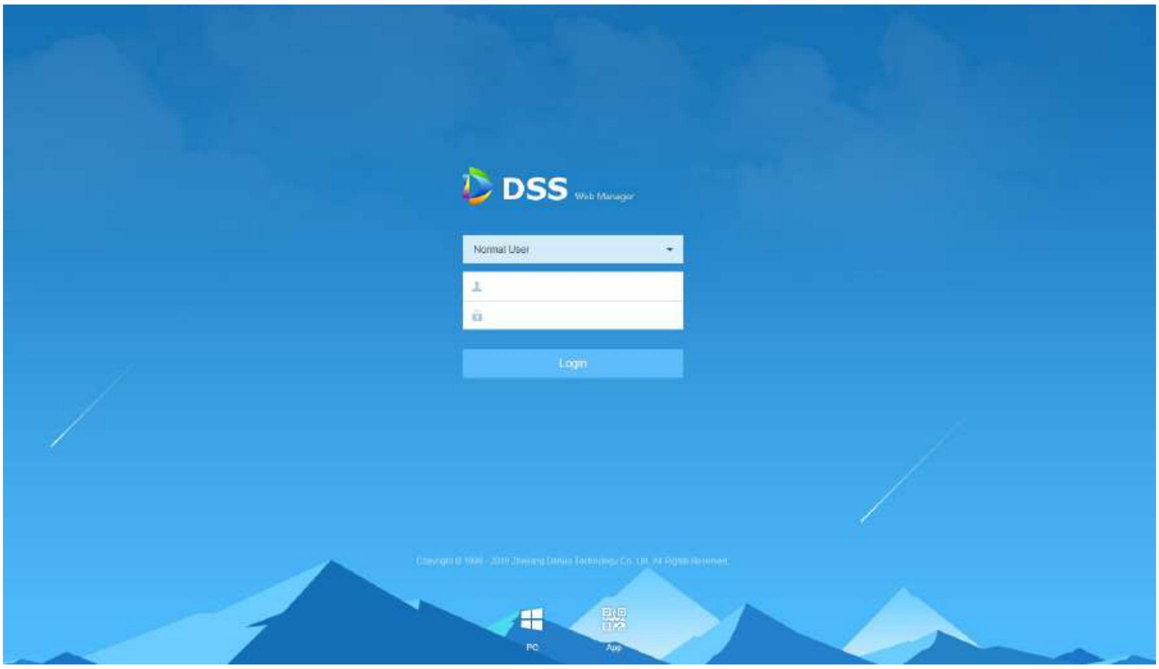
4.1 Logging in Manager

You can configure relevant functions remotely after logging in manager.

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

The login interface is displayed. See Figure 4-1.

Figure 4-1 Login interface


DSS Web Manager
Normal User
Login
Copyright © 1996 - 2019 Zhejiang Dahua Technology Co., Ltd. All Rights Reserved.
PC
App

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

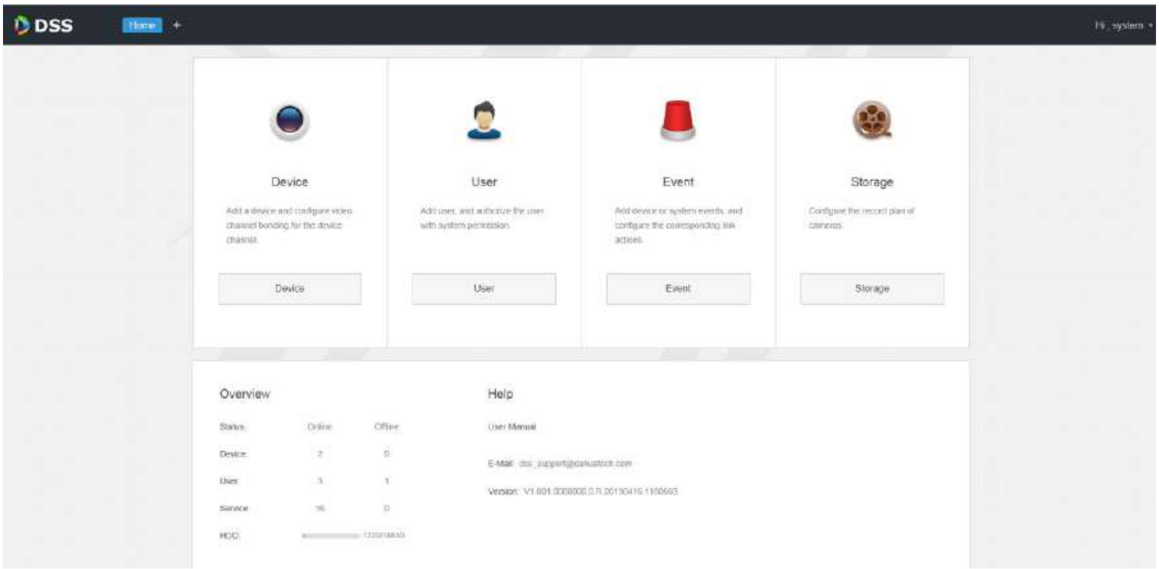
The default username is system.

📖

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

The homepage is displayed after login. See Figure 4-2.

Figure 4-2 Home



Add a device and configure video channel bonding for the device channel.

Add user, and authorize the user with system permission.

Add device or system events, and configure the corresponding link actions.

Configure the record plan of cameras.

Overview

Status	Online	Offline
Device	2	0
User	3	1
Service	16	0
HDD	[illegible]	

Help

User Manual

E-Mail: dss_support@dahuatech.com

Version: V1.001.0000000.0.R.20150416.1100663

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

4.2 System Settings

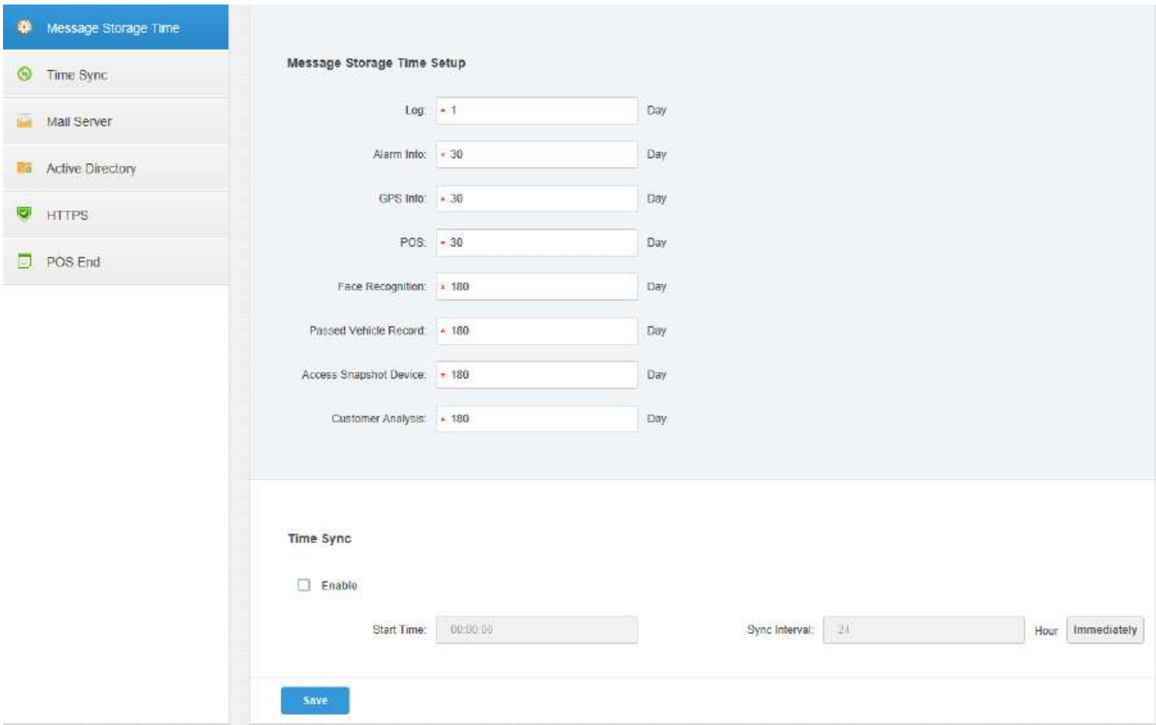
4.2.1 Setting System Parameters

You need to configure system parameters when you log in DSS system for the first time, which is to make sure that the system runs normally.

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

The system displays the interface. See Figure 4-3.

Figure 4-3 System setting



Message Storage Time Setup

Log: * 1 Day

Alarm Info: * 30 Day

GPS Info: * 30 Day

POS: * 30 Day

Face Recognition: * 180 Day

Passed Vehicle Record: * 180 Day

Access Snapshot Device: * 180 Day

Customer Analysis: * 180 Day

Time Sync

□ Enable

Start Time: 00:00:00 Sync Interval: 24 Hour Immediately

Save

Table 4-1 System setting parameter description

Parameter		Description
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.
	Face Recognition	Sets the longest keep time of face recognition info; it is 180 days by default.
	Passed Vehicle Record	Sets the longest keep time of passed vehicle record; it is 180 days by default.
	Access Snapshot Device	Sets the longest keep time of entrance snapshot record.
	Customer Analysis	Sets the longest keep time of people flow statistics record.
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. 📖 The time between device and server is synchronized via SDK.
	Immediately	Click the button to start time sync immediately.

Parameter		Description
Mail Server	–	Set mail server IP, port, encryption type, username/password, sender and test recipient. 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.
POS End	–	After setting POS end mark, it will display on the location of POS receipts end.

Step 2 Configure corresponding parameters.

Step 3 Click **Save**.

4.2.2 Setting Mail Server

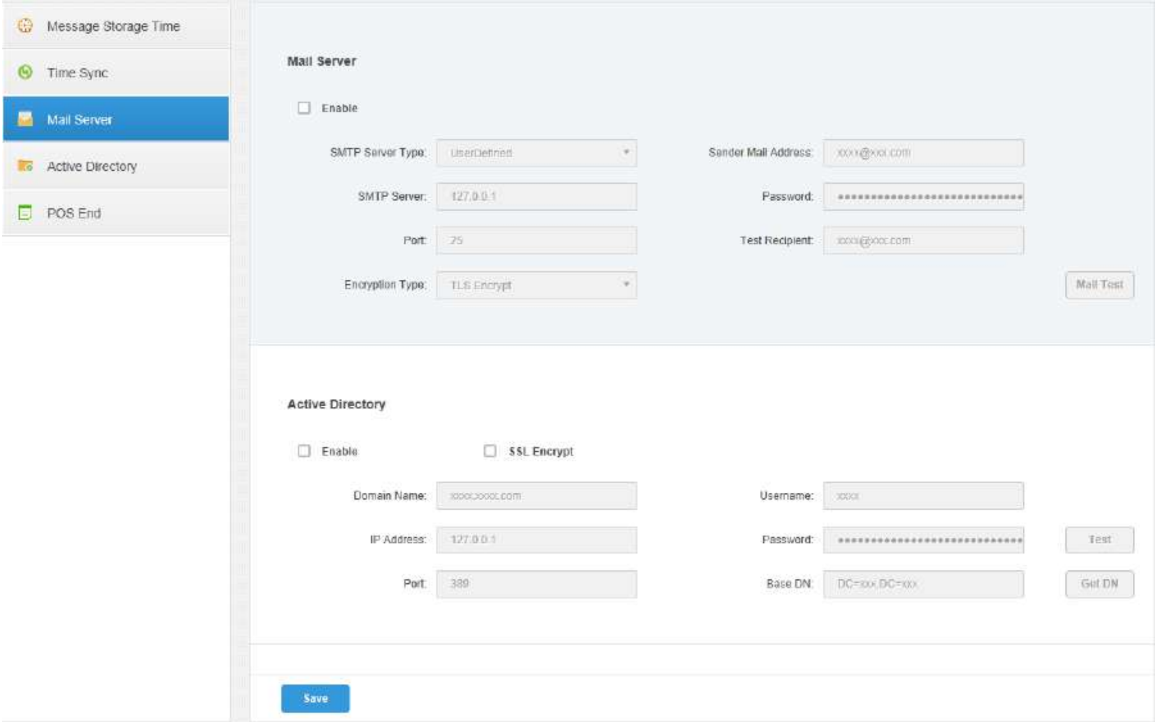
You can select to send mail to user when the administrator is configuring alarm linkage and client handling alarm, at this moment, you need to configure mail server first.

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

Step 2 Click the tab of **Mail Server** and the config interface is displayed.

Step 3 Select **Enable** and mail config is enabled. See Figure 4-4.

Figure 4-4 Mail server setting



Mail Server

□ Enable

SMTP Server Type: UserDefined

SMTP Server: 127.0.0.1

Port: 25

Encryption Type: TLS Encrypt

Sender Mail Address: xxxx@xxx.com

Password: ••••••••••••••••••••••••••••

Test Recipient: xxxx@xxx.com

Active Directory

□ Enable □ SSL Encrypt

Domain Name: xxxx.xxxx.com

IP Address: 127.0.0.1

Port: 389

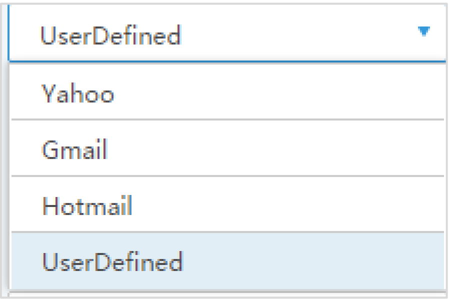
Username: xxxx

Password: ••••••••••••••••••••••••••••

Base DN: DC=xxx,DC=xxx

Step 4 Select the type of mail server in the drop-down box. See Figure 4-5.

Figure 4-5 Select type



Step 5 Set mail server IP, port, encryption type, username/password, sender and test recipient.

Step 6 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 7 Click **Save** after the test is successful, and then config info is saved..

4.3 Adding Organization

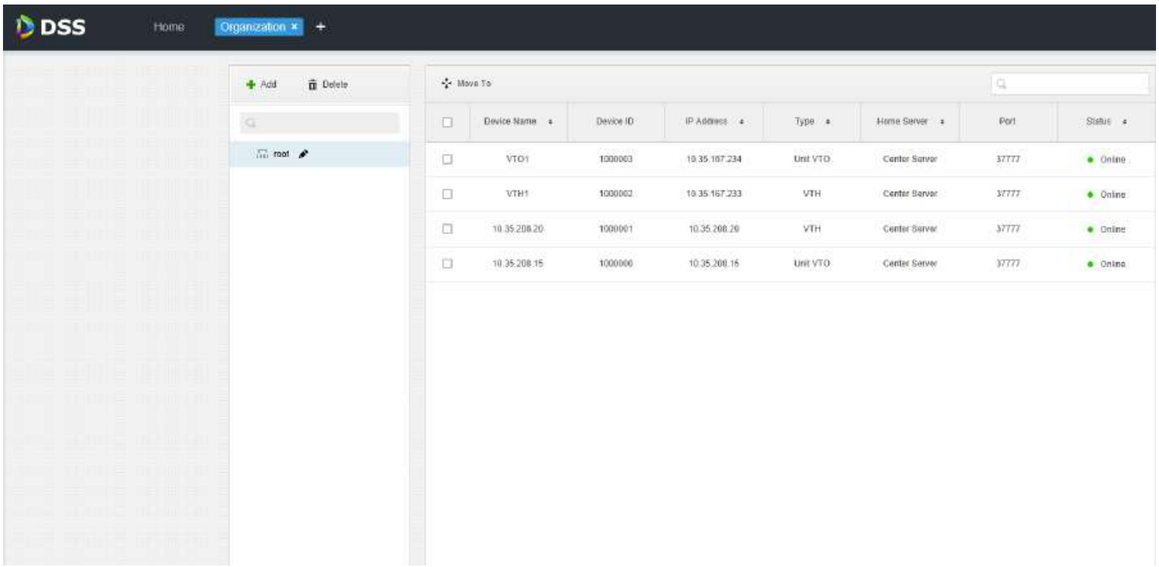
Adding organizations is to deploy the hierarchy of organization or device, which is to make it easy to manage. It doesn’t have to add organizations, the added users or devices are classified to the default organization.

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

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

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

Figure 4-6 Organization

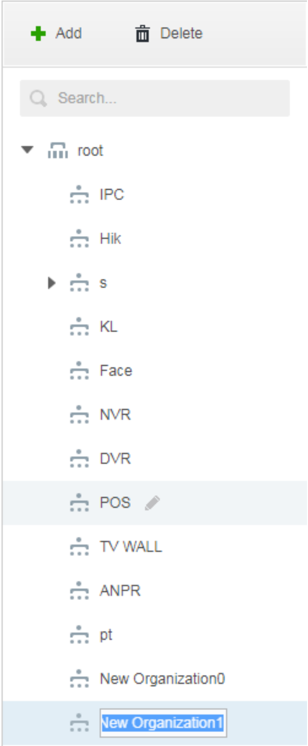


□	Device Name	Device ID	IP Address	Type	Home Server	Port	Status
□	VTO1	1000003	10.35.167.234	Unit VTO	Center Server	37777	● Online
□	VTH1	1000002	10.35.167.233	VTH	Center Server	37777	● Online
□	10.35.208.20	1000001	10.35.208.20	VTH	Center Server	37777	● Online
□	10.35.208.15	1000000	10.35.208.15	Unit VTO	Center Server	37777	● Online

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

Add new organizations under the root organization. See Figure 4-7.

Figure 4-7 Add organization



Step 3 Enter organization name and click **Enter**.

Operations

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

4.4 Adding Role and User

4.4.1 Adding User Role

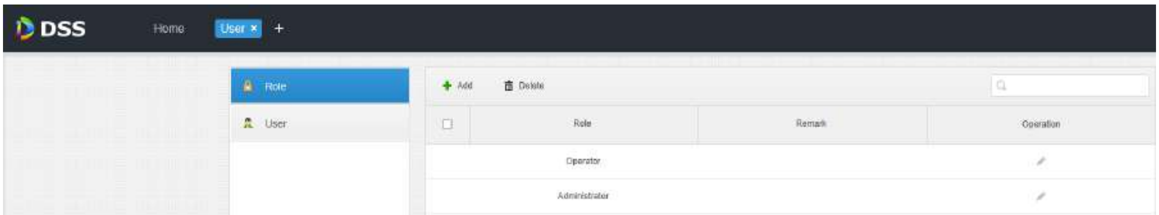
You can create user role and add user. The created user can log in both admin and client. Different user roles decide users to have different operation permissions.

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

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

The **User** interface is displayed. See Figure 4-8.

Figure 4-8 User



	Role	Remark	Operation
	Operator		
	Administrator		

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

The system pops out the **Add Role** interface.

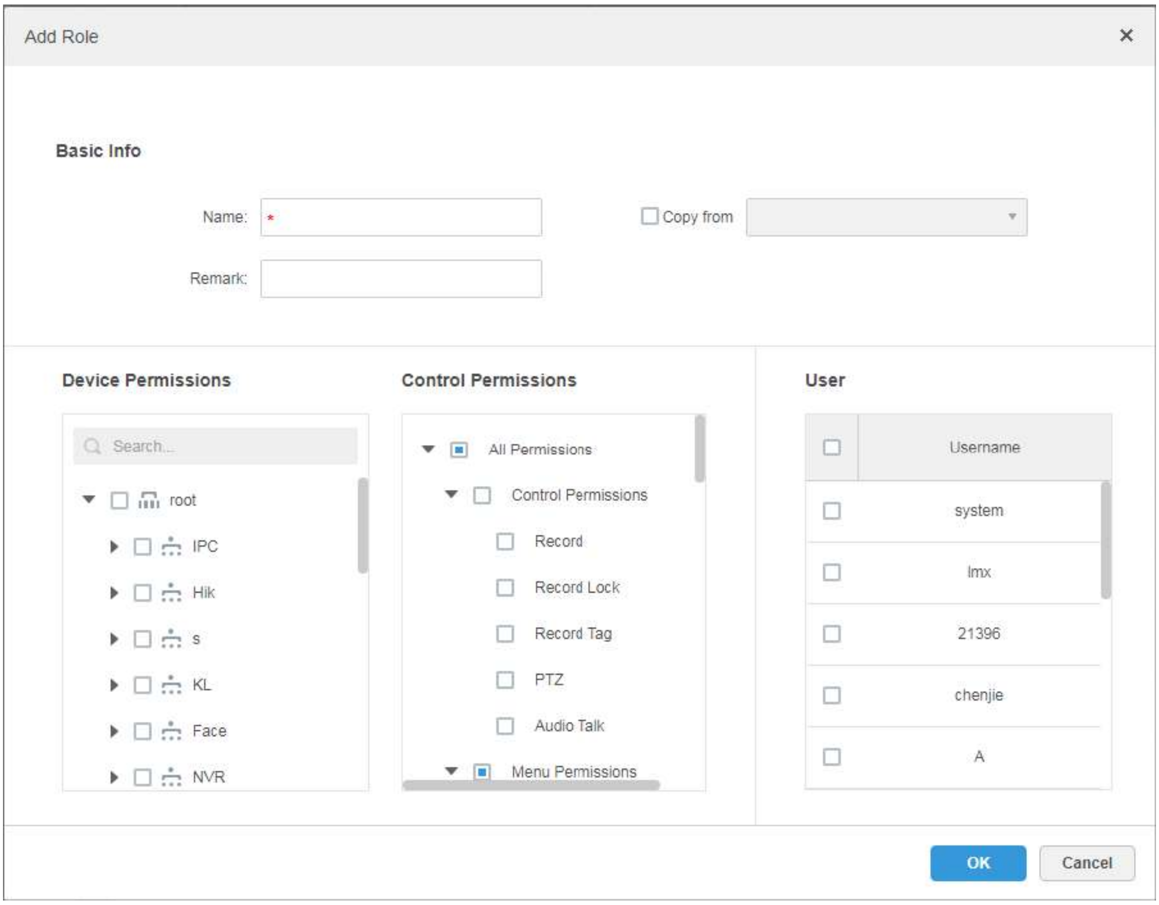
Step 3 Enter **Role Name**.

If you select **Copy from** next to the **Role Name** and select some role in the drop-down List, then you can copy the config info into the selected roles and realize quick config.

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

The system displays the interface. See Figure 4-9.

Figure 4-9 Configure device permission



□	Username
□	system
□	lmx
□	21396
□	chenjie
□	A

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

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

4.4.2 Adding User

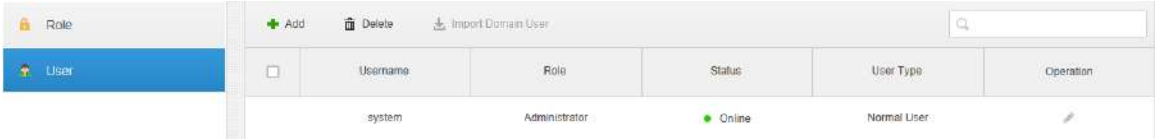
Create user for platform, used for management and operation. User permission is restricted by selected role.

Operation Steps

Step 1 Click **User** tab.

The **User** interface is displayed. See Figure 4-10.

Figure 4-10 User

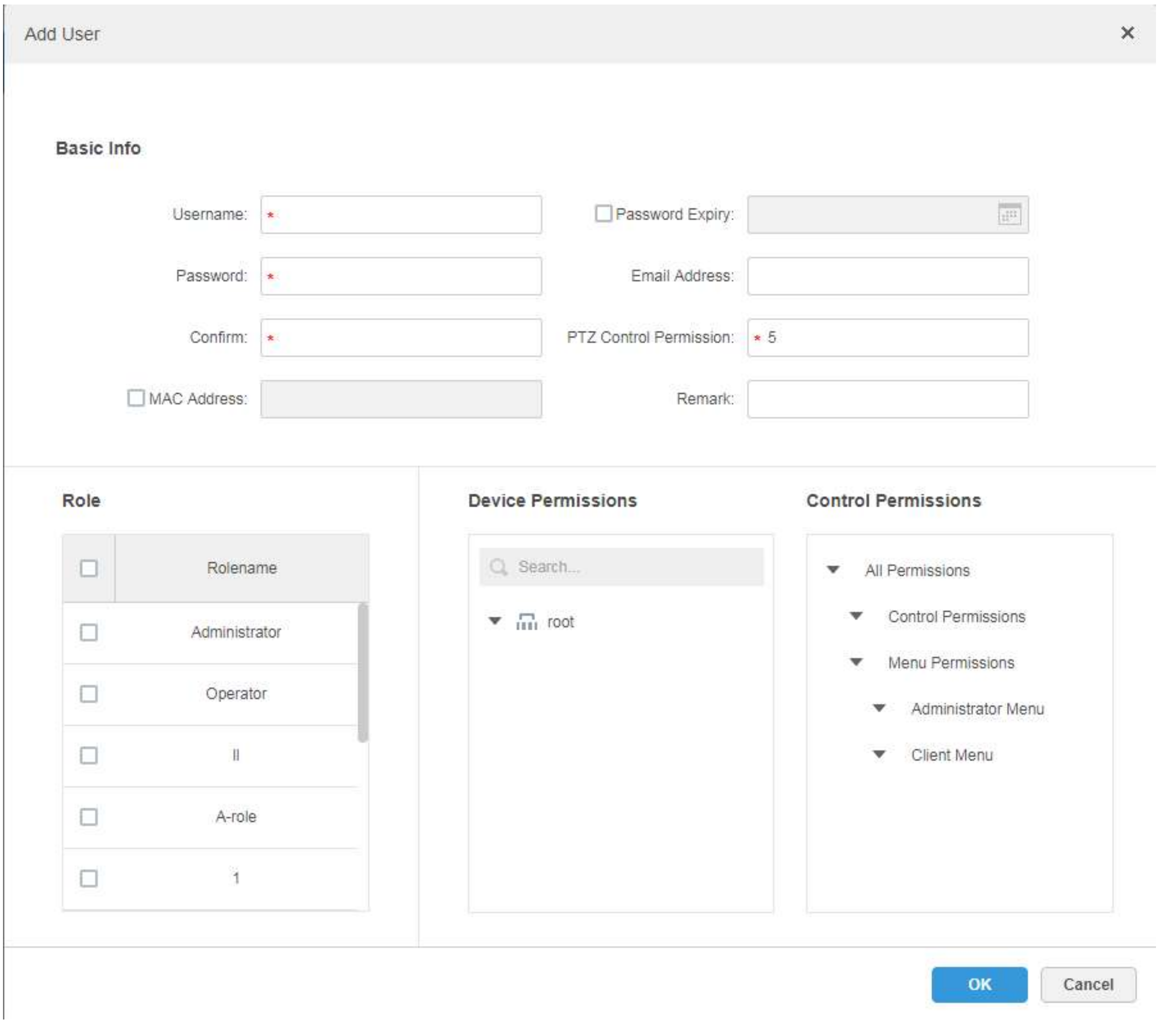


□	Username	Role	Status	User Type	Operation
	system	Administrator	● Online	Normal User	

Step 2 Click **Add**.

The system will pop out the **Adding User** interface.

Figure 4-11 Add user



Username: *

Password: *

Confirm: *

□ MAC Address:

□ Password Expiry:

Email Address:

PTZ Control Permission: * 5

Remark:

□	Rolename
□	Administrator
□	Operator
□	ll
□	A-role
□	1

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

- The user has no **Device Permission** or **Operation Permission** if you do not 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.

4.4.3 Setting Domain User

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

4.4.3.1 Application Scenario

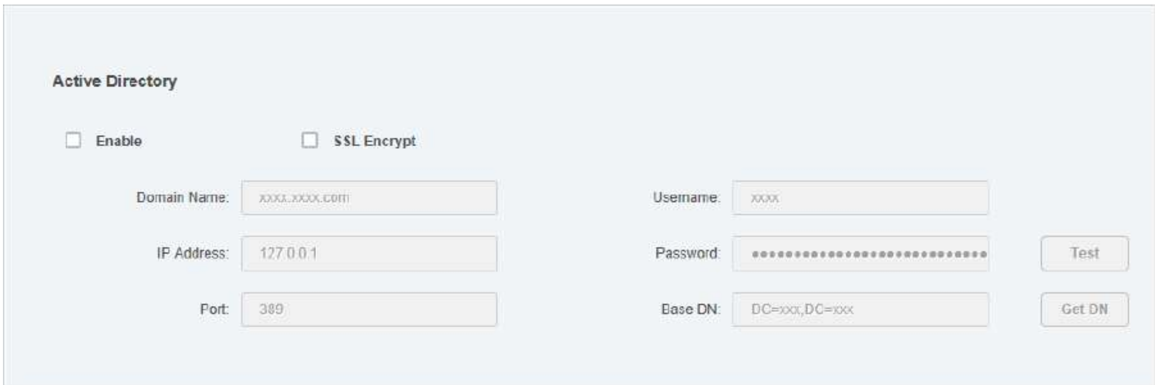
For the companies with domain information and want to use domain users as system login users, using domain user import can improve the convenience of project deployment.

4.4.3.2 Setting Domain Info

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

Step 2 Click the tab of **Active Directory** and configure domain info. See Figure 4-12.

Figure 4-12 Domain setting



Active Directory

□ Enable □ SSL Encrypt

Domain Name: xxxx.xxxx.com

Username: xxxx

IP Address: 127.0.0.1

Password: ••••••••••••••••••••••••••••

Test

Port: 389

Base DN: DC=xxx,DC=xxx

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.

You can import domain user on the interface of **User** after it prompted successfully.

Please refer to the next chapter for more operation details.

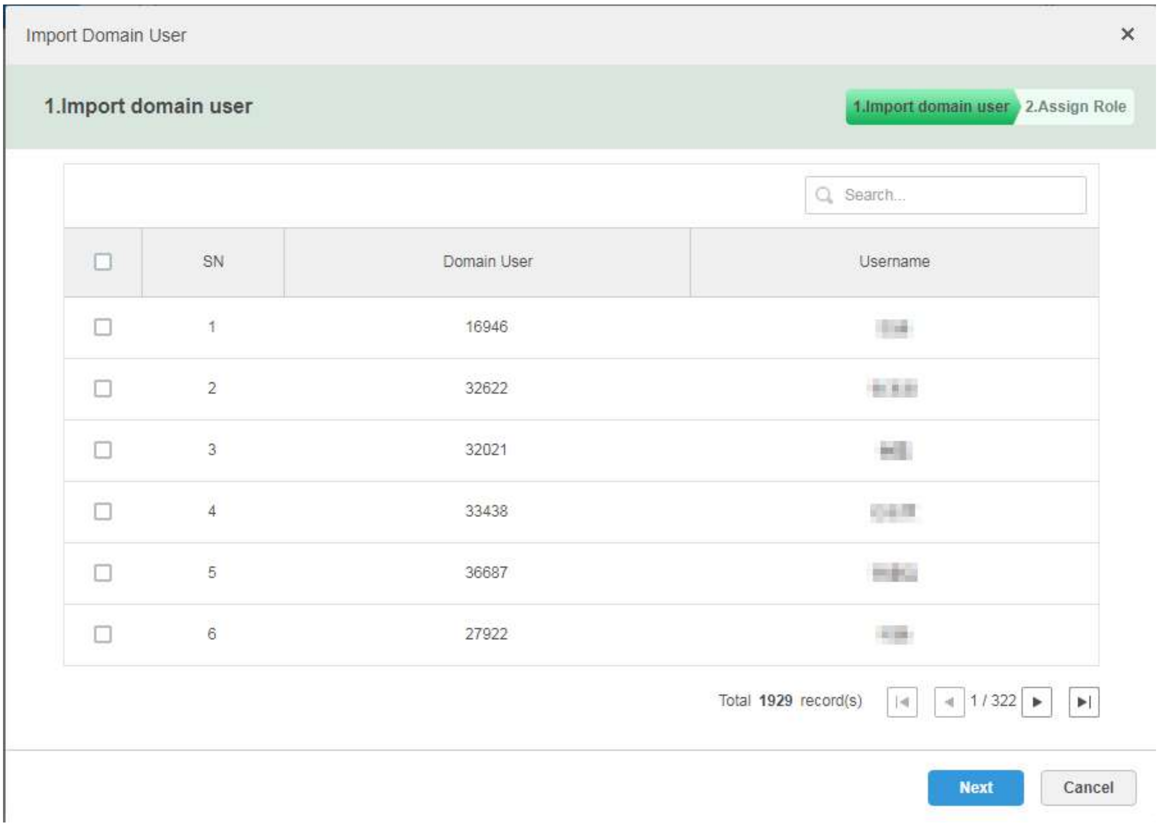
4.4.3.3 Importing Domain User

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

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

The system will display the interface of **Import Domain User**. See Figure 4-13.

Figure 4-13 Import domain user



Import Domain User ×

1.Import domain user

1.Import domain user 2.Assign Role

Search...

□	SN	Domain User	Username
□	1	16946	[redacted]
□	2	32622	[redacted]
□	3	32021	[redacted]
□	4	33438	[redacted]
□	5	36687	[redacted]
□	6	27922	[redacted]

Total 1929 record(s) |◀ ◀ 1 / 322 ▶ ▶|

Next Cancel

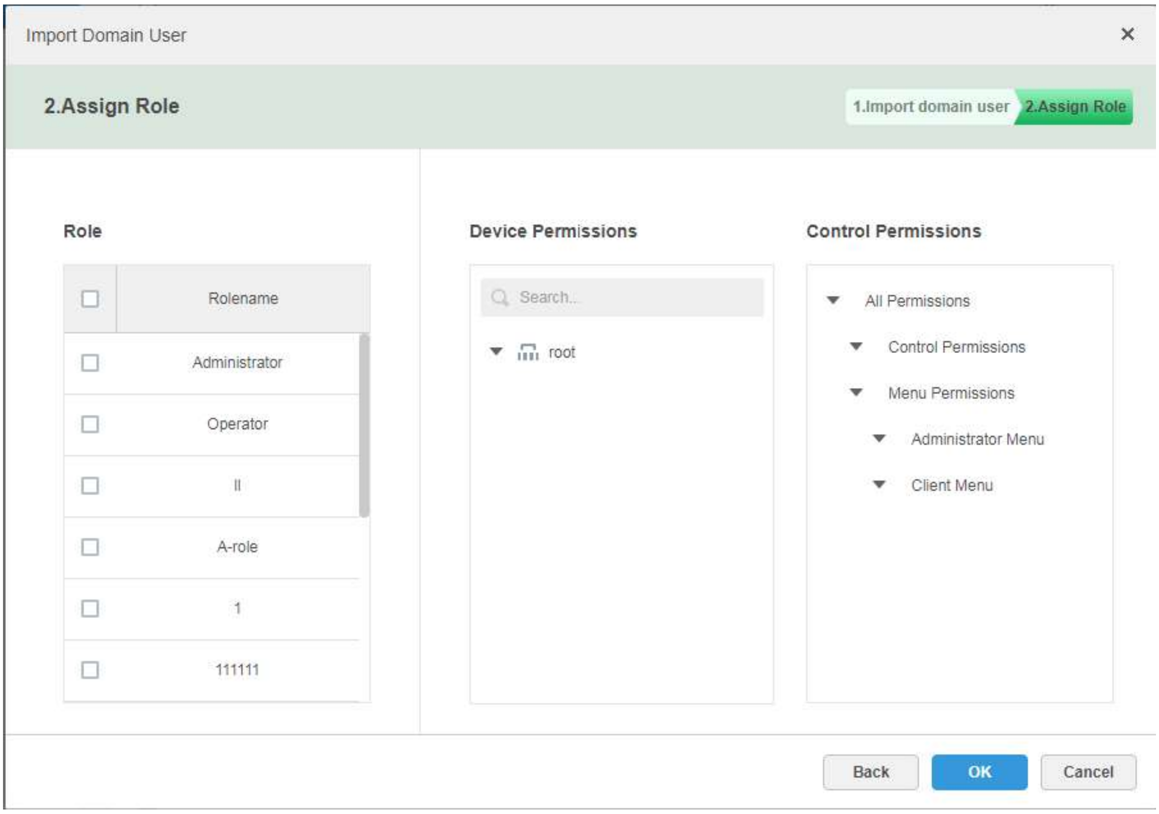
Step 3 Select the users which need to be imported from the acquired domain users.

You can search users by entering key words in the box.

Step 4 Click **Next**.

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

Figure 4-14 Import domain user



Import Domain User ×

2.Assign Role

1.Import domain user 2.Assign Role

Role

□	Rolename
□	Administrator
□	Operator
□	ll
□	A-role
□	1
□	111111

Device Permissions

Search...

▼ root

Control Permissions

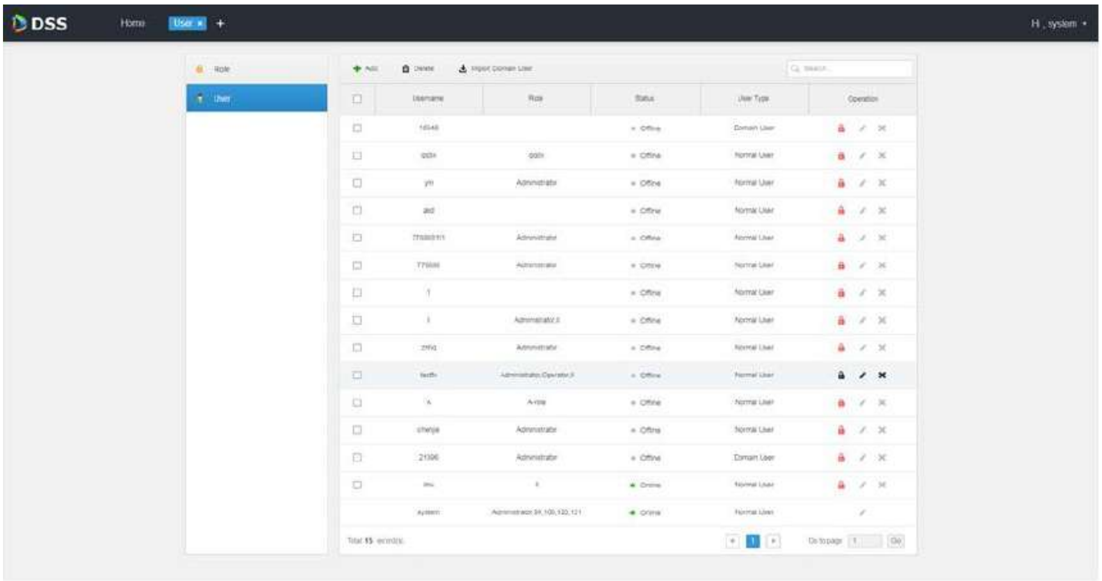
▼ All Permissions
- ▼ Control Permissions
- ▼ Menu Permissions
  - ▼ Administrator Menu
  - ▼ Client Menu

Back OK Cancel

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 4-15.

Figure 4-15 Imported domain user



□	Username	Role	Status	User Type	Operation
□	16548		Offline	Domain User	
□	gsdx	gsdx	Offline	Normal User	
□	yin	Administrator	Offline	Normal User	
□	asd		Offline	Normal User	
□	[illegible]	Administrator	Offline	Normal User	
□	77888	Administrator	Offline	Normal User	
□	1		Offline	Normal User	
□	i	Administrator,3	Offline	Normal User	
□	zhfq	Administrator	Offline	Normal User	
□	testfn	Administrator,Operator,3	Offline	Normal User	
□	A	A-role	Offline	Normal User	
□	chenjie	Administrator	Offline	Normal User	
□	21306	Administrator	Offline	Domain User	
□	[illegible]	3	Online	Normal User	
	system	Administrator,34,100,120,121	Online	Normal User	

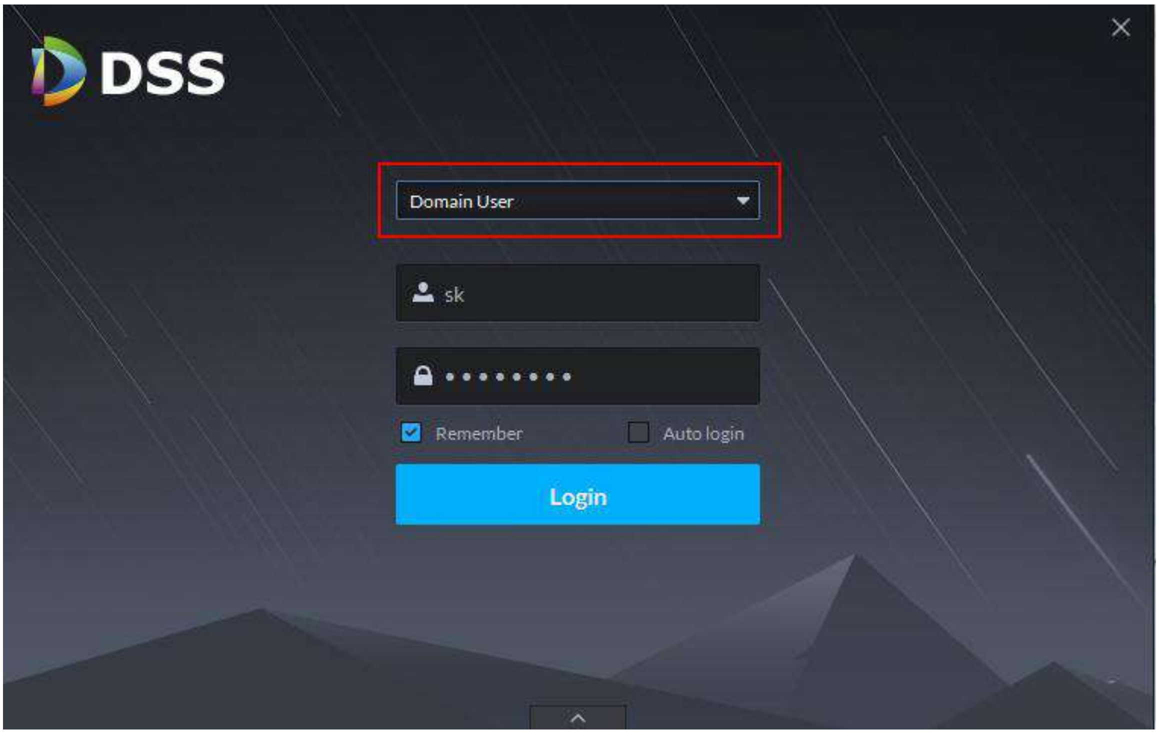
Total 15 record(s)   Go to page 1 Go

4.4.3.4 Logging in Domain User

Domain user logs in platform. Client login is introduced as an example in the following chapter.

Step 1 Select **Domain User** in the drop-down box of **User Type** on the client login interface. See Figure 4-16.

Figure 4-16 Select domain user type



Domain User

sk

●●●●●●●●

☑ Remember   □ Auto login

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.

4.5 Adding Device

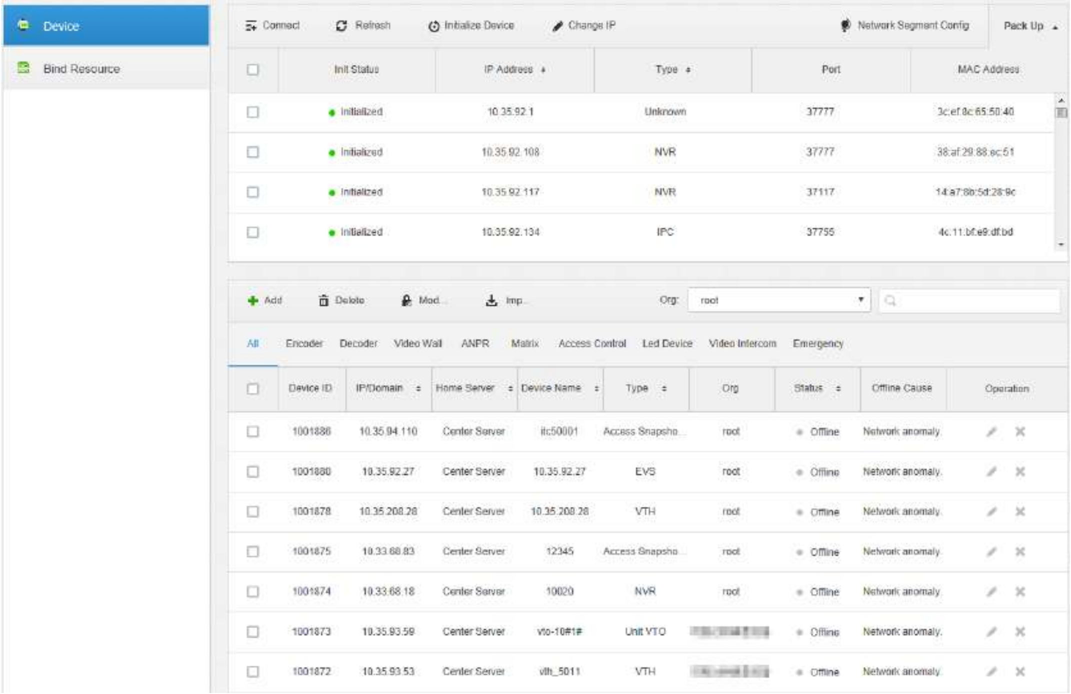
You can add different types of devices according to different business requirements. These devices include encoder, decoder, large display, matrix, ANPR device, access control, LED, video intercom and emergency assistance device. In this chapter, it takes adding encoder as an example to introcude configuration.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

4.5.1 Adding Device Manually

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

The **Device** interface is displayed. See Figure 4-17.

Figure 4-17 Device



□	Init Status	IP Address	Type	Port	MAC Address
□	● Initialized	10.35.92.1	Unknown	37777	3c:ef:8c:65:50:40
□	● Initialized	10.35.92.108	NVR	37777	38:af:29:88:ec:51
□	● Initialized	10.35.92.117	NVR	37117	14:a7:8b:5d:28:9c
□	● Initialized	10.35.92.134	IPC	37755	4c:11:bf:e9:df:bd

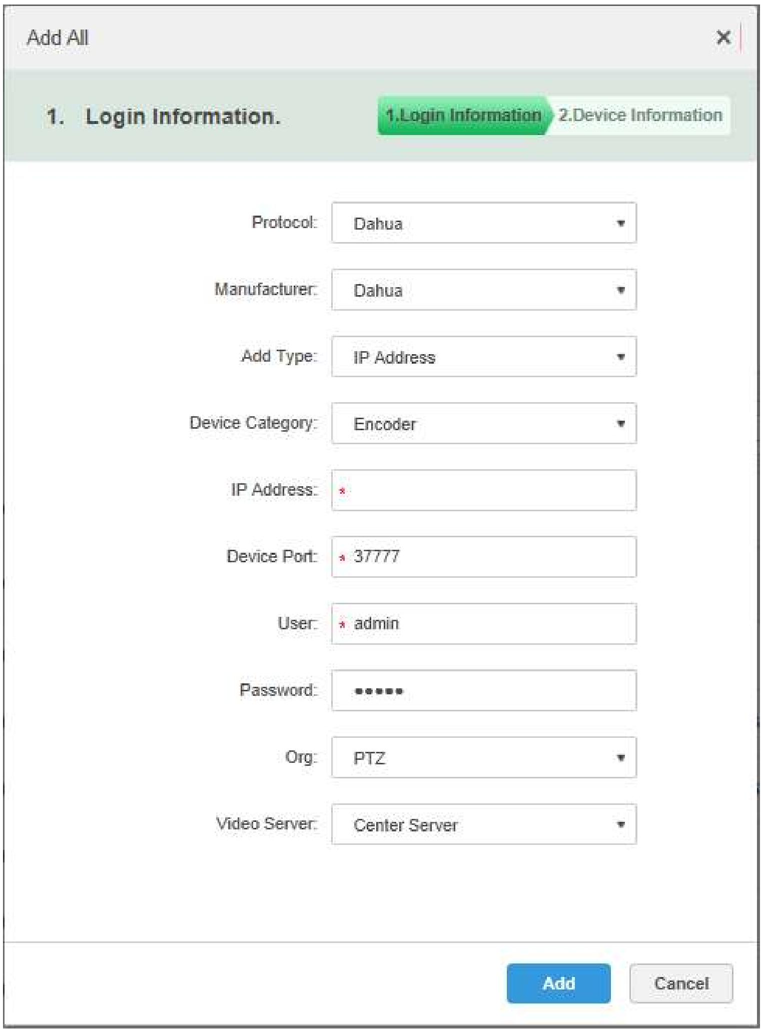
Org: root

□	Device ID	IP/Domain	Home Server	Device Name	Type	Org	Status	Offline Cause	Operation
□	1001886	10.35.94.110	Center Server	itc50001	Access Snapsho...	root	● Offline	Network anomaly.	✎ ✕
□	1001880	10.35.92.27	Center Server	10.35.92.27	EVS	root	● Offline	Network anomaly.	✎ ✕
□	1001878	10.35.208.28	Center Server	10.35.208.28	VTH	root	● Offline	Network anomaly.	✎ ✕
□	1001875	10.33.68.83	Center Server	12345	Access Snapsho...	root	● Offline	Network anomaly.	✎ ✕
□	1001874	10.33.68.18	Center Server	10020	NVR	root	● Offline	Network anomaly.	✎ ✕
□	1001873	10.35.93.59	Center Server	vto-10#1#	Unit VTO	[redacted]	● Offline	Network anomaly.	✎ ✕
□	1001872	10.35.93.53	Center Server	vth_5011	VTH	[redacted]	● Offline	Network anomaly.	✎ ✕

Step 2 Click **Add**.

The interface of **Login Information** is shown in Figure 4-18.

Figure 4-18 Login information



1. Login Information.

Protocol: Dahua

Manufacturer: Dahua

Add Type: IP Address

Device Category: Encoder

IP Address: *

Device Port: * 37777

User: * admin

Password: •••••

Org: PTZ

Video Server: Center Server

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

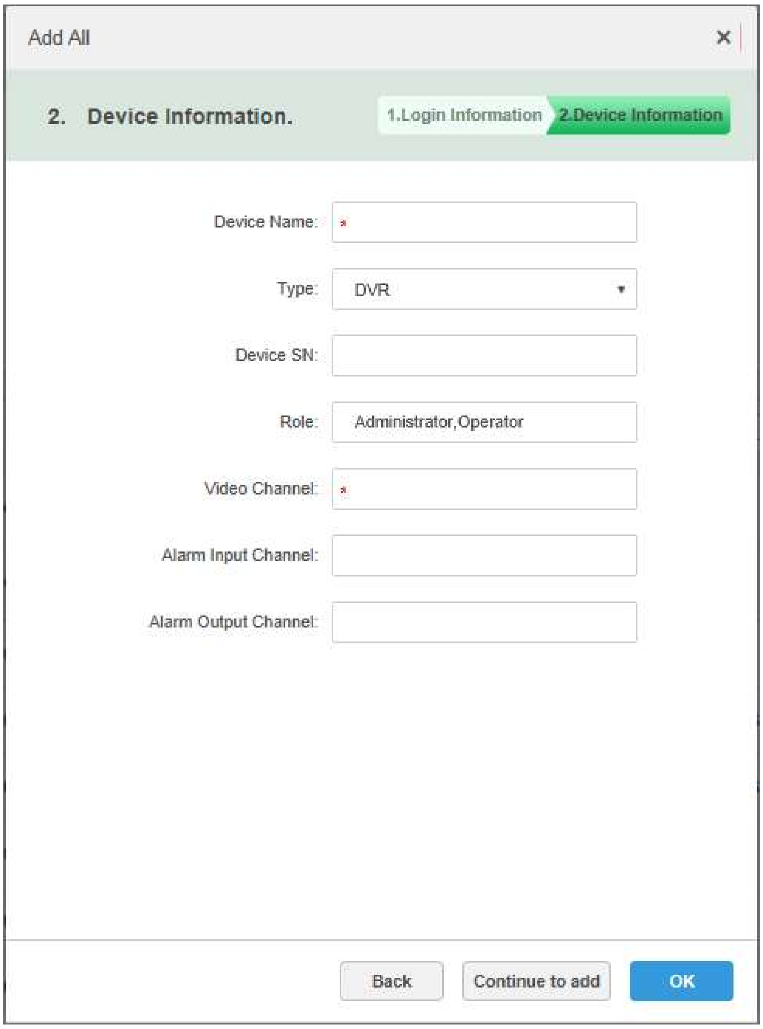
Select different **Protocol**, it will configure different parameters, please refer to the interface for more details.

- 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 4-19.

Figure 4-19 Device information



Add All

2. Device Information.

Device Name: *

Type: DVR

Device SN:

Role: Administrator,Operator

Video Channel: *

Alarm Input Channel:

Alarm Output Channel:

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

Step 6 Click **OK**.

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

4.5.2 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 **New Tab** interface.

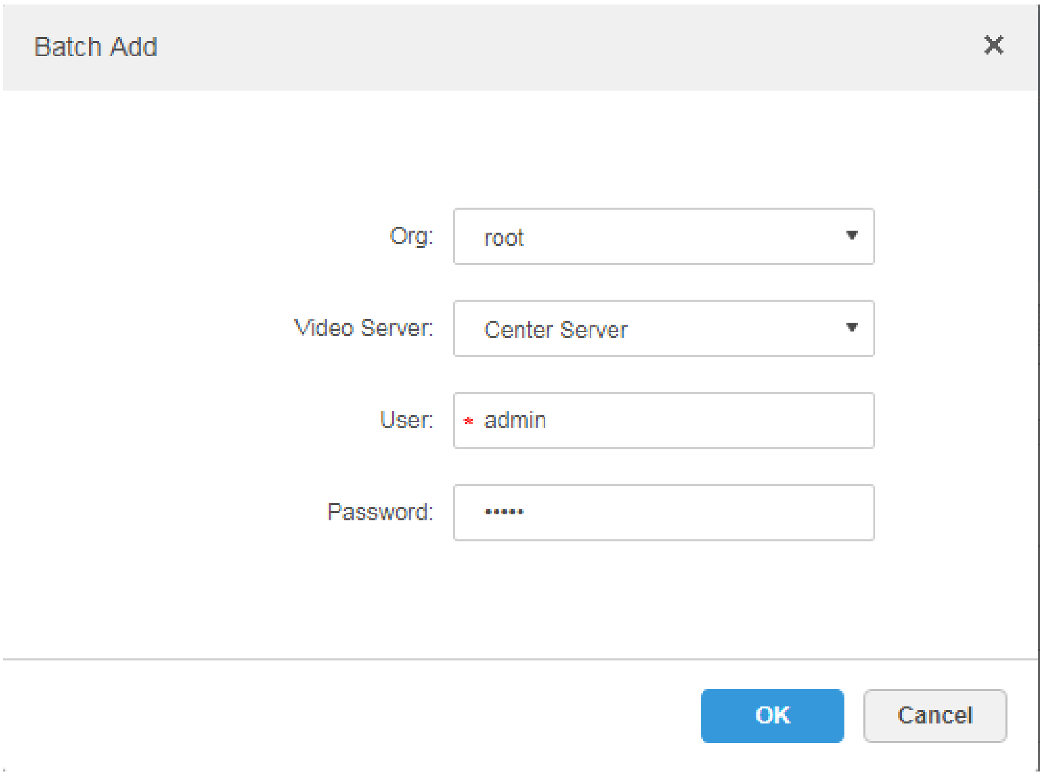
Step 2 Click **Search Again** on the **Device** interface.

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

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

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

Figure 4-20 Batch add



Batch Add

Org: root

Video Server: Center Server

User: * admin

Password: •••••

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

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

Step 5 Click **OK**.

The system will add the devices into corresponding organization.

4.5.3 Importing Video Intercom Device

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

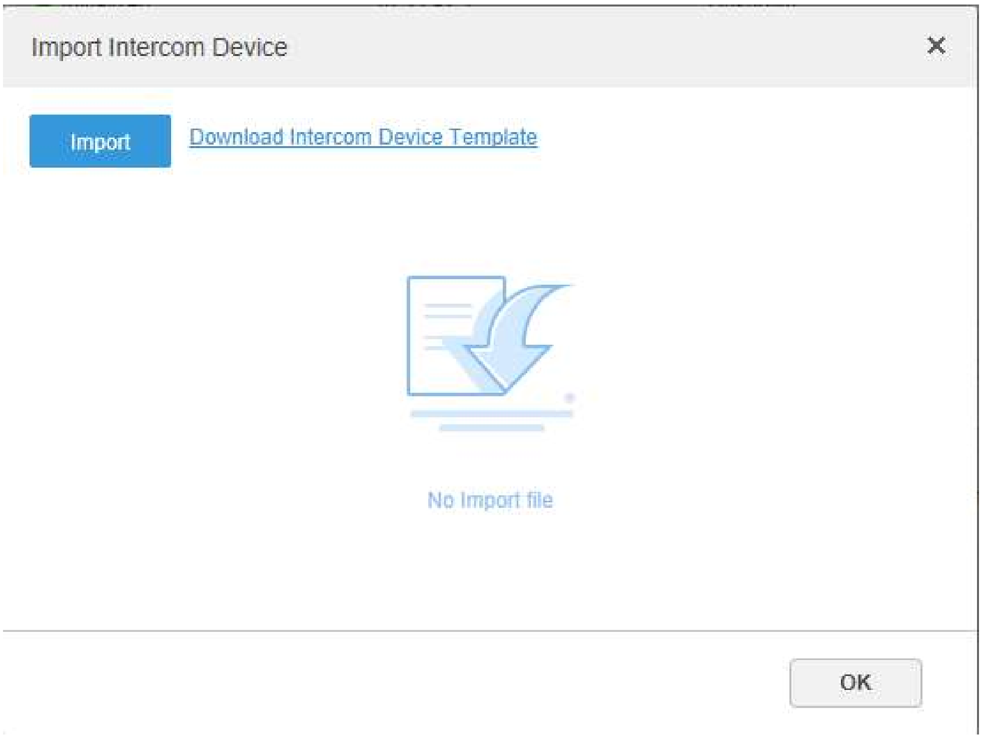
Step 1 Click + and select **Device** on the interface of **New Tab.**

The device management interface is displayed.

Step 2 Click **Import**.

The interface of Import Intercom Device is displayed. See Figure 4-21.

Figure 4-21 Import intercom device



Import Intercom Device

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

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

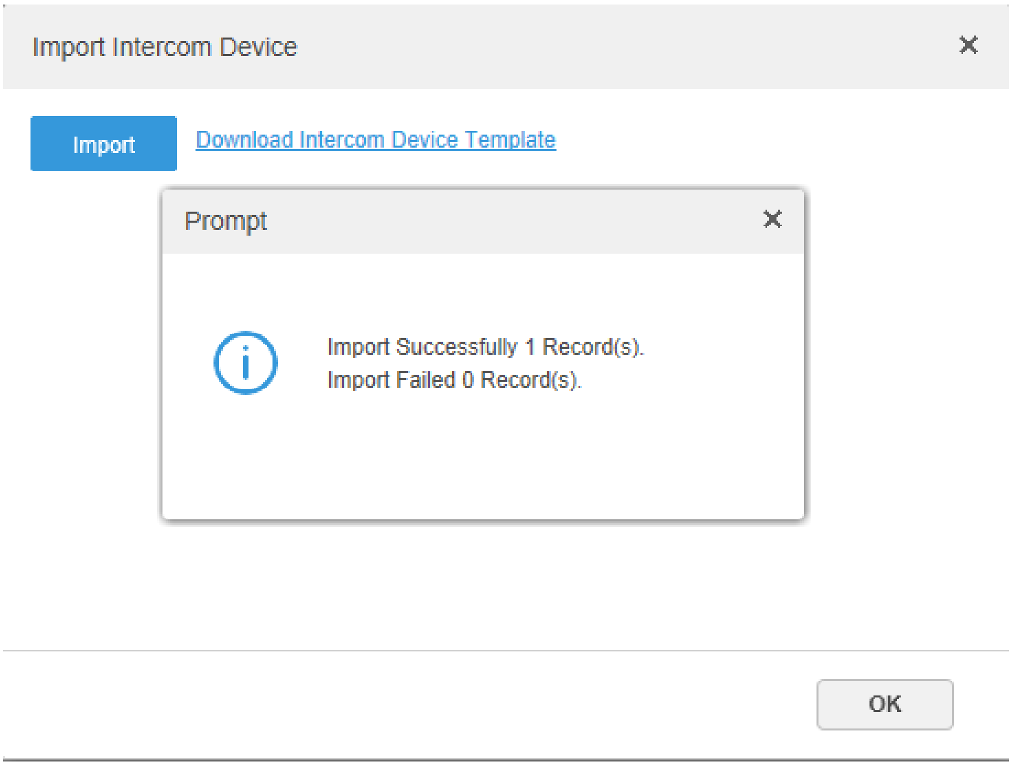
Step 5 Click **Import** and select the completed template according to interface tips.

See Figure 4-22 for import progress and result. You can view the added device in the device list.

📖

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

Figure 4-22 Import intercom device result



Import Successfully 1 Record(s).
Import Failed 0 Record(s).

Step 6 Click ✕ and close the prompt box.

Step 7 Click **OK**.

4.5.4 Editing Device

You need to edit device after adding devices, and set relevant channel info.

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

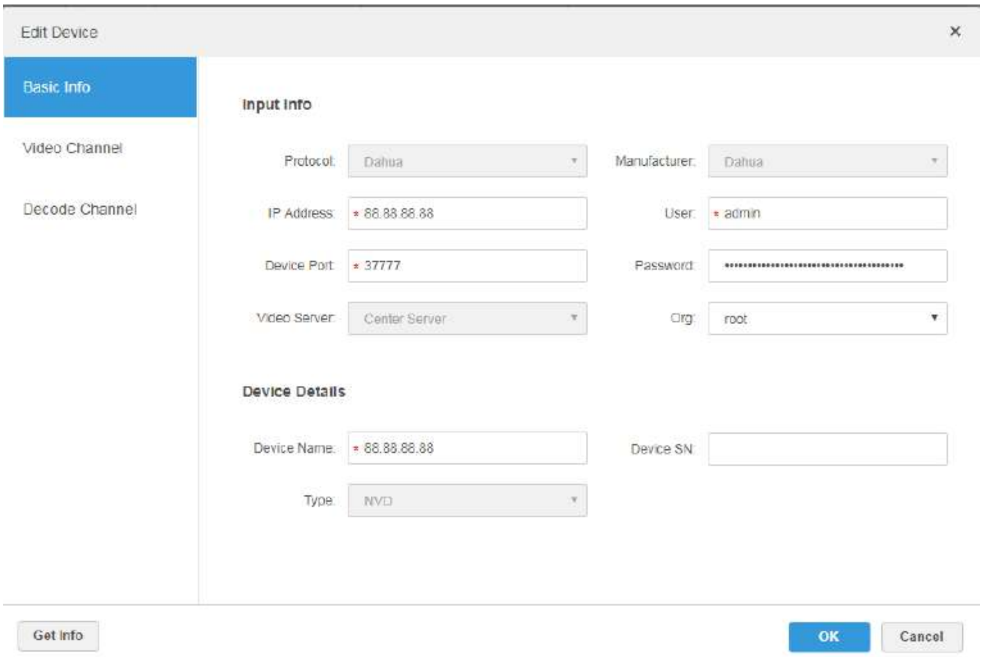
Step 2 Click the corresponding ✎ of device list.

The system displays the interface of **Edit Device**. See Figure 4-23.

📖

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

Figure 4-23 Edit device



Input Info

Protocol:	Dahua	Manufacturer:	Dahua
IP Address:	* 88.88.88.88	User:	* admin
Device Port:	* 37777	Password:	••••••••••••••••••••••••••••••••••••
Video Server:	Center Server	Org:	root

Device Details

Device Name:	* 88.88.88.88	Device SN:	
Type:	NVD		

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

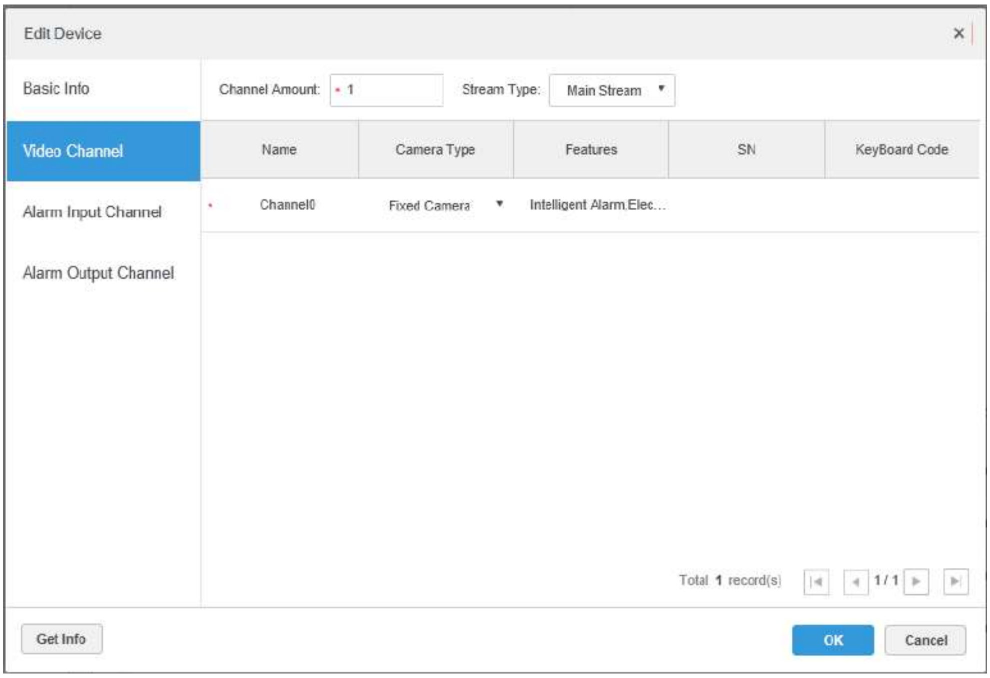
Step 4 Click **Video Channel** tab, set the device channel name, channel function, camera type, SN, keyboard code and face function.

The interface is shown in Figure 4-24.

📖

- Device channel capacity set currently includes smart alarm, fisheye dewarp, face snapshot and target snapshot. You can select according to connected camera performance and requirement. For example, if you need to use target detection function of connected camera, then select channel capacity set as **Target Snapshot**.
- Device channel capacity is not compatible with third party manufacturer.

Figure 4-24 Modify video channel



Channel Amount: * 1 Stream Type: Main Stream

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

Total 1 record(s) 1 / 1

Step 5 Click the tab of **Alarm Input Channel**, configure channel name and alarm type of alarm input. See Figure 3-25.

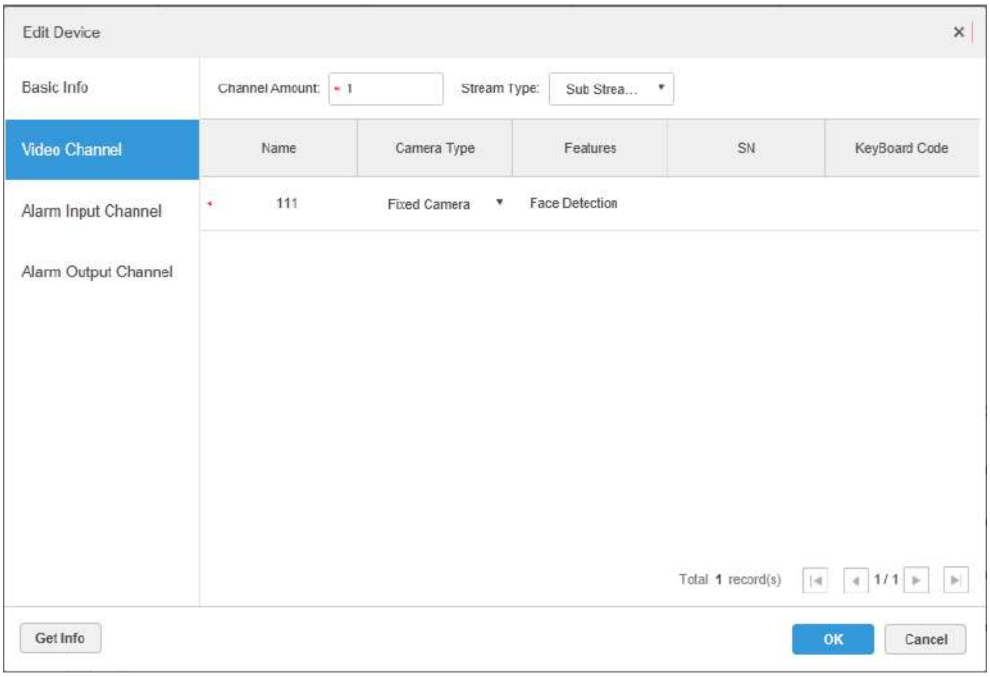
Please skip the step only when added devices need to be configured during alarm input.

- 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 **Alarm Type** drop-down list. Click **Add** to add new alarm type. It supports max 30 custom newly-added alarm types.

  Custom alarm supports modification and deletion.

  - If custom alarm type is used by alarm plan, then it is not allowed to deleted but modified.
  - 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.

Figure 4-25 Configure alarm input channel info



Channel Amount: * 1

Stream Type: Sub Strea...

	Name	Camera Type	Features	SN	KeyBoard Code
*	111	Fixed Camera	Face Detection		

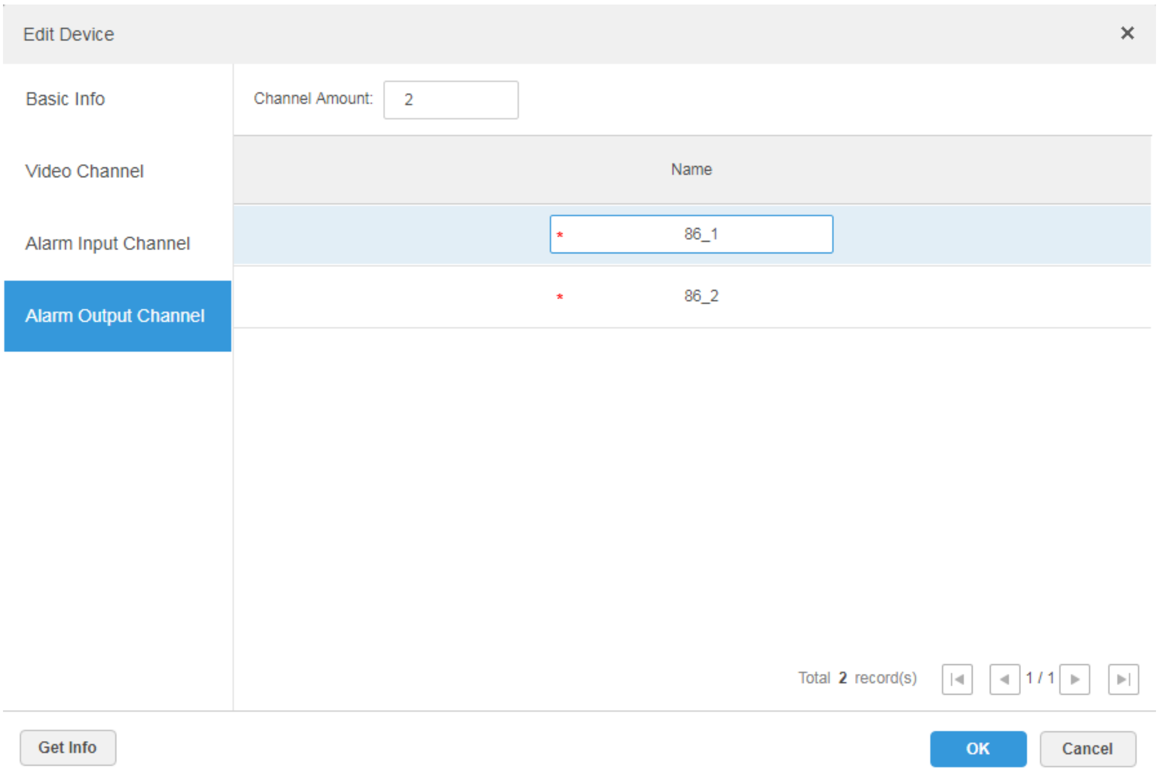
Total 1 record(s) 1 / 1

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.

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

Figure 4-26 New alarm type



Channel Amount: 2

Name
* 86_1
* 86_2

Total 2 record(s) 1 / 1

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

4.5.5 Binding Resource

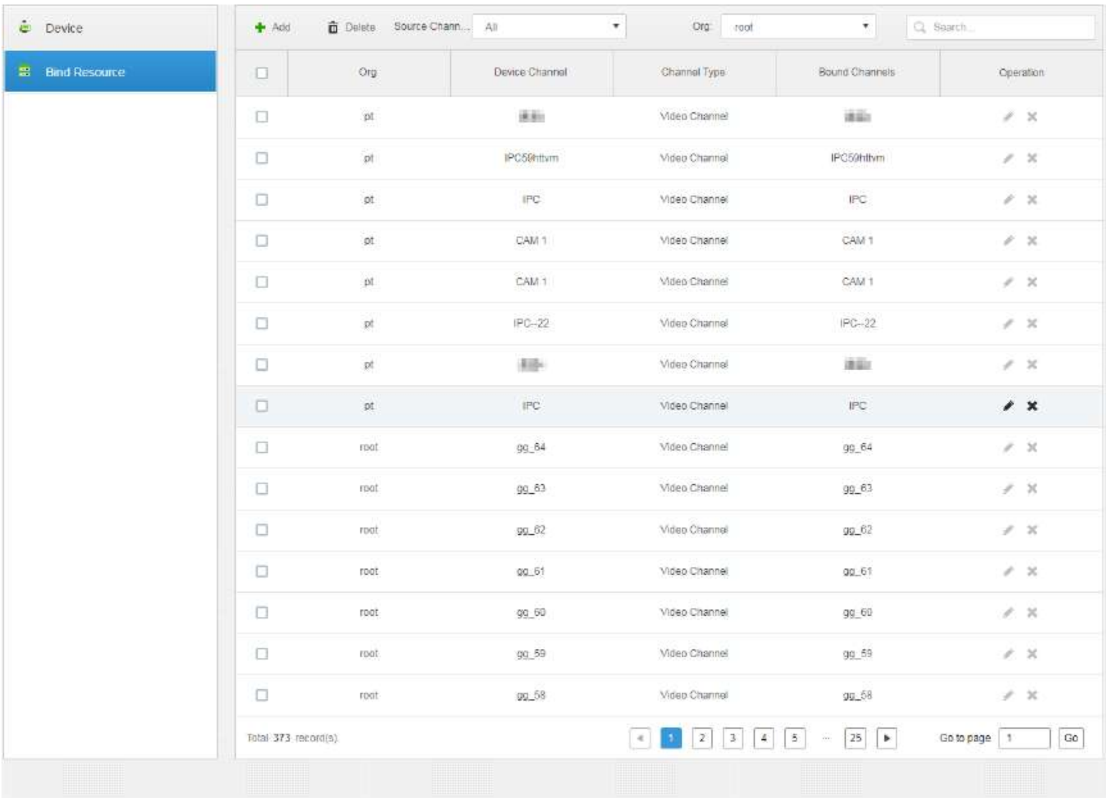
The platform supports setting video channel, alarm input channel, ANPR channel, POS channel, face channel, access control channel and video channel resource binding. It can check bound video via resource bind for businesses such as map, alarm, commercial intelligence and face.

Adding Resource Bind

Step 1 Click **Resource Bind**.

The system displays the **Resource Bind** interface. See Figure 4-27.

Figure 4-27 Bind resource



Source Chann... All

Org: root

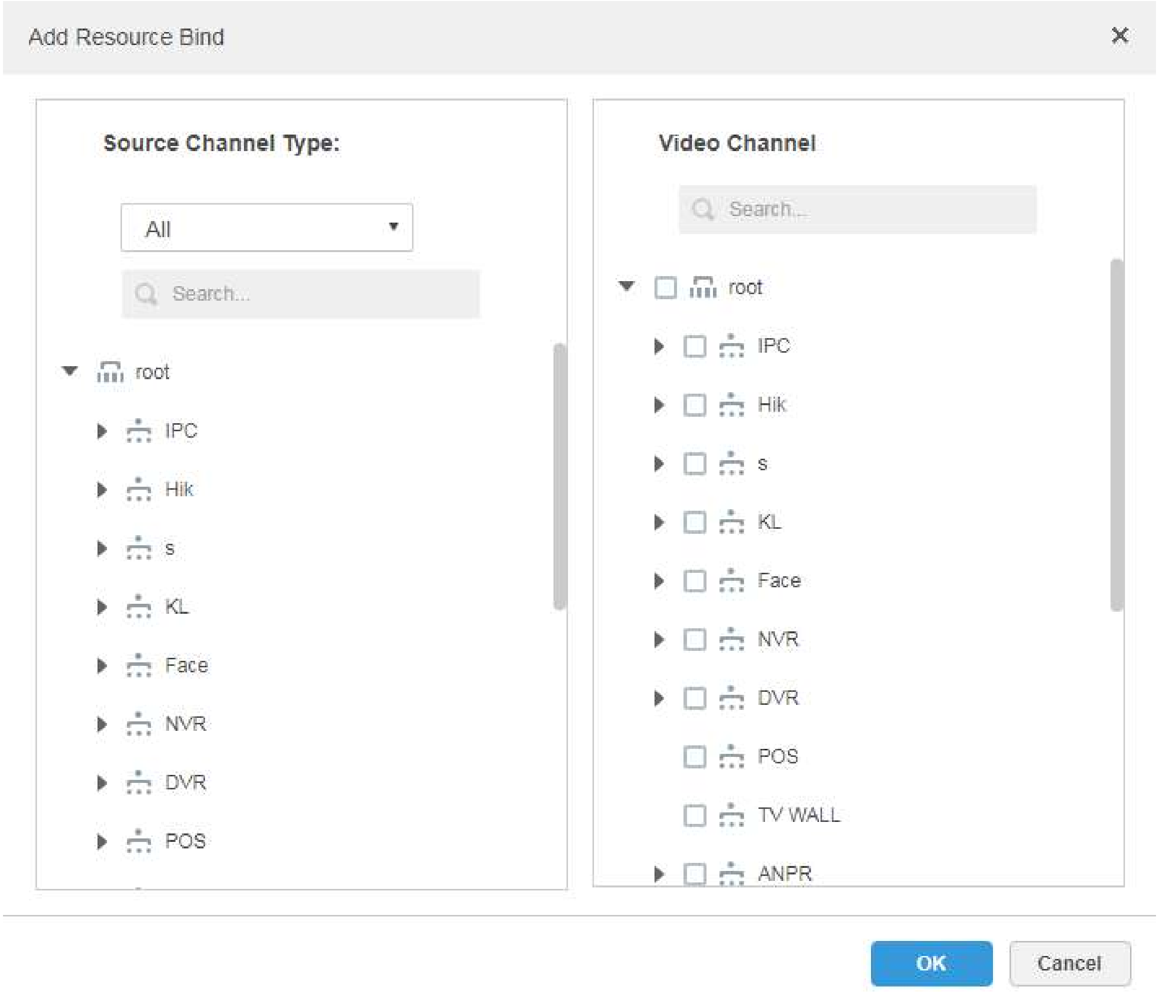
□	Org	Device Channel	Channel Type	Bound Channels	Operation
□	pt	[redacted]	Video Channel	[redacted]	✎ ✕
□	pt	IPC59httvm	Video Channel	IPC59httvm	✎ ✕
□	pt	IPC	Video Channel	IPC	✎ ✕
□	pt	CAM 1	Video Channel	CAM 1	✎ ✕
□	pt	CAM 1	Video Channel	CAM 1	✎ ✕
□	pt	IPC--22	Video Channel	IPC--22	✎ ✕
□	pt	[redacted]	Video Channel	[redacted]	✎ ✕
□	pt	IPC	Video Channel	IPC	✎ ✕
□	root	gg_64	Video Channel	gg_64	✎ ✕
□	root	gg_63	Video Channel	gg_63	✎ ✕
□	root	gg_62	Video Channel	gg_62	✎ ✕
□	root	gg_61	Video Channel	gg_61	✎ ✕
□	root	gg_60	Video Channel	gg_60	✎ ✕
□	root	gg_59	Video Channel	gg_59	✎ ✕
□	root	gg_58	Video Channel	gg_58	✎ ✕

Total 373 record(s)

Step 2 Click **Add**.

The interface of **Add Resource Bind** is displayed. See Figure 4-28.

Figure 4-28 Add resource bind



Source Channel Type: All

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

4.6 Configuring Record Plan

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

4.6.1 Configuring Storage Disk

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

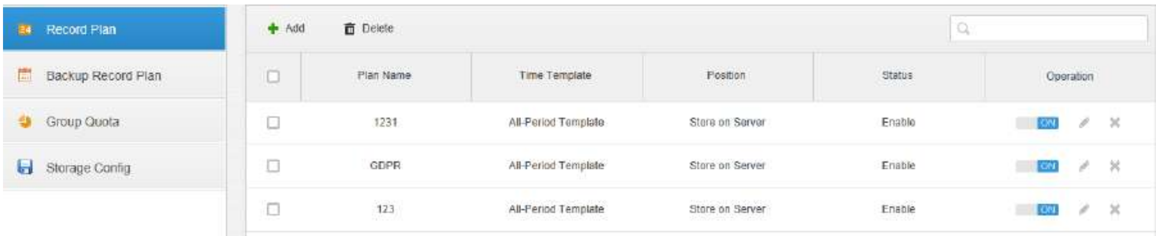
4.6.1.1 Configuring Net Disk

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

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

The system displays the interface of **Storage.** See Figure 4-29**.**

Figure 4-29 Record storage

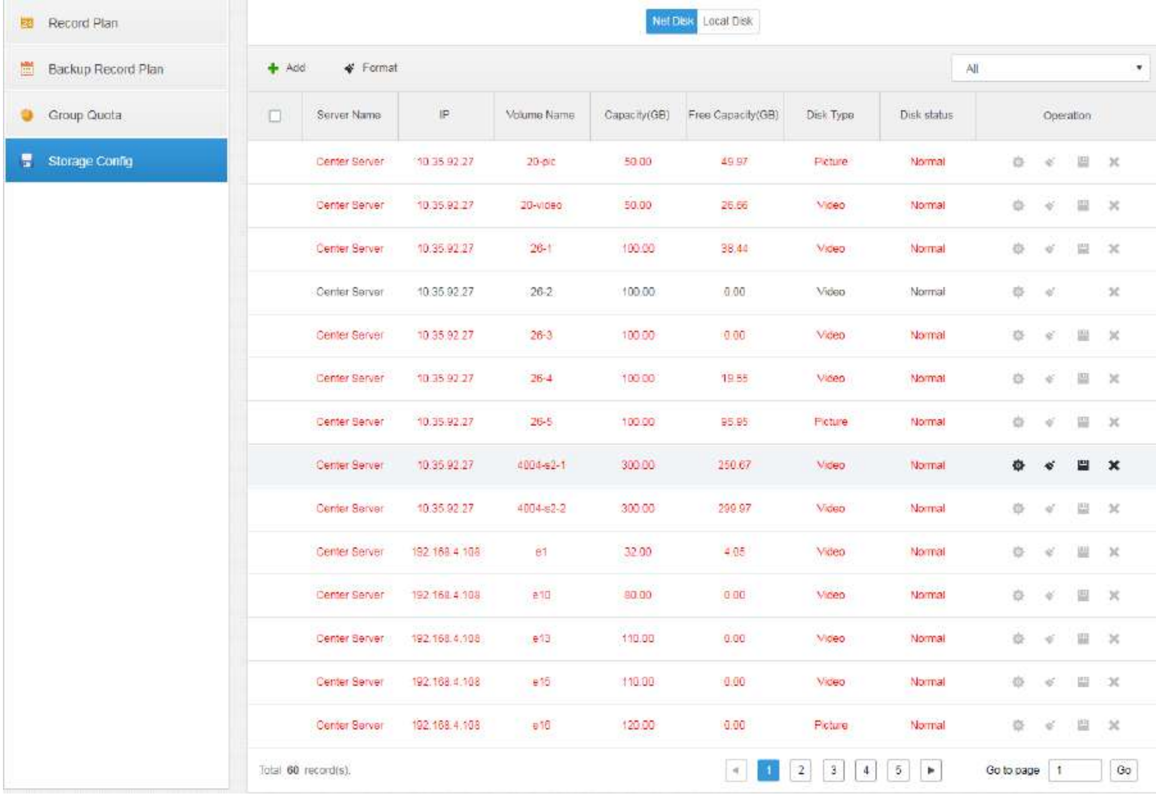


☐	Plan Name	Time Template	Position	Status	Operation
☐	1231	All-Period Template	Store on Server	Enable	ON
☐	GDPR	All-Period Template	Store on Server	Enable	ON
☐	123	All-Period Template	Store on Server	Enable	ON

Step 2 Select “**Storage Config** > **Net Disk**”

The system displays the interface of **Net Disk.** See Figure 4-30.

Figure 4-30 Net disk



☐	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	

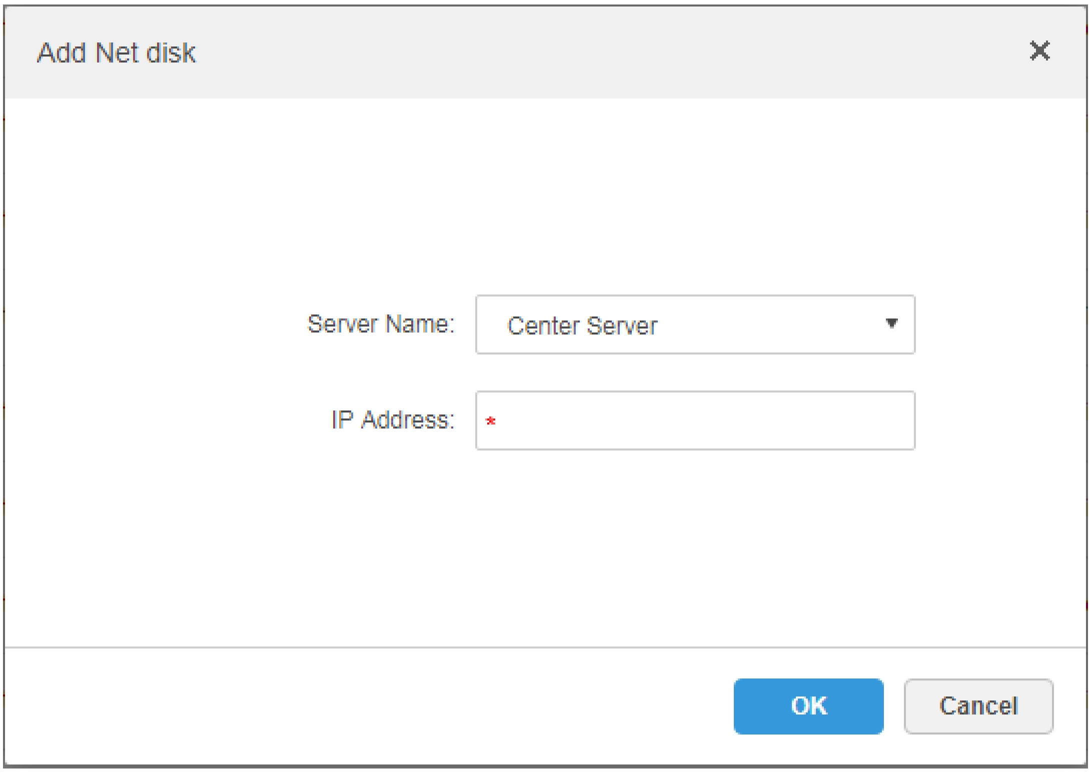
Total 60 record(s).

◂ 1 2 3 4 5 ▸ Go to page 1 Go

Step 3 Click **Add**.

The system displays the interface of **Add Net Disk**. See Figure 4-31.

Figure 4-31 Add net disk



Add Net disk

Server Name: Center Server

IP Address: *

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

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

Step 5 Select disk and click **Format** or click the 🖌 next to the disk 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.

📖

One user volume can only be used by one server at the same time. If the disk info of the list shows red, then it is already added and used by other server. Click 💾 and take the right to use, then the disk needs to be formatted. It will fail to take the right of use if task manager is enabled.

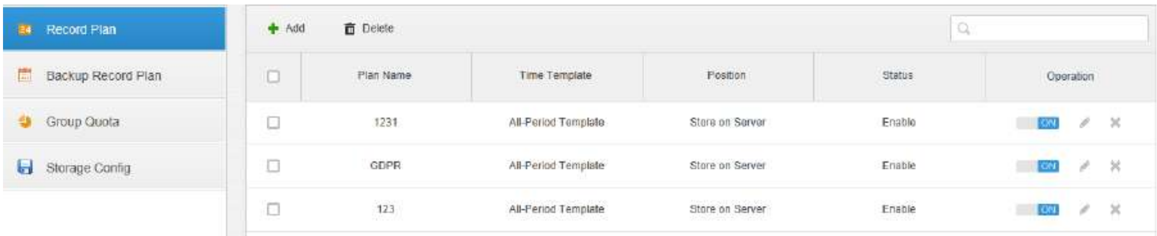
4.6.1.2 Configuring Local Disk

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

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

The system displays the interface of **Storage**. See Figure 4-32.

Figure 4-32 Storage

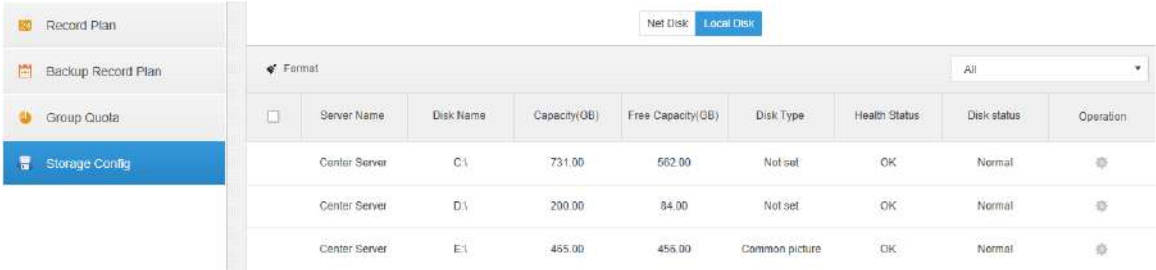


□	Plan Name	Time Template	Position	Status	Operation
□	1231	All-Period Template	Store on Server	Enable	ON
□	GDPR	All-Period Template	Store on Server	Enable	ON
□	123	All-Period Template	Store on Server	Enable	ON

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

The system displays the interface of **Local Disk**. See Figure 4-33.

Figure 4-33



□	Server Name	Disk Name	Capacity(GB)	Free Capacity(GB)	Disk Type	Health Status	Disk status	Operation
	Center Server	C:\	731.00	562.00	Not set	OK	Normal	
	Center Server	D:\	200.00	84.00	Not set	OK	Normal	
	Center Server	E:\	455.00	456.00	Common picture	OK	Normal	

Step 3 Configure local disk.

- Set disk type.

  Click and configure disk type according to interface prompt. Different type of disk stores different data.
- Format disk. Only external disk supports formatting.

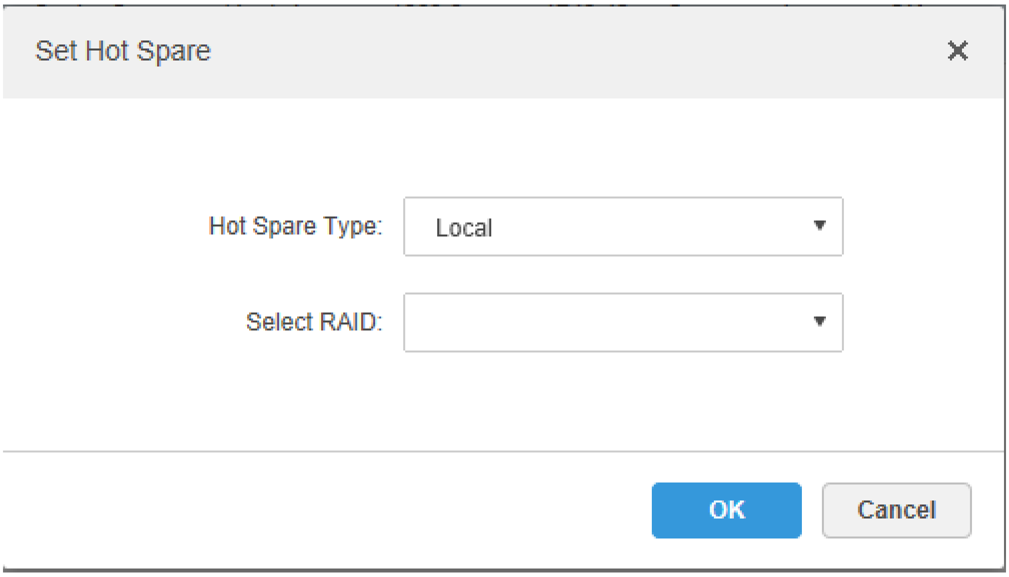
  All the data in the disk will be deleted after disk formatting. Please use the function with care.

  Select disk and click **Format**, or click next to disk info and format the disk according to interface prompt and configure disk type. Only external disk supports formatting.
- Hot spare

  Set disk as backup disk of RAID group, replace the damaged disk of RAID group.

  Click and set parameters, click OK. See Figure 4-34.

Figure 4-34 Set hot spare



Hot Spare Type: Local

Select RAID:

Table 4-2 Hot spare parameter description

Parameter	Description
Hot Spare Type	Supported types include: ● Local Set disk as backup disk of designated RAID group. Recreate system immediately when disk error happens in the RAID group. ● Global Set disk as backup disk of all RAID group. Recreate system immediately when disk error happens in any RAID group.

Configuring RAID Group

The platform supports creating RAID group, and provides higher storage performance than single disk and data redundancy technology.

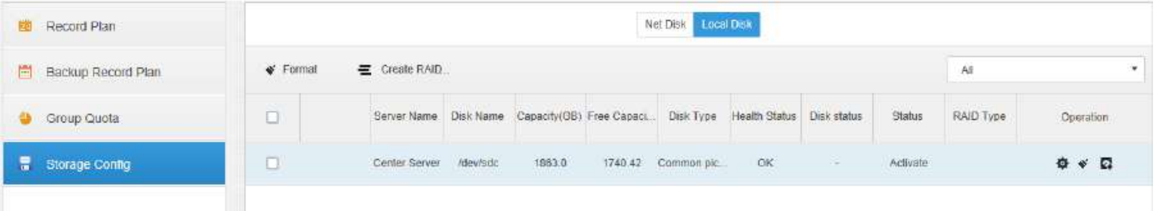
Step 1 Click ➕, and select **Storage** on the interface of **New Tab**.

The interface of **Storage** is displayed.

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

The interface of **Local Disk** is displayed. See Figure 4-35.

Figure 4-35 Local disk

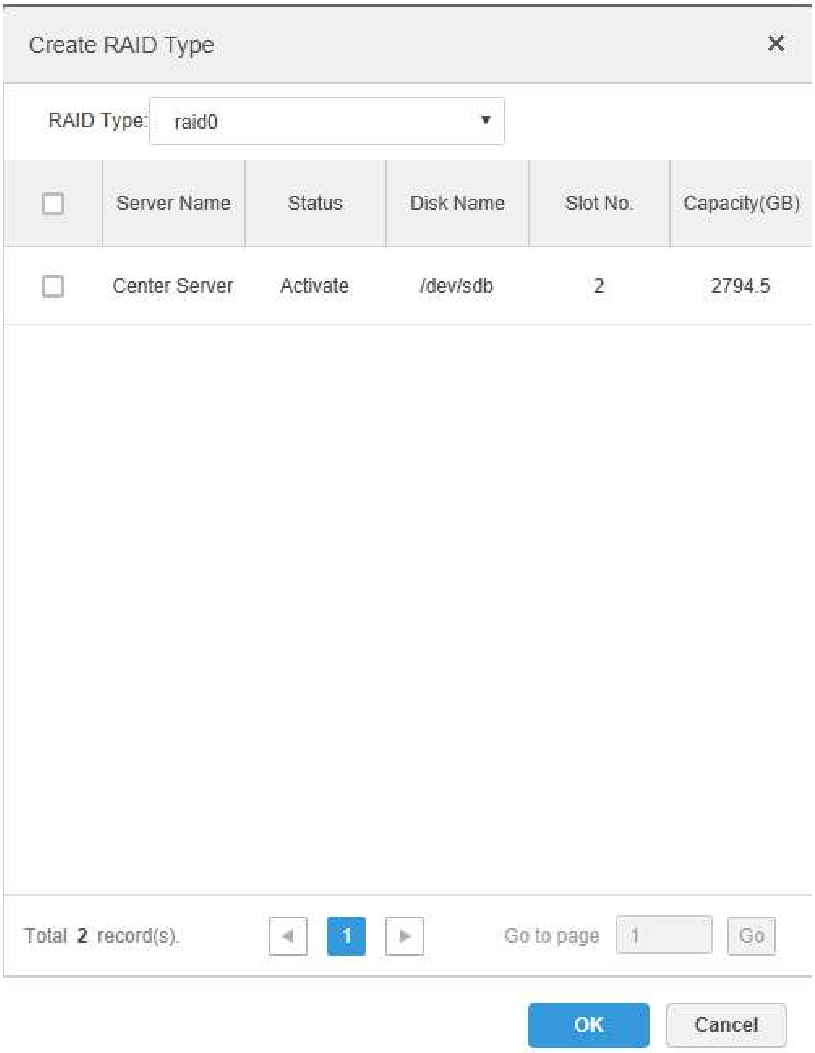


□		Server Name	Disk Name	Capacity(GB)	Free Capaci...	Disk Type	Health Status	Disk status	Status	RAID Type	Operation
□		Center Server	/dev/sdc	1863.0	1740.42	Common pic...	OK	-	Activate		⚙

Step 3 Click **Create RAID**.

The interface of **Create RAID** is displayed. See Figure 4-36.

Figure 4-36 Create RAID



Create RAID Type ×

RAID Type: raid0

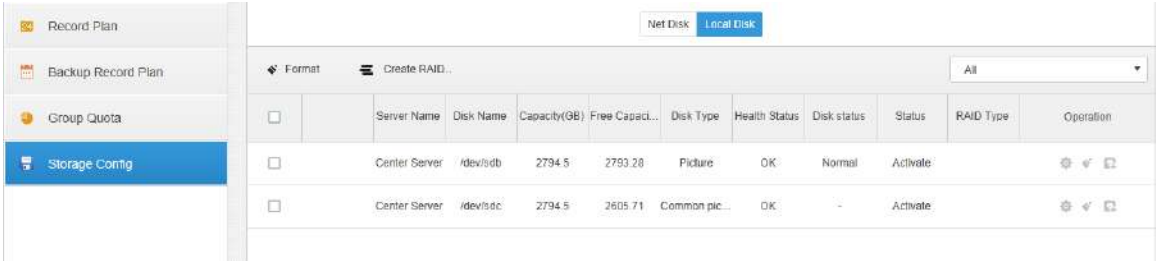
□	Server Name	Status	Disk Name	Slot No.	Capacity(GB)
□	Center Server	Activate	/dev/sdb	2	2794.5

Total 2 record(s).

Step 4 Select **RAID Type**, select disk and click **OK**.

The system displays the created RAID group info. See Figure 4-37.

Figure 4-37 RAID group info



□		Server Name	Disk Name	Capacity(GB)	Free Capaci...	Disk Type	Health Status	Disk status	Status	RAID Type	Operation
□		Center Server	/dev/sdb	2794.5	2793.28	Picture	OK	Normal	Activate		
□		Center Server	/dev/sdc	2794.5	2605.71	Common pic...	OK	-	Activate		

Step 5 Configure RAID group.

- Set disk type.

  Click ⚙ and configure disk type according to interface prompt. Different type of disk stores different data.

- Format disk. Only external disk supports formatting.

⚠

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

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

- Delete RAID group

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

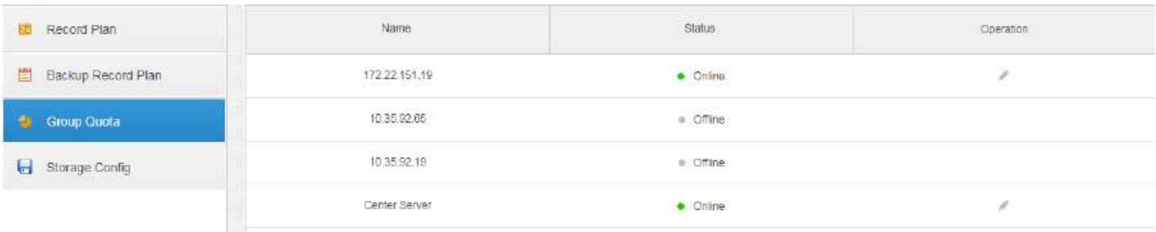
4.6.2 Setting Disk Group Quota

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

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

The system will display the online status of server. See Figure 4-38.

Figure 4-38 Group Quota

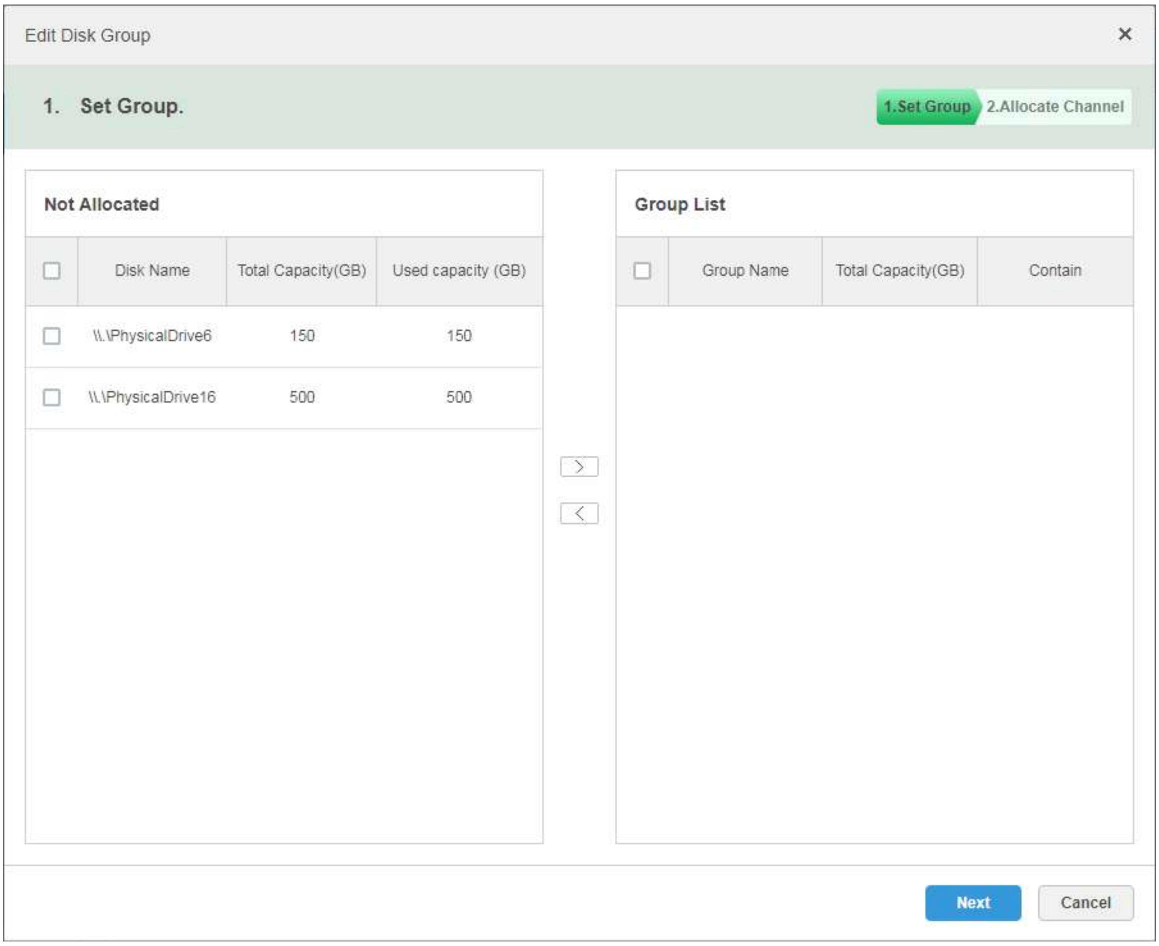


Name	Status	Operation
172.22.151.19	● Online	✎
10.35.92.65	● Offline	
10.35.92.19	● Offline	
Center Server	● Online	✎

Step 2 Click next to the Online status server.

The system will pop out the interface of **Edit Disk Group**. See Figure 4-39.

Figure 4-39 Edit disk group



Edit Disk Group ×

1. Set Group.

Not Allocated

□	Disk Name	Total Capacity(GB)	Used capacity (GB)
□	\\.\PhysicalDrive6	150	150
□	\\.\PhysicalDrive16	500	500

Group List

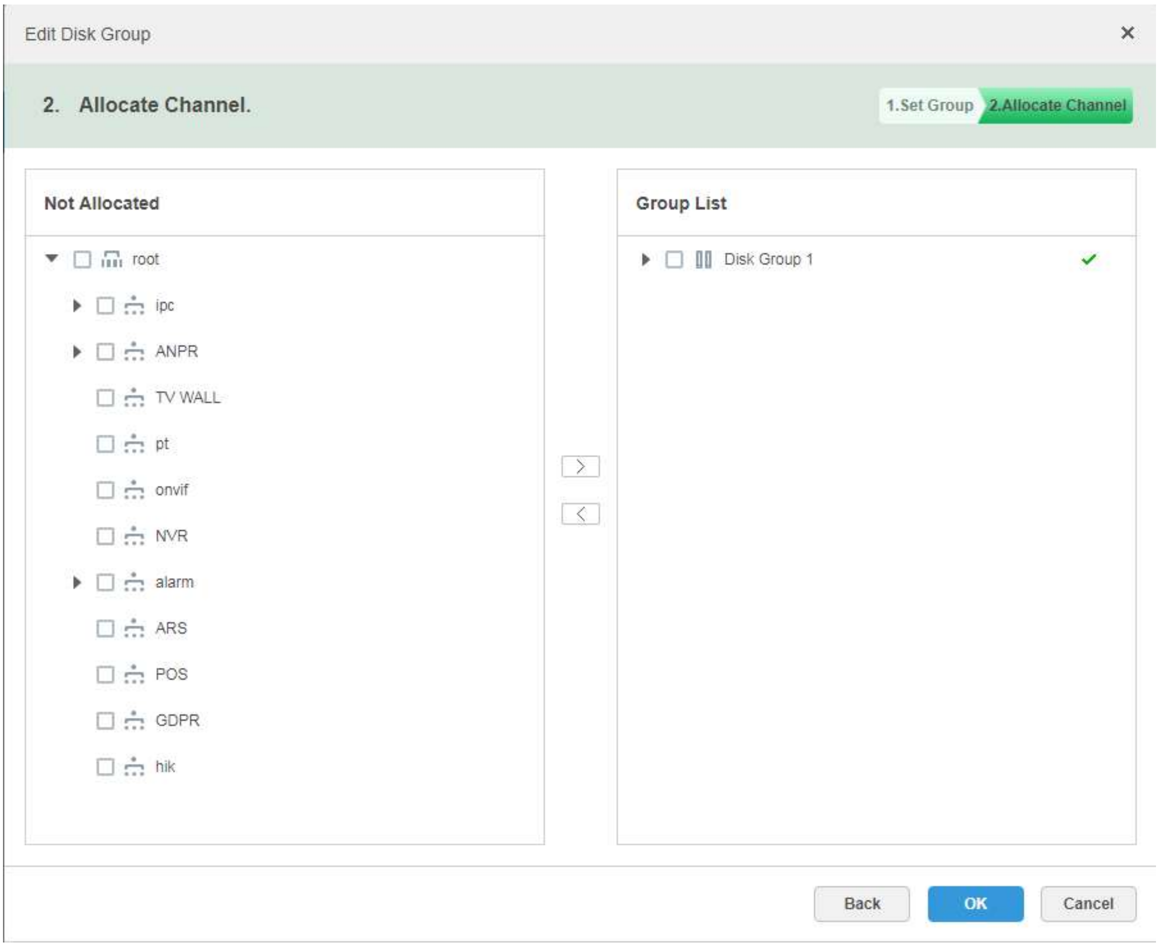
□	Group Name	Total Capacity(GB)	Contain

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 4-40.

Figure 4-40 Allocate channel



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

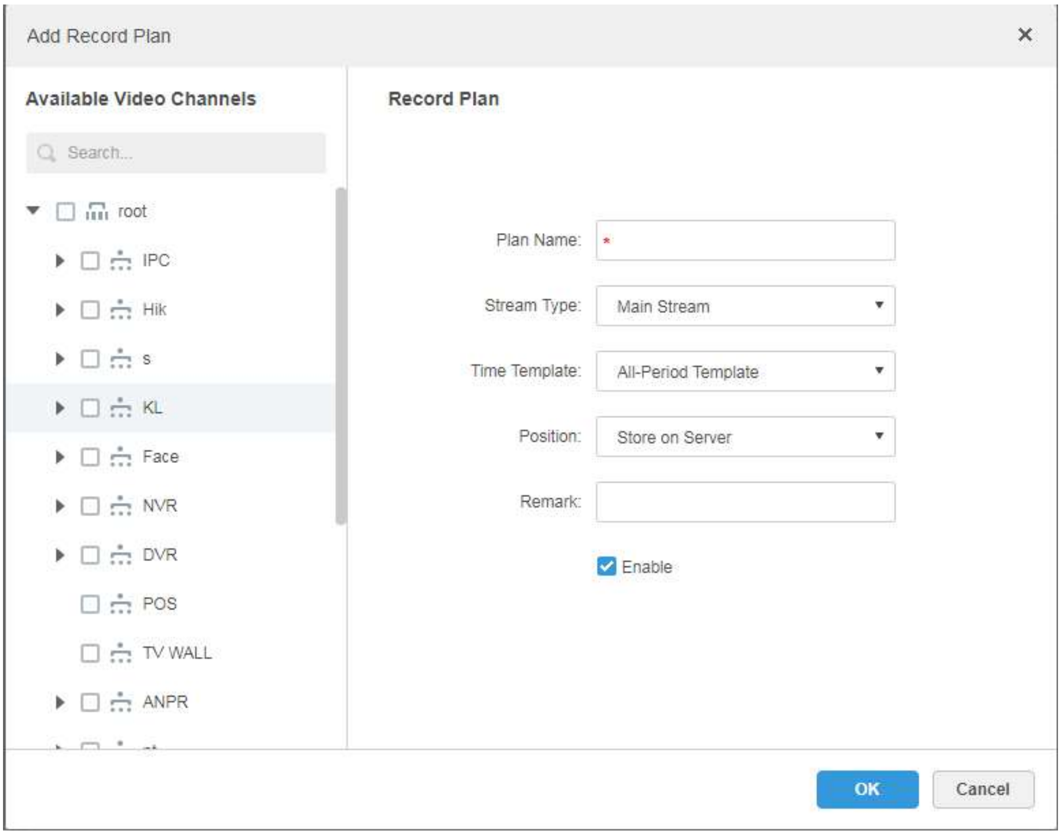
Step 6 Click **OK**.

4.6.3 Adding General Plan

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

It is to add record plan. See Figure 4-41.

Figure 4-41 Record plan



Add Record Plan ×

Available Video Channels

Search...

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

Record Plan

Plan Name: *

Stream Type: Main Stream

Time Template: All-Period Template

Position: Store on Server

Remark:

☑ Enable

OK Cancel

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

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

Step 3 Click **OK**.

Operations

- Enable/disable general plan

  In the operation column, ON means that the plan has been enabled, click the icon and it becomes OFF , and it means that the plan has been disabled.
- Edit General Plan

  Click ✎ of corresponding plan to edit the general plan.
- Delete General Plan
  - ◇ Select general plan, click 🗑 Delete to delete plans in batches.
  - ◇ Click ✖ of corresponding general plan to delete the individual general plan.

4.6.4 Adding Backup Record Plan

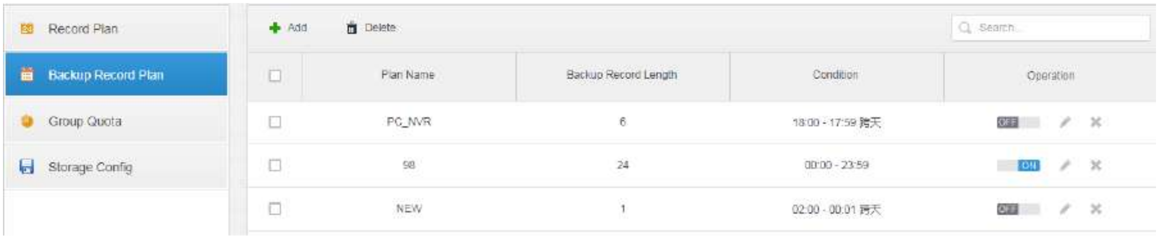
The system supports backup recording over the devices 3 days ago, the implementation time of backup plan can span the day, the condition of backup record is time/Wi-Fi optional.

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

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

The interface is shown in Figure 4-42.

Figure 4-42 Backup record plan



□	Plan Name	Backup Record Length	Condition	Operation
□	PC_NVR	6	18:00 - 17:59 跨天	OFF
□	58	24	00:00 - 23:59	ON
□	NEW	1	02:00 - 00:01 跨天	OFF

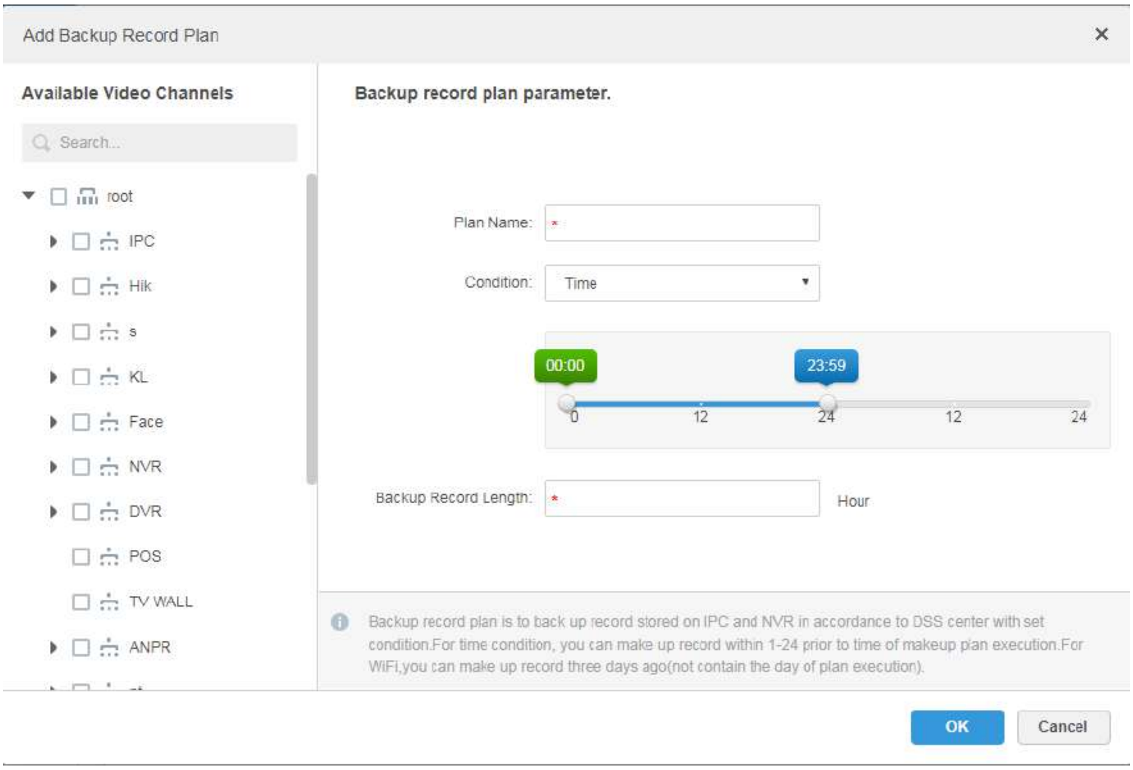
Step 2 Click **Add** to add backup plan.

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

Step 4 Set backup conditions.

- Take time as condition.

Figure 4-43 Time



Plan Name: *

Condition: Time

Backup Record Length: *

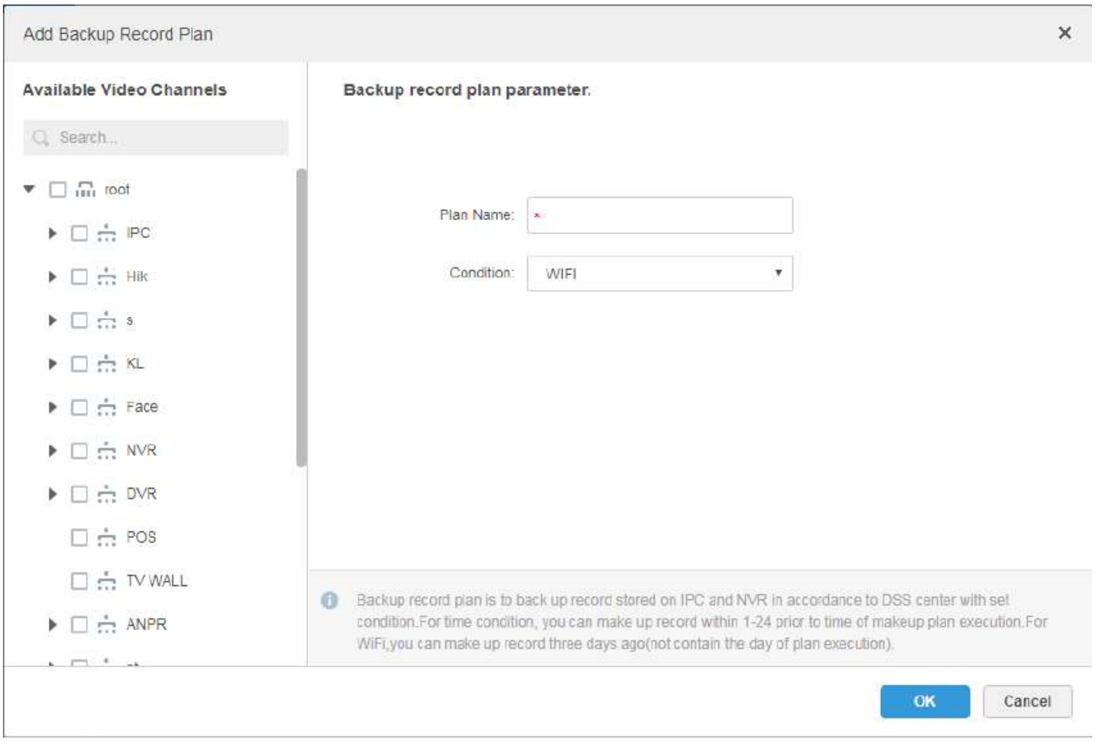
Backup record plan is to back up record stored on IPC and NVR in accordance to DSS center with set condition.For time condition, you can make up record within 1-24 prior to time of makeup plan execution.For WiFi,you can make up record three days ago(not contain the day of plan execution).

1) Select **Time** in the backup condition.
2) Drag time line and set the time period of backup record plan.
3) Enter backup record length, click **OK**.

The time range is 1-24 hours.

- Take Wi-Fi as condition.

Figure 4-44 Wi-Fi



Add Backup Record Plan

Backup record plan parameter.

Plan Name: *

Condition: WIFI

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

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, ON means that the plan has been enabled; click the icon and it becomes OFF, it means that the plan has been disabled.
- Edit backup record plan

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

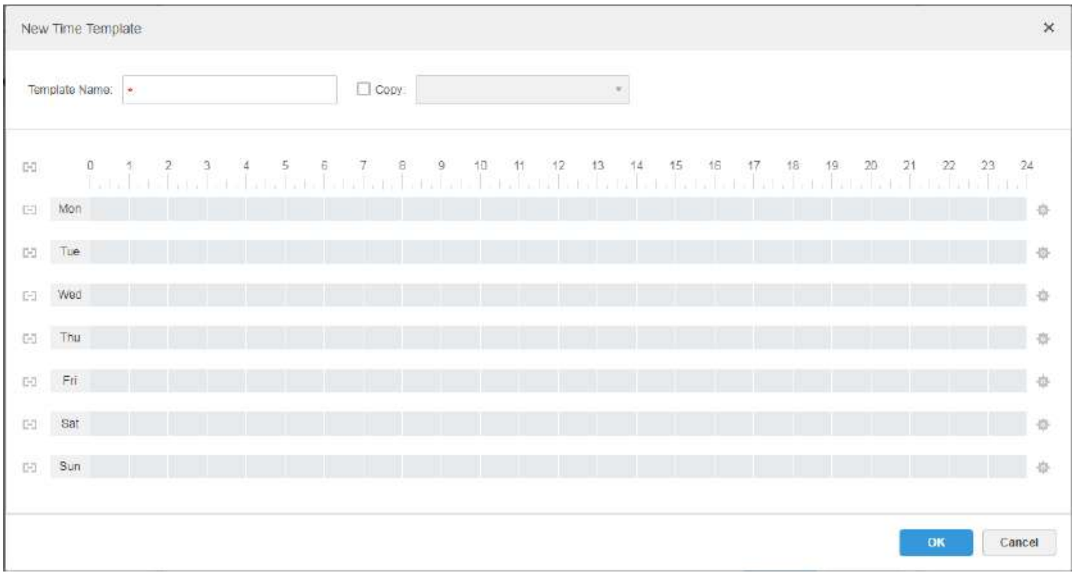
  ◇ Select backup record plan, click Delete to delete plan in batch.

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

4.6.5 Adding Time Template

Step 1 Select **New Time Template** in the drop-down box of **Time Template**.
The system displays the interface of **New Time Template**. See Figure 4-45.

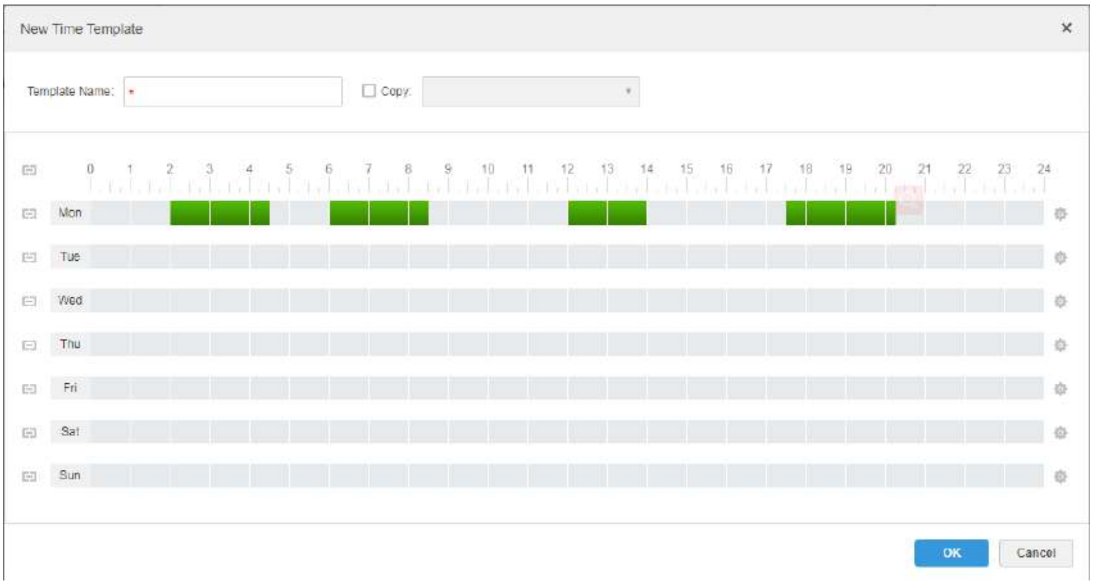
Figure 4-45 New time template



Step 2 Sets template name and time period.

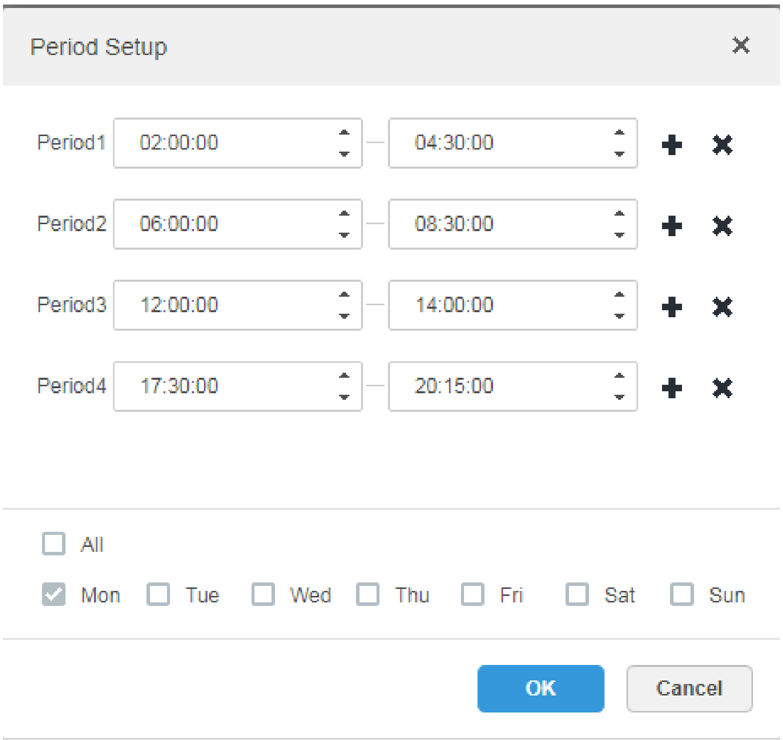
- Press the left button and drag it to draw time period on the time line. See Figure 4-46.

Figure 4-46 Draw period



- Click the ⚙ of the corresponding day, set time period on the interface of Period Setup. See Figure 4-47.

Figure 4-47 Set period



Period Setup

Period1 02:00:00 — 04:30:00

Period2 06:00:00 — 08:30:00

Period3 12:00:00 — 14:00:00

Period4 17:30:00 — 20:15:00

□ All

☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

You can set max 6 periods in one day.

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

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

4.7 Configuring Event

You can configure if the platform receives alarm messages reported by device, and display reported events on client. If receiving reported events, linkage actions are shown as follows when alarm happens to device.

- Link camera

  Play video of designated channel on client, or record over designated channel, or take snapshot over designated channel.

  In order to realize playing video of designated channel on client, you need to select **Enable Alarm Associated Video** on the interface of **Local Config** on client, besides, you need to enable the function that "**Open camera video on client when alarm is triggered**" on manager.

- Link PTZ

  PTZ moves to designated preset.

- Alarm output

  Output alarm signal over alarm output channel on designated device. Alarm is responsed when alarm device is connected to alarm output port.

- Link video wall

  Video channel is displayed on video wall in sequence.
- Link email

  Send email and inform designated personnel that alarm happened.
- Link user

  Push alarm message to designated personnel. If designated personnel logs in to client, then alarm prompt is received.
- Link access control

  Use designated access control channel to unlock or lock.

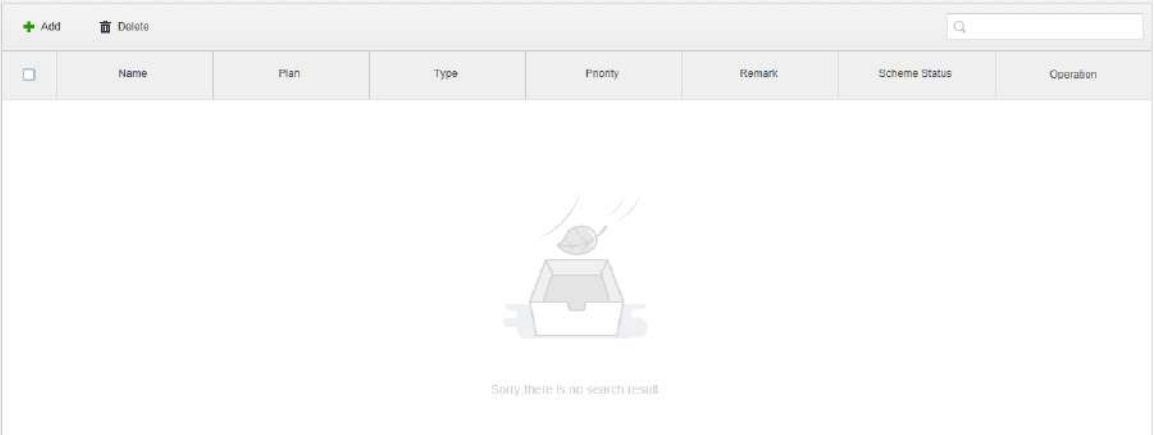
Operation Steps

Step 1

Click+ on manager, select **Event** on the interface of **New Tab**.

The interface of **Event** is displayed. See Figure 4-48.

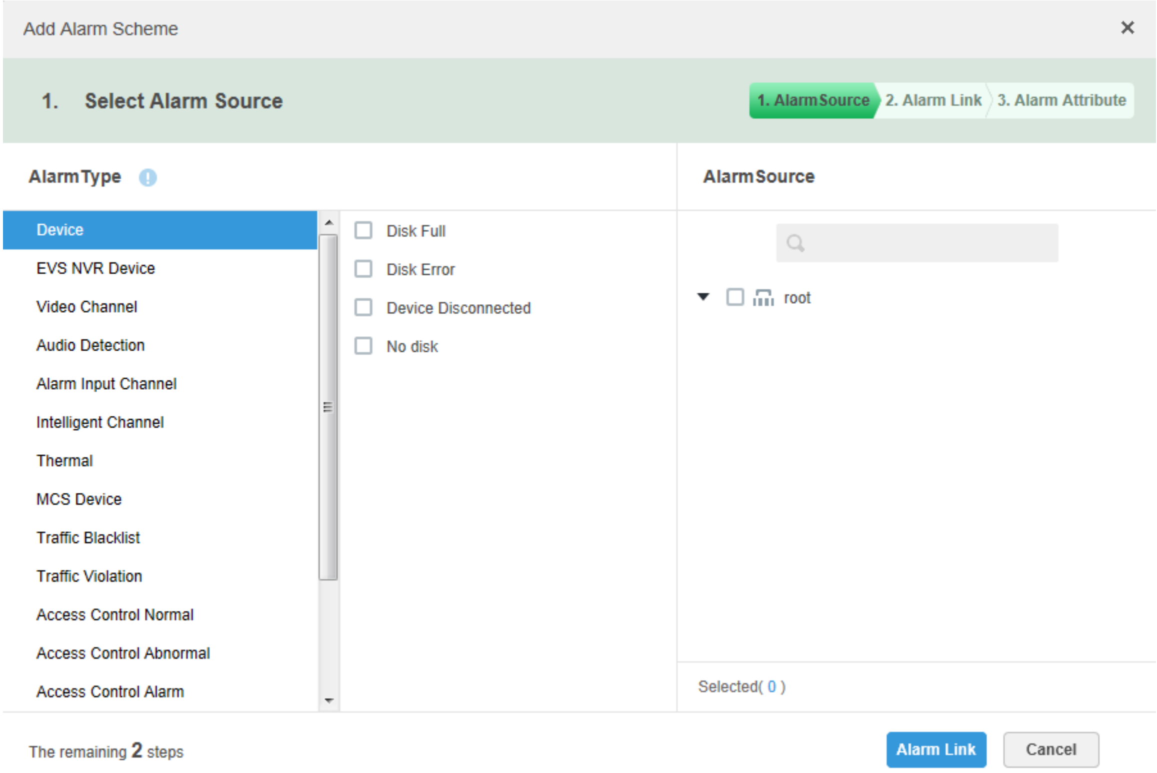
Figure 4-48 Event



Step 2 Click **Add**.

The interface of **Add Alarm Scheme** is displayed. See Figure 4-49.

Figure 4-49 Add alarm scheme



Add Alarm Scheme ×

1. Select Alarm Source

AlarmType

- Device
- EVS NVR Device
- Video Channel
- Audio Detection
- Alarm Input Channel
- Intelligent Channel
- Thermal
- MCS Device
- Traffic Blacklist
- Traffic Violation
- Access Control Normal
- Access Control Abnormal
- Access Control Alarm

□ Disk Full
□ Disk Error
□ Device Disconnected
□ No disk

AlarmSource

□ root

Selected(0)

The remaining 2 steps

Step 3 Configure alarm source.

⚠

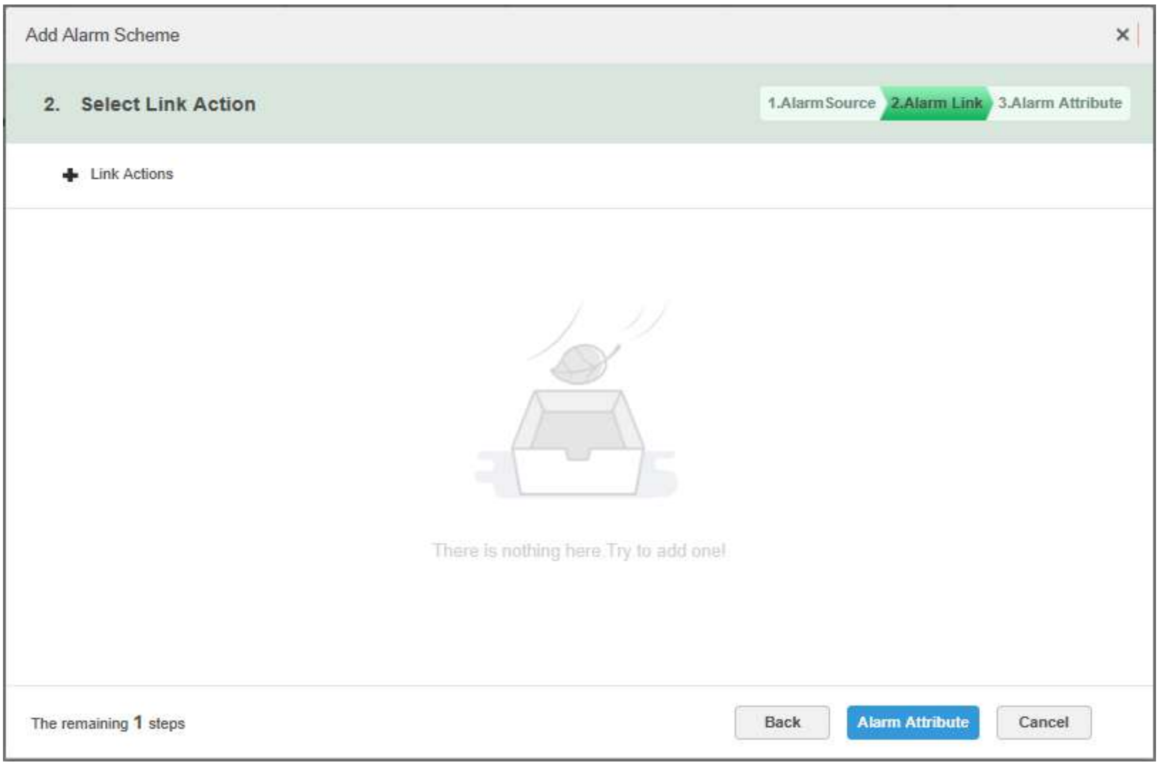
Please make sure the channel capacity set and alarm type are well matched before config, otherwise, it cannot be alarm source. For more details about channel capacity set, please refer to "4.5.4 Editing Device "**.**

1) Select alarm type and alarm source.

2) Click **Alarm Link**.

The system displays the interface of **Add Alarm Scheme**. See Figure 4-50.

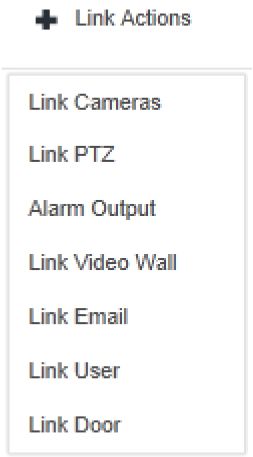
Figure 4-50 Alarm link



Step 4 Configure alarm link.

1) Click ✚ , the system pops out the list of **Link Actions**. See Figure 4-51.

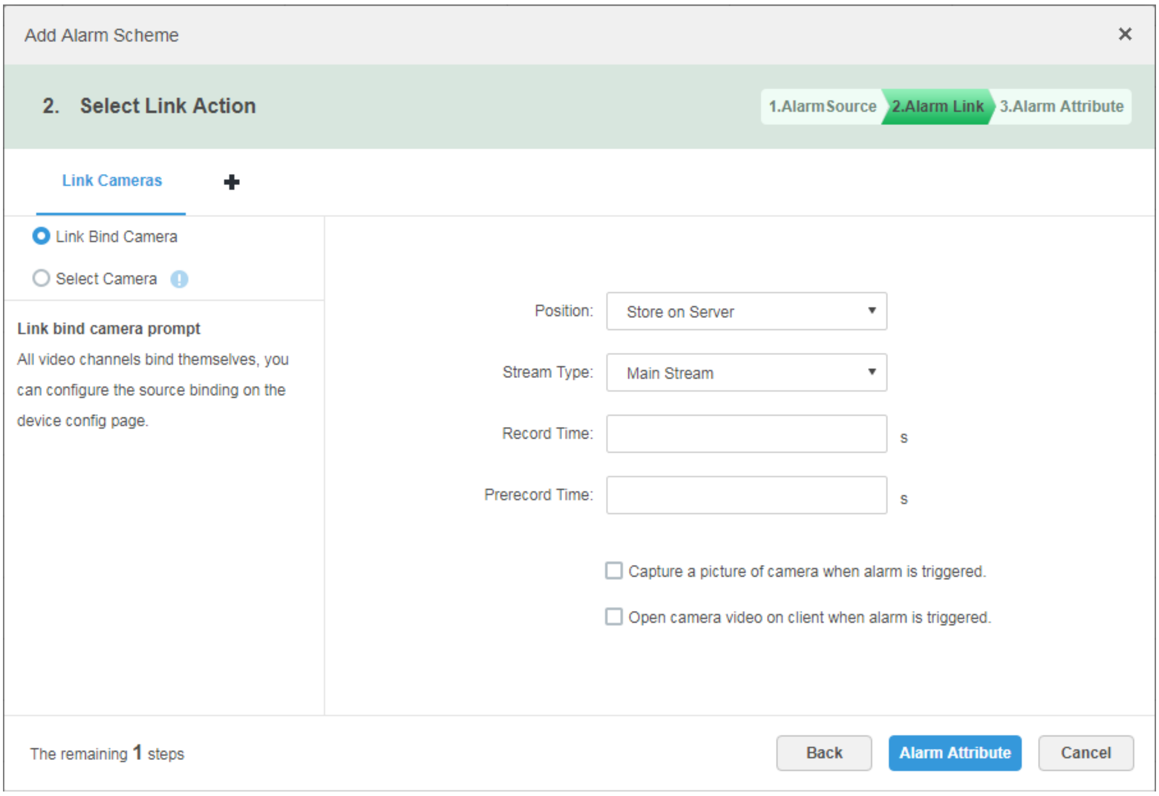
Figure 4-51 Link actions



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 Link camera



Add Alarm Scheme ×

2. Select Link Action

1.AlarmSource 2.Alarm Link 3.Alarm Attribute

Link Cameras ✚

● Link Bind Camera

○ Select Camera

Link bind camera prompt

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

Position: Store on Server

Stream Type: Main Stream

Record Time: s

Prerecord Time: s

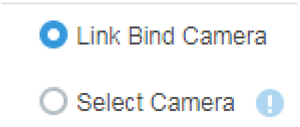
□ Capture a picture of camera when alarm is triggered.

□ Open camera video on client when alarm is triggered.

The remaining 1 steps

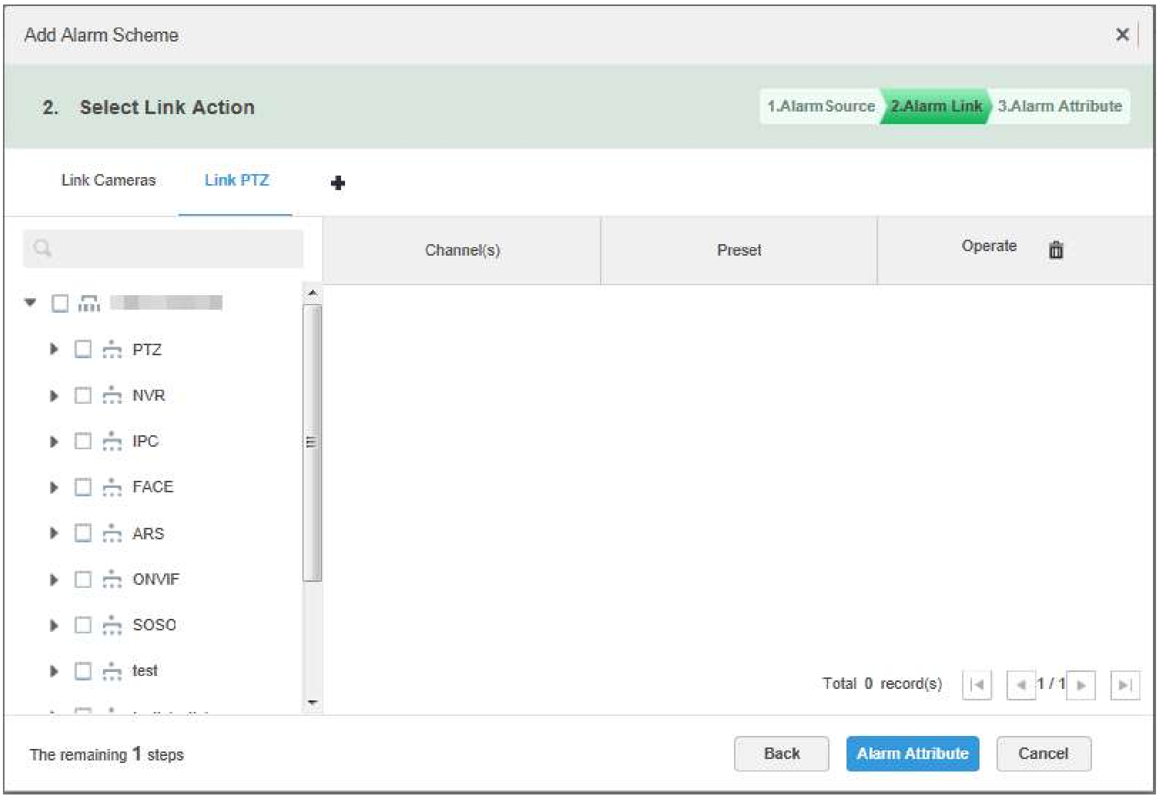
Back | Alarm Attribute | Cancel

Table 4-3 Link camera parameter

Parameter	Description
 ● Link Bind Camera ○ Select Camera	● Link bind camera: Video channel has been bound with alarm source. It is to quickly configure scheme via resource binding of device management. ● Select link camera: It needs link camera to manually select the alarm source.
Position	It is to set whether store the video on server.
Stream Type	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 a picture of camera when alarm is triggered.	Confirm if it captures camera picture.
Open camera video on client when alarm is triggered.	Confirm if it opens camera video window on the client during alarm.

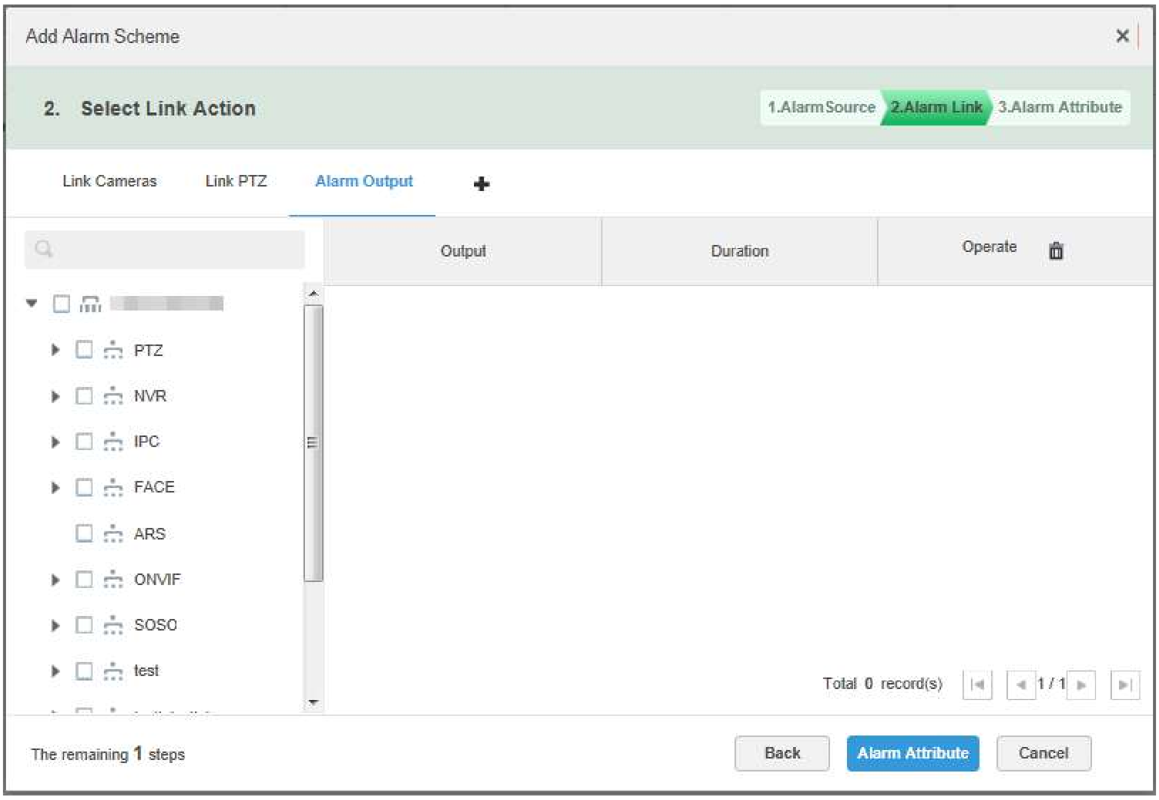
◇ Click **Link PTZ**, select the channels which need PTZ to link device, set prerecord actions. See Figure 4-53.

Figure 4-53 Link PTZ



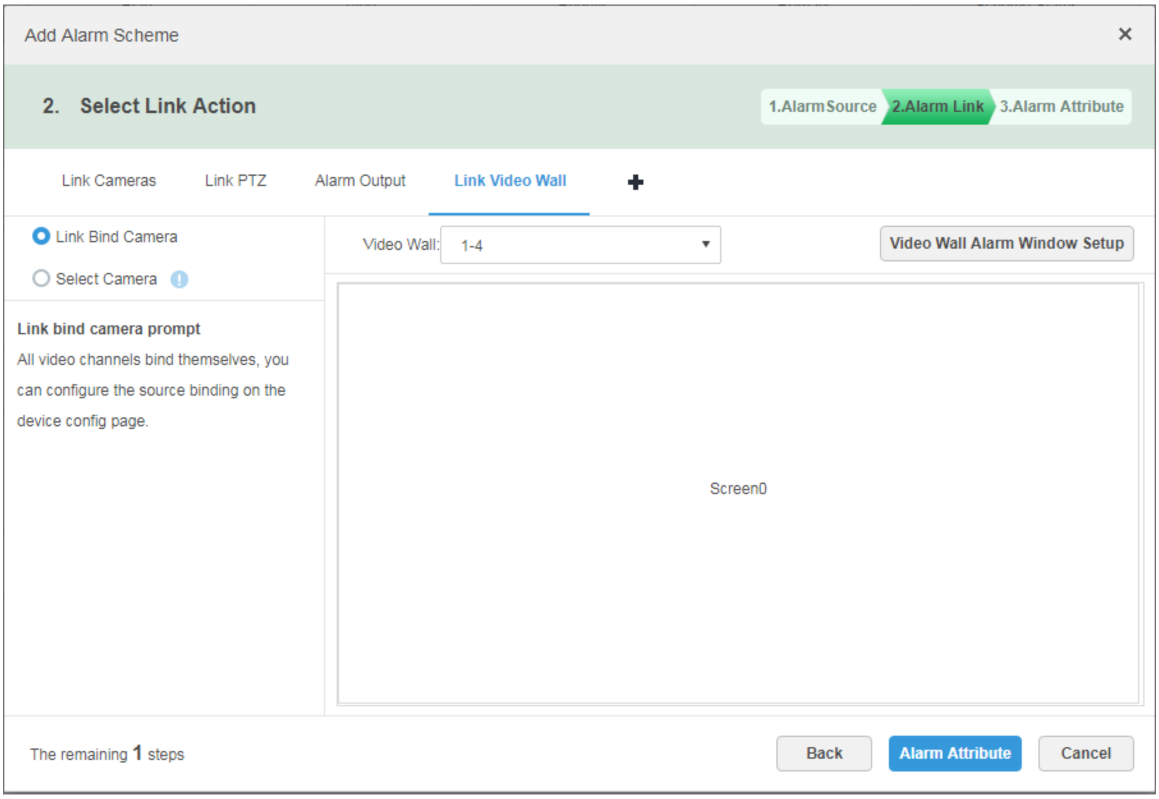
◇ Click **Alarm Output**, select alarm output channel, set duration. See Figure 4-54.

Figure 4-54 Alarm output



◇ Click **Link Video Wall**, select link camera on the left of the interface, select video wall on the right of the interface. See Figure 4-55. When selecting **Link Bind Camera** and **Link Camera**, the interfaces will display differently, please base on the actual display. Click **Video Wall Alarm Window Setup** to set duration and select the video channel which needs to be displayed on wall. See Figure 4-56.

Figure 4-55 Link video wall



Add Alarm Scheme

2. Select Link Action

● Link Bind Camera

○ Select Camera

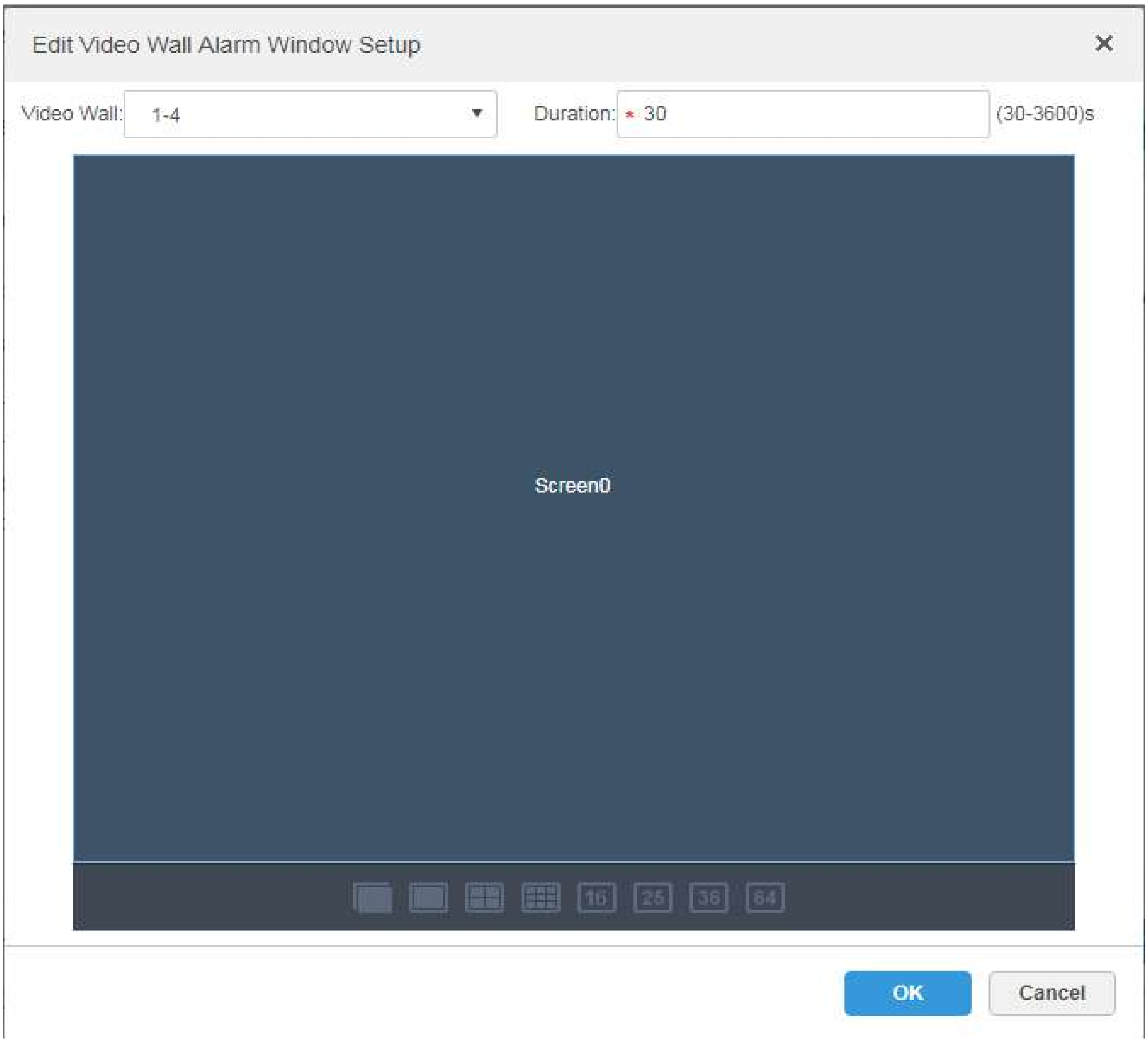
Link bind camera prompt

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

Video Wall: 1-4

The remaining **1** steps

Figure 4-56 Video wall alarm window setup



Edit Video Wall Alarm Window Setup

Video Wall: 1-4

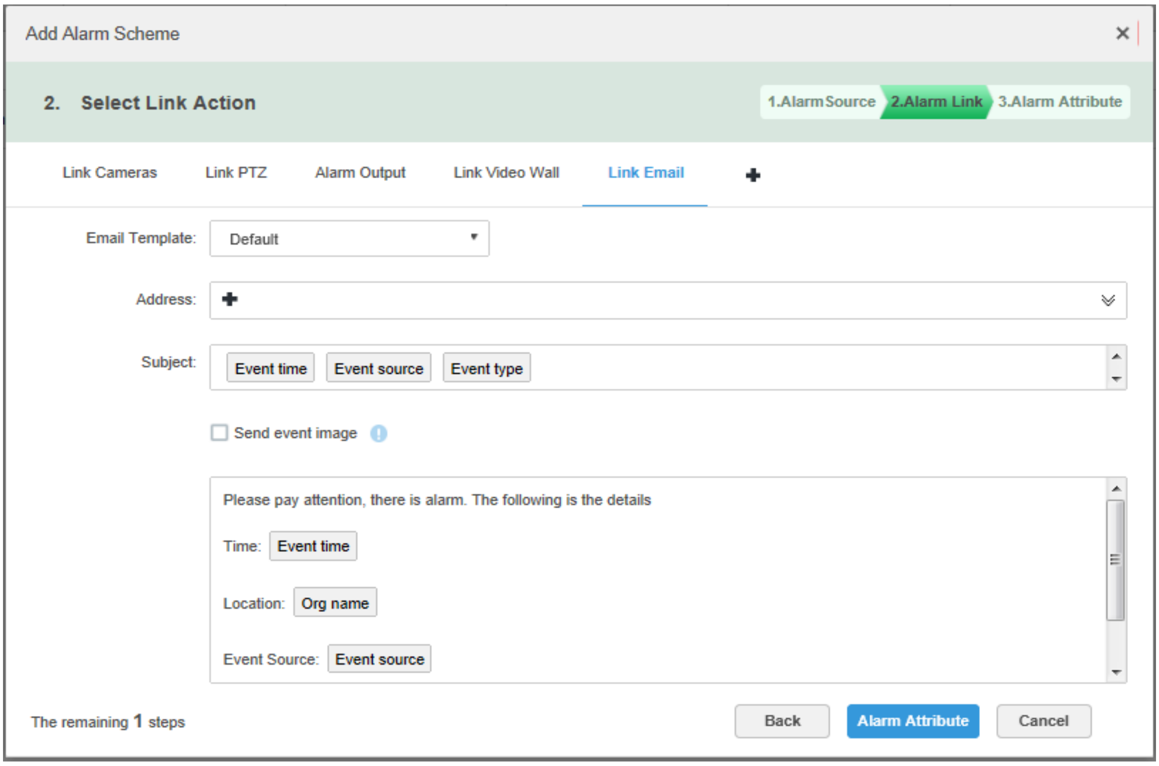
Duration: * 30 (30-3600)s

◇ 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 Link email


Add Alarm Scheme

2. Select Link Action

1.AlarmSource 2.Alarm Link 3.Alarm Attribute

Link Cameras | Link PTZ | Alarm Output | Link Video Wall | Link 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

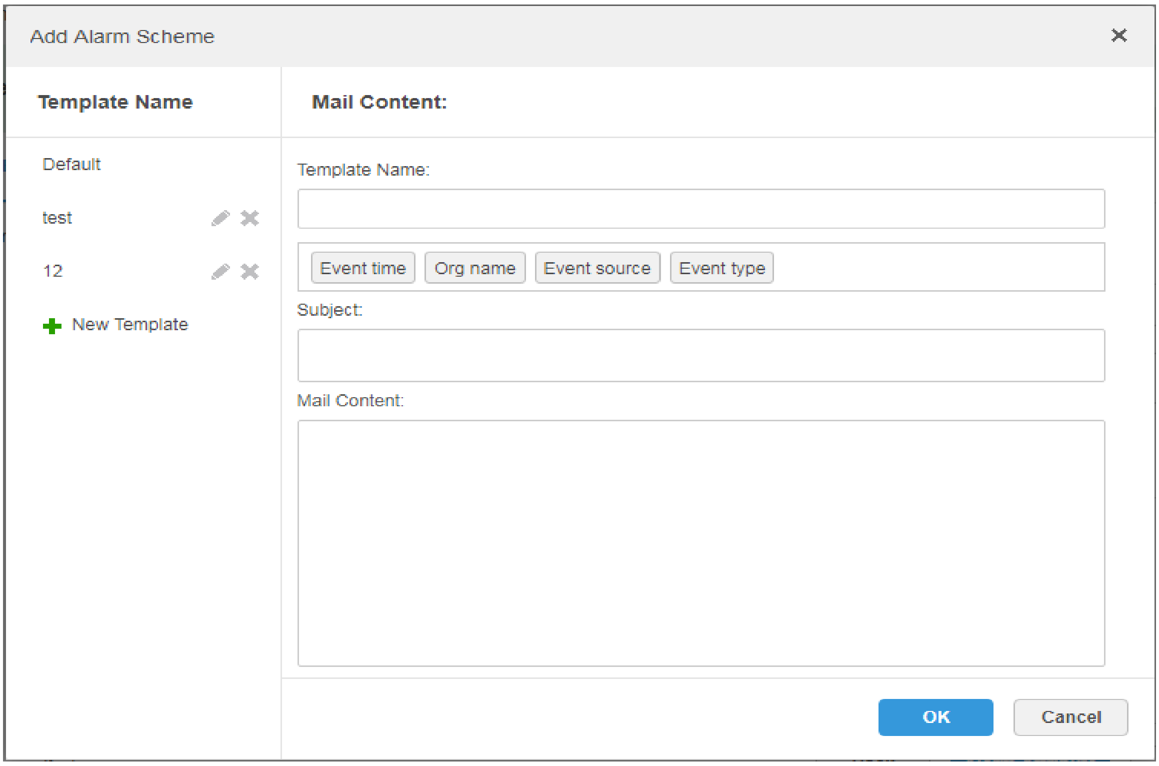
Location: Org name

Event Source: Event source

The remaining 1 steps

Back | Alarm Attribute | Cancel

Figure 4-58 Email template


Add Alarm Scheme

Template Name

Default

test

12

New Template

Mail Content:

Template Name:

Event time Org name Event source Event type

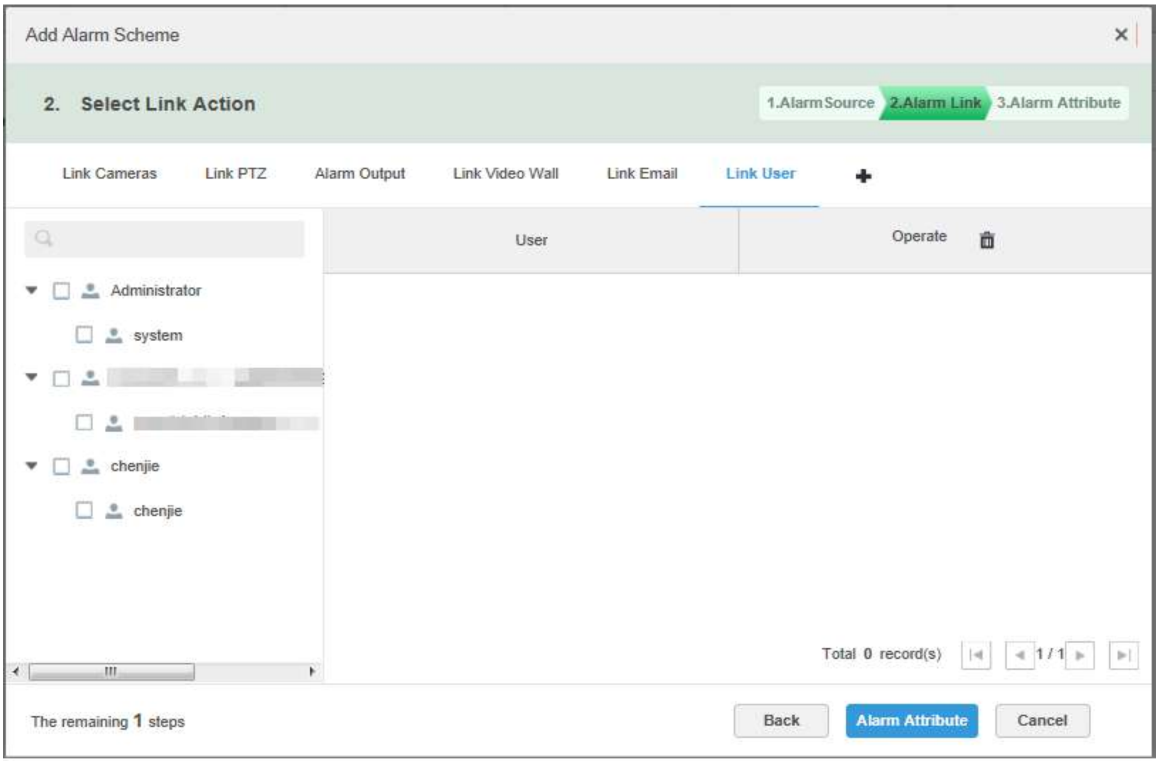
Subject:

Mail Content:

OK | Cancel

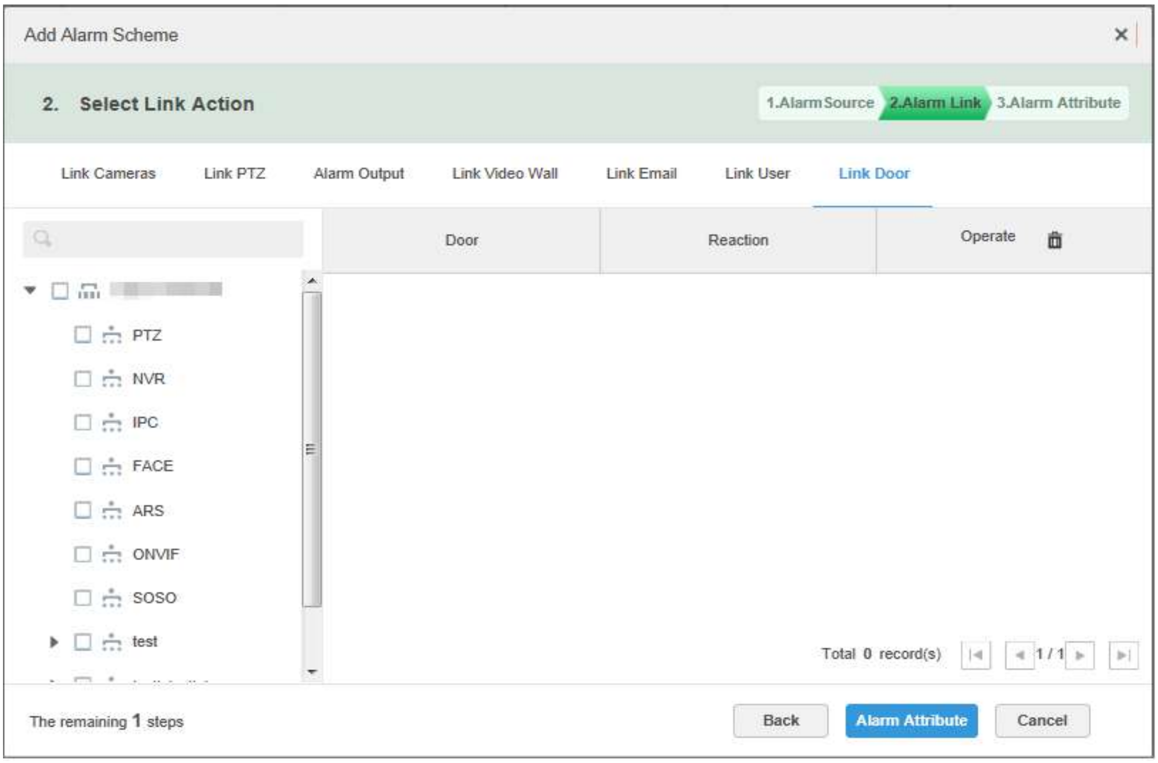
◇ Click **Link User**, select the users who need to be informed. See Figure 4-59.

Figure 4-59 Link user



◇ Click **Link Door**, select the access control device, and set the link action. See Figure 4-60.

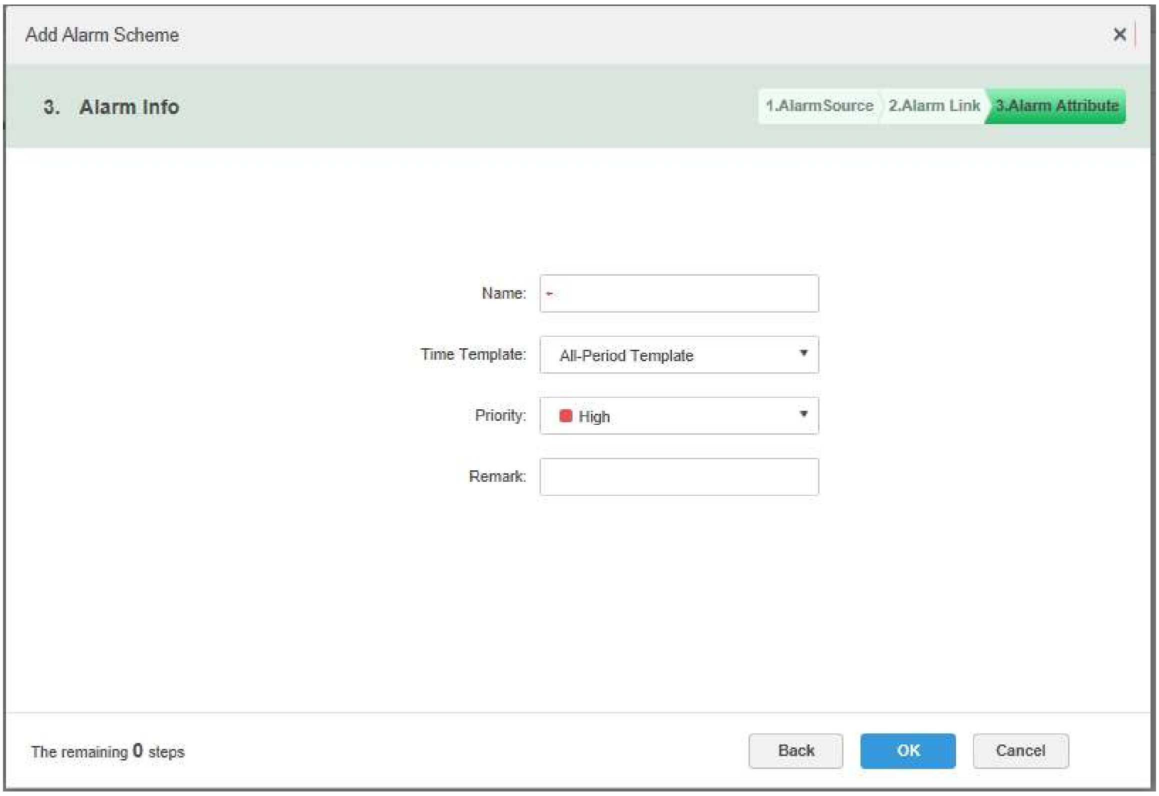
Figure 4-60 Link door



Step 5 Click **Alarm Attribute**.

The system displays the interface of **Alarm Attribute**. See Figure 4-61.

Figure 4-61 Alarm attribute



Add Alarm Scheme ×

3. Alarm Info

Name: *

Time Template: All-Period Template

Priority: 🟥 High

Remark:

The remaining 0 steps

Step 6 Configure alarm attribute.

1) Set alarm name.

2) Select alarm time template and priority.

3) Click **OK**.

The system displays the added alarm scheme.

Step 7 In the **Operation** column, click OFF to enable scheme. When the icon changes into ON, means that the scheme has been enabled.

Operations

- Edit

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

- Delete

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

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

- Disable scheme

  In the Operation column, click ON. When the icon changes into OFF, means that the scheme has been disenabled.

4.8 Configuring Map

Before using the electronic map function, you need to select the map category on the administrative side, including rater map and GIS 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), access control, people counting, retail and some other indoor scenarios. The server enables raster map by default.
- GIS map
  GIS map supports Baidu map, A map and Google map. It takes Google map as an example to make introduction.
  - ◇ 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.

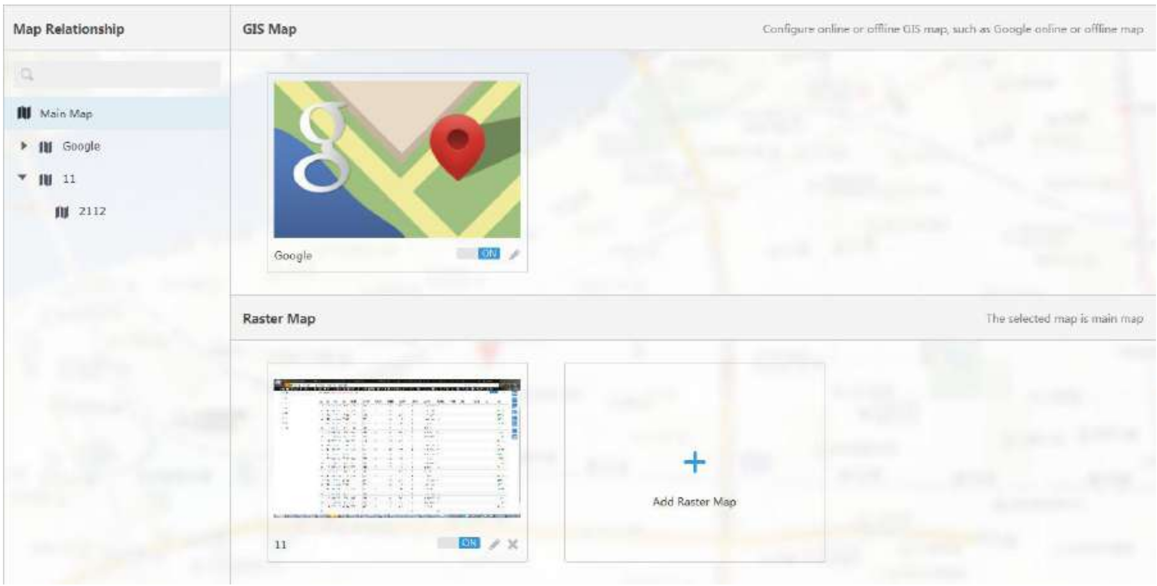
4.8.1 Adding Map

4.8.1.1 Adding GIS Map

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

The system displays the map interface. See Figure 4-62.

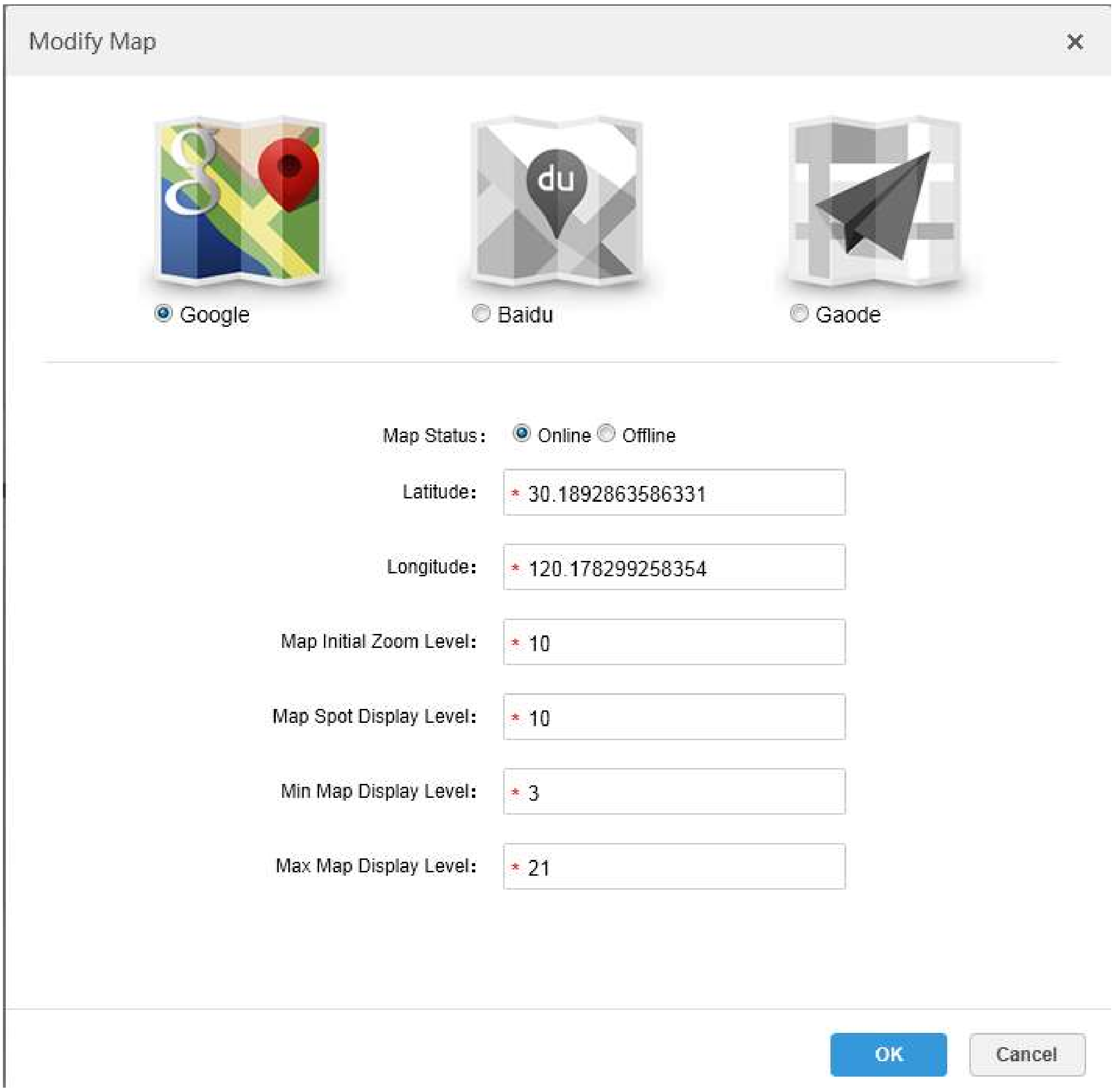
Figure 4-62 Map interface


Map Relationship
GIS Map
Configure online or offline GIS map, such as Google online or offline map
Main Map
Google
11
2112
Google
ON
Raster Map
The selected map is main map
11
ON
+
Add Raster Map

Step 2 Click in the GIS map area.

The system pops out the map config interface. See Figure 4-63.

Figure 4-63 Select map



Modify Map ×

● Google ○ Baidu ○ Gaode

Map Status: ● Online ○ Offline

Latitude: * 30.1892863586331

Longitude: * 120.178299258354

Map Initial Zoom Level: * 10

Map Spot Display Level: * 10

Min Map Display Level: * 3

Max Map Display Level: * 21

Step 3 Select map type and configure map info.

- Online map

1) Select **Map Status** as **Online.**

2) Configure map info, click **OK**.

- Offline map

1) Select **Map Status** as **Offline**.

2) Click **Import** and import offline map.

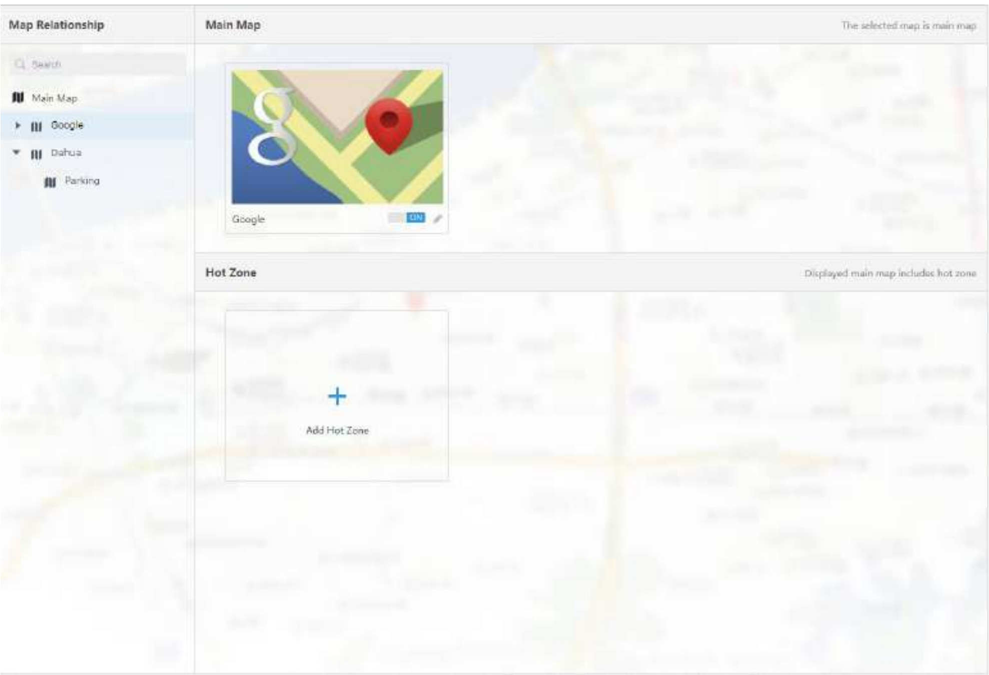
3) Configure map info, click **OK**.

Step 4 Adding hot zone

You can add detailed map of the area on the map if you want to see the detailed scene map of some area, such as flattened scene in parking lot.

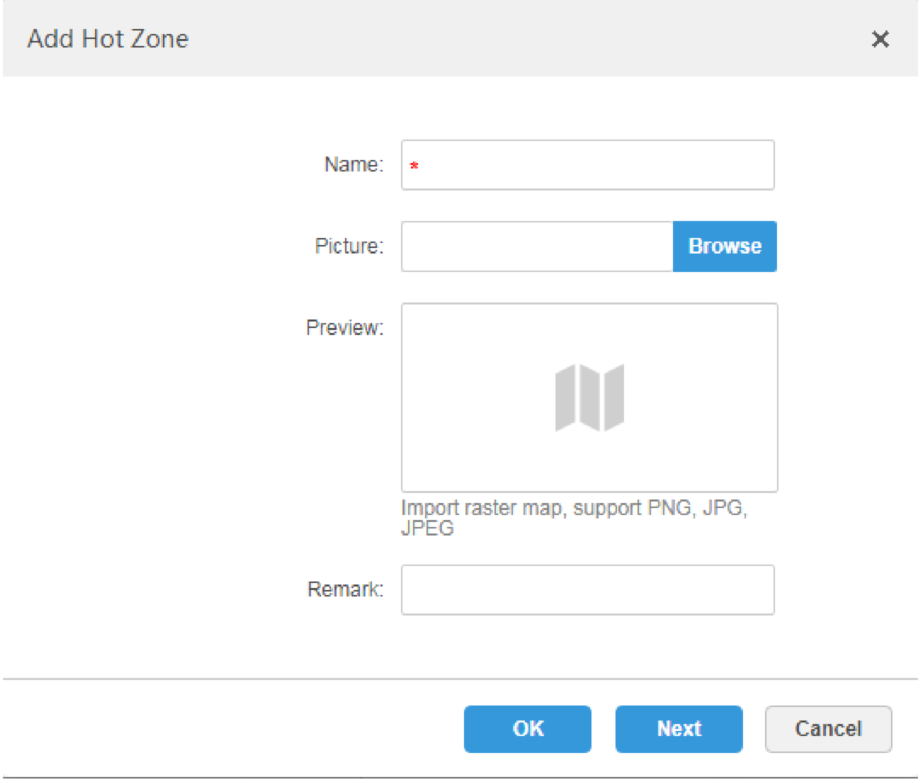
1) Click the GIS map on the left, and the added hot zone module is displayed on the right. See Figure 4-64.

Figure 4-64 Add hot zone(1)



2) Click **Add Hot Zone**.
The interface of **Add Hot Zone** is displayed. See Figure 4-65.

Figure 4-65 Add hot zone(2)



Import raster map, support PNG, JPG, JPEG

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

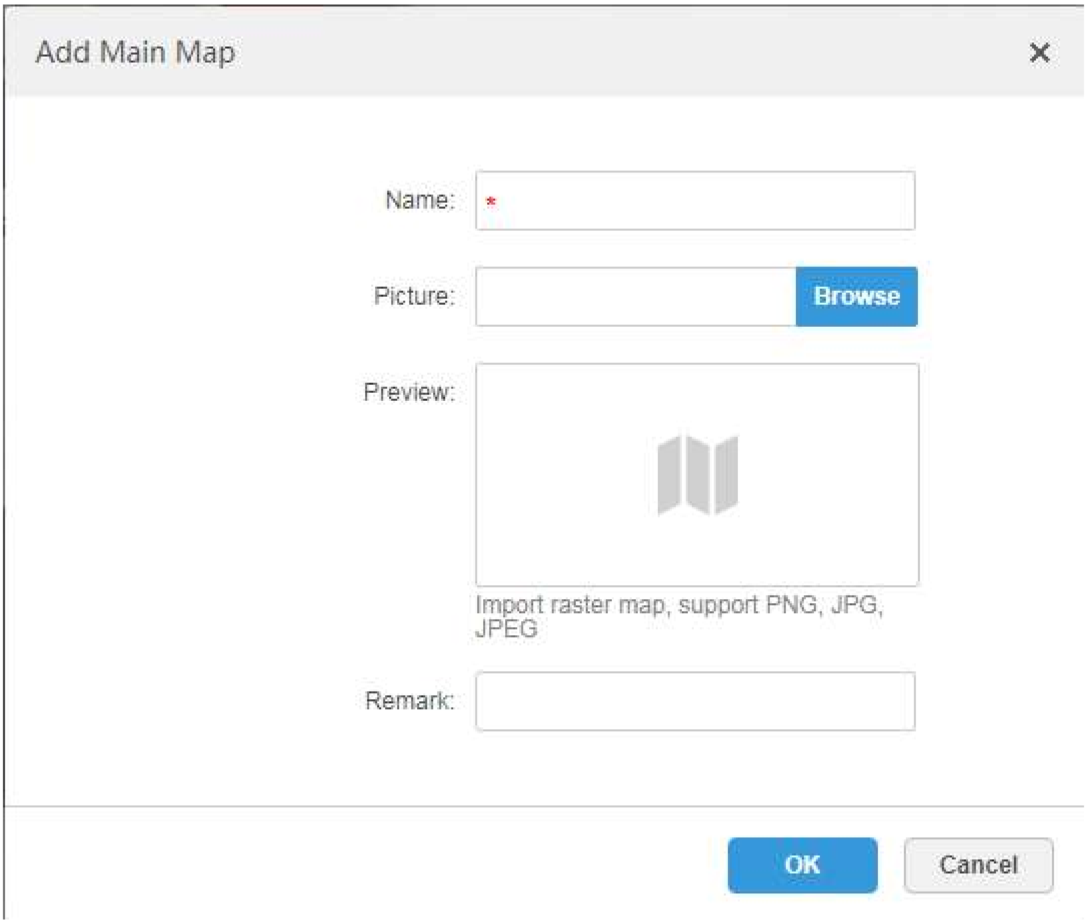
4.8.1.2 Adding Raster Map

Add raster map as hot zone, make it convenient to view detailed scene map, such as flattened scene in parking lot.

Step 1 Click **Add Raster Map** on the interface of **Map**.

The interface of **Add Main Map** is displayed. See Figure 4-66.

Figure 4-66 Add main map



Add Main Map

Name: *

Picture:

Preview:

Import raster map, support PNG, JPG, JPEG

Remark:

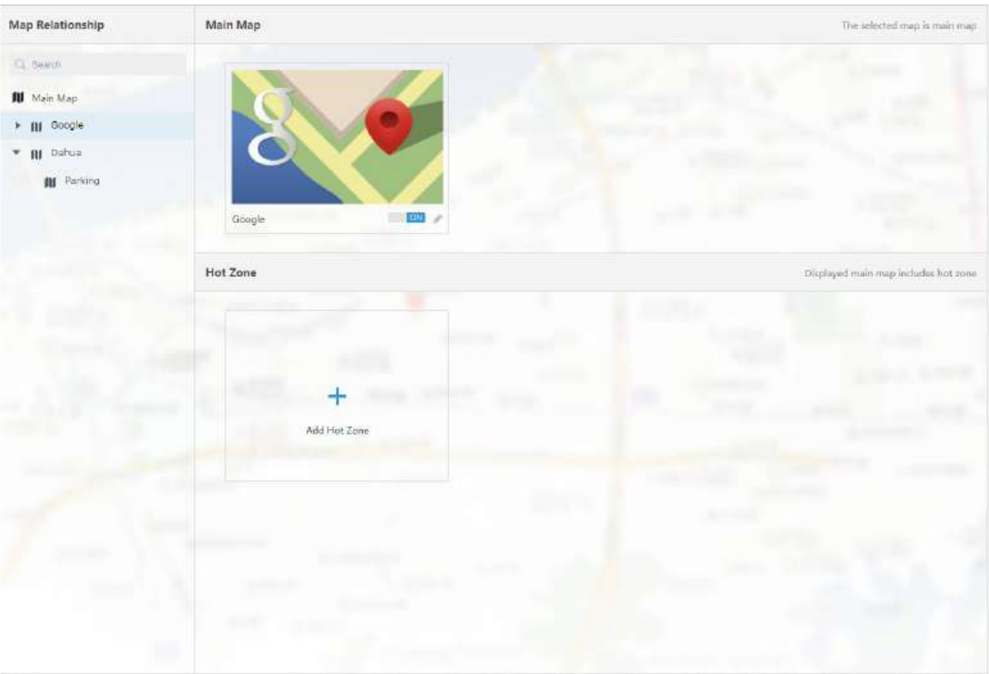
Step 2 Enter **Name**, select upload picture, click **OK**.

You can continue to add several raster maps.

Step 3 Add hot zone.

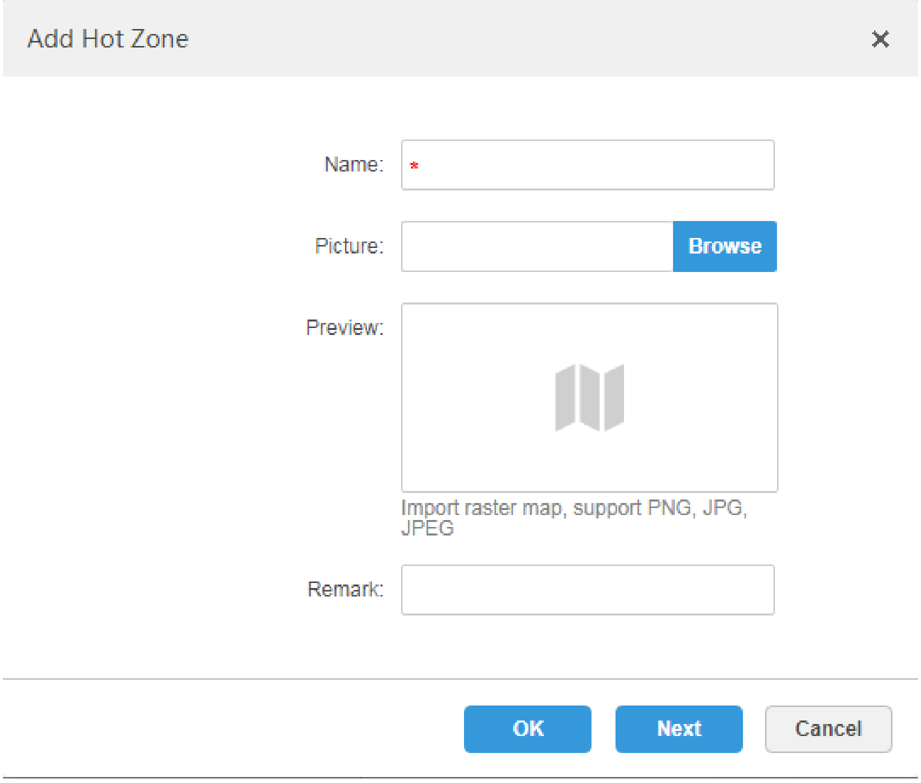
1) Click the raster map on the left, and the added hot zone module is displayed on the right. See Figure 4-67.

Figure 4-67 Add hot zone



2) Click **Add Hot Zone**.
The system displays the interface of **Add Hot zone**. See Figure 4-68.

Figure 4-68 Add hot zone



Add Hot Zone

Name: *

Picture:

Preview:

Import raster map, support PNG, JPG, JPEG

Remark:

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

4) Drag icon and confirm hot zone location, and then click **OK**.

4.8.2 Marking Device

Drag the device to corresponding location of the map according to the device installation location. Therefore, the device and map are linked on the system.

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

The system displays the map info. See Figure 4-69.

Figure 4-69 Map

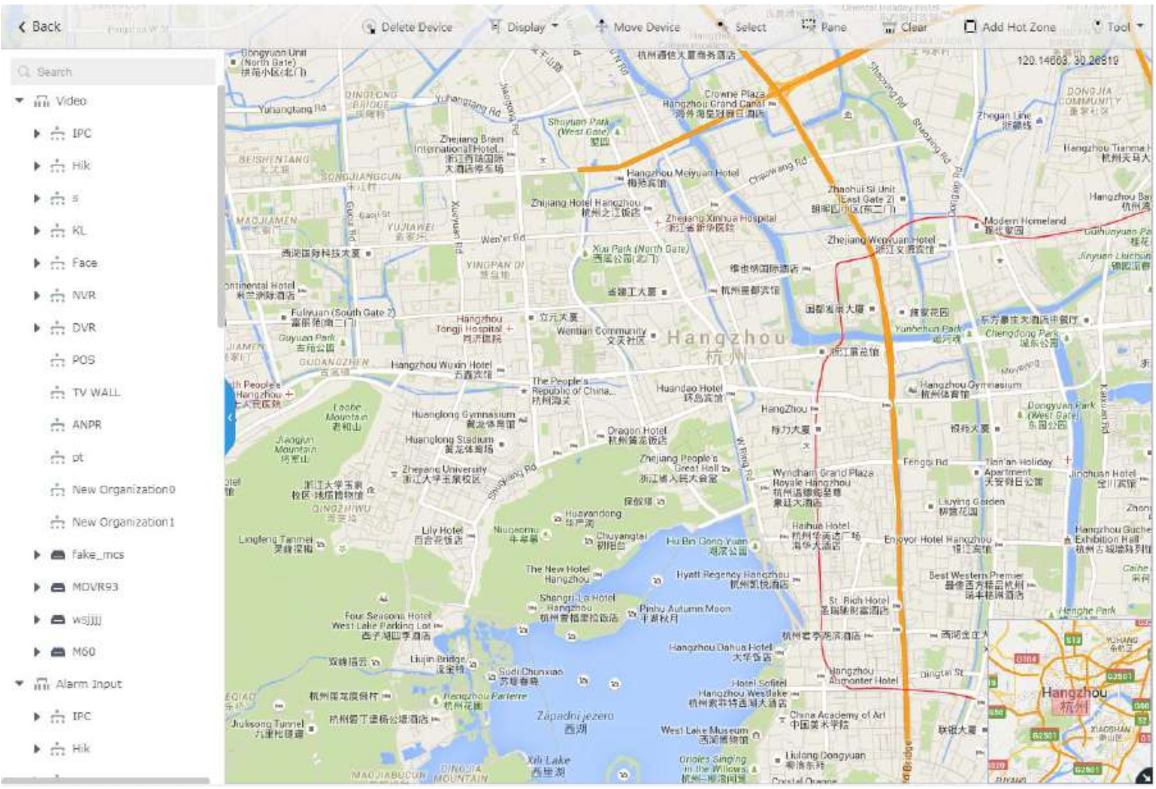


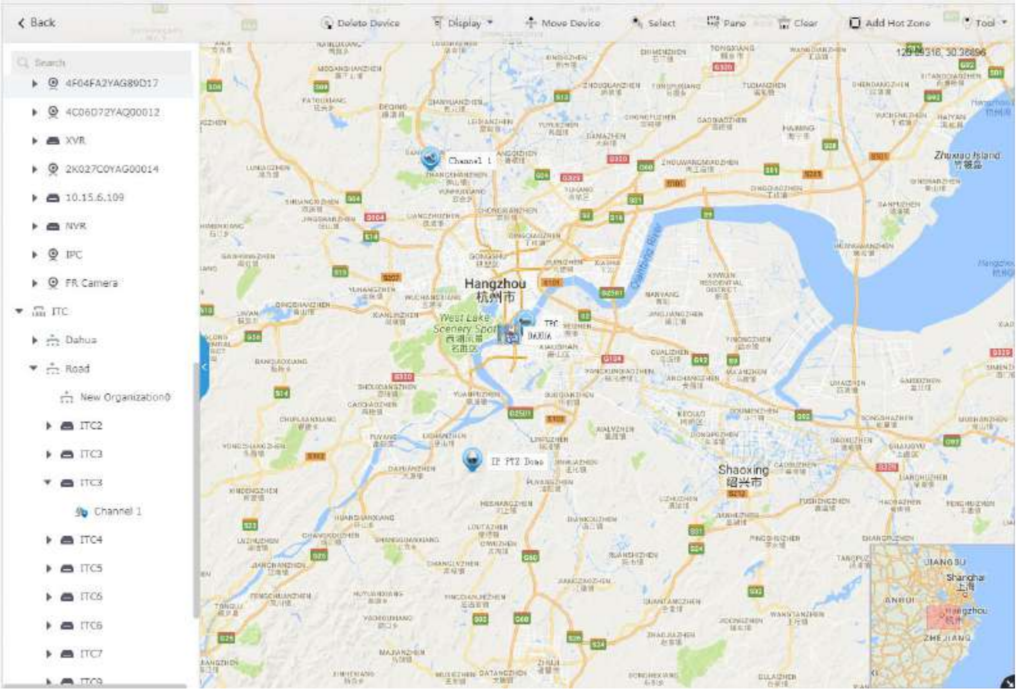
Table 4-4 Map interface function

Parameter	Description
Display	● Raster map displays: video; access control; alarm input; intelligence device ● GIS map displays: video; alarm input; ITC; intelligence device
Delete Device	Click to move the device location on the map.
Select	Select device via clicking on it.
Pane	Select device via box selection.
Clear	Clear the boxing trace on the screen.
Add Hot Zone	Click Add Hot Zone, select location on the map and add hot zone map. After entering hot zone, it can also continue to add lower-level hot zone map. Click hot zone on the client map, the system will automatically link the map to the hot zone map.

Tool	Includes length, area, mark and reset. ● Length: it is to measure the actual distance between two spots on the map. ● Area: It is to measure the actual area of the previous area on the map. ● Mark: It is to mark on the map. ● Reset: it is restored back the initial default location of the map.
Others	● Click hot zone, and it can modify the info of hot zone map. ● Double click hot zone, the system will automatically skip to hot zone map, and then it can drag it into the channel on the hot zone map.

Step 2 Drag the device channel from the left device tree to the corresponding location of the map. The interface is shown in Figure 4-70.

Figure 4-70 Mark device



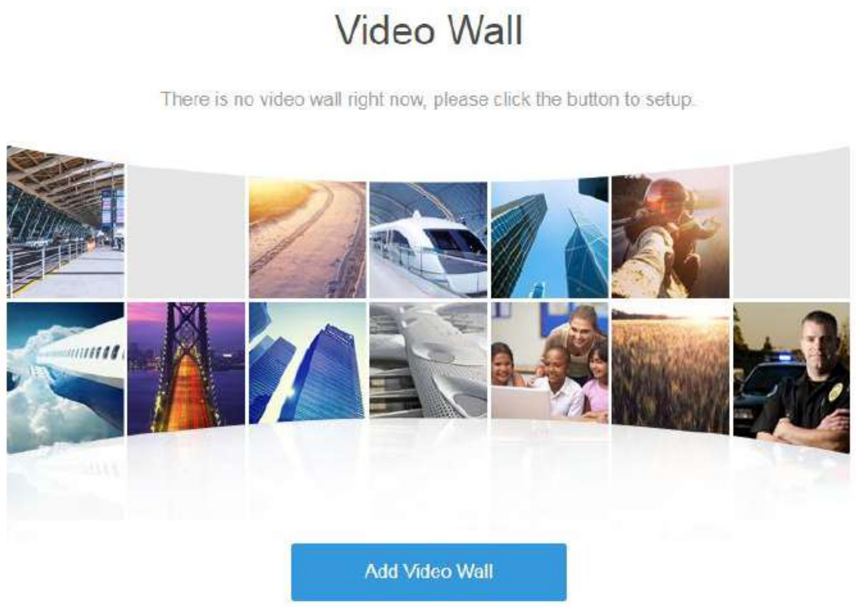
4.9 Adding Video Wall

You 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 **New Tab** interface.

See Figure 4-71.

Figure 4-71 Video wall config

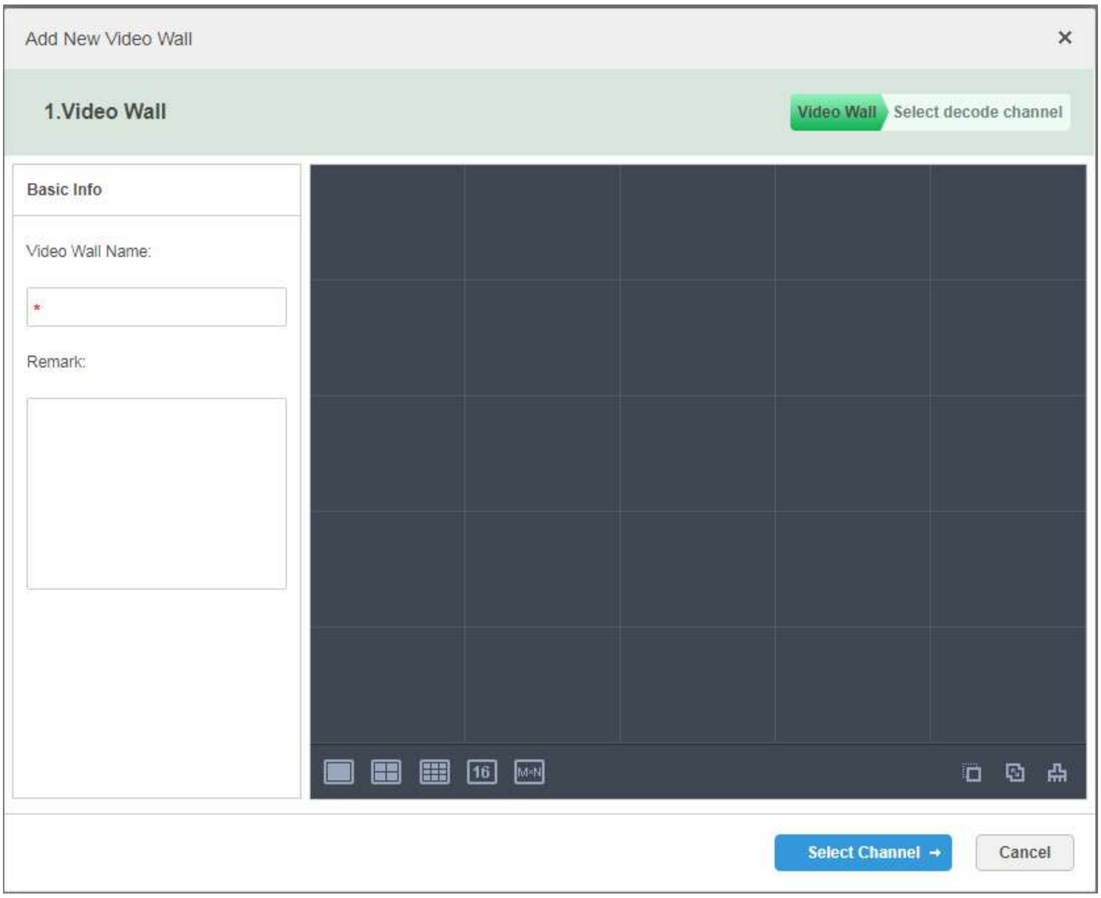

Video Wall

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 New Video Wall**. See Figure 4-72.

Figure 4-72 Add new video wall


Add New Video Wall

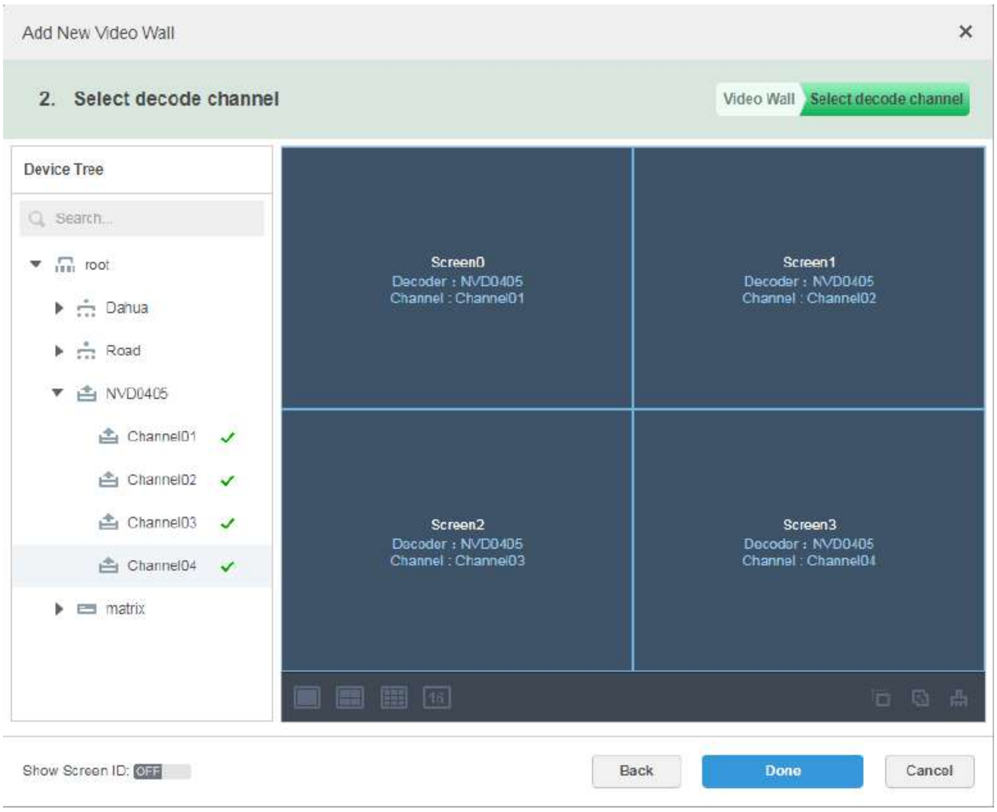
1.Video Wall

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

Step 4 Click **Select Channel**.

The system will display the interface of **Select decode channel**. See Figure 4-73.

Figure 4-73 Select decode channel



Screen0
Decoder : NVD0405
Channel : Channel01

Screen1
Decoder : NVD0405
Channel : Channel02

Screen2
Decoder : NVD0405
Channel : Channel03

Screen3
Decoder : NVD0405
Channel : Channel04

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

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

Step 6 Click **Done**.

4.10 Configuring Face Recognition

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

4.10.1 Creating Face Database

Support creating face library, managing face info in the library, and add face images to the library as references for comparison.

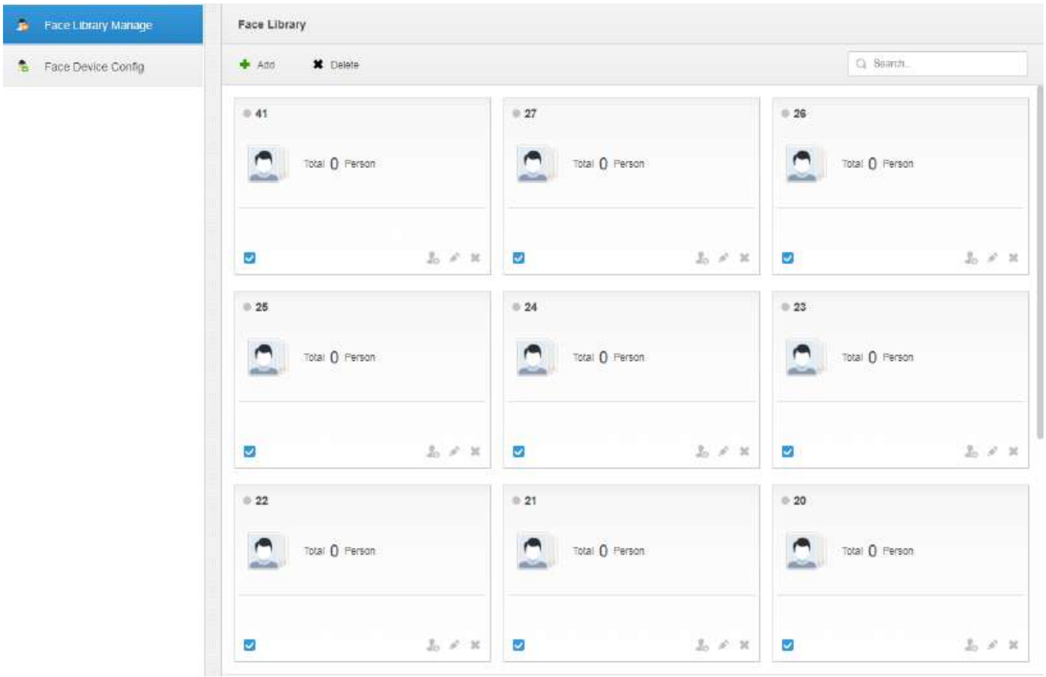
4.10.1.1 Adding Face Library

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

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

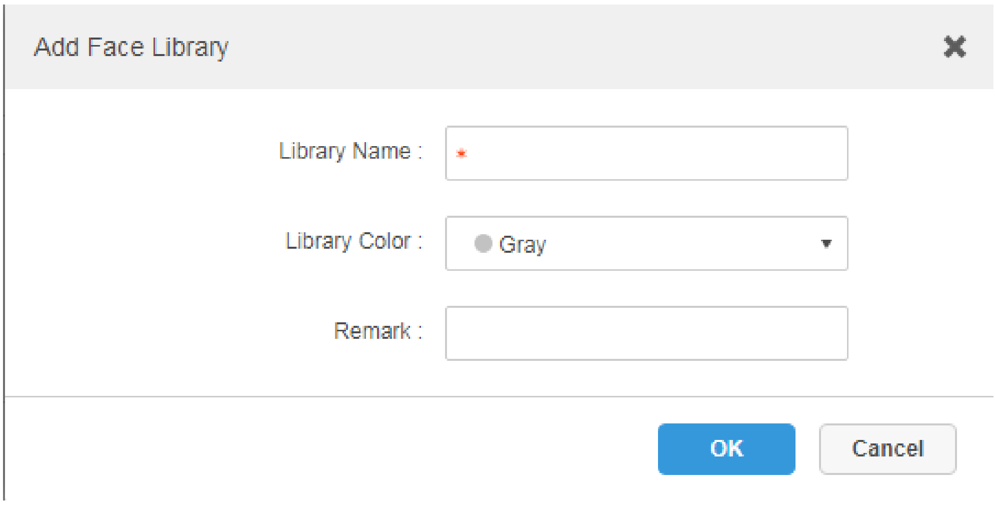
The system displays the interface of **Face Library**. See Figure 4-74.

Figure 4-74 Face library(1)



Step 2 Click **Add**.

Figure 4-75 Add face library



Library Name : *

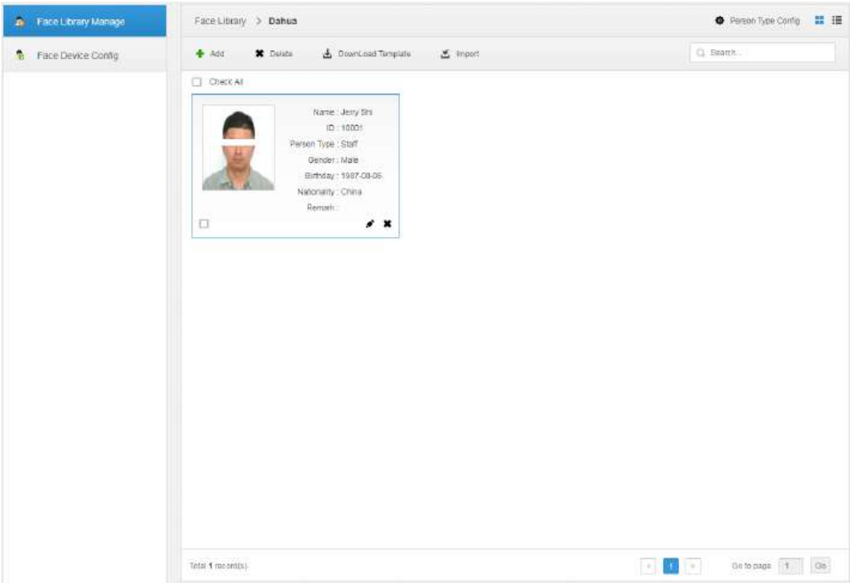
Library Color : Gray

Remark :

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

The interface is shown in Figure 4-76.

Figure 4-76 Face library(2)



Name : Jerry Shi
ID : 10001
Person Type : Staff
Gender : Male
Birthday : 1987-08-06
Nationality : China
Remark :

Total 1 record(s)

Operations

- Search library

  Filter the library via face library type or keyword.
- Add face library

  Click to add staff info. Please refer to "4.10.1.3 Adding Face Library Info."
- Modify Staff Library

  Click to modify library name and library description.
- Delete Staff Library

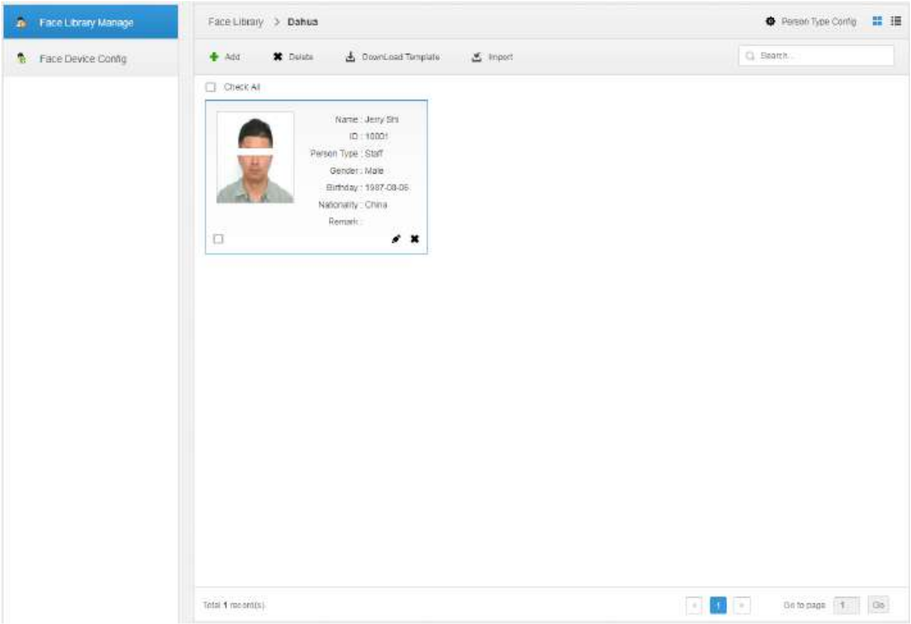
  Click to delete face library only when there is no face info under the library.

4.10.1.2 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 4-77.

Figure 4-77 Face library

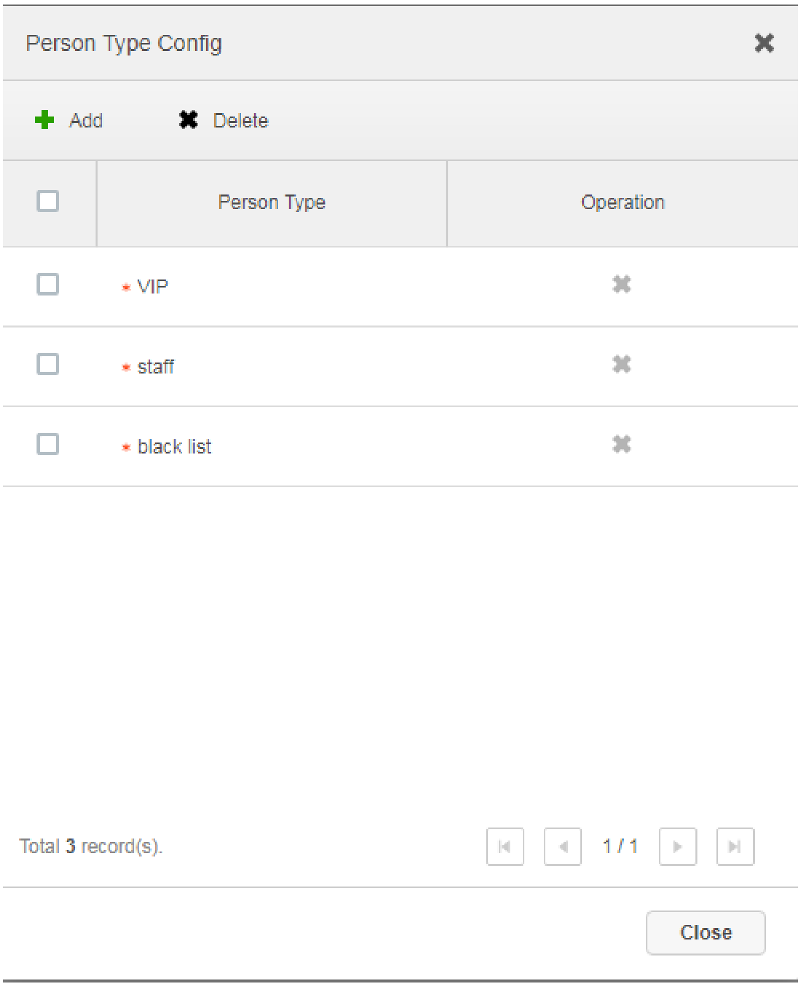


Name : Jerry Shi
ID : 10001
Person Type : Staff
Gender : Male
Birthday : 1987-08-06
Nationality : China
Remark :

Total 1 record(s).

Step 2 Click **Person Type Config**. The interface is shown in Figure 4-78.

Figure 4-78 Persone type config



□	Person Type	Operation
□	* VIP	✖
□	* staff	✖
□	* black list	✖

Total 3 record(s). 1 / 1

Step 3 Click **Add** and enter type name in the column of **Person Type**.

Step 4 Click ✖ to disable the window.

4.10.1.3 Adding Face Library Info

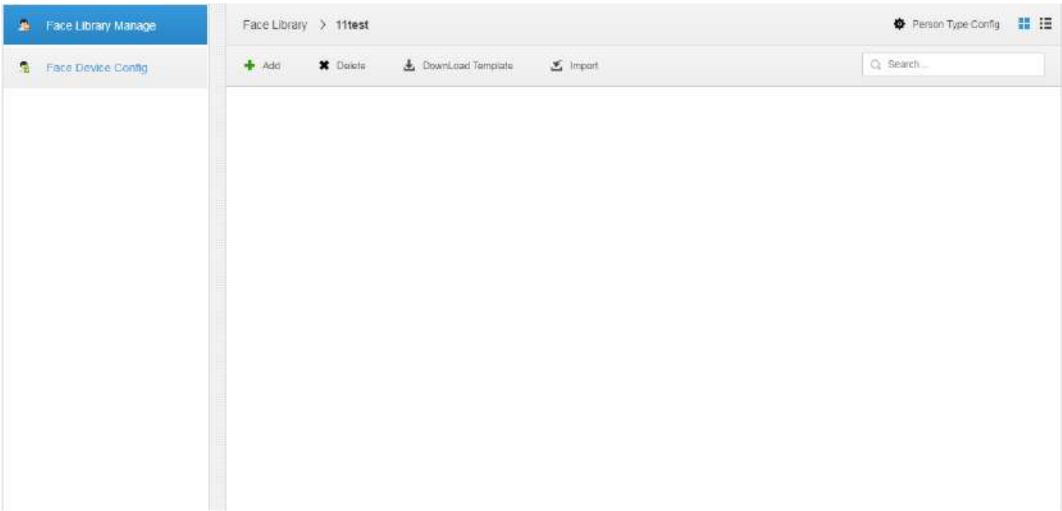
It can add person info via adding individual person and importing in batches.

4.10.1.3.1 Adding Individually

Step 1 Enter the interface of adding person.

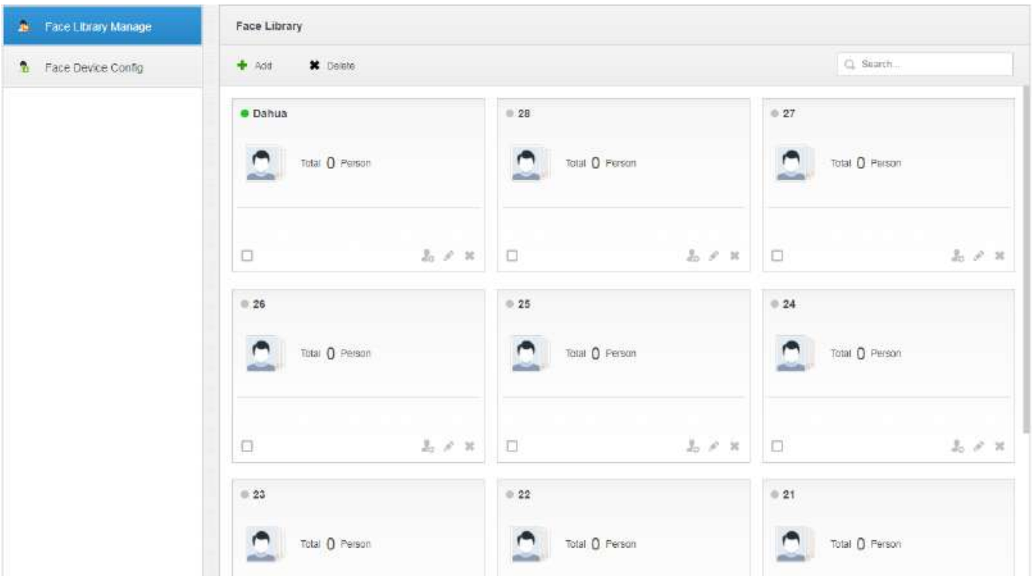
- Click the library which needs to be added with person on the interface of **Face Library Manage**. See Figure 4-79. Click **Add**.

Figure 4-79 Library person info



- Click on the card of person library, the interface is shown in Figure 4-80.

Figure 4-80 Add person



Step 2 Enter person info.

Step 3 Click profile photo and upload the picture.

Step 4 Click **OK**.

Click **Continue to add** of 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

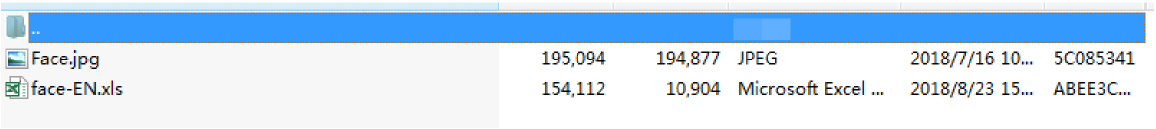
  ◇ Click ✖ on person interface and then you can delete person individually.

  ◇ Select person, click ‘Delete to delete person in batches.

4.10.1.3.2 Batch Import

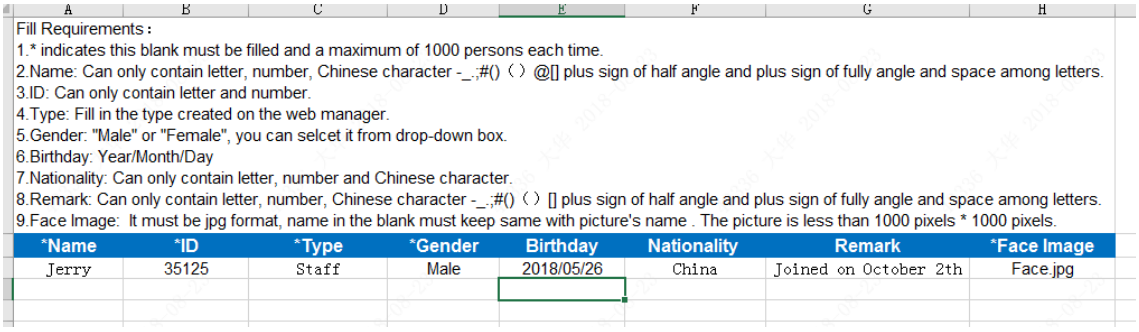
Need to prepare person picture in advance if you want to import in batches, and compress it into zip RAR. RAR and excel style are shown in Figure 4-81 and Figure 4-82. Currently batch import supports max 1000 pictures at one time.

Figure 4-81 Zip



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

Figure 4-82 Table format



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

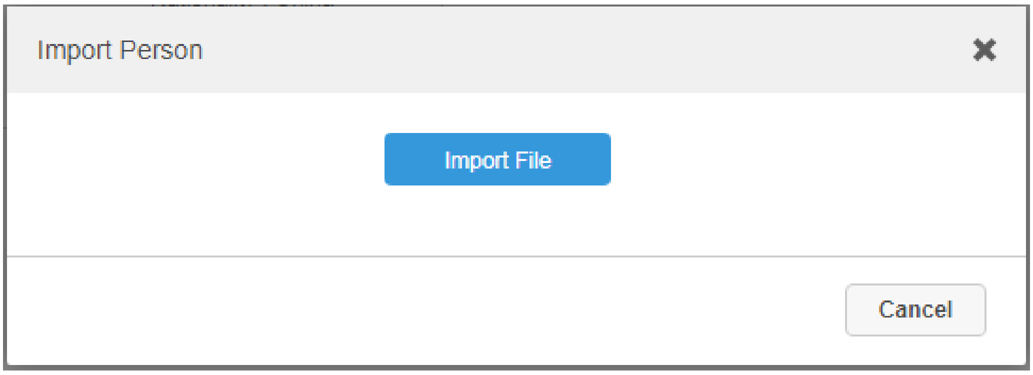
*Name	*ID	*Type	*Gender	Birthday	Nationality	Remark	*Face Image
Jerry	35125	Staff	Male	2018/05/26	China	Joined on October 2th	Face.jpg

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 4-83.

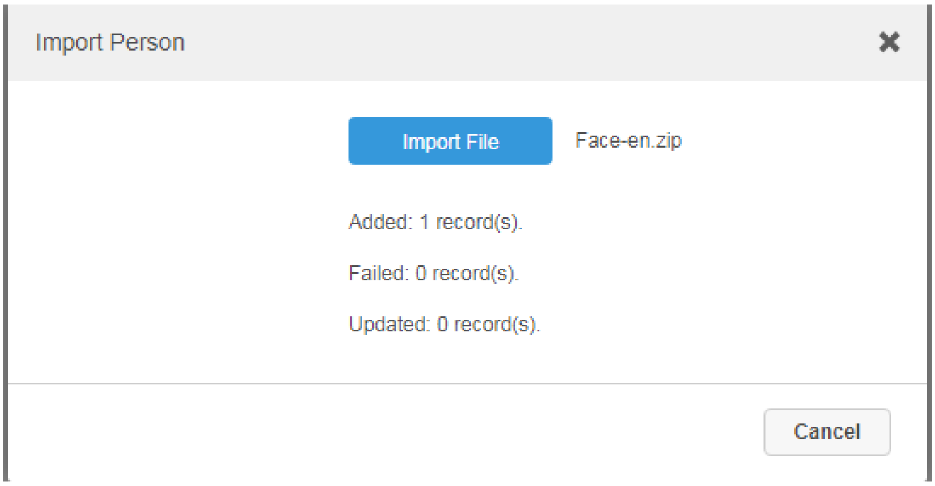
Figure 4-83 Import person



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

The system displays import progress, import info is displayed after import is completed. See Figure 4-84.

Figure 4-84 Import person


Import Person

Import File Face-en.zip

Added: 1 record(s).

Failed: 0 record(s).

Updated: 0 record(s).

Operations

Relevant operation is the same as that in **4.10.1.3.1 Adding Individually**.

4.10.2 Arm Config

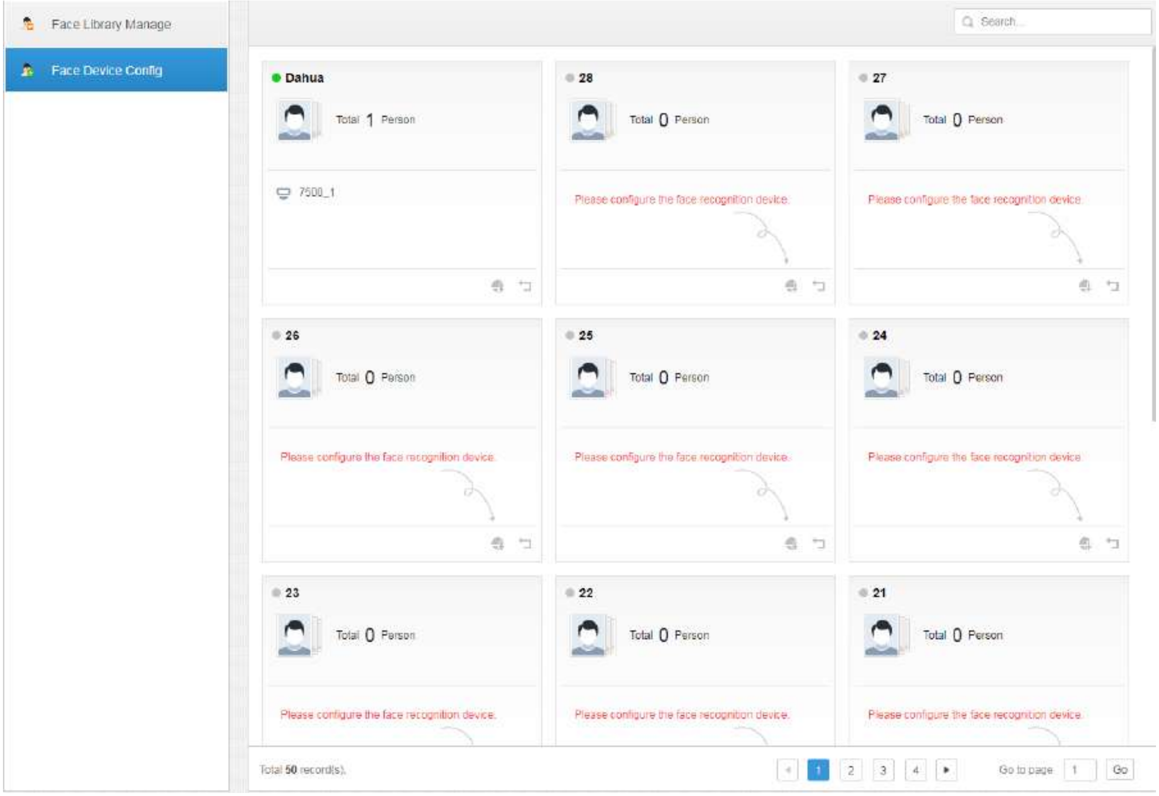
Arm means real-time comparison between capture image and face database image; it will trigger real-time alarm when the similarity reaches the value which has been set. It can make arm upon the face database where the person exists if it needs to take real-time surveillance over the designated person.

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

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

The system displays the interface of **Face Device Config**. See Figure 4-85.

Figure 4-85 Face device config



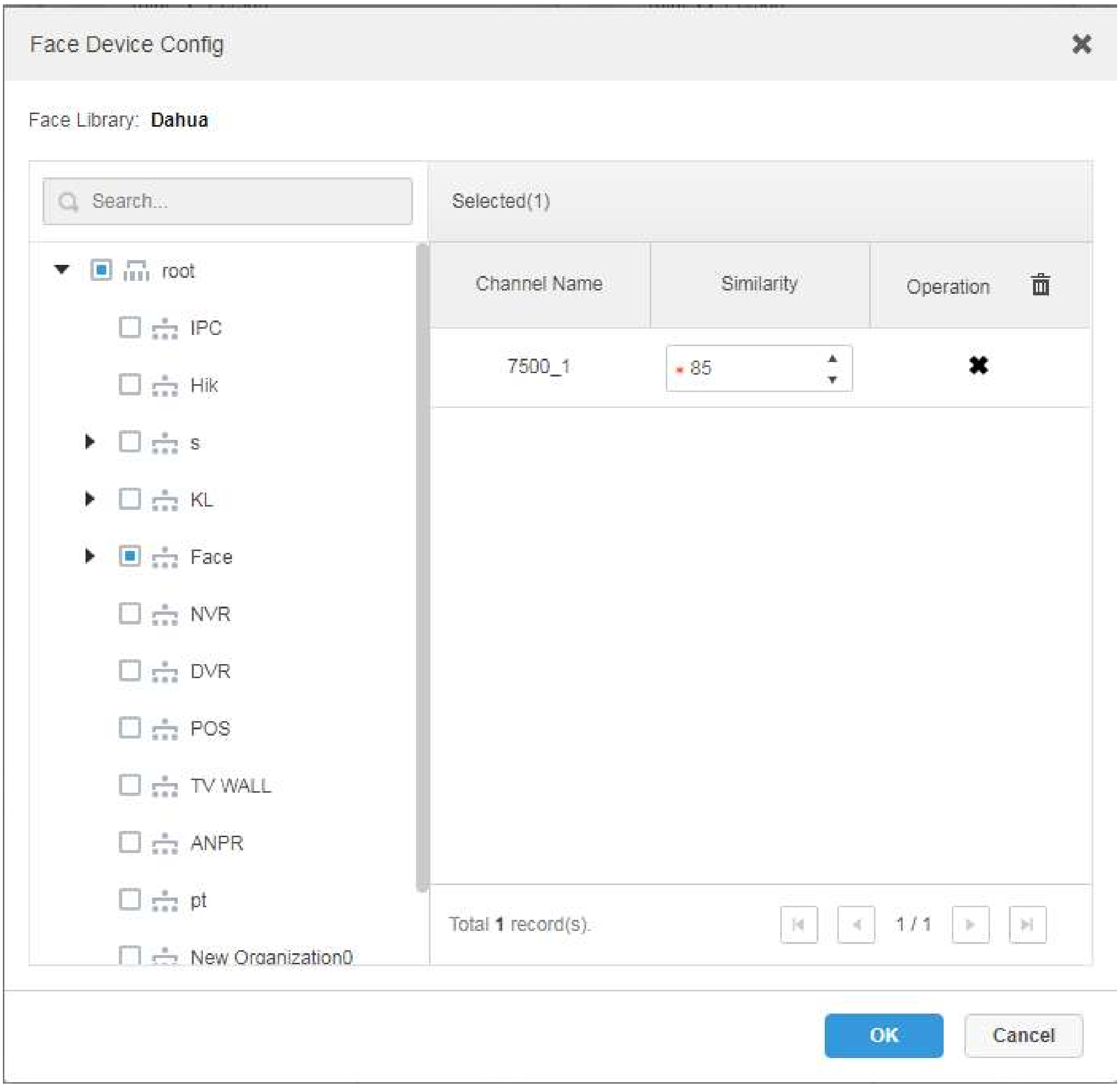
Please configure the face recognition device.

Total 50 record(s).

Step 3 Click to start arm.

The interface is shown in Figure 4-86.

Figure 4-86 Arm



Face Device Config

Face Library: **Dahua**

- ☑ root
  - □ IPC
  - □ Hik
  - □ s
  - □ KL
  - ☑ Face
  - □ NVR
  - □ DVR
  - □ POS
  - □ TV WALL
  - □ ANPR
  - □ pt
  - □ New Organization0

Selected(1)

Channel Name	Similarity	Operation
7500_1	* 85	✖

Total 1 record(s). 1 / 1

Step 4 Select arm channel and set similarity.

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

Operations

- Modify arm

  Arm has been implemented; click and it can modify related device and similarity value on the arm interface.
- Disarm

  Click on the interface of Arm Manage to disarm.

4.11 Adding Vehicle Blacklist

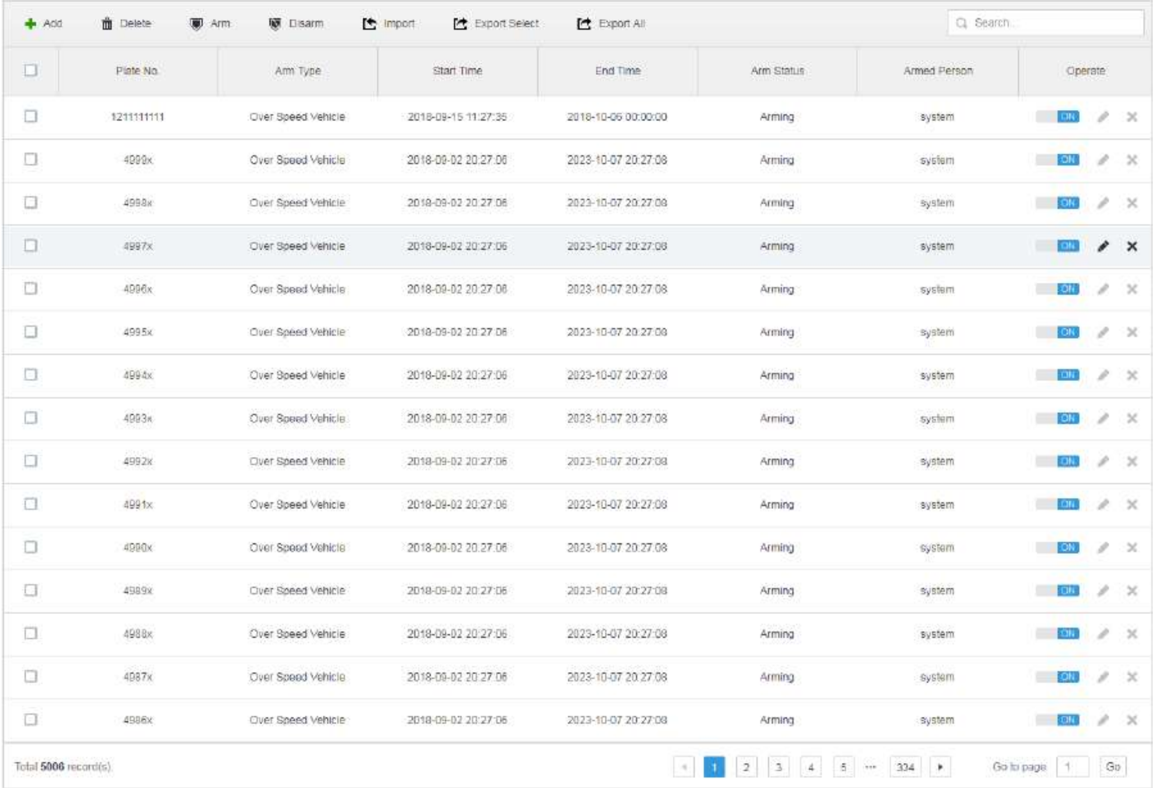
Arm means monitoring vehicles, it will trigger alarm when it takes snapshot and recognizes the vehicle with designated license plate. Arm management includes adding vehicle blacklist, arming and disarming.

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

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

The system displays the interface of **Vehicle Blacklist**. See Figure 4-87.

Figure 4-87 Vehicle blacklist



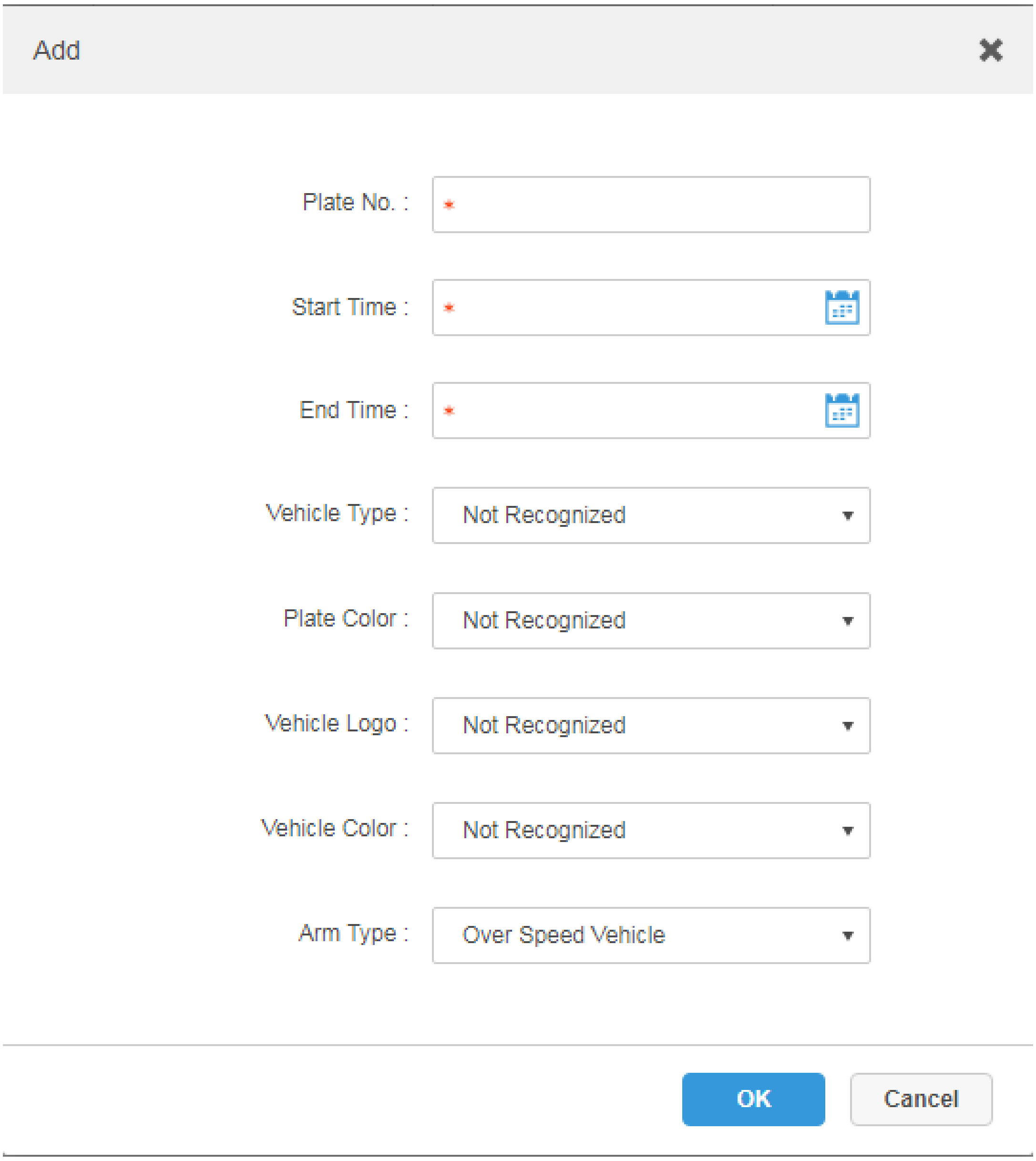
□	Plate No.	Arm Type	Start Time	End Time	Arm Status	Armed Person	Operate
□	1211111111	Over Speed Vehicle	2018-09-15 11:27:35	2018-10-05 00:00:00	Arming	system	ON ✎ ✕
□	4999x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4998x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4997x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4996x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4995x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4994x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4993x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4992x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4991x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4990x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4989x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4988x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4987x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕
□	4986x	Over Speed Vehicle	2018-09-02 20:27:06	2023-10-07 20:27:08	Arming	system	ON ✎ ✕

Total **5006** record(s)

Step 2 Click **Add**.

The system displays the interface of **Add**. See Figure 4-88.

Figure 4-88 Add



Add ✖

Plate No. : *

Start Time : *

End Time : *

Vehicle Type : Not Recognized

Plate Color : Not Recognized

Vehicle Logo : Not Recognized

Vehicle Color : Not Recognized

Arm Type : Over Speed Vehicle

OK Cancel

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.

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.

4.12 Video Intercom Management

4.12.1 Configuring Building/Unit

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

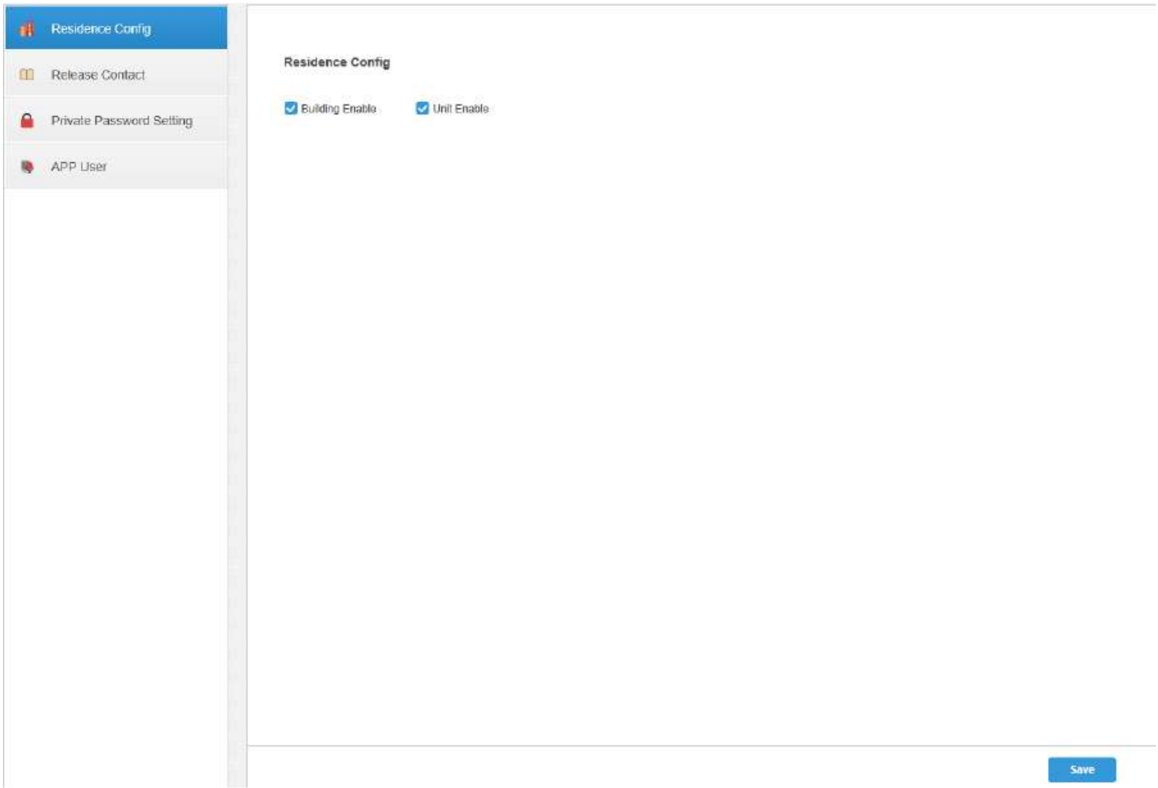
- If building is enabled, unit is not enabled, and then the number is “1#1001”.
- If building is enabled, unit is enabled as well, and then the number is “1#2#1001”.
- If building is not enabled, unit is not enabled either, and then the number is “1001”.

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

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

The system displays the interface of **Residence Config**. See Figure 4-89

Figure 4-89 Residence config



Residence Config

☑ Building Enable ☑ Unit Enable

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

4.12.2 Synchronizing Contacts

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

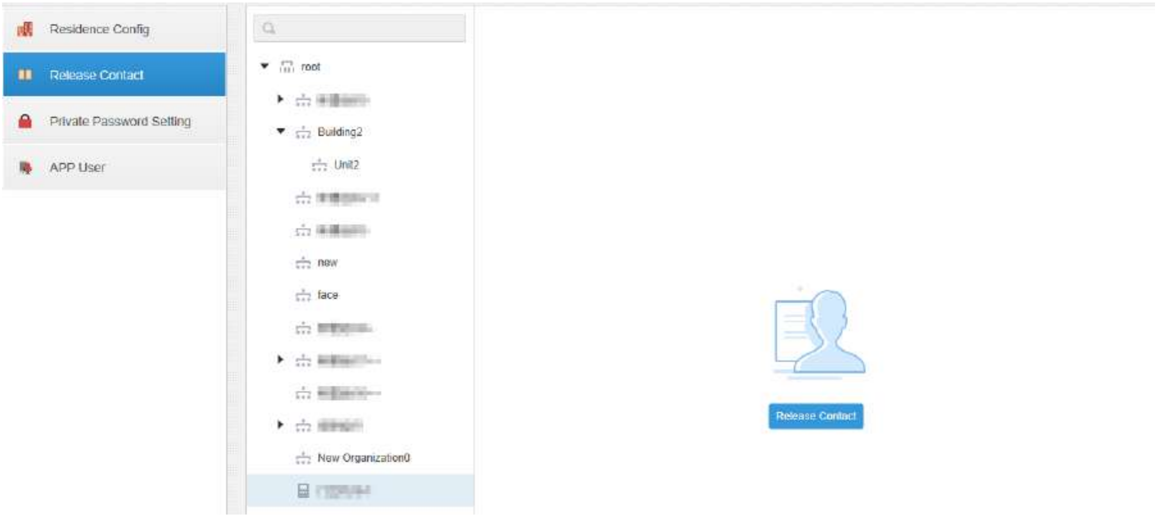
Step 1 Click + and select **Video Intercom Management** on the interface.

The system displays the interface of **Video Intercom Management**.

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

The system displays the interface of **Release Contact**. See Figure 4-90.

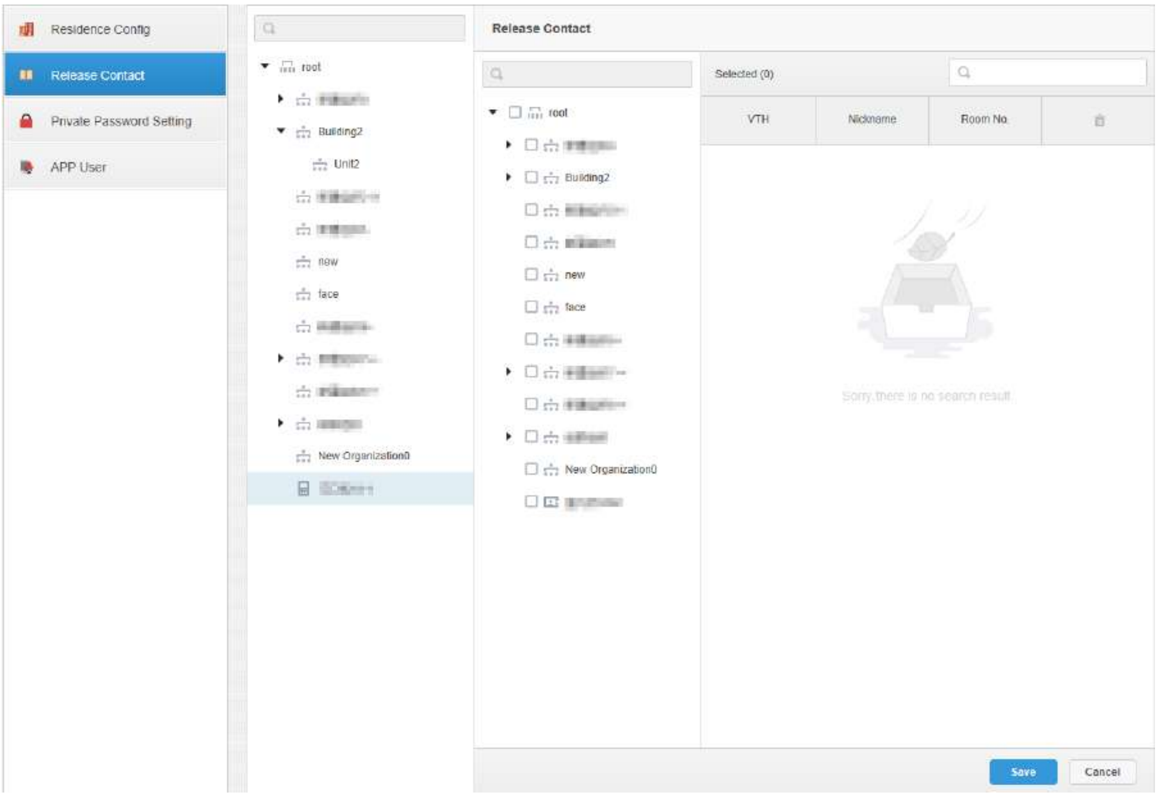
Figure 4-90 Release contact



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

The system displays the information of all the VTH bound by VTO. See Figure 4-91.

Figure 4-91 Select VTH



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

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

4.12.3 Setting Private Password

Set the unlock password of corresponding VTO bound by VTH.

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

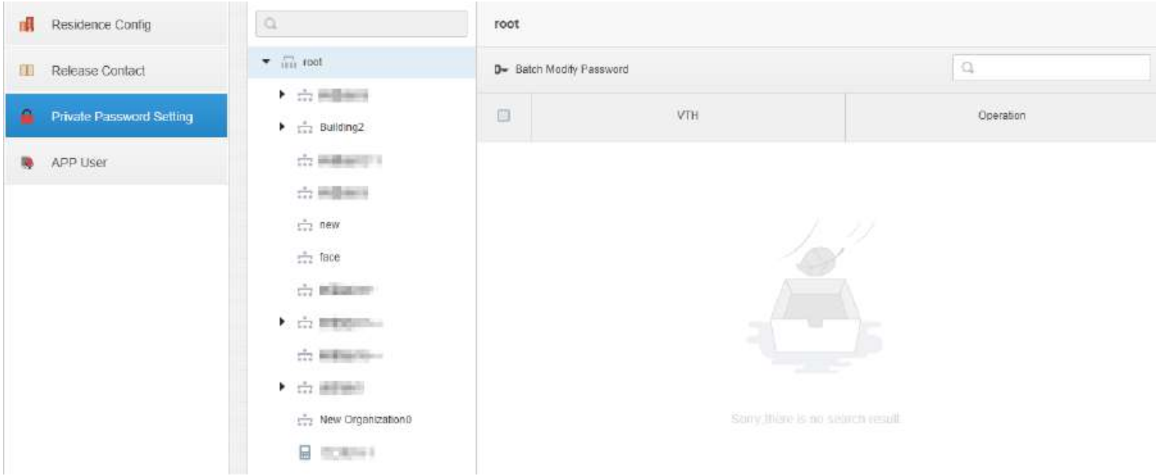
Step 1 Click+ and select **Video Intercom Management** on the interface.

The system displays the interface of **Video Intercom Management**.

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

The system displays the interface of **Private Password Setting**. See Figure 4-92。

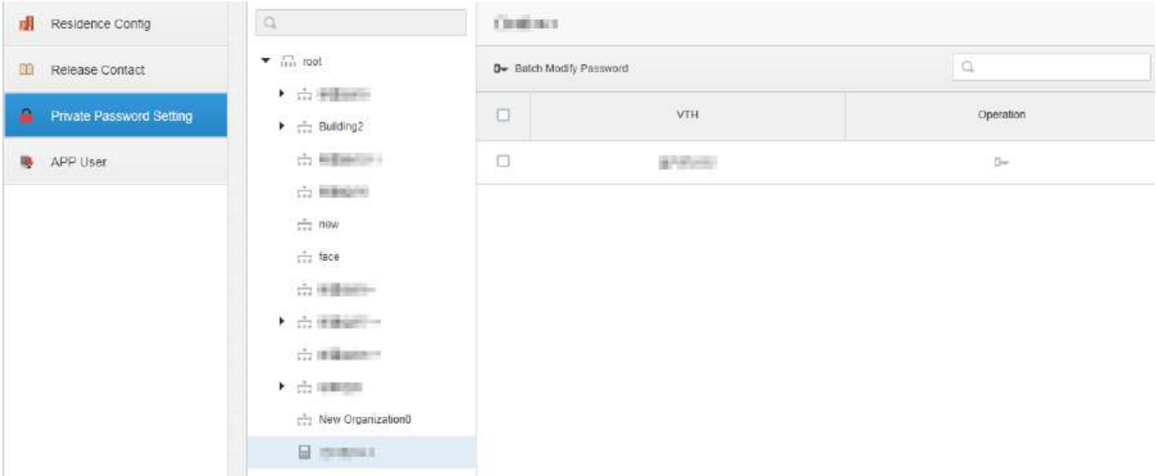
Figure 4-92 Private password setting



Step 3 Select organization node (VTO).

The system displays the information of all VTH bound by VTO. See Figure 4-93.

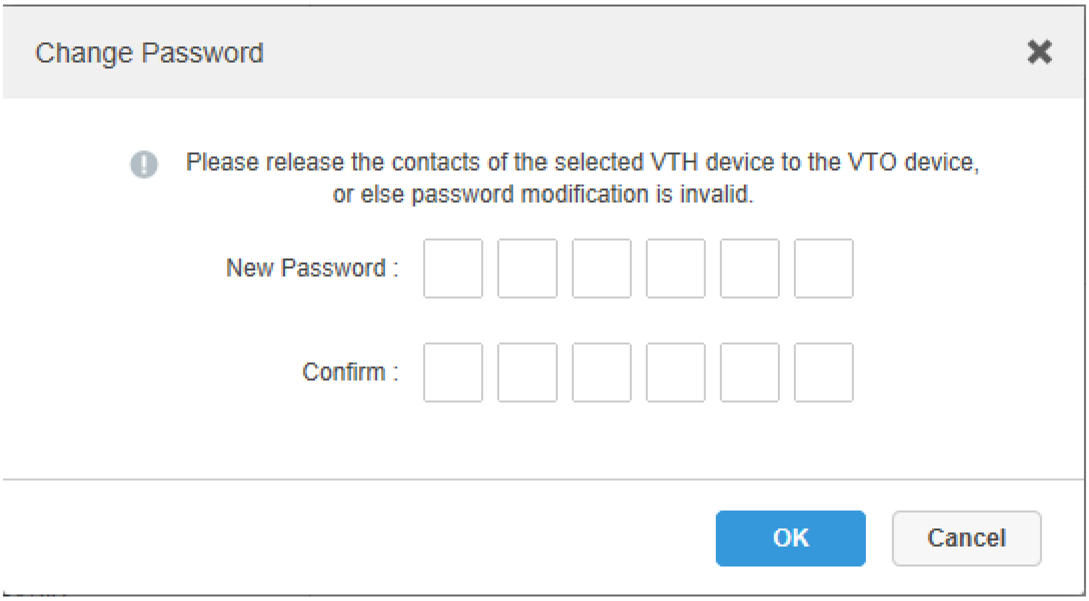
Figure 4-93 Select VTH



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

The interface of **Modify Password** is displayed. See Figure 4-94.

Figure 4-94 Modify password



Please release the contacts of the selected VTH device to the VTO device, or else password modification is invalid.

Step 5 Enter password, click **OK.**

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

4.12.4 APP User

Support viewing information of APP users, freeze user, modify login password and delete user.

📖

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

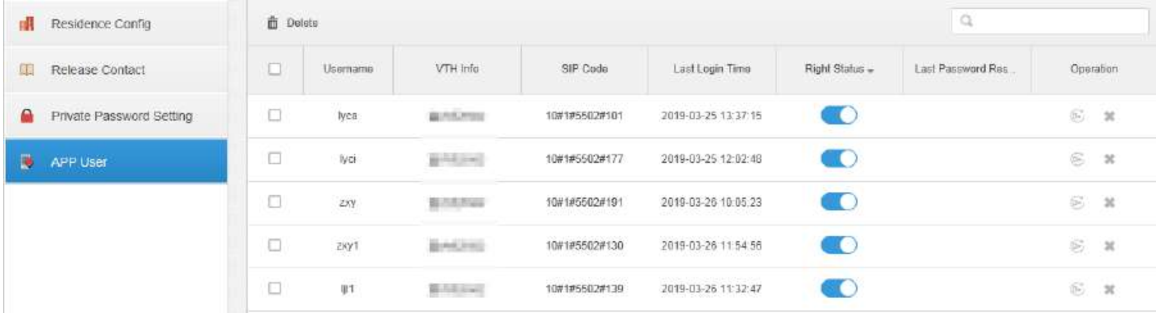
Step 1 Click + and select **Video Intercom Management** on the interface.

The system displays the interface of **Video Intercom Management**.

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

The system displays the interface of **APP User** and information of all registered APP users. See Figure 4-95. Refer to Table 4-5 for more operation details.

Figure 4-95 App user



□	Username	VTH Info	SIP Code	Last Login Time	Right Status	Last Password Res...	Operation
□	lyca	[redacted]	10#1#5502#101	2019-03-25 13:37:15	ON		🔑 ✖
□	lyci	[redacted]	10#1#5502#177	2019-03-25 12:02:48	ON		🔑 ✖
□	zxy	[redacted]	10#1#5502#191	2019-03-26 10:05:23	ON		🔑 ✖
□	zxy1	[redacted]	10#1#5502#130	2019-03-26 11:54:56	ON		🔑 ✖
□	ljl1	[redacted]	10#1#5502#139	2019-03-26 11:32:47	ON		🔑 ✖

Table 4-5 Operation description

Operation	Description
Freeze APP user	After APP user is frozen, it fails to log in within 600s. ON means normal status, OFF means freezes status, both statuses can be switched 📖 The account will be frozen when invalid password attempts exceeds 5 by APP user.
Modify APP user login passowrd	Click 🔑 and enter new password on the interface of **Reset Passoword**. Click OK. 📖 ● The password shall be between 8 and 16 characters, including number and letter. ● 👁 means password can be seen while ⌒ means password is protected. Click icon to switch.
Delete APP user	Click ✖ or select APP user (several users can be selected); click **Delete** and the selected users will be deleted according to the interface tips.

4.13 System Maintenance

4.13.1 Server Management

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

4.13.1.1 Server Management

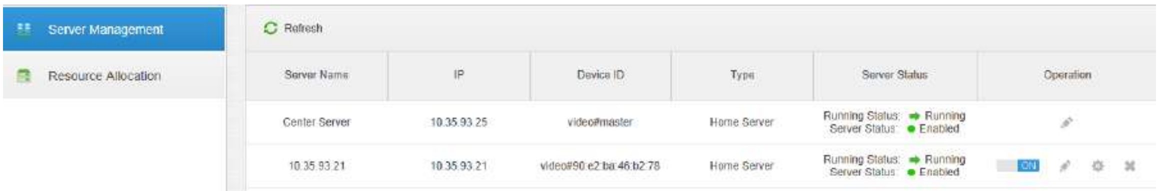
Server management supports a series of operations, such as switching master/spare mode of server, modifying server name, enabling or disabling service.

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

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

The system displays the interface of **Server Management**. See Figure 4-96.

Figure 4-96 Service management



Server Name	IP	Device ID	Type	Server Status	Operation
Center Server	10.35.93.25	video#master	Home Server	Running Status: ➡ Running Server Status: ● Enabled	✎
10.35.93.21	10.35.93.21	video#90:e2:ba:46:b2:78	Home Server	Running Status: ➡ Running Server Status: ● Enabled	ON ✎ ⚙ ✖

Step 3 The management server supports following operations:

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

4.13.1.2 Resource Allocation

Adjust the device server during distributed deployment.

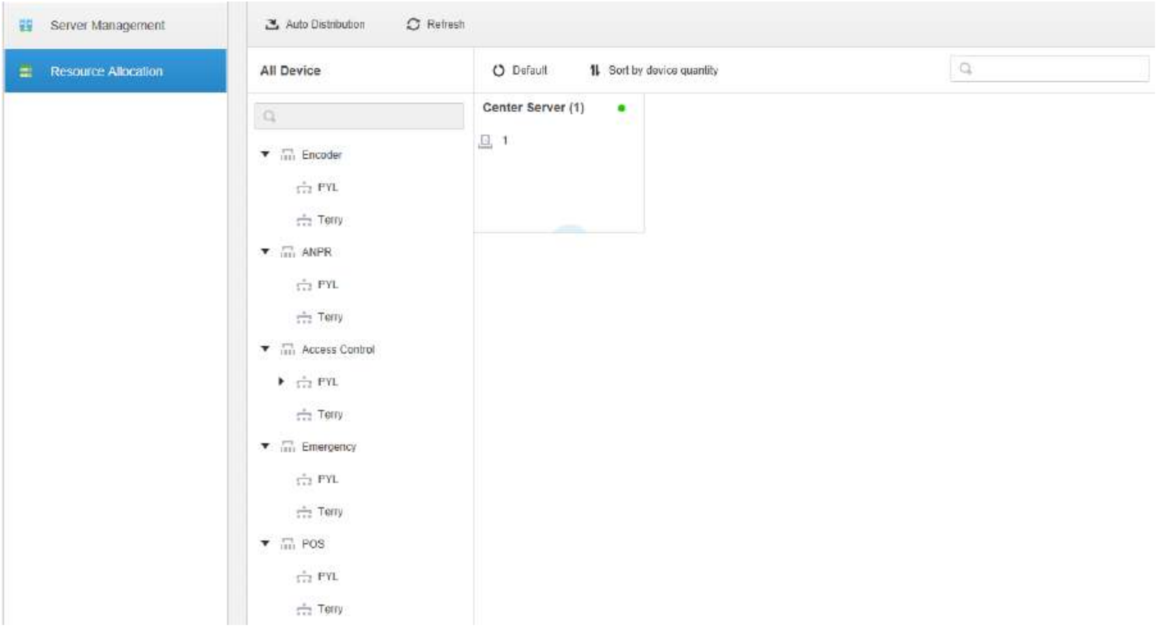
Step 1 Click + and select **Server Management** on the interface of **New Tab**.

Step 2 Click the tab of **Resource Allocation**.

The system displays the interface of **Resource Allocation**. See Figure 4-97.

- Click Default and the servers will be sorted according to the time when they are added.
- Click Sort by device quantity and the servers will be sorted according to quantity of devices attached to them.

Figure 4-97 Resource allocation



Step 3 Adjust the attached server.

- Manual adjustment

Select the device on the left and drag it to the server on the right. The device quantity of attached server will increase while the device quantity of original server will decrease.

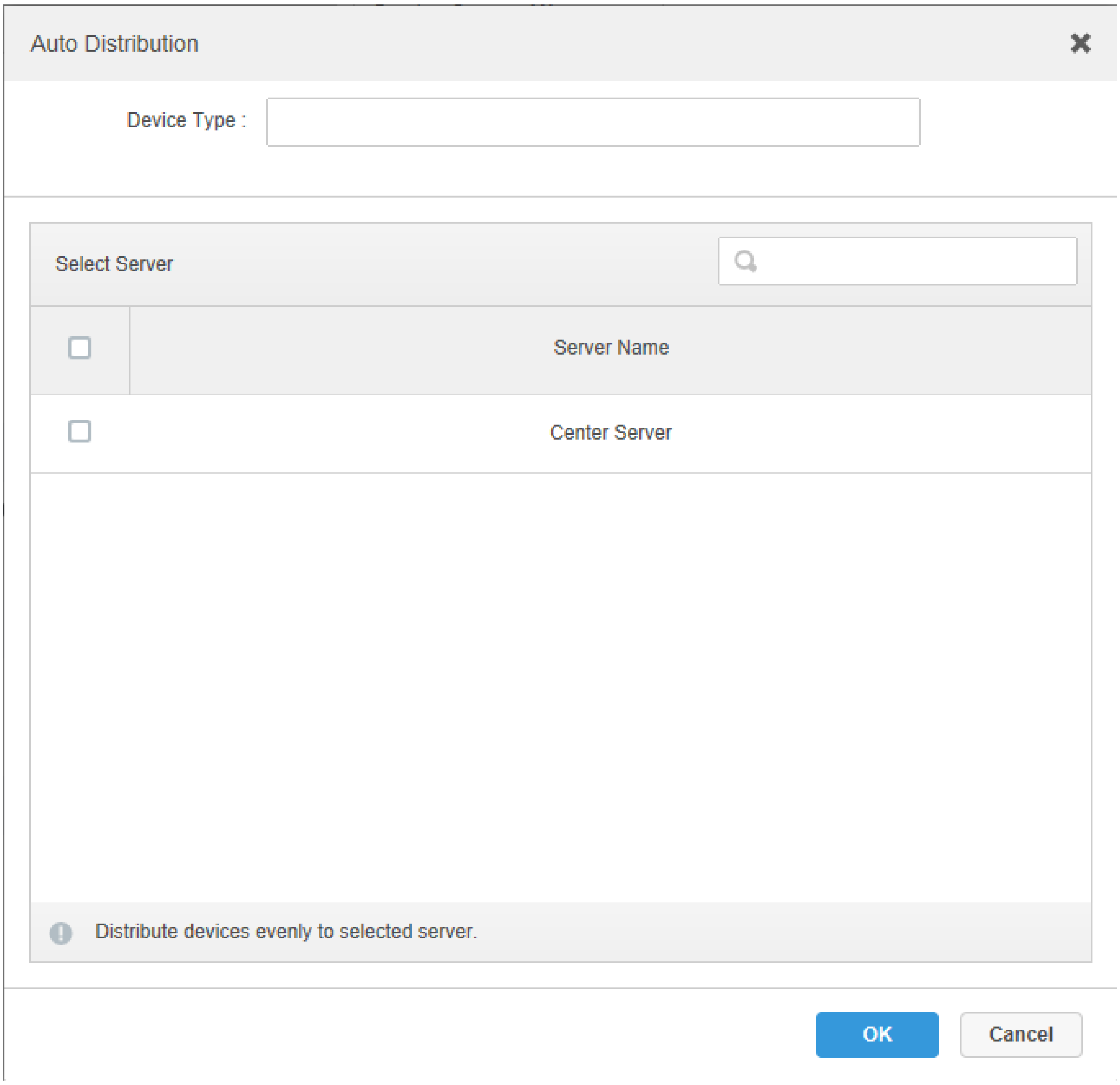
- Auto distribution

  Averagely distribute the same type of device to the server that is deployed by distribution.

1) Click **Auto Distributio**n.

   The system displays the interface of **Auto Distribution**. See Figure 4-98.

Figure 4-98


Auto Distribution

Device Type :

Select Server

☐	Server Name
☐	Center Server

Distribute devices evenly to selected server.

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

4.13.2 Backup and Restore

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

📖

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

4.13.2.1 System Backup

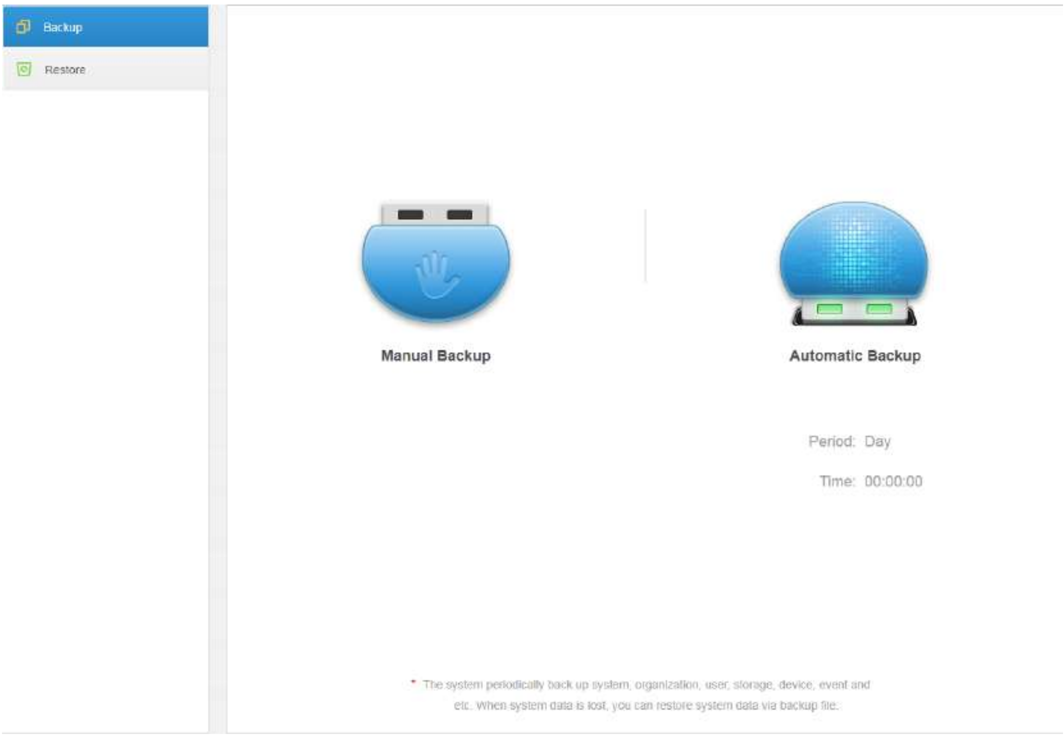
In order to guarantee the security of user data, DSS platform system provides data backup function. The backup includes manual backup and automatic backup.

Manual Backup

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

The system displays the interface of **Backup**. See Figure 4-99.

Figure 4-99 Backup



Period: Day

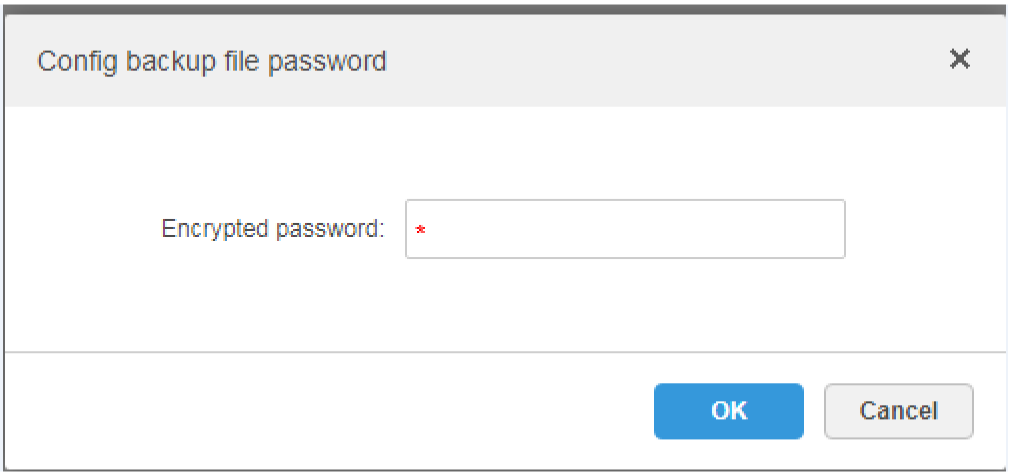
Time: 00:00:00

* The system periodically back up system, organization, user, storage, device, event and etc. When system data is lost, you can restore system data via backup file.

Step 2 Click **Manual Backup**.

The system displays the interface which is shown in Figure 4-100.

Figure 4-100 Backup file password setting



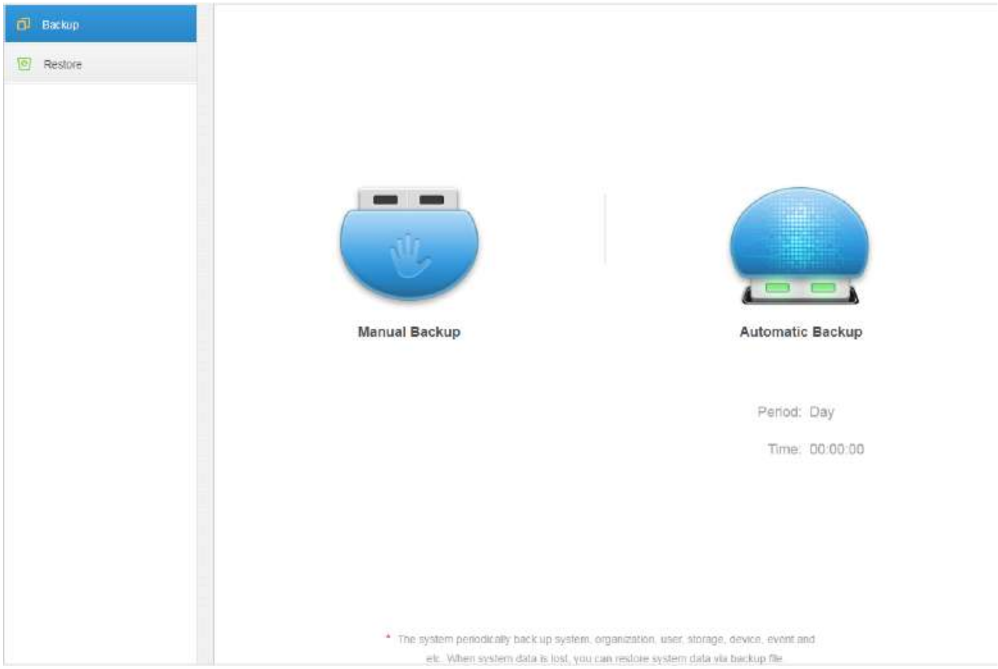
Config backup file password

Encrypted password: *

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

The backup result is displayed in Figure 4-101.

Figure 4-101 Backup result



Period: Day

Time: 00:00:00

* The system periodically back up system, organization, user, storage, device, event and etc. When system data is lost, you can restore system data via backup file

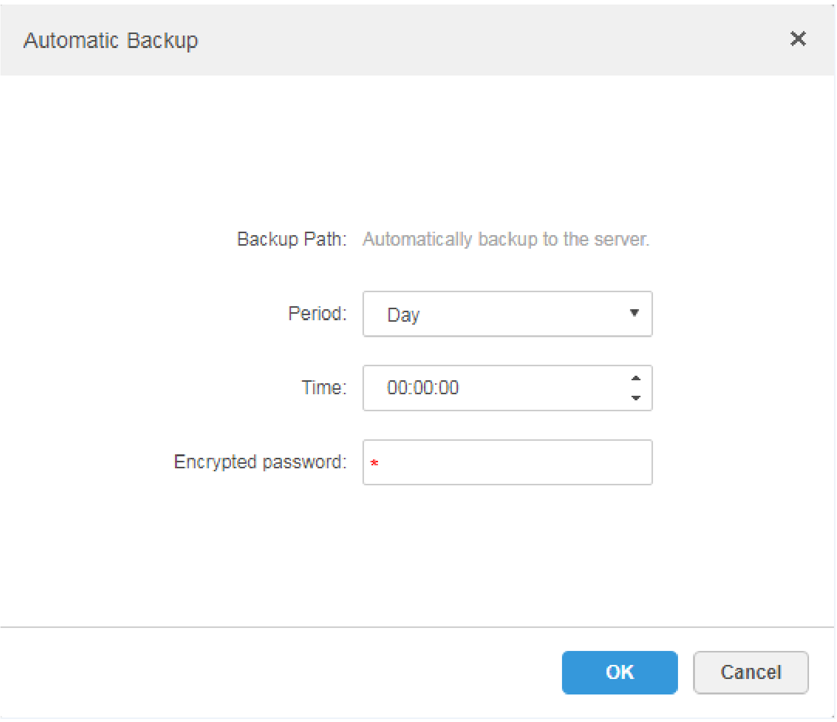
Automatic Backup

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

Step 2 Click **Automatic Backup**.

The system pops out the interface of **Automatic Backup**. See Figure 4-102.

Figure 4-102 Auto backup



Backup Path: Automatically backup to the server.

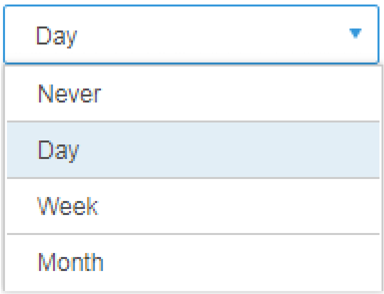
Period: Day

Time: 00:00:00

Encrypted password: *

Step 3 Select backup period, it includes: never, day, week, and month. See Figure 4-103.

Figure 4-103 Backup period

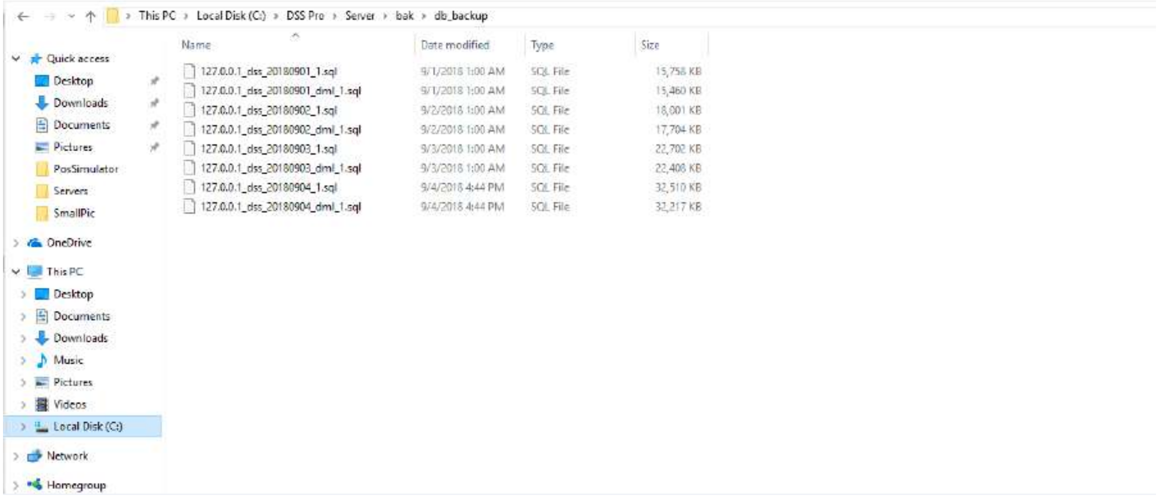


Step 4 Click **OK** to save config.

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 4-104.

Figure 4-104 View backup directory



Name	Date modified	Type	Size
127.0.0.1_dss_20180901_1.sql	9/1/2018 1:00 AM	SQL File	15,758 KB
127.0.0.1_dss_20180901_dml_1.sql	9/1/2018 1:00 AM	SQL File	15,460 KB
127.0.0.1_dss_20180902_1.sql	9/2/2018 1:00 AM	SQL File	18,001 KB
127.0.0.1_dss_20180902_dml_1.sql	9/2/2018 1:00 AM	SQL File	17,704 KB
127.0.0.1_dss_20180903_1.sql	9/3/2018 1:00 AM	SQL File	22,702 KB
127.0.0.1_dss_20180903_dml_1.sql	9/3/2018 1:00 AM	SQL File	22,408 KB
127.0.0.1_dss_20180904_1.sql	9/4/2018 4:44 PM	SQL File	32,510 KB
127.0.0.1_dss_20180904_dml_1.sql	9/4/2018 4:44 PM	SQL File	32,217 KB

4.13.2.2 System Restore

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

⚠

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

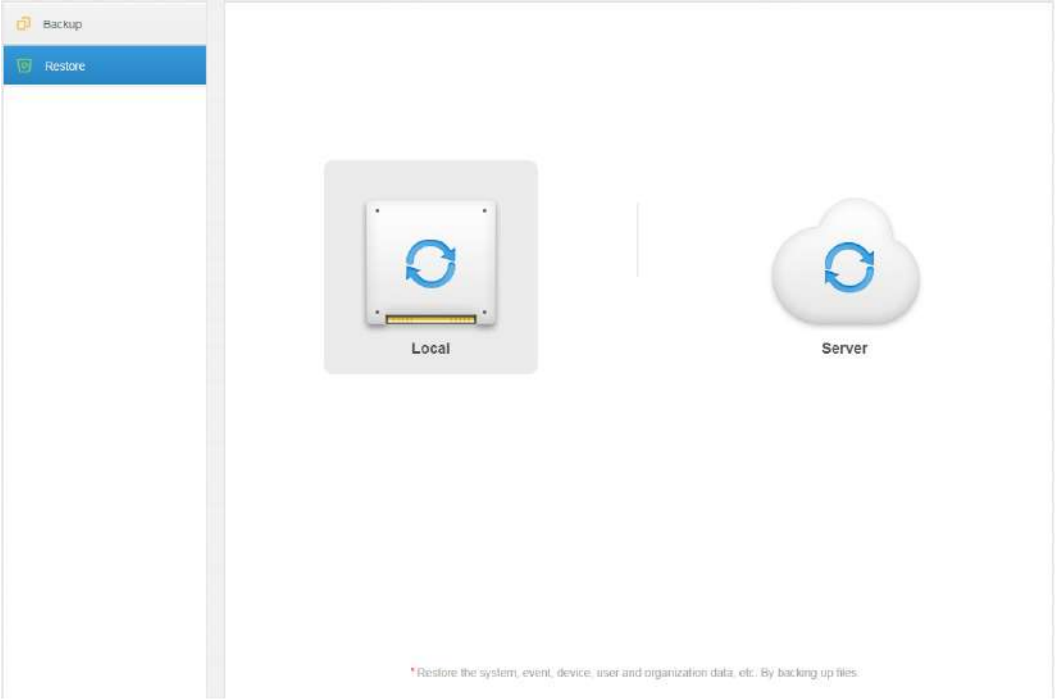
Local

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

Step 1 Select **Restore** tab.

The system enters the interface of **Restore**. See Figure 4-105.

Figure 4-105 System restore

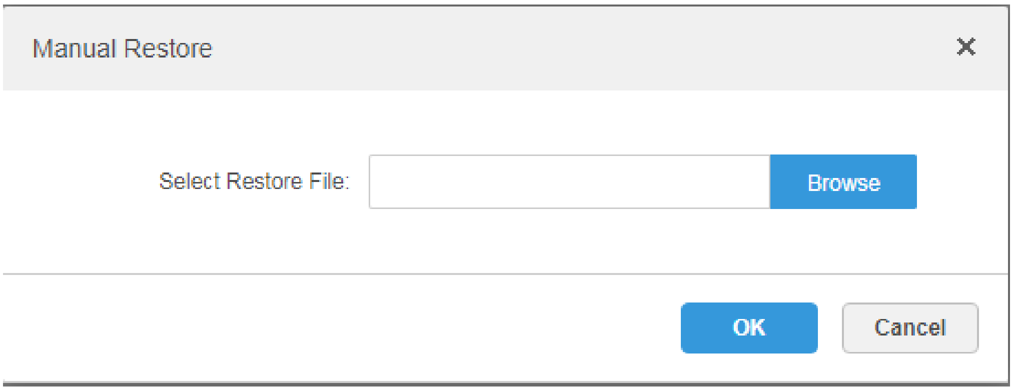


*Restore the system, event, device, user and organization data, etc. By backing up files.

Step 2 Click **Local**.

The interface is shown in Figure 4-106.

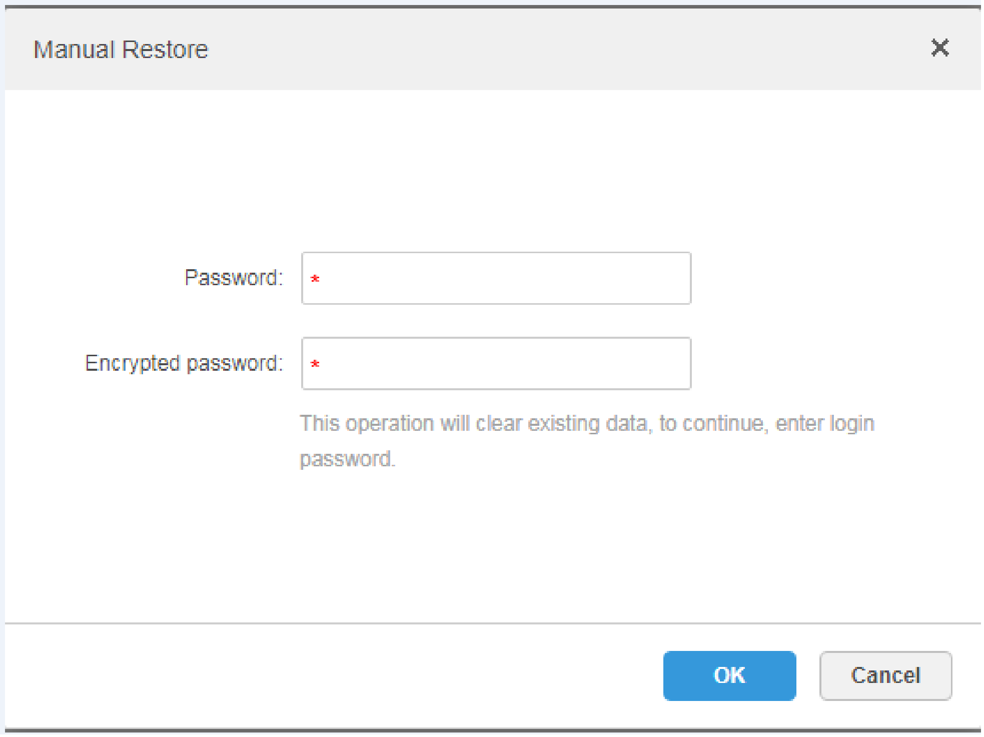
Figure 4-106 Select backup file path



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

Step 4 Enter administrator login **Password** and backup file **Encrypted Password**. See Figure 4-107.

Figure 4-107 Enter password


Manual Restore

Password: *

Encrypted password: *

This operation will clear existing data, to continue, enter login password.

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.

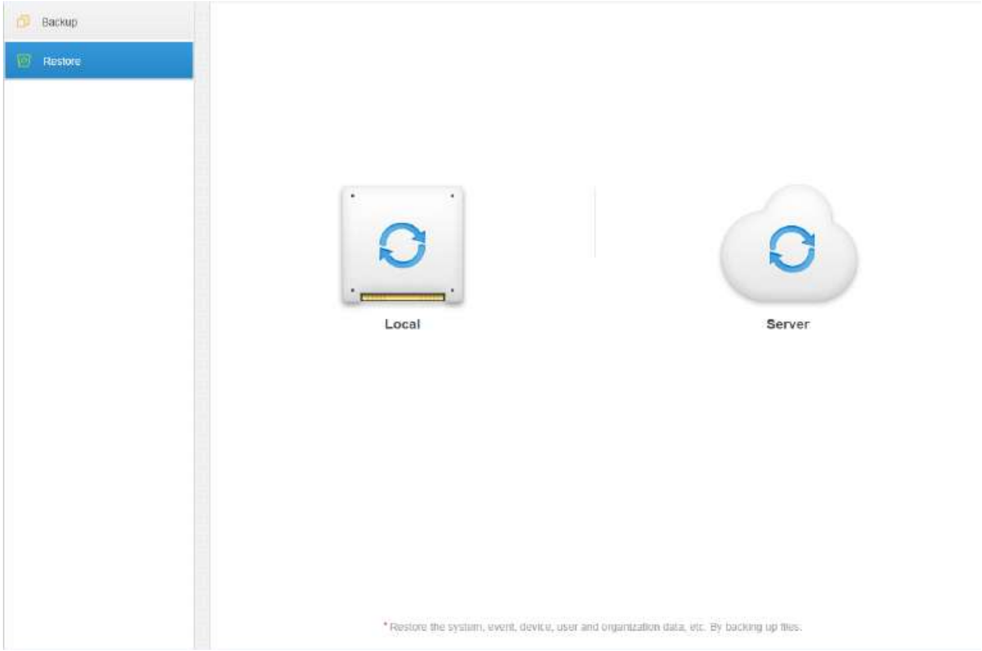
Server

You can select to restore the data from the backup file on the server side. The precondition is that you need to enable the auto backup function, the server end backs up the database according to the set period and form backup file.

Step 1 Select **Restore** tab.

The system enters the interface of **Restore**. See Figure 4-108.

Figure 4-108 System restore



* Restore the system, event, device, user and organization data, etc. By backing up files.

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).

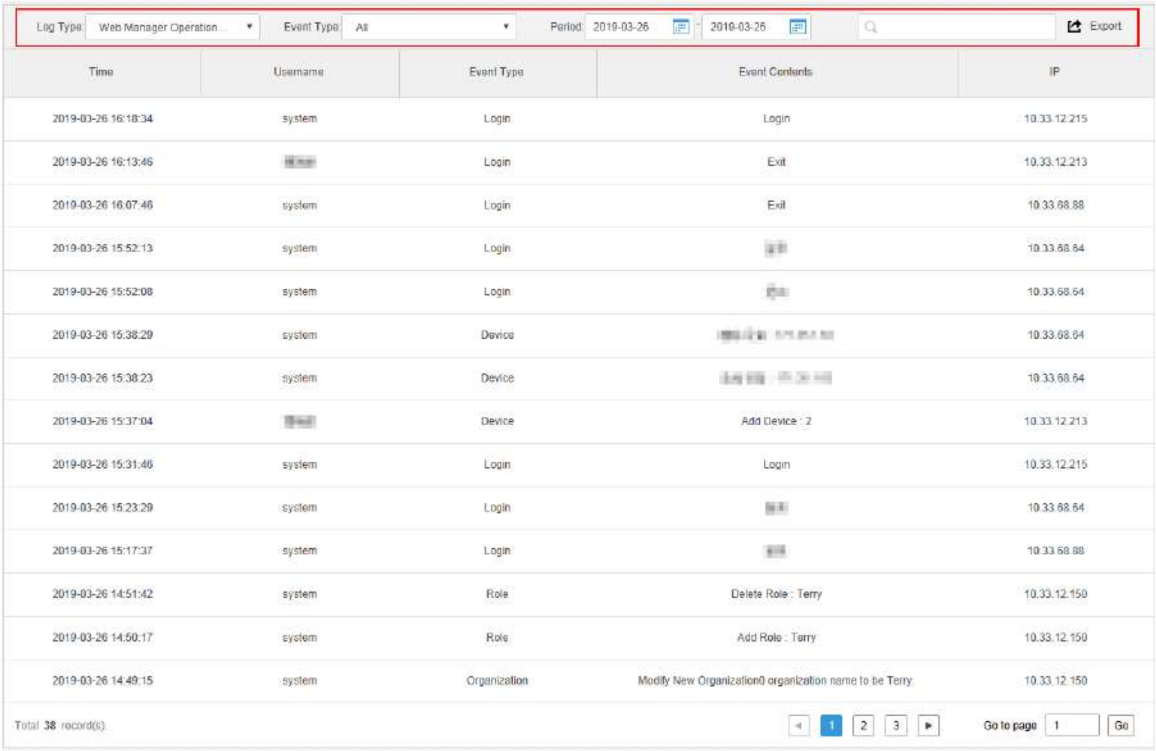
Take **Management Configuring Log** for an example.

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 4-109.

Figure 4-109 Log



Log Type: Web Manager Operation... ▾ Event Type: All ▾ Period: 2019-03-26 - 2019-03-26 Export

Time	Username	Event Type	Event Contents	IP
2019-03-26 16:18:34	system	Login	Login	10.33.12.215
2019-03-26 16:13:46	[redacted]	Login	Exit	10.33.12.213
2019-03-26 16:07:46	system	Login	Exit	10.33.68.88
2019-03-26 15:52:13	system	Login	[redacted]	10.33.68.64
2019-03-26 15:52:08	system	Login	[redacted]	10.33.68.64
2019-03-26 15:38:29	system	Device	[redacted]	10.33.68.64
2019-03-26 15:38:23	system	Device	[redacted]	10.33.68.64
2019-03-26 15:37:04	[redacted]	Device	Add Device : 2	10.33.12.213
2019-03-26 15:31:46	system	Login	Login	10.33.12.215
2019-03-26 15:23:29	system	Login	[redacted]	10.33.68.64
2019-03-26 15:17:37	system	Login	[redacted]	10.33.68.88
2019-03-26 14:51:42	system	Role	Delete Role : Terry	10.33.12.150
2019-03-26 14:50:17	system	Role	Add Role : Terry	10.33.12.150
2019-03-26 14:49:15	system	Organization	Modify New Organization0 organization name to be Terry	10.33.12.150

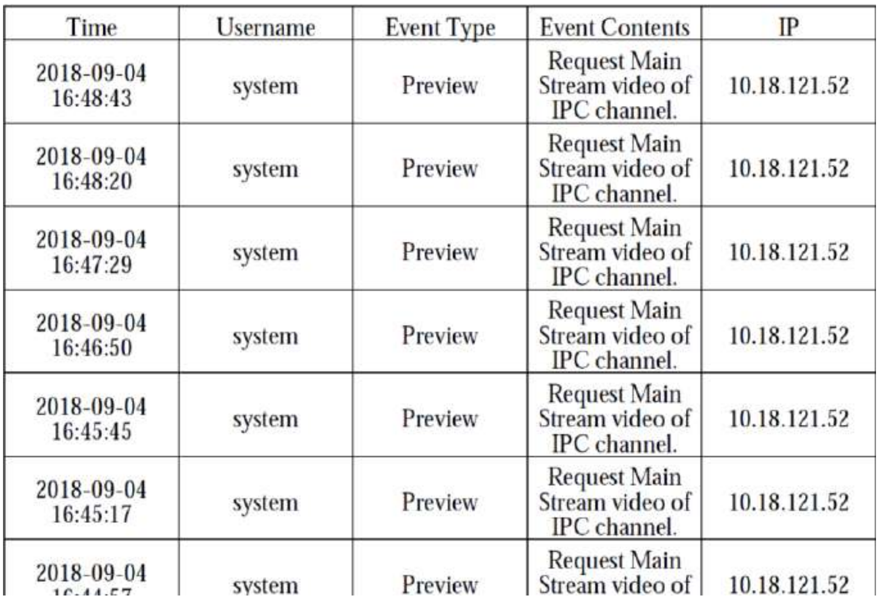
Total 38 record(s) ◂ 1 2 3 ▸ Go to page 1 Go

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 4-110.

Figure 4-110 Log record



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	10.18.121.52

4.13.4 Overview

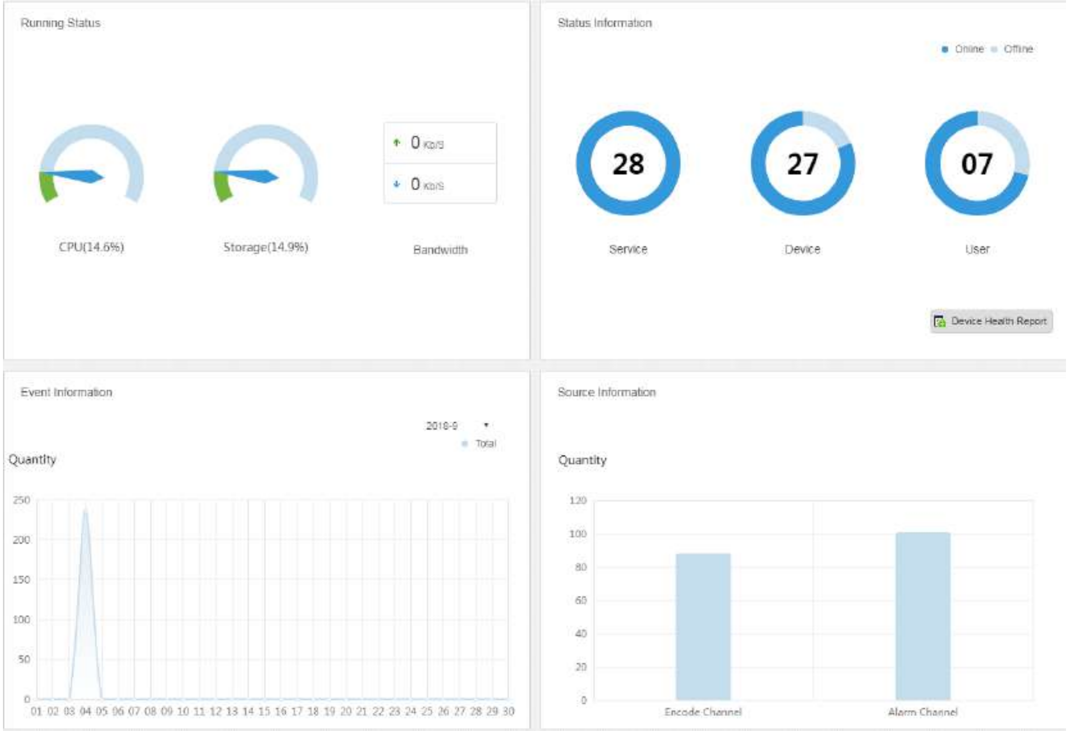
DSS platform supports function of inquiring system operation and maintenance statistics, which is to know the system running situation in time.

4.13.4.1 Overview

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

The system displays the interface of **Overview**. See Figure 4-111.

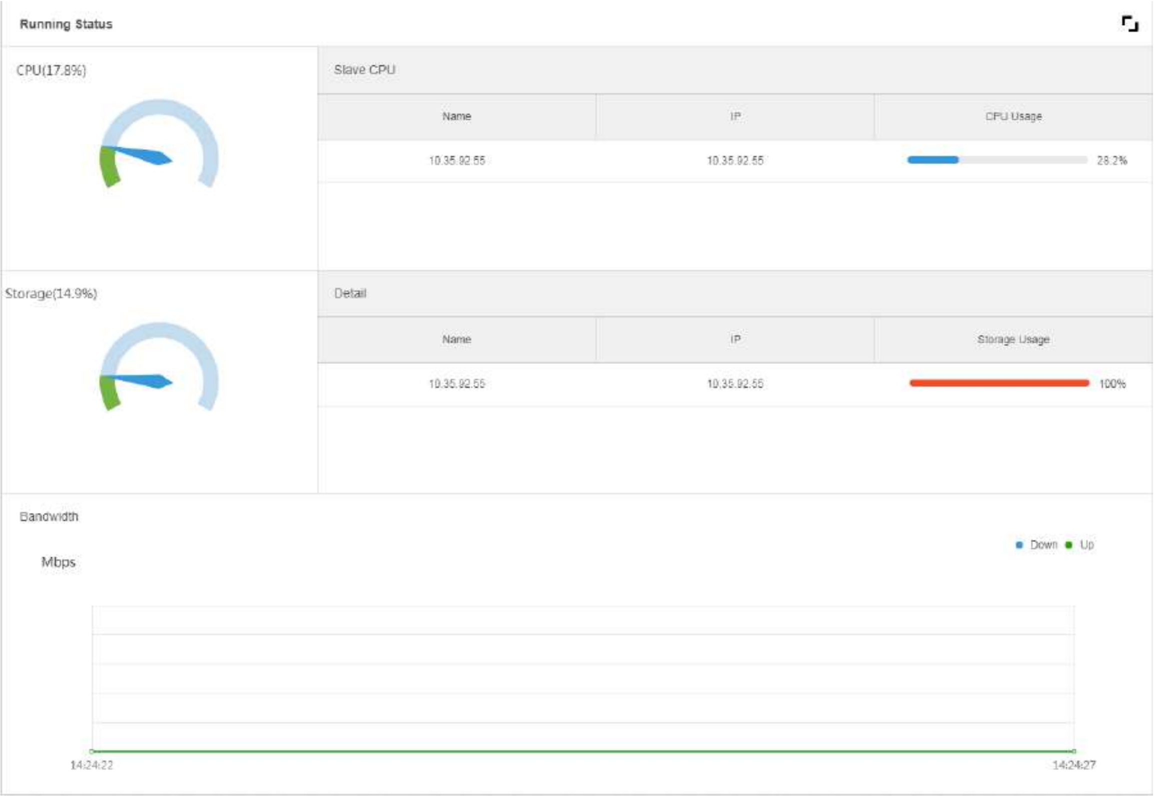
Figure 4-111 Overview



4.13.4.2 Running Status

Check CPU, storage, bandwidth and so on; click **Running Status** or the icon below and jump to the detail interface. See Figure 4-112.

Figure 4-112 System info



Running Status

CPU(17.8%)

Slave CPU

Name	IP	CPU Usage
10.35.92.55	10.35.92.55	28.2%

Storage(14.9%)

Detail

Name	IP	Storage Usage
10.35.92.55	10.35.92.55	100%

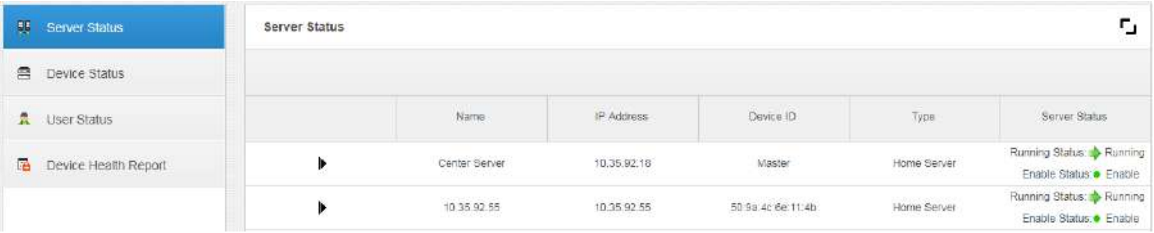
4.13.4.3 Status Information

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 4-113.

Figure 4-113 Service status



Server Status

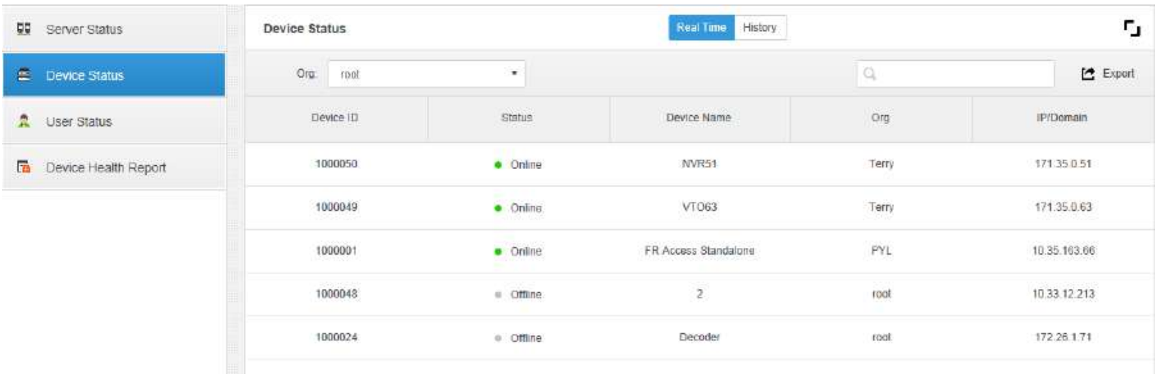
	Name	IP Address	Device ID	Type	Server Status
▶	Center Server	10.35.92.18	Master	Home Server	Running Status: Running Enable Status: ● Enable
▶	10.35.92.55	10.35.92.55	50:9a:4c:6e:11:4b	Home Server	Running Status: Running Enable Status: ● Enable

Device Status Information

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

The system will display device real-time status by default. See Figure 4-114.

Figure 4-114 Device realtime status

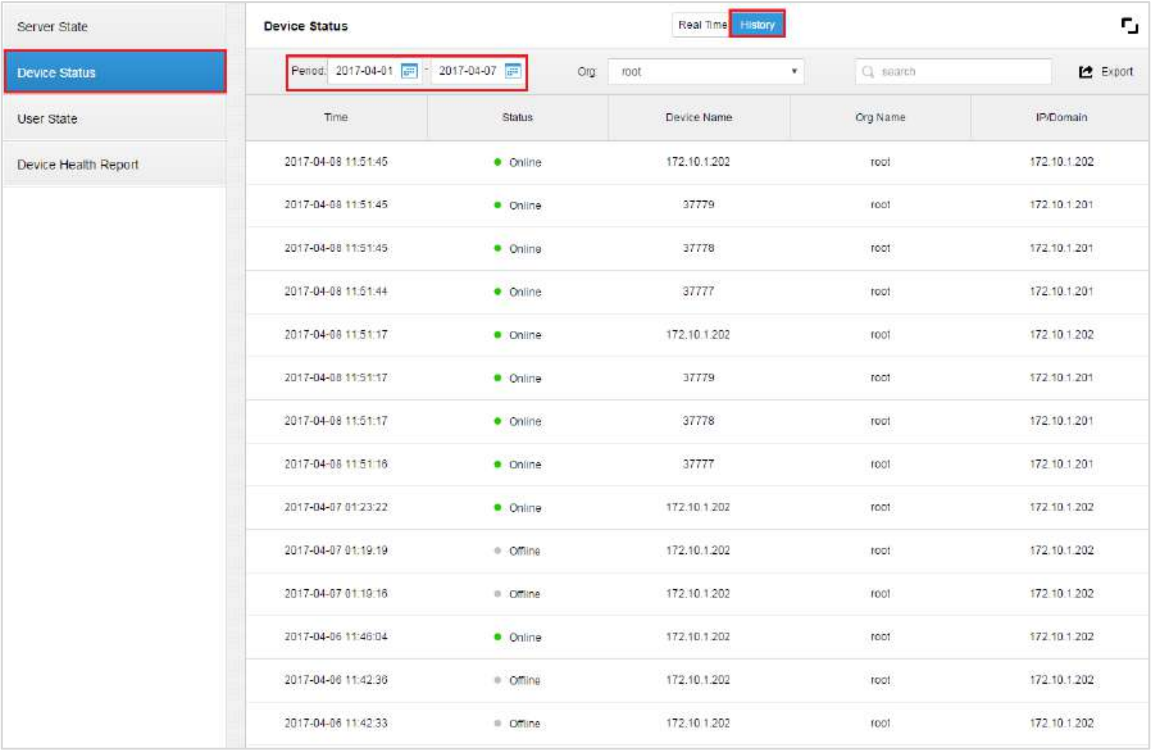


Device ID	Status	Device Name	Org	IP/Domain
1000050	● Online	NVR51	Terry	171.35.0.51
1000049	● Online	VTO63	Terry	171.35.0.63
1000001	● Online	FR Access Standalone	PYL	10.35.163.66
1000048	● Offline	2	root	10.33.12.213
1000024	● Offline	Decoder	root	172.26.1.71

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 4-115.

Figure 4-115 History status



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**.

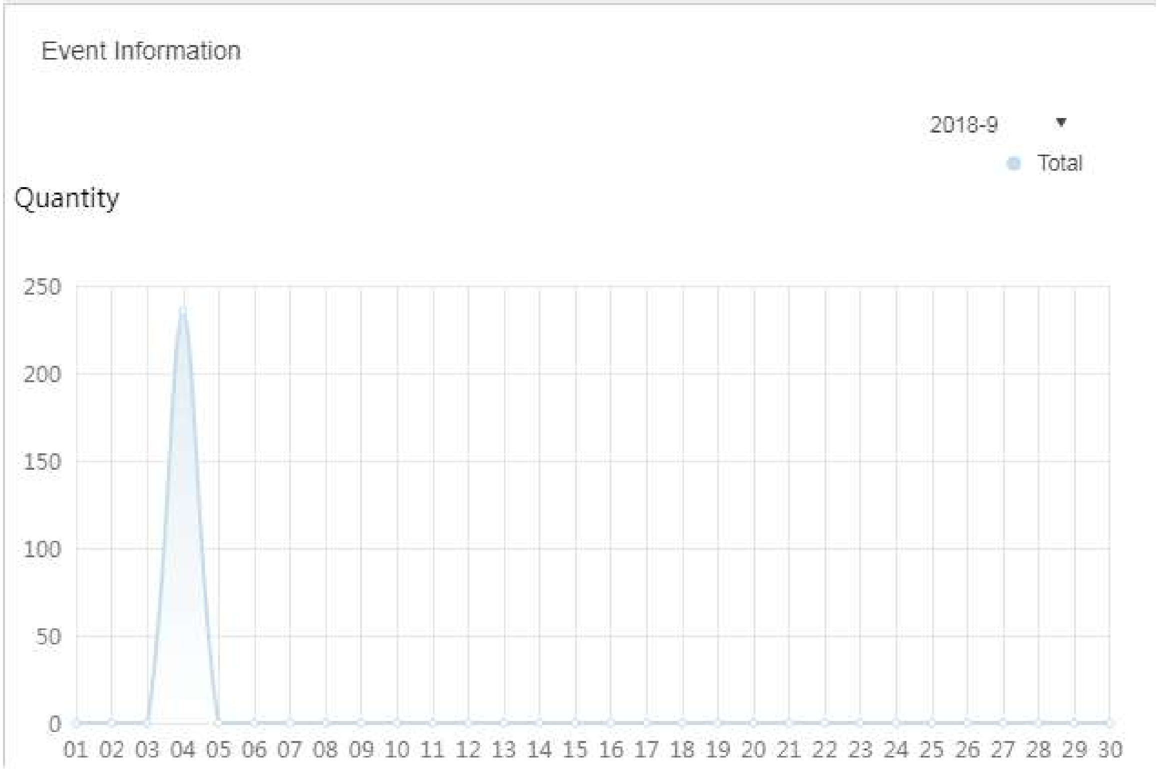
Export device realtime status information (PDF format).

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

4.13.4.4 Event Information

Check total number of alarm events and processed events according to month. See Figure 4-116.

Figure 4-116 Event info

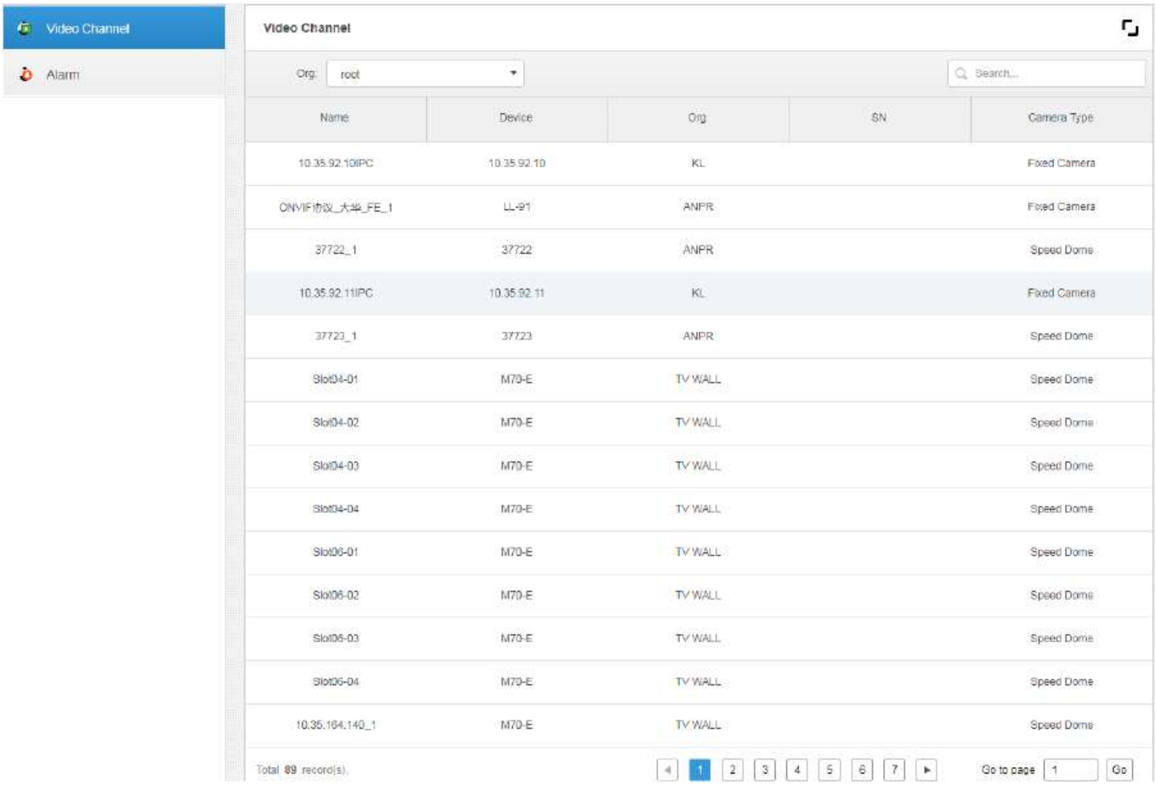


4.13.4.5 Source Information

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

- Check video channel details. See Figure 4-117.

Figure 4-117 Video channel



Org: root

Search...

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).

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

4.14 Configuring Cascade

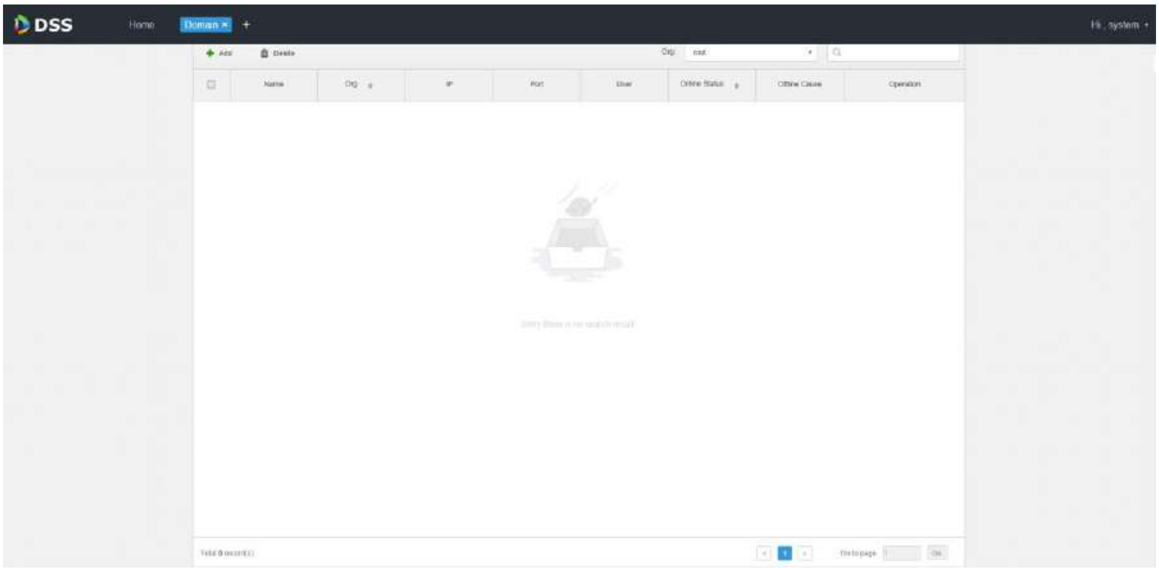
The system supports cascading. After cascading, platform of higher level can view the live video and video record of platforms of lower level. Configuring cascade refers to adding lower-level platforms to higher-level ones. It supports up to 3 levels.

- Before configuring, make sure the platform is deployed.
- Currently, the systems supports cascading between Pro and Express platforms. Express can only be lower-level platform.

Step 1 Click+, and select **Domain** on the **New Tab** tab.

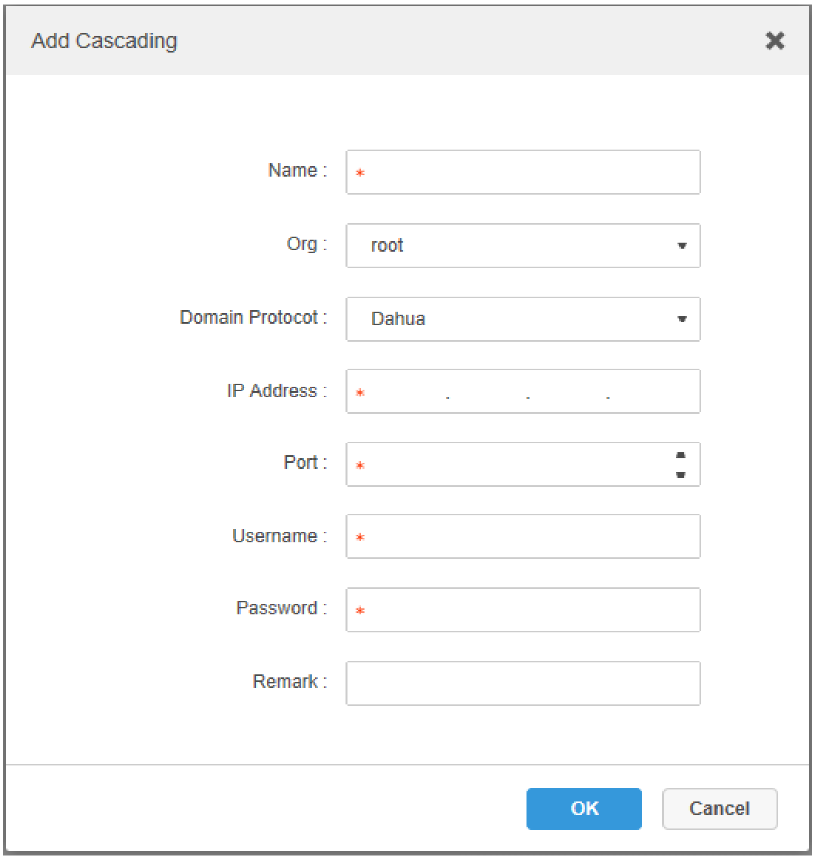
The Domain interface is displayed. See Figure 4-118.

Figure 4-118 Cascade



Step 2 Click **Add**, and the **Add Cascading** interface is displayed. See Figure 4-119.

Figure 4-119 Add cascading



Add Cascading

Name : *

Org : root

Domain Protocot : Dahua

IP Address : * . . .

Port : *

Username : *

Password : *

Remark :

Step 3 Configure the parameters, and click **OK** to save the configuration.

For detailed parameters, refer to Table 4-6

Table 4-6 Cascading parameter

Parameter	Description
Organization	Set higher-level platform of added cascading platform, after that all the organizations and devices of the platform can be called for monitoring by higher-level platform.
Port number	HTTPS port number of added cascading platform.

Step 4 If there is more than one level of platform, repeat this process.

5 Client Functions

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

5.1 Client Installation and Login

5.1.1 PC Requirements

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

Table 5-1 Config requirement

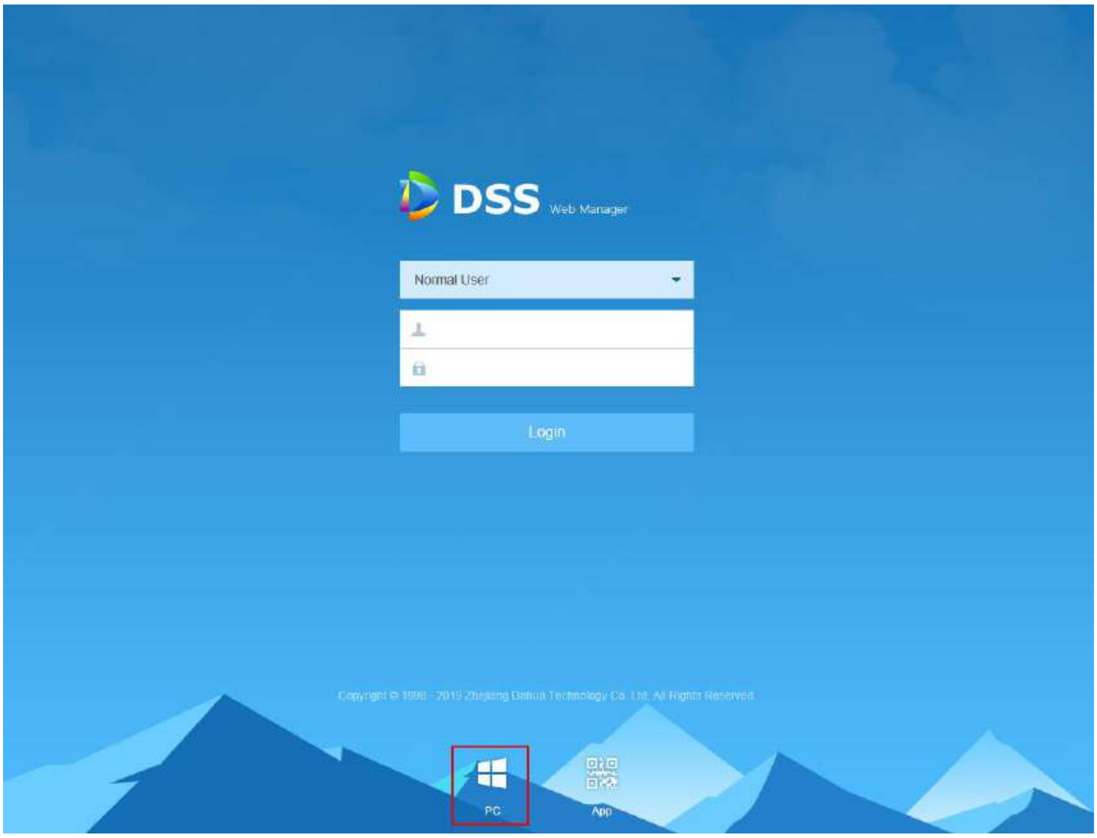
Parameters	Description
Recommended Config	● CPU: i5-6500 ● Main frequency:3.20GHz ● Memory:8GB ● Graphics:Inter HD Graphics 530 ● Network adapter:1Gbps ● HDD Type:HDD 1T ● DSS client installation space:200GB
Min. Config	● CPU:i3-2120 ● Memory:4GB ● Graphics:Inter(R) Sandbridge Desktop Gra ● Network adapter:1Gbps ● HDD Type:HDD 300GB ● DSS client installation space:100GB

5.1.2 Downloading and Installing Client

5.1.2.1 Installing PC Client

Step 1 Input IP address of DSS paltform into the browser and then press **Enter**.
The **Login** interface is displayed. See Figure 5-1.

Figure 5-1 Download Pc client


DSS Web Manager
Normal User
Login
Copyright © 1998 - 2019 Zhejiang Dahua Technology Co. Ltd. All Rights Reserved.
PC
App

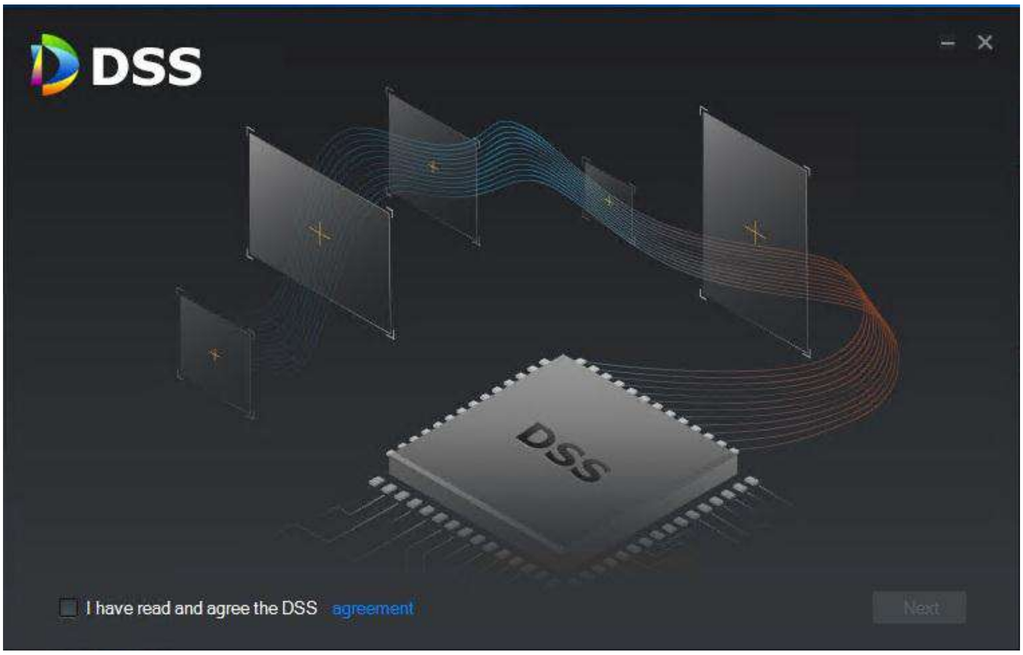
Step 2 Click ⊞ to download the client.

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

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

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

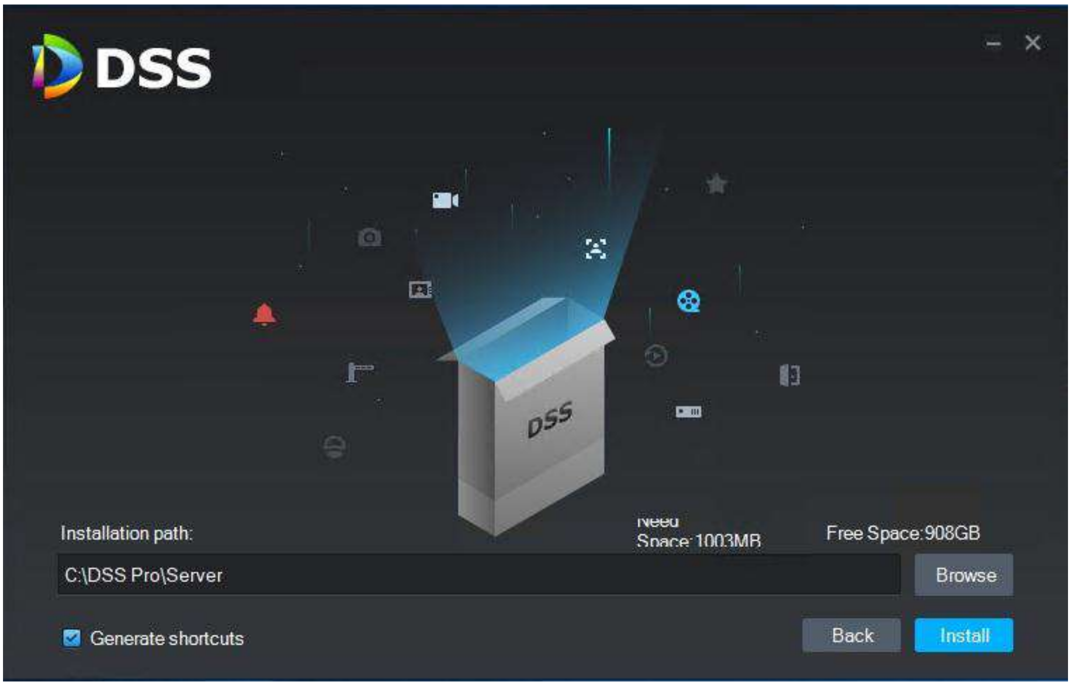
Figure 5-2 Install client



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

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

Figure 5-3 Select installation directory



Installation path:

Need Space: 1003MB

Free Space:908GB

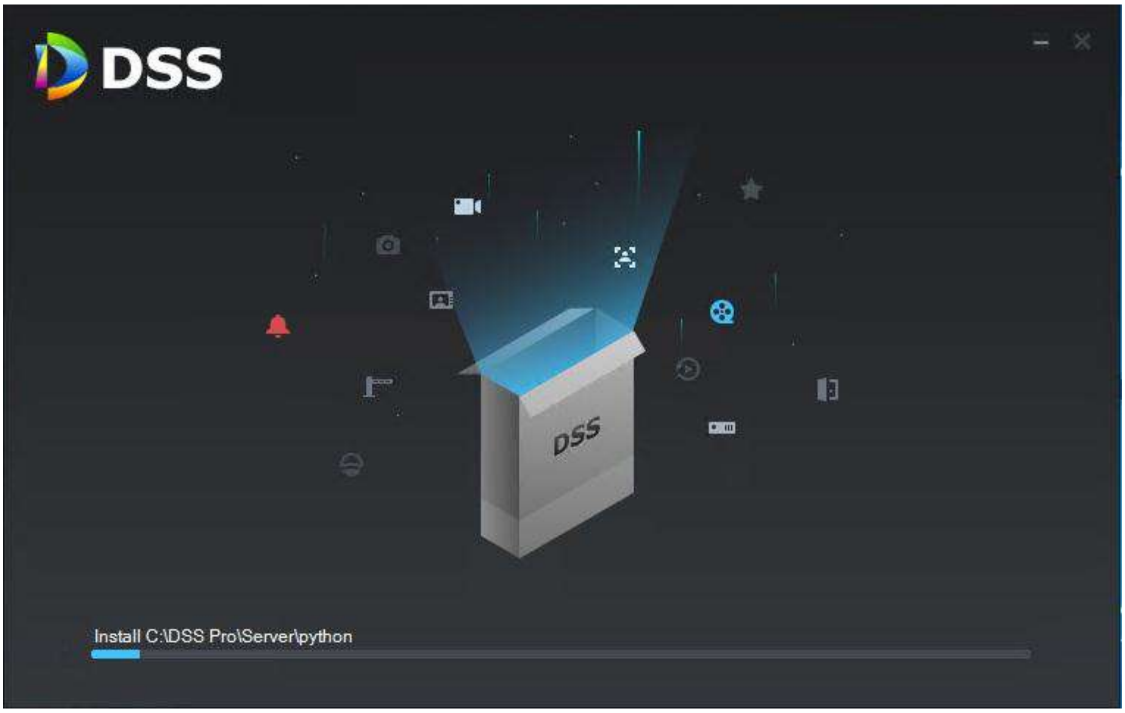
C:\DSS Pro\Server

☑ Generate shortcuts

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 Run client



Install C:\DSS Pro\Server\python

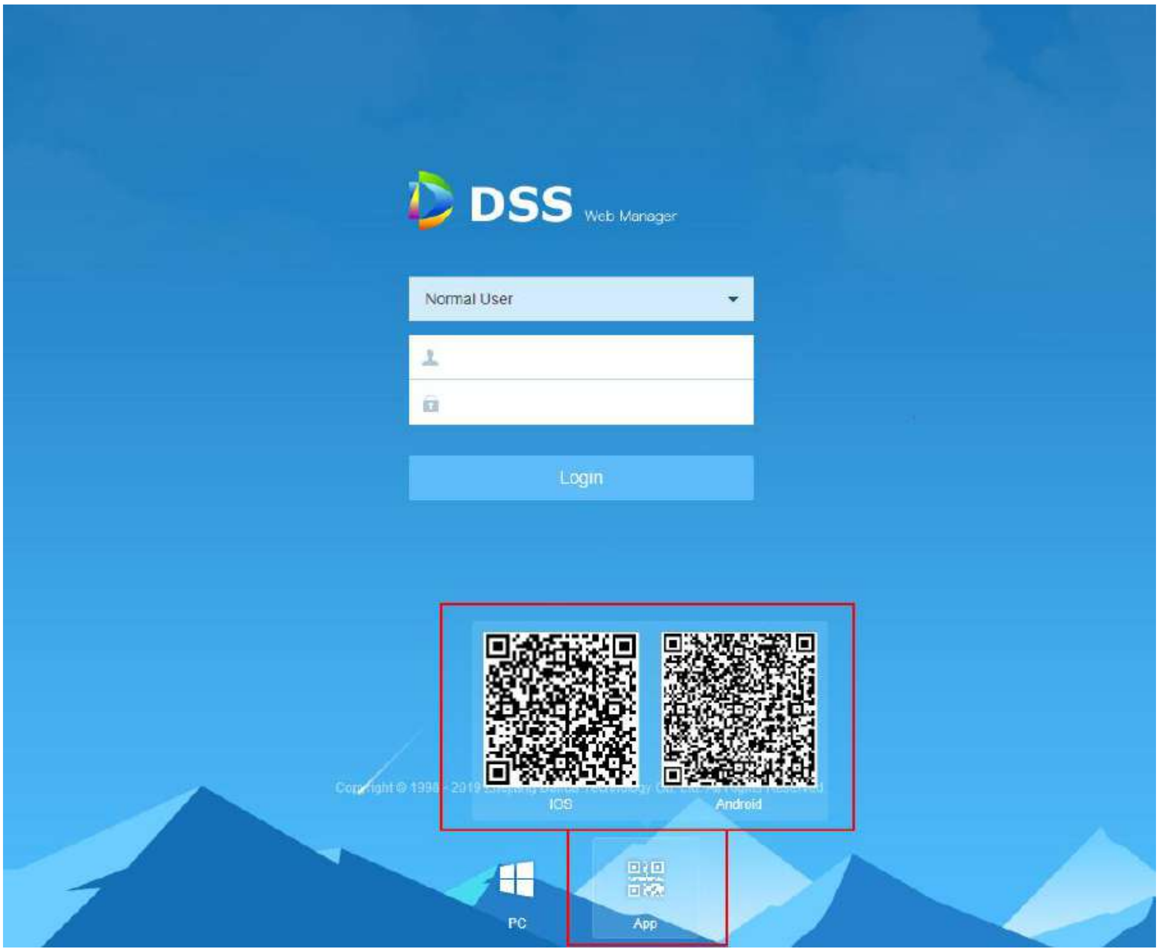
Step 8 Click **Run** to run the client.

5.1.2.2 Mobilephone App

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

Step 2 Click to view QR code of mobilephone APP. Currently it supports iOS and Android. See Figure 5-5.

Figure 5-5 Mobilephone app QR code

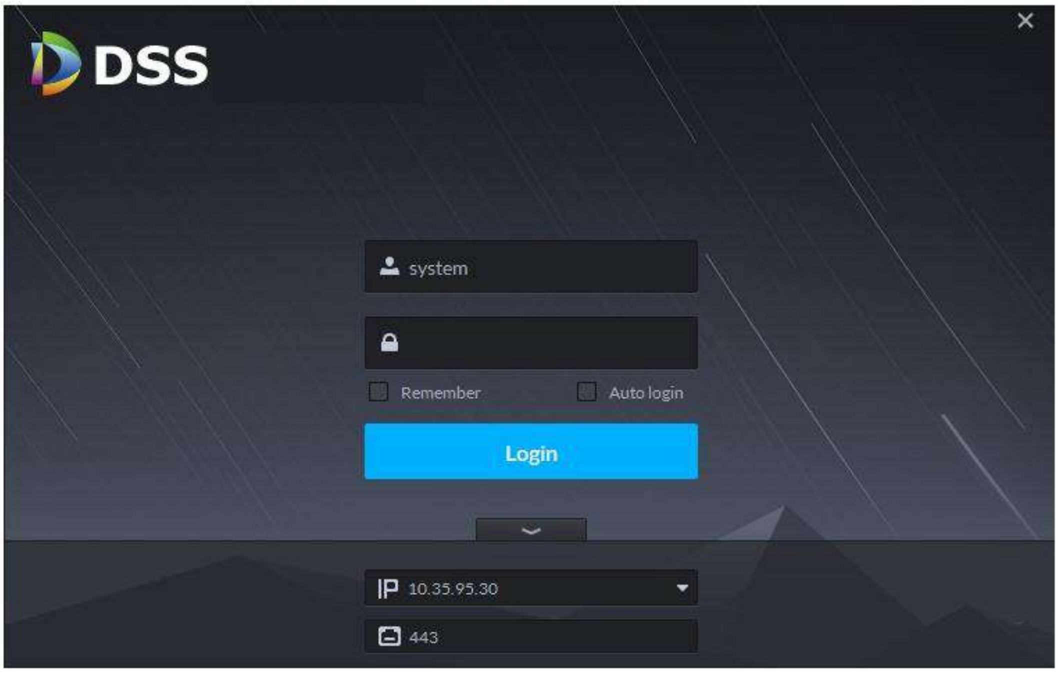


Step 3 Scan the QR code and then download the mobilephone App.

5.1.3 Logging in Client

Step 1 Double click icon DSS Client on the desktop.
The client login interface is displayed. See Figure 5-6.

Figure 5-6 Client login interface



Step 2 Enter **Username**, **Password**, **Server IP** and **Port**. Server IP means the IP address to install DSS server or PC, Port is 443 by default.

Step 3 Click **Login**.

The **Live** interface is displayed by default. See Figure 5-7.

Figure 5-7

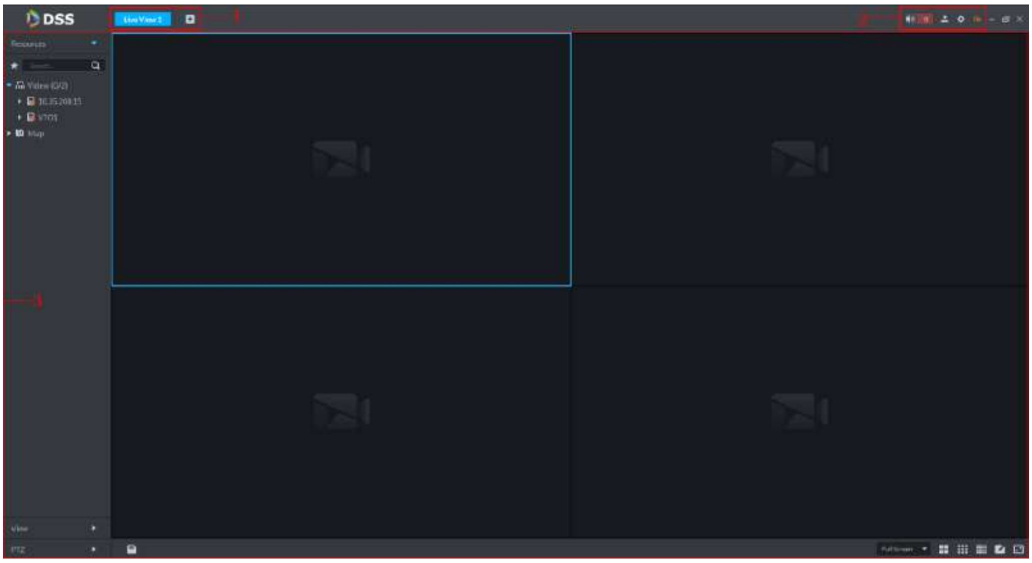


Table 5-2

SN	Name	Function
1	Tab	Display all valid tabs. Click + and you can open the module you want.

SN	Name	Function
2	System operation pane	Refer to the following contents for icon definition. ● 🔊: Open/close alarm audio. ● 0: It displays alarm amount. Click an alarm; you can go to Event center interface. ● 👤: 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. ◇ Select platform IP address, system goes to platform manager login interface. ◇ Select Modify password, you can change user password. ◇ Select Lock Client, it is to lock the system, you cannot operate on the client. Input the login password again to unlock. ◇ Select About, it is to view version information, released date. ◇ Select Logout, it is to logout the system. System goes back to the client login interface. ● ⚙: Local config. It is to set general, video, playback, snapshot, record, alarm shortcut settings. Refer to 5.2 Local Configuration for detailed information. ● ⏲: It is to view system status. It includes network status, CPU status, and memory status.
3	Operation area	It is to operate the functions.

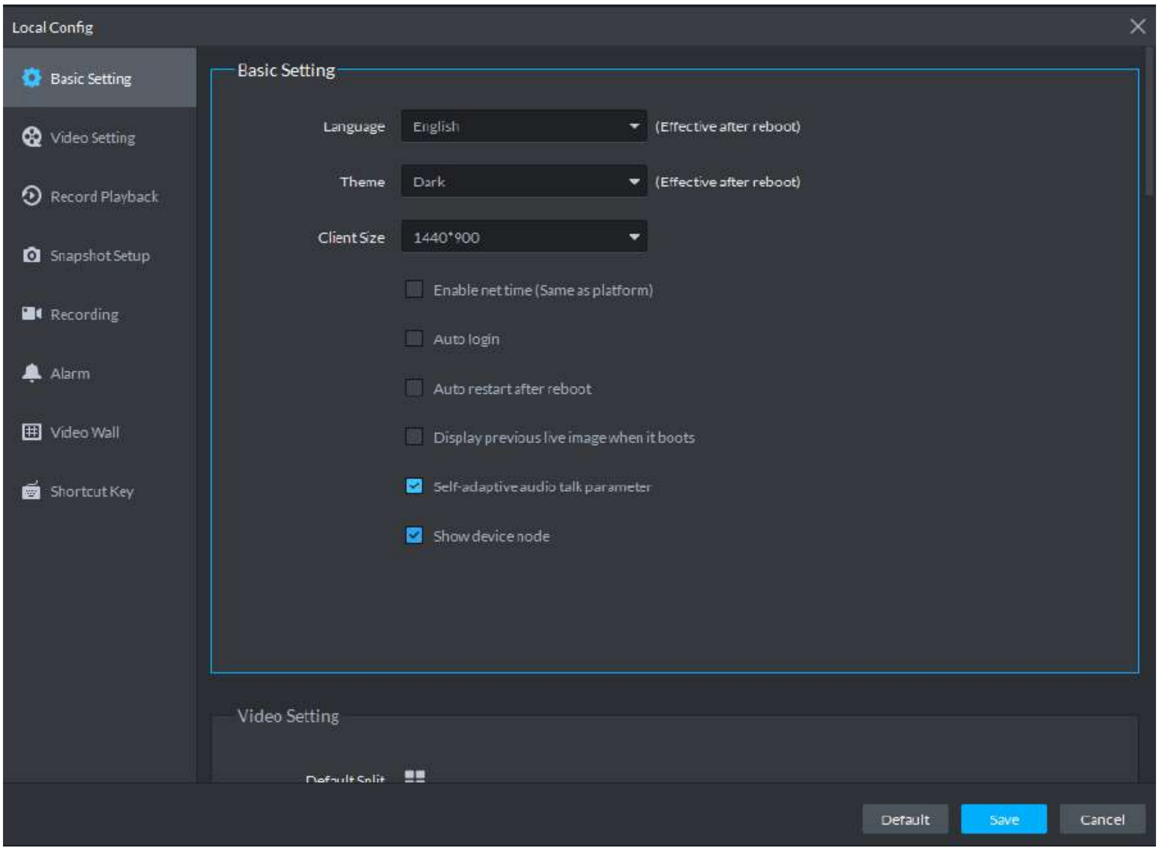
5.2 Local Configuration

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 **Local Config** interface is displayed. See Figure 5-8.

Figure 5-8 Local config



Basic Setting

Language: English (Effective after reboot)

Theme: Dark (Effective after reboot)

Client Size: 1440*900

□ Enable net time (Same as platform)

□ Auto login

□ Auto restart after reboot

□ Display previous live image when it boots

☑ Self-adaptive audio talk parameter

☑ Show device node

Video Setting

Default Split

Step 2 Click **Video Setting** and set relevant parameters. Refer to Table 5-3 for more details.

Table 5-3

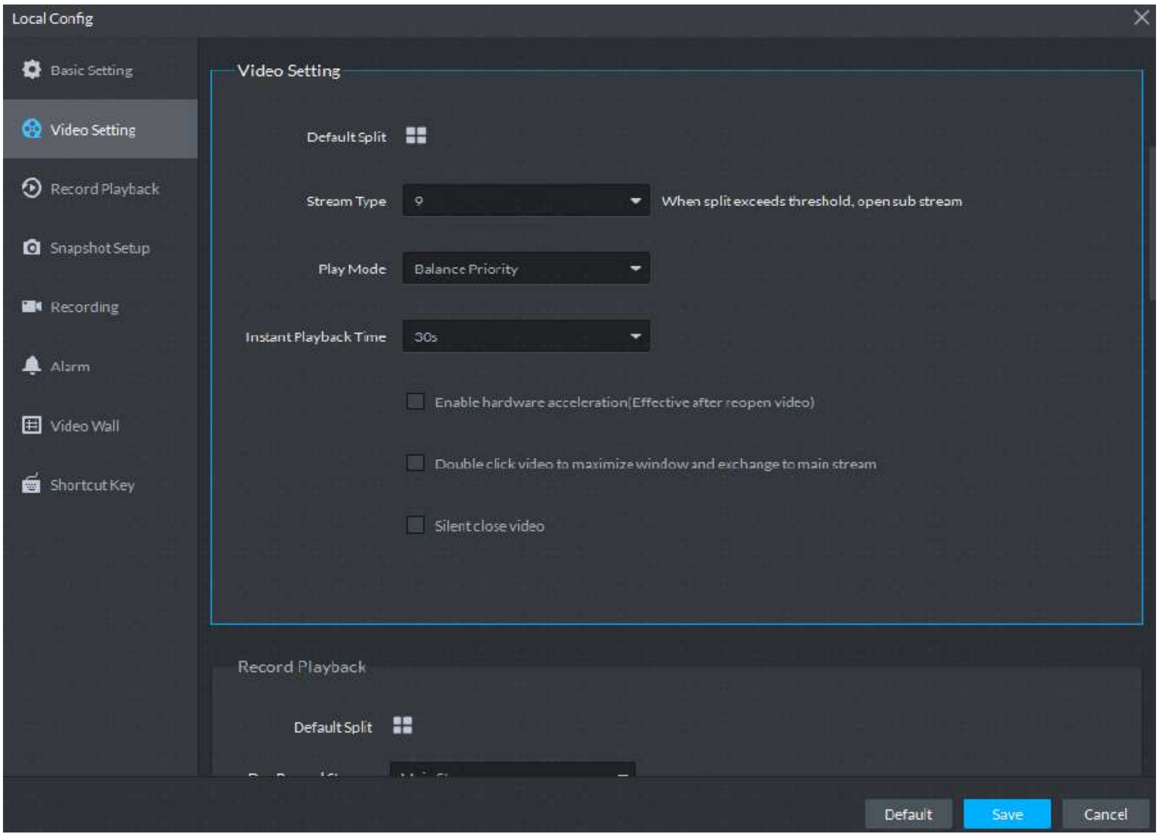
Parameters	Description
Language	Modify the language displayed on client; reboot the client to make it valid after setting.
Theme	Theme color includes dark and white. Reboot the client to make it valid after setting.
Client size	It is to set client display size.
Enable net time	If checked, the client starts to synchronize network time with the server. It is to complete time synchronization.
Auto Login	If checked, auto login is allowed when Client starts running.
Auto Reboot	If checked, auto reboot of the Client is allowed when the PC power is on.
Display Previous live Image when it boots	If checked, system displays the last Live video automatically after rebooting the client.

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

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

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

Figure 5-9 Video setting



Video Setting

Default Split

Stream Type: 9 When split exceeds threshold, open sub stream

Play Mode: Balance Priority

Instant Playback Time: 30s

□ Enable hardware acceleration(Effective after reopen video)

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

□ Silent close video

Record Playback

Default Split

Table 5-4 Video setting parameter description

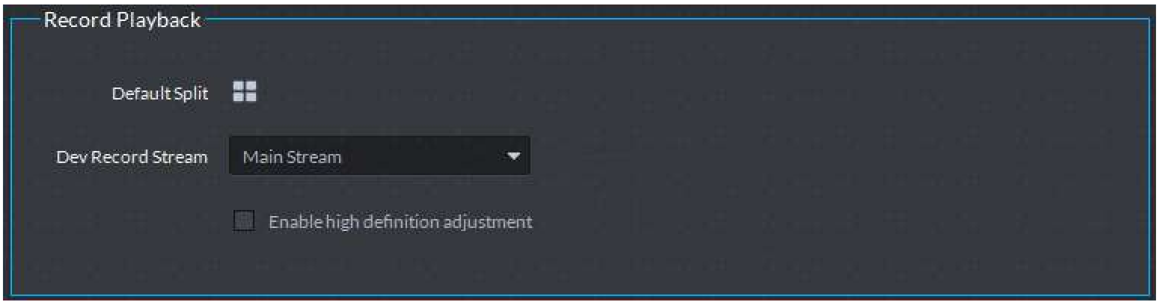
Parameters	Description
Default Split	Set split mode of the video window.
Stream type	Defines bit stream type for video transmission. With main bit stream as default, the auxiliary bit stream will be used when number of window splits is greater than the value selected here.
Play Mode	Play mode to be selected as required, including Real Time Priority, Fluency Priority, Balance Priority, as well as user-defined modes.

Parameters	Description
Instant playback time	Select instant playback time and then click Instant playback on the Live view interface, you can view the record of current period.
Enable hardware acceleration (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.
Slient close video	After being enabled, if the time of no operation for the Live interface exceeds the set value, the system will close Live automatically.

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

The **Record Playback** interface is shown as Figure 5-10. Refer to Table 5-5 to set parameters.

Figure 5-10 Record playback



Record Playback

Default Split

Dev Record Stream: Main Stream

□ Enable high definition adjustment

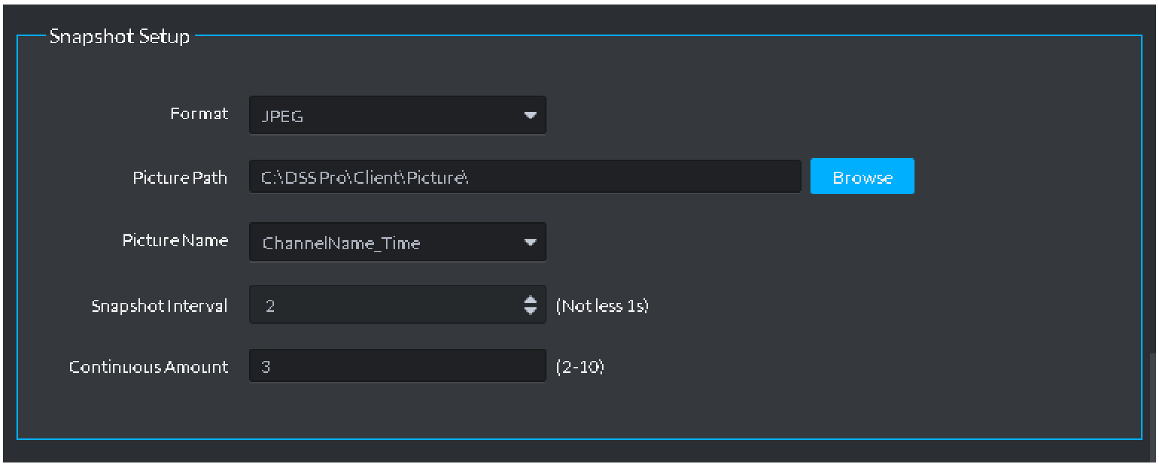
Table 5-5 Record playback parameter description

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

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

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

Figure 5-11 Snapshot setup



Snapshot Setup

Format: JPEG

Picture Path: C:\DSS Pro\Client\Picture\

Picture Name: ChannelName_Time

Snapshot Interval: 2 (Not less 1s)

Continuous Amount: 3 (2-10)

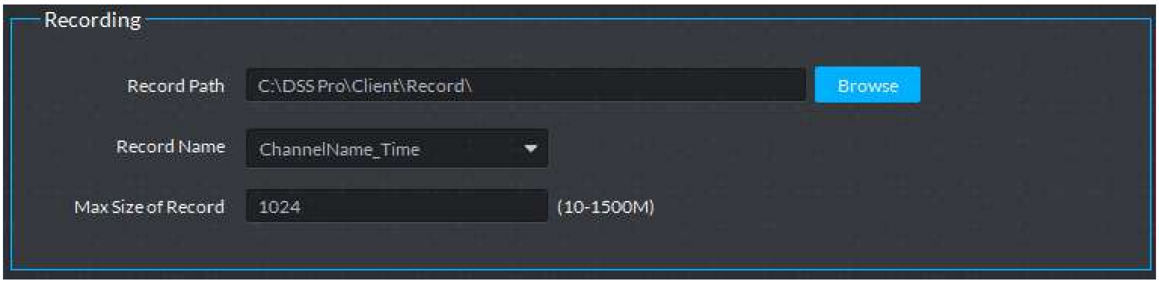
Table 5-6 Snapshot setup parameter description

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

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

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

Figure 5-12 Recording



Recording

Record Path: C:\DSS Pro\Client\Record\

Record Name: ChannelName_Time

Max Size of Record: 1024 (10-1500M)

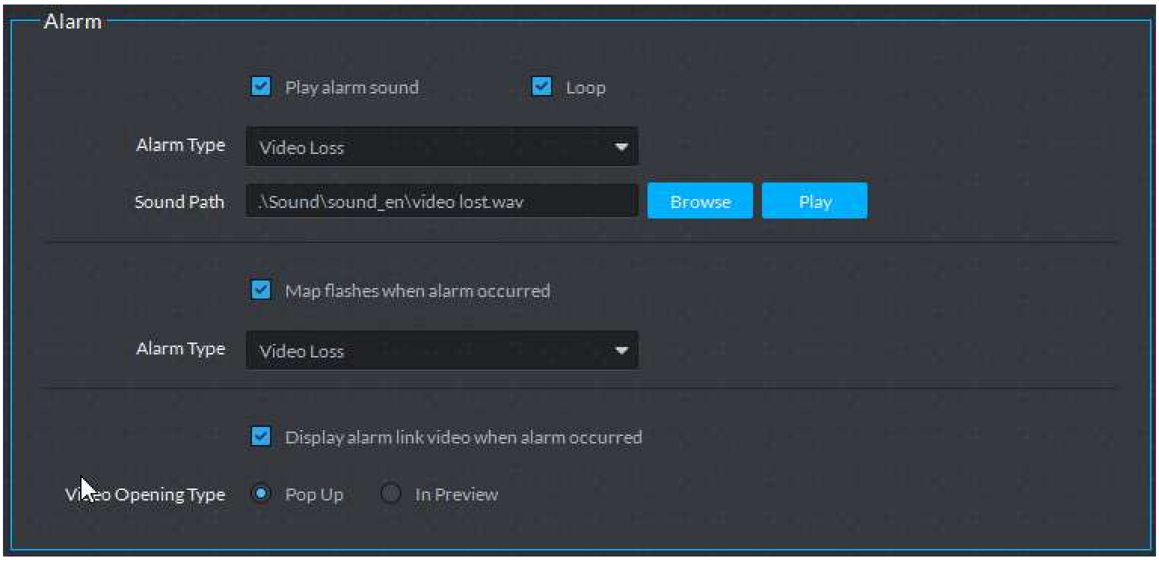
Table 5-7 Recording parameter description

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



Alarm

☑ Play alarm sound ☑ Loop

Alarm Type: Video Loss

Sound Path: .\Sound\sound_en\video lost.wav

☑ Map flashes when alarm occurred

Alarm Type: Video Loss

☑ Display alarm link video when alarm occurred

Video Opening Type: ● Pop Up ○ In Preview

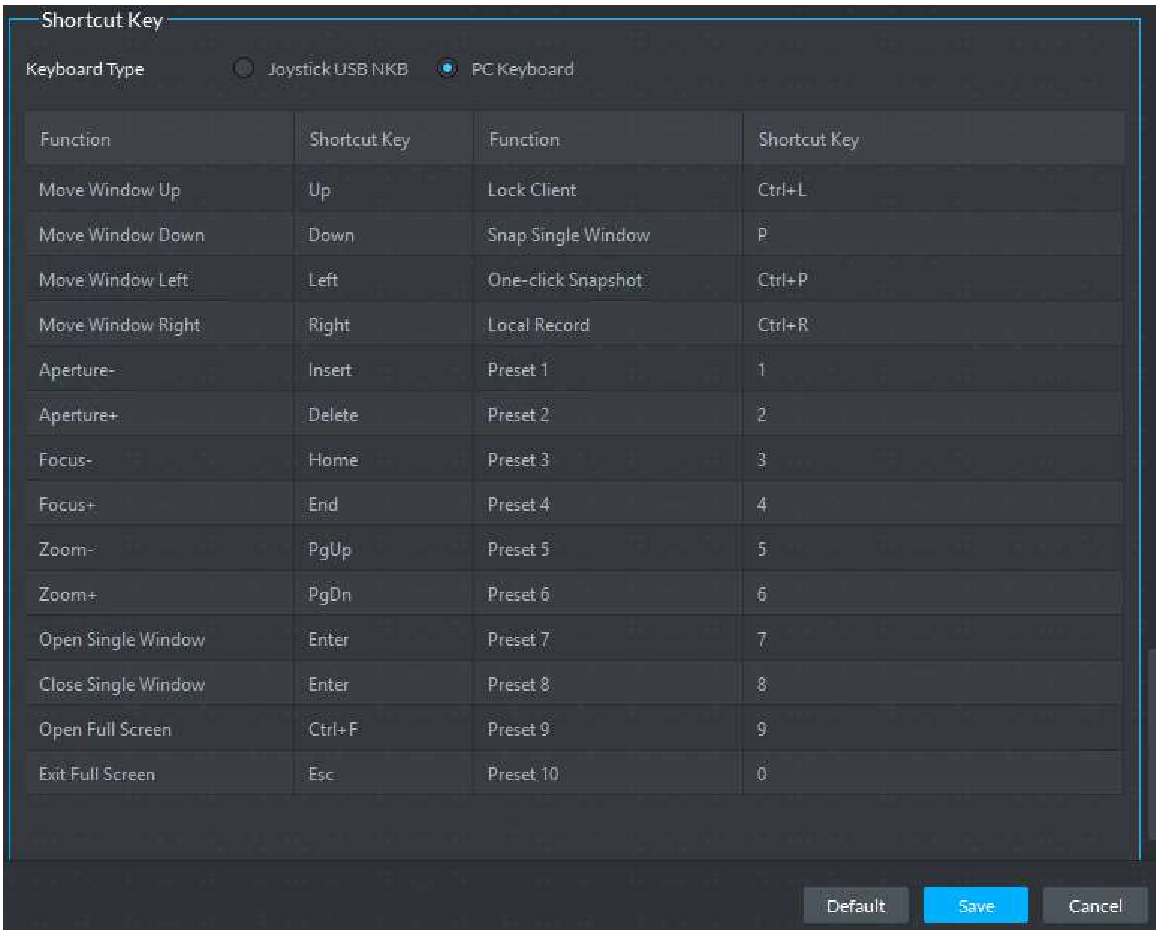
Table 5-8 Alarm parameter description

Parameters	Description
Play alarm sound	Check the box, system generates a sound when an alarm occurs.
Loop	Check the box; system plays alarm sound repeatedly when an alarm occurs. 📖 This item is only valid when Play alarm sound function is enabled.
Alarm Type	Set alarm type. System can play sound when corresponding alarm occurs. 📖 This item is only valid when Play alarm sound function is enabled.
Sound Path	Select alarm audio file path.
Map flashes when alarm occurred	Check the box and then select alarm type. When the corresponding alarm occurs, the device on the emap can flash.
Display alarm link video when alarm occurred	Check the box, system automatically opens linkage video when an alarm occurs.
Video opening type	System automatically opens linkage video when an alarm occurs. You can view on the pop-up window or on the preview interface.

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

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

Figure 5-14 Shortcut key



Shortcut Key

Keyboard Type ○ Joystick USB NKB ● PC Keyboard

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

Step 9 Click **Save**.

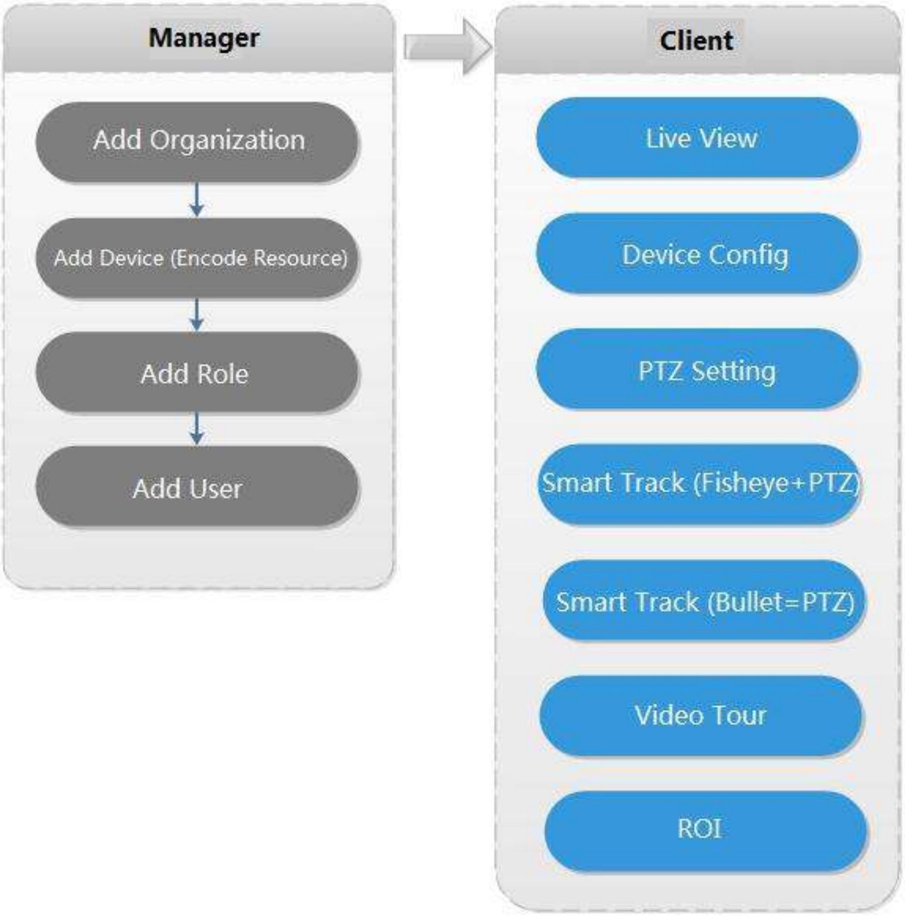
5.3 Video Preview

5.3.1 Preparations

Before the operation, refer to "4.5 Adding Device " to add decode device on the manager.

Refer to Figure 5-15 for video preview flows information.

Figure 5-15 Live video flow



5.3.2 Live View

5.3.2.1 View Live Video

Step 1 Click + and then on the **New Tab** interface, select Live View, system displays Live view interface by default.

Step 2 View real-time video by:

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

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 Live

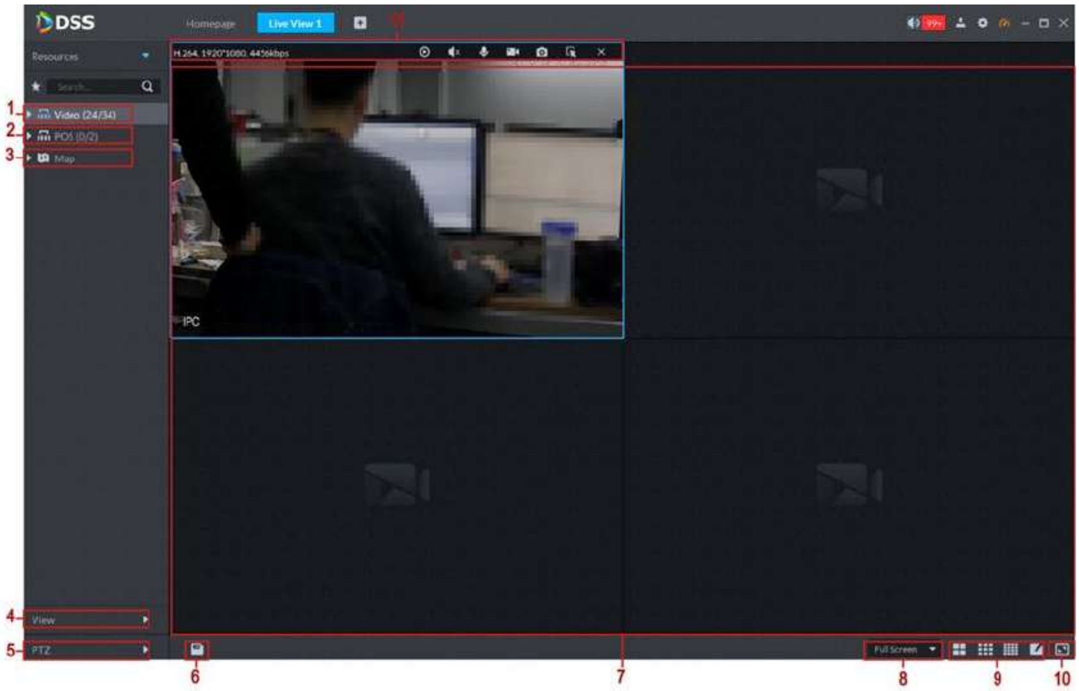


Table 5-9 Live interface function

No.	Name	Function
1	Favorites and Device Tree Search	● From Local config > General, if you enable Show device node, device tree displays all channels of current device. If you cancel the box, system display all channels of all device. ● Search is supported by input device name or channel name in Search.. 🔍 here. ● ★: Add, Delete or Rename Favorite. Favorite Tour supported.
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	● 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.
5	PTZ	More info about PTZ of PTZ camera, refer to 5.3.4 PTZ.
6	Save view	Click 💾 to save current video window as a view.

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

5.3.2.2 Right–Click Shortcut Menu

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

Figure 5-17 Right click menu

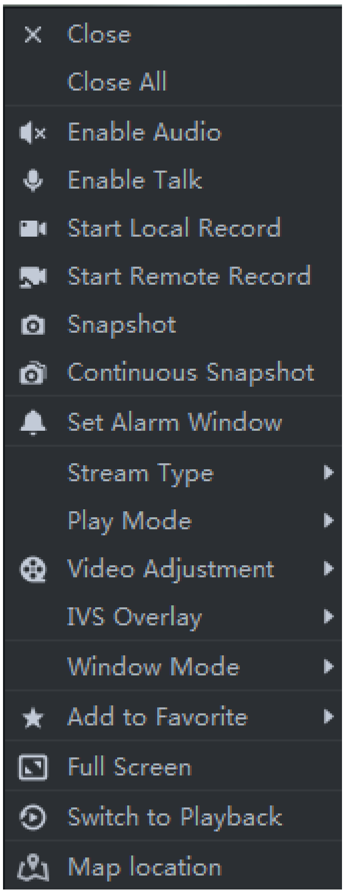


Table 5-10 Right click menu description

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

Parameters	Description
Switch Bit Stream	Switch among Main stream, Sub stream and Third stream. 📖 If selecting Sub stream or Third stream, you need to check enable Sub Stream and enable Third Stream in the Bit Stream dropdown list when adding encoder from the Manager.
Play Mode	Switch between the modes of Real Time Priority, Fluency Priority, Balance Priority and custom defined mode.
Video Adjustment	Perform video adjustment and video enhancement.
IVS Overlay	Enable IVS rules and target box, after that IVS rule and target box will be displayed during live view. The config is only valid to the configured channel. The IVS rule and target box are not displayed by default.
Open crowd density map	📖 This function is only available for multisensor camera with flow analysis function. After selecting this function, the crowd density will be displayed on the image of the video. Double-click the image to hide it, and people in the video will be shown in blue dots.
Installation mode	📖 For fisheye camera only. The installation mode has three types:ceiling mount, wall mount and ground mount. Select corresponding installation mode according to the actual situation, the real-time video can automatically dewarp according to the installation mode.
Fisheye view mode	📖 For fisheye camera only. When changing the video stream, the fisheye view mode keeps the configuration before the stream is changed. It refers to current video display mode (system supports original video mode by default.). System supports following display modes according to different installation mode. ● Ceiling mount: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8. ● Wall mount: 1P, 1P+3, 1P+4, 1P+8. ● Ground mount: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8.
Split mode	Support standard mode, 1+3 mode, 1+5 mode.
Alarm output control	It control alarm input/output.
Add To Favorites	You can add the active channel or all channels into Favorite.
Full Screen	Switch the video window to full screen mode. To exit full screen, double click video window, or right click to select exit full screen.
Switch to Playback	You can switch between live view interface and playback interface quickly, without going back to homepage first.
Map location	After enabling map location, a map that centers on the device will be displayed.

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 Window shortcut menu

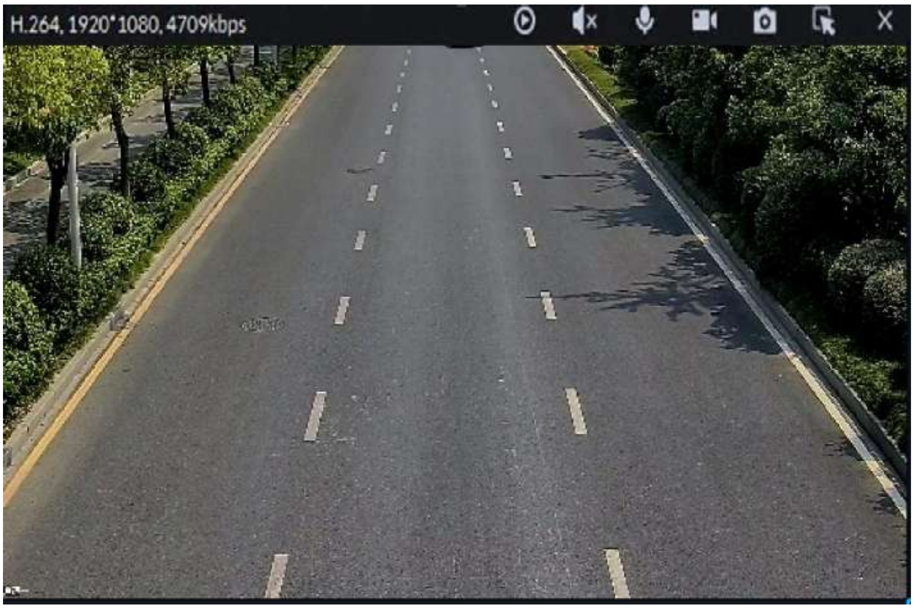


Table 5-11 Window shortcut menu description

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

5.3.3 Device Config

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

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

5.3.3.1 Configuring Camera Properties

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

5.3.3.1.1 Configuring Property Files

Step 1 On the **Preview** interface, right-click the video device and select **Device Config**. See Figure 5-19.

The **Device Config** interface interface is displayedis displayed. See Figure 5-20.

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

Figure 5-19 Enter device config

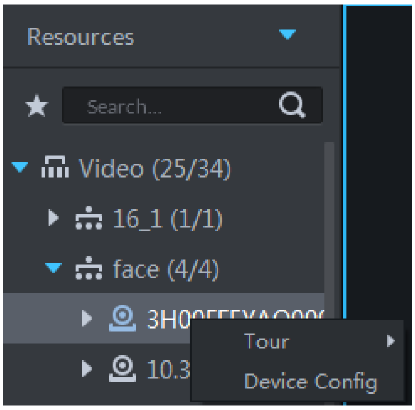
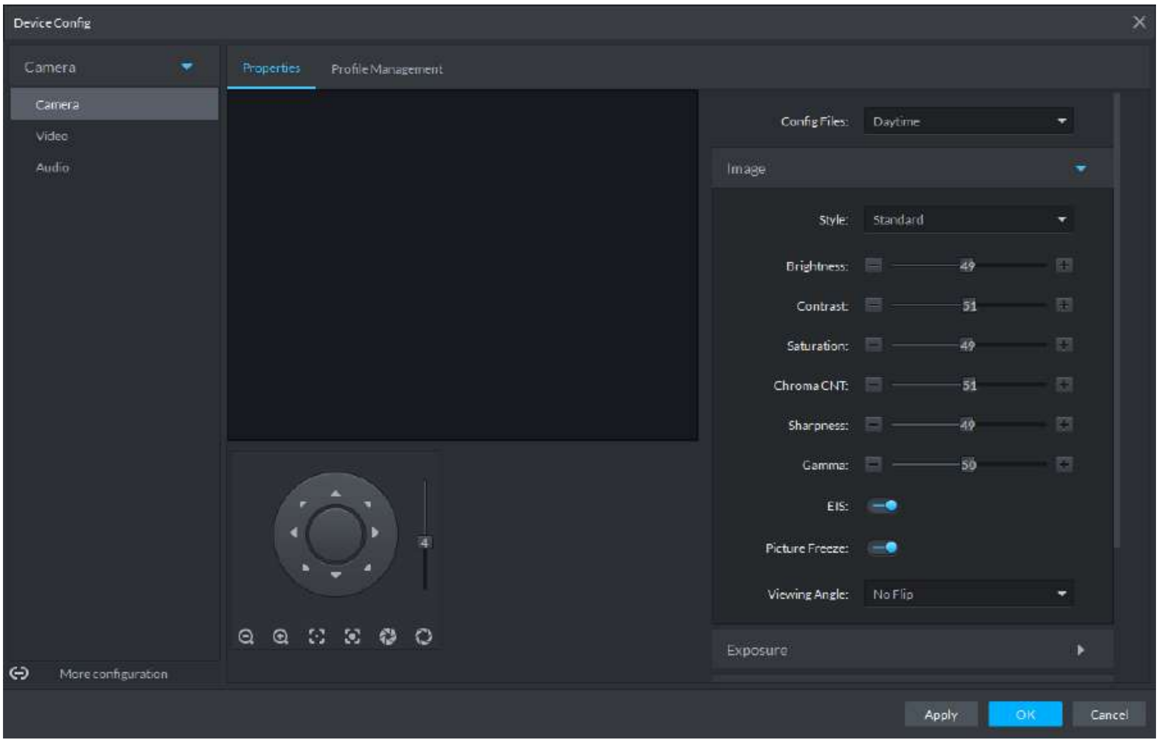


Figure 5-20 Device config



Config Files: Daytime

Style: Standard

Brightness: 49

Contrast: 51

Saturation: 49

Chroma CNT: 51

Sharpness: 49

Gamma: 50

EIS:

Picture Freeze:

Viewing Angle: No Flip

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

The **Properties** interface is displayed. See Figure 5-20.

Step 3 Select **Profile Management**.

Step 4 Click **Image**. See Figure 5-20. For details of the parameters, see Table 5-12.

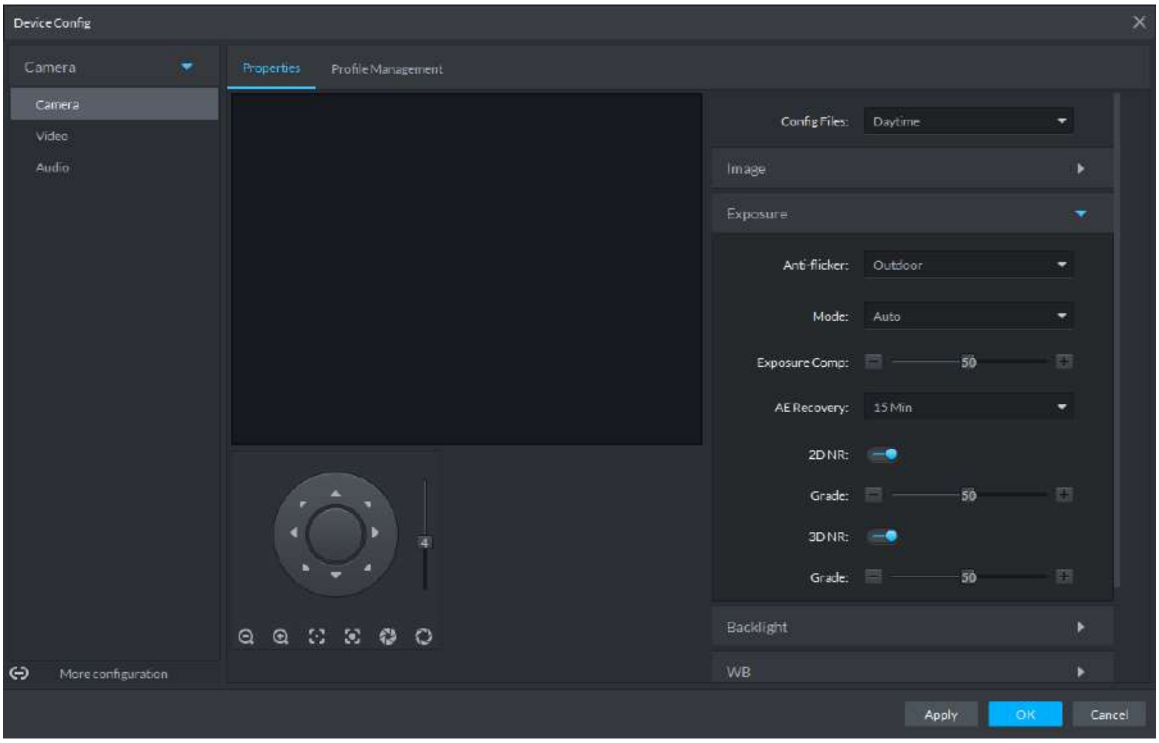
Table 5-12 Image parameter description

Parameter	Description
Style	You can set the image style to be Standard, Gentle, or Flamboyant.
Brightness	You can adjust the overall image brightness through linear tuning. The higher the value, the brighter the image and vice versa. If this value is set too high, images tend to look blurred.
Contrast	Adjusts the contrast of the images. The higher the value, the bigger the contrast between the bright and dark portions of an image and vice versa. If the contrast value is set too high, the dark portions of an image might become too dark, and the bright portions might be over-exposed. If the contrast value is set too low, images tend to look blurred.
Saturation	Adjusts color shade. The higher the value, the deeper the color and vice versa. The saturation value does not affect the overall brightness of the images.
Sharpness	Adjusts the edge sharpness of images. The higher the value, the sharper the image edges. Setting this value too high might easily result in noises in images.
Gamma	Changes image brightness by non-linear tuning to expand the dynamic display range of images. The higher the value, the brighter the image and vice versa.

Step 5 Click **Exposure** to set up relevant parameters. See Figure 5-21. For details of the parameters, see Table 5-13.

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

Figure 5-21 Exposure



Config Files: Daytime

Anti-flicker: Outdoor

Mode: Auto

Exposure Comp: 50

AE Recovery: 15 Min

2D NR:

Grade: 50

3D NR:

Grade: 50

Table 5-13 Exposure parameter description

Parameter	Description
Anti-flicker	You can select from these three modes: 50Hz, 60Hz, or Outdoor. ● 50Hz: With the 50Hz household power supply, the mode can automatically adjust exposure based on the brightness of the scene to ensure that the image does not yield horizontal stripes. ● 60Hz: With the 60Hz household power supply, the mode can automatically adjust exposure based on the brightness of the scene to ensure that the image does not yield horizontal stripes. ● Outdoor: In an outdoor scenario, you can switch the exposure modes to achieve your target effect.
Mode	The following options are available for the different exposure modes of the camera: 📖 ● If the **Anti-flicker** is set to **Outdoor**, you can set the **Mode** to **Gain Priority** or **Shutter Priority**. ● Different devices have different exposure modes. The actual interfaces shall prevail. ● Auto: Auto tuning of the image brightness based on the actual environment. ● Gain Priority: Within the normal exposure range, the device adjusts itself automatically first in the preset range of gains as per the brightness of the scenes. If the image has not achieved the target brightness when the gains hit the upper limit or lower limit, the device adjusts the shutter automatically to achieve the best brightness. The Gain Priority mode also allows for adjusting the gains by setting up a gain range. ● Shutter Priority: Within the normal exposure range, the device adjusts itself automatically first in the preset range of shutter values as per the brightness of the scenes. If the image has not achieved the target brightness when the shutter value hits the upper limit or lower limit, the device adjusts the gains automatically to achieve the best brightness. ● Aperture Priority: The aperture is fixed at a preset value before the device adjusts the shutter value automatically. If the image has not achieved the target brightness when the shutter value hits the upper limit or lower limit, the device adjusts the gains automatically to achieve the best brightness. ● Manual: You can set up the gains and shutter values manually to adjust image brightness.
3D NR	Reduces the noises of multiple-frame (at least two frames) images by using inter-frame information between two adjacent frames in a video.
Grade	When 3D NR is On, you can set up this parameter. The higher the grade, the better the noise reduction effect.

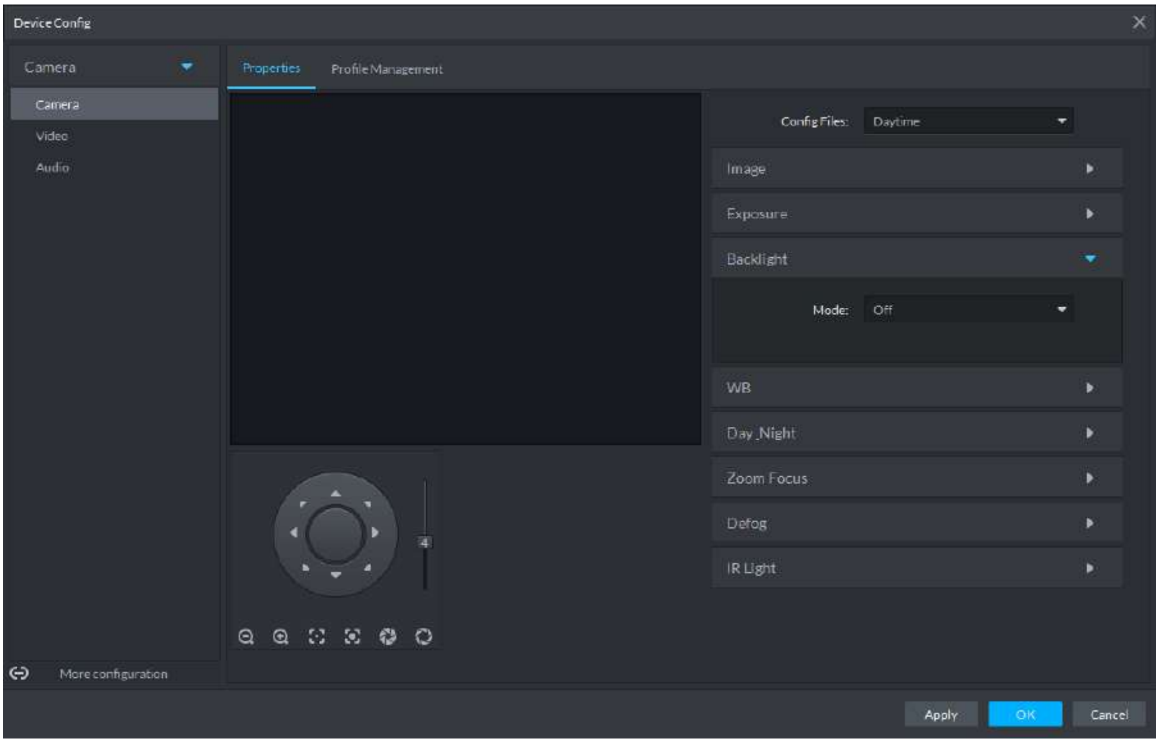
Step 6 Click **Backlight** to set up relevant parameters. See Figure 5-22. For details of the parameters, see Table 5-14.

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

- Turning on Backlight Correction avoids silhouettes of relatively dark portions in pictures taken in a backlight environment.

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

Figure 5-22 Backlight



Config Files: Daytime

Mode: Off

Table 5-14 Backlight mode description

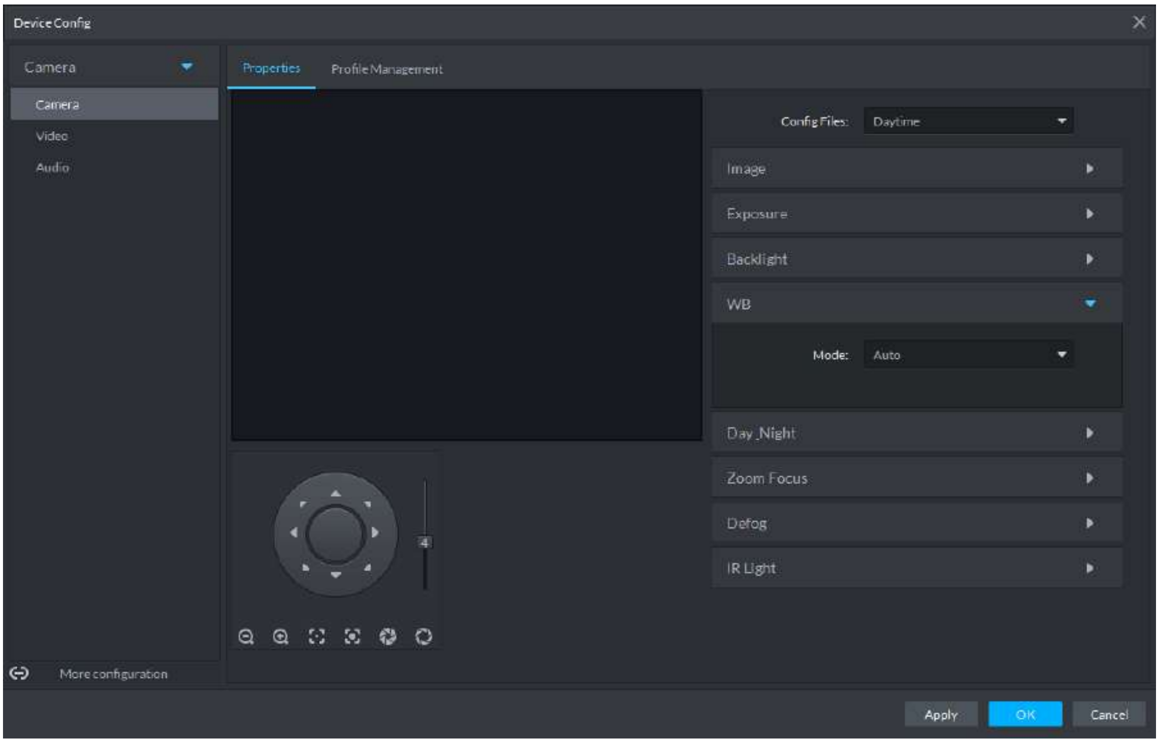
Backlight mode	Description
SSA	The system adjusts image brightness automatically based on the environmental lighting conditions to show image details clearly.
Backlight Correction	You can select Default mode or Custom mode. ● When selecting the **Default** mode, the system adjusts exposure automatically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

Backlight mode	Description
Glare Inhibition	The system inhibits the brightness in bright regions and reduces the size of the halo, to make the entire image less bright.

Step 7 Click **WB** to set up relevant parameters. See Figure 5-23. For details of the parameters, see Table 5-15.

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

Figure 5-23 WB



Config Files: Daytime

Mode: Auto

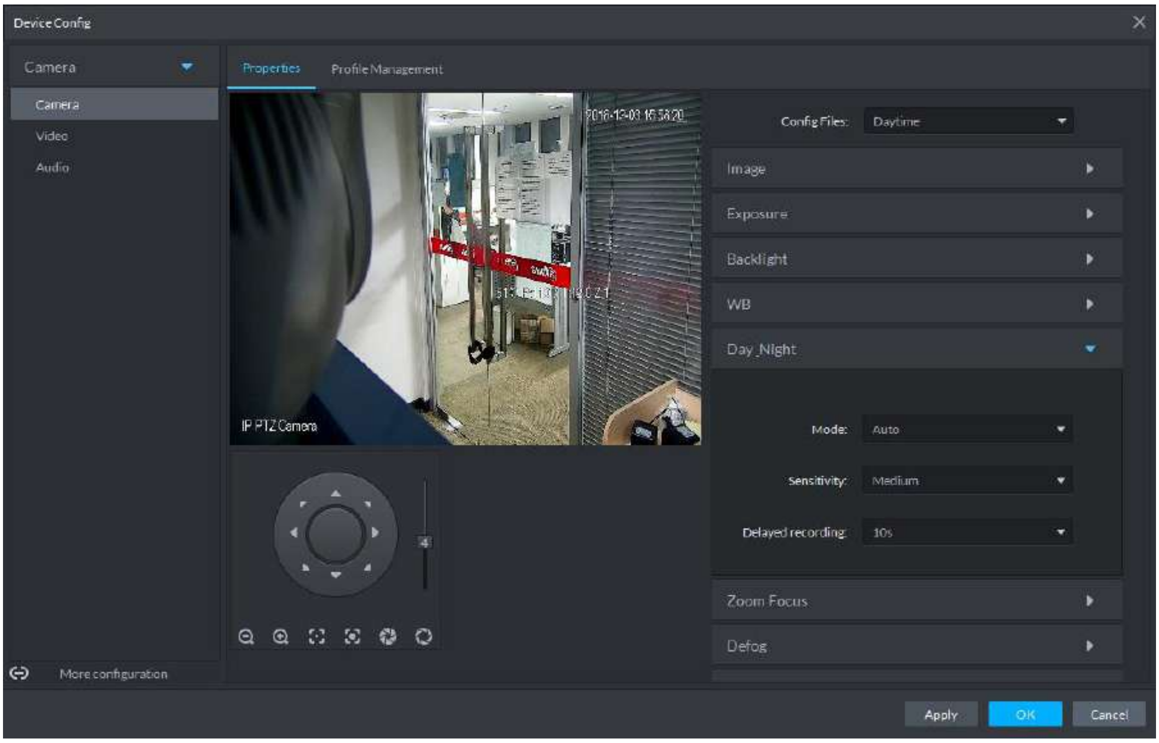
Table 5-15 WB mode description

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

Step 8 Click **Day & Night** to set up relevant parameters. See Figure 5-24. For details of the parameters, see Table 5-16.

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

Figure 5-24 Day/night



Config Files: Daytime

Mode: Auto

Sensitivity: Medium

Delayed recording: 10s

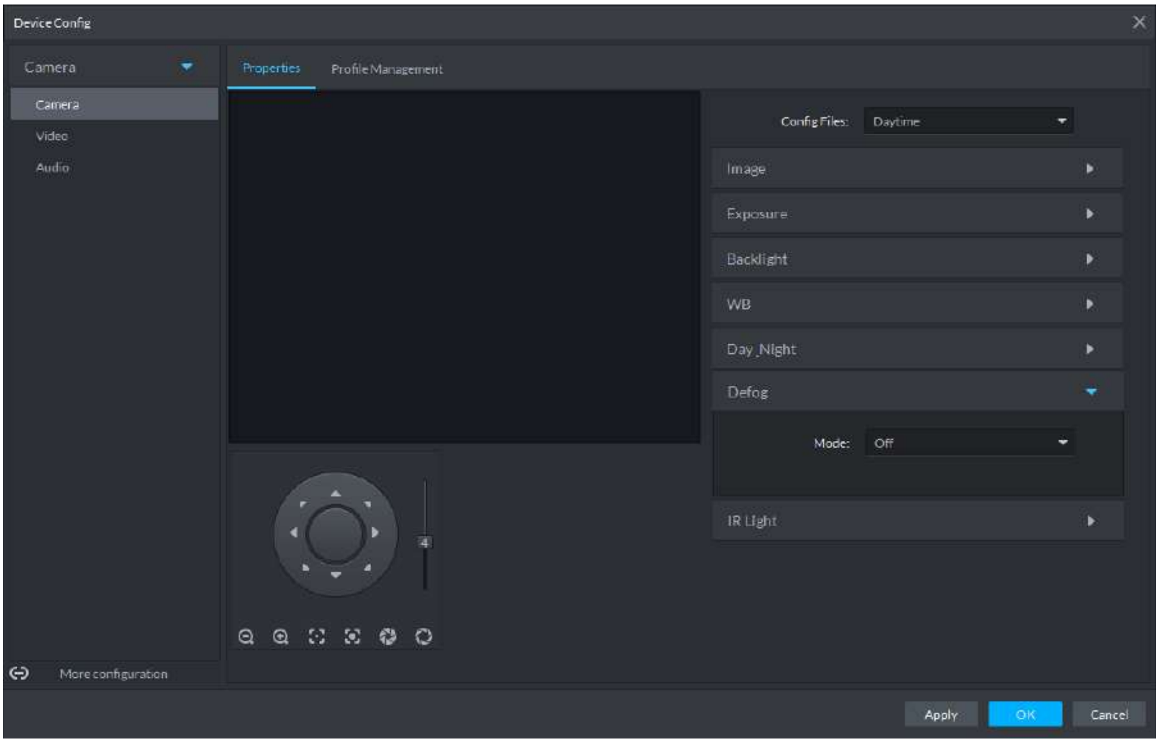
Table 5-16 Day/night parameter description

Parameter	Description
Mode	You can set up the image display of the camera to the Colored mode or the Black&White mode, including the following options: 📖 The **Day & Night** settings are independent of the **Config Files** settings. ● Colored: The camera displays colored images. ● Auto: The camera automatically selects to display colored or black&white images based on the environmental brightness. ● Black&White: The camera displays black&white images.
Sensitivity	You can set up this parameter when the **Day & Night** mode is set to **Auto**. Defines the sensitivity of the camera in switching between the Colored mode and the Black&White mode.
Delayed recording	You can set up this parameter when the **Day & Night** mode is set to **Auto**. Defines the delay of the camera in switching between the Colored mode and the Black&White mode. The lower the delay, the faster the switch between the Colored mode and the Black&White mode.

Step 9 Click **Defog** to set up relevant parameters. See Figure 5-25. For details of the parameters, see Table 5-17.

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

Figure 5-25 Defog



Config Files: Daytime

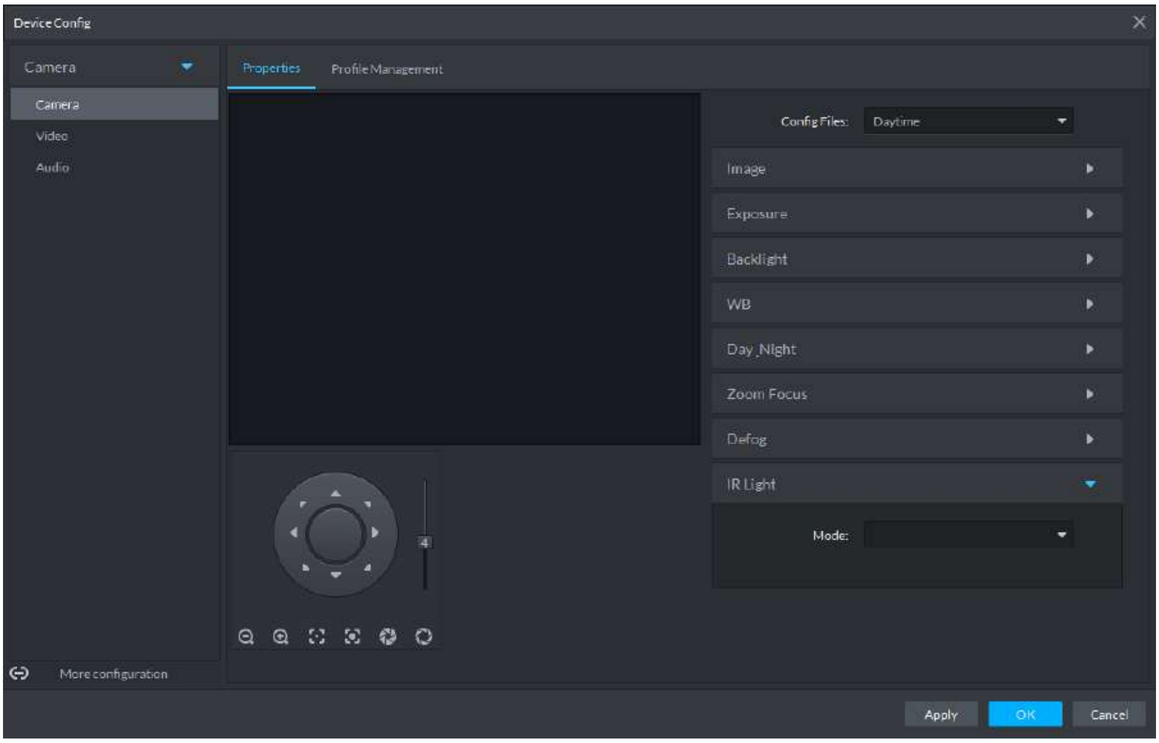
Mode: Off

Table 5-17 Defog description

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

Step 10 Click **IR Light** to set up relevant parameters. See Figure 5-26. For details of the parameters, see Table 5-18.

Figure 5-26 IR light



Config Files: Daytime

Table 5-18 IR light description

IR Light mode	Description
Manual	You can set up the IR Light brightness manually. The system fills light for images as per the preset IR Light brightness.
SmartIR	The system adjusts the brightness of the light to adapt to the surrounding conditions.
ZoomPrio	The system adjusts the IR Light automatically to adapt to the brightness changes in the environment. ● When the scene darkens, the system opens the near light first. If the required brightness still cannot be achieved when the near light runs at full power, the system turns on the far light. ● When the scene becomes brighter, the system reduces the brightness of the far light all the way until it is turned off, before adjusting the brightness of the near light. ● When the lens focus is adjusted to a certain wide end, the system keeps the far light off to avoid over-exposure at the near end, You can also set up lighting correction manually to fine tune the brightness of the IR Light.
Off	IR Light disabled.

Step 11 Click **OK**.

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

5.3.3.1.2 Applying Config Files

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

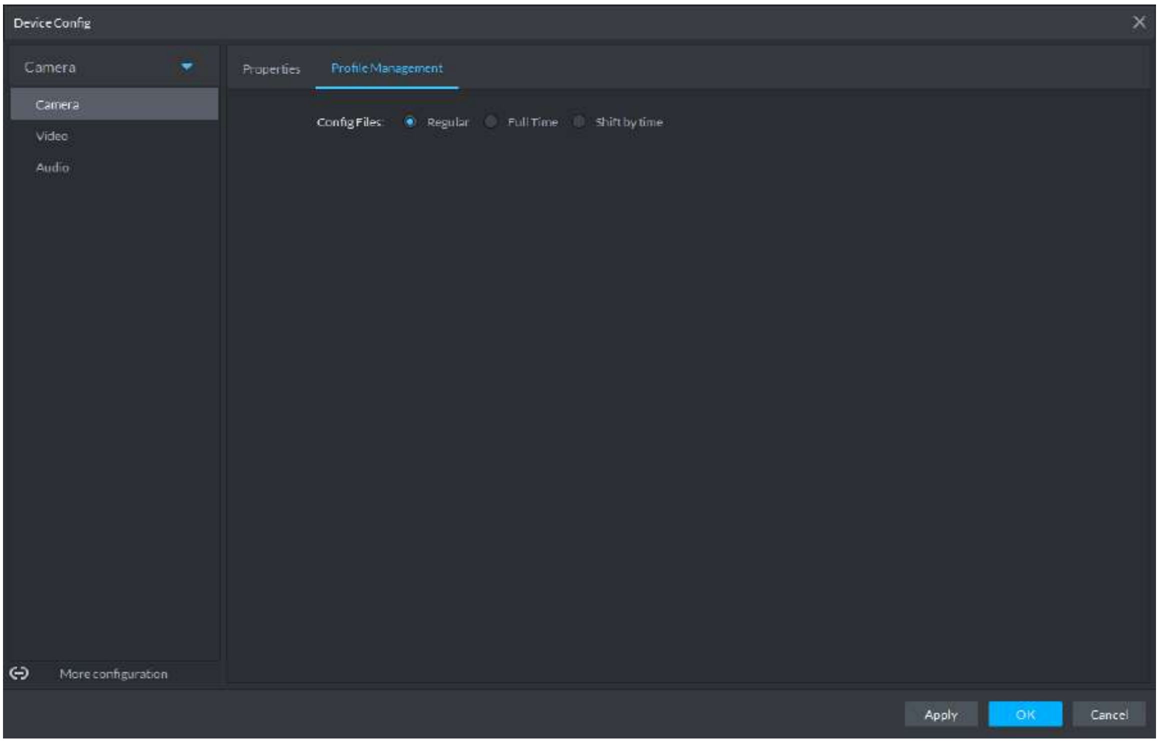
Step 1 Select **Camera** > **Camera** > **Properties** > **Profile Management**.

The **Profile Management** interface is displayed.

Step 2 Setting up config files.

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

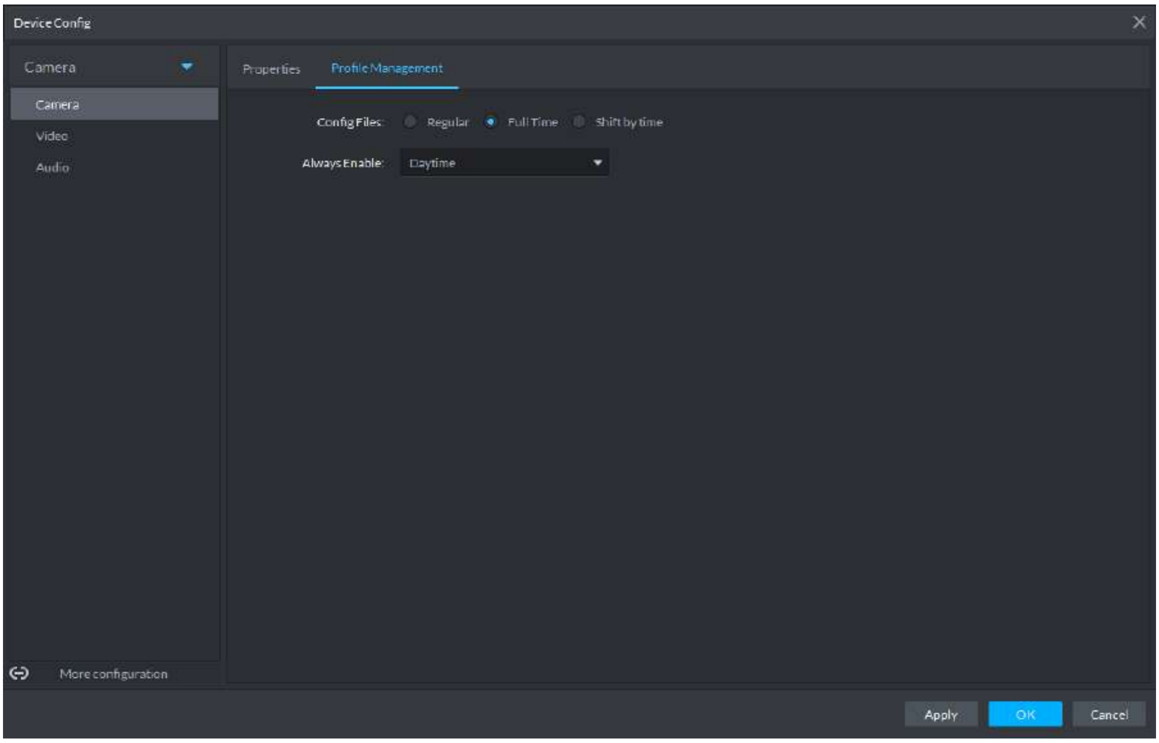
Figure 5-27 Regular



Config Files: ● Regular ○ Full Time ○ Shift by time

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

Figure 5-28 Full time

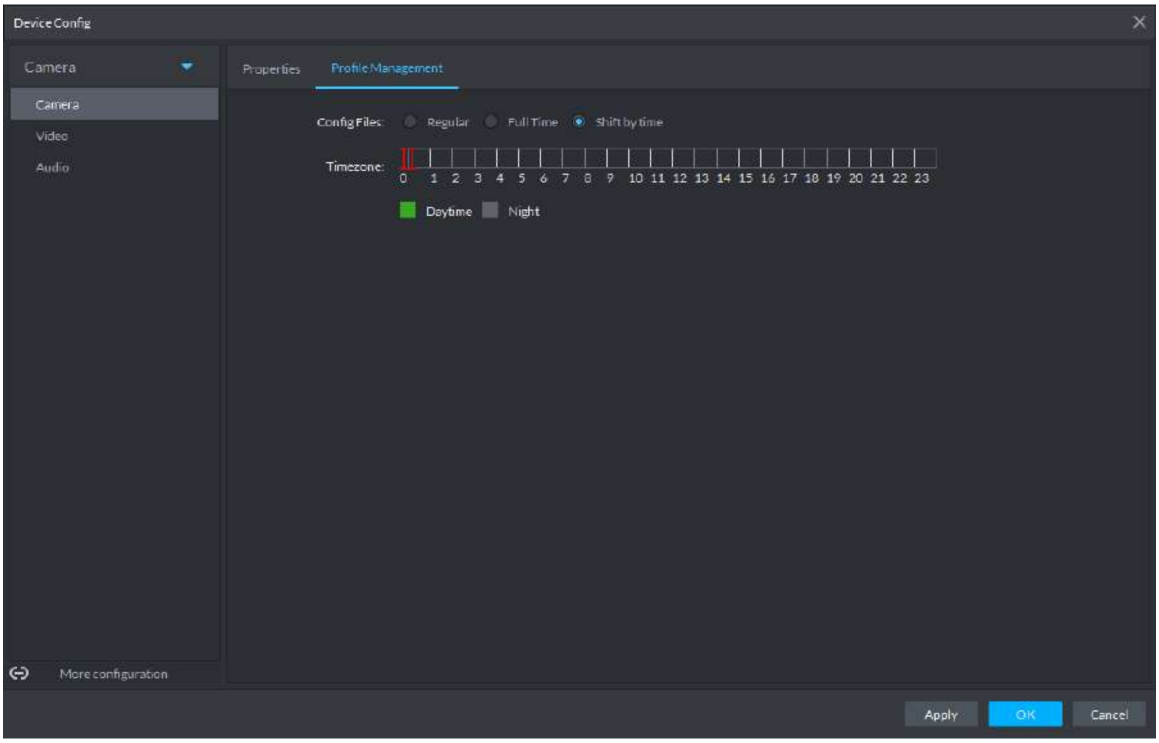


Config Files: ○ Regular ● Full Time ○ Shift by time

Always Enable: Daytime

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

Figure 5-29 Shift by time



Config Files: ○ Regular ○ Full Time ● Shift by time

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

- PTZ control interface is available for PTZ or speed dome.
- Click More Configuration, and open WEB config interface of the device.

5.3.3.2 Video

You can set some video parameters, including video stream, snapshot stream, overlay, ROI, save path, and video encryption.

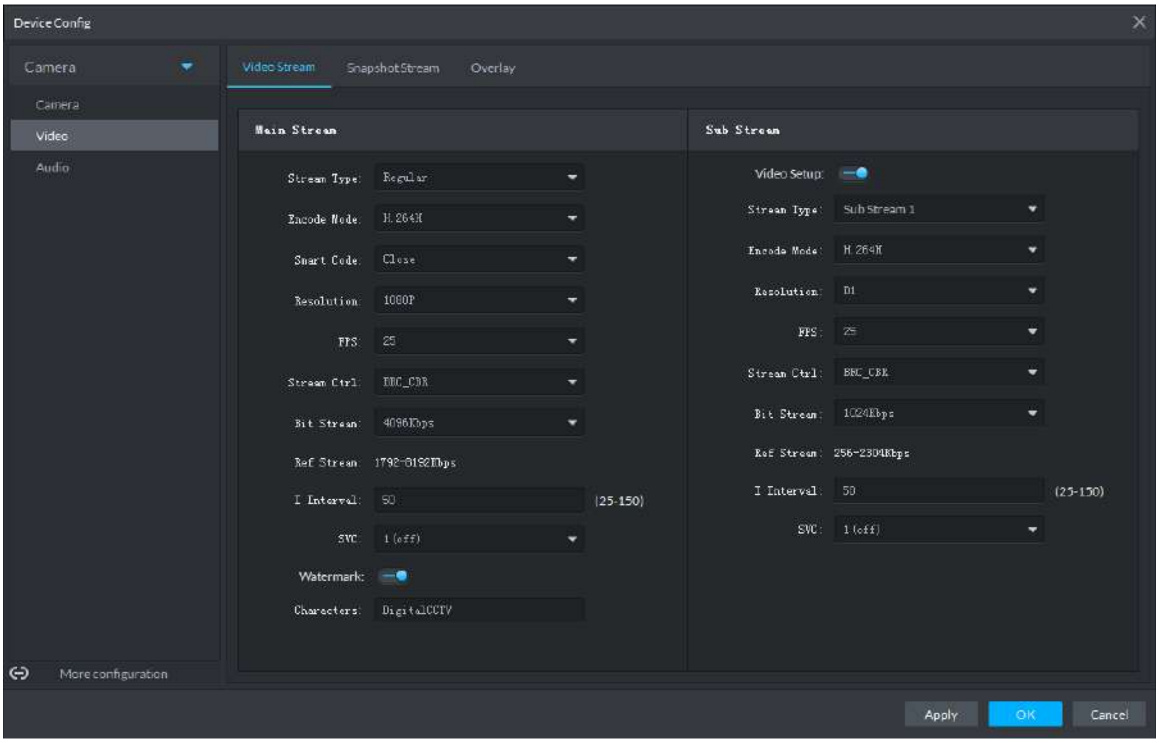
5.3.3.2.1 Video Stream

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

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

The **Video Stream** interface is displayed. See Figure 5-30.

Figure 5-30 Video stream



Main Stream

Stream Type: Regular
Encode Mode: H.264H
Smart Code: Close
Resolution: 1080P
FPS: 25
Stream Ctrl: BRC_CBR
Bit Stream: 4096Kbps
Ref Stream: 1792-8192Kbps
I Interval: 50 (25-150)
SVC: 1 (off)
Watermark:
Characters: DigitalCCTV

Sub Stream

Video Setup:
Stream Type: Sub Stream 1
Encode Mode: H.264H
Resolution: D1
FPS: 25
Stream Ctrl: BRC_CBR
Bit Stream: 1024Kbps
Ref Stream: 256-2304Kbps
I Interval: 50 (25-150)
SVC: 1 (off)

Step 2 To set up Video Stream, see Table 5-19 for the details of various parameters.

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

Table 5-19 Video stram parameter description

Parameter	Description
Video Setup	Indicates whether to set up the Sub Stream parameters.
Encode Mode	The following video encoding modes are available: ● H.264: Main Profile. ● H.264H: High Profile. ● H.265: Main Profile.
Smart Code	Turning on Smart Code helps compress the images more and reduce the storage space. When Smart Code is on, the device does not support sub stream 2, ROI, IVS event detection. The actual screens shall prevail.
Resolution	The resolution of the videos. Different devices might have different max resolutions. The actual interfaces shall prevail.
FPS	The number of frames per second in a video. The higher the FPS, the more distinct and smooth the images.
Stream Ctrl	The following video stream control modes are available: ● BRC_CBR: The bit stream changes slightly around the preset value. ● BRC_VBR: The bit stream changes according to the monitored scenes. When the **Encode Mode** is set to **MJPEG**, BRC_CBR remains the only option for stream control.

Parameter	Description
Image Quality	This parameter can be set only when **Stream Ctrl** is set to BRC_VBR. Video image quality is divided into six grades: Best, Better, Good, Bad, Worse and Worst.
Bit Stream	This parameter can be set only when **Stream Ctrl** is set to **BRC_CBR**. You can select the proper stream value from the dropdown box based on actual scenarios.
Ref Stream	The system will recommend an optimal range of stream values to users based on the resolution and FPS set up by them.
I Interval	Refers to the number of P frames between two I frames. The range of I Interval changes with FPS. It is recommended to set the I Interval to be two times as the FPS value.
SVC	FPS is subject to layered encoding. SVC is a scalable video encoding method on time domain. The default value is 1, that is non-layered encoding.
Watermark	Turn on **Watermark** to enable this feature. You can verify the watermark characters to check whether the video has been tempered or not.
Characters	Characters for watermark verification. The default value is DigitalCCTV.

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

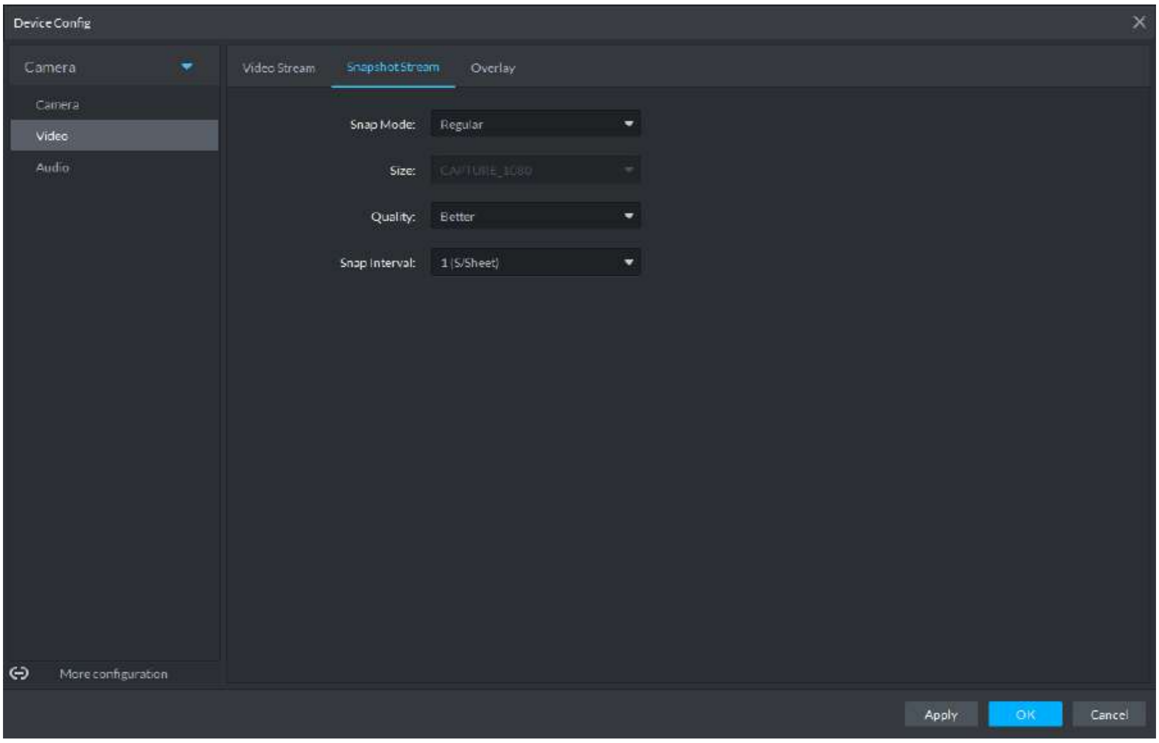
5.3.3.2.2 Snapshot Stream

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

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

The **Snapshot Stream** interface is displayed. See Figure 5-31.

Figure 5-31 Snapshot stream



Snap Mode: Regular

Size: CAPTURE_1080

Quality: Better

Snap Interval: 1 (S/Sheet)

Step 2 To set up Snapshot Stream, see Table 5-20 for the details of various parameters.

Table 5-20 Snapshot stream parameter description

Parameter	Description
Snap Mode	It includes **Regular** and **Trigger**. ● **Regular** refers to capturing pictures within the time range set up in a time table. ● **Trigger** refers to capturing pictures when video detection, audio detection, IVS events, or alarms are triggered, provided that video detection, audio detection, and corresponding snapshot functions are turned on.
Size	Same as the resolution in Main Stream.
Quality	Sets up image quality. It is divided into six grades: Best, Better, Good, Bad, Worse and Worst.
Snap Interval	Sets up the frequency of snapshots. Select Custom to manually set up the frequency of snapshots.

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

5.3.3.2.3 Overlay

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

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

The **Overlay** interface is displayed.

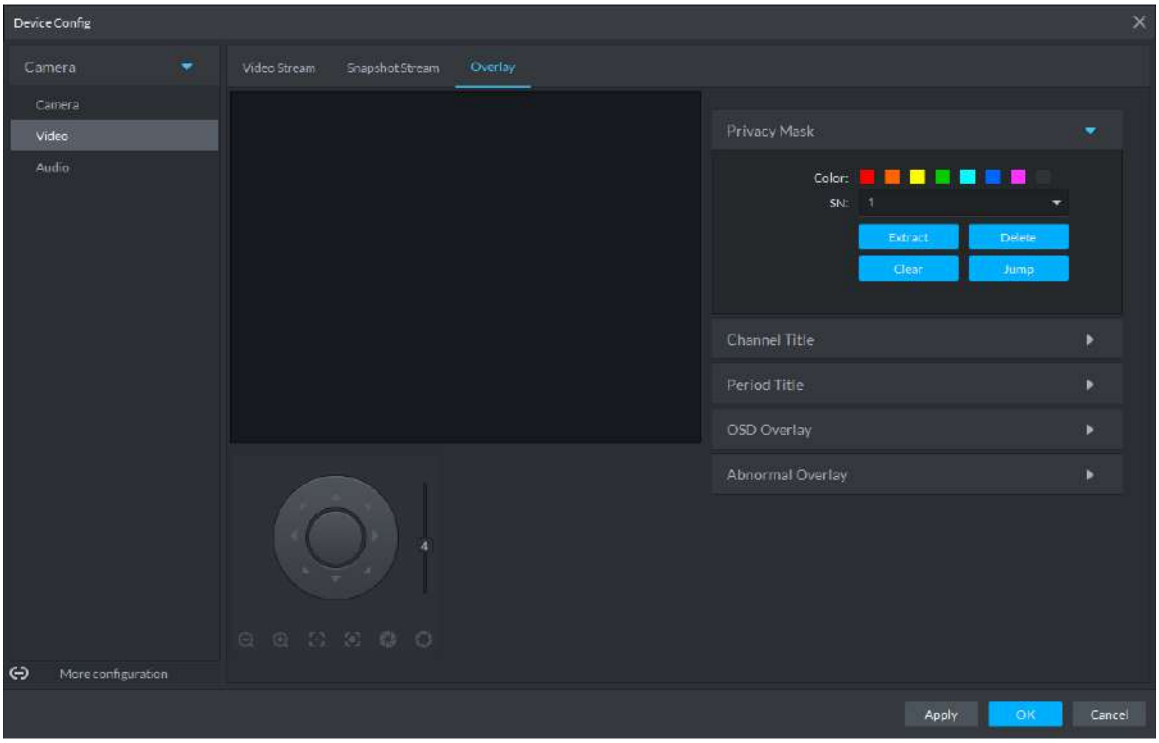
Step 2 (Optional) Set up Privacy Mask.

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

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

The **Privacy Mask** interface is displayed. See Figure 5-32.

Figure 5-32 Privacy mask



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

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

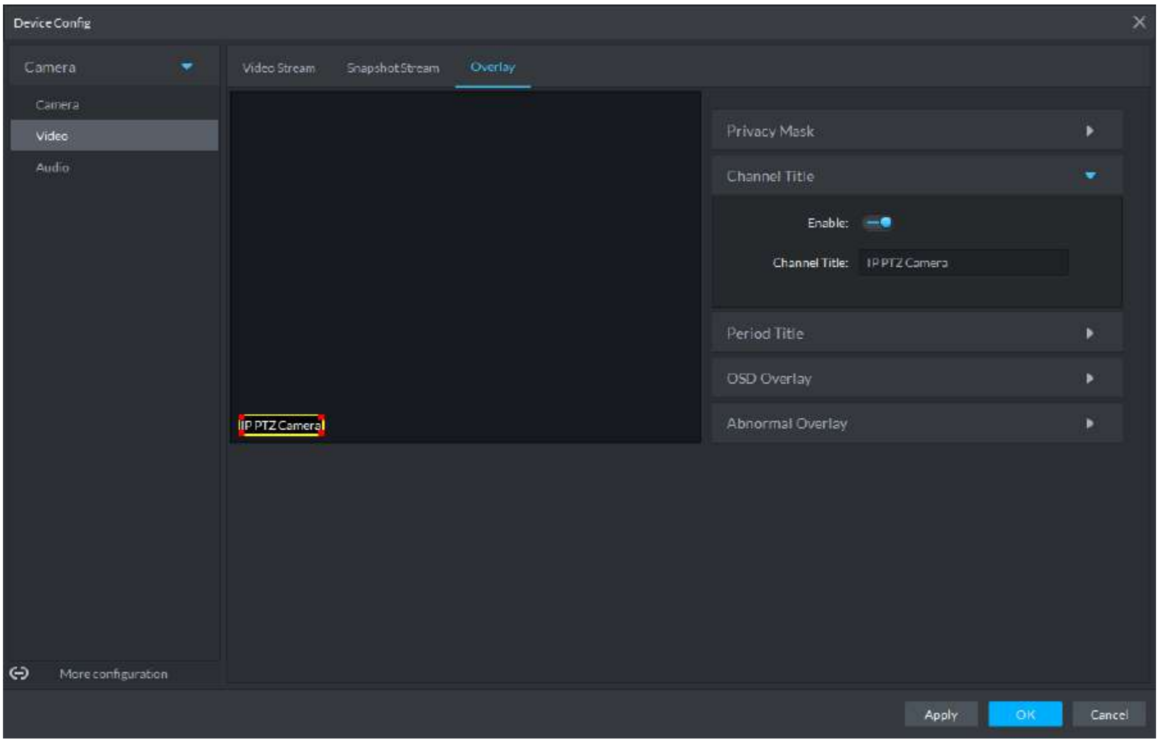
Step 3 (Optional) Set up Channel Title.

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

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

The **Channel Title** interface is displayed. See Figure 5-33.

Figure 5-33 Channel title



Enable:

Channel Title: IP PTZ Camera

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

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

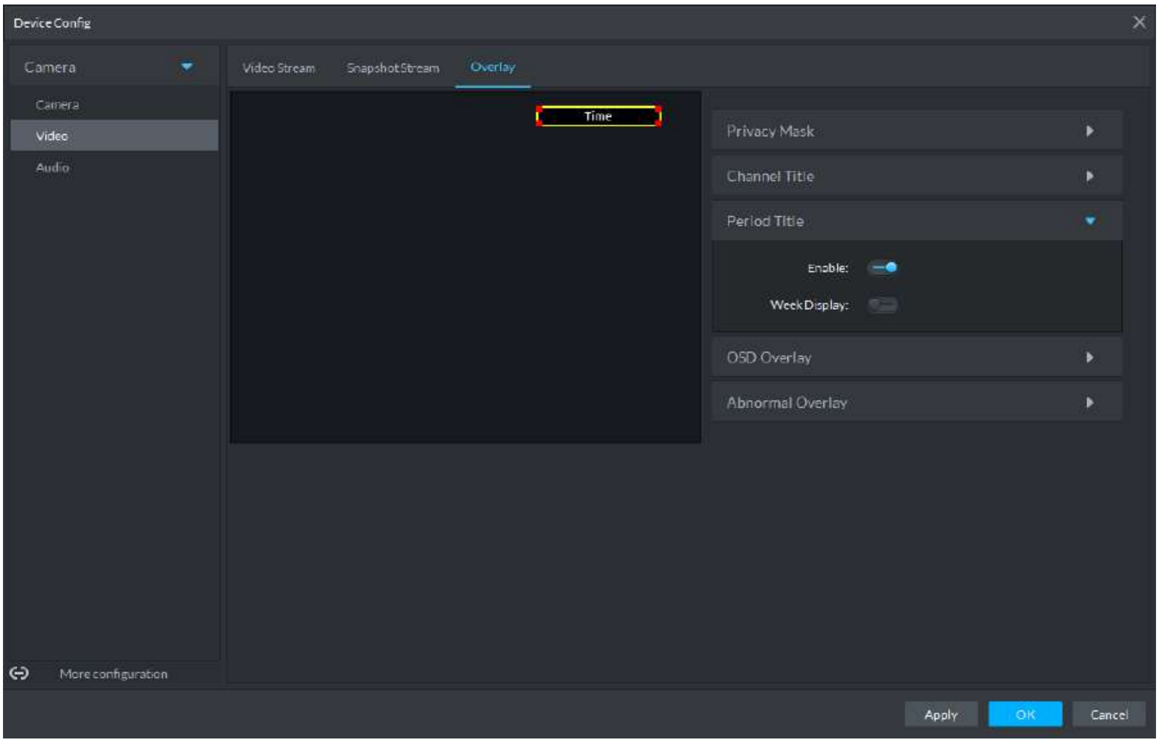
Step 4 (Optional) Set up Period Title.

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

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

The **Period Title** interface is displayed. See Figure 5-34.

Figure 5-34 Period title



2) Select **Enable** and the time information is displayed in the video images.

3) Select **Week Display** and the week information displays in video images.

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

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

5.3.3.3 Audio

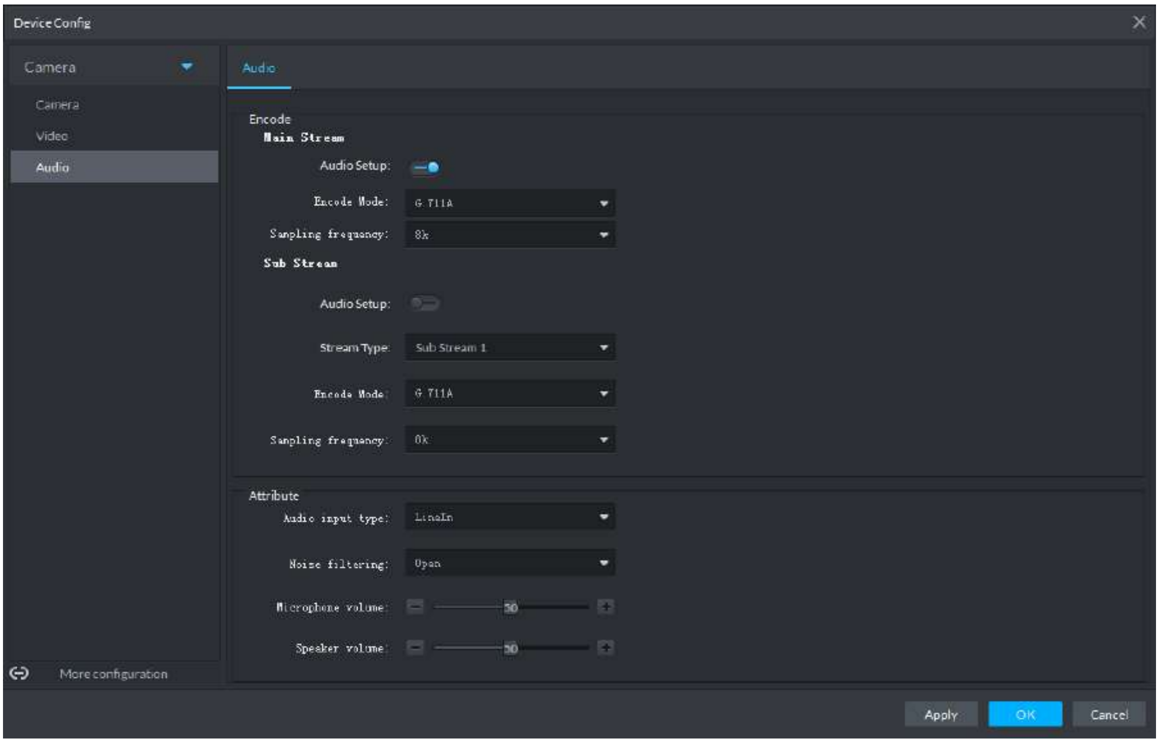
You can set some audio parameters such as Encode Mode, Sampling frequency, Audio input type, Noise filtering.

Some devices do not support audio functions.

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

The **Audio** interface is displayed. See Figure 5-35.

Figure 5-35 Audio



Encode

Main Stream

Audio Setup:

Encode Mode: G.711A

Sampling frequency: 8k

Sub Stream

Audio Setup:

Stream Type: Sub Stream 1

Encode Mode: G.711A

Sampling frequency: 0k

Attribute

Audio input type: LineIn

Noise filtering: Open

Microphone volume: 50

Speaker volume: 50

Step 2 To set up audio parameters, see Table 5-21 for details.

Table 5-21 Audio parameter

Parameter	Description
Enable	Audio cannot be enabled unless video has been enabled. After choosing Enable in Main Stream or Sub Stream sections, the network transmits a mixed flow of videos and audios. Otherwise, the transmitted flow only contains video images.
Encode Mode	The encoding modes of audios include G.711A, G.711Mu, AAC, and G.726. The preset audio encode mode applies both to audio talks and voice talks.
Sampling frequency	Available audio sampling frequencies include 8K, 16K, 32K, 48K, and 64K.
Audio input type	The following types of audios connected to devices are available: ● LineIn: The device must connect to external audio devices. ● Mic: The device does not need external audio devices.
Noise filtering	After enabling noise filtering, the system automatically filters out the noises in the environment.
Microphone volume	Adjusts the microphone volume. Only some devices support adjusting microphone volume.
Speaker volume	Adjusts the speaker volume. Only some devices support adjusting speaker volume.

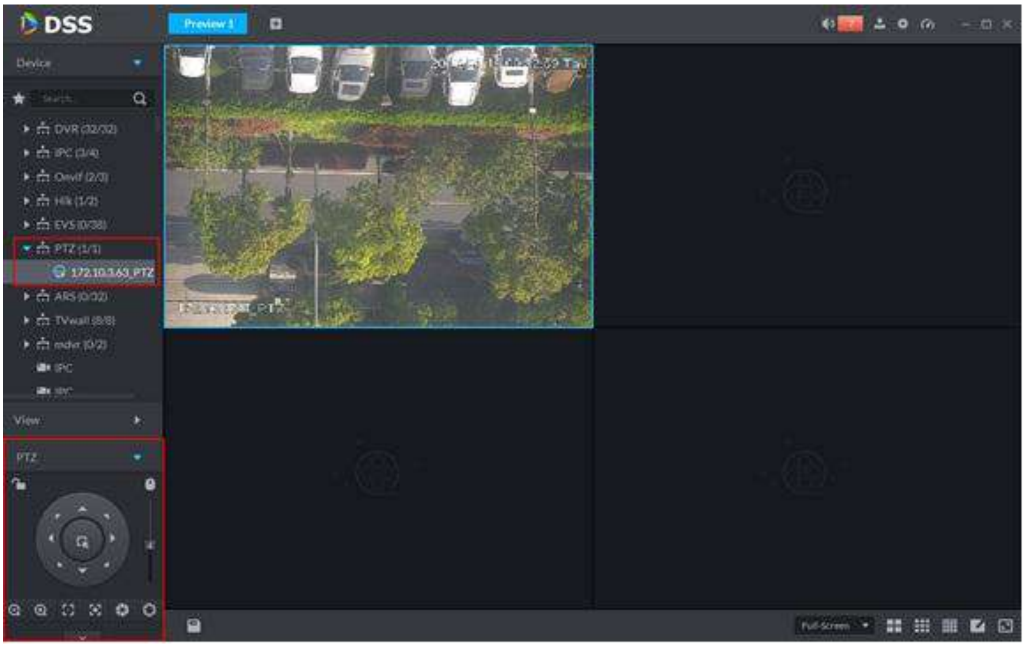
Step 3 Click **OK** to save the configurations.

5.3.4 PTZ

5.3.4.1 PTZ Operation Interface

Step 1 On Preview interface, open video from the PTZ camera, you can see PTZ operation interface on the left. See Figure 5-36.

Figure 5-36 Preview



Step 2 Click ⌄ at the bottom of the interface to operate. See Figure 5-37.

Figure 5-37 PTZ

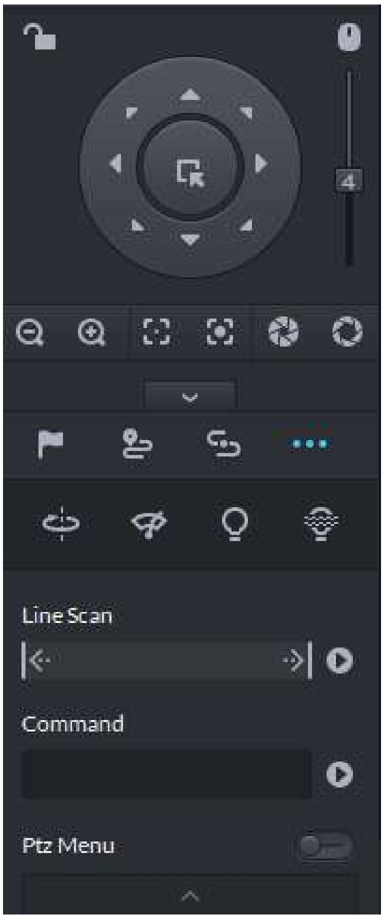


Table 5-22 PTZ operation

Parameters	Description
🔓	Click 🔓 to lock the current PTZ. Locked status shows as 🔒. Control over PTZ varies depending on user level. ● When user of low level locks PTZ, user of high level can unlock and enable the PTZ by clicking🔒. ● When user of high level locks PTZ, user of low level can't unlock the PTZ, unless PTZ automatically unlock itself. ● Users of the same level can unlock PTZ locked by each other. 🕮 Default time for automatically unlocking PTZ is 30s.
🖱	• Control speed dome with mouse.
Direction Key	• Set rotation direction of PTZ, eight directions are available in total: up, down, left, right, upper left, upper right, lower left and lower right.

Parameters	Description
⬚	- 3D Location and Partially Zoom In (for Speed Dome PTZ), to zoom in or zoom out the selected area. 📖 This function can be controlled with mouse only.
4	From top to the bottom to adjust rotation speed of PTZ, to set the step size chosen from 1 to 8.
⊖ ⊕	- Zoom, to control zoom operation of speed dome.
⛶ ⊡	- Focus, to adjust focus.
◎ ◎	- Aperture, to adjust brightness.
⚑, ⚑, ⚑, •••	It is to set preset, tour, pattern, scan, rotation, wiper, light and IR light function. Refer to 5.3.4.2 PTZ Settings for more information.

5.3.4.2 PTZ Settings

5.3.4.2.1 Configuring Preset

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

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

Step 2 Click ⚑.

Step 3 Place mouse over 1 and click ✎.

Step 4 Input preset point SN, and click ✓.

Adding preset point completed.

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

5.3.4.2.2 Configuring Tour

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

📖

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

Step 1 Click⚑.

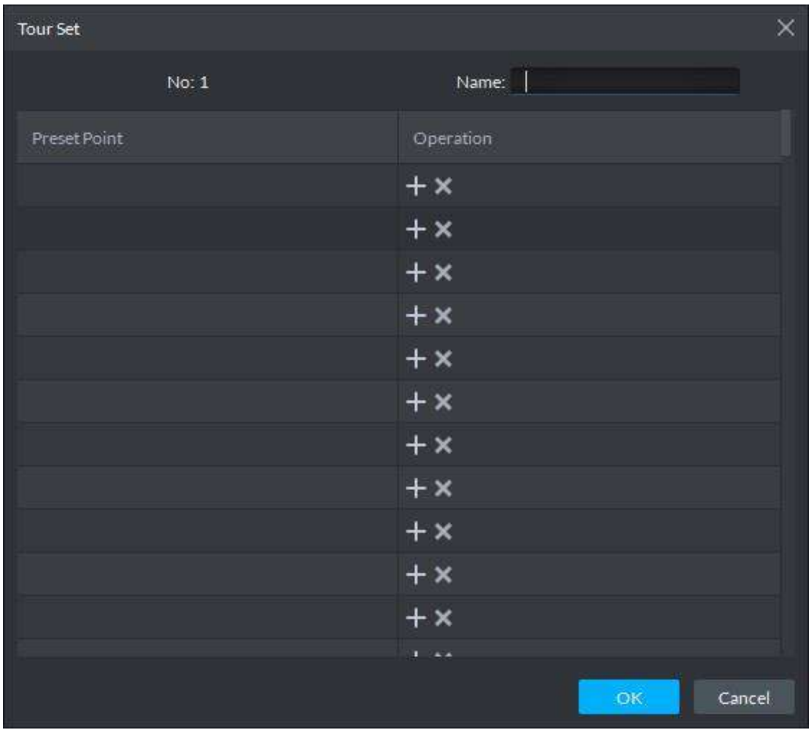
Step 2 Place mouse over 1 and click ✎.

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 5-38.

Figure 5-38 Add preset



Step 4 Click **OK**.

System prompts Tour Saved Successfully.

Step 5 Click **OK**.

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

5.3.4.2.3 Configuring Pattern

Pattern is equivalent to a record process.

Step 1 Click .

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

Step 3 Click to complete pattern setup.

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

5.3.4.2.4 Configuring Scan

Step 1 Click •••.

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

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

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

5.3.4.2.5 Enable/Disable Pan

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

5.3.4.2.6 Enable/Disable wiper

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

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

5.3.4.2.7 Enable/Disable light

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

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

5.3.4.2.8 Enable/Disable IR light

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

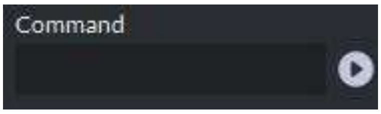
5.3.4.2.9 Configuring custom commands

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

Step 1 Click•••.

Step 2 Input command on the customized command interface. See Figure 5-39.

Figure 5-39 Command



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

5.3.4.2.10 PTZ Menu

Step 1 Click•••.

The PTZ menu is shown as in Figure 5-40.

Figure 5-40 Menu

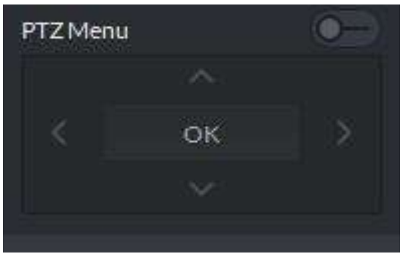


Table 5-23

Parameters	Description
⌃/⌄	Up/down button. Move the cursor to the corresponding item.
‹/›	Left/right. Move the cursor to set parameters.
○—	Click ○— to enable PTZ menu function. System displays main menu on the monitor window.
—●	Click —● to close PTZ menu function.
OK	It is the confirm button. It has the following functions. ● If the main menu has the sub-menu, click OK to enter the sub-menu. ● Move the cursor to Back and then click OK to go to go back to the previous menu. ● Move the cursor to Exit and then click OK to exit the menu.

Step 2 Click OK.

The monitor window displays main menu. See Figure 5-41.

Figure 5-41 Main menu

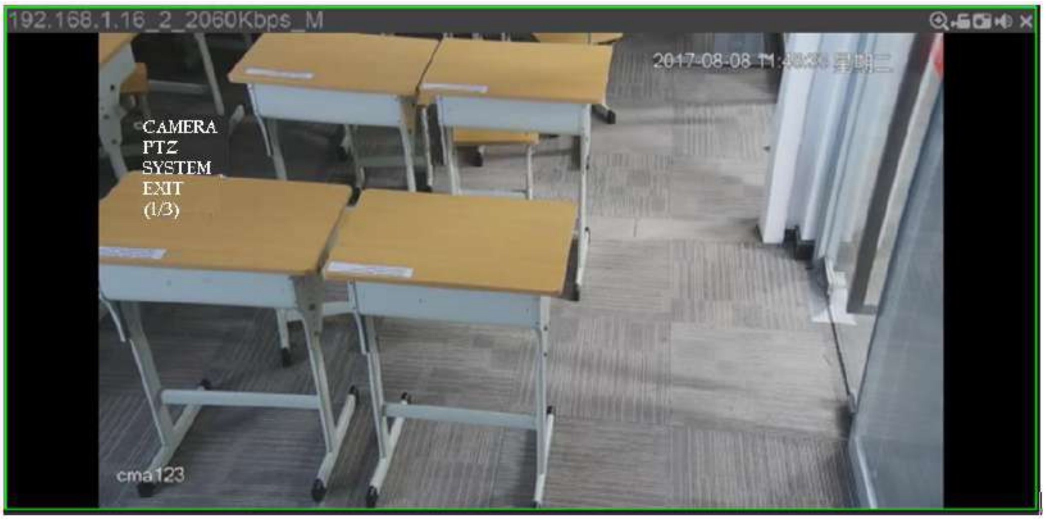


Table 5-24 Main menu parameter

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

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

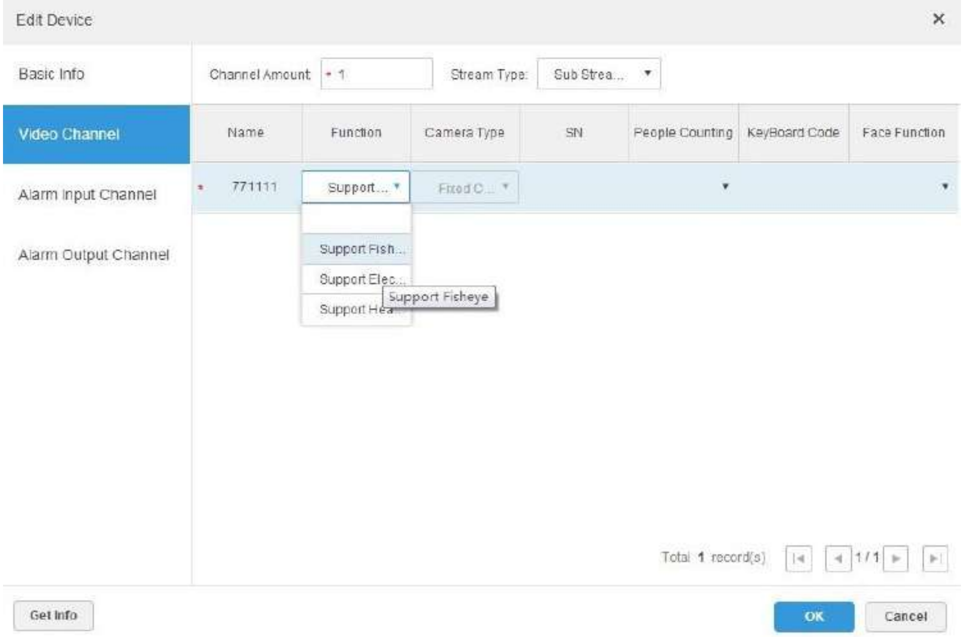
5.3.5 Smart Track

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

5.3.5.1 Preparations

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

Figure 5-42 Fisheye



Channel Amount: * 1 Stream Type: Sub Strea...

Name	Function	Camera Type	SN	People Counting	KeyBoard Code	Face Function
* 771111	Support...	Fixed C...				

Total 1 record(s) 1/1

5.3.5.2 Adding Smart Track Config

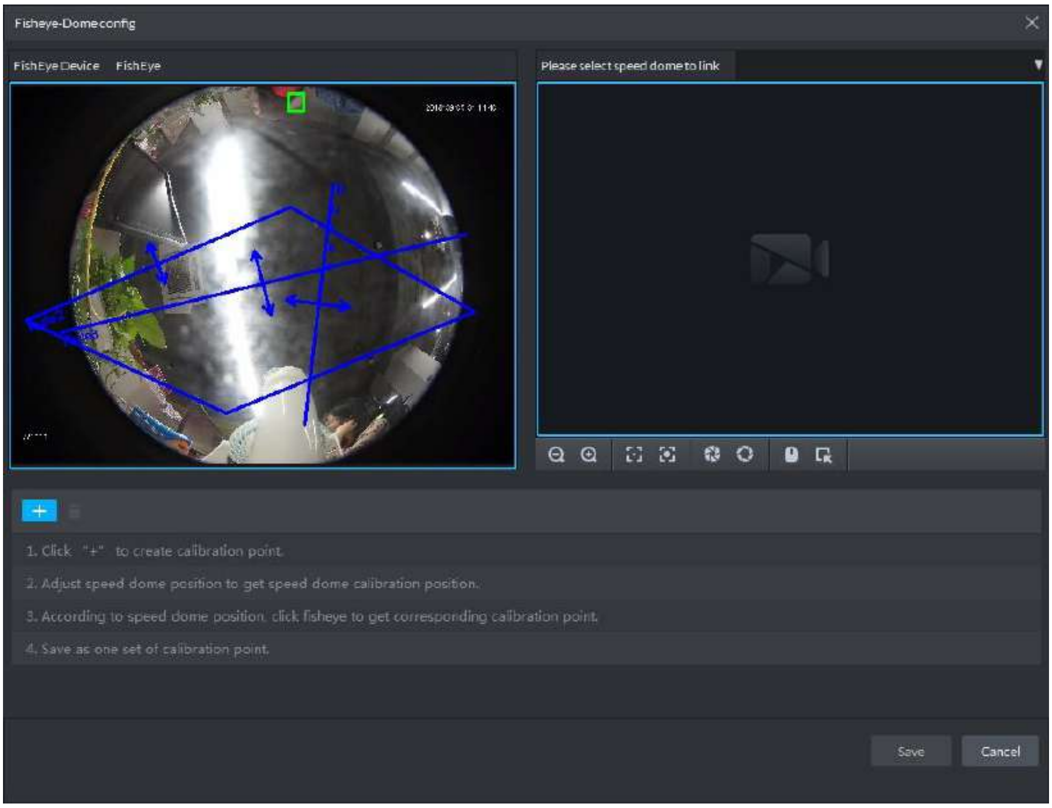
Step 1 Select the fisheye device on the device tree and then right click to select Smart track.

📖

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

The Smart track interface is displayed. See Figure 5-43.

Figure 5-43 Fisheye dome config



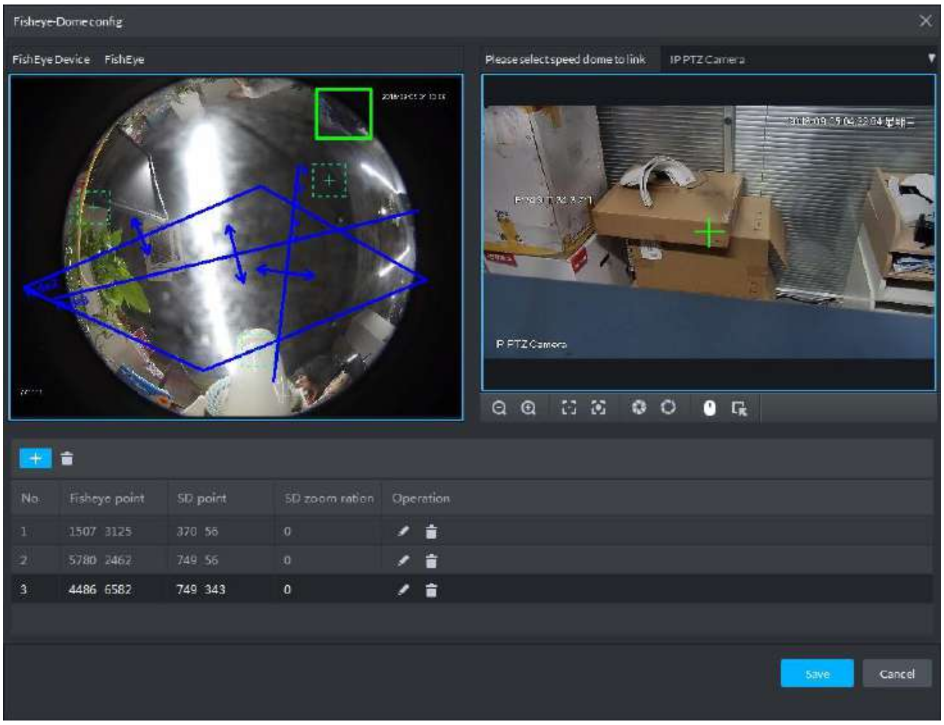
1. Click "+" to create calibration point.
2. Adjust speed dome position to get speed dome calibration position.
3. According to speed dome position, click fisheye to get corresponding calibration point.
4. Save as one set of calibration point.

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 5-44.

Figure 5-44 Configure calibration point



No.	Fisheye point	SD point	SD zoom ration	Operation
1	1507 3125	370 56	0	✎ 🗑
2	5780 2462	749 56	0	✎ 🗑
3	4486 6582	749 343	0	✎ 🗑

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

Step 4 Click✓ to save the calibration point.

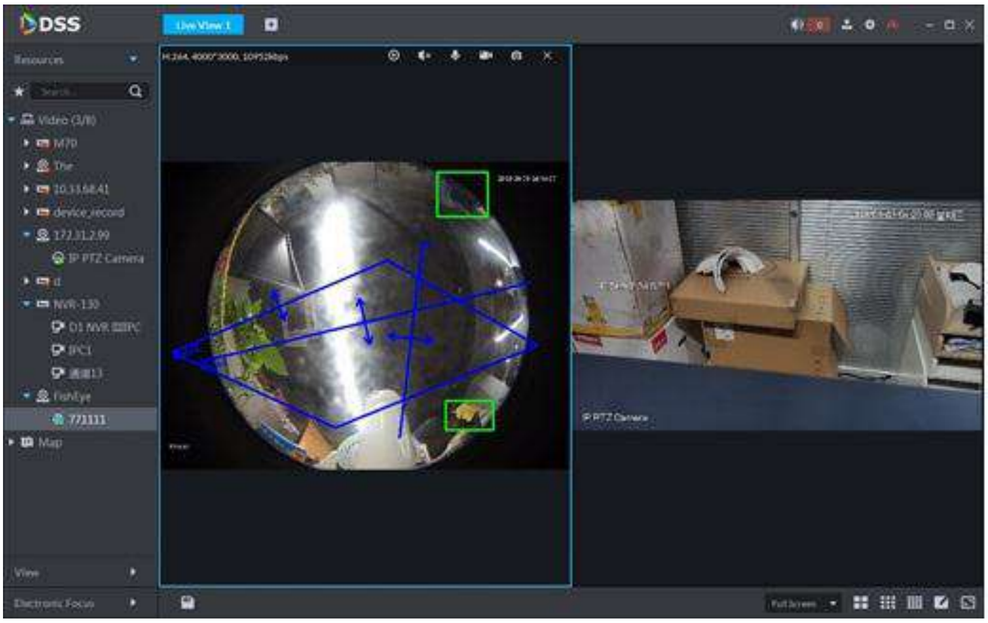
Refer to above steps to add at least three calibration points. These three points shall not be on the same straight line.

Step 5 Click Save.

5.3.5.3 Enable Smark Track Function

Step 1 Select the fisheye device on the device tree and then right click to select Smart track. See Figure 5-45.

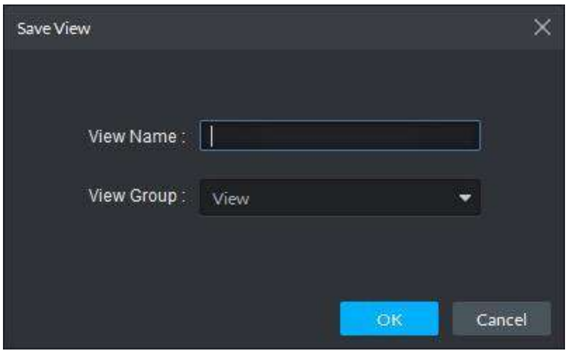
Figure 5-45 Smart track



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 5-46.

Figure 5-46 Save view



Save View

View Name :

View Group : View

OK Cancel

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

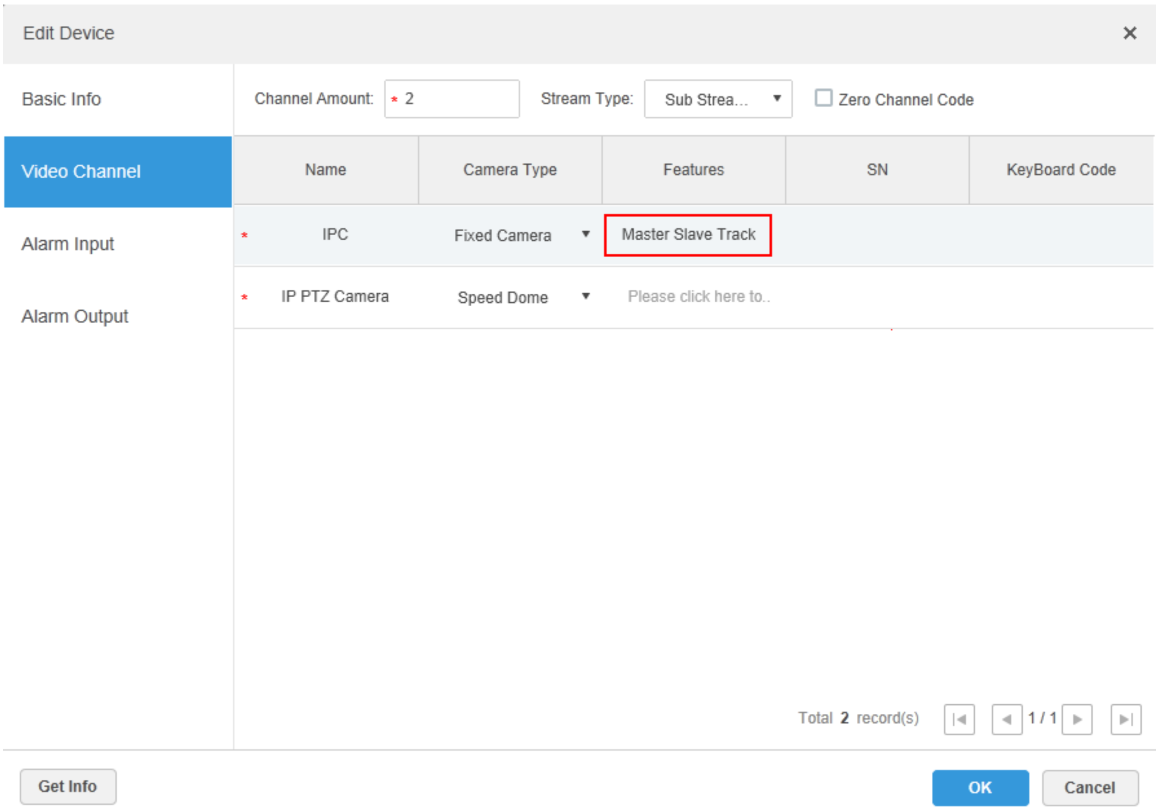
5.3.6 Smart Track

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

5.3.6.1 Preparation before Operation

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

Figure 5-47 Master slave track



Channel Amount: * 2 Stream Type: Sub Strea... ▼ □ Zero Channel Code

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

Total 2 record(s) 1 / 1

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

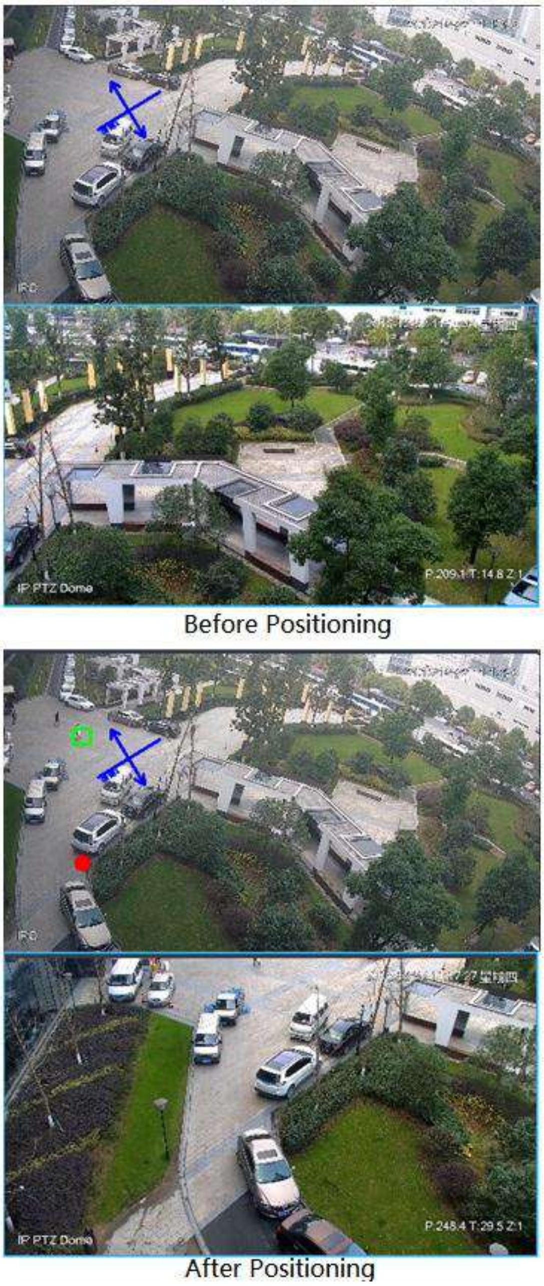
5.3.6.2 Applying Smart Track

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

5.3.6.2.1 Manual Positioning

Click any position on the bullet image, and the PTZ will position the image to the area designated by bullet due to smart track. See Figure 5-48. Click the red spot on the bullet image, and the PTZ central point will move to the corresponding location automatically.

Figure 5-48



Before Positioning

After Positioning

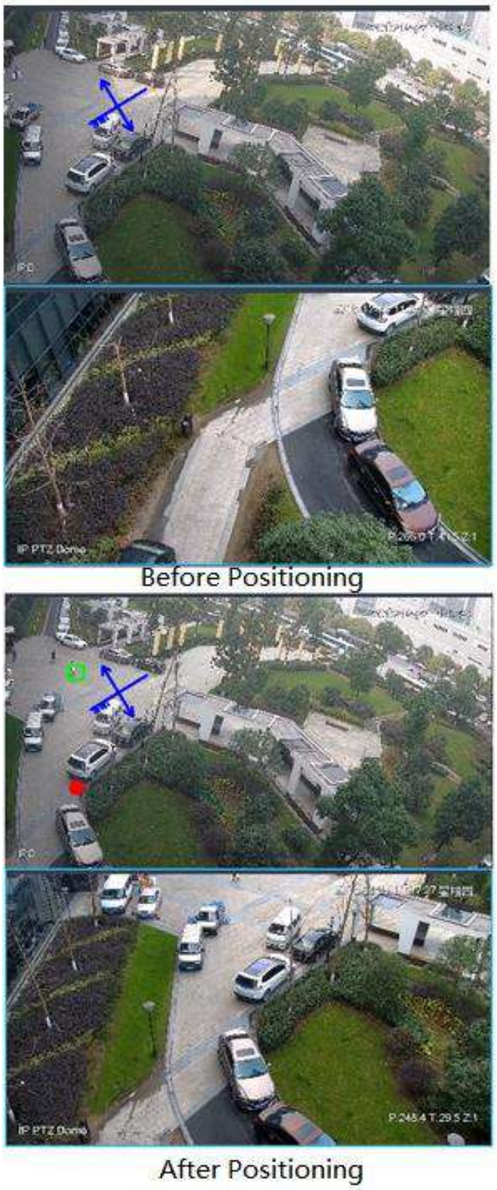
5.3.6.2.2 3D Positioning

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

Draw rectangular box from upper left to lower right, zoom in after being positioned by PTZ camera. See Figure 5-49.

Draw rectangular box from lower right to upper left; zoom out after being positioned by PTZ camera. See Figure 5-50.

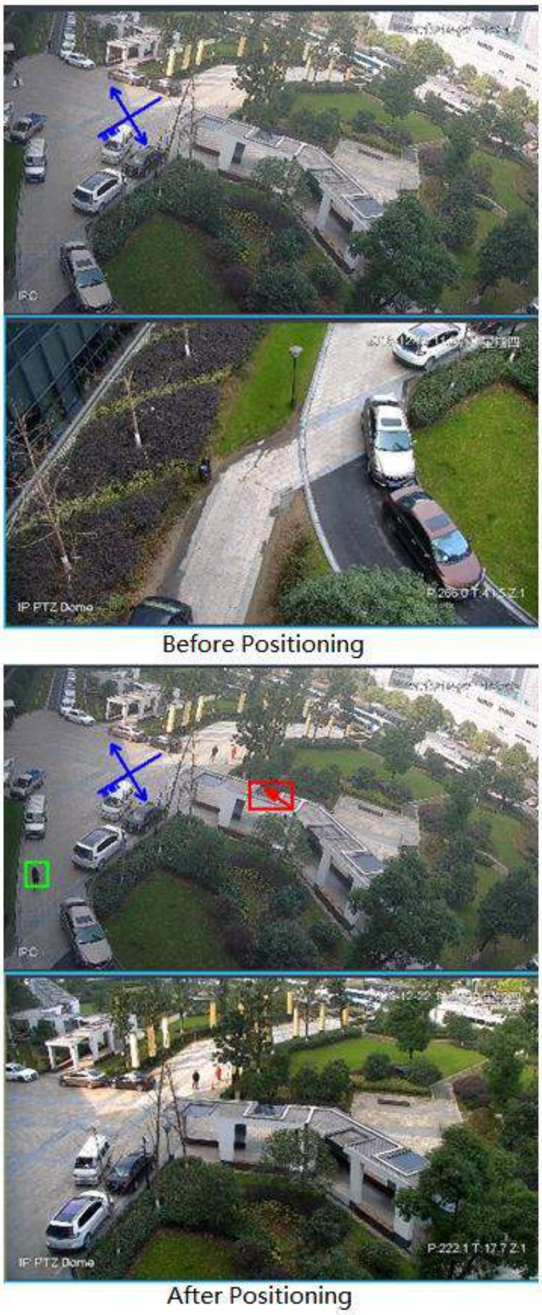
Figure 5-49 3D positioning (Zoom in after positioning)



Before Positioning

After Positioning

Figure 5-50 3D positioning (Zoom out after positioning)



Before Positioning

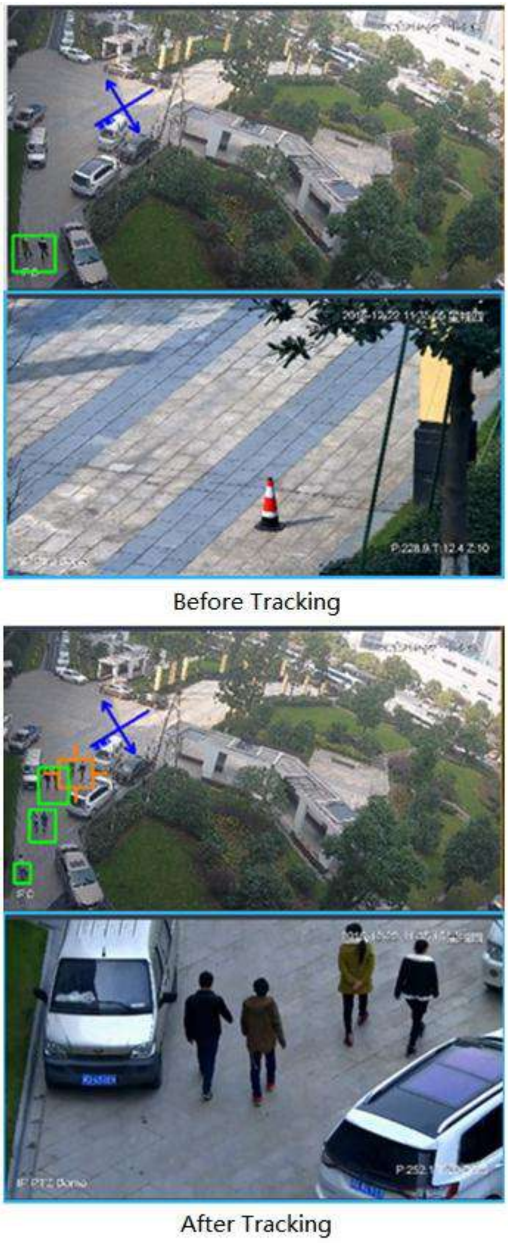
After Positioning

5.3.6.2.3 Manual Track

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

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

Figure 5-51 Manual track



Before Tracking

After Tracking

5.3.6.2.4 Auto Track

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

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

In the device list on **Live** interface, select individual bullet, bullet PTZ all-in-one camera or panoramic+PTZ camera, right click and select Auto **Track** > **On** and eenable auto track. When there is moving target in the image, then PTZ camera will track the target automatically. See Figure 5-52 and Figure 5-53.

Figure 5-52 Auto track

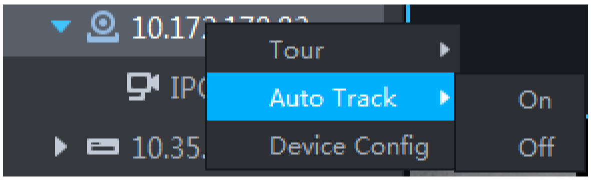
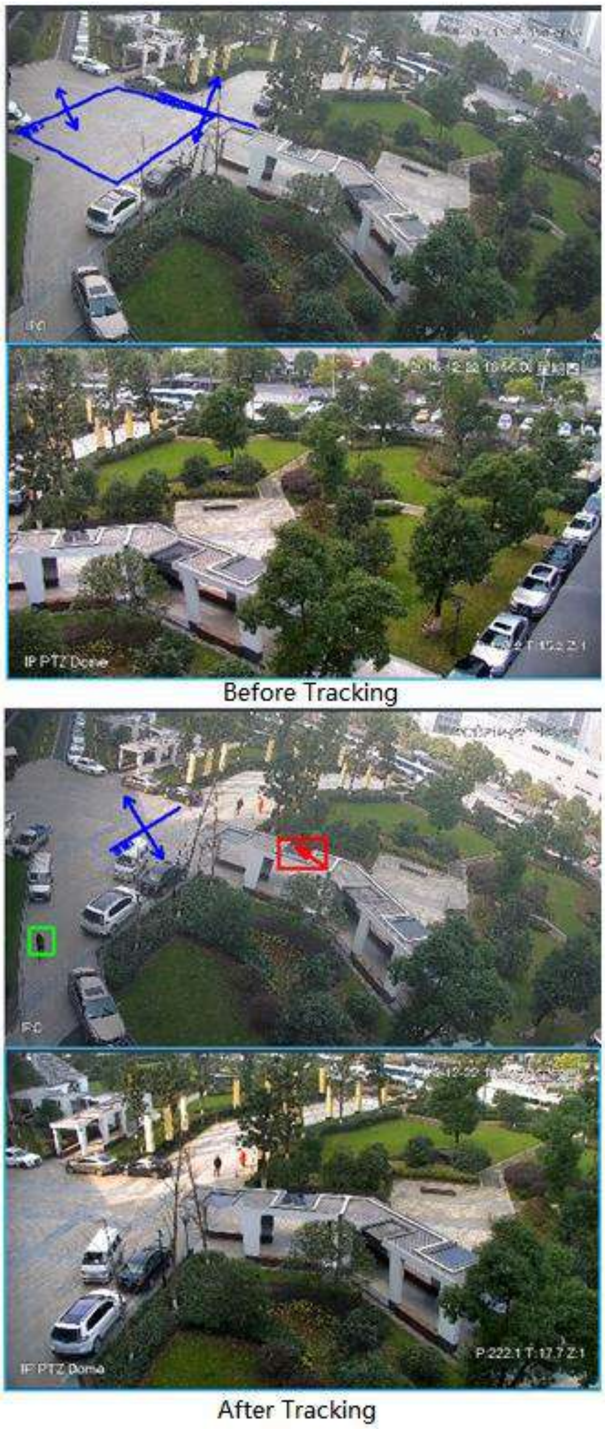


Figure 5-53 Auto track



5.3.6.2.5 Preset Return

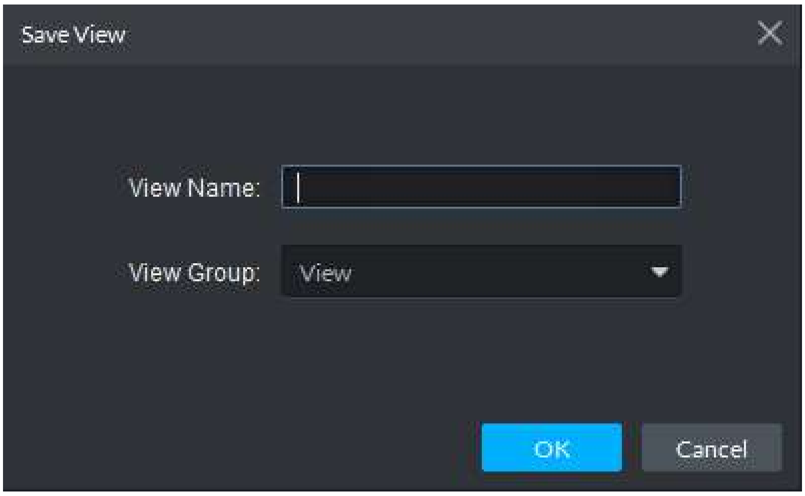
Enable preset return when idle during calibration, in any status, when there is no target triggering track within the specific period on the bullet image, then PTZ image will return to the designated preset.

5.3.7 View Tour

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

Step 2 Click 💾 in the lower part, system pops up **Save View** dialogue box. See Figure 5-54.

Figure 5-54 Save view



Save View

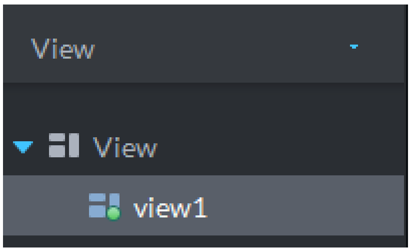
View Name:

View Group: View

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

Check the added view under View tab on the left. See Figure 5-55.

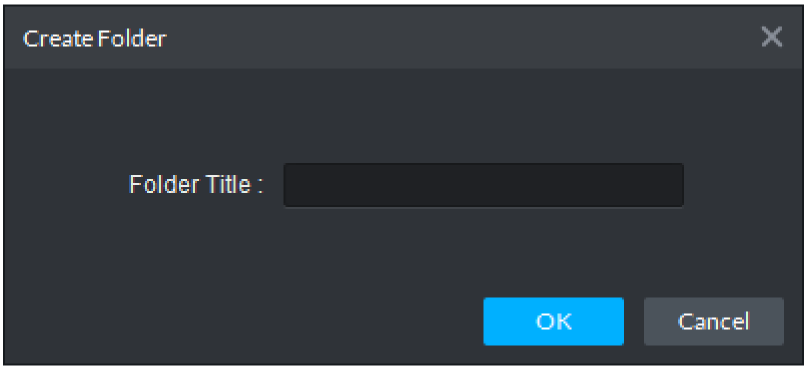
Figure 5-55 View



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

Create folder dialogue box is displayed. See Figure 5-56.

Figure 5-56 Create folder



Create Folder

Folder Title :

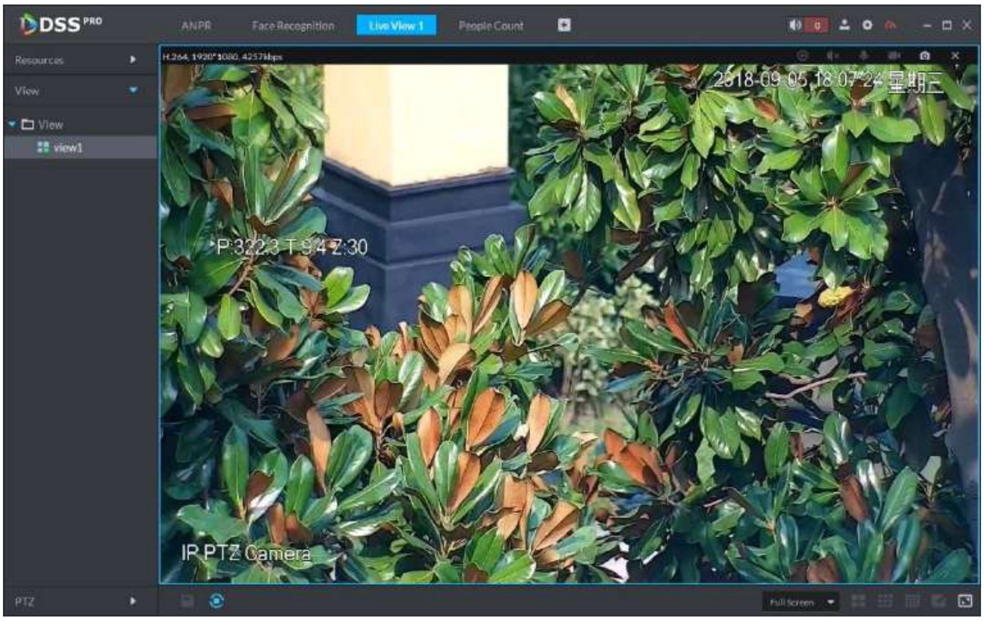
Step 5 Input **Folder Title** and click **OK**.

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

A View Tour will be initiated at intervals of 10s. See Figure 5-57.

Click to stop Tour.

Figure 5-57 View tour

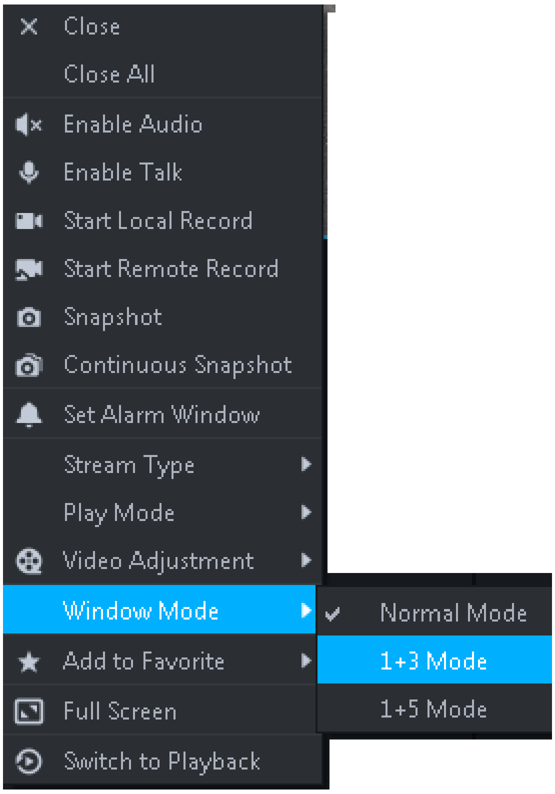


5.3.8 Region of Interest (RoI)

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

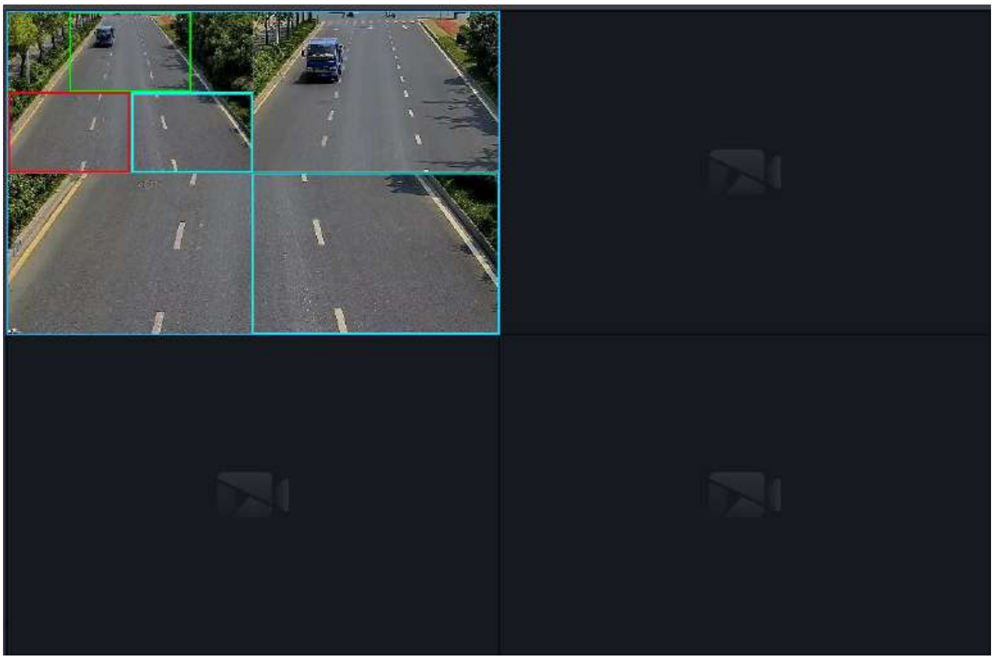
Right click to select Screen Mode in the live view window. See Figure 5-58.

Figure 5-58 Window mode



For example, select 1+3 mode. See Figure 5-59.

Figure 5-59 1+3 Mode



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.

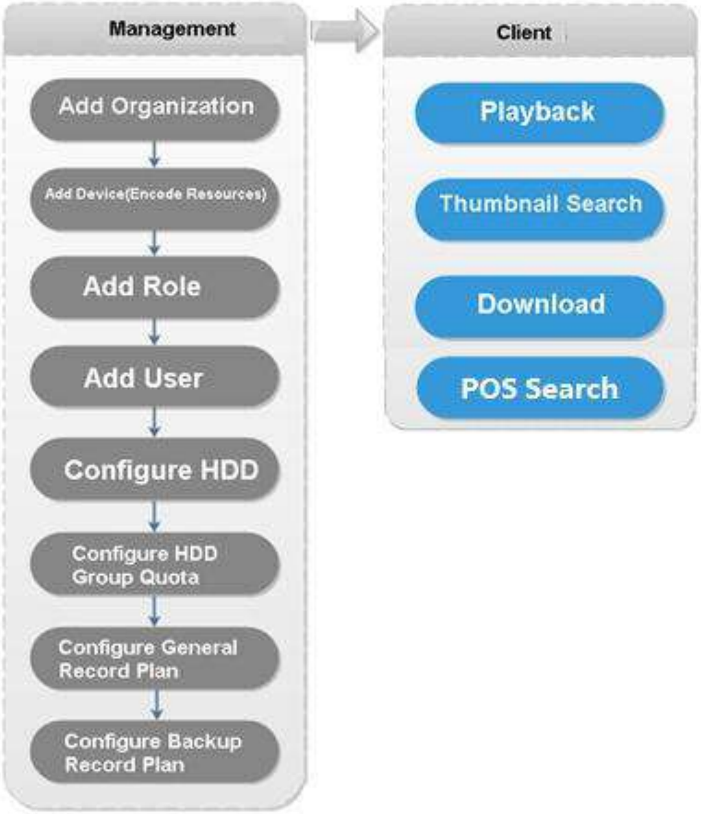
- Device Storage: Record to be stored in front-end SD card, or disks like DVR or NVR. Storage plan is configured on the device.
- Center Storage: Record to be stored in network storage server or DSS disks. For detailed configuration, see Storage config in System Introduction. To play back the record, 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 "4.6 Configuring Record Plan" for detailed information.

Refer to Figure 5-60 for Playback flows information.

Figure 5-60 Record playback flow


Management
Add Organization
Add Device(Encode Resources)
Add Role
Add User
Configure HDD
Configure HDD Group Quota
Configure General Record Plan
Configure Backup Record Plan
Client
Playback
Thumbnail Search
Download
POS Search

5.4.2 Record Playback

5.4.2.1 Search Record

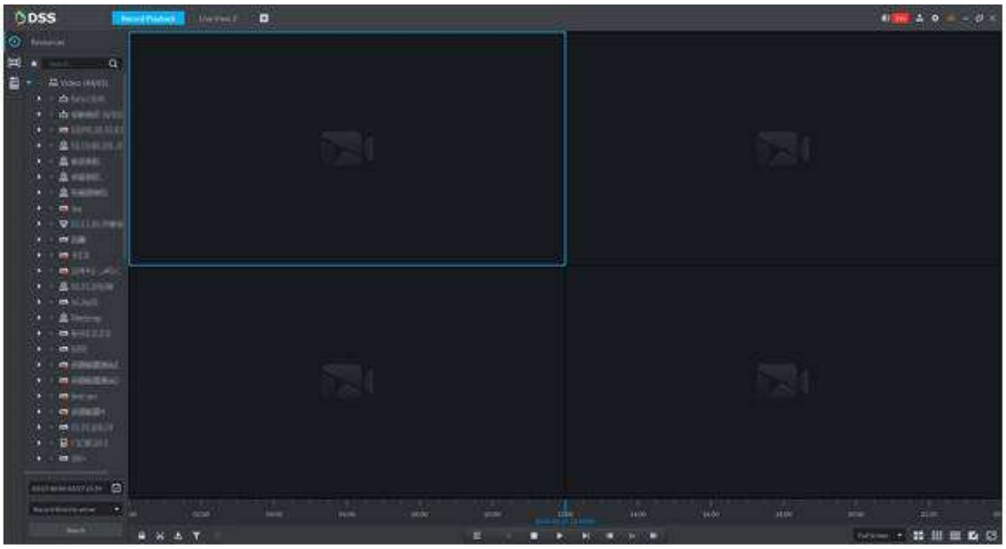
Search record of today, specified date or specified period.

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

Step 2 Click ⊙.

The **Record Playback** interface displayed. See Figure 5-61.

Figure 5-61 Record playback



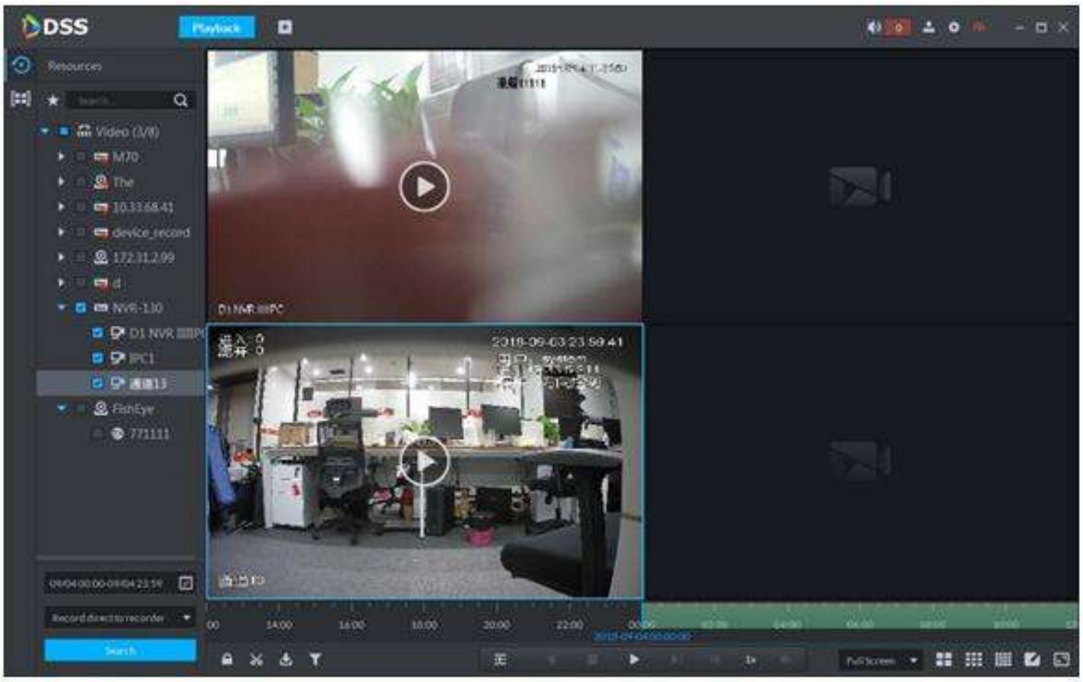
Step 3 Select a channel on the device tree.

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

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

Corresponding window begins playback the record of current channel. See Figure 5-62.

Figure 5-62 Playback



5.4.2.2 Record Control

Refer to Table 5-25 for buttons at the bottom of record playback interface and the description.

Table 5-25 Playback button

Icon	Description
🔒	Lock the video stored on server within some period of designated channel. Locked video will not be overwritten when disk is full.
✂	Cut video
⤓	Download video
▼	Filter video according to record type.
▦	Make dynamic detection analysis over some area of the record image, it only replays the video with dynamic image in the detection area.
☰	Playback record files of the same period from different channels on selected windows.
■ ‖	Stop/pause playback
⏮/⏭	Frame by frame playback/frame by frame backward.
« 1x »	Fast/slow playback. Max. supports 64X or 1/64X.
10:00 12:00 14:00 16:00 2018-07-18 12:16:09	During playback, you can drag time progress bar to play back record at the specific time.

5.4.2.3 Record Type Filter

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

Step 1 On **Record Playback** interface, click. See Figure 5-63.

The system displays the interface of **Record Type Filter**. See Figure 5-64.

Figure 5-63 Record type filter

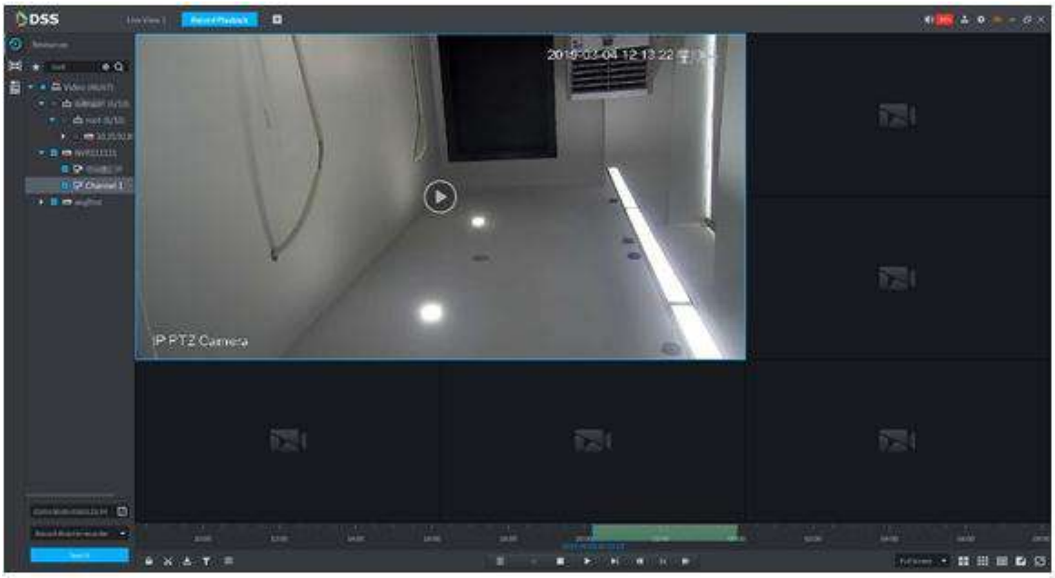
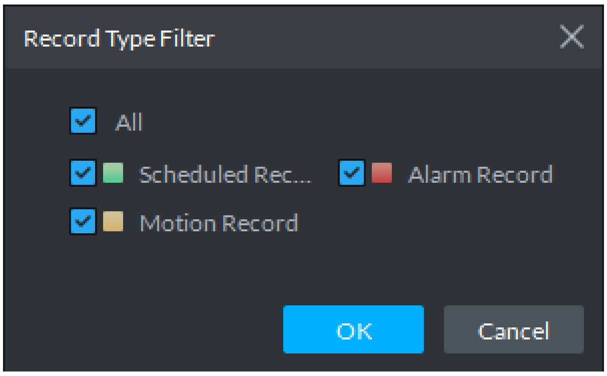


Figure 5-64 Record filter



Record Type Filter

☑ All

☑ 🟩 Scheduled Rec... ☑ 🟥 Alarm Record

☑ 🟨 Motion Record

OK Cancel

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

The system only displays the video of selected type.

5.4.2.4 Smart Search

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

Step 1 Click on the interface of **Record Playback**. See Figure 5-65.

The system displays the interface of Smart Search. See Figure 5-66. 22×18 squares are displayed in the window.

Figure 5-65 Enable smart search

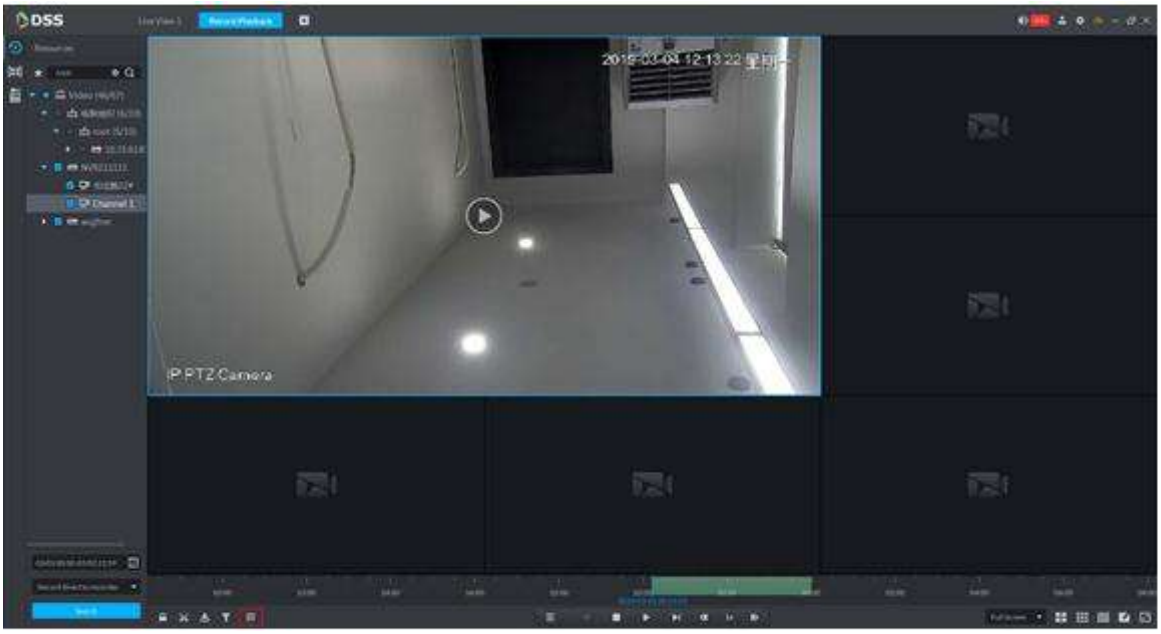
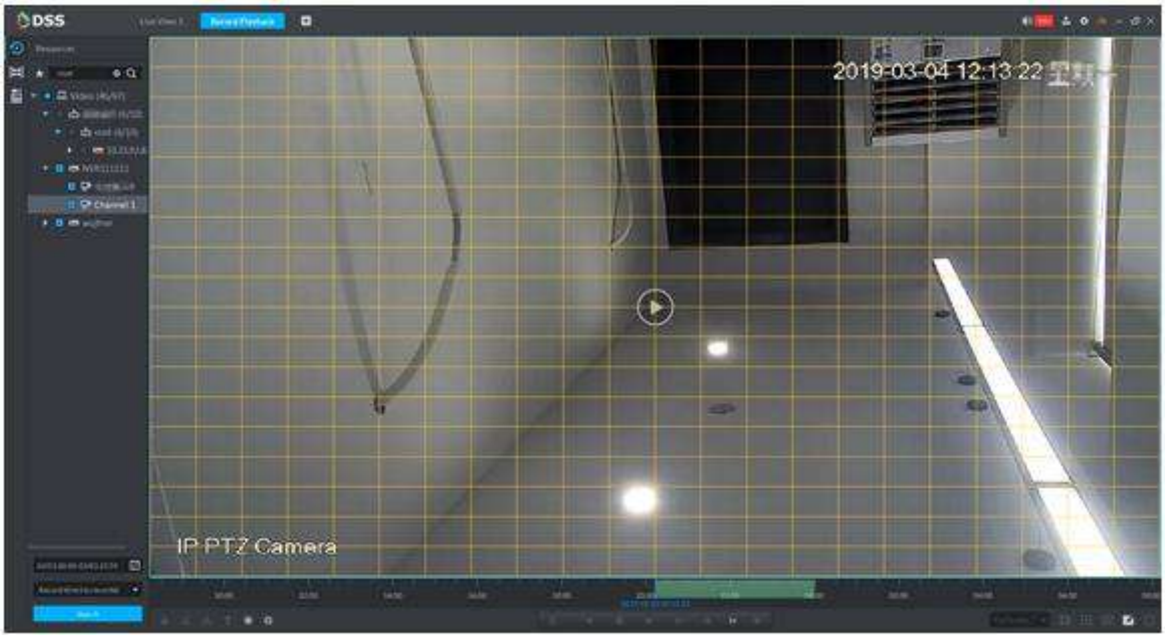


Figure 5-66 Smart search



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

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

Step 3 Click and start smart search analysis.

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

Click and you can reselect detection area.

Step 4 Click the play button on the image or control bar.

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

Step 5 Click and exit smart search.

5.4.2.5 Lock Record

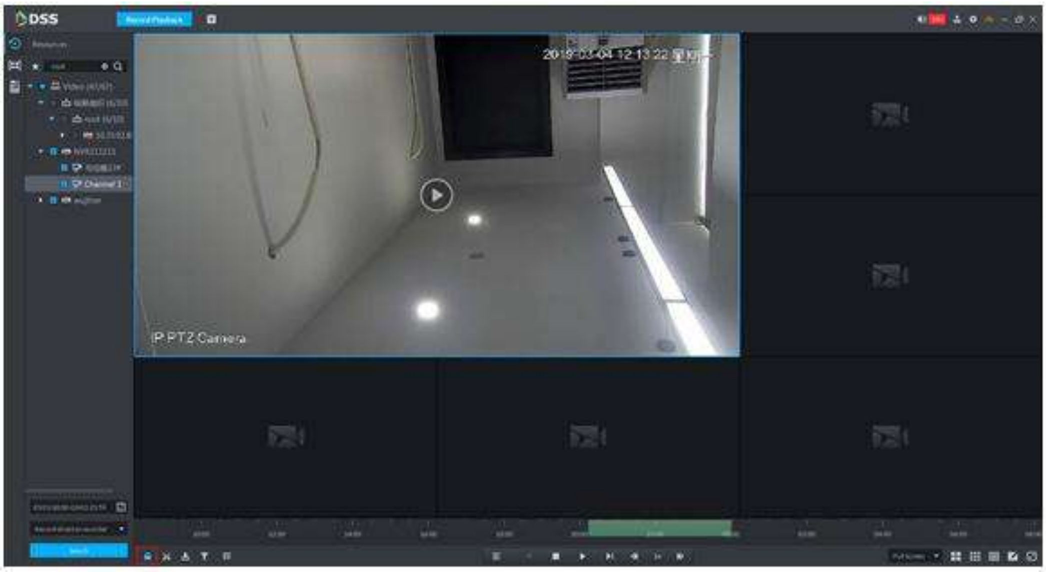
Lock the video stored on the server within some period of specific channel. The locked video will not be overwritten when disk is full.

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

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

Place the mouse to the time progress bar. See Figure 5-67.

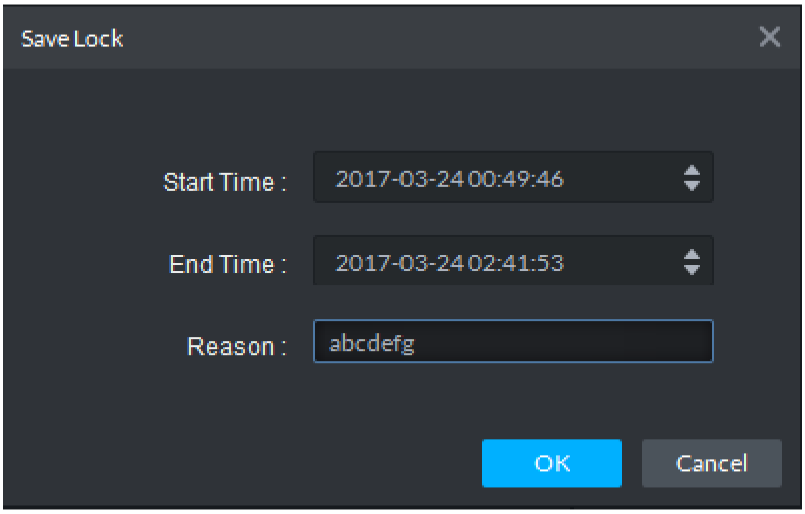
Figure 5-67 Select lock time



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

System pops up **Save Lock** dialogue box. See Figure 5-68.

Figure 5-68 Save lock



Save Lock

Start Time : 2017-03-24 00:49:46

End Time : 2017-03-24 02:41:53

Reason : abcdefg

Step 3 Click **OK**.

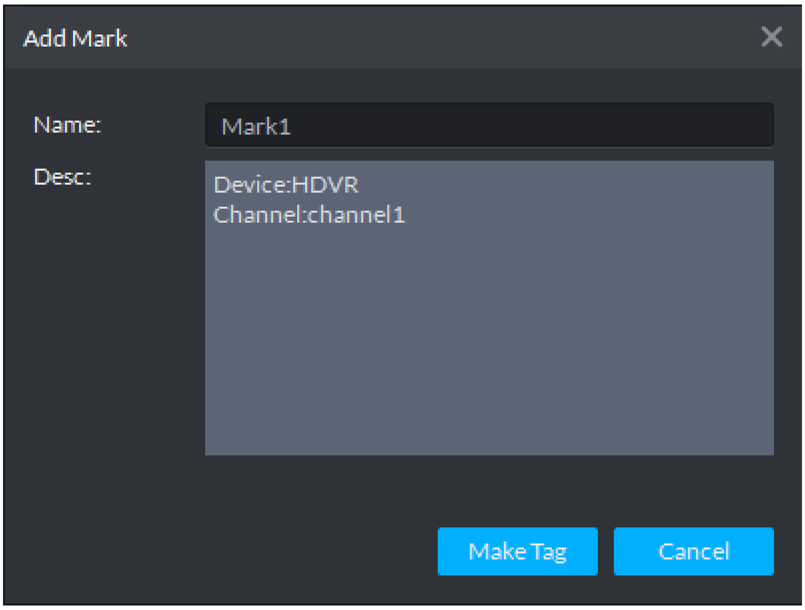
5.4.2.6 Add Mark

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

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

Add Mark interface is displayed. See Figure 5-69.

Figure 5-69



Add Mark

Name: Mark1

Desc: Device:HDVR
Channel:channel1

Step 2 Input **Name** and **Description**, and then click **Make Tag**.

System prompts **Tag Creation Successful**. You can search record via mark in the **Download Center**.

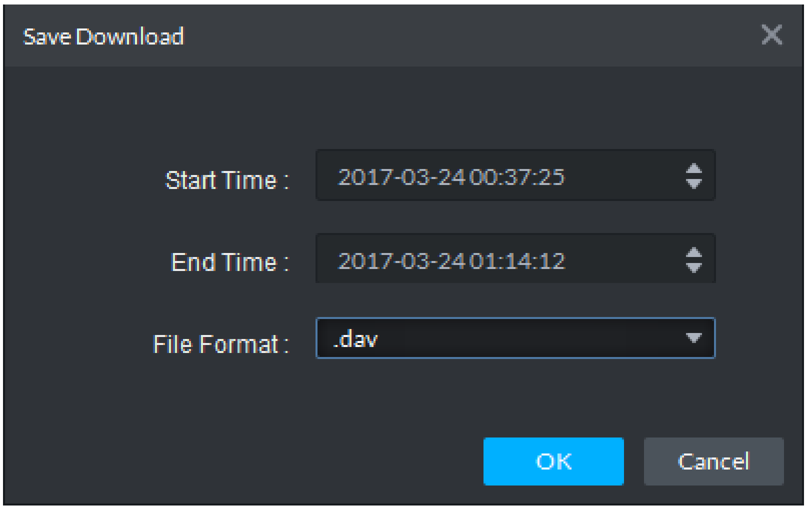
5.4.2.7 Clip Record

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

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

The **Save Download** interface is displayed. See Figure 5-70.

Figure 5-70



Save Download

Start Time : 2017-03-24 00:37:25

End Time : 2017-03-24 01:14:12

File Format : .dav

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

5.4.2.8 Downloading Recording

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

Click at the bottom side of the **Record Playback** interface, and the **Download Center** interface is displayed. For details, see **5.5 Record Download**.

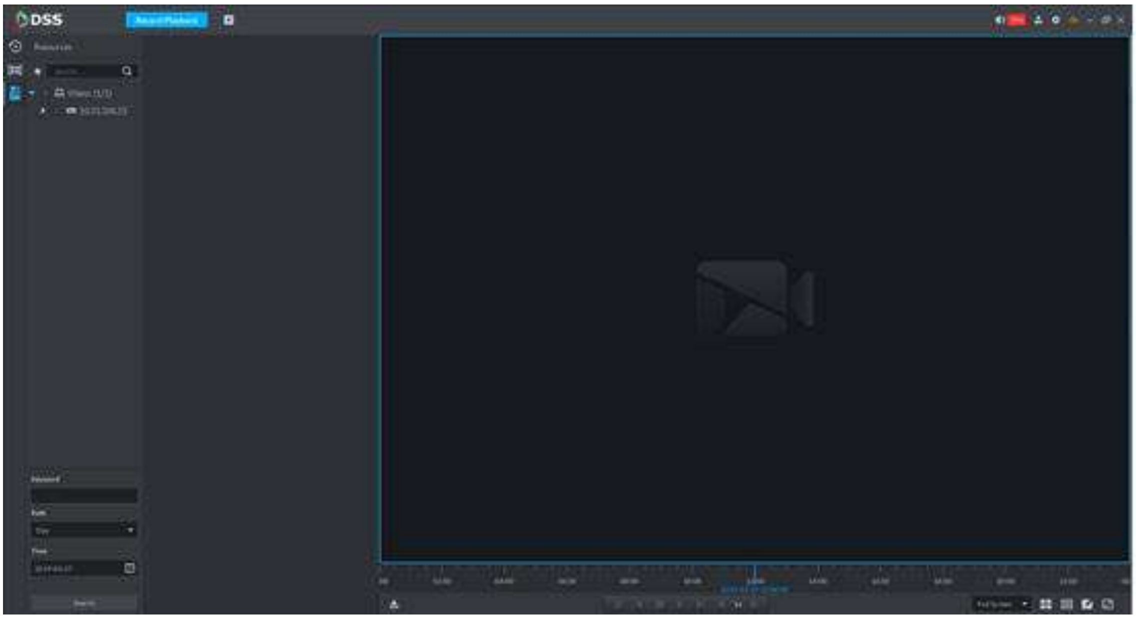
5.4.3 POS Search

Search POS receipt, check related video record. Search the video half an hour before and half an hour after POS receipt is printed, play the video 30s before the receipt is printed.

Step 1 Click on the interface of **Record Playback**.

The system displays the interface of **POS Search**. See Figure 5-71.

Figure 5-71 POS search

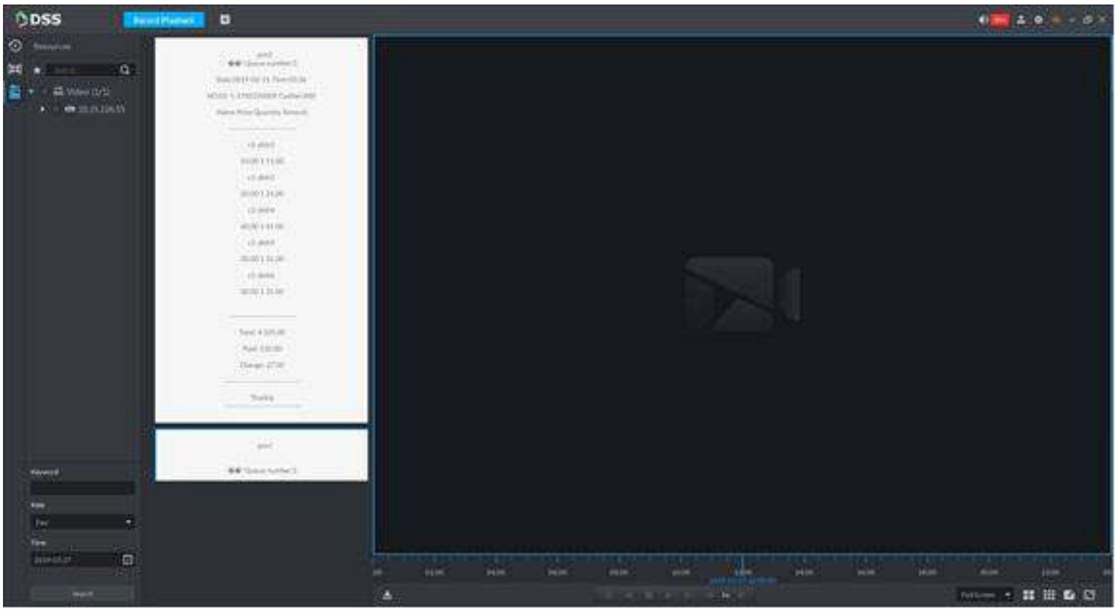


Step 2 Select channel from the device tree.

Step 3 Enter **Keyword**, select **Date** and **Time**, click **Search**.

The system displays search result. See Figure 5-72.

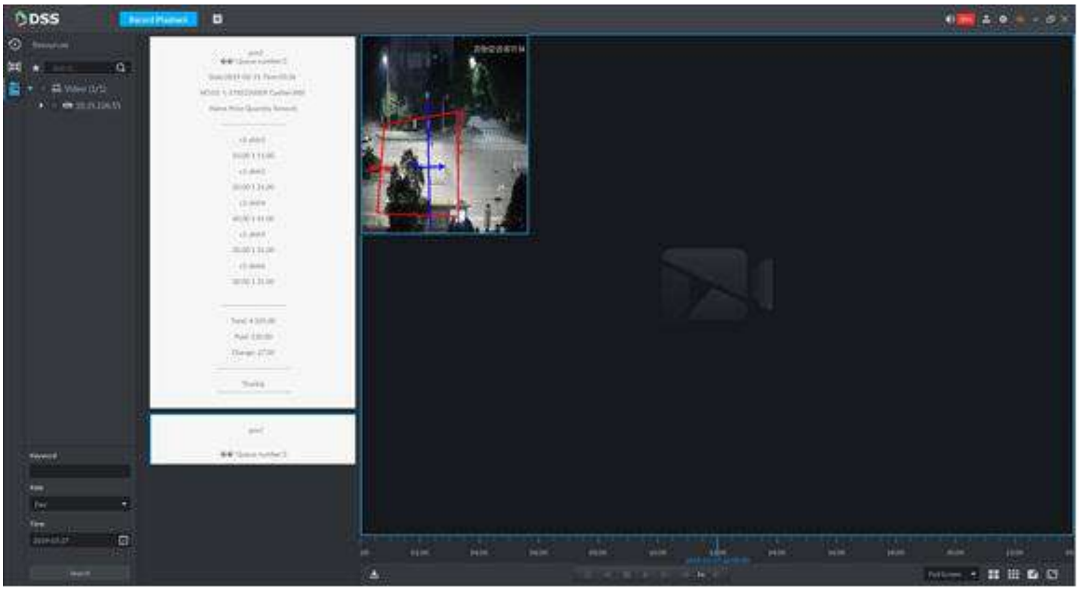
Figure 5-72 POS search result



Step 4 Double click the POS information to replay related video.

The window will play the related video. See Figure 5-73.

Figure 5-73

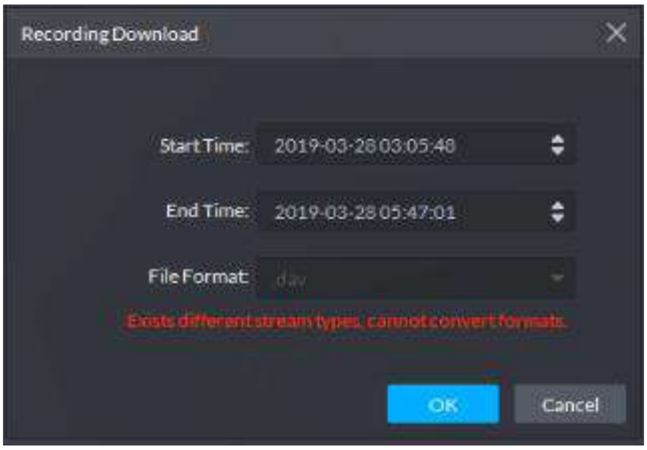


Step 5 Download record.

1) Click on the bottom of the interface.

The system displays the interface of **Record Download**. See Figure 5-74.

Figure 5-74



Recording Download

Start Time: 2019-03-28 03:05:48

End Time: 2019-03-28 05:47:01

File Format: dav

Exists different stream types, cannot convert formats.

2) Confirm start time and end time, click **OK**.

View download details in the **Download Center**; refer to "5.5 Record Download" for more details.

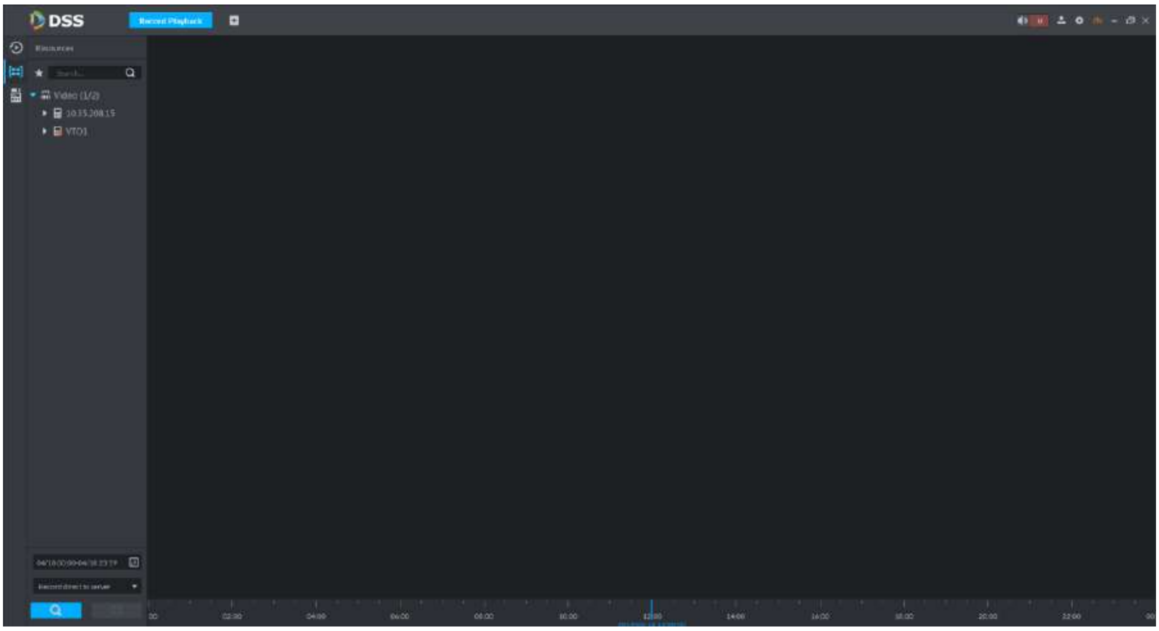
5.4.4 Search Thumbnail

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

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

The system displays the interface. See Figure 5-75.

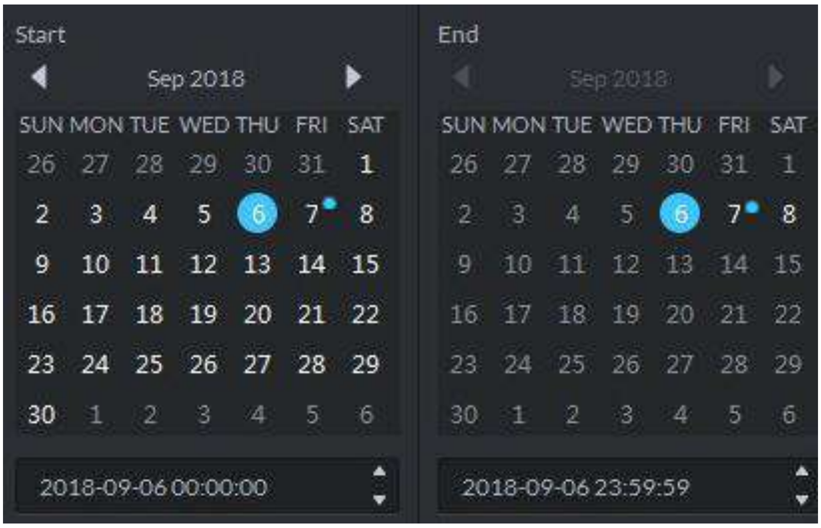
Figure 5-75 Thumbnail



Step 2 In the organization tree, select a video channel and then set search period and record position. Click 🔍.

There is a blue dot at the date top left corner if the channel has a record. See Figure 5-76.

Figure 5-76 Search period



Start

Sep 2018

SUN	MON	TUE	WED	THU	FRI	SAT
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

2018-09-06 00:00:00

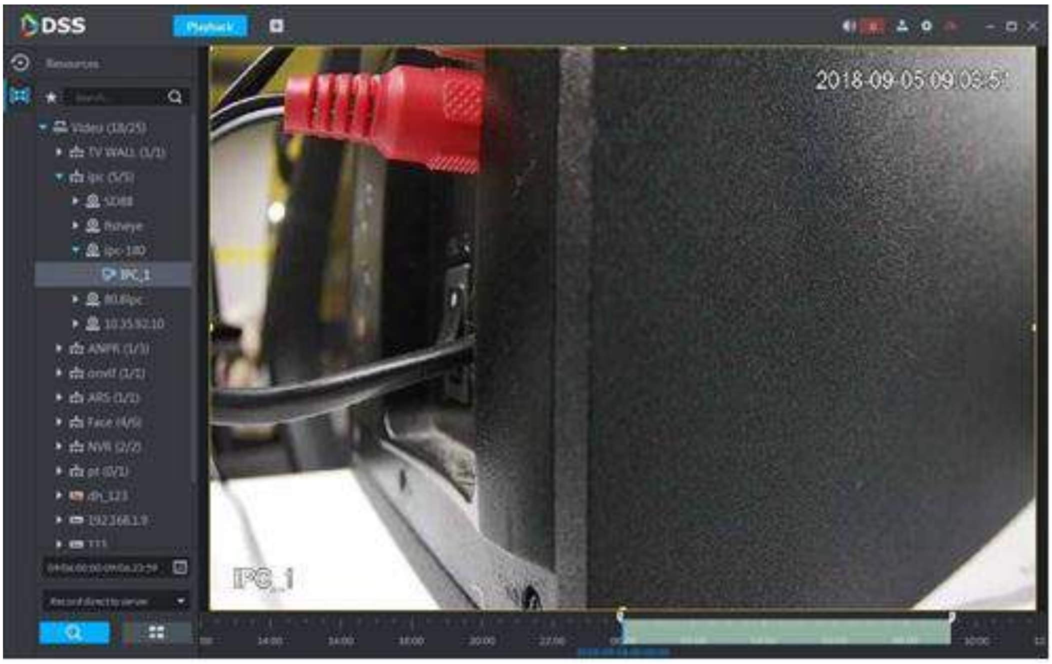
End

Sep 2018

SUN	MON	TUE	WED	THU	FRI	SAT
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

2018-09-06 23:59:59

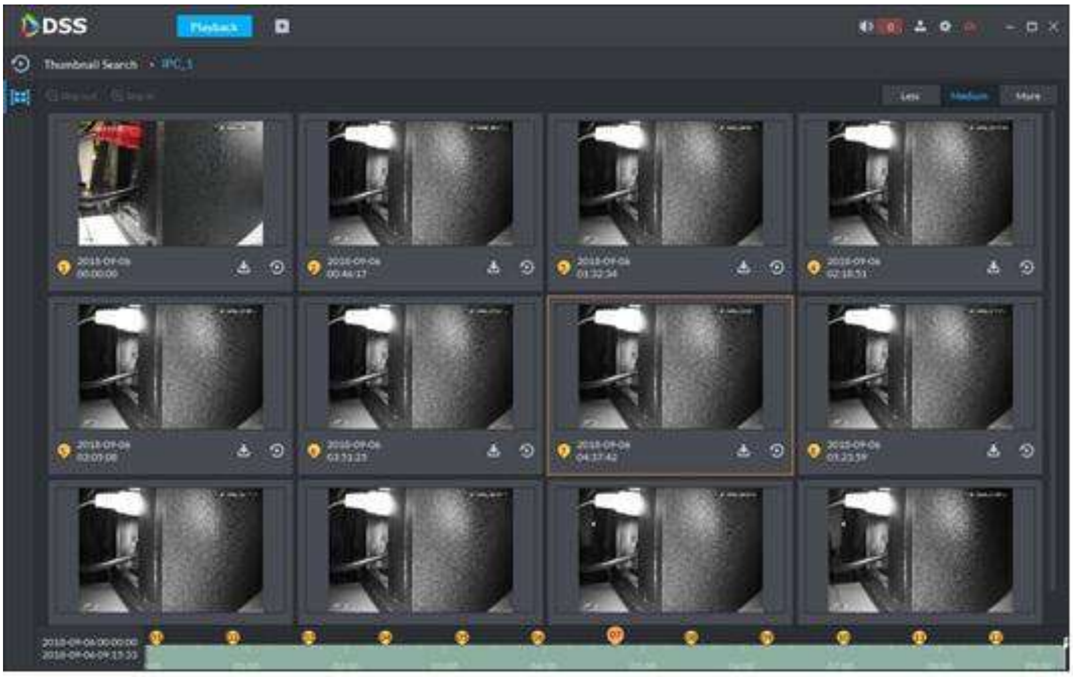
Figure 5-77 Search result



Step 3 Drag the yellow frame on the right to set thumbnail range. Click ⊞.

System displays the video of current range. See Figure 5-78.

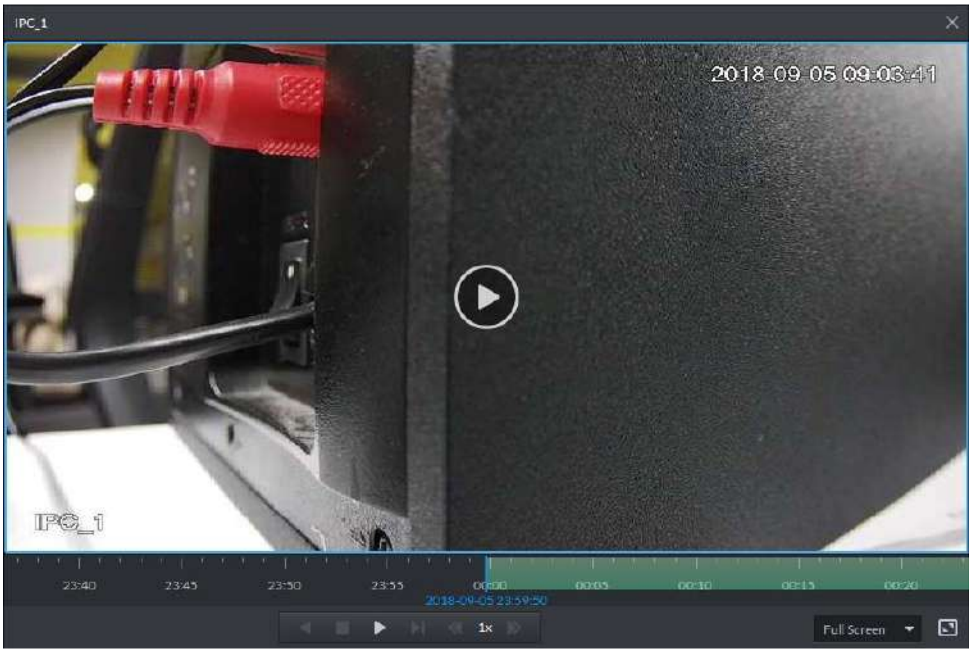
Figure 5-78 Thumbnail search



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

Step 4 Click the ⟲ at the bottom right corner of the thumbnail, you can view the corresponding video related to the thumbnail. See Figure 5-79.

Figure 5-79 Playback record

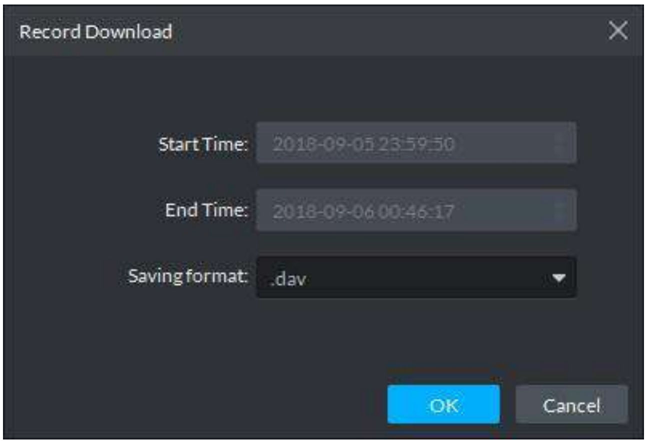


Step 5 Download Record

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

1) Click at the right corner of the thumbnail, system downloads the record between current image and the next image. See Figure 5-80.

Figure 5-80 Record download



Record Download

Start Time: 2018-09-05 23:59:50

End Time: 2018-09-06 00:46:17

Saving format: .dav

2) Select file format and then click OK.
Go to the Download center to view download detailed information. Refer to "5.5 Record Download" for detailed information.

5.5 Record Download

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

5.5.1 Preparation

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

5.5.2 Timeline

Download video within some period.

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

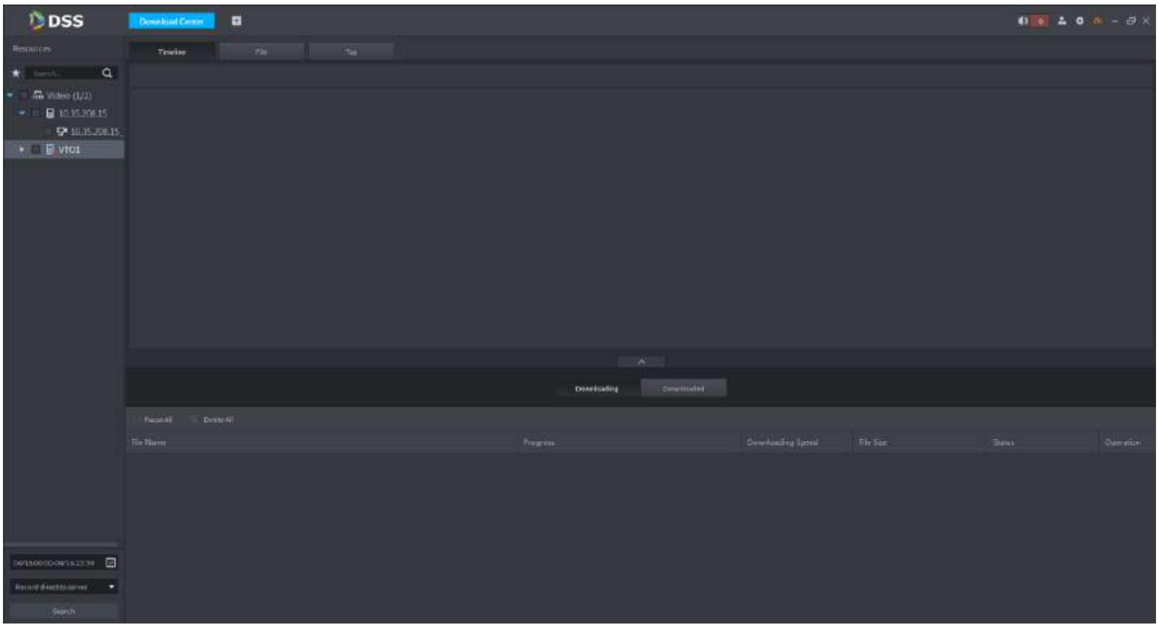
Step 1 Go to D**ownload Cente**r.

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 5-81.

Figure 5-81 Download

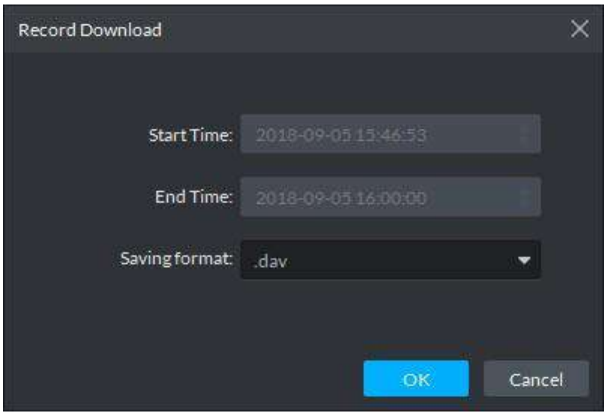


Step 2 Click Timeline.

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 5-82.

Figure 5-82 Record download



Record Download

Start Time: 2018-09-05 15:46:53

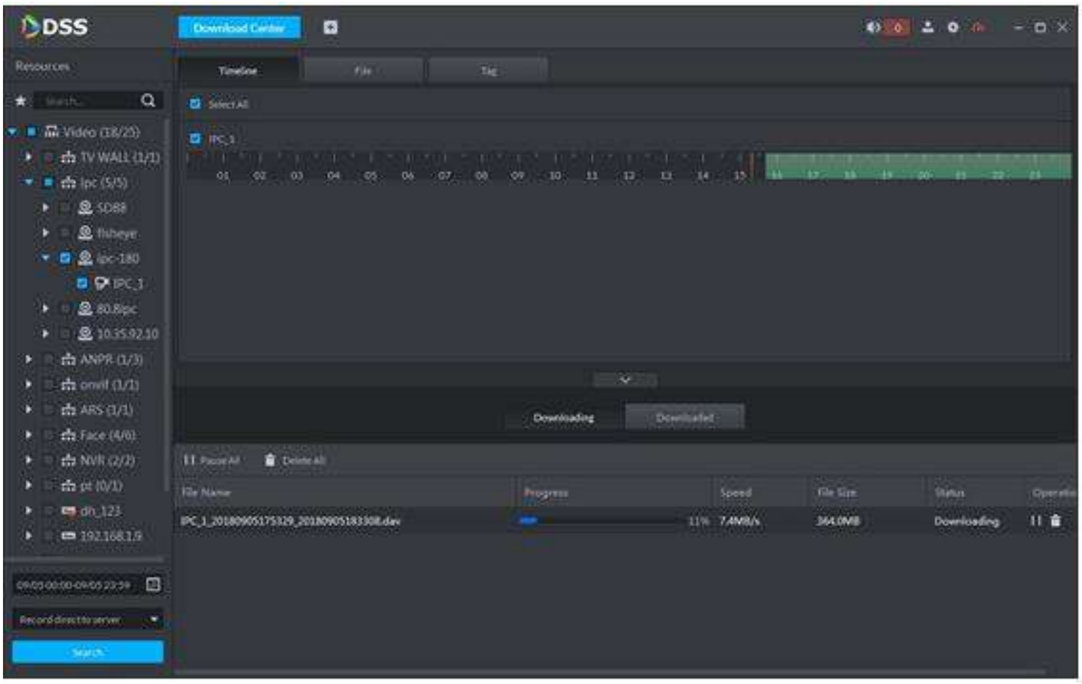
End Time: 2018-09-05 16:00:00

Saving format: .dav

Step 5 Set file format and then click OK.

You can view the download process at the bottom of the interface. See Figure 5-83.

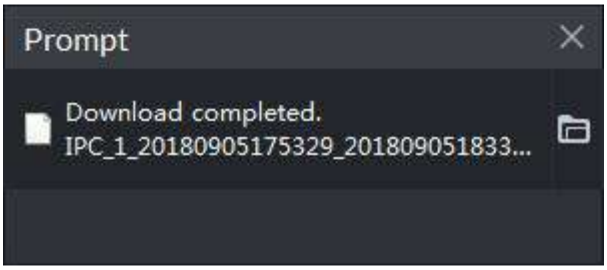
Figure 5-83 Timeline



File Name	Progress	Speed	File Size	Status	Operation
IPC_1_20180905175329_20180905183308.dav	11%	7.4MB/s	364.0MB	Downloading	

System pops up the following dialogue box once the download is complete. See Figure 5-84.

Figure 5-84 Download completed



Prompt

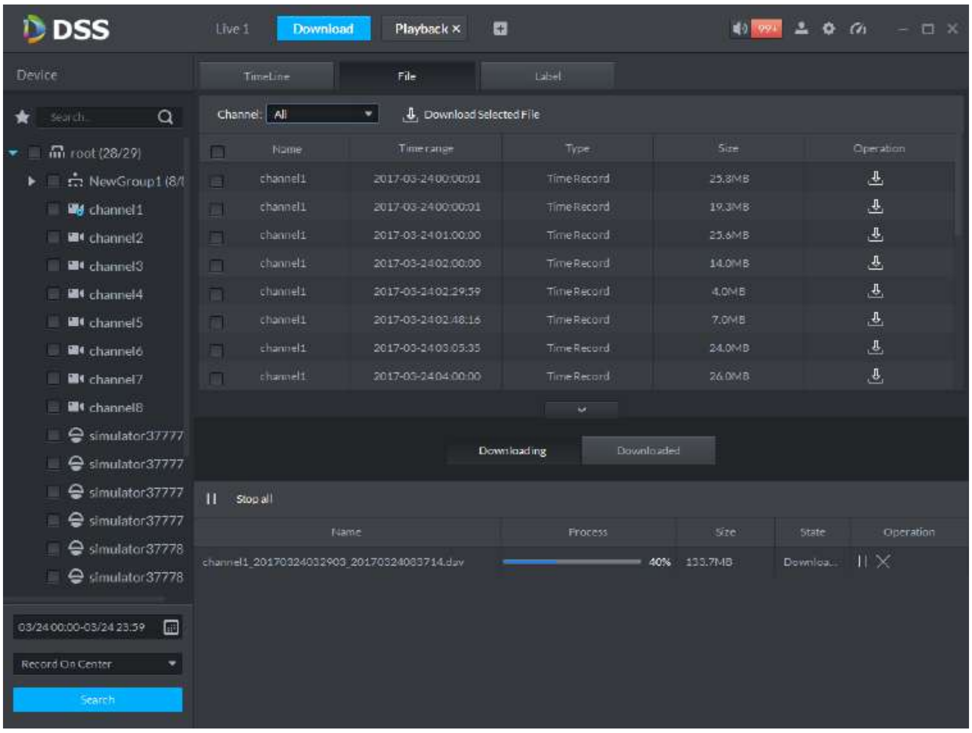
Download completed.
IPC_1_20180905175329_201809051833...

5.5.3 File List

Step 1 On Download interface, click File tab.

System displays record files. See Figure 5-85.

Figure 5-85 File



Channel: All

□	Name	Time range	Type	Size	Operation
□	channel1	2017-03-24 00:00:01	Time Record	25.8MB	⇩
□	channel1	2017-03-24 00:00:01	Time Record	19.3MB	⇩
□	channel1	2017-03-24 01:00:00	Time Record	25.6MB	⇩
□	channel1	2017-03-24 02:00:00	Time Record	14.0MB	⇩
□	channel1	2017-03-24 02:29:59	Time Record	4.0MB	⇩
□	channel1	2017-03-24 02:48:16	Time Record	7.0MB	⇩
□	channel1	2017-03-24 03:05:35	Time Record	24.0MB	⇩
□	channel1	2017-03-24 04:00:00	Time Record	26.0MB	⇩

Name	Process	Size	State	Operation
channel1_20170324032903_20170324083714.dav	40%	133.7MB	Downloa...	ǁ ×

03/24 00:00-03/24 23:59

Record On Center

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

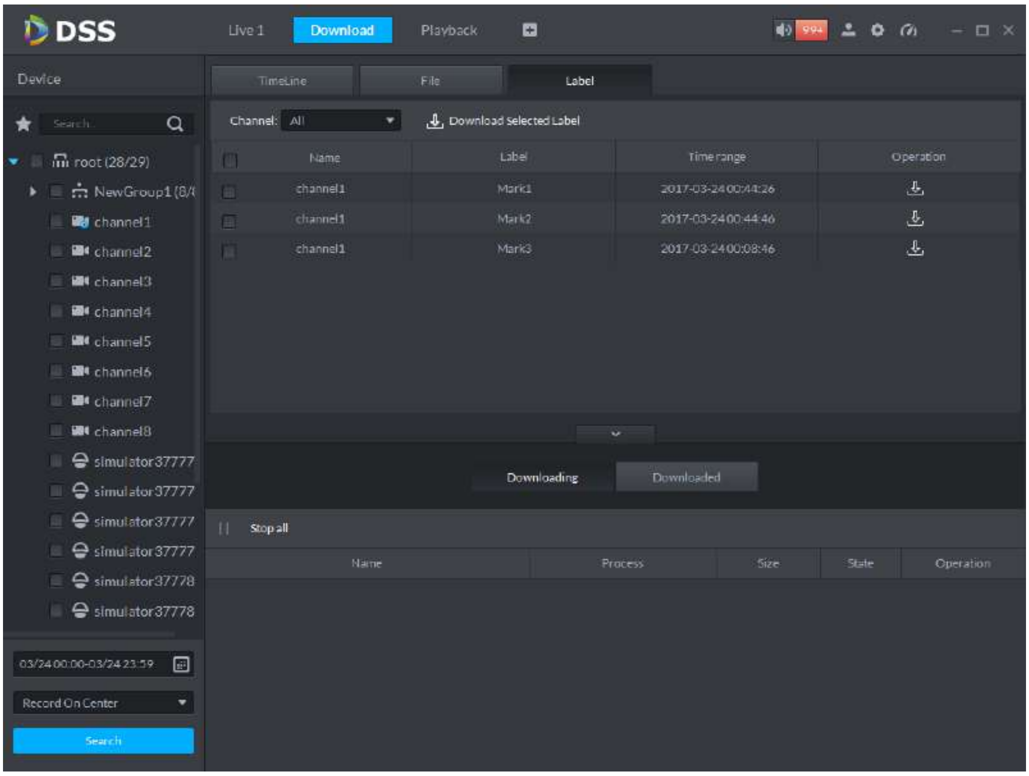
System displays download process at the bottom of the interface. System pops up dialogue box once the download is complete.

5.5.4 Label

Step 1 On Download interface click Label tab.

System displays marked record files. See Figure 5-86.

Figure 5-86 Label



Channel: All

03/24 00:00:00-03/24 23:59

Record On Center

	Name	Label	Time range	Operation
□	channel1	Mark1	2017-03-24 00:44:26	⤓
□	channel1	Mark2	2017-03-24 00:44:46	⤓
□	channel1	Mark3	2017-03-24 00:08:46	⤓

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

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

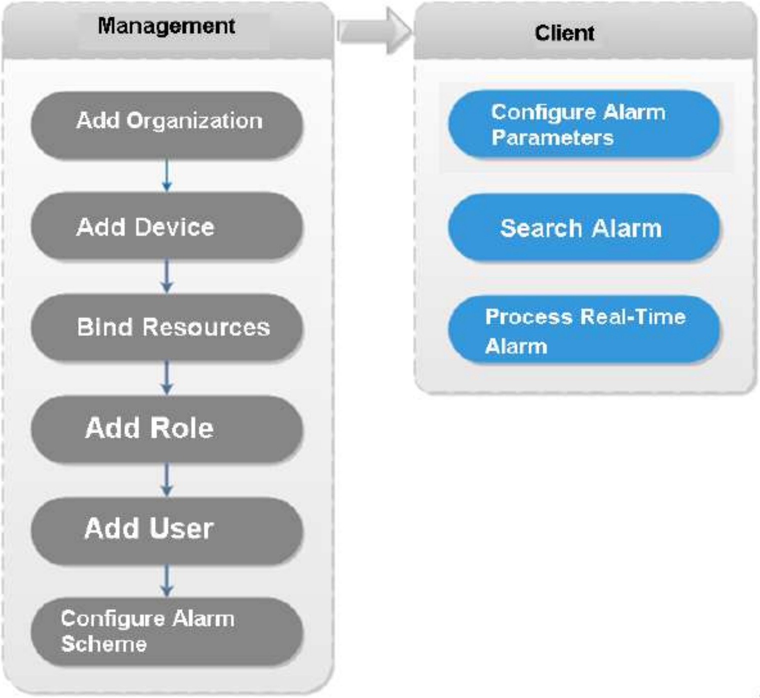
5.6 Event Center

5.6.1 Preparations

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

Refer to Figure 5-87 for event management flows.

Figure 5-87 Event center flow

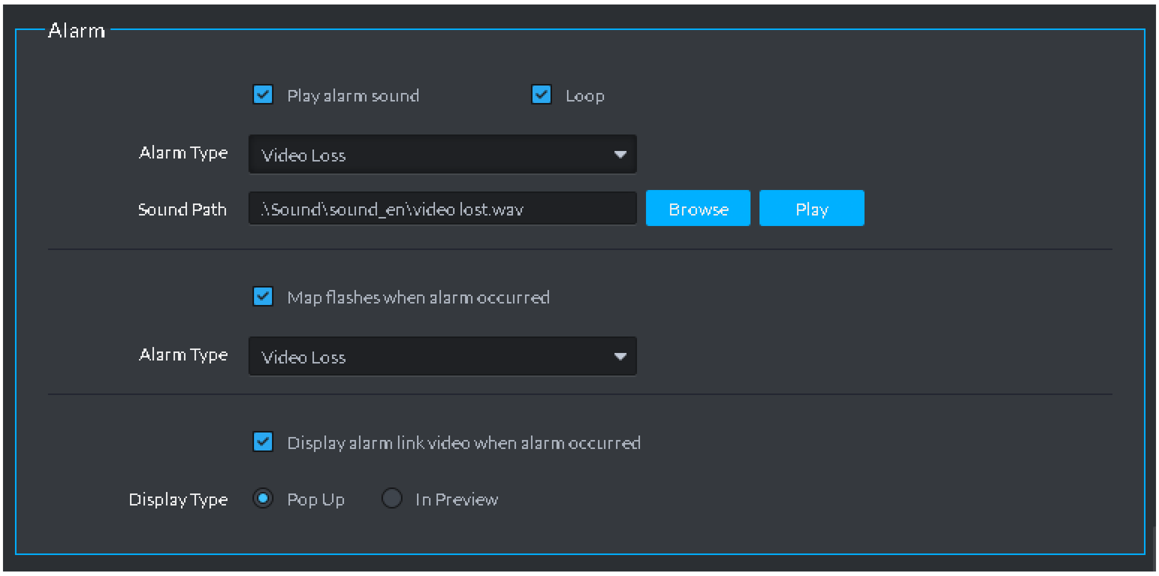


5.6.2 Configuring Alarm Parameters

Set alarm mode on the client. It includes alarm audio, alarm flashing on the map or not.

Step 1 Click ⚙ at the top right corner, from General > Alarm, the interface is shown as below. See Figure 5-88.

Figure 5-88 Alarm



Alarm

☑ Play alarm sound ☑ Loop

Alarm Type: Video Loss

Sound Path: .\Sound\sound_en\video lost.wav

☑ Map flashes when alarm occurred

Alarm Type: Video Loss

☑ Display alarm link video when alarm occurred

Display Type: ● Pop Up ○ In Preview

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

Refer to Table 5-26 for detailed information.

Table 5-26 Alarm parameter description

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

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

5.6.3 Searching and then Processing Real-Time Alarm

📖

The customized alarm supports modification and deletion.

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

5.6.3.1 Processing Real-Time Alarm

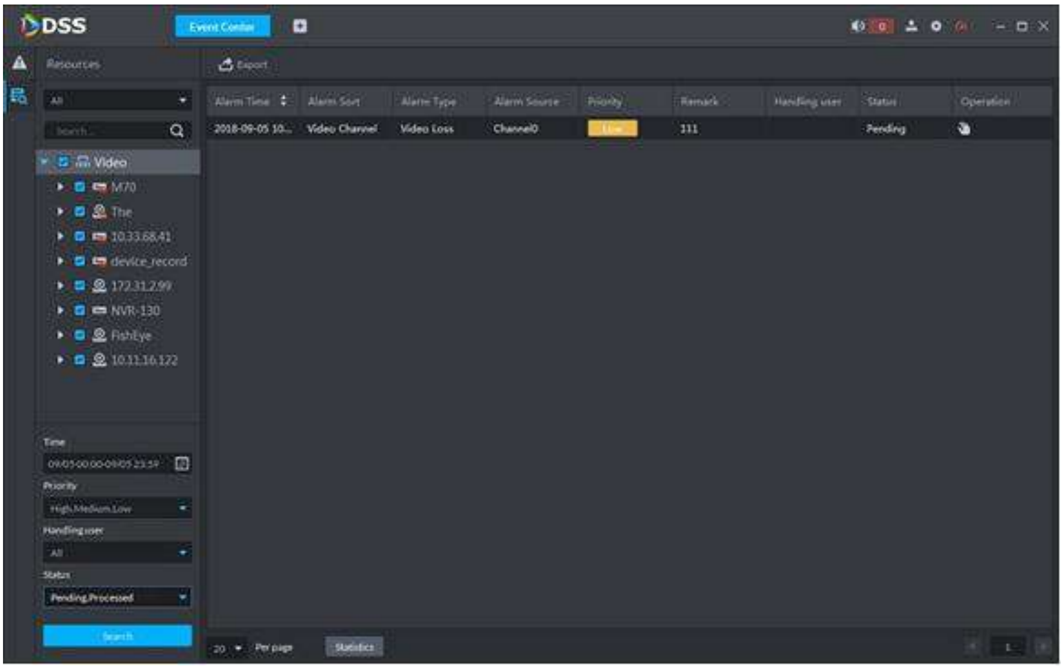
Step 1 Click+, on the **New Tab** interface select **Event Center**.

Enter Event center interface.

Step 2 Click ⚠ on the left navigation bar.

System displays alarm processing interface. See Figure 5-89.

Figure 5-89 Real-time alarm



Alarm Time	Alarm Sort	Alarm Type	Alarm Source	Priority	Remark	Handling user	Status	Operation
2018-09-05 10...	Video Channel	Video Loss	Channel0	Low	111		Pending	✋

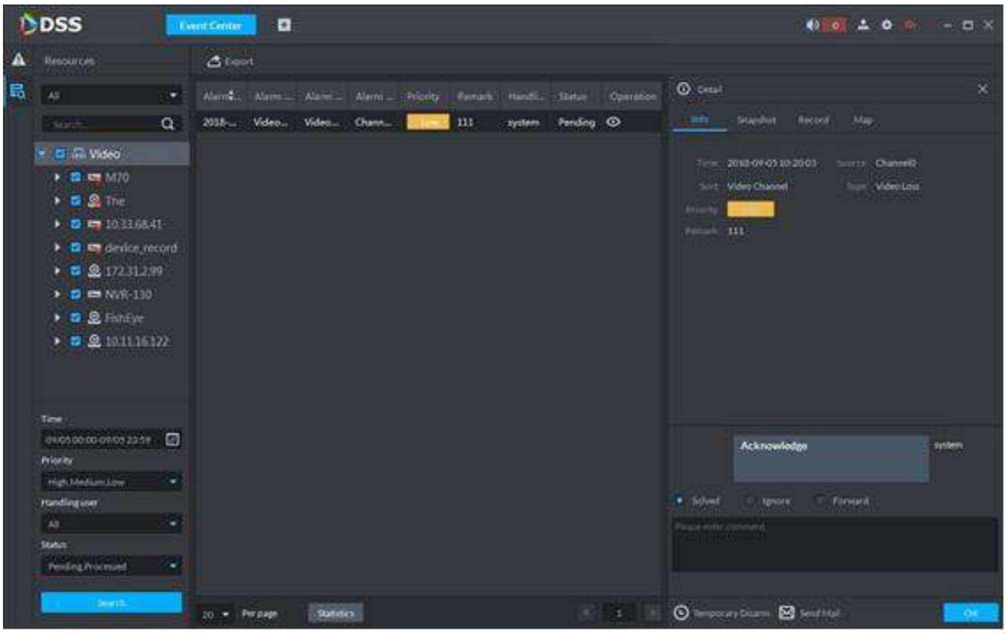
System refreshes to display real-time alarm by default. Click Pause Refresh to pause refresh, click Refresh to continue refresh.

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 5-90.

Figure 5-90 Process alarm



Alarm...	Alarm ...	Alarm ...	Alarm ...	Priority	Remark	Handl...	Status	Operation
2018-...	Video...	Video...	Chann...	Low	111	system	Pending	👁

Time: 2018-09-05 10:20:03 Source: Channel0
Sort: Video Channel Type: Video Loss
Priority: Low
Remark: 111

Acknowledge system

● Solved ○ Ignore ○ Forward

Please enter comment

Step 5 Click Message, Snapshot, Record, and Map tag, view corresponding alarm information.

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

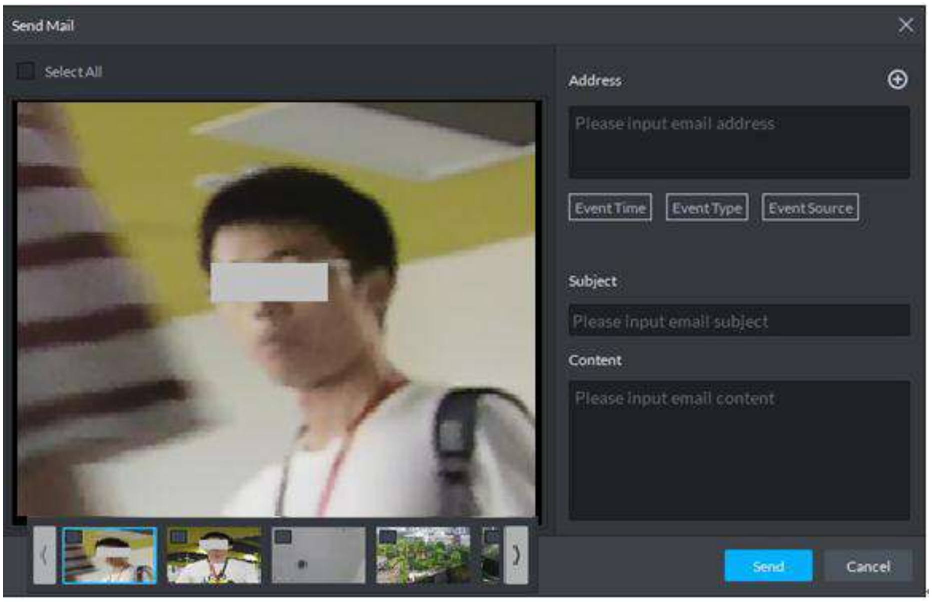
When you are selecting **Forward**, you can select other user on the dialogue box. Send current event to specified user to process.

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 5-91.

Figure 5-91 Send email



5.6.3.2 Searching Alarm Record

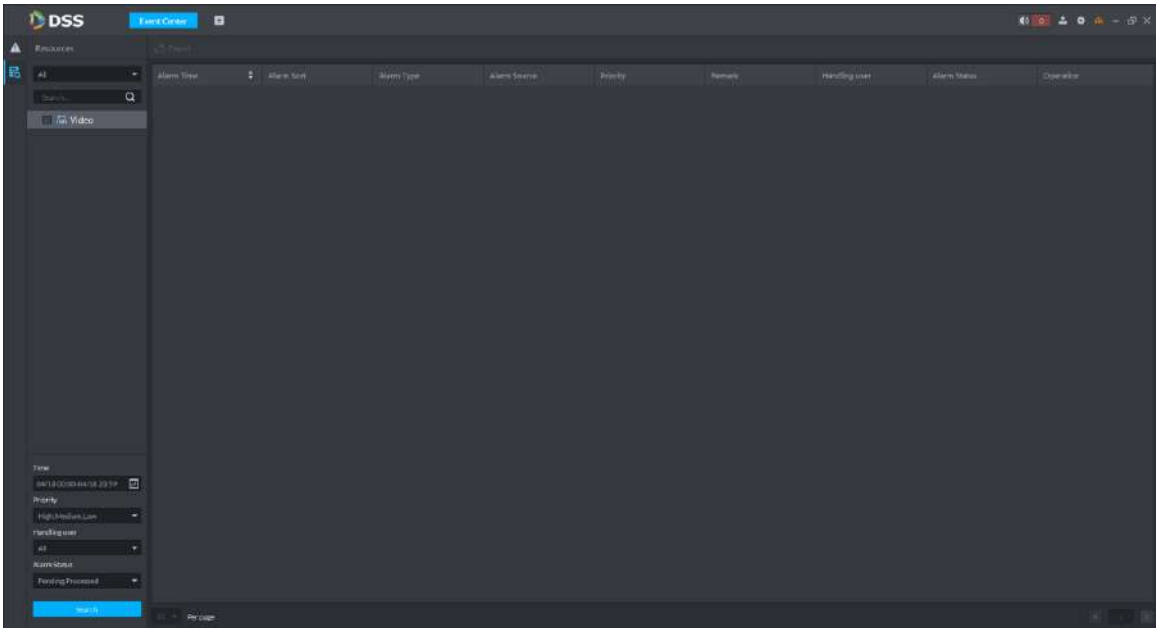
Step 1 Click+, on the **New Tab** interface select **Event center**.

Enter Event center interface.

Step 2 Click on the left navigation bar.

System displays search interface. See Figure 5-92.

Figure 5-92 Search alarm record

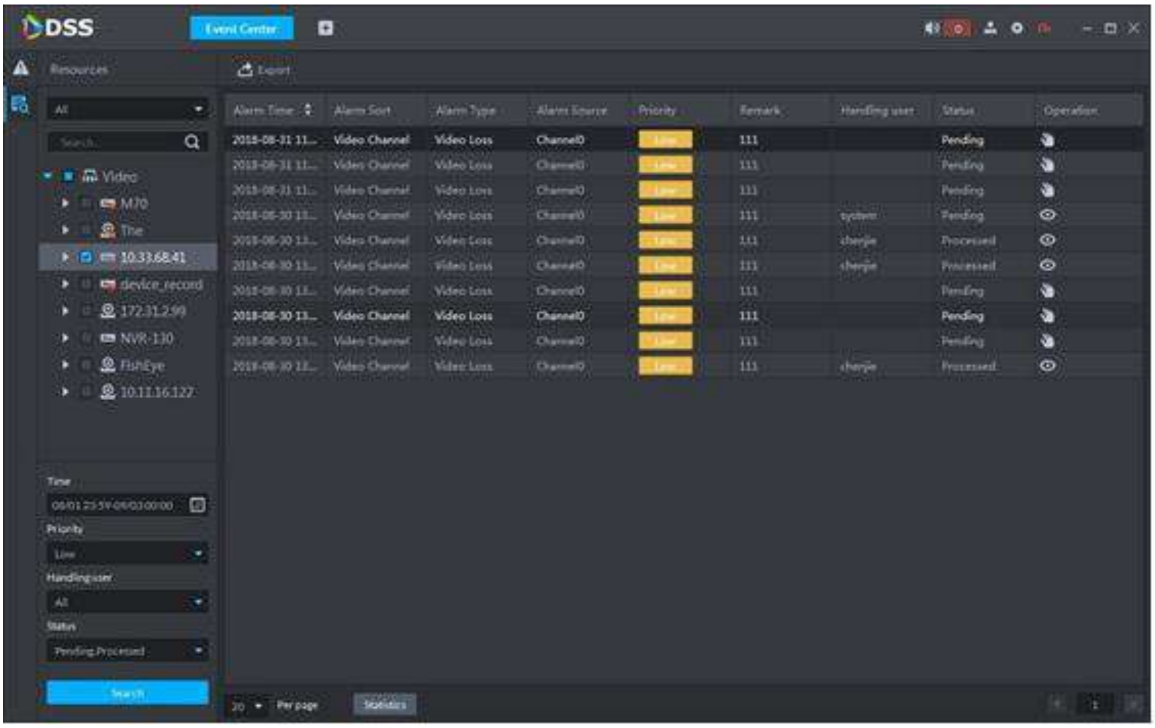


Step 3 Select device channel, search time, alarm level, user or alarm status.

Step 4 Click Search.

System displays corresponding alarm information. See Figure 5-93.

Figure 5-93



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

Operations

- Select amount on per page, it is to set displayed alarm message amount each time.
- Click Statistics, it is to display the total alarm message amount of corresponding device.
- Click Export, it is to export device alarm message.

- Click ✋ to claim alarm, click 👁 to process alarm. Refer to "5.6.3.1 Processing Real-Time Alarm" for detailed information.

5.7 Video Wall

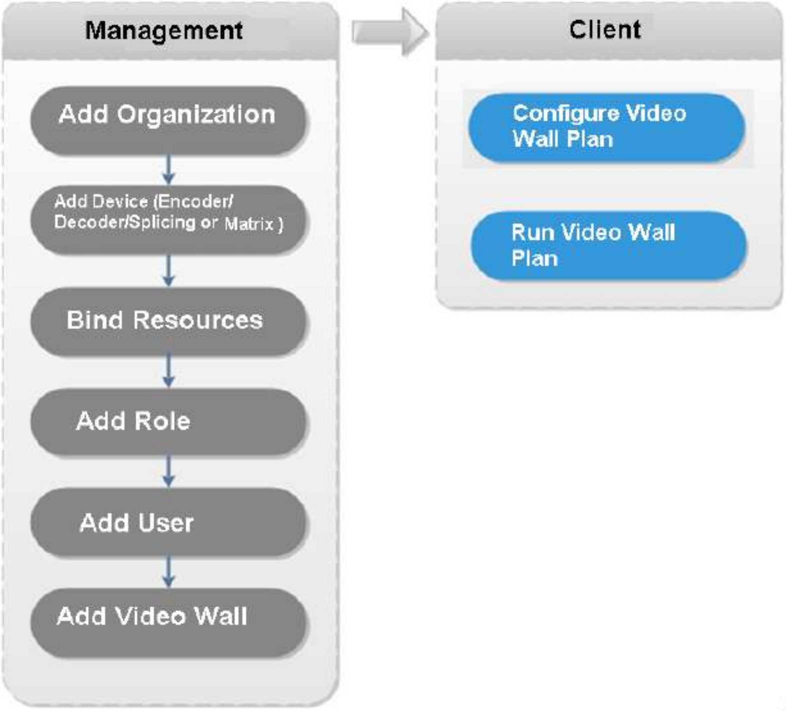
5.7.1 Preparations

View the video on the video wall on the client. You need to complete the following settings.

- Adding corresponding device: It includes decoder, encoder or matrix device. Refer to "4.5 Adding Device" for detailed information.
- Refer to "4.9 Adding Video Wall" to add the video wall first.

Refer to Figure 5-94 for video wall flows.

Figure 5-94 Video wall flow



5.7.2 Output to the Wall

Step 1 Click +, on the **New Tab** interface select **Video Wall**, system displays **Video Wall** interface. See Figure 5-95.

Figure 5-95

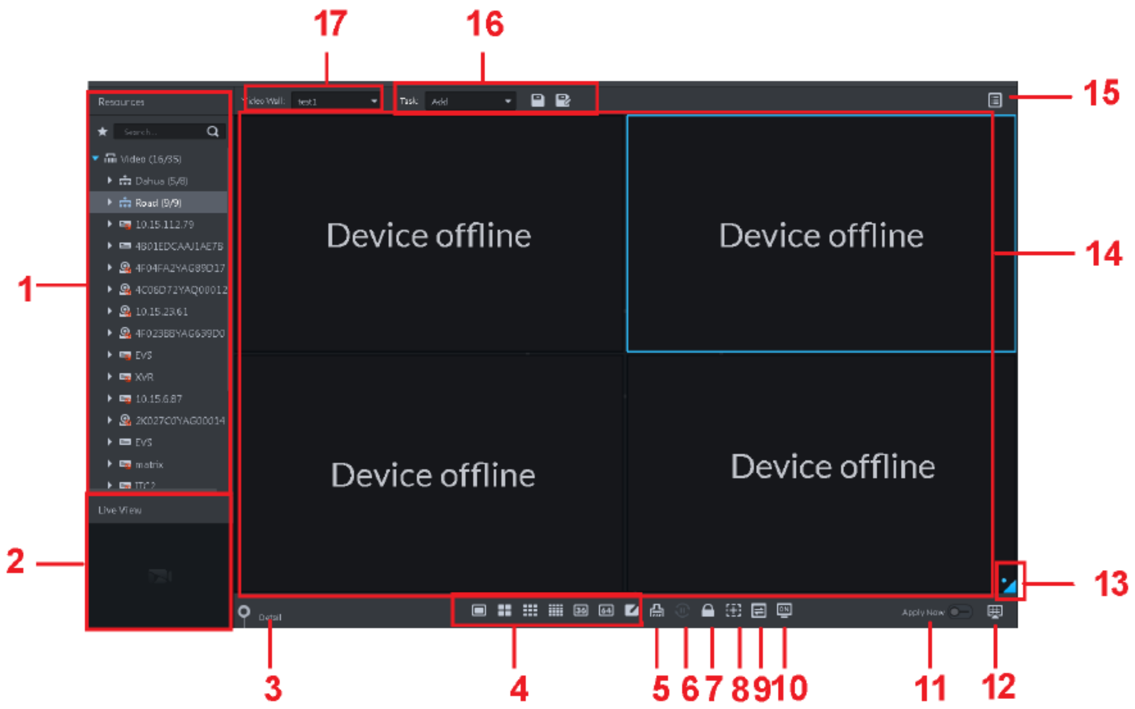

17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
Resources
Search...
Video (16/35)
Dahua (5/8)
Road (9/9)
10.15.112.79
4B01EDCAAJ1AE7B
4F04FA2YAG89D17
4C06D72YAQ00012
10.15.23.61
4F023BBYAG639D0
EVS
XVR
10.15.6.87
2K027C0YAG00014
EVS
matrix
ITC2
Live View
Video Wall:
test1
Task:
Add
Device offline
Device offline
Device offline
Device offline
Detail
Apply Now

Table 5-27 Video wall description

SN	Name	Function
1	Device tree	From Local config> General, if you enable Show device node, device tree displays all channels of current device. If you cancel the box, system display all channels of all device. Click ★ to view the channels on the favorites folder. Search is supported by input device name or channel name in Search.. here.
2	Preview	View channel video.
3	Detailed information	Click to view the screen, window, and channel bound information. ● Click ▶ to preview the video at the bottom left pane. It is to check current channel is what you want or not. ● Click ↑ ↓ to adjust sequence. ● Click 🗑 to delete the video channel that adds to current window. ● Click Stay time column or click✎, it is to modify signal interval on current channel when tour. ● Click Stream column or✎, it is to modify video bit stream.
4	Window split	Set window split mode.
5	Clear	Clear information on all screens.
6	Start/stop all tours	Start or stop all tours.
7	Lock window	Click to lock the window. You cannot operate on the locked window.
8	Add box	You can click to add a box, and click again to cancel box.
9	Back display	View current layout
10	Screen On/Off	In Screen On mode, the system will automatically display the video after configuring the tasks.
9	Apply now	If you enable the function, system automatically outputs the video to the wall after you set the task.
10	Decode to wall	Click to manually output the video to the wall.
11	Eagle eye	View current video wall layout.
12	Video wall	Video wall area.
13	Video wall task	Schedule task and tour task. Refer to 5.7.3 Video Wall Plan for detailed information.
14	Task managem ent pane	Add, save delete task.

SN	Name	Function
15	Video wall selection	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**

- Input device name or channel name to search.
- One window can bind several video channels at the same time.
- You can bind video source mode in local config, bind mode includes tour, tile and query. Refer to "5.2 Local Configuration" for more details**.**

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.

- Stream type can be self-adaptive according to window splits when displaying video on wall. Refer to "5.2 Local Configuration" for more details.
- Right click on video window and then you can operate the same way as live. Refer to "5.3.2.2 Right–Click Shortcut Menu"

5.7.3 Video Wall Plan

5.7.3.1 Configuring Schedule plan

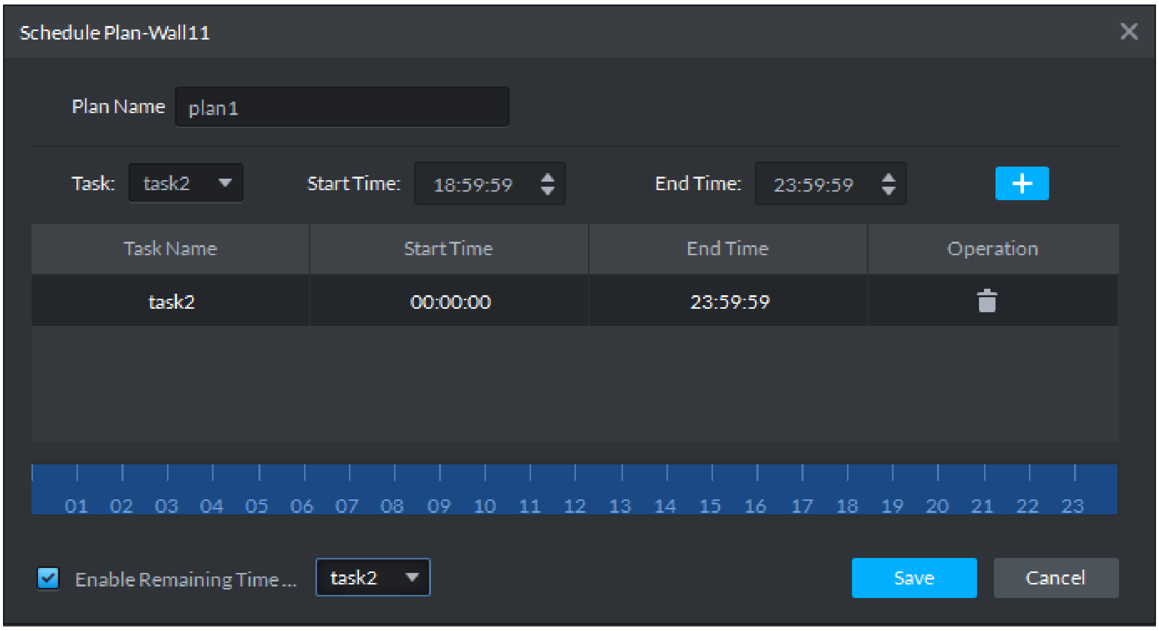
After set schedule plan, you can play video file on the video wall at the specified time.

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

Step 2 Select.

Enter Schedule plan interface. See Figure 5-96.

Figure 5-96 Schedule plan



Schedule Plan-Wall11

Plan Name: plan1

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

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

☑ Enable Remaining Time... task2

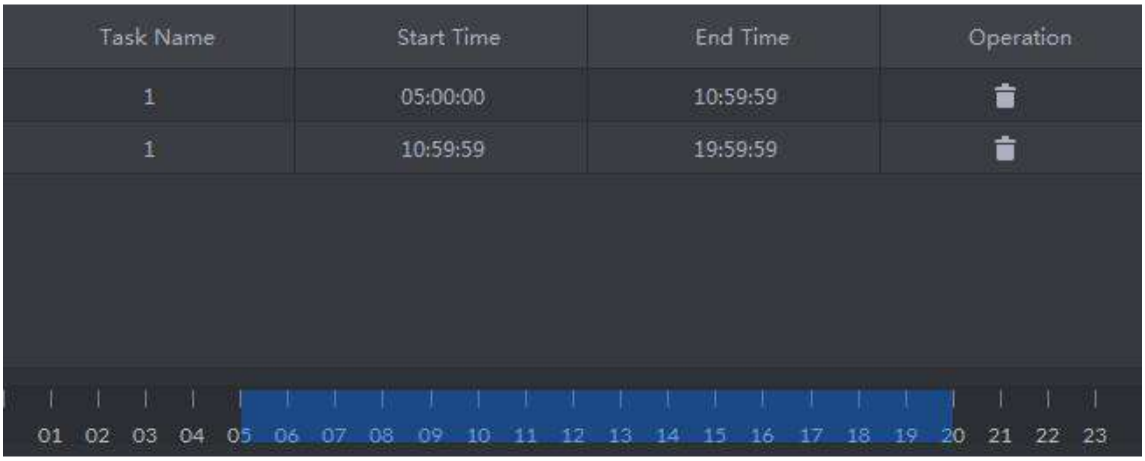
Step 3 Input the plan name.

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 5-97.

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 5-97 Plan info and timeline



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

Step 5 Click Save

Enter Video wall interface.

Step 6 Click to start the plan.

Operations

- Modify plan: Click ⚙ of the corresponding plan, and then modify plan.

- Delete plan: Click 🗑 of the corresponding plan and then delete the plan.

5.7.3.2 Configuring Tour Plan

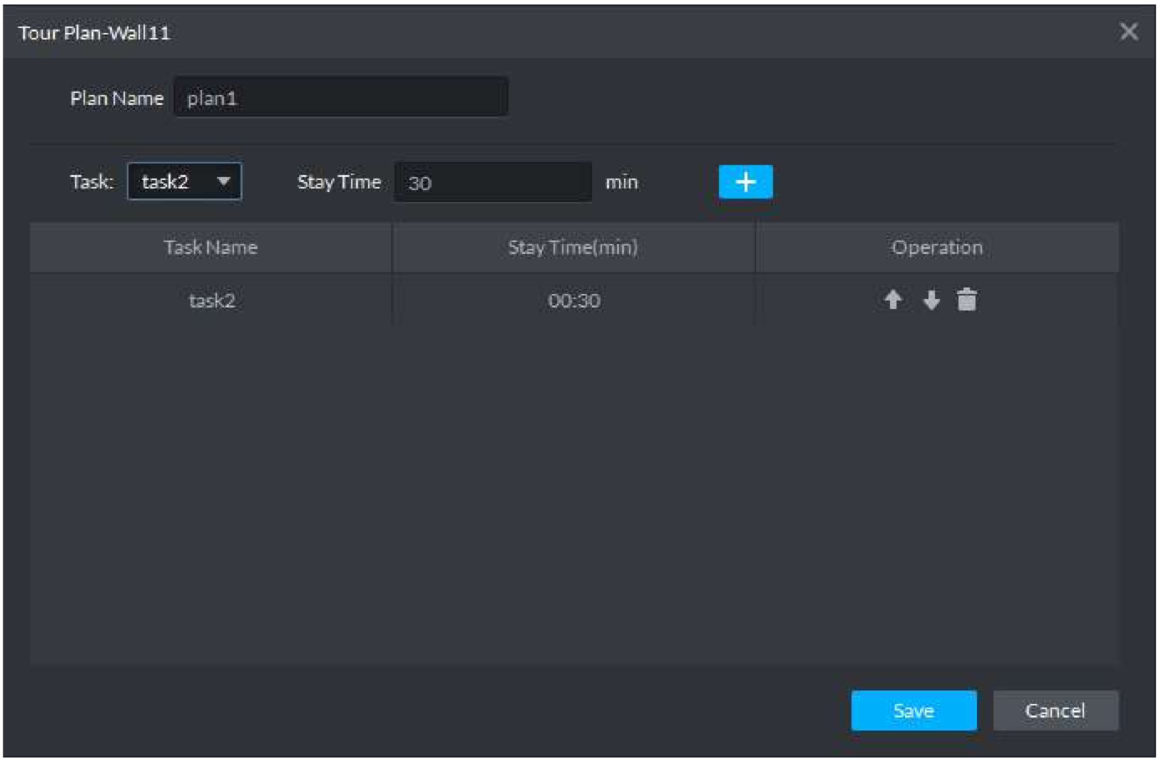
After setting tour plan, you can output several plans to the TV wall.

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

Step 2 Click ⏱.

Enter Tour plan interface. See Figure 5-98.

Figure 5-98 Tour plan



Tour Plan-Wall11

Plan Name: plan1

Task: task2 Stay Time: 30 min

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

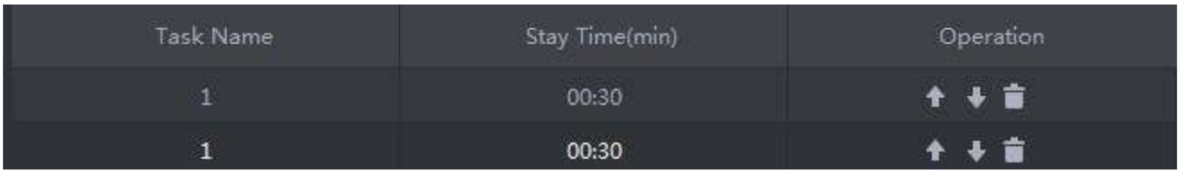
Step 3 Input task name.

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

The list displays tour information. See Figure 5-99.

Click ↑ ↓ to adjust task sequence, click 🗑 to delete task.

Figure 5-99 Tour info



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, modify plan.
- Delete plan: Click 🗑 of the corresponding plan, delete the plan.

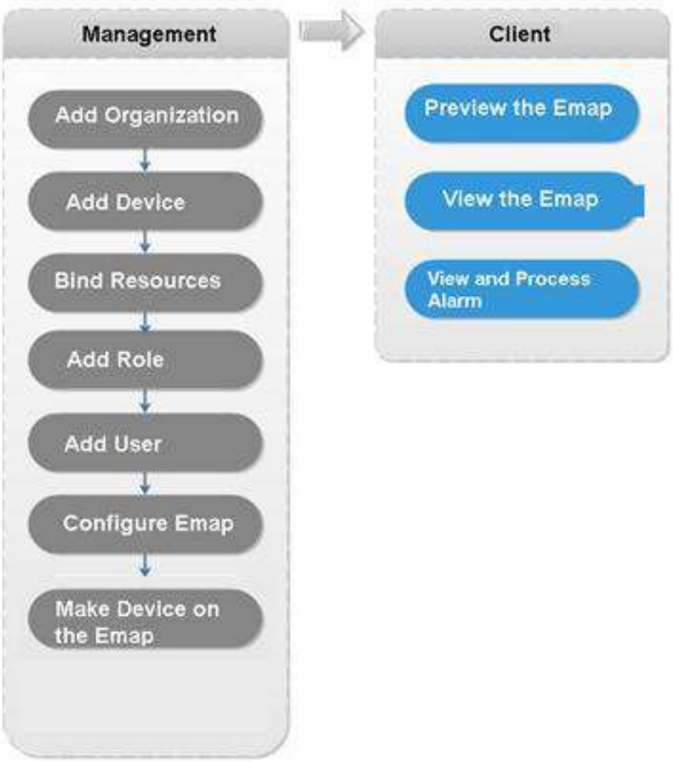
5.8 Emap

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

5.8.1 Preparations

Refer to "4.8 Configuring Map" to add emap and hot zone on the platform manager and mark the device on the map. Refer to Figure 5-100 for flows information.

Figure 5-100 Emap flow

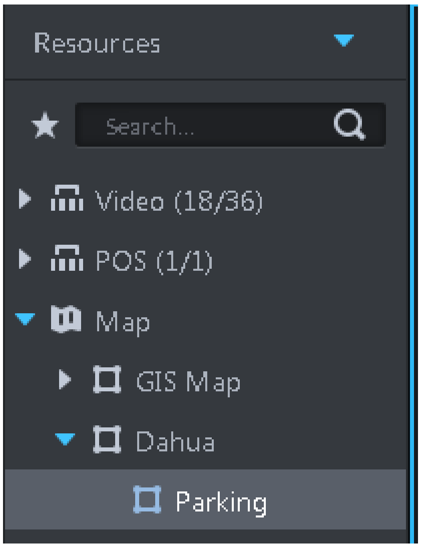


5.8.2 Open Emap on the Real-Time Preview

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 5-101.

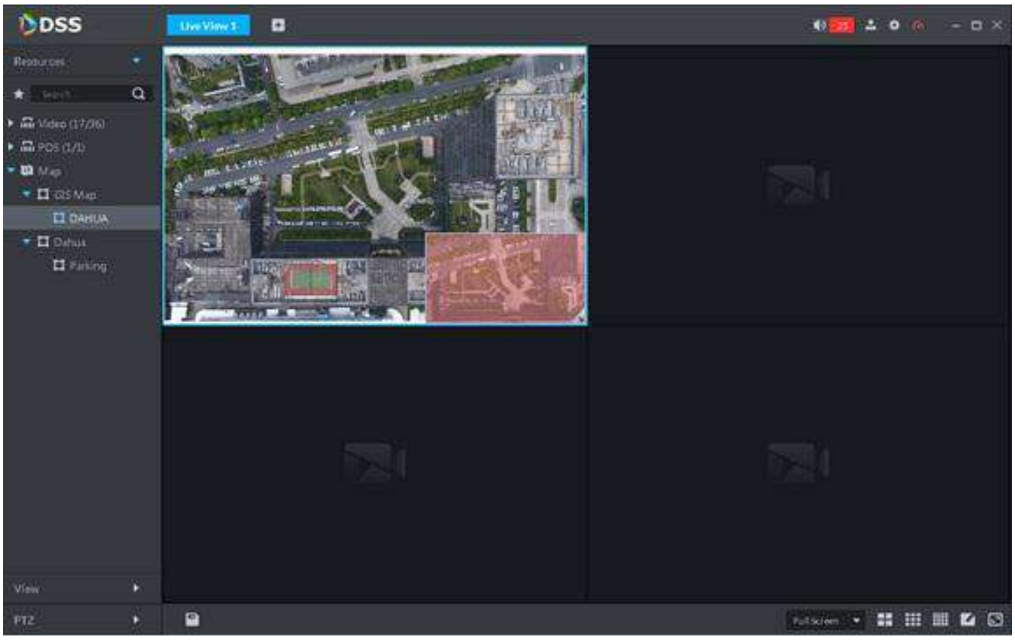
Figure 5-101 Map



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 and cancel alarm. See Figure 5-102.

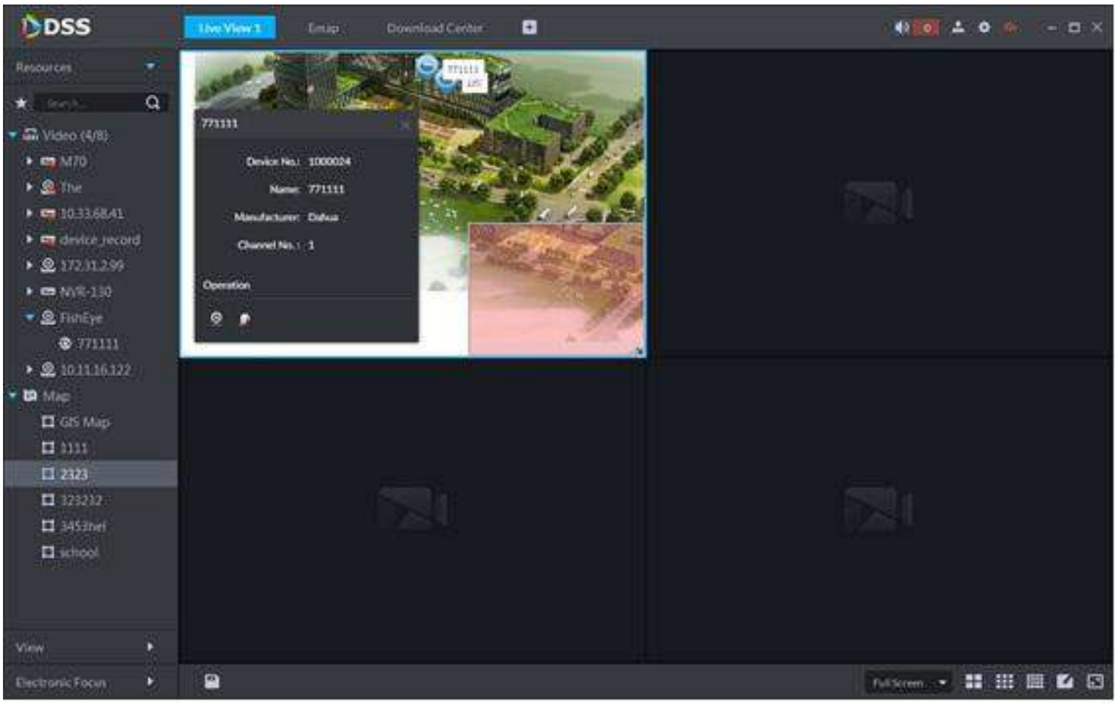
Figure 5-102 Map display



Step 3 Click the marked channel.

System displays channel information. See Figure 5-103.

Figure 5-103 Channel info



771111

Device No.: 1000024

Name: 771111

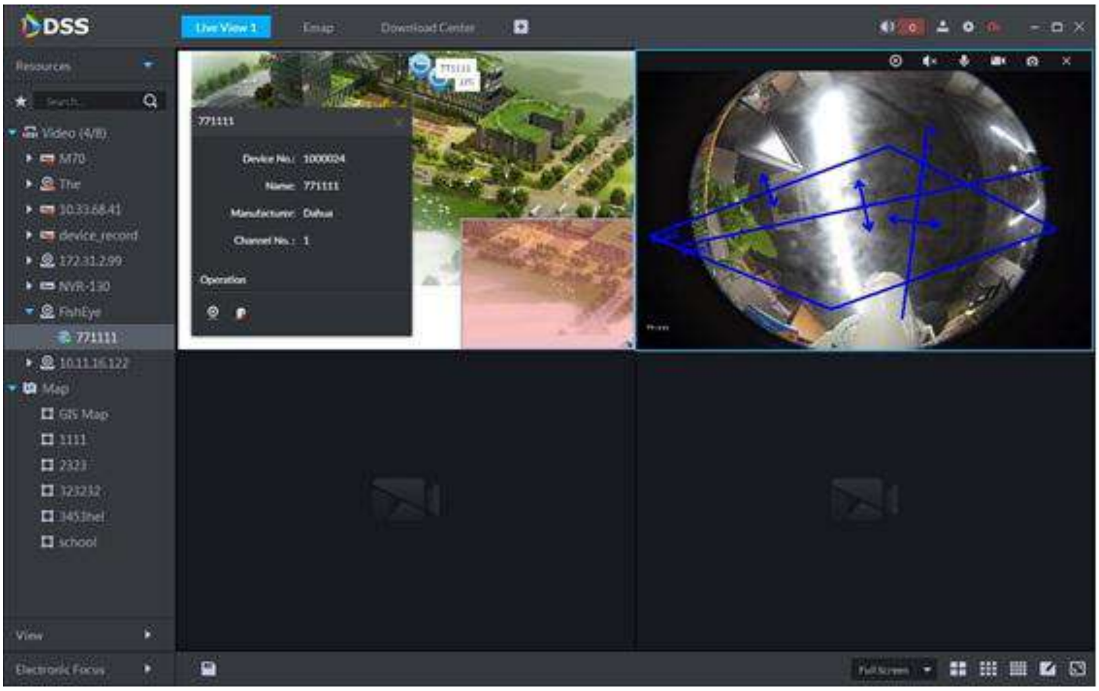
Manufacturer: Dahua

Channel No.: 1

Operation

Step 4 Click to playback real-time video on the window. See Figure 5-104.

Figure 5-104 View channel video



771111

Device No.: 1000024

Name: 771111

Manufacturer: Dahua

Channel No.: 1

Operation

5.8.3 Viewing Map

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 5-105.

Figure 5-105 Emap

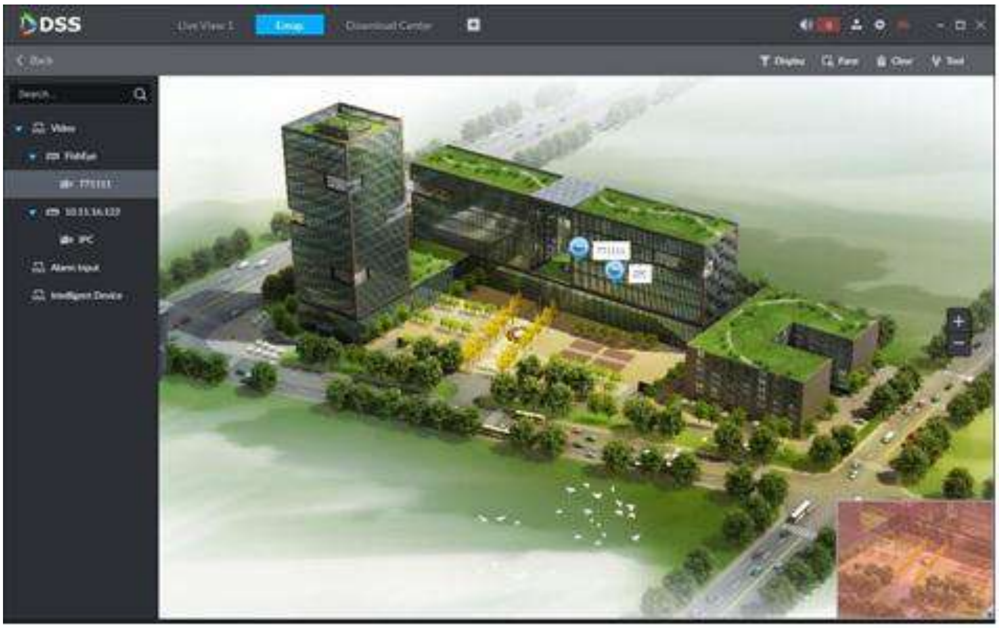


Table 5-28 Map function description

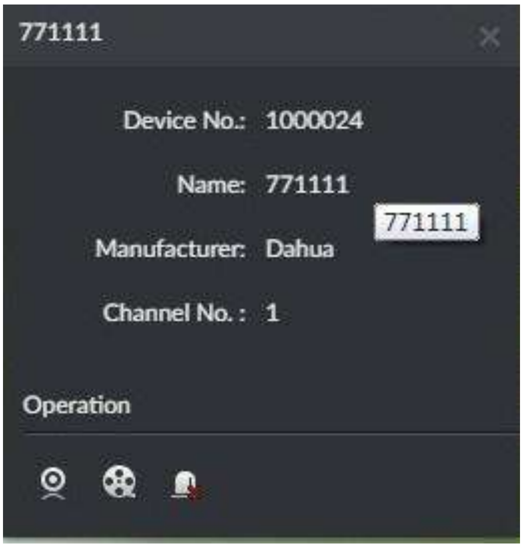
SN	Name	Description
1	Display device	Filter to display video device, alarm input channel.
2	Use frame to select	Use frame to select a device.
3	Clear data on the screen	Clear selection track on the screen.
4	Tools	Include mark, reset, and video relay. ● Mark: It is to give a mark on the map. ● Reset: The map restores default position. ● Video relay: This function is null right now.

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

Step 4 Click the channel on the map.

System displays device SN, channel name, manufacture and channel information. See Figure 5-106.

Figure 5-106 Channel info



771111

Device No.: 1000024

Name: 771111

Manufacturer: Dahua

Channel No. : 1

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

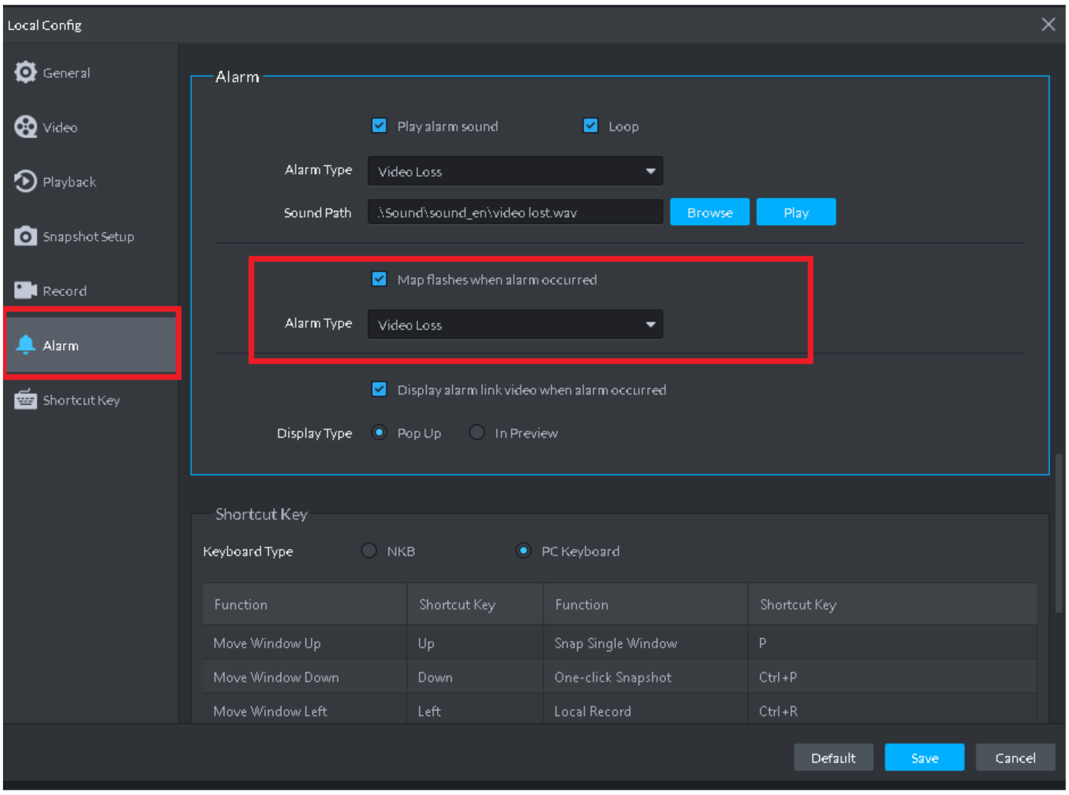
5.8.4 Alarm Flashing on the Map

5.8.4.1 Configuring Alarm Flashing on the Client

Step 1 Click at the top right corner, and then 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 5-107.

Figure 5-107 Select alarm flash



Local Config

- General
- Video
- Playback
- Snapshot Setup
- Record
- Alarm
- Shortcut Key

Alarm

☑ Play alarm sound ☑ Loop

Alarm Type: Video Loss

Sound Path: .\Sound\sound_en\video lost.wav

Browse Play

☑ Map flashes when alarm occurred

Alarm Type: Video Loss

☑ Display alarm link video when alarm occurred

Display Type: ● Pop Up ○ In Preview

Shortcut Key

Keyboard Type: ○ NKB ● PC Keyboard

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

Default Save Cancel

Step 3 Click **Save**.

5.8.4.2 Client Triggering Alarm

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

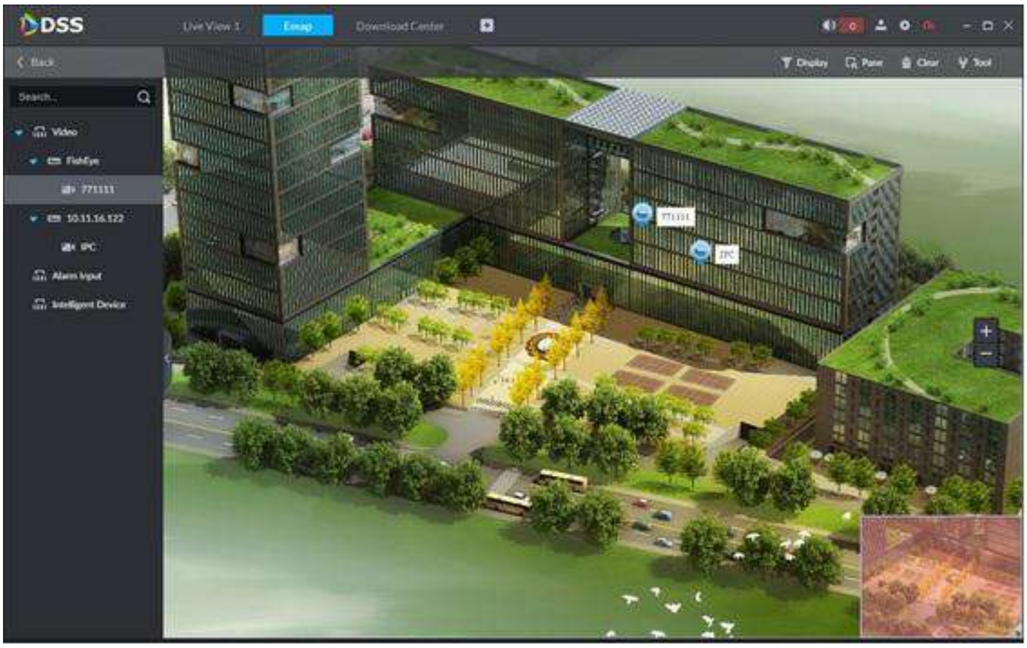
Enter Map interface.

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 5-108.

Figure 5-108 Alarm flash



5.9 POS

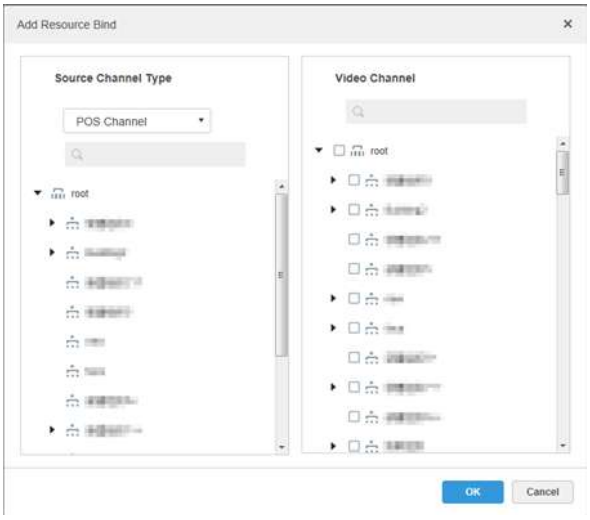
If NVR with POS channel is added on Web, then you can view related video and playback of POS channel on client.

5.9.1 Preparations

- NVR device with POS channel is already added on Web. On the interface of **Bind Resource**, bind video channel for POS channel. See Figure 5-109.

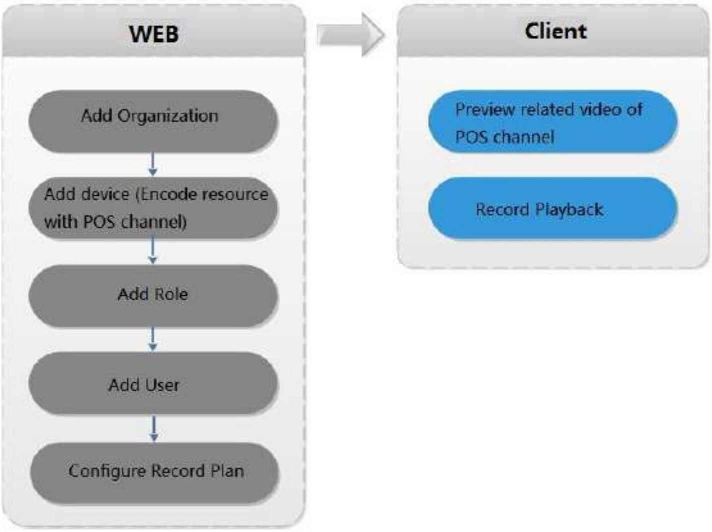
At least one POS channel is bound to NVR which is required to be added.

Figure 5-109 Bind video channel for POS channel



- Record plan is already configured on Web. For more details, please contact administrator or see Figure 5-110.

Figure 5-110 POS business flow


WEB
Add Organization
Add device (Encode resource with POS channel)
Add Role
Add User
Configure Record Plan
Client
Preview related video of POS channel
Record Playback

5.9.2 Live View

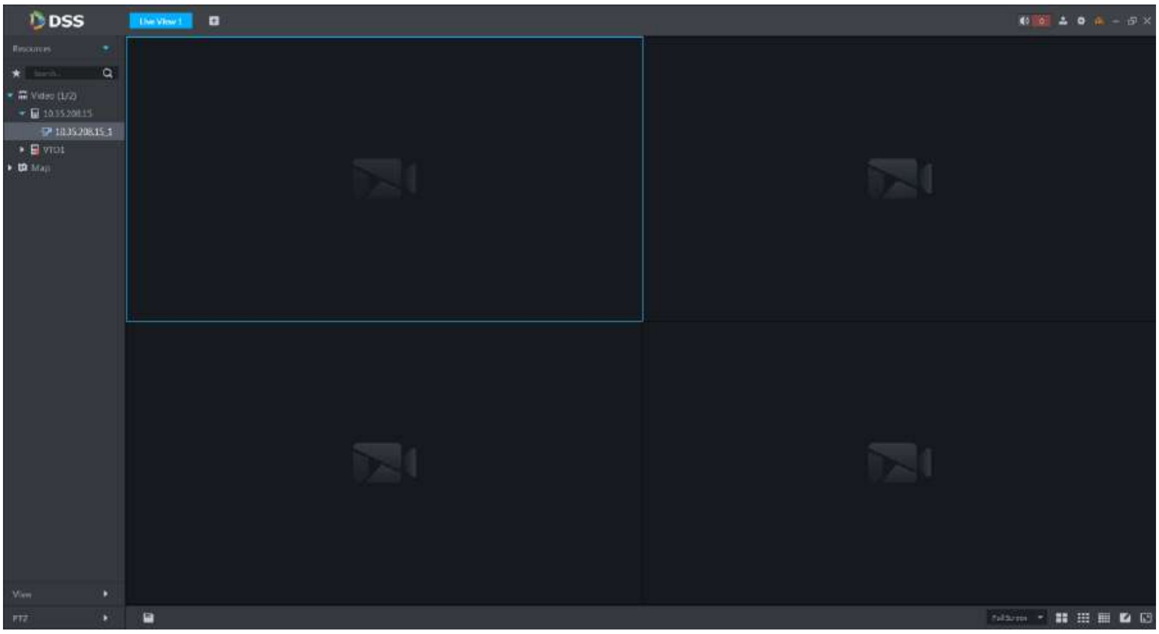
Preview realtime video and POS info of video channel linked to POS channel.

In this chapter, it will introduce how to enable settings of video preview and POS format. For more details, refer to "5.3 Video Preview".

Step 1 Click ⊞ and select **Live View** on the interface of **Homepage**.

The interface of **Live View** is displayed. See Figure 5-111.

Figure 5-111 Open realtime live interface



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

POS channel info is displayed.

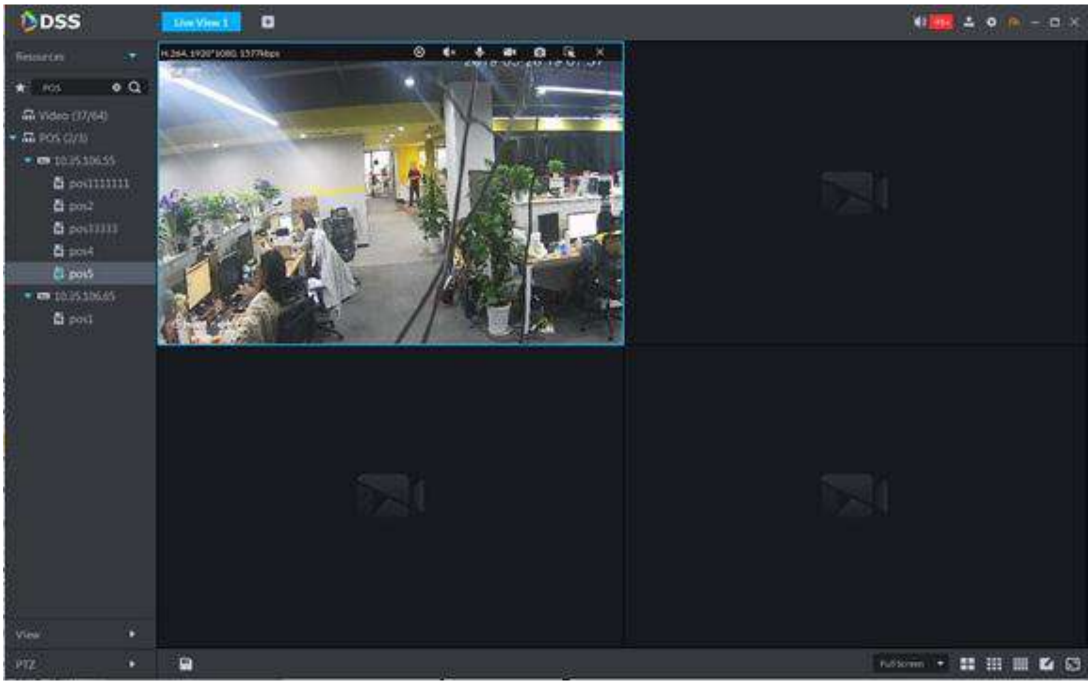
Step 3 Preview realtime channel video linked by POS.

Support following methods to preview.

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

Corresponding video and POS info of linked channel are displayed. See Figure 5-112.

Figure 5-112 Start realtime live



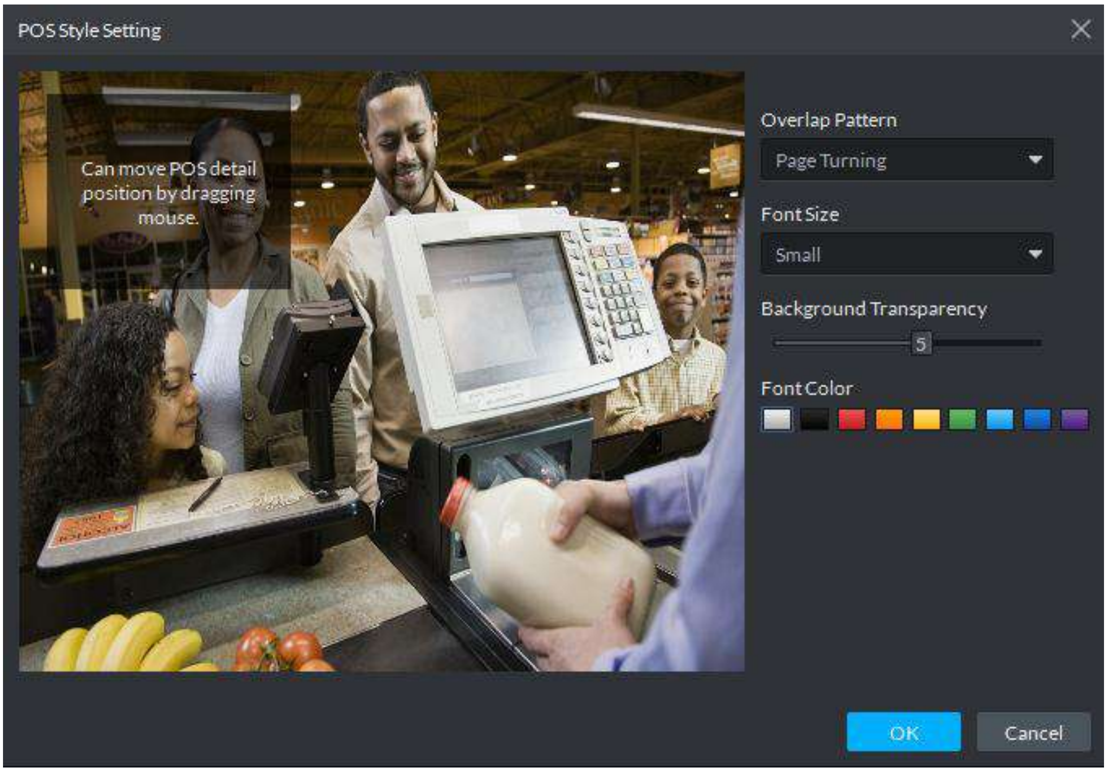
Step 4 Set POS format.

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

1) Right click and select **Set POS Style** on the live interface.

The interface of **POS Style Setting** is displayed. See Figure 5-113.

Figure 5-113 POS format setting



POS Style Setting

Can move POS detail position by dragging mouse.

Overlap Pattern: Page Turning

Font Size: Small

Background Transparency: 5

Font Color

2) Set Overlap Pattern, Font Size, Background Transparency and Font Color.

3) Move the mouse to POS info overlay area, press mouse left button and move it to adjust POS info overlay position.

4) Click OK and save config.

5.9.3 Record Playback

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

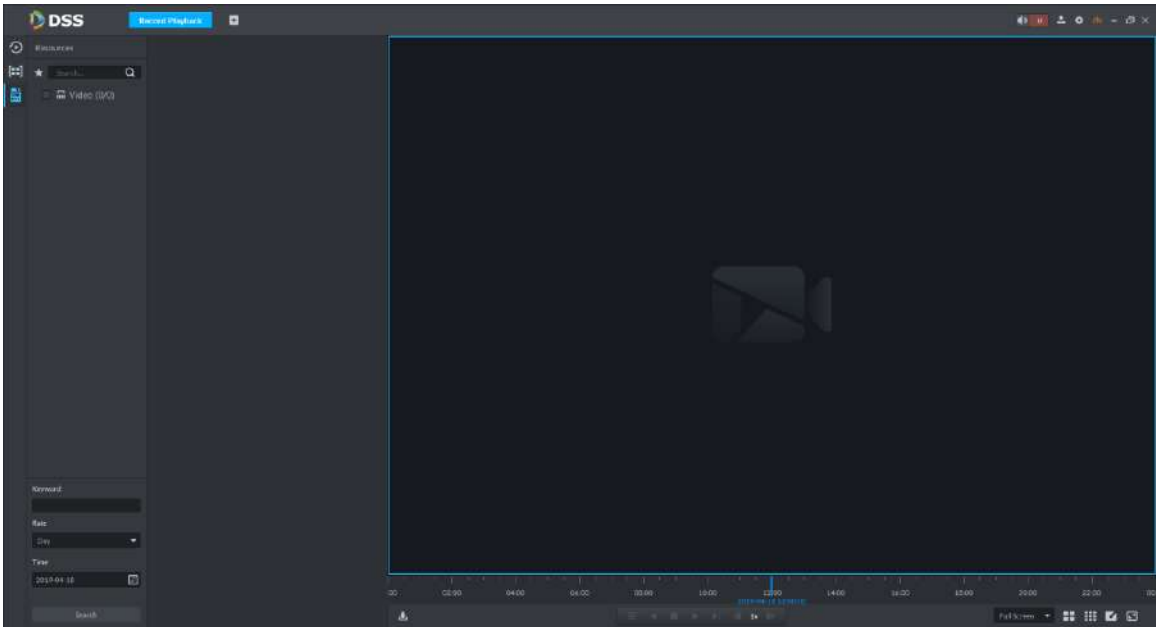
In this chapter, it mainly introduces how to replay related video of POS receipt. For more operation details, refer to "5.4 Record"

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

Step 2 Click .

The interface of **POS Search** is displayed. See Figure 5-114.

Figure 5-114 POS search

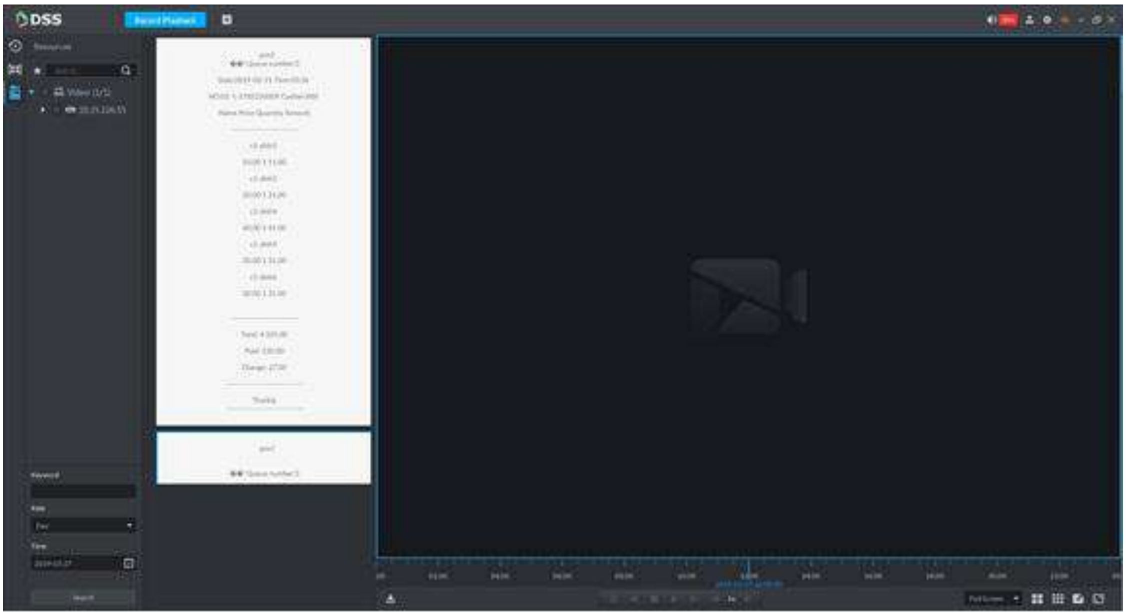


Step 3 Select channel from the device tree.

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

The search result is displayed. See Figure 5-115

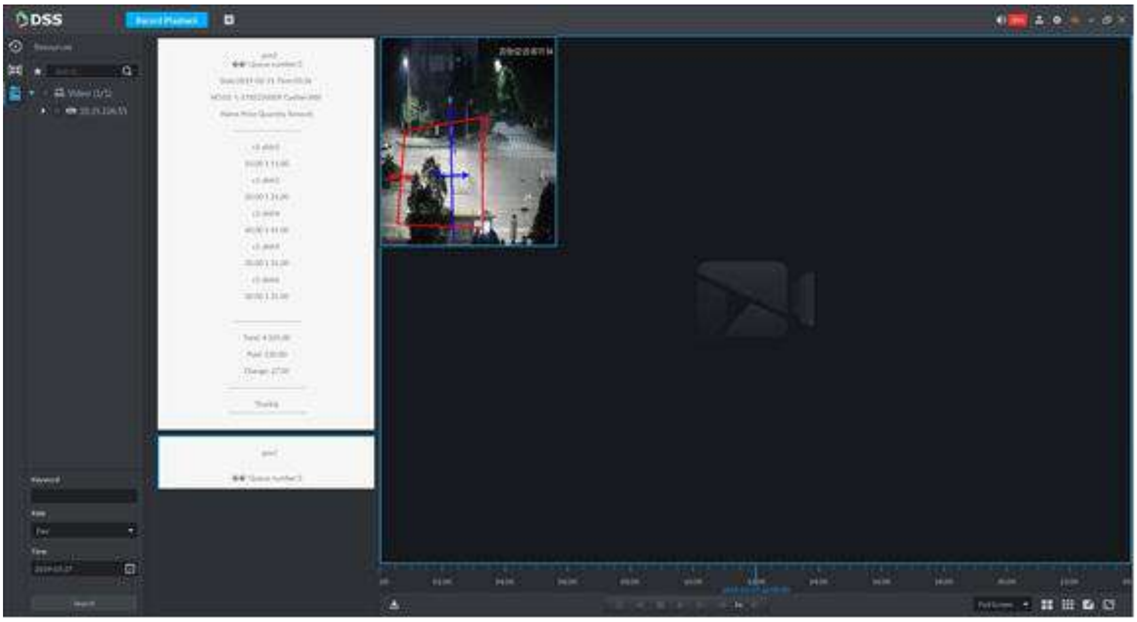
Figure 5-115 POS search result



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

The window will play related video of POS. See Figure 5-116.

Figure 5-116 Record playback



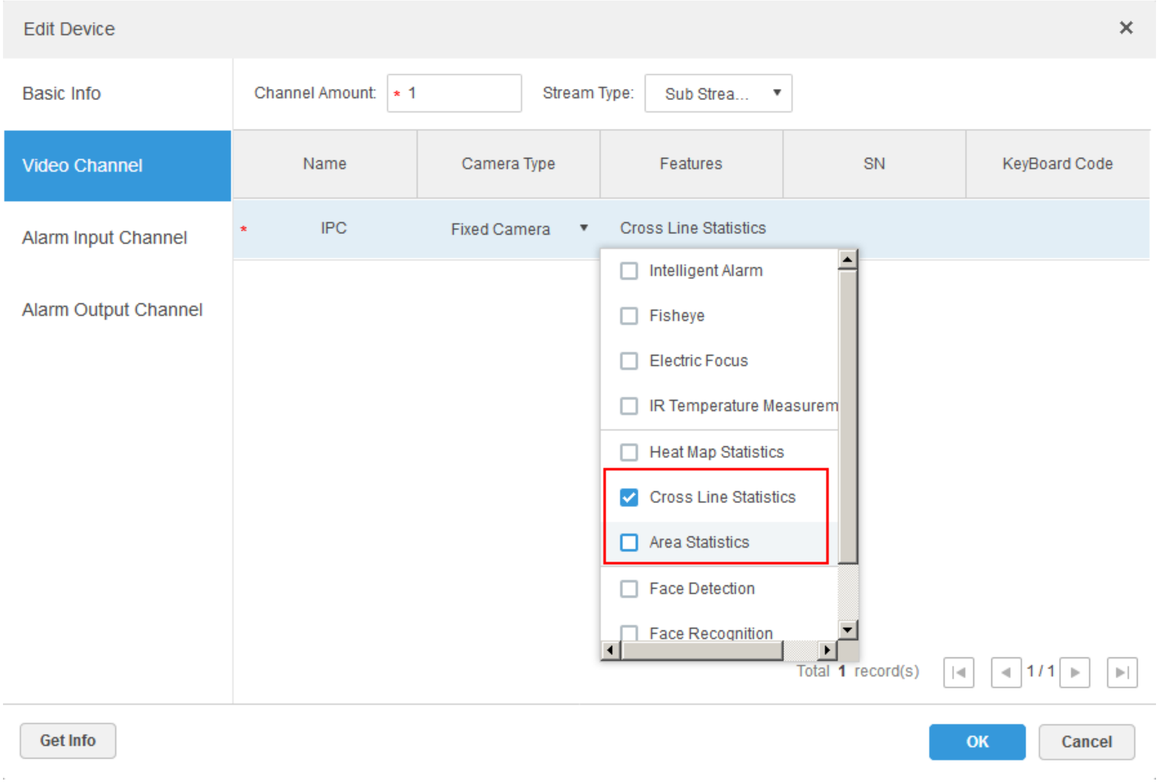
5.10 Flow Analysis

System supports people counting and heatmap function.

5.10.1 Preparations

- IPC with people counting or area statistics function is added to the client. Refer to "4.5 Adding Device".
- After adding the IPC, click ✎, and then select the Cross Line Statistics or Area Statistics from the drop-down list according to the requirement. See Figure 5-117.

Figure 5-117 Modify channel capacity set



Edit Device ×

- Basic Info
- Video Channel
- Alarm Input Channel
- Alarm Output Channel

Channel Amount: * 1   Stream Type: Sub Strea... ▼

	Name	Camera Type	Features	SN	KeyBoard Code
*	IPC	Fixed Camera ▼	Cross Line Statistics		

- □ Intelligent Alarm
- □ Fisheye
- □ Electric Focus
- □ IR Temperature Measurem
- □ Heat Map Statistics
- ☑ Cross Line Statistics
- □ Area Statistics
- □ Face Detection
- □ Face Recognition

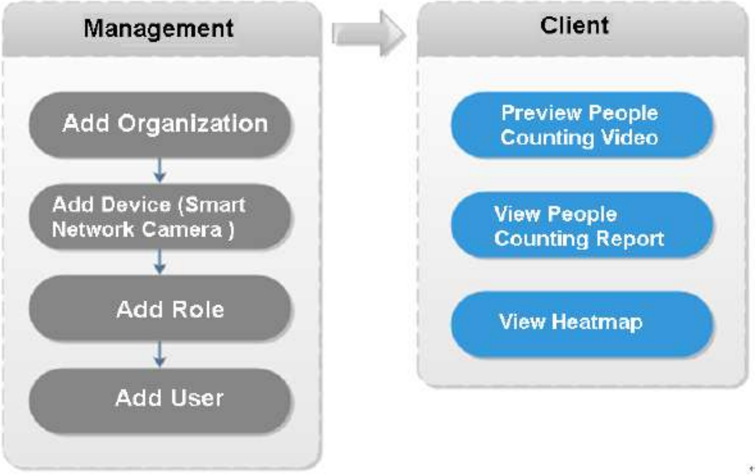
Total 1 record(s) 1 / 1

Get Info   OK   Cancel

- Set smart rules of the camera; refer to corresponding user manual for details.

Refer to Figure 5-118 for flows information.

Figure 5-118 Flow analysis flow


Management
Add Organization
Add Device (Smart Network Camera)
Add Role
Add User
Client
Preview People Counting Video
View People Counting Report
View Heatmap

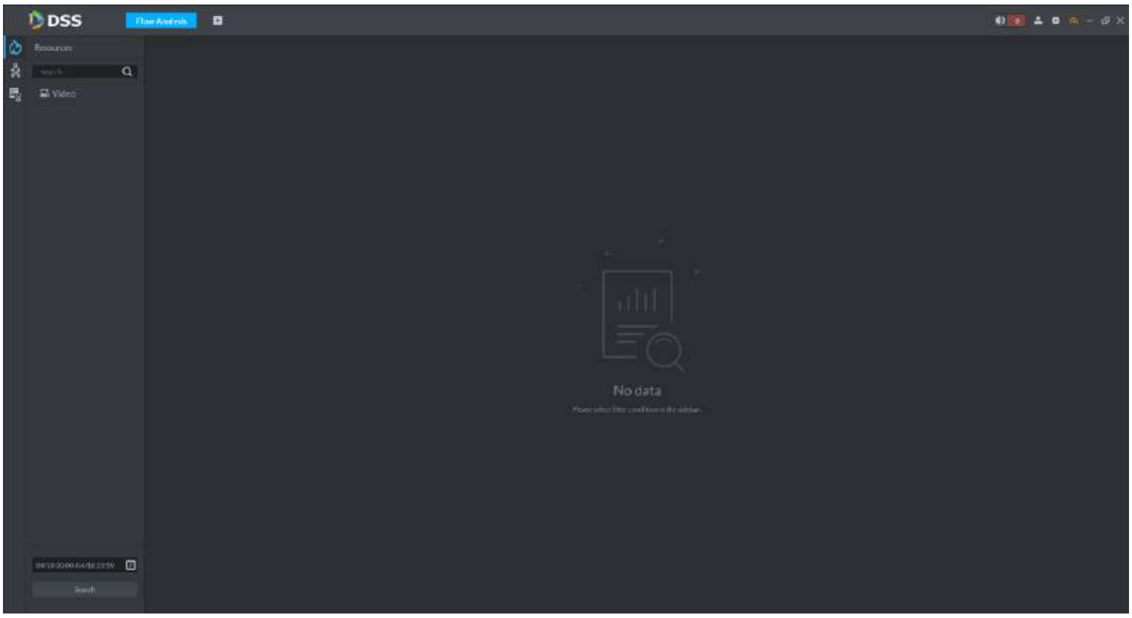
5.10.2 Heatmap

Heatmap displays the distribution of moving objects in colors of different shades. It reflects the temperature of regions by different colors, for example, red means the temperature is relatively high, and blue means the temperature is relatively low.

Step 1 Click + and select **Flow Analysis** on the interface of **Homepage**.

The interface of **Flow Analysis** is displayed. See Figure 5-119.

Figure 5-119 Flow analysis



Step 2 Click .

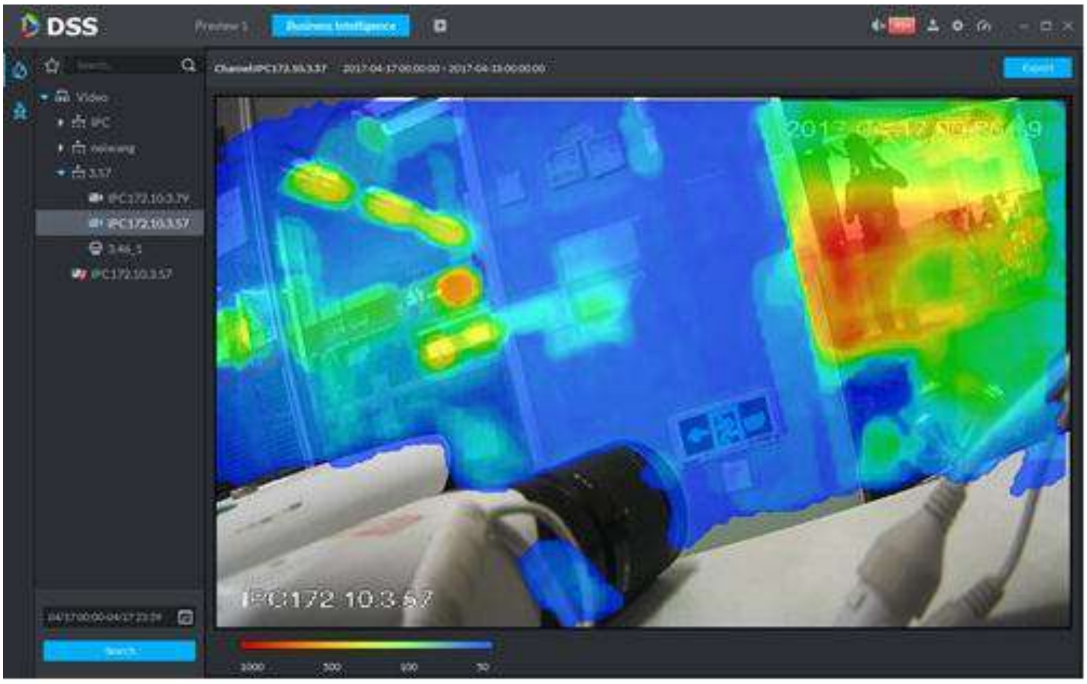
The **Heatmap** interface is displayed.

Step 3 Select a channel to show heat map, and select time, click **Search**

System displays heatmap interface. See Figure 5-120.

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 5-120 Heatmap



Step 4 Click **Export** at the top right corner, you can export heat map in bmp format.

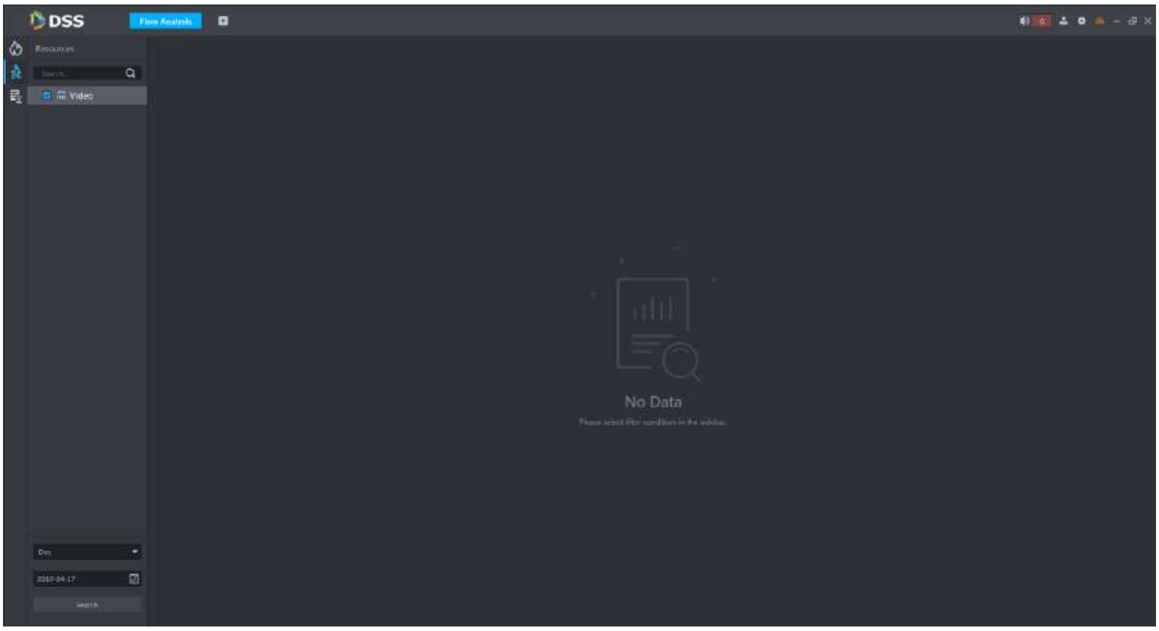
5.10.3 People Counting Report

Form data report by searching entry and exit people number within specific period. Strand people number can be searched via day report.

Step 1 Click on the interface of **Flow Analysis**.

The interface of flow analysis is displayed. See Figure 5-121.

Figure 5-121 Flow analysis report



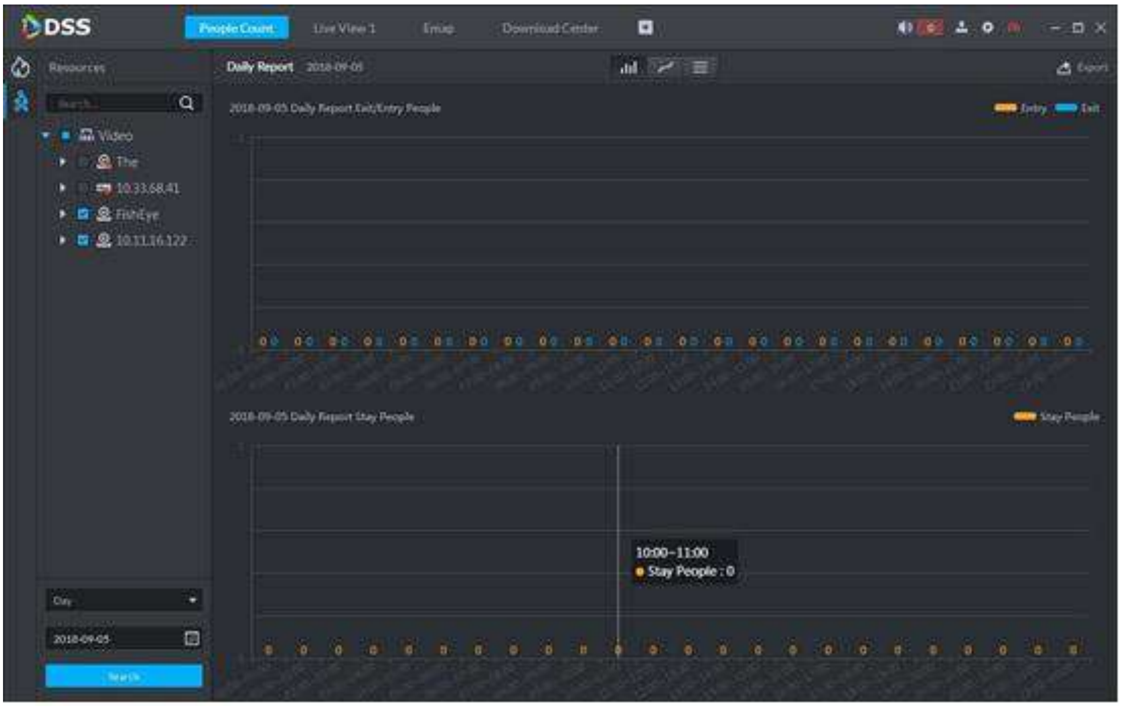
Step 2 Select device channel, search period and statistics time, and click **Search**.

The system generates report data. See Figure 5-122.

The report is displayed by bar chart, line chart and list. Click on top of the interface to switch display format.

Stranded people number is not calculated if search period is week, month or year.

Figure 5-122 Search result



Step 3 Click **Export** on the right corner of the interface, and then save report locally in the form of pdf according to interface prompt.

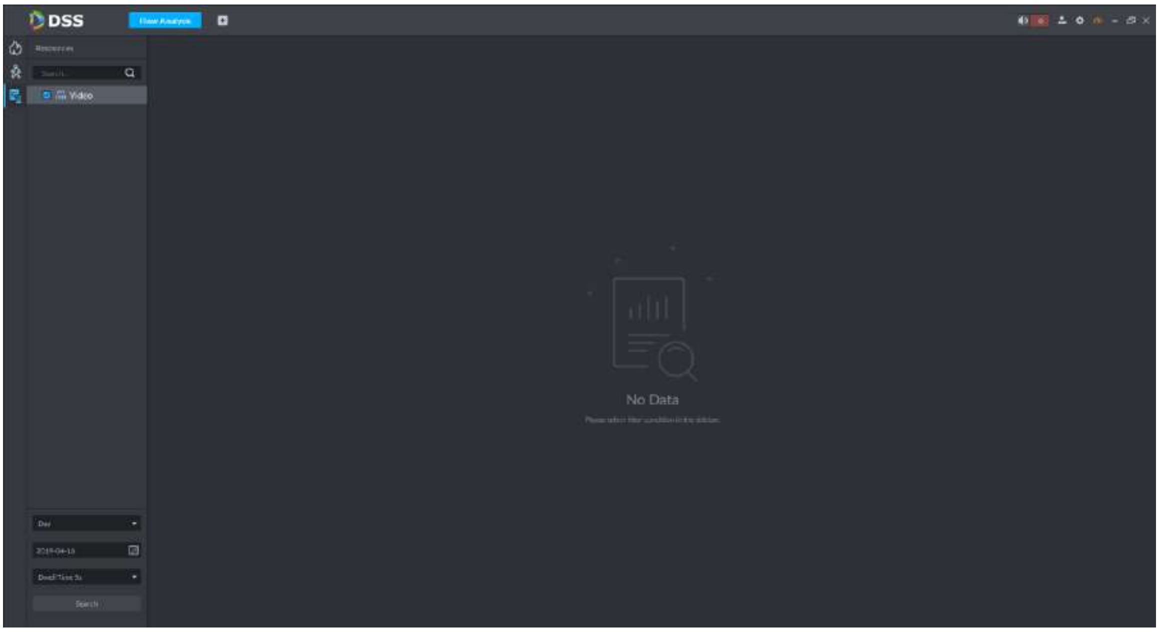
5.10.4 Dwell Time Report

Form data report by searching entry and exit people number within specific period. Strand people number can be searched via day report.

Step 1 Click on the interface of **Flow Analysis**.

The **Dwell Time** report interface is displayed. See Figure 5-123.

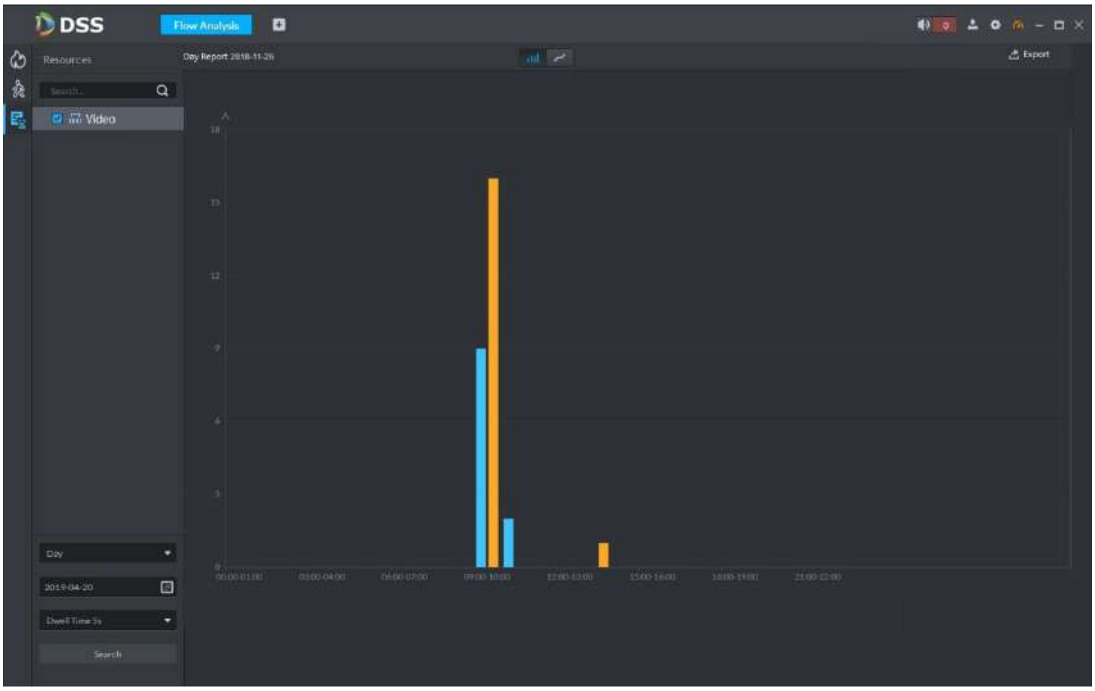
Figure 5-123 Dwell time report



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

The system generates report data, see Figure 5-124.

Figure 5-124 Search result



Step 3 Click **Export** on upper right corner of the interface and save report locally in the form of pdf according to interface prompt.

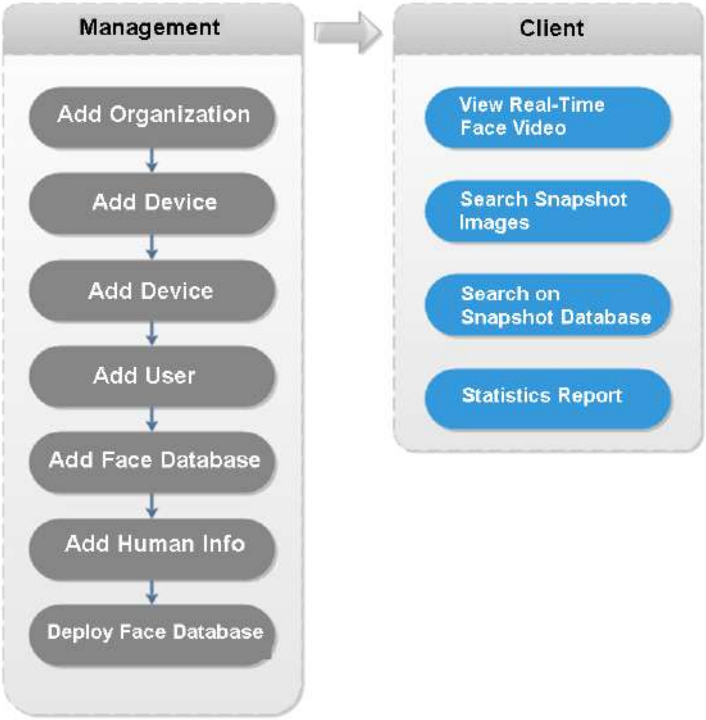
5.11 Face Recognition

5.11.1 Preparations

- Refer to "4.10.1 Creating Face Database" to create human face database on the manager.
- Refer to "4.10.2 Arm Config" to arm human face database on the platform manager.

Refer to Figure 5-125 for flows information.

Figure 5-125 Face recognition flow



5.11.2 Real-Time 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 5-126.

Figure 5-126 Realtime video

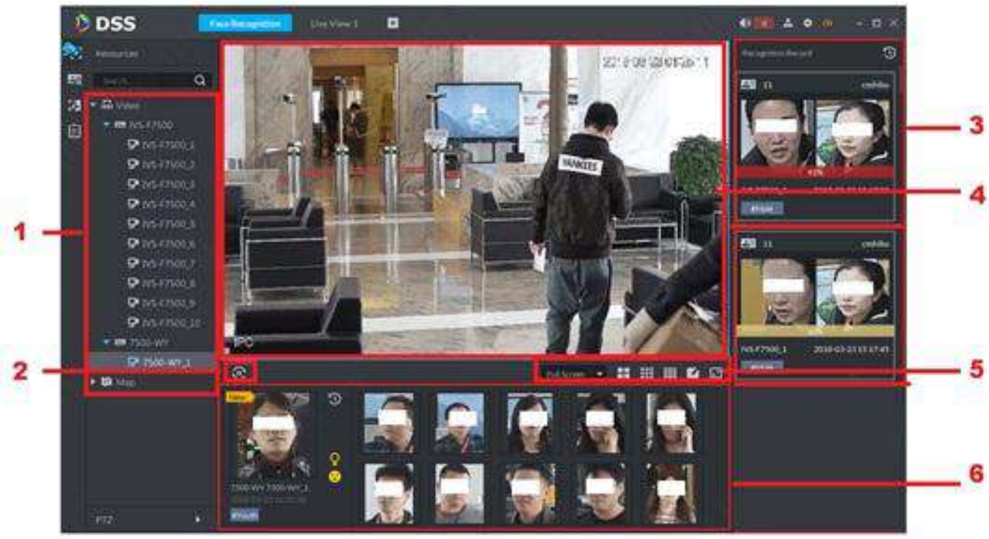


Table 5-29 Real-time video interface description

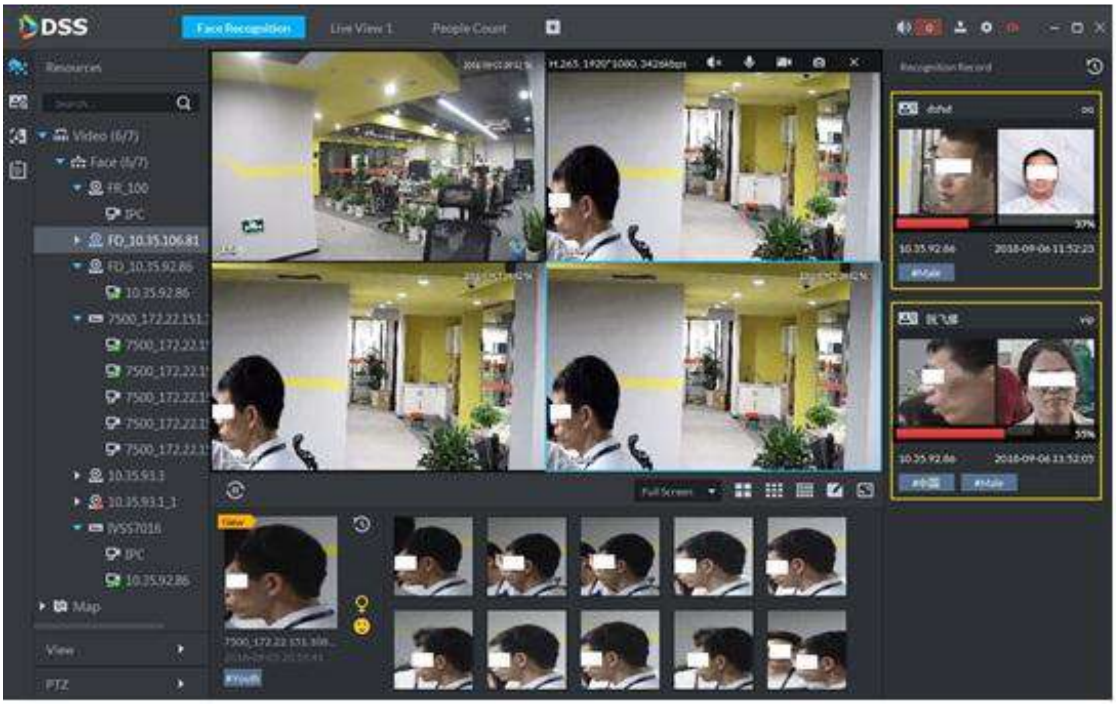
SN	Name		Description
1	Device tree		Display device information.
2	Pause refresh/start refresh		● ▶: When this icon is on the interface, the snapshot display pane does not refresh human face snapshot image. Click the icon, system displays real-time face image. ● ⏸: When this icon is on the interface, the snapshot display pane refresh human face snapshot image. Click the icon, system refreshes human face snapshot image.
3	Recognition history record		Display the snapshot human face image of the video.
4	Monitor window		Display channel preview video. In multiple-window display mode, double click the window to switch to 1-window display mode. Double click the window again to restore original mode.
5	Full Screen ▾	Image display rate	There are two modes: full screen, original scale. The full screen refers to one window at the full screen.
	⊞ ⊞ ⊞ ✎	Window split switch	Display switched window amount. System supports customized settings.
	⤡	Full screen display	The system displays window at full screen.
6	Snapshot human face image display pane		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.

Enable video preview interface. See Figure 5-127.

Figure 5-127 Video preview



Step 4 Double click snapshot human image.

System displays human detailed information interface.

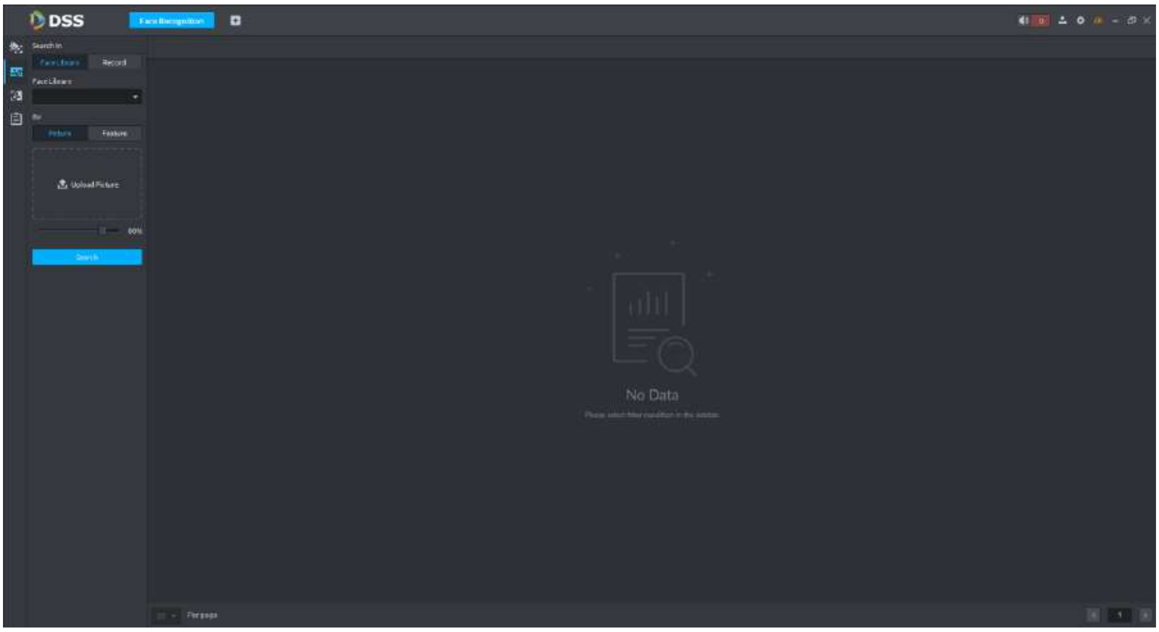
5.11.3 Snapshot Search

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 Click on the interface of **Face Recognition**.

The interface of **Face Search** is displayed. See Figure 5-128.

Figure 5-128 Face search



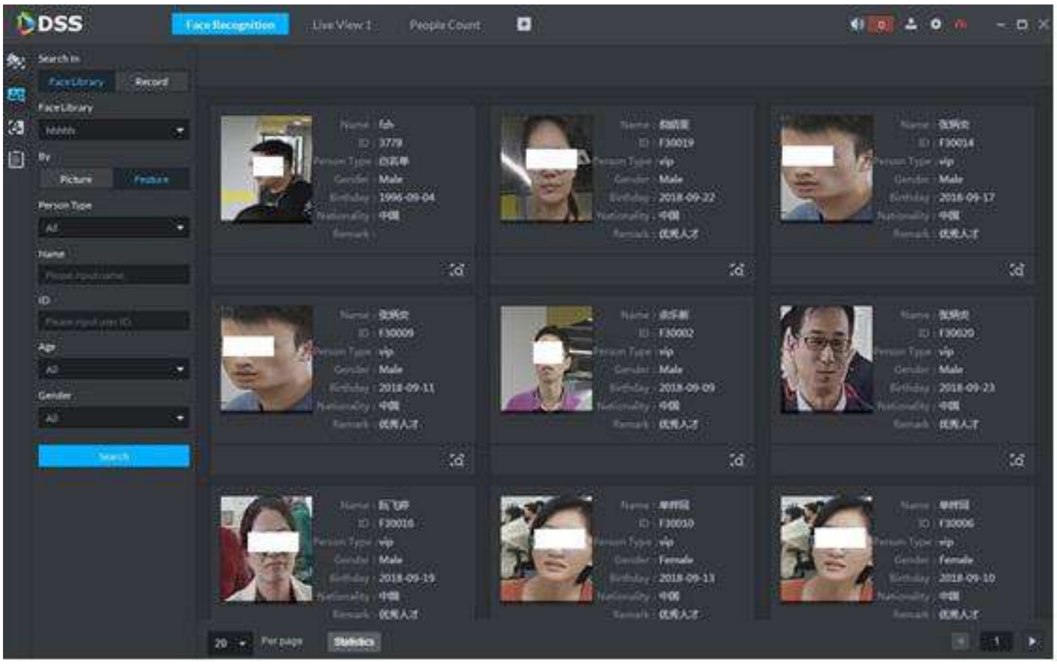
Step 2 Set search condition.

- You can search from **Face Library** or **Record**.
- Select a human face database already exists.
- The search condition can be Picture or Feature.

Step 3 Click **Search**.

The search interface is displayed. See Figure 5-129.

Figure 5-129 Snapshot search result



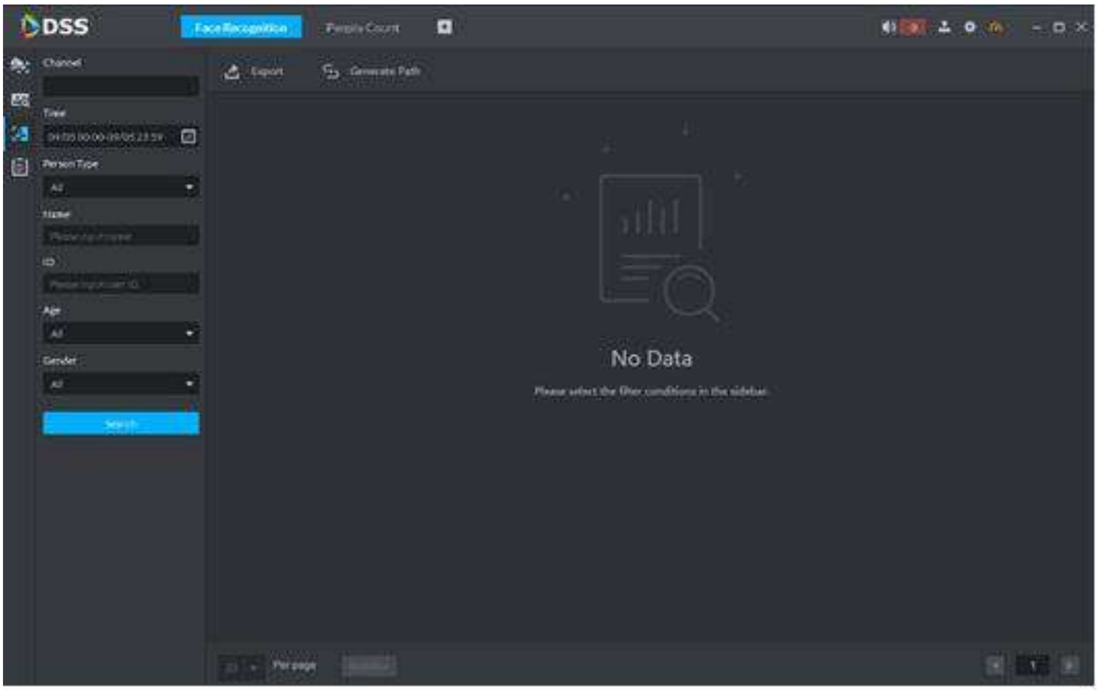
5.11.4 Snapshot Database Search

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 interface of **Face Search** is displayed. See Figure 5-130.

Figure 5-130 Snapshot database search



Channel

Time: 09/05 00:00-09/05 23:59

Person Type: All

Name

ID

Age: All

Gender: All

No Data

Please select the filter conditions in the sidebar.

Step 2 Set search condition.

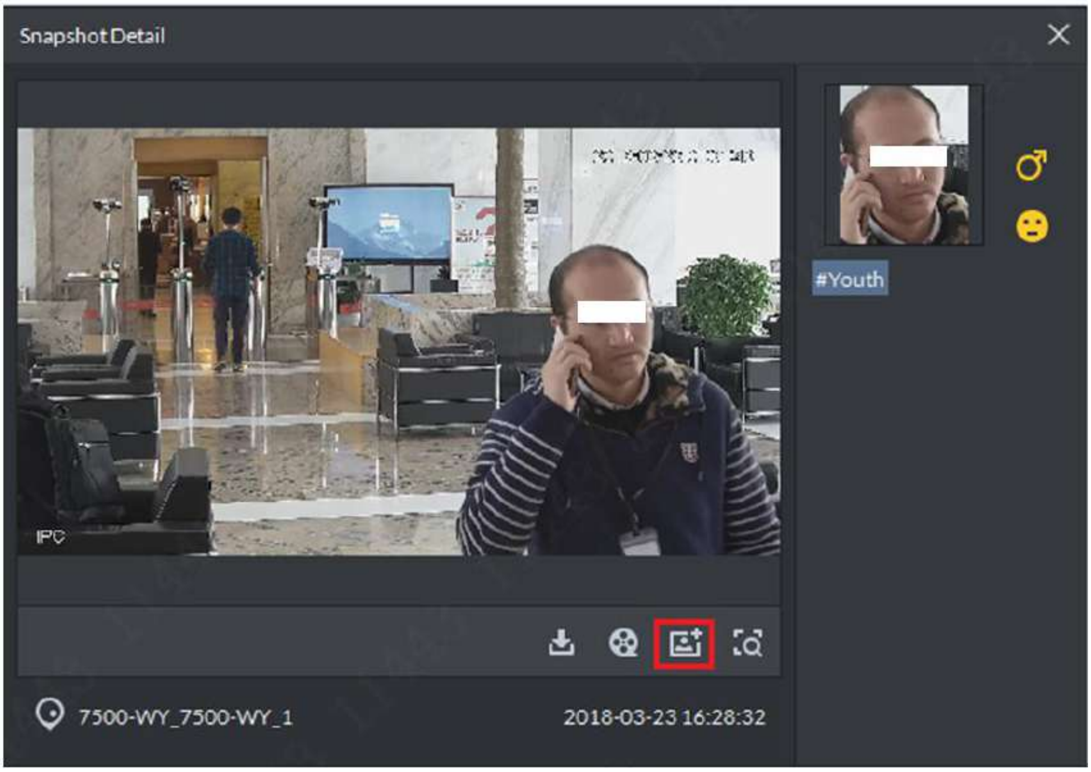
System supports search by channel, time, human face features, name, ID, age and gender.

Step 3 Click **Search**.

Step 4 Double click the search result

System displays human information. See Figure 5-131. There is no image on the left if you do not upload image when setting search criteria. Refer to Table 5-30 for detailed operation information.

Figure 5-131 Snapshot detail



7500-WY_7500-WY_1

2018-03-23 16:28:32

Table 5-30 Operation description

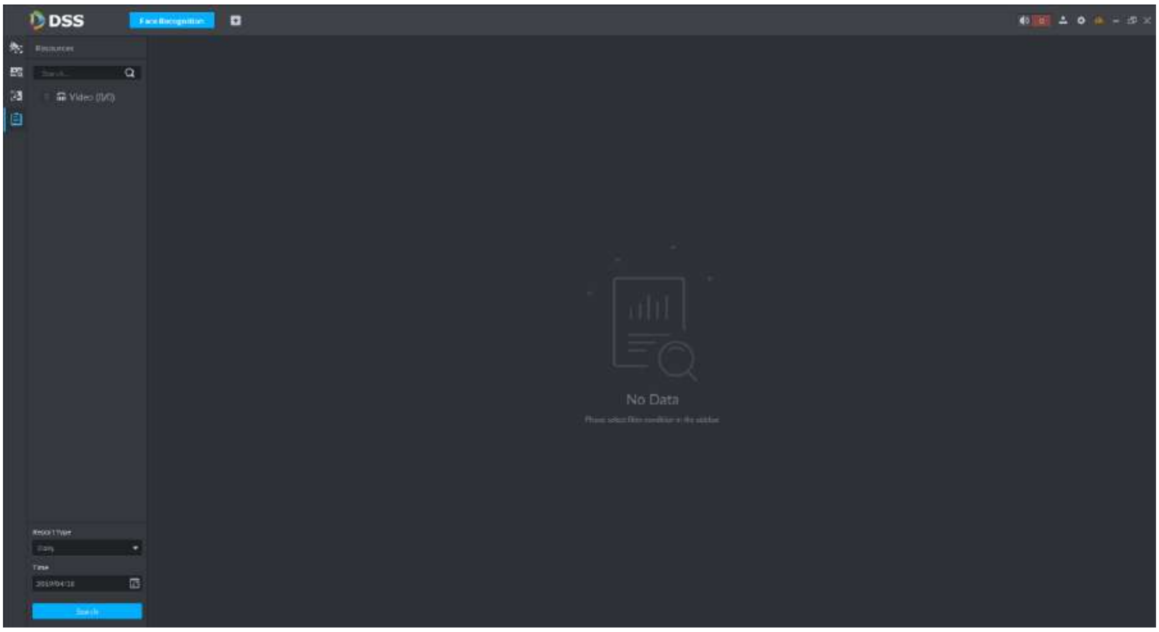
Operation	Description
Download Record	Click and save RAR file on the specified path. The .RAR file contains the human face snapshot image and snapshot panorama images.
Playback record	Click to playback the 15-seconds video record before and after the snapshot.
Add person	Add the snapshot person to the 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. 2. Click Search, system displays search result.

5.11.5 Statistics Report

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

The interface of **Report** is displayed. See Figure 5-132.

Figure 5-132 Report



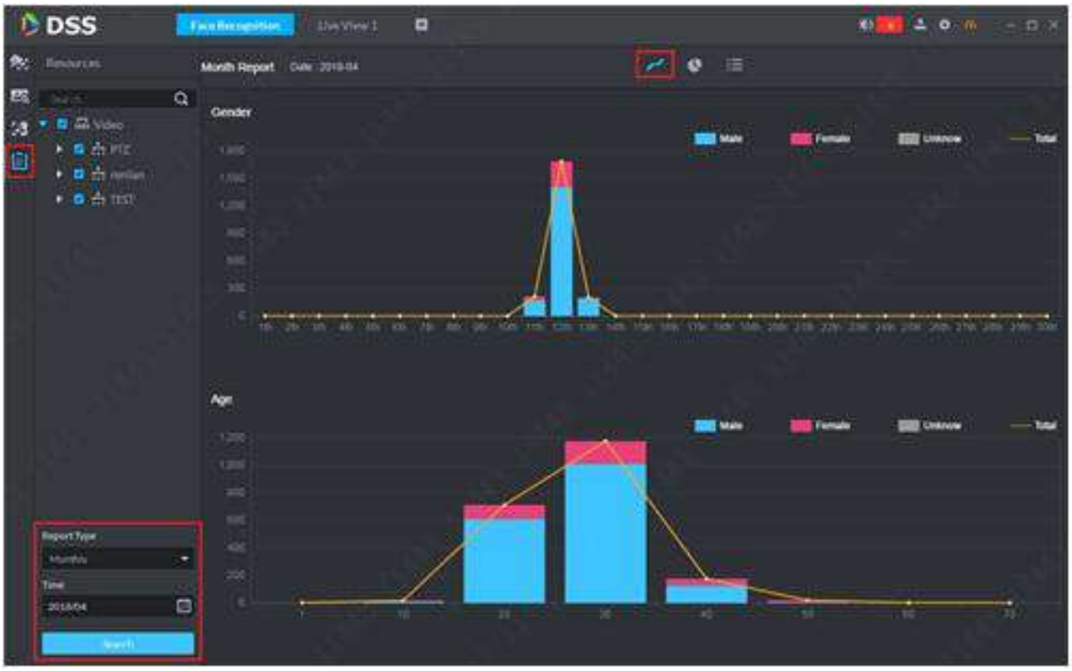
Step 2 Set search condition.

Set video channel, report type and time.

Step 3 Click **Search**.

The statistics search result is displayed. See Figure 5-133.

Figure 5-133 Statistics report



Report Type

Monthly

Time

2018/04

- 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.

5.12 ANPR

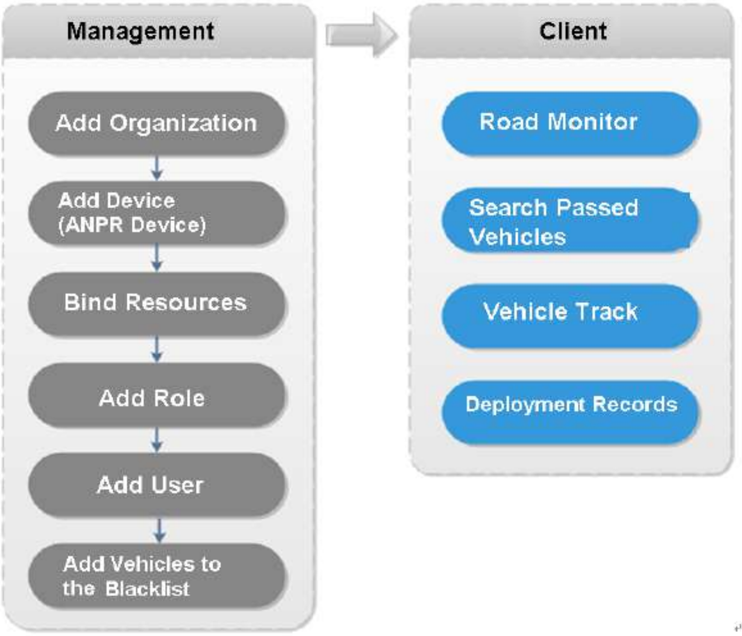
The platform integrates vehicle module and receive vehicle recognition info reported by ANPR, search passed vehicle record, vehicle track and arm record.

5.12.1 Preparations

- Refer to "4.5 Adding Device" to add ANPR device on the platform manager.
- Refer to "4.11 Adding Vehicle Blacklist" to add vehicle blacklist on the platform manager.

Refer to Figure 5-134 for road monitor flows.

Figure 5-134 ANPR flow



5.12.2 Number Plate Recognition

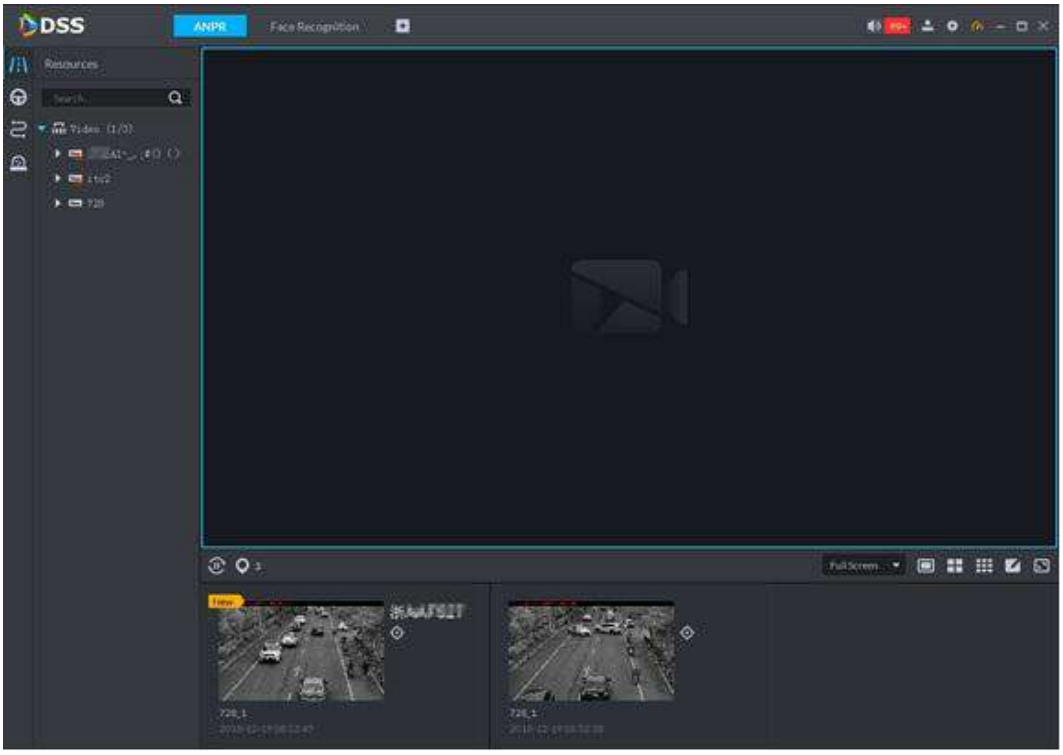
Receive vehicle recognition info reported by ANPR and display on client.

Step 1 Click and select **ANPR** on the **Homepage.**

Step 2 Click and the interface of **ANPR** is displayed. See Figure 5-135.

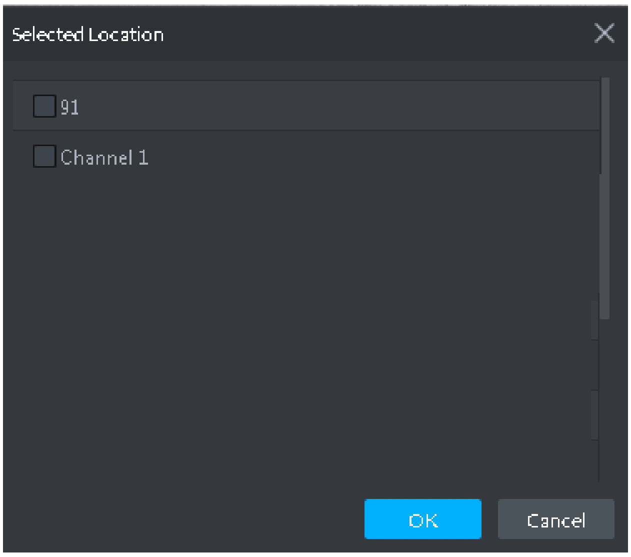
Emap is displayed by single window by default; you can switch number of windows manually.

Figure 5-135 ANPR



Step 3 Click to select the ANPR channel. See Figure 5-136.

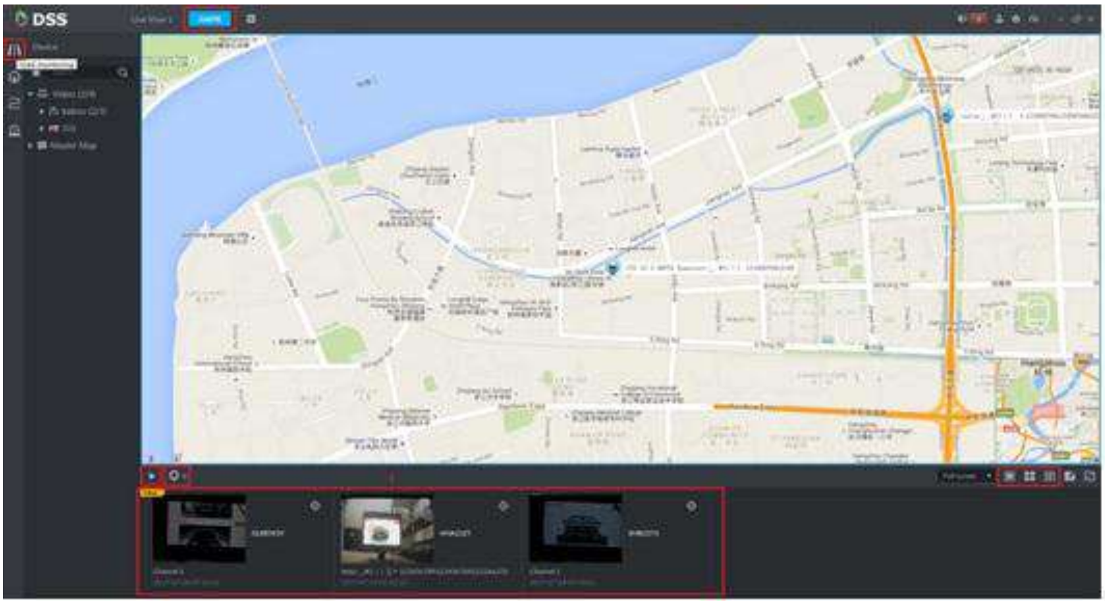
Figure 5-136 Select channel



Step 4 Select ANPR device and then click **OK**.

System displays the selected channel amount and the latest passing vehicle image on the rolling pane. See Figure 5-137.

Figure 5-137 Recognition result



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

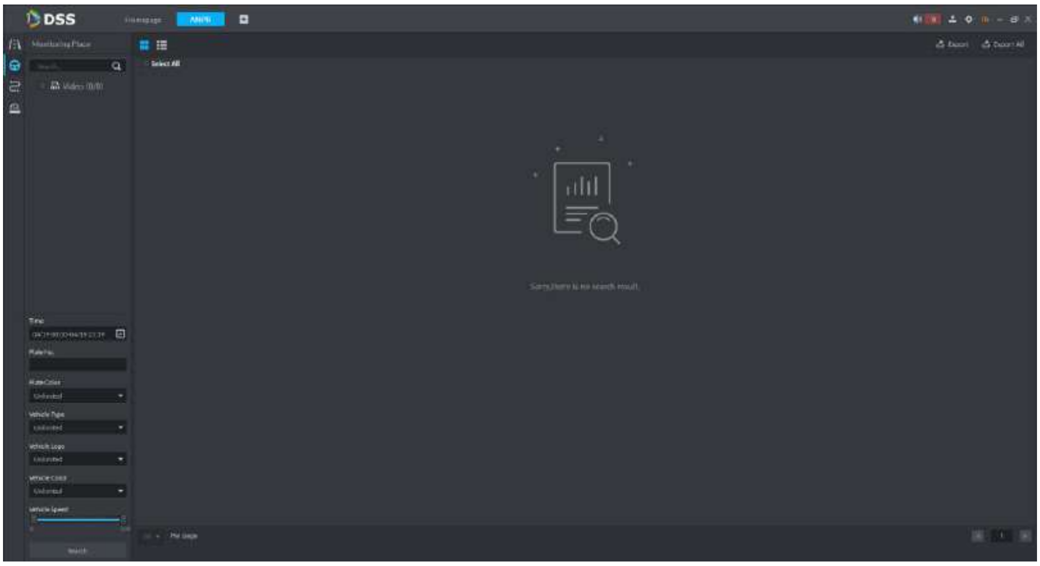
5.12.3 Vehicle Record

Search vehicle records captured and reported by ANPR.

Step 1 Click .

The interface of **Vehicle Record** is displayed. See Figure 5-138.

Figure 5-138 Vehicle record

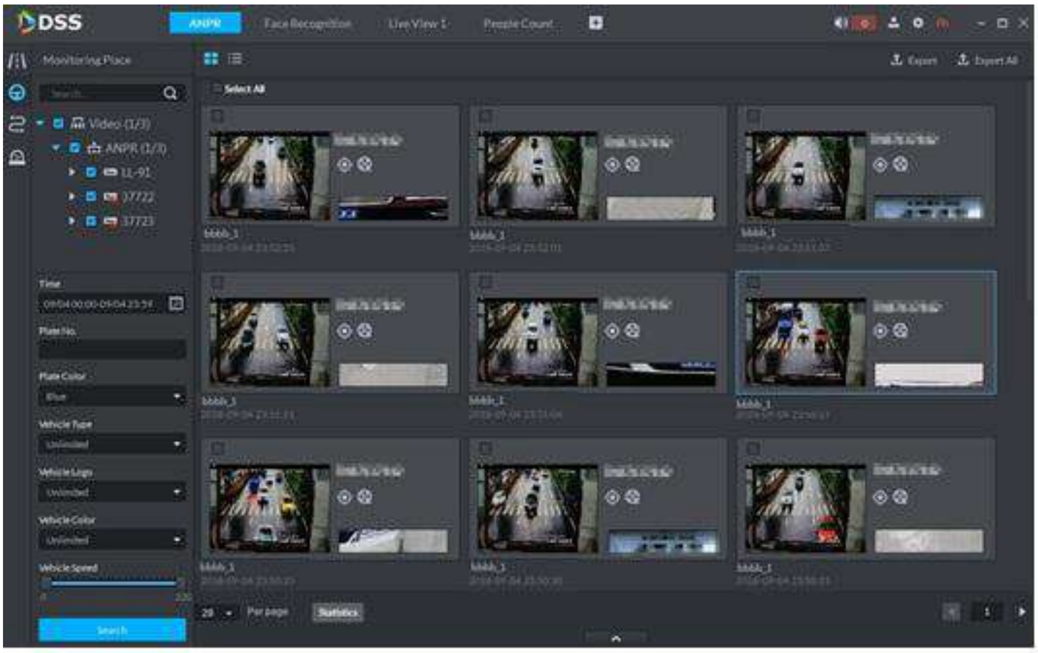


Step 2 Select video channel and search criteria. It includes time, plate number, plate color, plate type, vehicle logo, vehicle body color and lane.

Step 3 Click **Search**.

System displays search result. See Figure 5-139.

Figure 5-139 Search result



For the passed vehicle, you can view its detailed information, record and running track. Refer to the operations listed below.

- Click View mode (⊞) or list mode (☰), and select different display mode.
- Select a snapshot image and then click ^ or double click the image, system displays detailed information. See Figure 5-140. Move the cursor to the middle and select the specified zone, then you can zoom in it. See Figure 5-141.

Figure 5-140 Vehicle detail

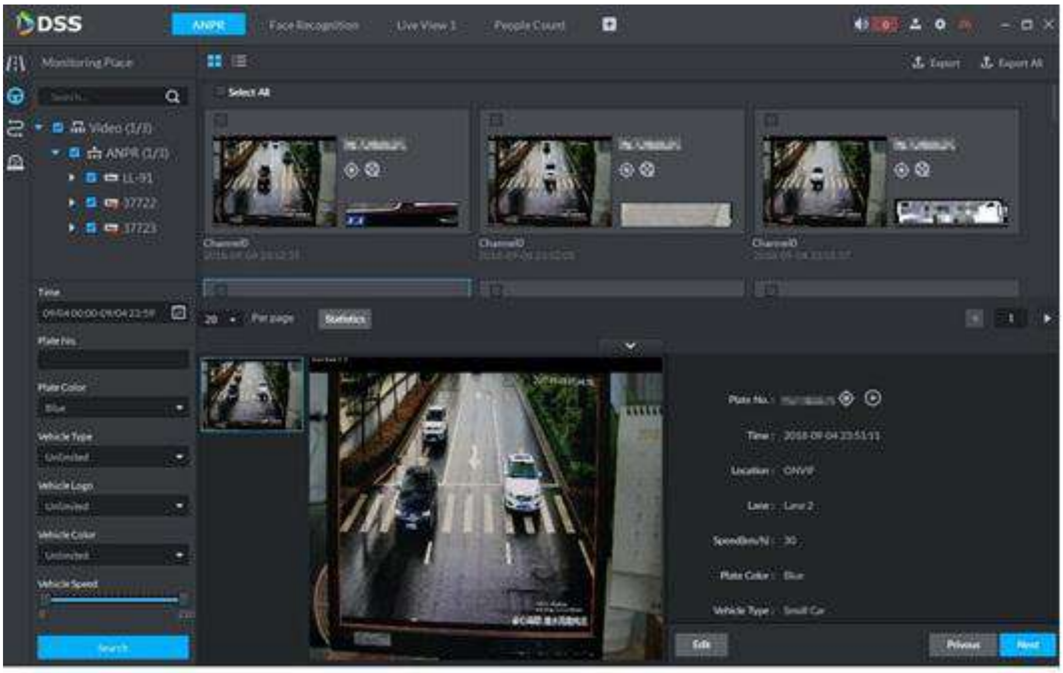


Plate No.: [redacted]

Time: 2018-09-04 23:51:11

Location: ONVIF

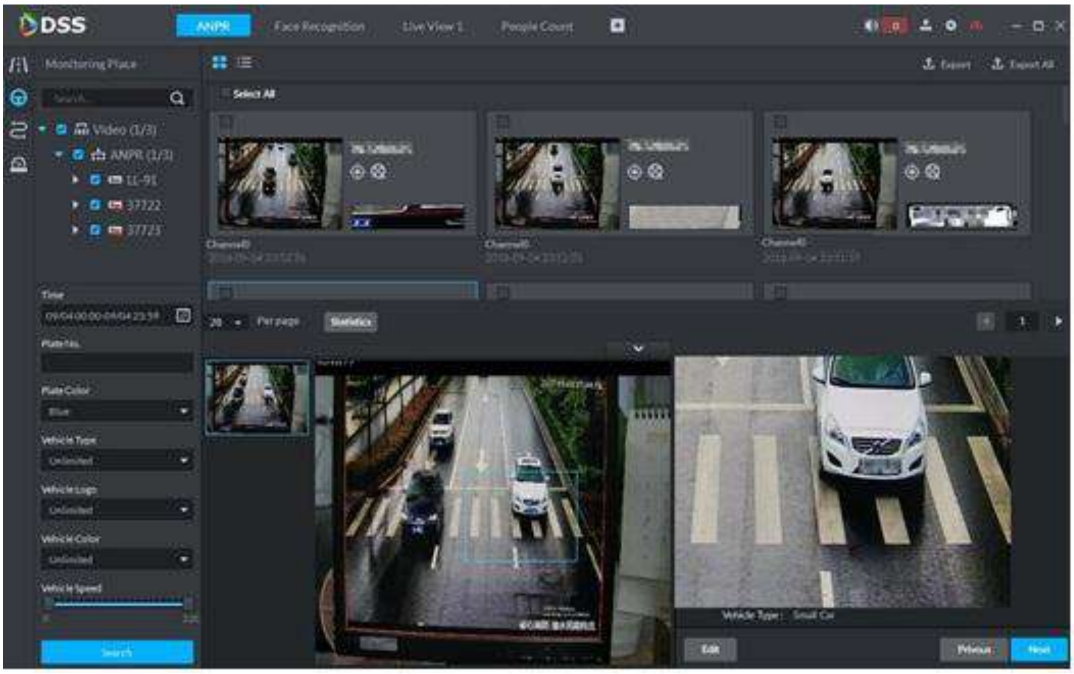
Lane: Lane 2

Speed(km/h): 30

Plate Color: Blue

Vehicle Type: Small Car

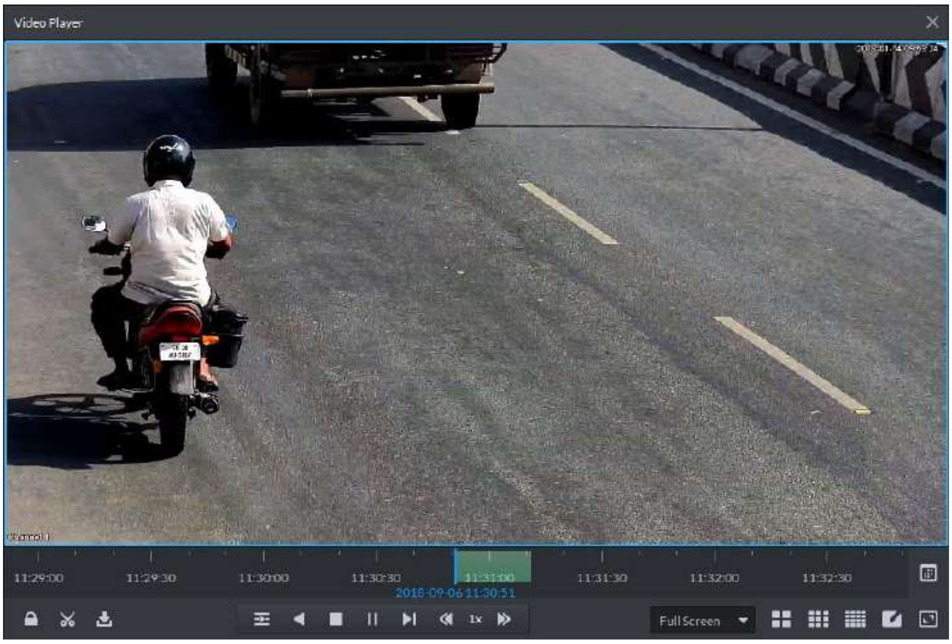
Figure 5-141 Zoom in



Vehicle Type: Small Car

- Click ⊙ to playback the 15-second video before and after the vehicle passed time. See Figure 5-142. The video file is total 30 seconds. Display the 15-second video before and after the vehicle passed.

Figure 5-142 Replay video



- Click to view the vehicle running track. Refer to 5.12.4 Vehicle Track for detailed information.
- Export: Select the passed vehicle information and then click **Export**, and export selected passed vehicle. Click **Export All**, and then export all searched passed vehicle information.

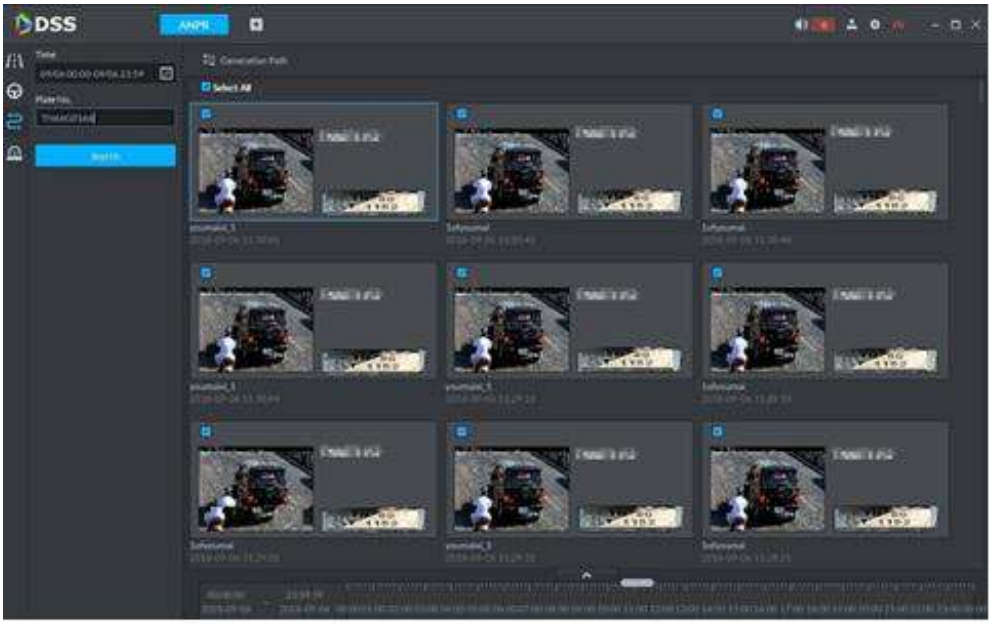
5.12.4 Vehicle Track

Step 1 Click , and system displays Road monitor interface.

Step 2 Select time and then input plate number. Click **Search**.

The system displays search result of vehicle track. See Figure 5-143.

Figure 5-143 Search result



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 5-144. Move the cursor to the middle to select the specified zone, you can zoom in it. See Figure 5-145.

Figure 5-144 Snapshot vehicle detail

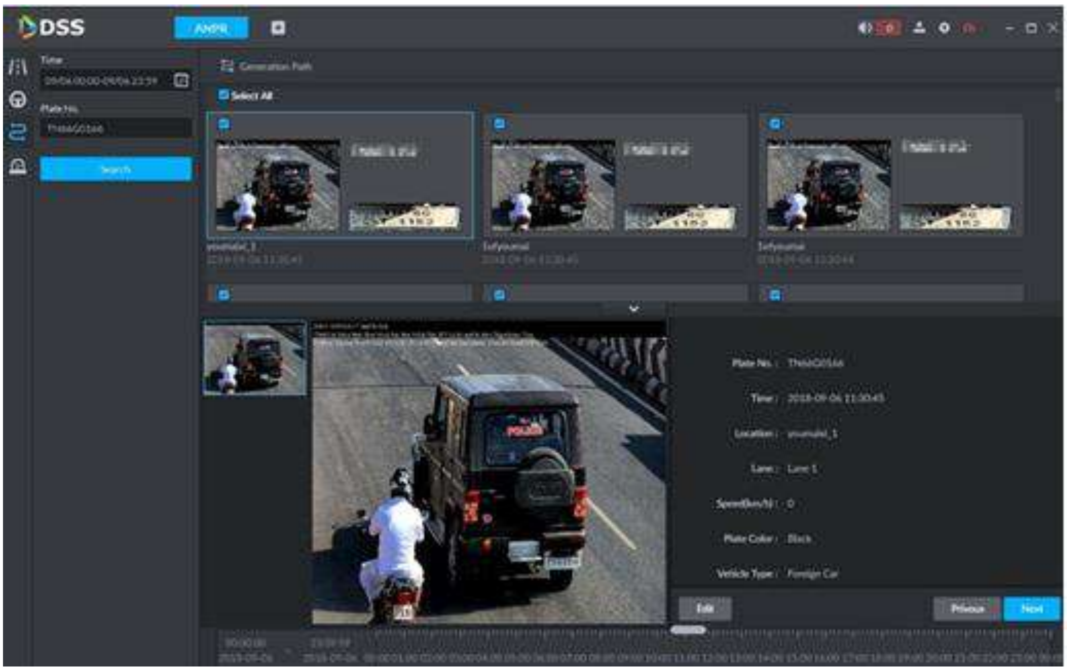


Plate No.: TN66G0166

Time: 2018-09-06 11:30:45

Location: youmulei_1

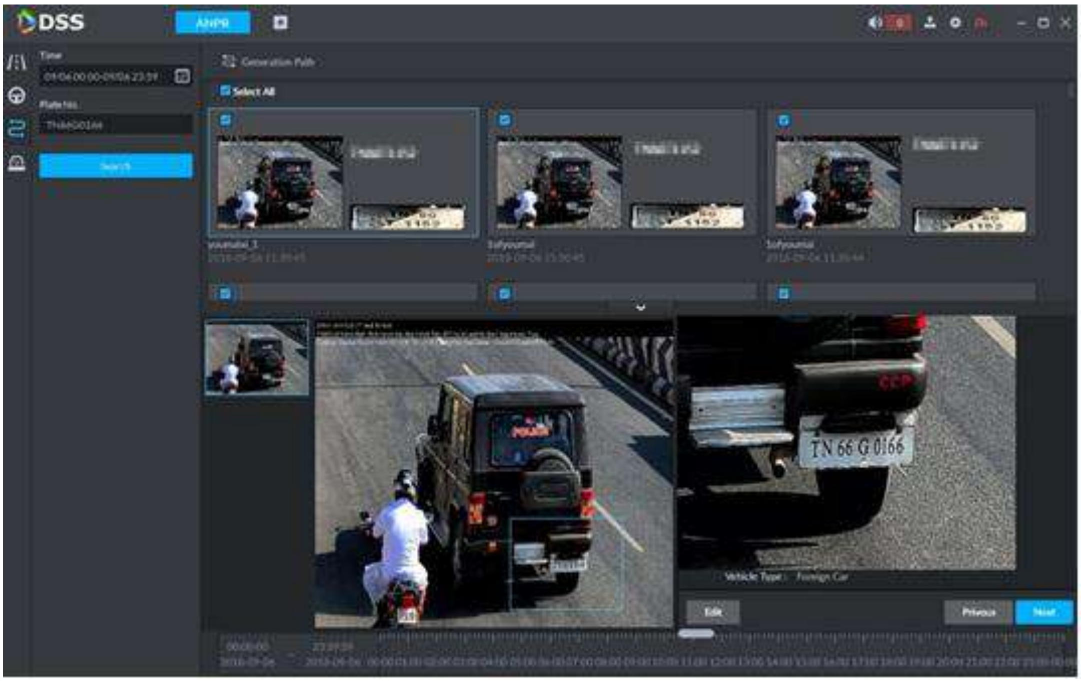
Lane: Lane 1

Speed(km/h): 0

Plate Color: Black

Vehicle Type: Foreign Car

Figure 5-145 Zoom in



- Click **Edit**, and you can 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 5-146.

Figure 5-146 Select specific time

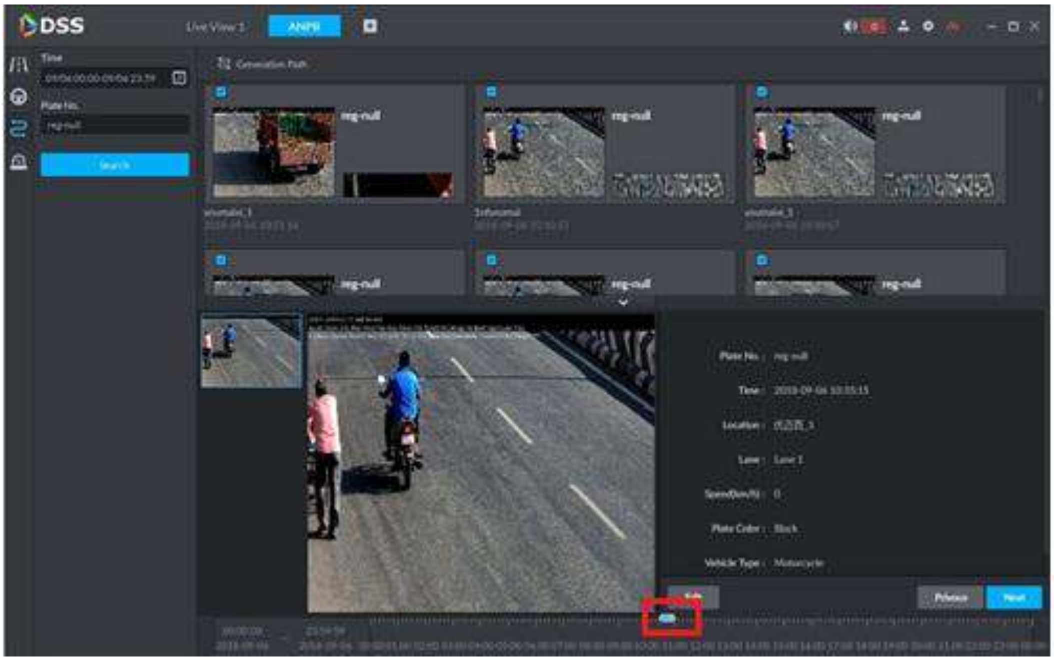


Plate No.: reg-null

Time: 2018-09-06 10:55:15

Lane: Lane 1

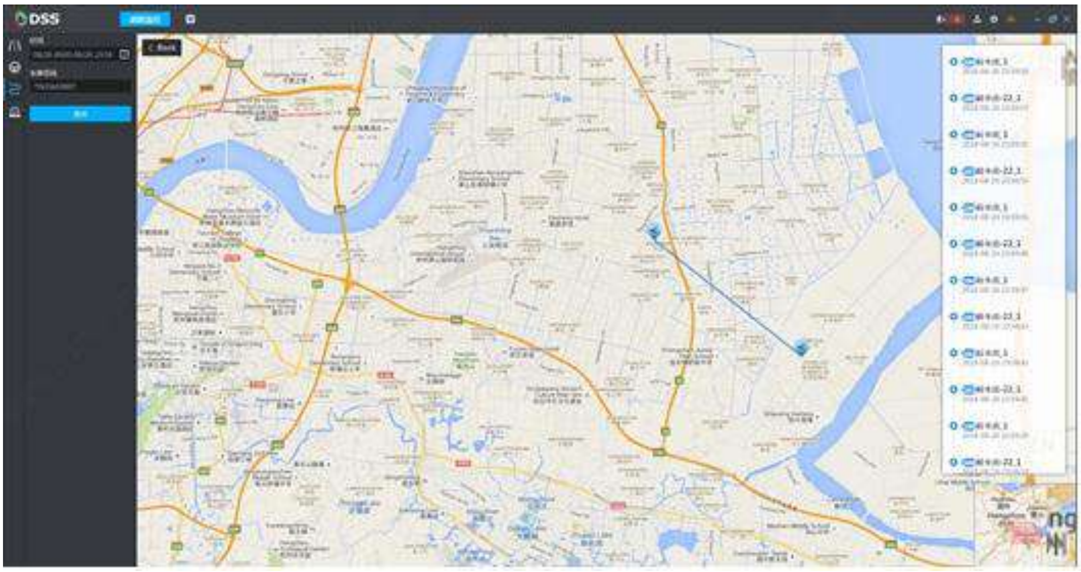
Speed(km/h): 0

Plate Color: Black

Vehicle Type: Motorcycle

- Select the snapshot image and then click the Generation path (track); you can view the vehicle track on the map. See Figure 5-147.

Figure 5-147 Vehicle track



5.12.5 Arm Record

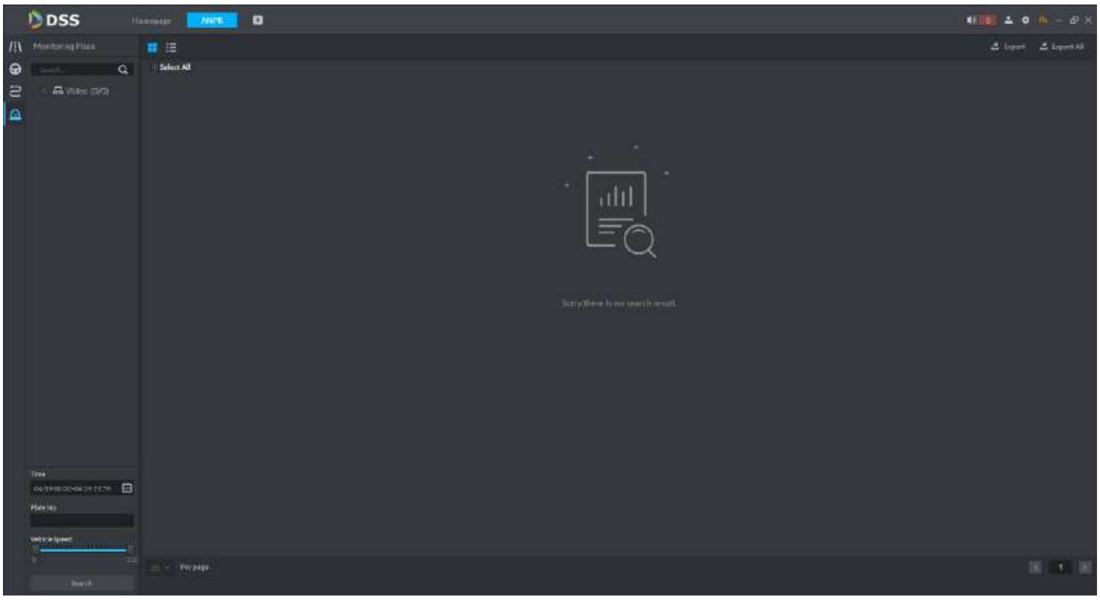
You can view and confirm the alarm information of vehicle arming.

Configure vehicle blacklist on manager, and then arming can be implemented by platform.

Step 1 Click .

The interface of **Arm Record** is displayed. See Figure 5-148.

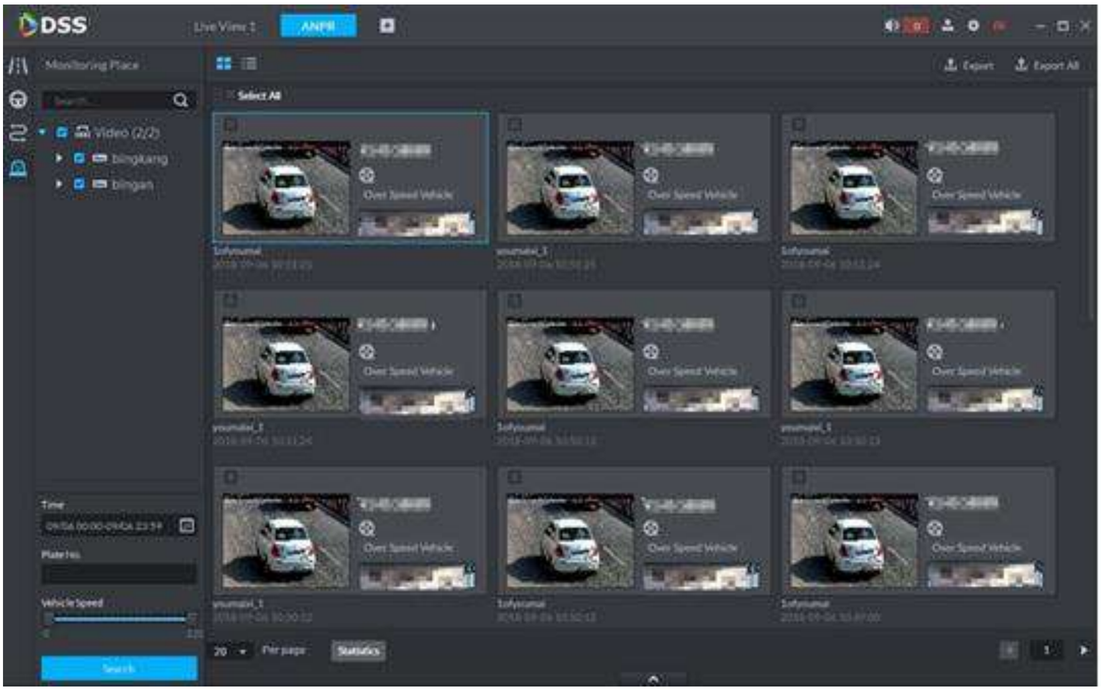
Figure 5-148 Arm Record



Step 2 Select device channel, and then set time, plate number, speed. Click **Search**.

System displays search result. See Figure 5-149.

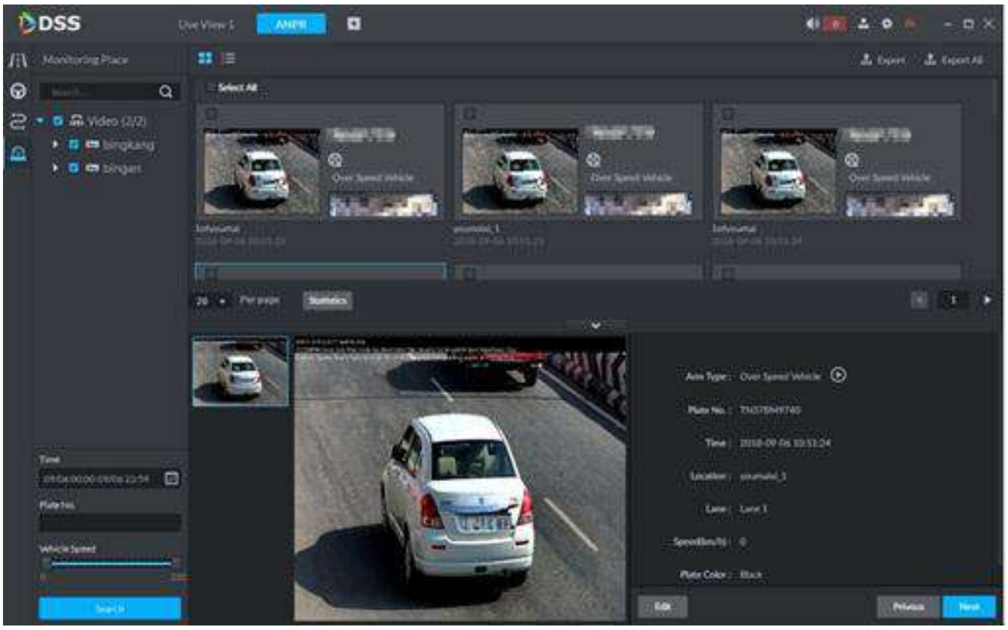
Figure 5-149 Search result of arm record



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 (☰), and 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 5-150. Move the cursor to the middle to select the specified zone, you can zoom in it. See Figure 5-151

Figure 5-150 Vehicle detail



Alm Type : Over Speed Vehicle

Plate No. : TN57BM9740

Time : 2018-09-06 10:51:24

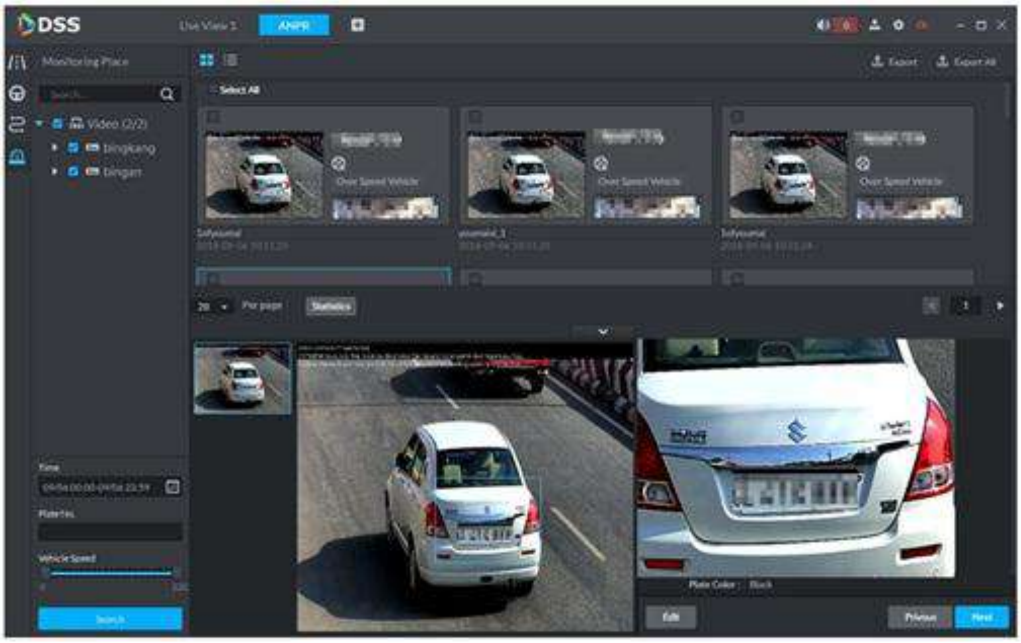
Location : sinumahl_1

Lane : Lane 1

Speed(km/h) : 0

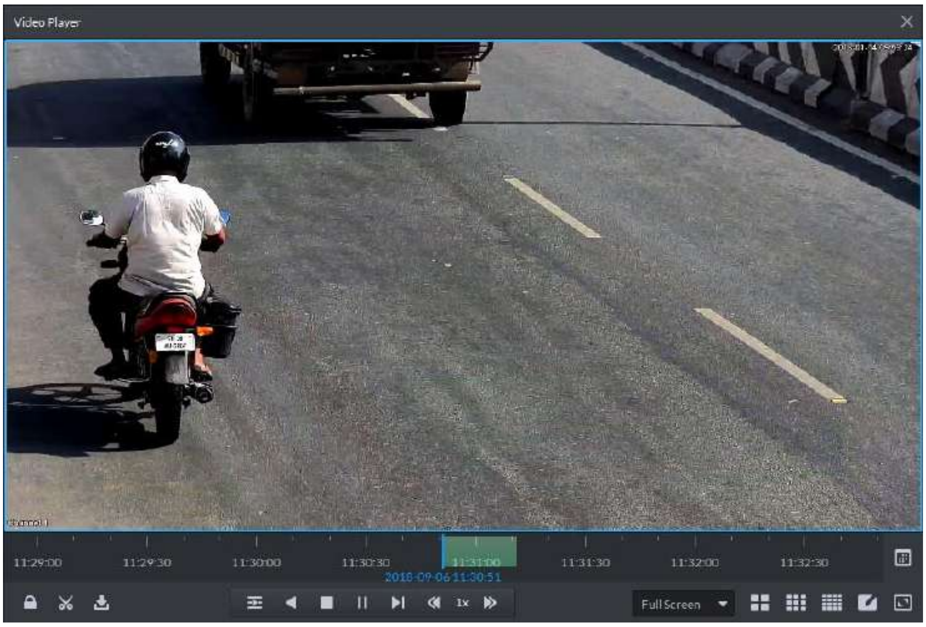
Plate Color : Black

Figure 5-151 Zoom in



- Click ⊙ to playback the 15-second video before and after the vehicle passed time. See Figure 5-152. The video file is total 30 seconds. Display the 15-second video before and after the vehicle passed.

Figure 5-152 Replay video



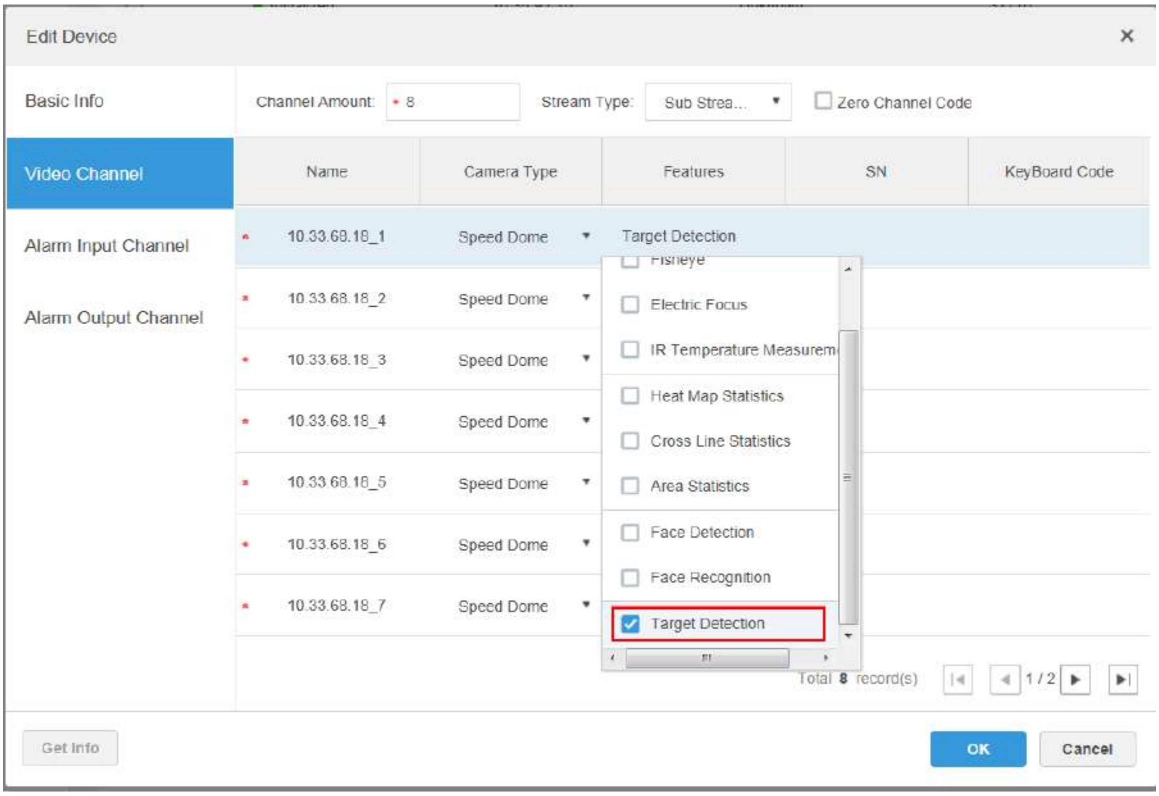
- Click to view the vehicle running track. Refer to 5.12.4 Vehicle Track for detailed information.
- Export: Select the passed vehicle information and click **Export,** then you can export selected monitor position information. Click **Export All**, and then you can export all monitor position information.

5.13 Object Detection

5.13.1 Preparations

- Cameras with structuring functions have been added to the platform's administrator end. See **4.5 Adding Device** for specific steps.
- After devices are added, click , and select **Target Detection** from the drop-down box. See Figure 5-153.

Figure 5-153 Modify channel



Edit Device ×

Basic Info

Video Channel

Alarm Input Channel

Alarm Output Channel

Channel Amount: * 8   Stream Type: Sub Strea... ▾   □ Zero Channel Code

	Name	Camera Type	Features	SN	KeyBoard Code
*	10.33.68.18_1	Speed Dome ▾	Target Detection		
*	10.33.68.18_2	Speed Dome ▾			
*	10.33.68.18_3	Speed Dome ▾			
*	10.33.68.18_4	Speed Dome ▾			
*	10.33.68.18_5	Speed Dome ▾			
*	10.33.68.18_6	Speed Dome ▾			
*	10.33.68.18_7	Speed Dome ▾			

□ Fisheye
□ Electric Focus
□ IR Temperature Measurem
□ Heat Map Statistics
□ Cross Line Statistics
□ Area Statistics
□ Face Detection
□ Face Recognition
☑ Target Detection

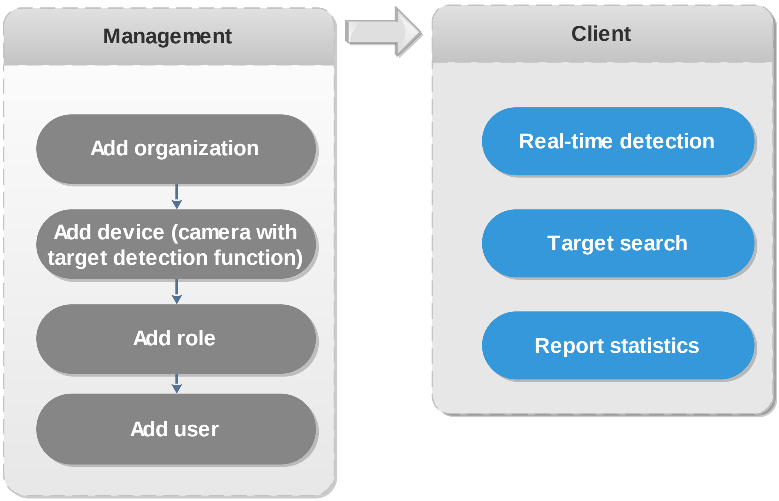
Total 8 record(s)   1 / 2

Get Info   OK   Cancel

- The video structuring IVS rules of the camera have been enabled. See the user manuals of cameras for detailed steps.

Target detection business flow is shown in Figure 5-154.

Figure 5-154 Business flow



5.13.2 View Real-time Detection

View the real-time snapshots captured by the cameras, including information about human, motorized vehicles, and non-motor vehicles:

Step 1 Click ⊞. On the **Homepage** interface, select **Object Detection**.

The **Target Detection** interface is displayed.

Step 2 Click .

The interface of **Real-time Detection** is displayed. See Figure 5-155 and Table 5-31.

Figure 5-155 Real-time video

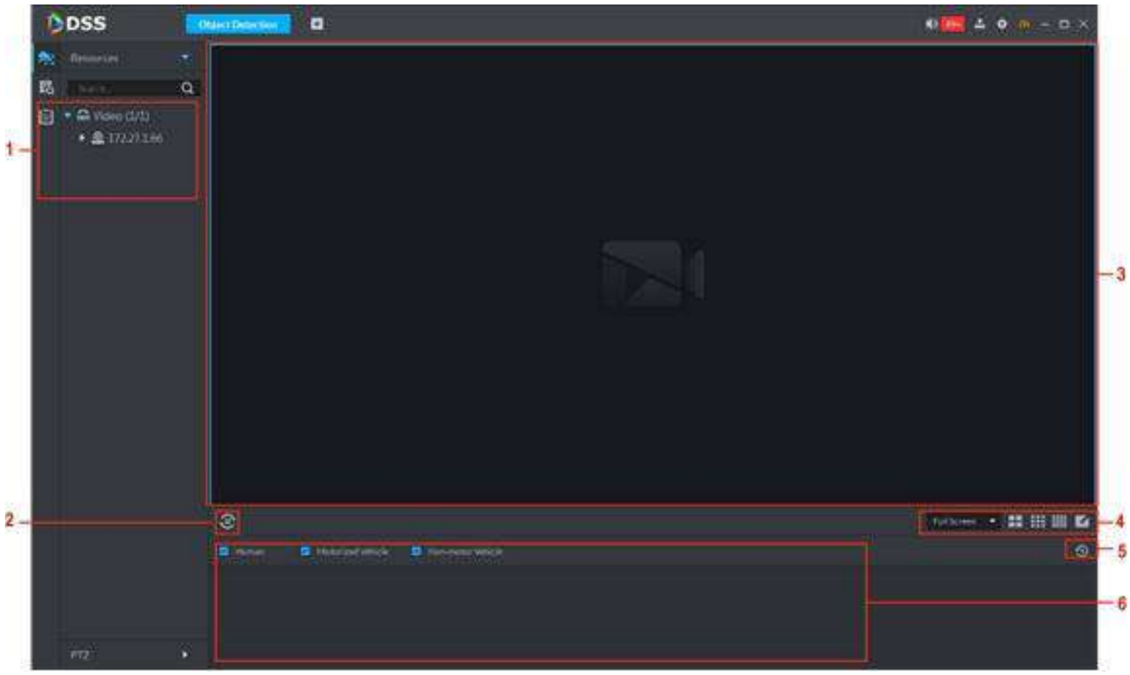


Table 5-31 Real-time video interface description

No.	Name		Description
1	Device Tree		Displays device information.
2	Pause Refresh/Start Refresh		● If the interface displays this icon▶, the snapshot display area does not refresh snapshots. Click this icon to refresh face snapshots in real time. ● If the interface displays this icon⏸, the snapshot display area refreshes face snapshots. Click this icon to stop refreshing snapshots.
3	Monitoring window		Displays the channel preview video. In the multi-window display mode, double-clicking a window switches to single window display. Another double-clicking returns to the original multi-window display mode.
4	全屏 ▾	Picture display ratio	Supports Full Screen and Original Scale modes. The Full Screen mode refers to the single window display in full screen.
	⊞ ⊞ ⊞ ✎	Number of windows	Supports switching the number of display windows, and you can customize the numbers.
5	The button that allows for jumping to the Report Statistics interface.		Click this icon to jump to the Report Statistics interface.
6	Snapshot display area		Displays the captured face snapshots.

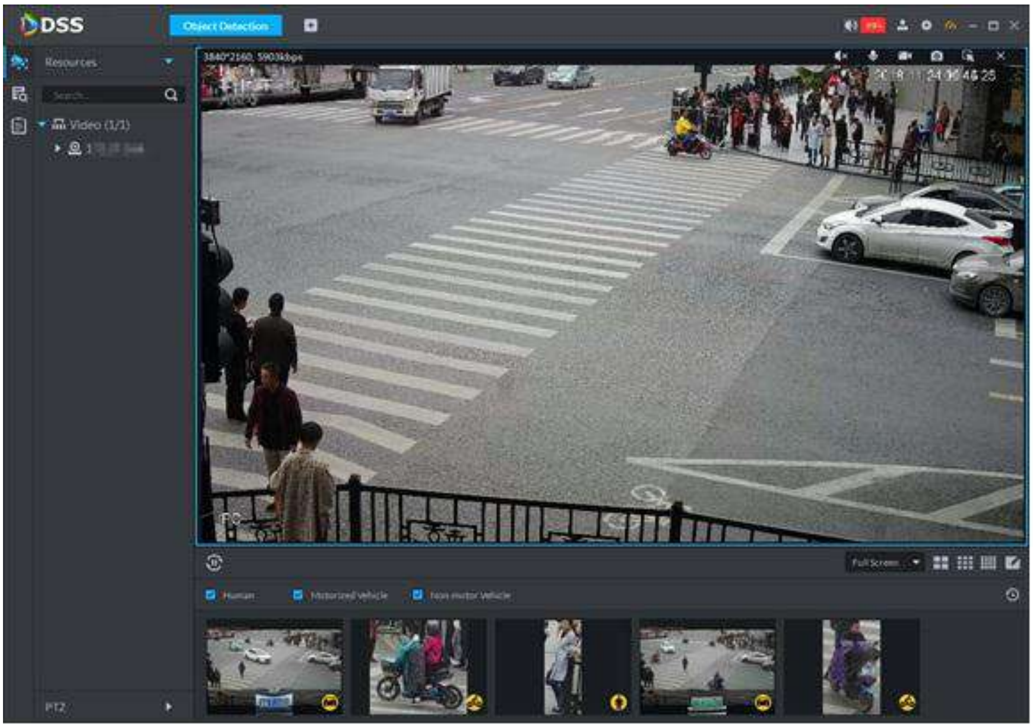
Step 3 Enable video preview.

- Select the monitoring window (a white frame means the window has been selected), and double-click any channel or video recording to enable real-time monitoring.

- Drag the channel or video recording to the monitoring window.

Enable the video preview display. See Figure 5-156. The snapshot display area displays snapshots in real time.

Figure 5-156 Video preview

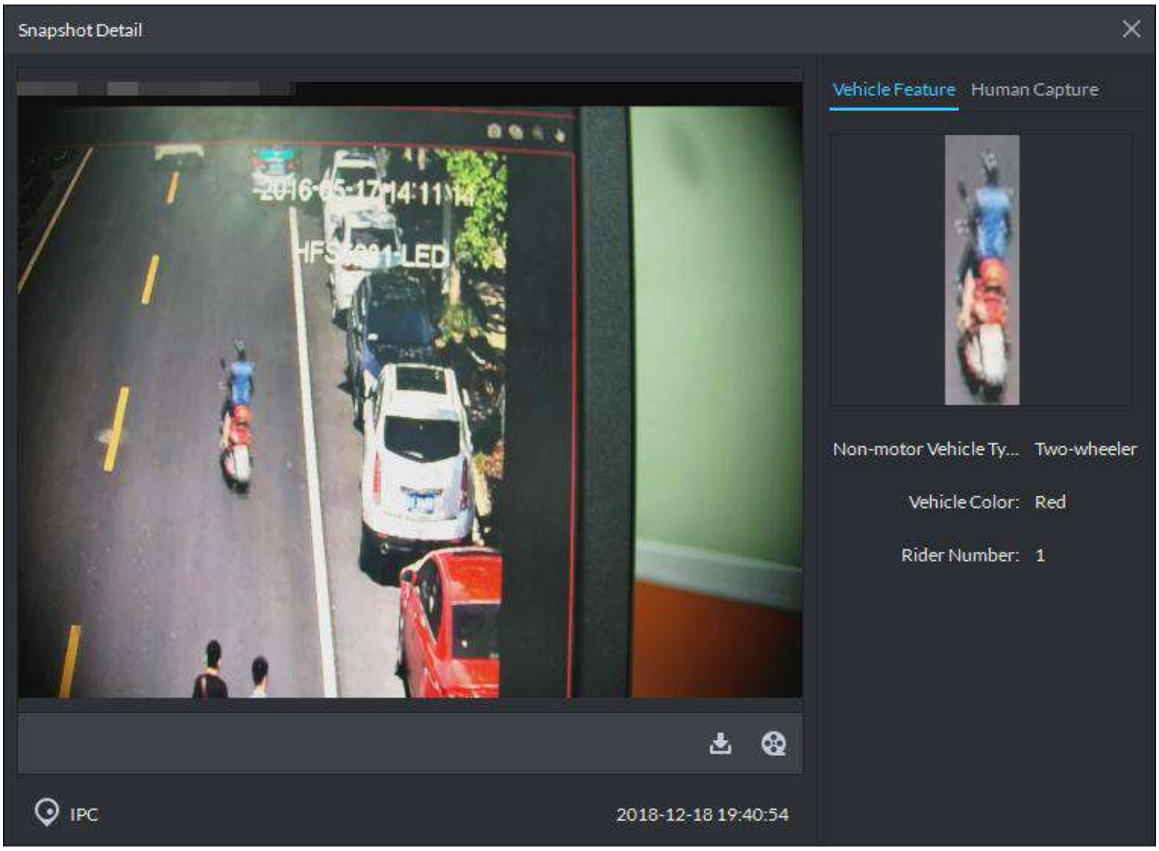


Step 4 Double-click the snapshot.

The **Snapshot Detail** interface is displayed. See Figure 5-157 and Table 5-32.

- Human snapshots display body cutout, types of tops, colors of tops, types of bottoms, colors of bottoms, carrying bags or not, wearing caps or not, and the gender. If faces are recorded, the system displays face snapshots, age, and facial expression, wearing glasses or face masks. You can zoom in any part of the human body image, jump to the search interface, and view the recordings. You can quickly jump to search by image for human faces.
- Motorized vehicle snapshots display the panoramic view of vehicles, vehicle type, vehicle color, license plate color, and logo. You can view license plate snapshots, play linked videos and zoom in specified parts of the vehicle image.
- Non-motor vehicle snapshots display the panoramic view, vehicle type, vehicle color, and the number of persons involved.

Figure 5-157 Snapshot detail



Snapshot Detail

Vehicle Feature Human Capture

Non-motor Vehicle Ty... Two-wheeler

Vehicle Color: Red

Rider Number: 1

IPC

2018-12-18 19:40:54

Table 5-32 Operation description

Operation	Description
Download	Click ⤓ and save .rar files in the specified path.
Playback	Click ⊛ to play back the video recordings timed before and after the snapshot.

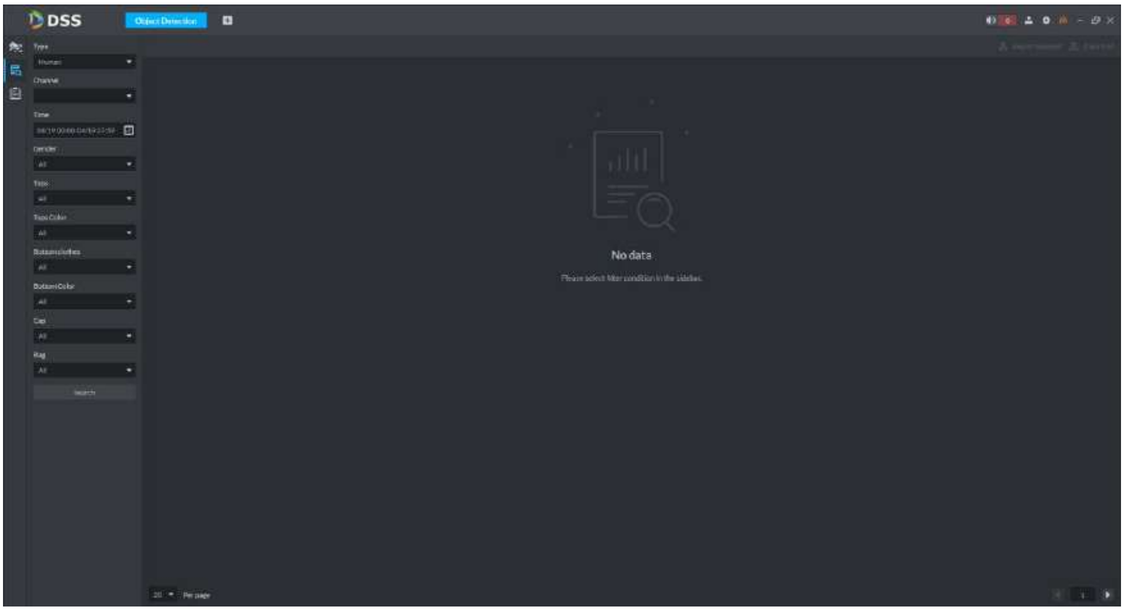
5.13.3 Object Search

Search needed snapshot target from database quickly by setting conditions.

Step 1 On the **Object Detection** interface, click .

The **Object Search** interface is displayed. See Figure 5-158.

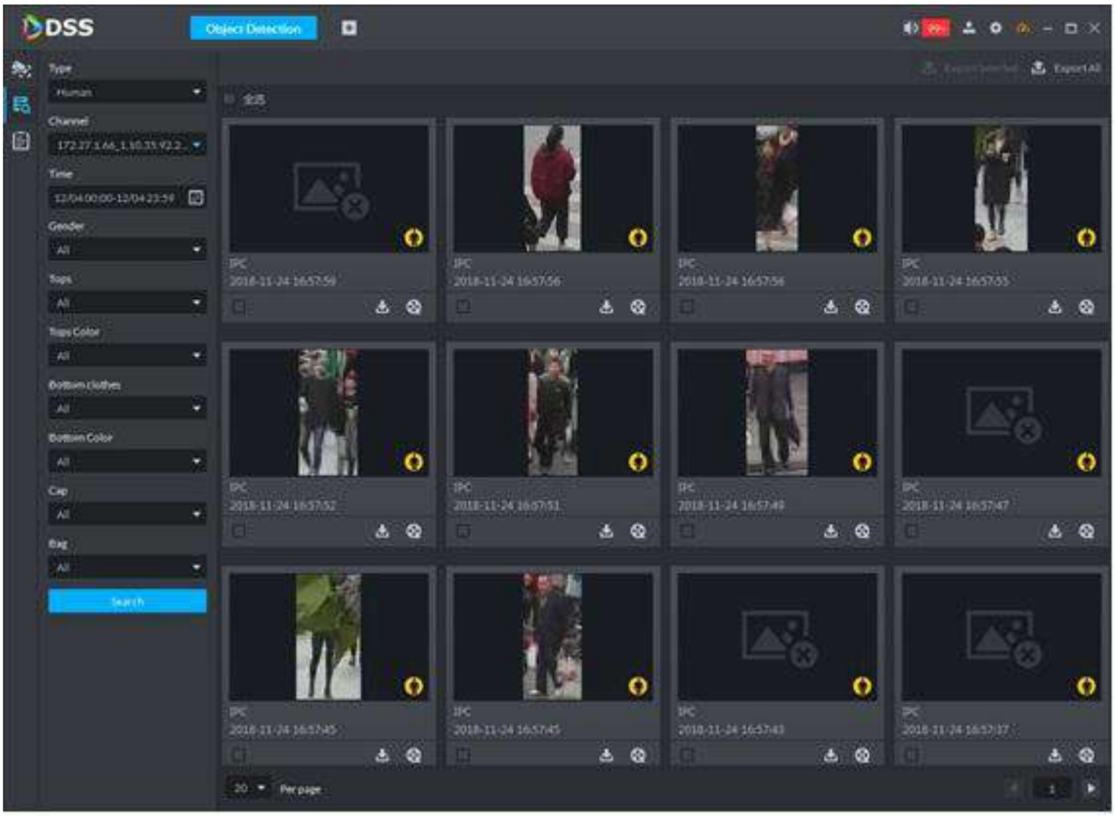
Figure 5-158 Search object



Step 2 Set up search condition and click **Search**.

The system displays search results. See Figure 5-159.

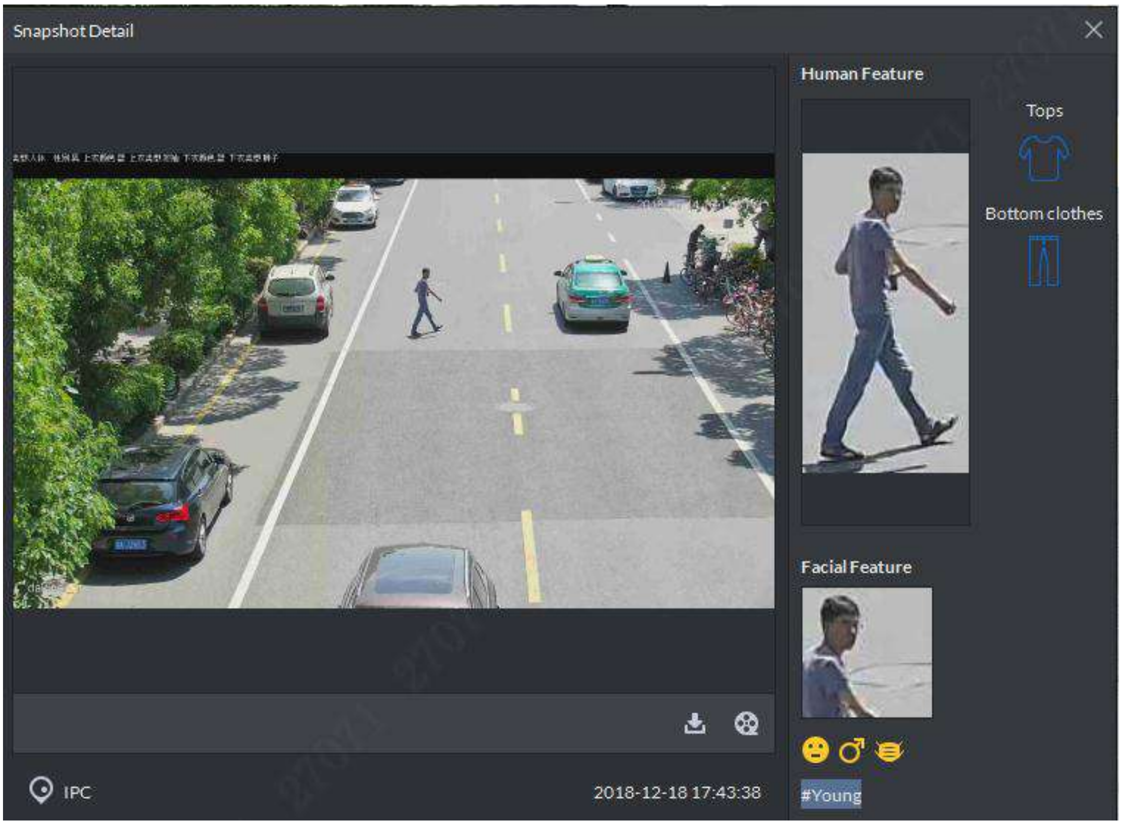
Figure 5-159 Search result



Step 3 Double-click the snapshot.

The **Snapshot Detail** interface is displayed. See Figure 5-160.

Figure 5-160 Snapshot detail

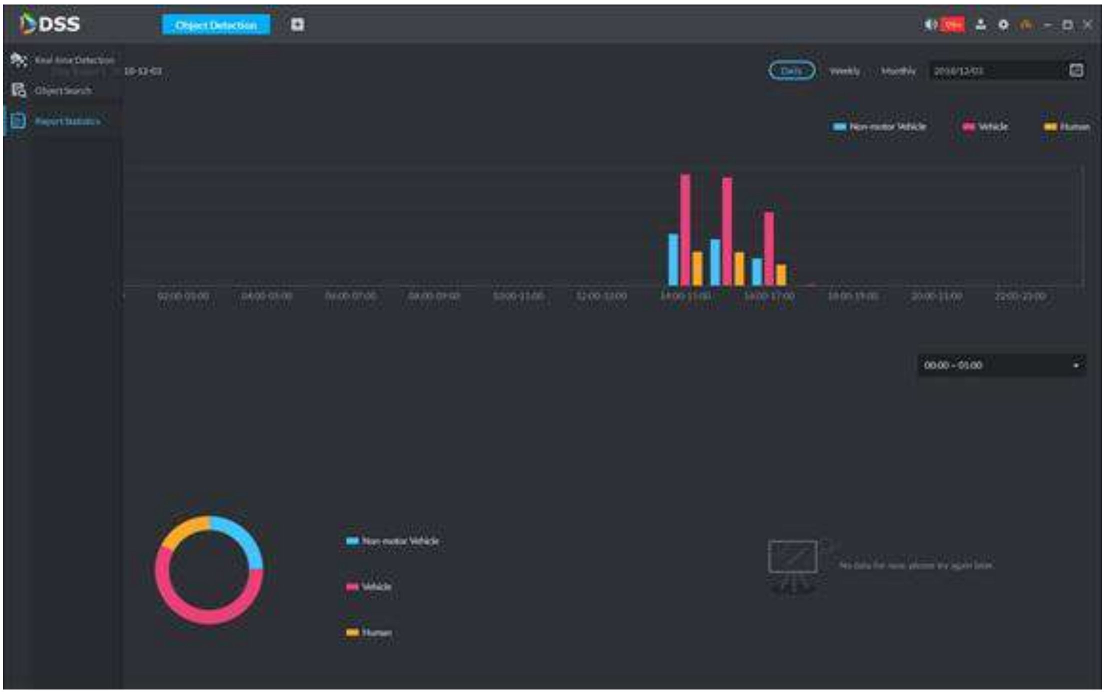


5.13.4 Statistics Report

Step 1 On the **Object Detection** interface, click ▤.

The **Report Statistics** interface is displayed. See Figure 5-161.

Figure 5-161 Report statistics

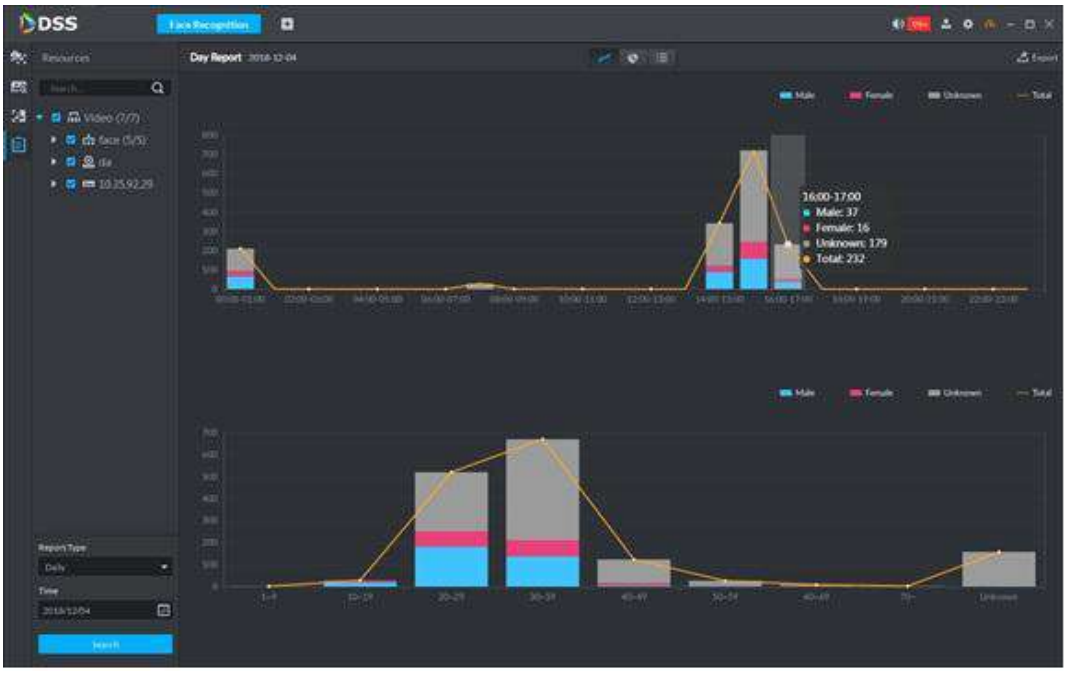


No data for now, please try again later.

Step 2 Set statistics condition.

The system displays statistics results. See Figure 5-162.

Figure 5-162 Statistics report



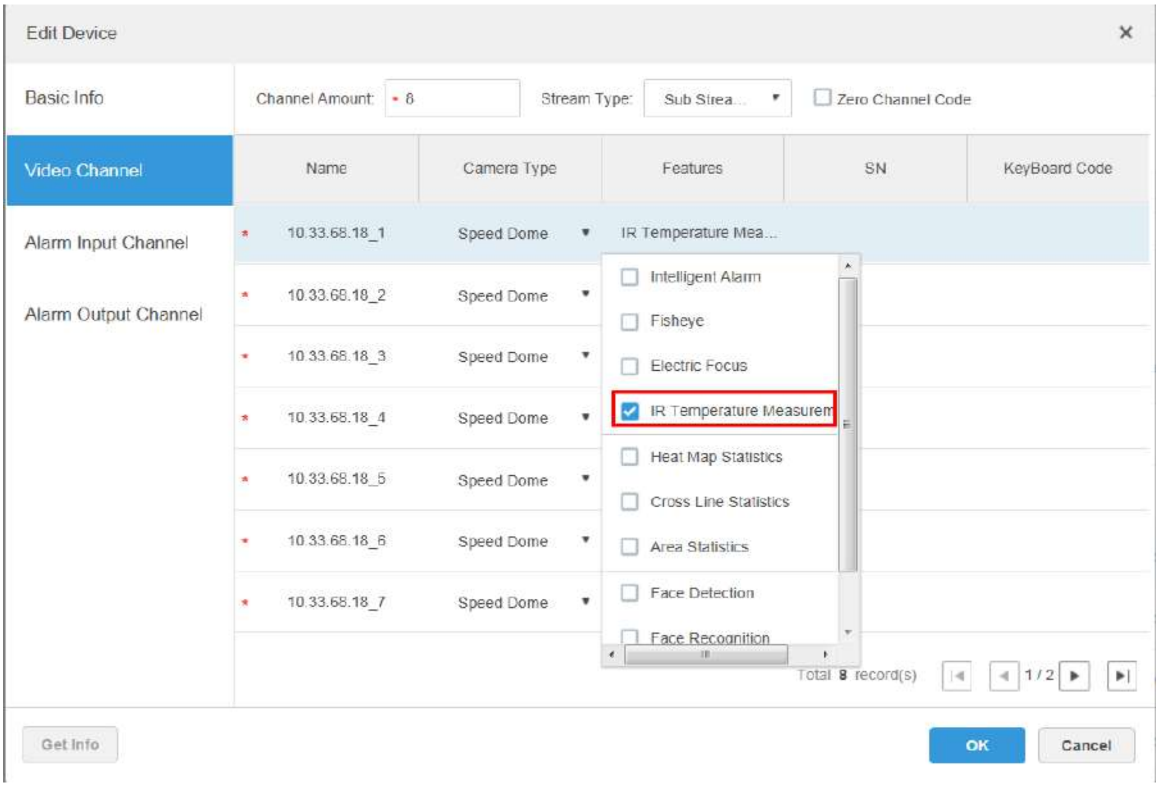
5.14 Thermal

The system comes with a thermal device management module. With a connected thermal camera, you can measure the in-video temperature, analyze local heatmap, and manage the thermal device alarms in real time.

5.14.1 Preparations

- An encoding device with a **Device Type** of **IPC** has been added in **Device Management** on the platform's administrator end. See **4.5 Adding Device** for specific steps.
- After the device is added, click ✎, and select **IR Temperature Measurement** from the Features drop-down box. See Figure 5-163.

Figure 5-163 Modify channel capacity set



Edit Device ×

Basic Info

Video Channel

Alarm Input Channel

Alarm Output Channel

Channel Amount: * 8 Stream Type: Sub Strea... ▾ □ Zero Channel Code

	Name	Camera Type	Features	SN	KeyBoard Code
*	10.33.68.18_1	Speed Dome ▾	IR Temperature Mea...		
*	10.33.68.18_2	Speed Dome ▾			
*	10.33.68.18_3	Speed Dome ▾			
*	10.33.68.18_4	Speed Dome ▾			
*	10.33.68.18_5	Speed Dome ▾			
*	10.33.68.18_6	Speed Dome ▾			
*	10.33.68.18_7	Speed Dome ▾			

- □ Intelligent Alarm
- □ Fisheye
- □ Electric Focus
- ☑ IR Temperature Measurem
- □ Heat Map Statistics
- □ Cross Line Statistics
- □ Area Statistics
- □ Face Detection
- □ Face Recognition

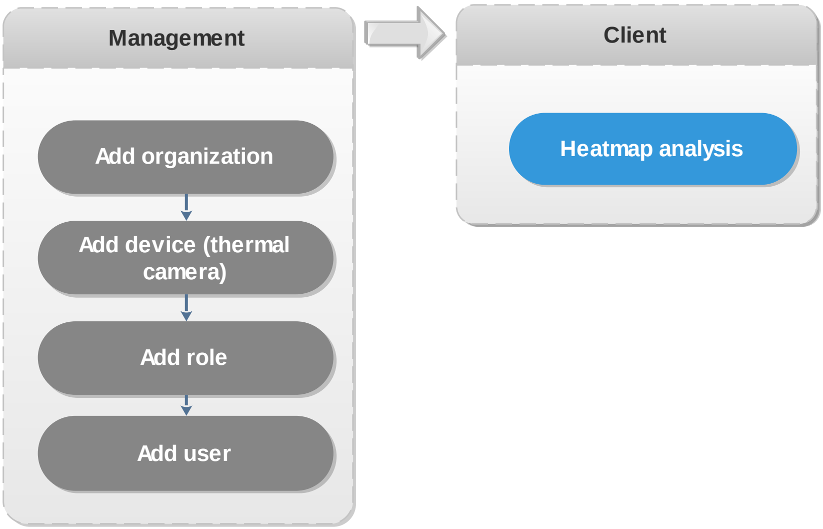
Total 8 record(s) 1 / 2

Get Info OK Cancel

- To collect temperature values in real time, the added thermal device must be able to measure temperatures.

The thermal config procedures are shown in Figure 5-164.

Figure 5-164 Thermal config flow



5.14.2 Interfaces and Functions

On the **Homepage**, click +. On the **New Tab** interface, select **Thermal**, and the **Thermal** interface is displayed. See Figure 5-165. For interface descriptions, see Table 5-33.

Figure 5-165 Thermal

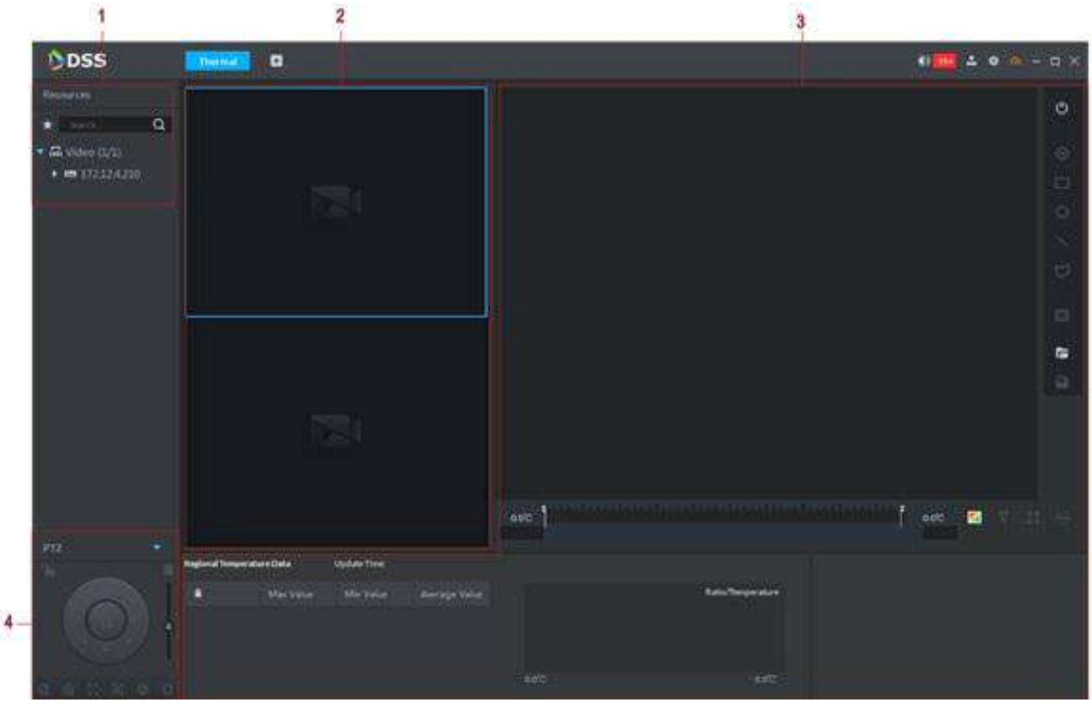
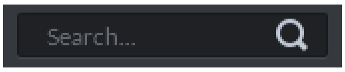


Table 5-33 IR temperature measurement

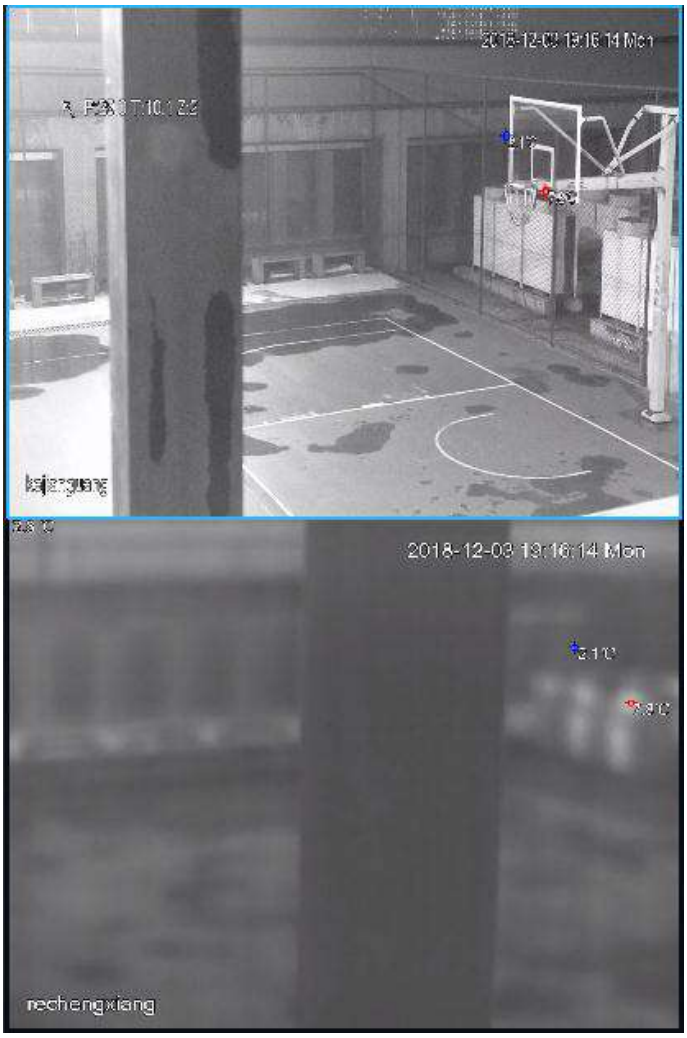
No.	Module name	Description
1	Device Tree	● If in **Local Config** > **Basic Setting**, you select **Show device node**, the Device Tree shows the device and the channels under it. If the selection is undone, channels of all devices are displayed. ● Supports searching and querying in  by organization name, device name, or channel name.
2	Preview	You can preview channel videos. Drag the channel to the window or select the window and double-click a channel to open videos of corresponding channels.
3	Heatmap	The heatmap is formed by capturing the temperature value of each pixel point on the thermal image and can be analyzed on the client. See 5.14.4 Heatmap Analysis for specific steps.
4	PTZ Control	To control the PTZ or speed dome, rotate the device to zoom in/out, change focus and adjust aperture.

5.14.3 Preview

You can preview the images of each video channel, turning on/off audios, video recordings, or capturing pictures.

You can drag the video channel in the Device Tree to the Preview section, and the system displays videos of the channel. Click any point on the video to measure temperature in real time. See Figure 5-166.

Figure 5-166 Open video channel



When you place the mouse on any of the preview interfaces, the window menu is displayed above the interface. See Figure 5-167 and Table 5-34.

Figure 5-167 Video preview window menu

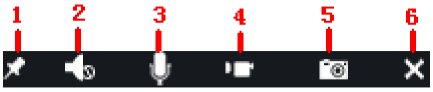


Table 5-34 Menu description

No.	Icon name	Description
1	Real-time Tagging	● If in **Local Config** > **Basic Setting**, you select **Silent Real-time Tagging**, the Tagging dialog box does not display at the time of real-time tagging. ● If Silent Real-time Tagging is not selected, you can edit the tag name.
2	Audio	Turn on or off audio.
3	Intercom	Turn on or off audio talks.
4	Local Record	Click this icon and the system begins recording a local video. Clicking this icon again stops recording and the recorded video file is stored locally.

No.	Icon name	Description
5	Snapshot	Click this icon and the system takes snapshots automatically.
6	Off	Click this icon to turn off this video channel.

5.14.4 Heatmap Analysis

Heatmap of devices can be obtained on the client. The heatmap analysis tools available on the client can generate temperature values and the ratio of each temperature value on the heatmap. You can also select one or more monitored regions on the heatmap. The tools can calculate the max temperature, min temperature, and average temperature within a region, and also temperature differences.

The heatmap and analysis tool interface is shown in Figure 5-168. For interface descriptions, see Table 5-35.

Figure 5-168 Heatmap

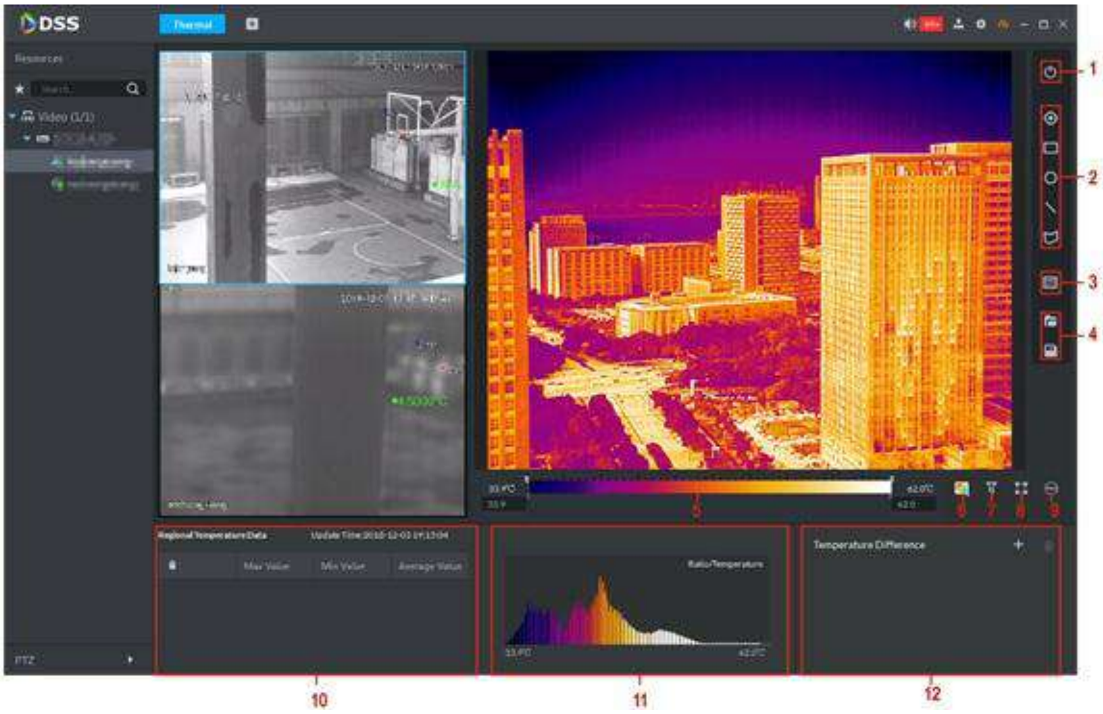


Table 5-35 Heatmap interface description

No.	Module name	Description
1	Query heatmap	You can obtain heatmap manually.
2	Draw a region	You can draw a region on the heatmap to measure the temperature. The region can be a point, a rectangle, a circle, a line segment, or a polygon. See 5.14.4.2Regional Temperature for specific steps.
3	Mode	Not supported for now.
4	File processing	You can import heatmap processing files (.dtp) to the client for analysis, or generate heatmap analysis reports. See 5.14.4.4 File processing for specific steps.

No.	Module name	Description
5	Temperature display	Generates a bar reflecting the color changes corresponding to different temperature values, based on the rendering plan selected in the heatmap. The data at the two ends defines the temperature range in the heatmap. ● Temperature-color correlation: When the mouse is placed at a color spot, the temperature of the color spot is displayed. ● Enhanced temperature comparison display: After inputting temperature values in the boxes at the two ends of the bar, the heatmap only displays the colors of the regions within this temperature range. Regions with temperatures below the preset min value are displayed in the leftmost color on the bar; regions with temperatures above the preset max value are displayed in the rightmost color on the bar.

No.	Module name	Description
6	Rendering Plan	Click to color the infrared image. 14 color plans are available. ● White-heat: In gray-scale images, the parts with higher temperature are brighter. ● Black: In gray-scale images, the parts with lower temperature are brighter. ● Purple-yellow: Colors mostly fall within the purple-red-yellow range. The parts with lower temperatures are purpler, and higher temperatures more yellow. ● Rainbow: Colors mostly fall within the blue-green-red-yellow range. The parts with lower temperatures are bluer, and higher temperatures more yellow. ● Red-yellow: Colors mostly fall within the red-yellow range. The parts with lower temperatures are redder, and higher temperatures more yellow. ● Blue-yellow: Colors mostly fall within the blue-purple-red-yellow range. The parts with lower temperatures are bluer, and higher temperatures more yellow. ● Iron red: Similar colorway to the Blue-yellow plan but less bright. ● Amber: Mainly dark brown. The parts with higher temperatures are brighter. ● Jade: Colors mostly fall within the purple-red-yellow-green-blue range. The parts with lower temperatures are purpler, and higher temperatures bluer. ● Sunset: Colors mostly fall within the blue-red-yellow range. The parts with lower temperatures are bluer, and higher temperatures more yellow. ● Red and Blue: In colored images, objects with higher temperatures are displayed in red, and those with lower temperatures are displayed in blue. Usually used to give warnings. ● Oil painting: Colors mostly fall within the purple-blue-green-yellow-red range. The parts with lower temperatures are purpler, and higher temperatures redder. ● Pomegranate: Mainly burgundy. The parts with higher temperatures are brighter. ● Emerald: Mainly azure green. The parts with higher temperatures are brighter. The default setting is White-heat.
7	Temperature Filter	Filters the temperatures on the heatmap. You can set up a temperature range. The heatmap within this temperature range is displayed in other colors. See 5.14.4.3 Temperature Filter for specific steps.

No.	Module name	Description
8	Select isothermal region	The isothermal lines are mainly used to highlight some parts of the image. The temperature range is around a median temperature, between an upper limit and a lower limit. Those above the lower limit appear in bright colors, and those below the lower limit appear in black & white. See 5.14.4.3 Temperature Filter for specific steps.
9	Auto	Click to delete the isothermal regions already drawn.
10	Regional Temperature Data	On the heatmap, select a region (except for points). The table displays the max temperature, min temperature, and average temperature of the selected region. See 5.14.4.2 Regional Temperature for specific steps.
11	Temperature ratio	It displays the ratios of various temperature values on the heatmap intuitively.
12	Temperature Difference	The differences of max temperature, min temperature, and average temperature within the same region or across different regions can be calculated. See 5.14.4.2 Regional Temperature for specific steps.

5.14.4.2 Regional Temperature

Draw a detection region on the heatmap and you can see the max temperature, min temperature, and average temperature in this region on the client. After adding multiple regions on the heatmap, you can compare the temperature differences across multiple regions.

Draw a Region and Measure the Temperature

Step 1 In the region drawing section, select a shape and draw on the heatmap. See Figure 5-169.

The Regional Temperature Data section is automatically updated with the max temperature, min temperature, and average temperature of the region. See Figure 5-170.

- Place the mouse near the edge of the region. When the mouse changes into ⤡, moving the mouse changes the size of the regular region.
- Place the mouse within the region. When the mouse changes into ✥, moving the mouse changes the position of the regular region.
- Delete a single regular region: Select a region in Regional Temperature Data section, or a regular region on the heatmap. Right-click and select **Delete** to delete the corresponding regular region.
- Delete all regular regions: In Regional Temperature Data section, click🗑, or select any regular region, right-click and select Delete All to delete all regular regions.

Figure 5-169 Draw area

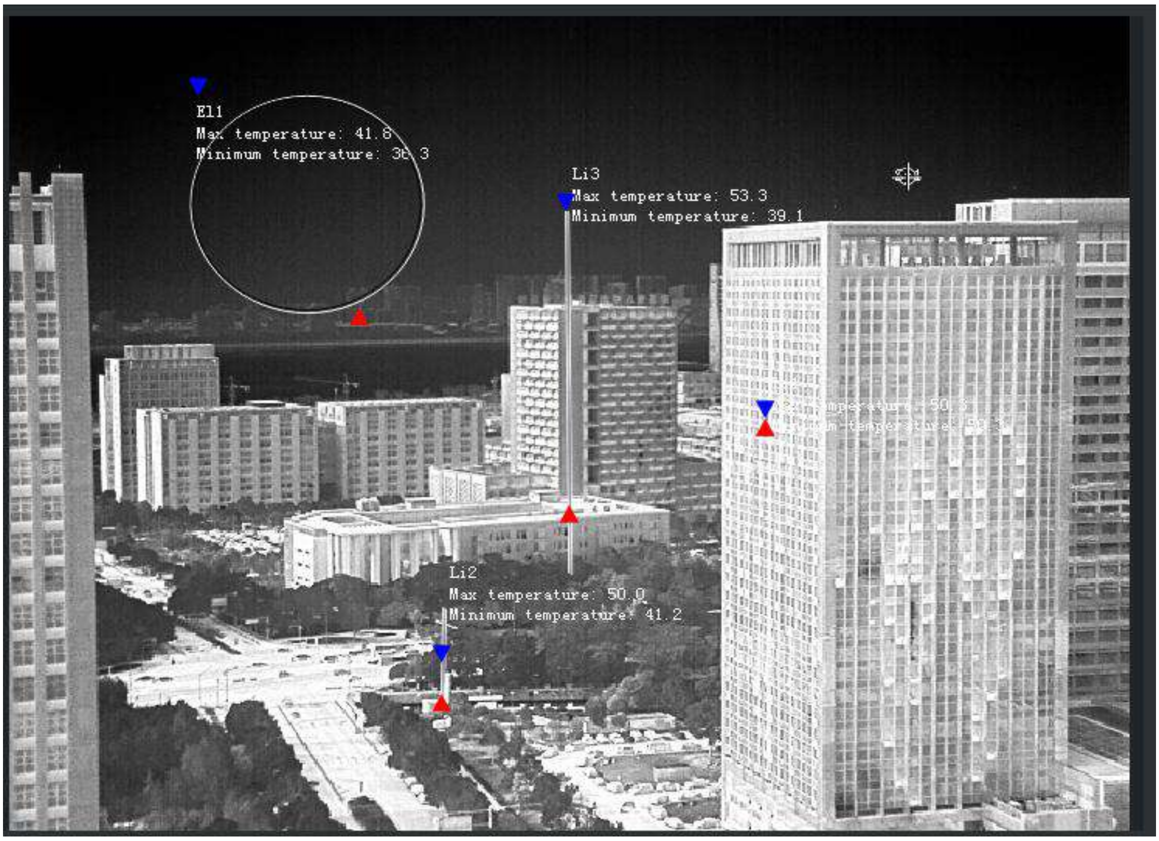
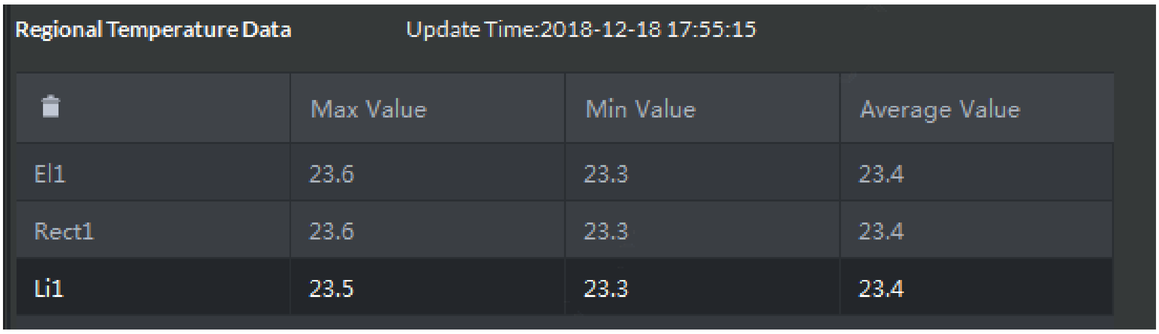


Figure 5-170 Regional temperature data



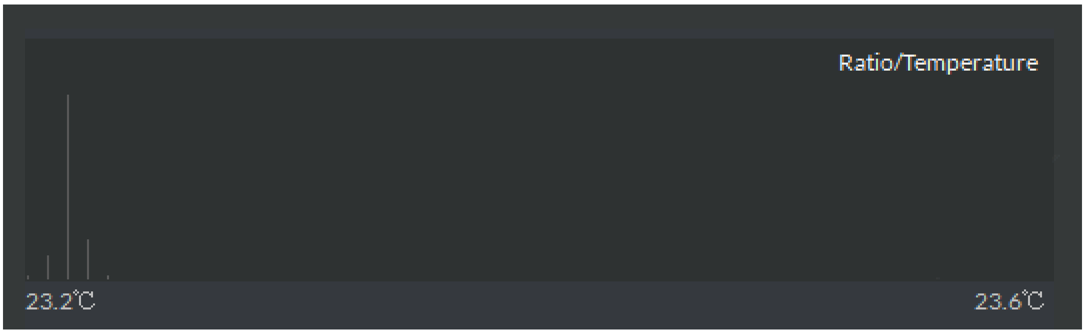
Regional Temperature Data　　Update Time:2018-12-18 17:55:15

🗑	Max Value	Min Value	Average Value
El1	23.6	23.3	23.4
Rect1	23.6	23.3	23.4
Li1	23.5	23.3	23.4

Step 2 Click any temperature data.

Temperature ratios of the region can be displayed in the gradient graph on the side. Place the mouse on the graph and the temperature range and its ratio on the heatmap can be displayed. See Figure 5-171.

Figure 5-171 Temperature ratio



Temperature Difference

📖

You can set max 100 rules of temperature difference calculation.

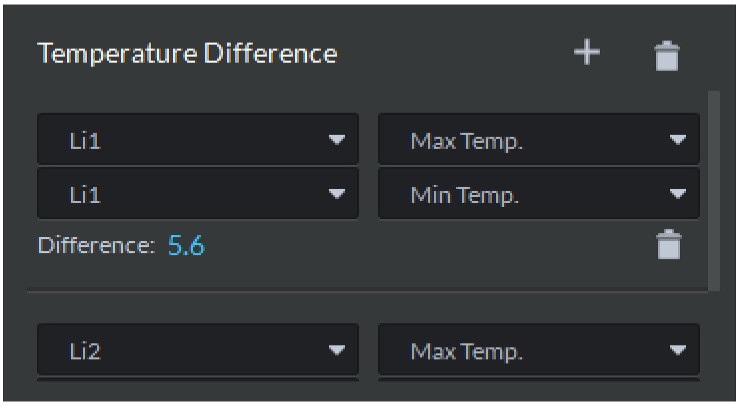
Step 1 Click + in the **Temperature Difference** section to add rules for calculating the temperature difference.

The system displays the added temperature difference calculation contents. See Figure 5-172.

📖

- Click 🗑 on the right side of + to delete all temperature difference calculation rules.
- Click 🗑 on the right side of each difference to delete the corresponding temperature difference calculation rule.

Figure 5-172 Add rule



Temperature Difference + 🗑

Li1 ▾ Max Temp. ▾
Li1 ▾ Min Temp. ▾
Difference: 5.6 🗑

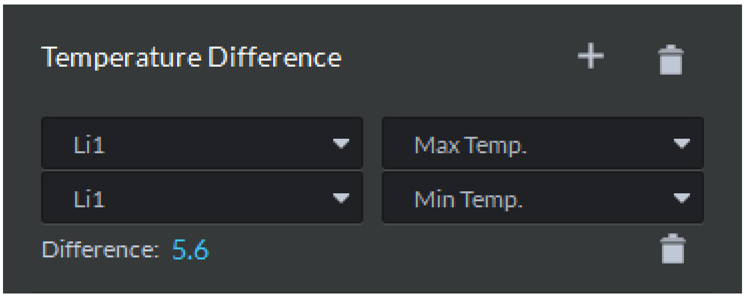
Li2 ▾ Max Temp. ▾

Step 2 Click the dropdown box on the left side and select regions that have been set up, such as Li1, El1.

Step 3 Click the dropdown box on the right side and select the temperature to be compared with, such as the Max Temp., Min Temp., or Average Temp.

The system automatically calculates the temperature difference. See Figure 5-173.

Figure 5-173 Calculation



Temperature Difference + 🗑

Li1 ▾ Max Temp. ▾
Li1 ▾ Min Temp. ▾
Difference: 5.6 🗑

5.14.4.3 Temperature Filter

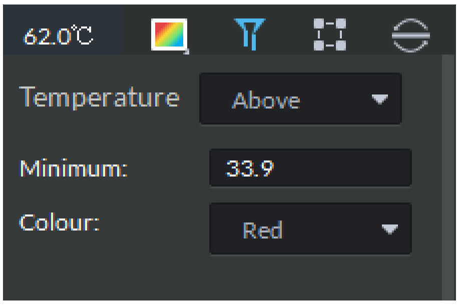
Temperature Filter

Set temperature limits, and select and highlight regions that fall within the limits on the heatmap.

Step 1 Click 🝖 to enable temperature filter.

The Temperature Filter interface is shown in Figure 5-174.

Figure 5-174 Temperature filter



62.0℃

Temperature: Above

Minimum: 33.9

Colour: Red

Step 2 Select the temperature filtering criteria. Available options include Above, Below, or Between.

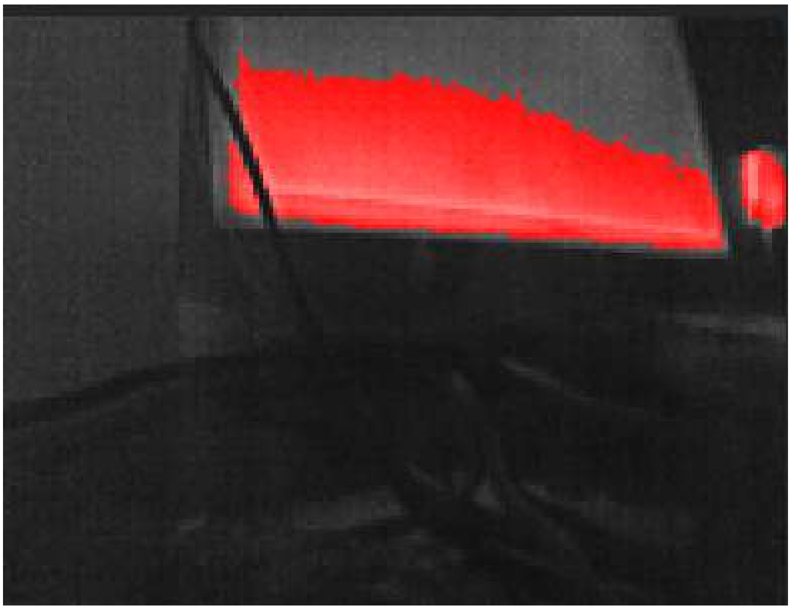
Step 3 Input the temperature limits and set up colors.

The client displays the temperature filtering results. See Figure 5-175.

📖

- When Above or Below is selected as the filtering criteria, just fill in one value as the limit.
- When Between is selected, fill in both the upper limit and the lower limit.

Figure 5-175 Temperature filter result



Select isothermal region

The isothermal region is mainly used to highlight some objects in the image. With the drawn isothermal region as the benchmark, regions with higher temperatures display in bright colors, and those with lower temperatures display in dark colors.

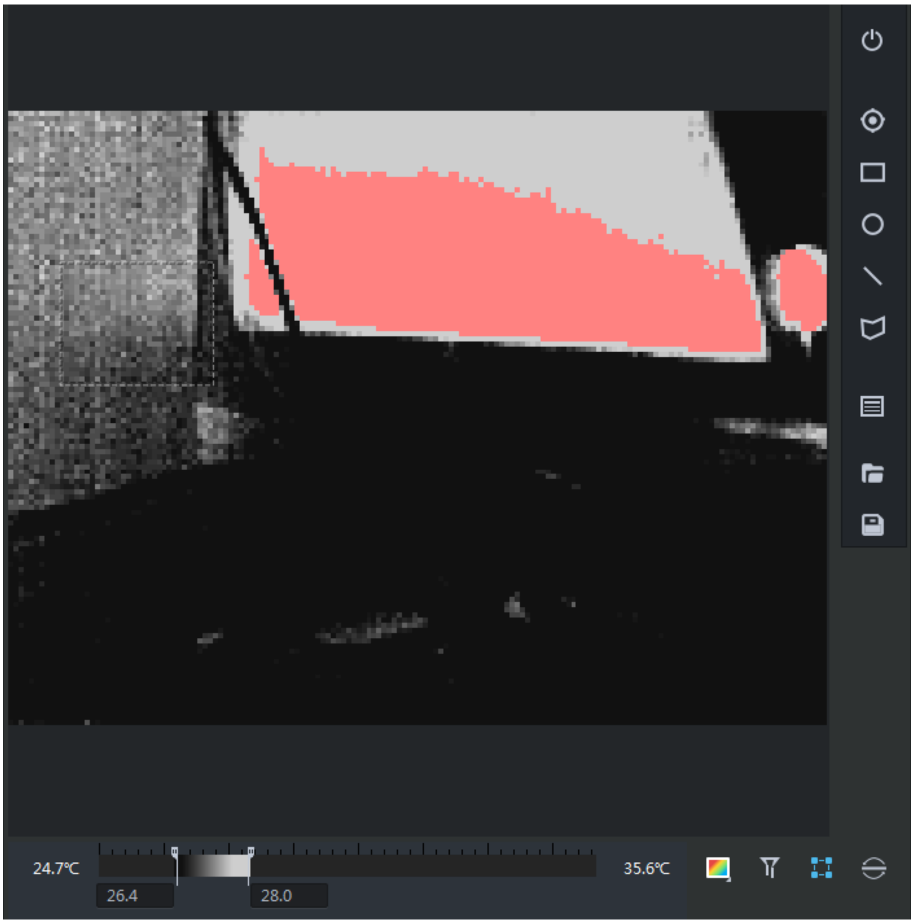
Step 1 Click ⛶ to enable the Select isothermal region.

Step 2 Draw regions on the heatmap.

The color bar below the heatmap only displays the temperatures within the region. See Figure 5-176.

- Place the mouse near the edge of the region. When the mouse changes into ⤡, dragging the mouse changes the region size.
- Only one isothermal region is allowed on the heatmap.
- Click 🗑 to delete the isothermal regions already drawn.

Figure 5-176 Isothermal region



5.14.4.4 File processing

Import Local Heatmap

Step 1 Click 📂.

The heatmap import interface is displayed.

The system supports .dtp heatmap file only.

Step 2 Select a heatmap file and follow the instructions on the interface to import it into the system.

Import heatmap files to the client and analyze them.

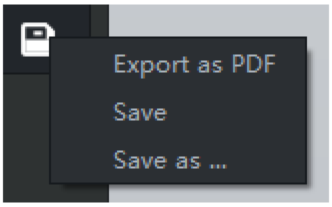
Generate Heatmap Analysis Result

You can generate heatmap analysis reports in .pdf.

Step 1 Click 💾.

The system displays the export interface for the analysis results. See Figure 5-177.

Figure 5-177 Export result



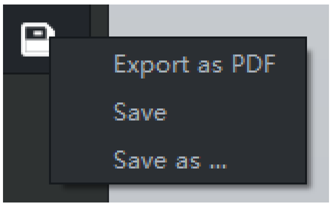
Step 2 Click **Export as PDF** and follow the instructions on the interface to save the exported file.

Save Heatmap

Step 1 Click💾.

The client displays the export interface for the analysis results. See Figure 5-178.

Figure 5-178 Export result



Step 2 Save heatmap.

- Click **Save** to save the rules already set up on the heatmap.
- Click **Save as…**, select the save path in the popup interface, and click **Save** to save the heatmap to a local disk.

5.15 Personnel Management

Personnel refer to the people responsible for access control management. They have the authorization to unlock doors with password, fingerprint, card, or face recognition.

5.15.1 Add Department

Adding department is to manage personnel in the added departments.

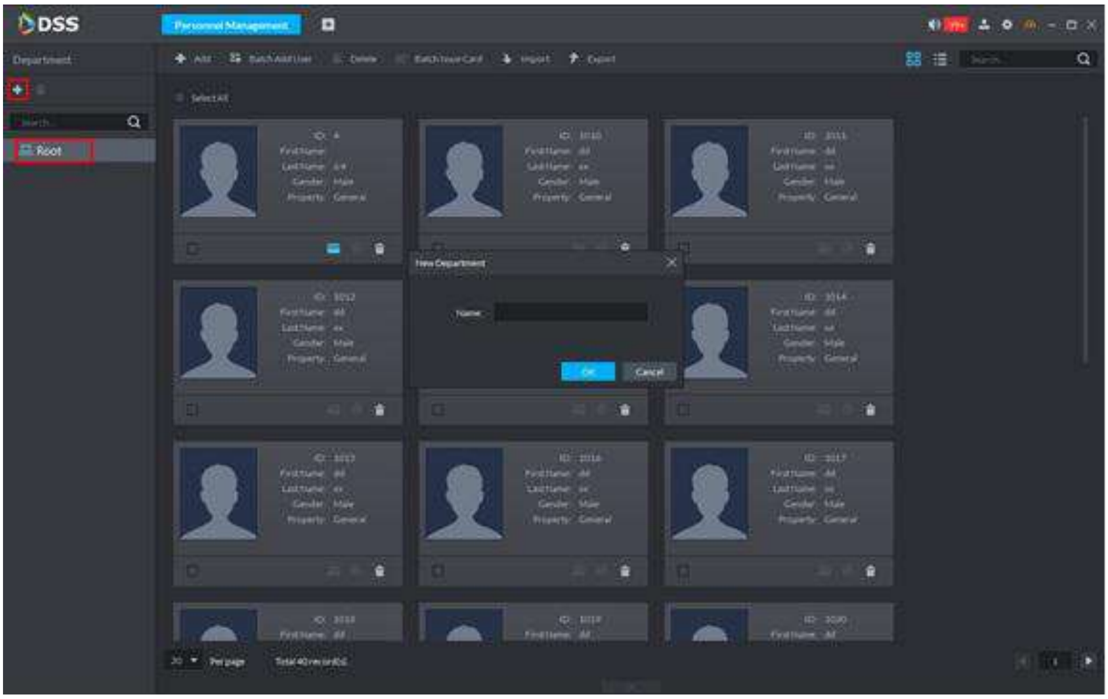
Step 1 Click⊞. On the **Homepage** interface, select **Personnel Management**.

The **Personnel Management** interface is displayed.

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

Step 3 The **New Department** interface is displayed. See Figure 5-179. The new department is directly under the selected node.

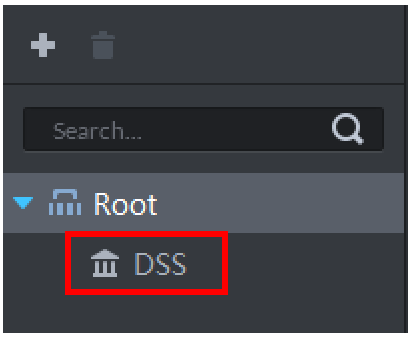
Figure 5-179 New department



Step 4 Input the department name and click **OK**.

Step 5 The newly added department is displayed. See Figure 5-180.

Figure 5-180 New departement



You can delete or rename a newly added department.

- To delete a department, select it, click🗑, and follow the instructions on the interface. You cannot delete a department with personnel.
- To rename a department, right-click it and select **Rename** to modify the name.

5.15.2 Add Personnel

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

- The ID of both added person and attendance person should be in accordance; otherwise, attendance data cannot be synchronized.
- Please make sure the fingerprint collector or reader is properly connected if you want to read or import fingerprint or card information from fingerprint collector or reader.

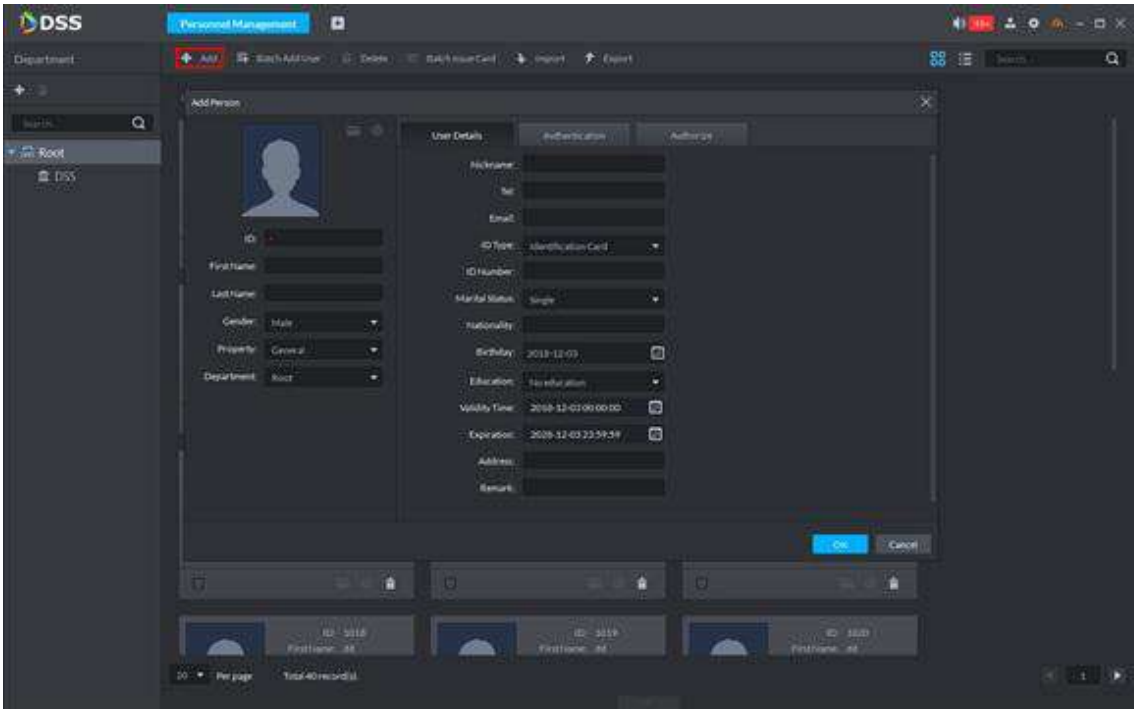
- IR face feature code can be read from IR face access control.

5.15.2.1 Add Person

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

The **Add Person** interface is displayed. See Figure 5-181.

Figure 5-181 Add person



ID:
First Name:
Last Name:
Gender: Male
Property: General
Department: Root
Nickname:
Tel:
Email:
ID Type: Identification Card
ID Number:
Marital Status: Single
Nationality:
Birthday: 2018-12-03
Education: No education
Validity Time: 2018-12-03 00:00:00
Expiration: 2028-12-03 23:59:59
Address:
Remark:

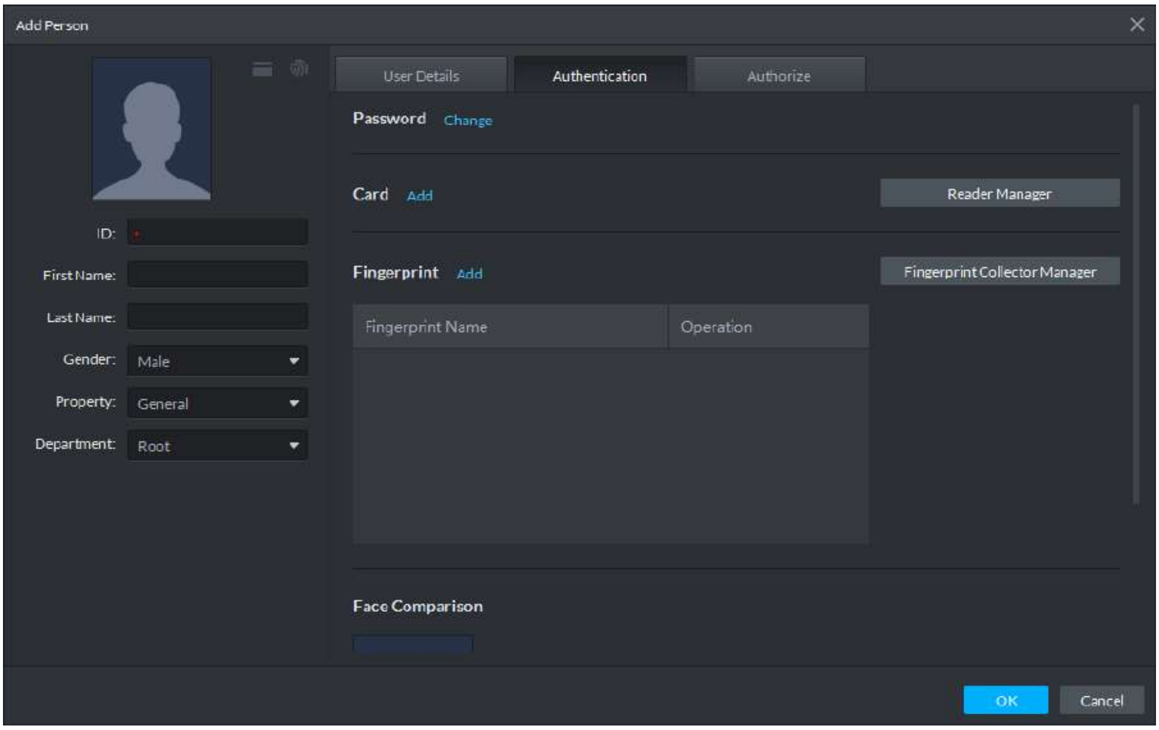
Step 2 Configure personnel details.

1) Move the mouse to the picture section and click **Upload**. Follow the instructions on the interface to upload a picture. If the PC is connected to a camera, click **Snapshot** to take a face snapshot and upload it.
2) Fill in personnel information as necessary. ID is required, and others are optional.

Step 3 Click the **Authentication** tab.

The **Authentication** interface is displayed. See Figure 5-182.

Figure 5-182 Authentication



Gender: Male

Property: General

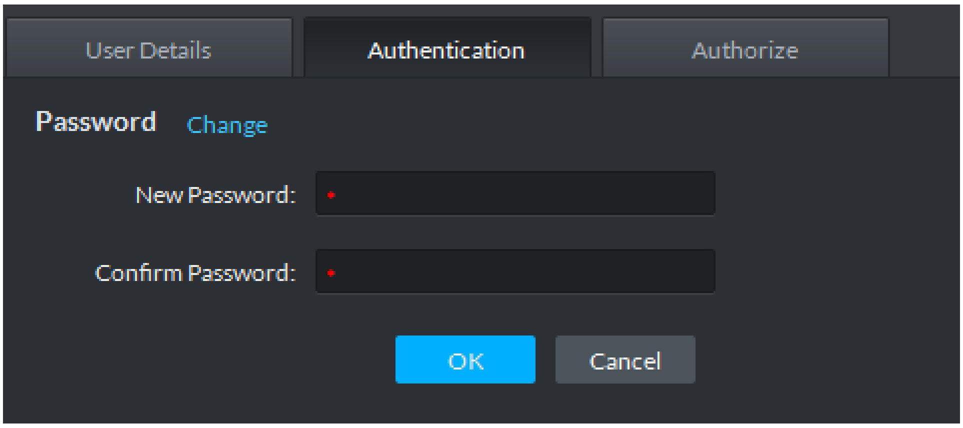
Department: Root

Step 4 Set a password.

1) Click **Change**.

The password setting is displayed. See Figure 5-183.

Figure 5-183 Set password



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

Step 5 Issue cards to personnel.

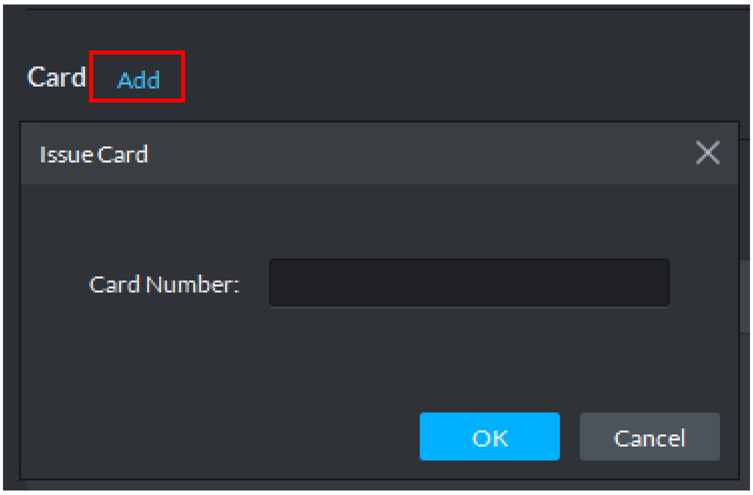
Support manual input of card numbers or using a card reading device.

- Manual input

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

The **Issue Card** interface is displayed. See Figure 5-184.

Figure 5-184 Add card



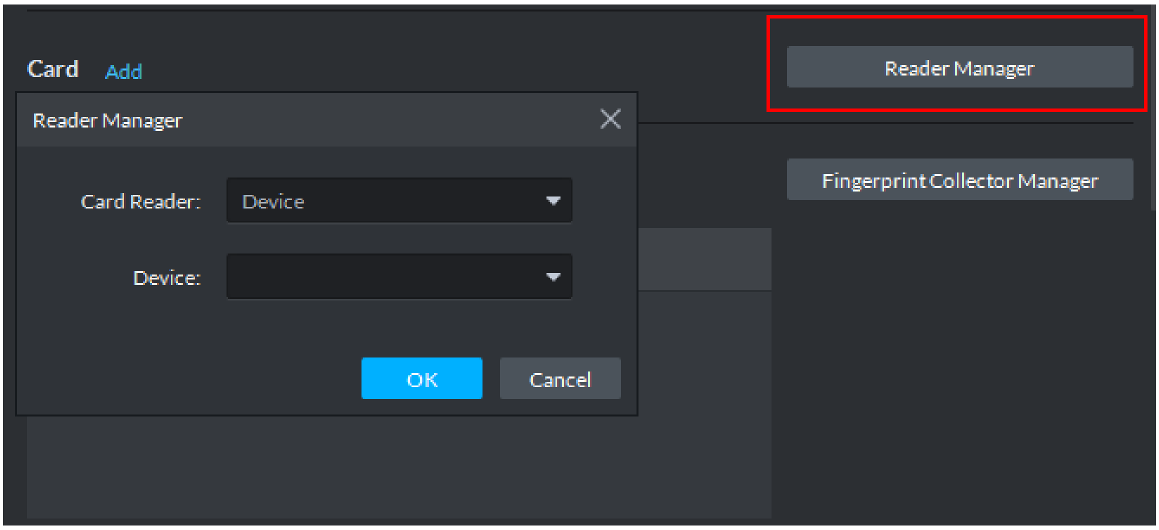
2) Input card number and click **OK** to save the card added.

- Via a card reader.

1) Click **Reader Manager**.

The **Reader Manager** interface is displayed. See Figure 5-185.

Figure 5-185 Read manager



2) Select **Card Reader** or **Device**, and click **OK**.

3) Swipe the card on the card reader or device.

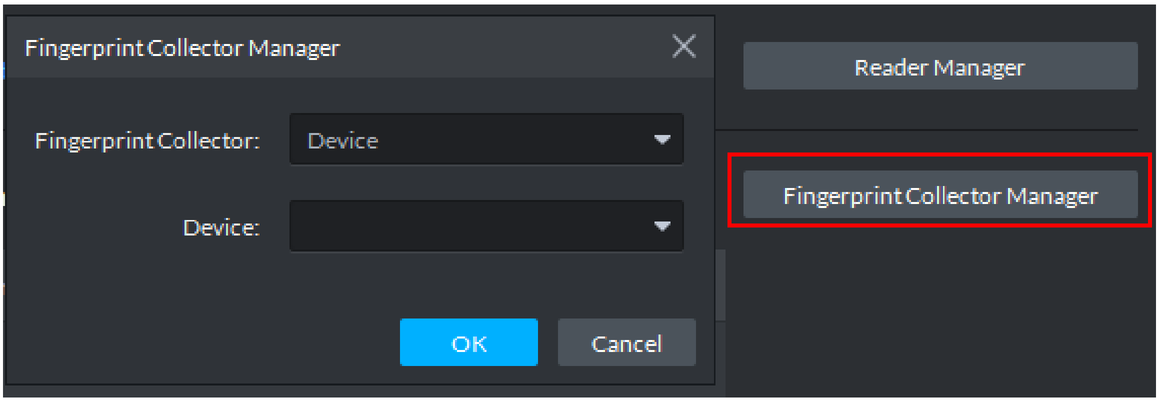
Complete issuing cards.

Step 6 Collect fingerprint.

1) Click **Fingerprint Collector Manager**.

The **Fingerprint Collector Manager** interface is displayed. See Figure 5-186.

Figure 5-186 Fingerprint collector manager

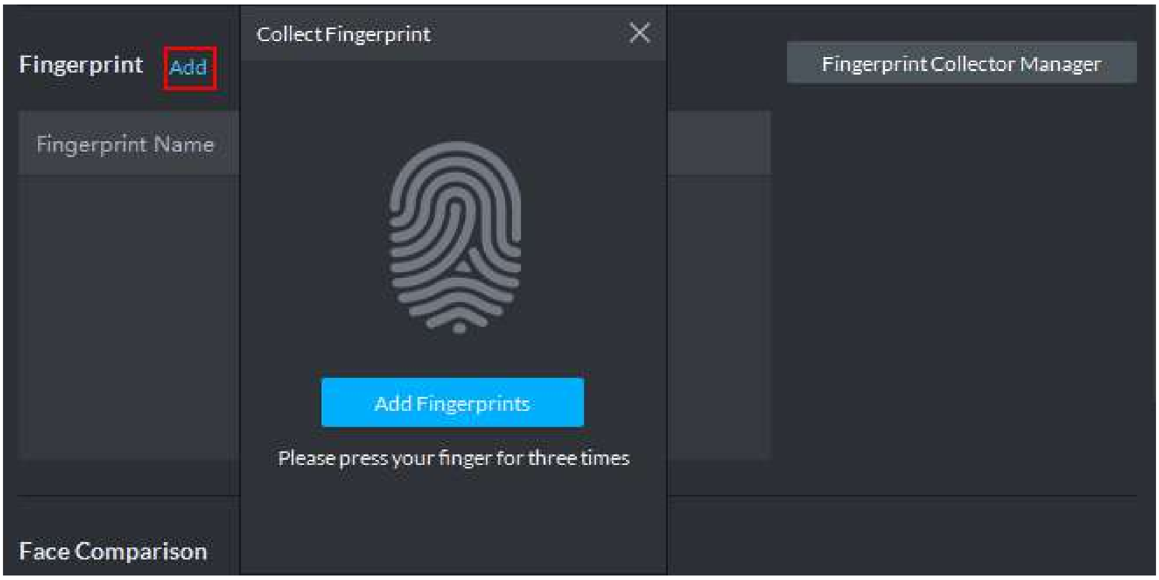


2) Select **Fingerprint Collector** and click **OK**.

3) Click **Add**.

The **Collect Fingerprint** interface is displayed. See Figure 5-187.

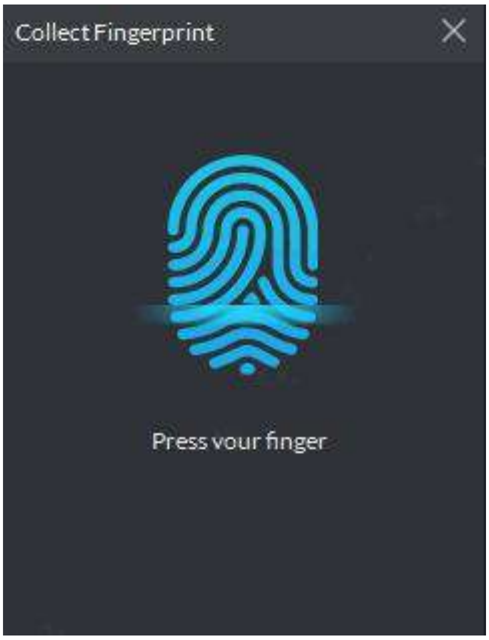
Figure 5-187 Add fingerprint



4) Click **Add Fingerprints**.

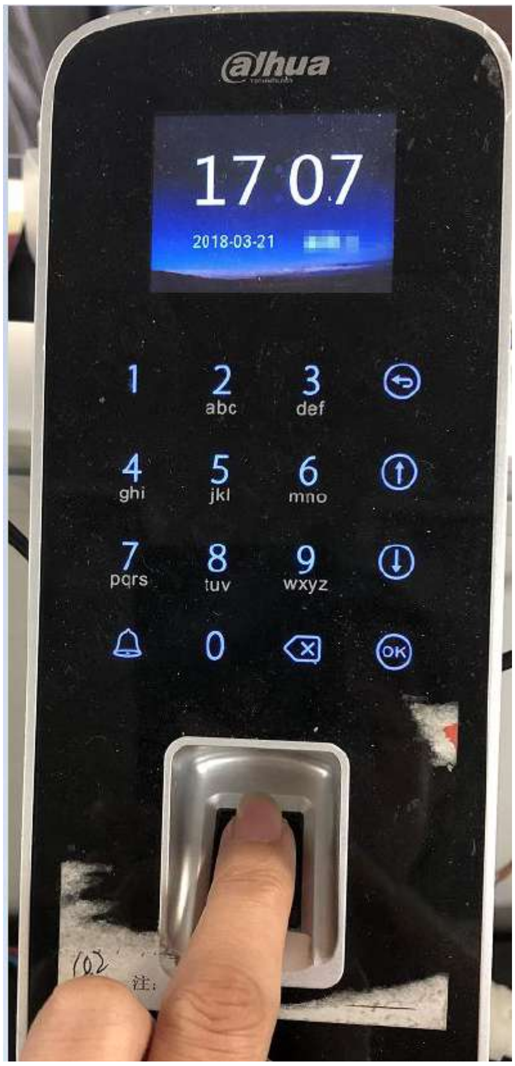
The **Collect Fingerprint** interface is displayed. See Figure 5-188.

Figure 5-188 Collect fingerprint



5) Record fingerprint on the reader by raising and then laying down the finger upon hearing the beep sound. Repeat this for three times. See Figure 5-189.
Complete fingerprint registration and the fingerprint status changes on the client.

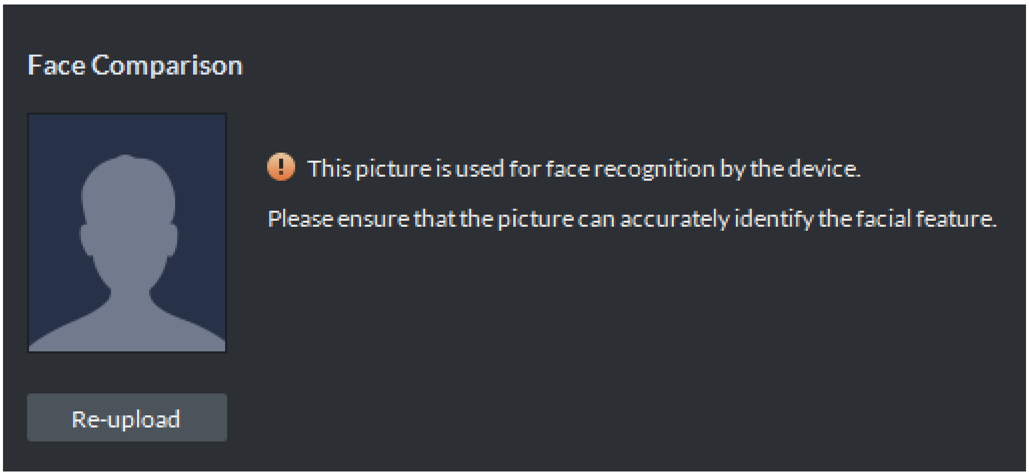
Figure 5-189 Collect fingerprint



Step 7 Upload pictures for face recognition.

Click **Re-upload**, and follow the instructions on the interface to select and upload face pictures. See Figure 5-190.

Figure 5-190 Upload face picture



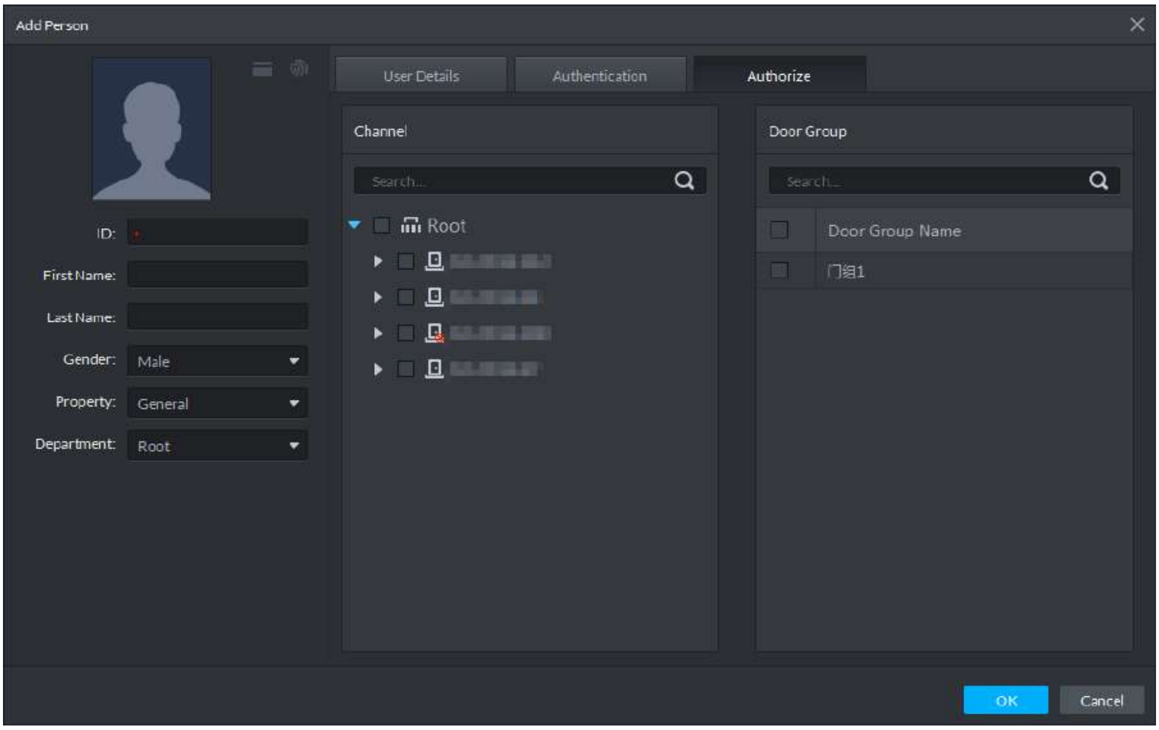
Face Comparison

This picture is used for face recognition by the device.

Please ensure that the picture can accurately identify the facial feature.

Step 8 Click **Authorize** and select the channels to which the authorized users can have access. See Figure 5-191.

Figure 5-191 Authorize



Add Person

User Details | Authentication | Authorize

ID: *

First Name:

Last Name:

Gender: Male

Property: General

Department: Root

Channel

Search...

- □ Root
  - □ [redacted]
  - □ [redacted]
  - □ [redacted]
  - □ [redacted]

Door Group

Search...

□	Door Group Name
□	门组1

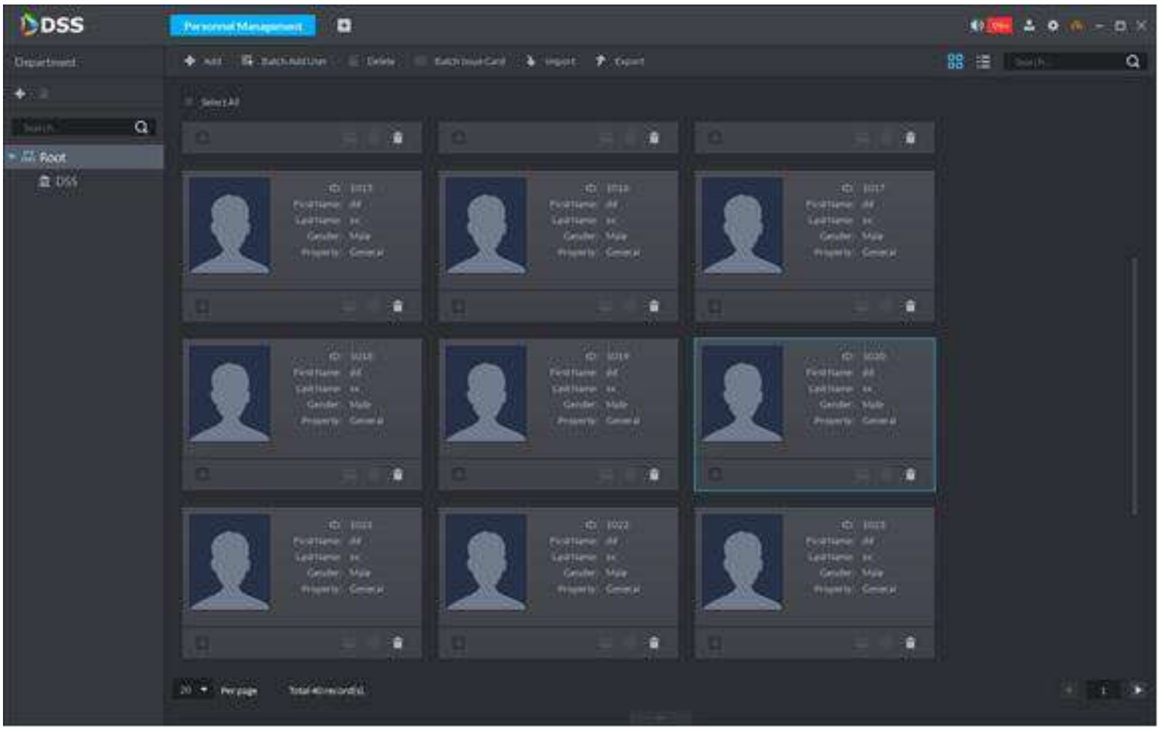
OK Cancel

Step 9 Click **OK**.

For the information of the added personnel, see Figure 5-192. If there are authorized fingerprint and card, the corresponding icon displays in blue.

- Double-click personnel information, or select a person and click ^ to go to the interface for editing personnel information. The system supports modifying personnel information.
- Select a person, click **Delete**, and follow the instructions on the interface to delete the selected personnel. Click **Select All** to quickly delete all personnel on the current page.

Figure 5-192 Personnel list



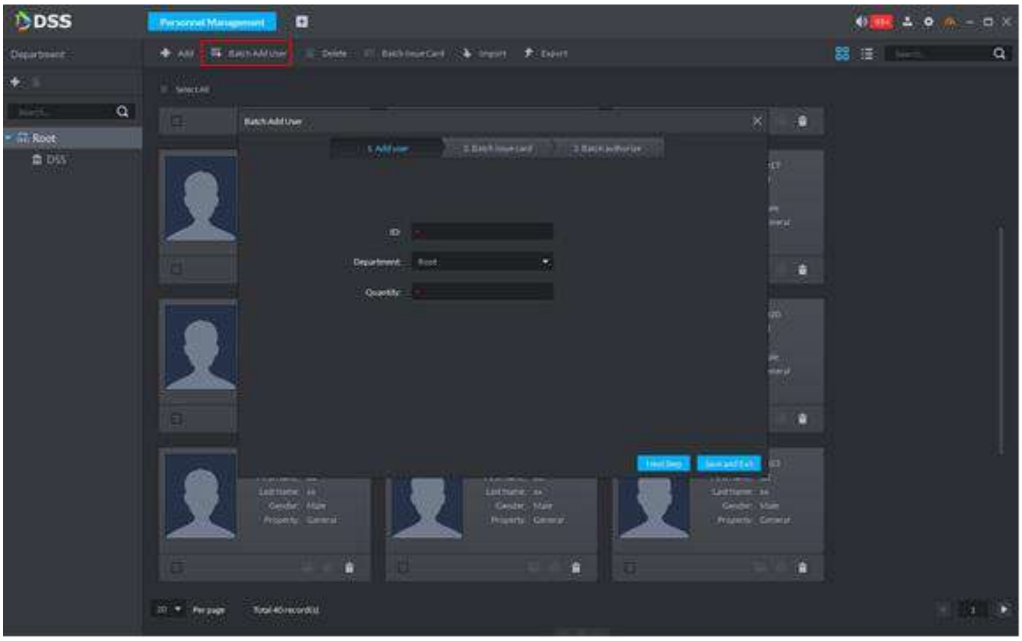
5.15.2.2 Batch Add

If multiple persons are added in one time, you can authorize them by issuing cards only. You cannot authorize password and fingerprint. If necessary, you can edit personnel authorization separately.

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

The **Batch Add User** interface is displayed. See Figure 5-193.

Figure 5-193 Batch add personnel



ID:

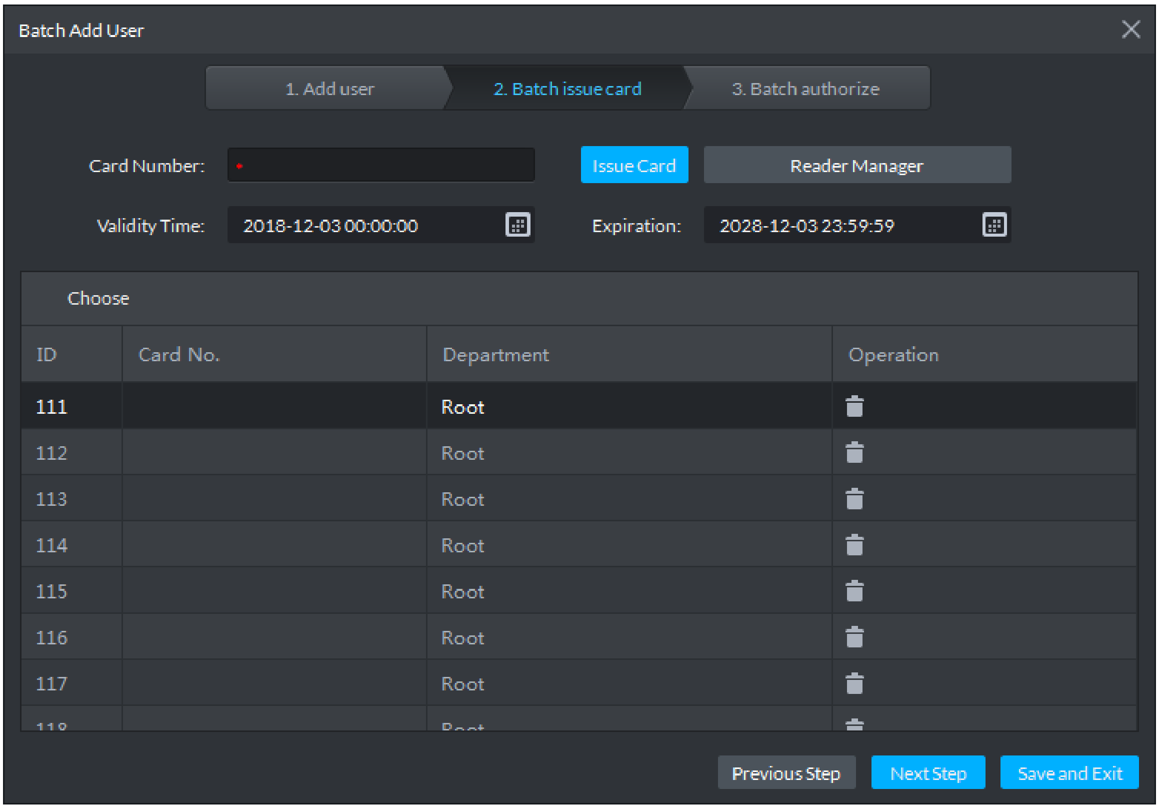
Department: Root

Quantity:

Step 2 Input the starting ID and user quantity, select their departments, and click **Next Step**.

The **Batch issue card** interfaceinterface is displayed. See Figure 5-194.

Figure 5-194 Batch add info



Card Number:

Validity Time: 2018-12-03 00:00:00

Expiration: 2028-12-03 23:59:59

ID	Card No.	Department	Operation
111		Root	🗑
112		Root	🗑
113		Root	🗑
114		Root	🗑
115		Root	🗑
116		Root	🗑
117		Root	🗑
118		Root	🗑

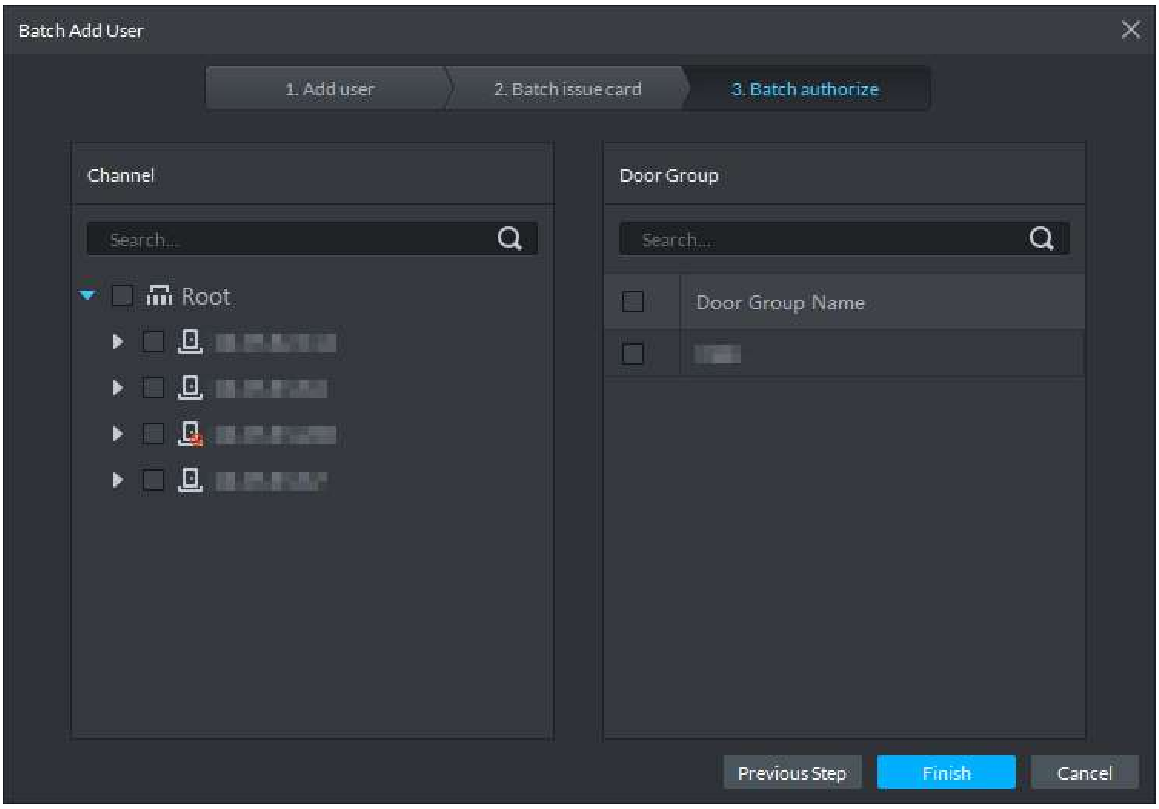
Step 3 Issue cards to personnel.

Step 4 Supports manual input of card numbers or using a card reader.

- Manual input

1) Select a person, input the card number, and set up the validity time and expiry time.
2) Click **Issue Card**.
   Complete issuing card to the selected personnel and the interface shows the personnel card number.
3) Repeat the steps until all personnel get their cards.
4) Click **Next Step**.
   The **Batch authorize** interface is displayed. See Figure 5-195.

Figure 5-195 Batch authorize

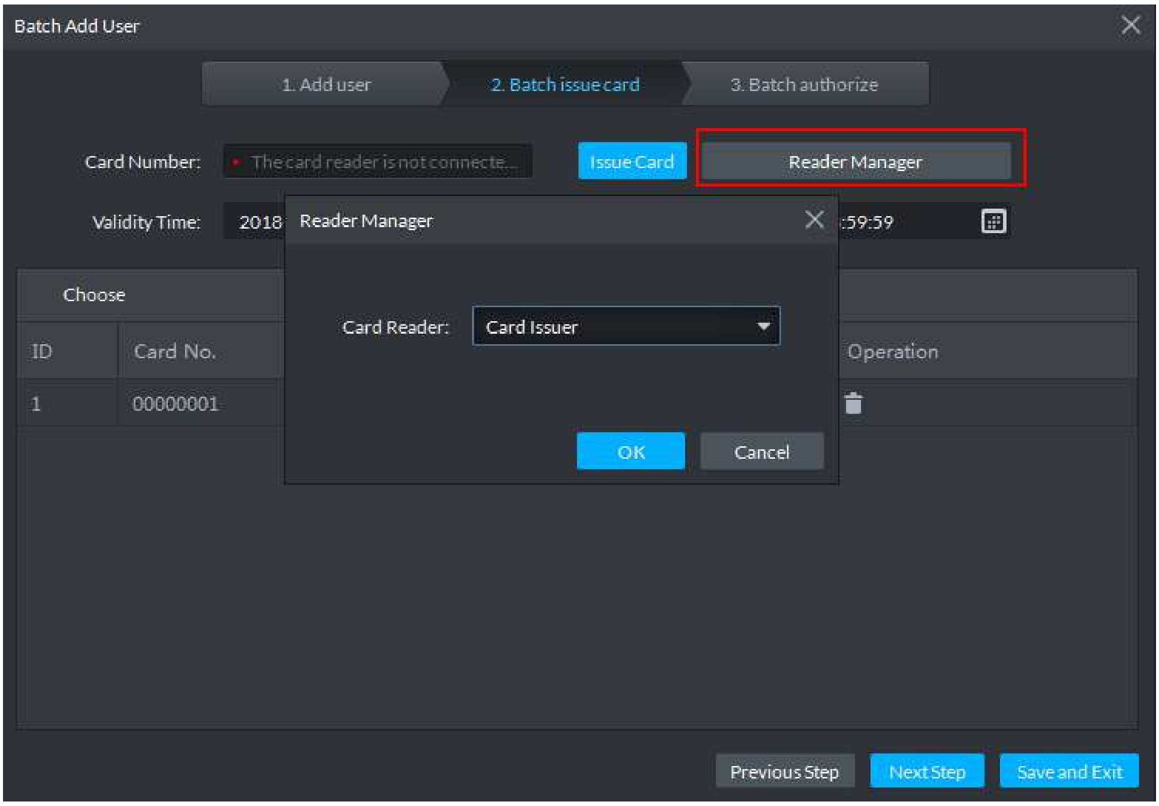


- Via a card reading device

1) Click **Reader Manager**.

The **Reader Manager** interface is displayed. See Figure 5-196.

Figure 5-196 Reader manager



Card Number: The card reader is not connecte...

Validity Time: 2018 … :59:59

Card Reader: Card Issuer

ID	Card No.	Operation
1	00000001	🗑

2) Select **Card Reader** or **Device**, and click **OK**.

3) Swipe the card on the card reader or device.

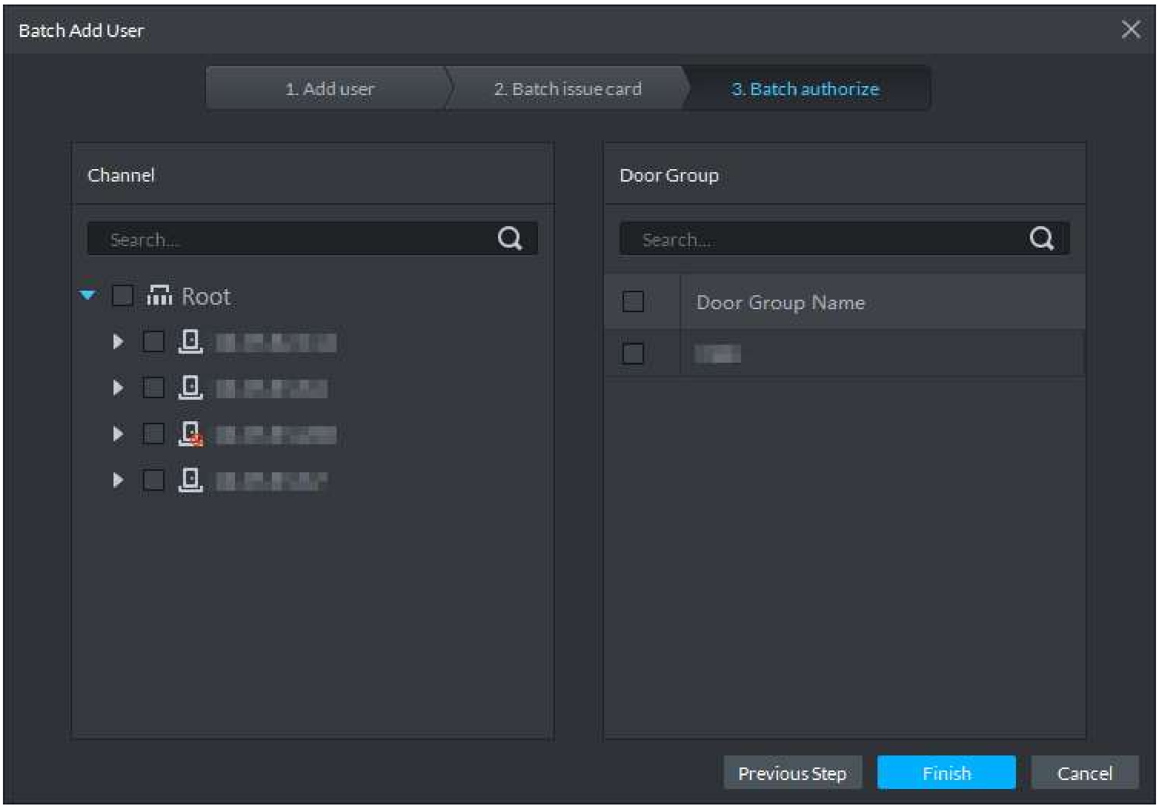
4) Select a person, set up the validity time and expiry time, and then click **Issue Card**.

5) Repeat the steps until all personnel get their cards.

6) Click **Next Step**.

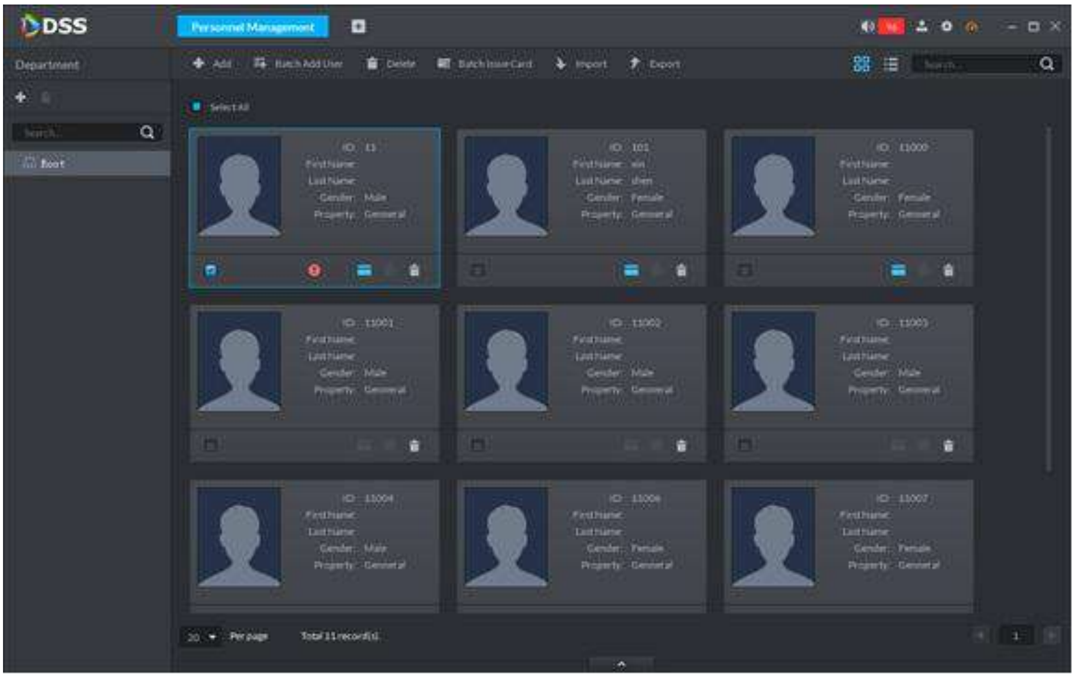
The **Batch authorize** interface is displayed. See Figure 5-197.

Figure 5-197 Batch authorize



Step 5 Select the access control channels or door groups to which the personnel have access, and click **Finish**.

Figure 5-198 Batch add personnel



ID: 11
First Name:
Last Name:
Gender: Male
Property: General

ID: 101
First Name: xin
Last Name: shen
Gender: Female
Property: General

ID: 11000
First Name:
Last Name:
Gender: Female
Property: General

ID: 11001
First Name:
Last Name:
Gender: Male
Property: General

ID: 11002
First Name:
Last Name:
Gender: Male
Property: General

ID: 11003
First Name:
Last Name:
Gender: Male
Property: General

ID: 11004
First Name:
Last Name:
Gender: Male
Property: General

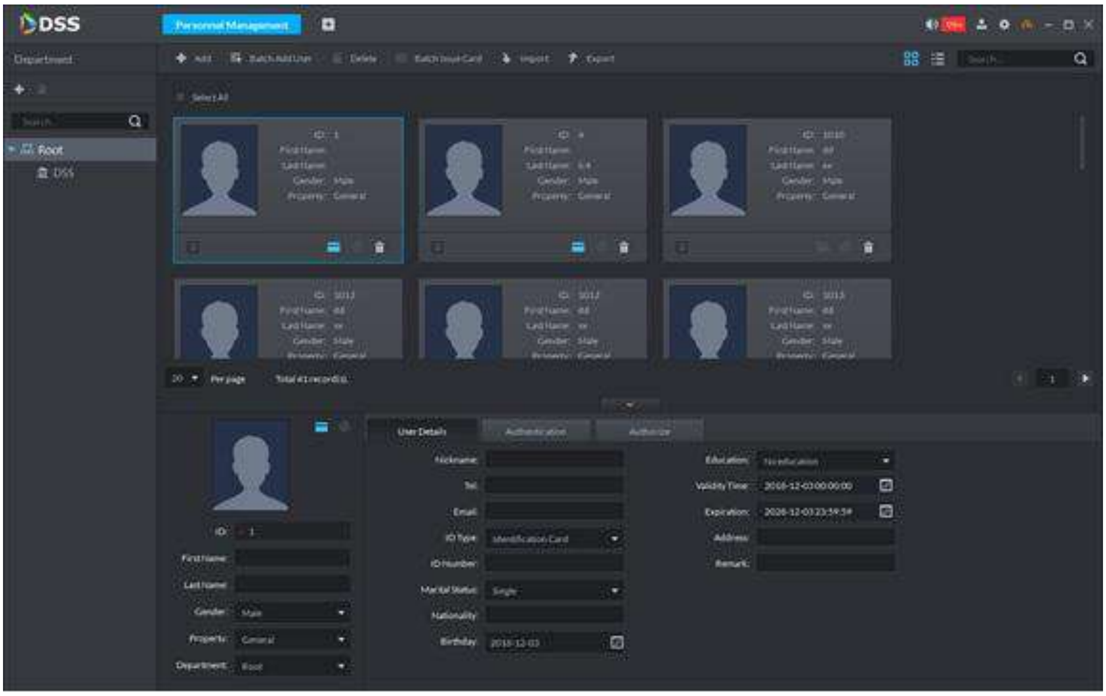
ID: 11006
First Name:
Last Name:
Gender: Female
Property: General

ID: 11007
First Name:
Last Name:
Gender: Female
Property: General

Step 6 Edit personnel information, including modifying personnel information, setting up password, and registering fingerprint or face pictures.

Step 7 Double-click a person, or select a person and click to go to the screen for editing personnel information, where you can modify the personnel information. See Figure 5-199. Edits take effect immediately.

Figure 5-199 Batch add personnel



ID: 1
First Name:
Last Name:
Gender: Male
Property: General

ID: 4
First Name:
Last Name: 64
Gender: Male
Property: General

ID: 1010
First Name: dd
Last Name: ee
Gender: Male
Property: General

ID: 1012
First Name: dd
Last Name: ee
Gender: Male
Property: General

ID: 1012
First Name: dd
Last Name: ee
Gender: Male
Property: General

ID: 1013
First Name: dd
Last Name: ee
Gender: Male
Property: General

20 Per page Total 41 record(s)

ID: 1
First Name:
Last Name:
Gender: Male
Property: General
Department: Root

Nickname:
Tel:
Email:
ID Type: Identification Card
ID Number:
Marital Status: Single
Nationality:
Birthday: 2018-12-03

Education: No education
Validity Time: 2018-12-03 00:00:00
Expiration: 2028-12-03 23:59:59
Address:
Remark:

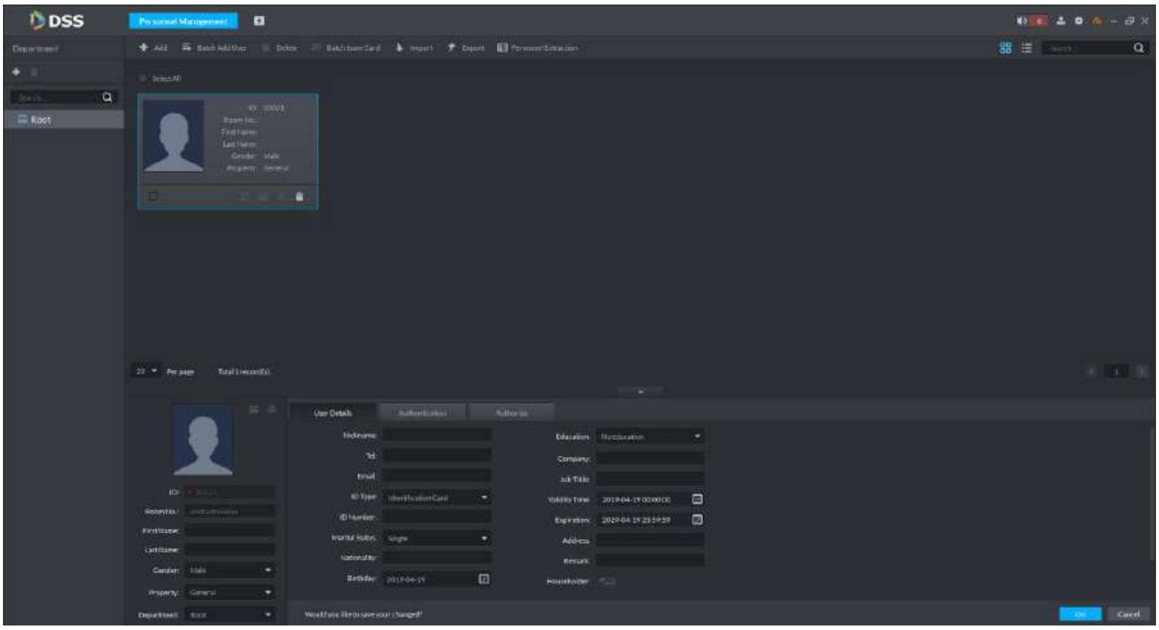
5.15.3 Edit Personnel

You can modify information of added personnel, includingID, detail, authentication and authorize.

- If the system adopts IR face attendance, you must extract face feature code of personnel with same ID from IR face attendance device by editing personnel.
- Please make sure the device is connected if you want to read or import fingerprint, card or face feature from fingerprint collector, reader and IR face access control.

Step 1 Double click the personnel or select the person and click on **Personnel Management** interface. See Figure 5-200.

Figure 5-200 Edit person



ID: 10021
Gender: Male
Property: General
Department: Root
ID Type: Identification Card
Marital Status: Single
Birthday: 2019-04-19
Education: No education
Validity Time: 2019-04-19 00:00:00
Expiration: 2029-04-19 23:59:59
Would you like to save your changes?

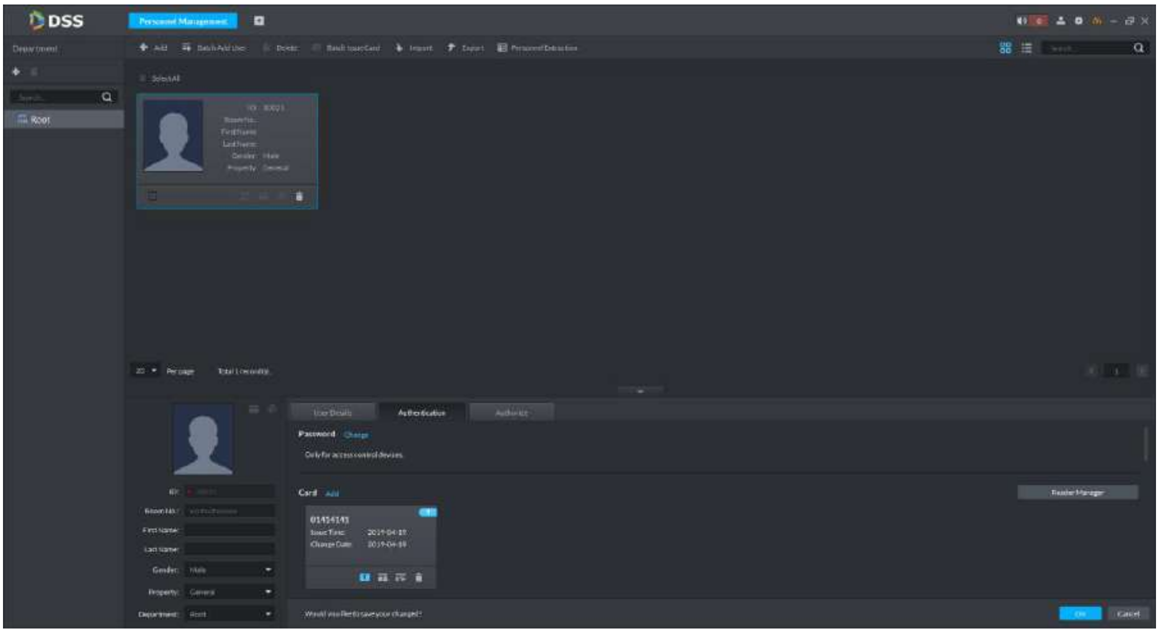
Step 2 Modify person info and detail except ID.

The person property is required to be set as **General** if you use first card to unlock.

Step 3 Click **Authentication**.

The interface is displayed. See Figure 5-201.

Figure 5-201 Authentication

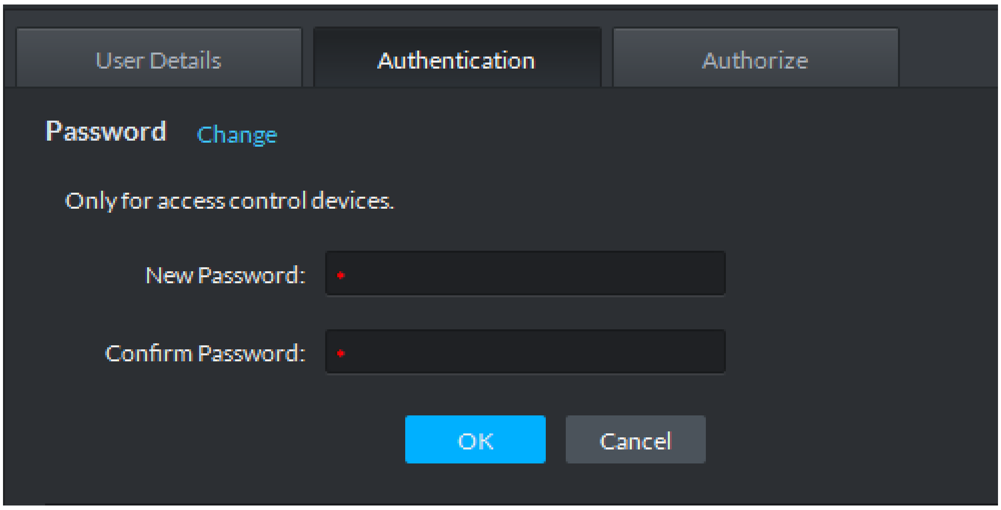


Only for access control devices.
01414141
Issue Time: 2019-04-19
Change Date: 2019-04-19
Gender: Male
Property: General
Department: Root
Would you like to save your changes?

Step 4 Click **Change** and set new password according to interface prompt. Click **OK**. See Figure 5-202.

You need to set password when using password to unlock.

Figure 5-202 Set password



User Details | Authentication | Authorize

Password Change

Only for access control devices.

New Password: *

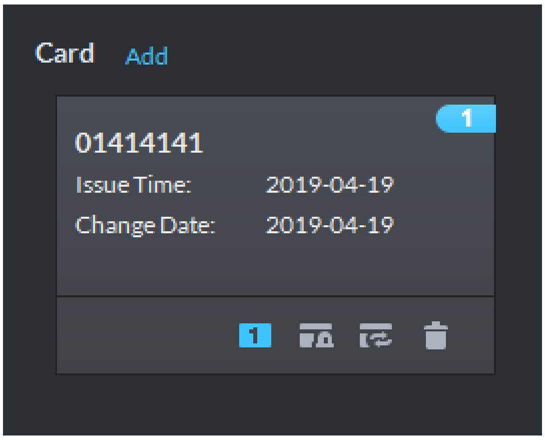
Confirm Password: *

OK Cancel

Step 5 Manage card info.

Select added card and you can modify card status. See Table 5-36 for more details.

Figure 5-203 Add card



Card Add

01414141

Issue Time: 2019-04-19

Change Date: 2019-04-19

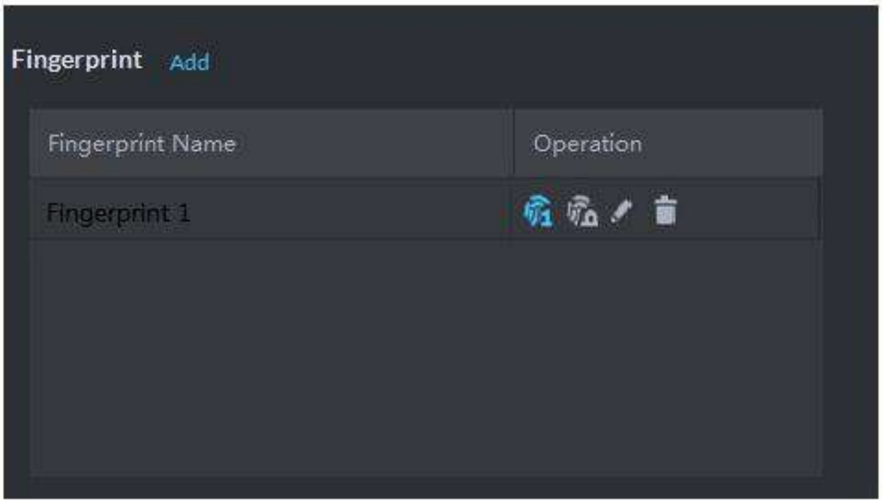
Table 5-36 Card operation

Icon	Description
1	If the person has several cards, only the main card can be issued to access control device. The firstly added card is main card by default. Click the icon and it becomes 1, display 1 on the upper right corner, then the card is set as main card. Click 1 and cancel master card setting.
	Set card as duress card. Duress alarm is triggered when using the card to unlock. Click the icon and it becomes , display on the upper right corner, then the card is set as duress card. Click and cancel duressc card setting.
⇄	Change card if the card is damaged and cannot be used.
🗑	Delete card info. Unlock permisson does not exist after the card is deleted.

Step 6 Manage fingerprint.

Collect person fingerprint and you can modify fingerprint status and name. See Table 5-37 for more details.

Figure 5-204 Fingerprint collection



Fingerprint Add

Fingerprint Name	Operation
Fingerprint 1	

Table 5-37 Fingerprint operation

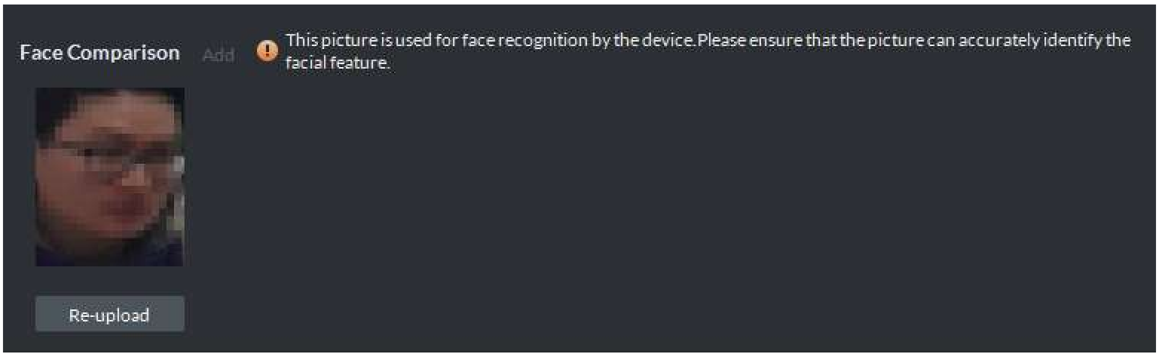
Icon	Description
	If more than 3 fingerprints are imported, then only the main fingerprint can be issued to access control device. The recently imported three fingerprints are considered as main fingerprint by default. One person can set up to 3 main fingerprints. Click the icon and it becomes, then the fingerprint is set as main fingerprint. Click and cancel main fingerprint setting.
	Set fingerprint as duress fingerprint. Duress alarm is triggered after using the fingerprint to unlock. Click the icon and it becomes, then the fingerprint is set as duress fingerprint. Click and cancel setting of duress fingerprint.
✎	Modify fingerprint name.
🗑	Delete fingerprint. Unlock permission does not exist after fingerprint is deleted.

Step 7 Update face recognition picture.

Click **Re-upload** and upload new face picture according to system prompt.

Move the mouse to the uploaded picture and 🗑 appears, click the icon and you can delete the picture.

Figure 5-205 Upload face picture



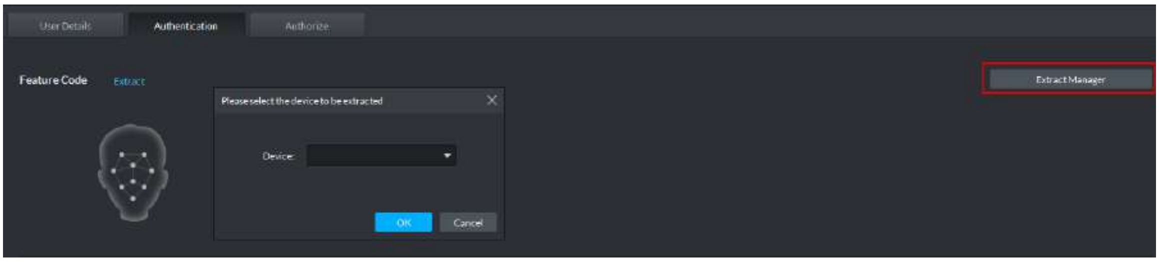
This picture is used for face recognition by the device.Please ensure that the picture can accurately identify the facial feature.

Step 8 Extract IR face feature code.

1) Click Extract Manager.

The **Please select the device to be extracted** interface is displayed. See Figure 5-206.

Figure 5-206 Extract face feature code



2) Select IR face device and click **OK**.

3) Click **Extract**.

The system extracted IR face feature code from device successfully.

📖

Click **Reextract** to update IR face feature code.

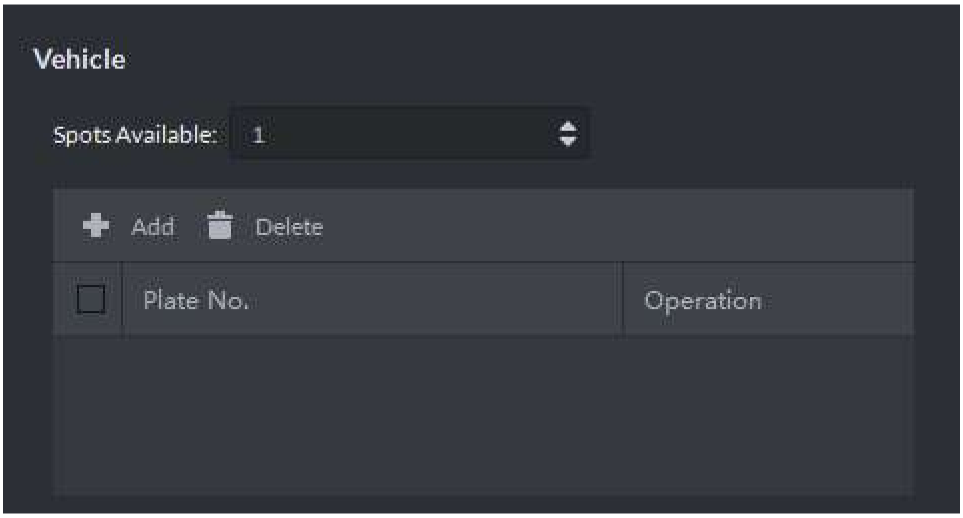
Step 9 Modify quantity of available spots and plate number.

Click **Spots Available** and **Plate No.**, and then you can modify both respectively.

📖

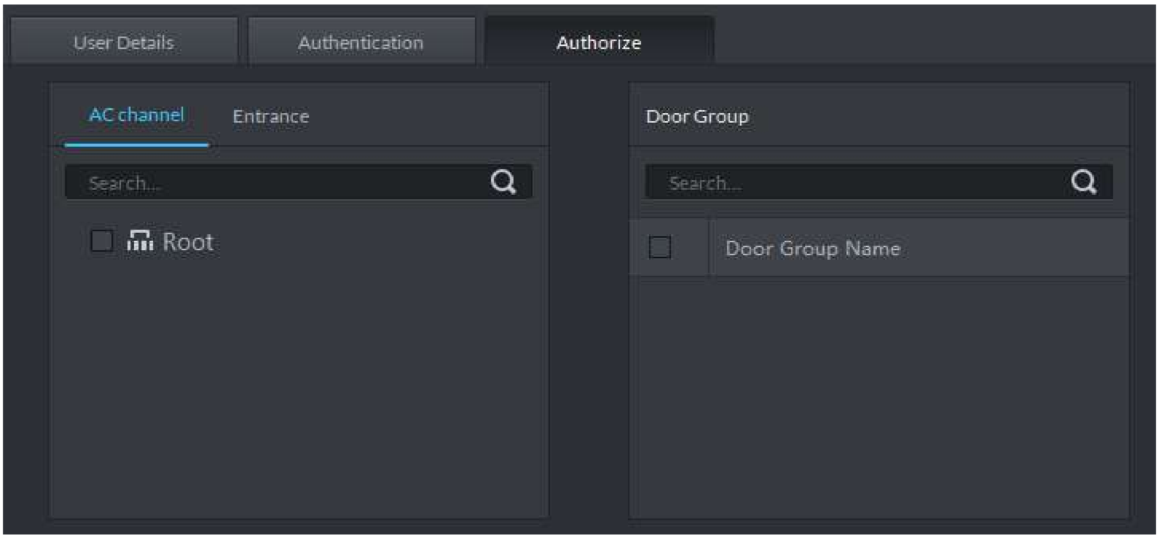
Click 🗑 next to license plate or select license plate, click 🗑 and you can delete it.

Figure 5-207 Add vehicle info



Step 10 Click **Authorize** and you can modify access control and entrance which are open to personnel. See Figure 5-208.

Figure 5-208 Authorize



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

5.15.4 Import/Export Personnel

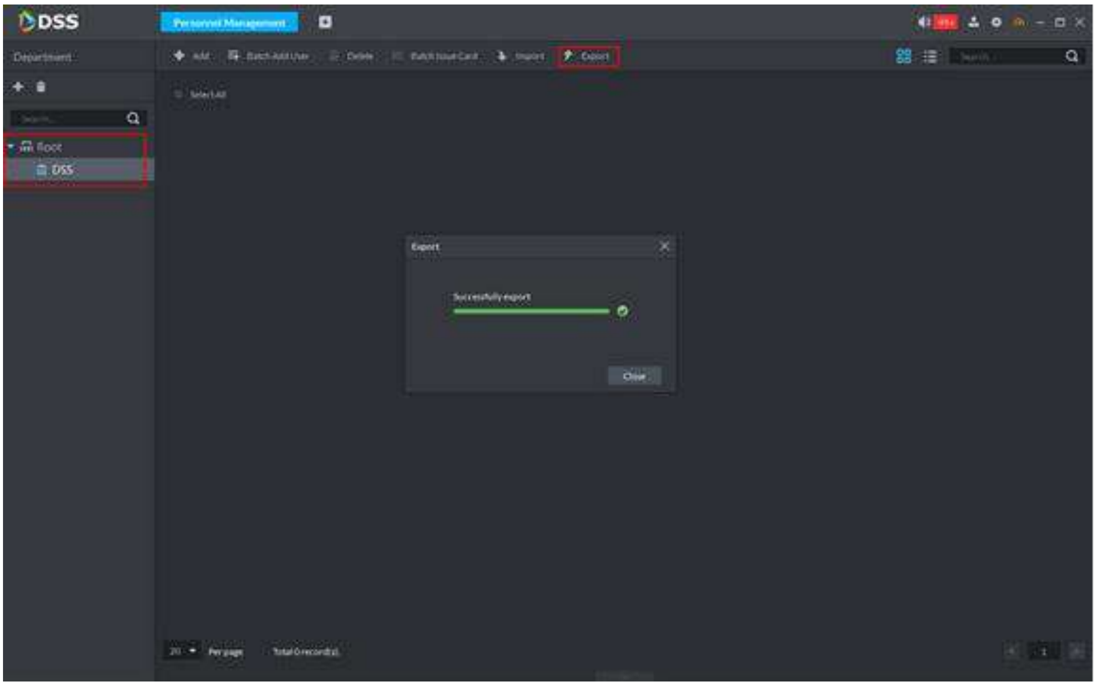
5.15.4.1 Export Personnel

Back up personnel data to restore damaged data or complete personnel configuration on the platform when there is a need for quick import of the personnel information.

Step 1 On the left side of the **Personnel Management** interface, select an organization, click **Export**, and follow the instructions on the interface to save the exported information to a local disk.

The system displays the progress of the export. See Figure 5-209.

Figure 5-209 Export personnel



Step 2 Click **Close**.

5.15.4.2 Import Personnel

Edit the template or import information of existing personnel to quickly add them. You can import a file in .xls no larger than 1 M.

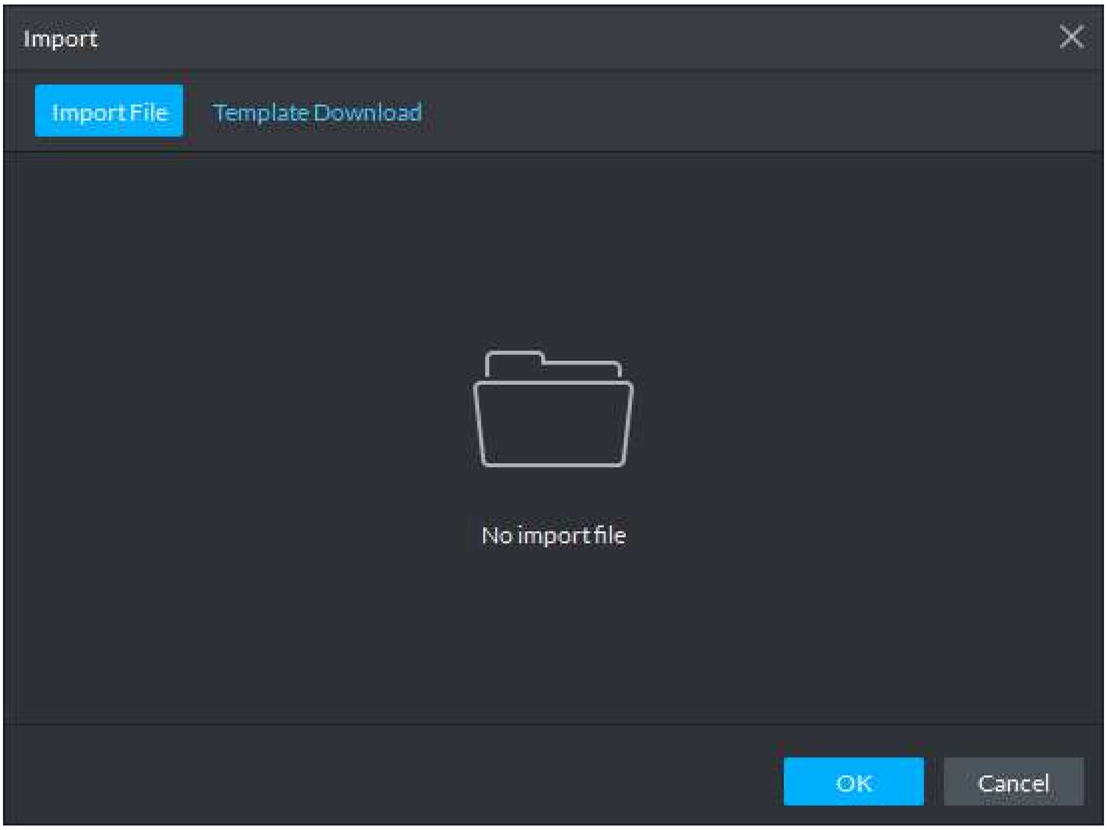
📖

- You can import the personnel info exported by SmartPSS.
- The person property is required to be set as General if the person is first card unlock.

Step 1 On the **Personnel Managemen**t interface, click **Import**.

The Import interface is displayed. See Figure 5-210.

Figure 5-210 Import



Step 2 Import personnel information files.

1) Click **Import**, and follow the instructions on the interface to select the files.

📖

If there is no personnel information file, click **Template Download** and follow the instructions on the interface to create personnel information.

2) Click **OK**.

Complete the import of personnel information.

Step 3 The following might occur during an import:

- The system prompts that the imported personnel already exist on the platform.
- Personnel ID duplicate in the imported file. If the same ID does not exist, the system accepts it as a new ID; if it already exists, the system gives a prompt.
- The system prompts that the imported personnel information is improperly filled, such as field length exceeding the limit on the client, and timeout resulting in a failure to upload to the database.

- Abnormal default values. The rules are: Gender (male), property (common staff), department (root node), ID type (Identification Card), marital status (null), education (No education). The valid period starts from now and ends in 2028 by default.
- A person does not exist. If the department does not exist, a new department is created under the root node; if the department exists, the person is created under the department; department information matches by name.
- Cannot read the contents with a parsing error reported directly.

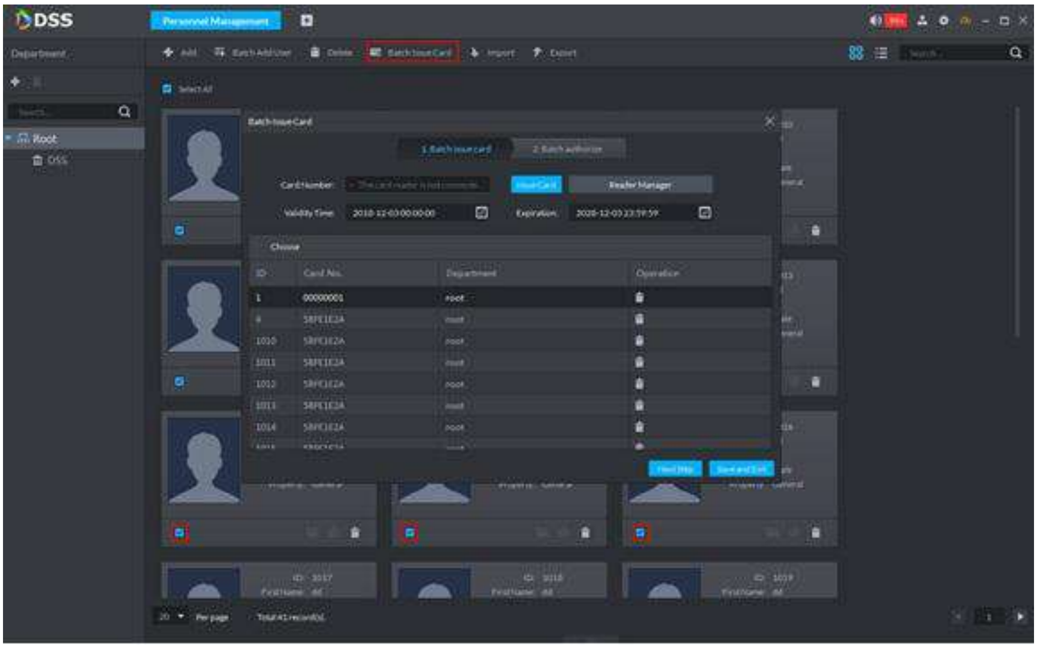
5.15.5 Batch Issue Card

Supports batch issuing cards to personnel to complete access control authorization.

Step 1 On the **Personnel Management** interface, select the personnel to issue card to, and click **Batch Issue Card**.

Step 2 The **Batch issue card** interface is displayed. See Figure 5-211.

Figure 5-211 Batch issue card



Card Number: The card reader is not connected

Validity Time: 2018-12-03 00:00:00

Expiration: 2028-12-03 23:59:59

Choose

ID	Card No.	Department	Operation
1	00000001	root	
4	5BFC1E2A	root	
1010	5BFC1E2A	root	
1011	5BFC1E2A	root	
1012	5BFC1E2A	root	
1013	5BFC1E2A	root	
1014	5BFC1E2A	root	

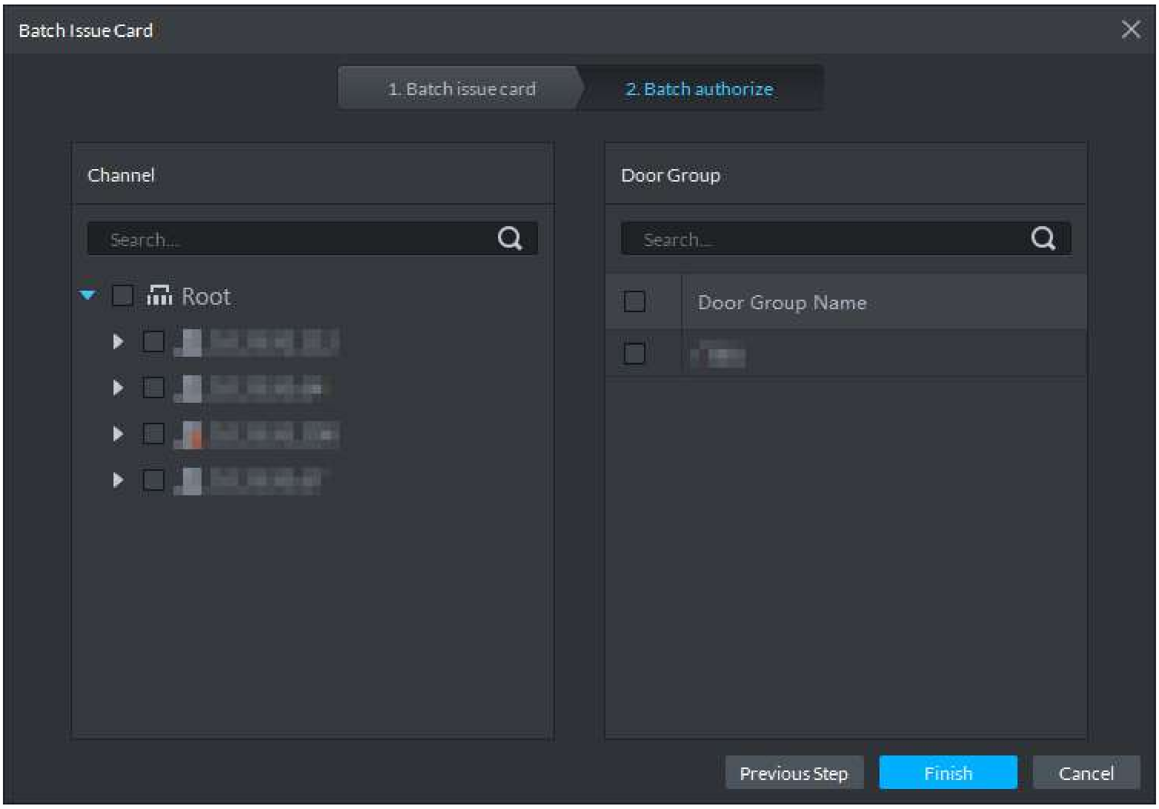
Step 3 Issue cards to personnel.

Step 4 Supports manual input of card numbers or using a card reading device.

- Manual input

1) Select a person, input the card number, and set up the validity time and expiry time.
2) Click **Issue Card**.
   Complete issuing card to the selected personnel and the interface shows the personnel card number.
3) Repeat the steps until all personnel get their cards.
4) Click **Next Step**.
   The **Batch authorize** interface is displayed. See Figure 5-212.

Figure 5-212 Batch authorize

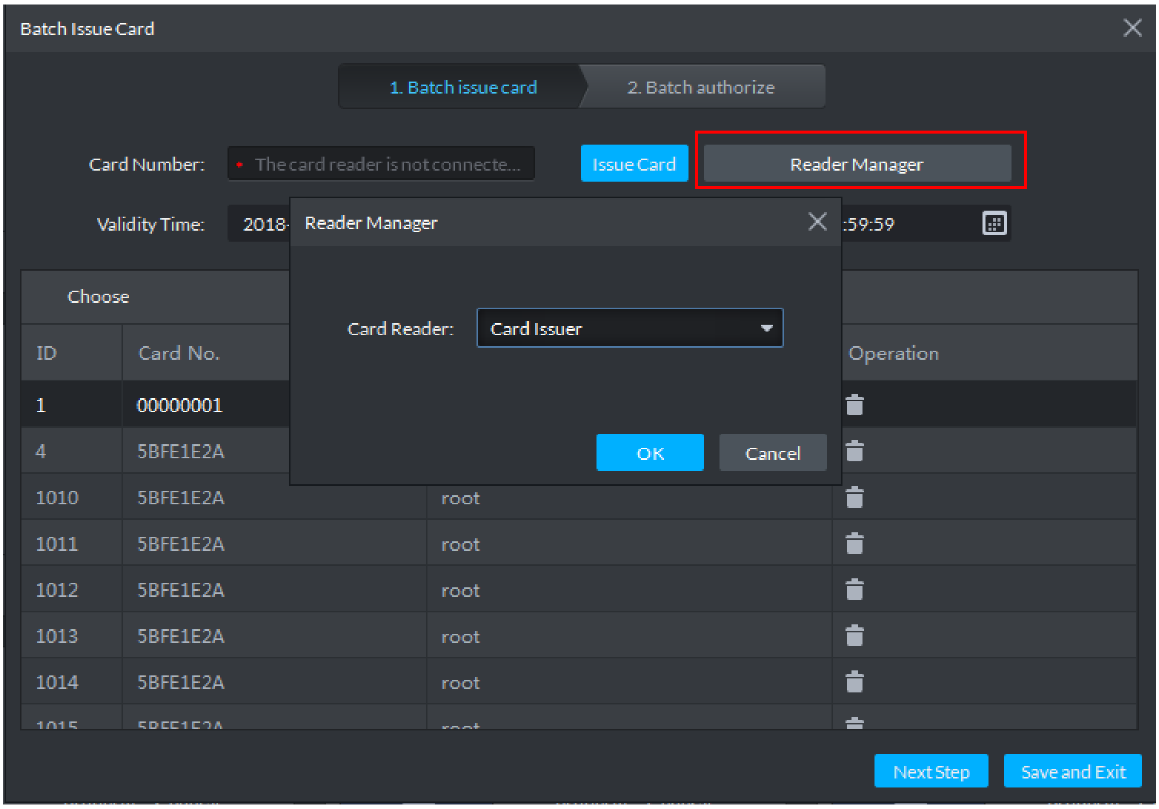


- Via a card reading device

1) Click **Reader Manager**.

The **Reader Manager** interface is displayed. See Figure 5-213.

Figure 5-213 Reader manager



Card Number: The card reader is not connecte...

Validity Time: 2018- :59:59

Card Reader: Card Issuer

ID	Card No.		Operation
1	00000001		🗑
4	5BFE1E2A		🗑
1010	5BFE1E2A	root	🗑
1011	5BFE1E2A	root	🗑
1012	5BFE1E2A	root	🗑
1013	5BFE1E2A	root	🗑
1014	5BFE1E2A	root	🗑
1015	5BFE1E2A	root	🗑

2) Select from **Card Reader** or **Device**, and click **OK**.

3) Swipe the card on the card reader or device.

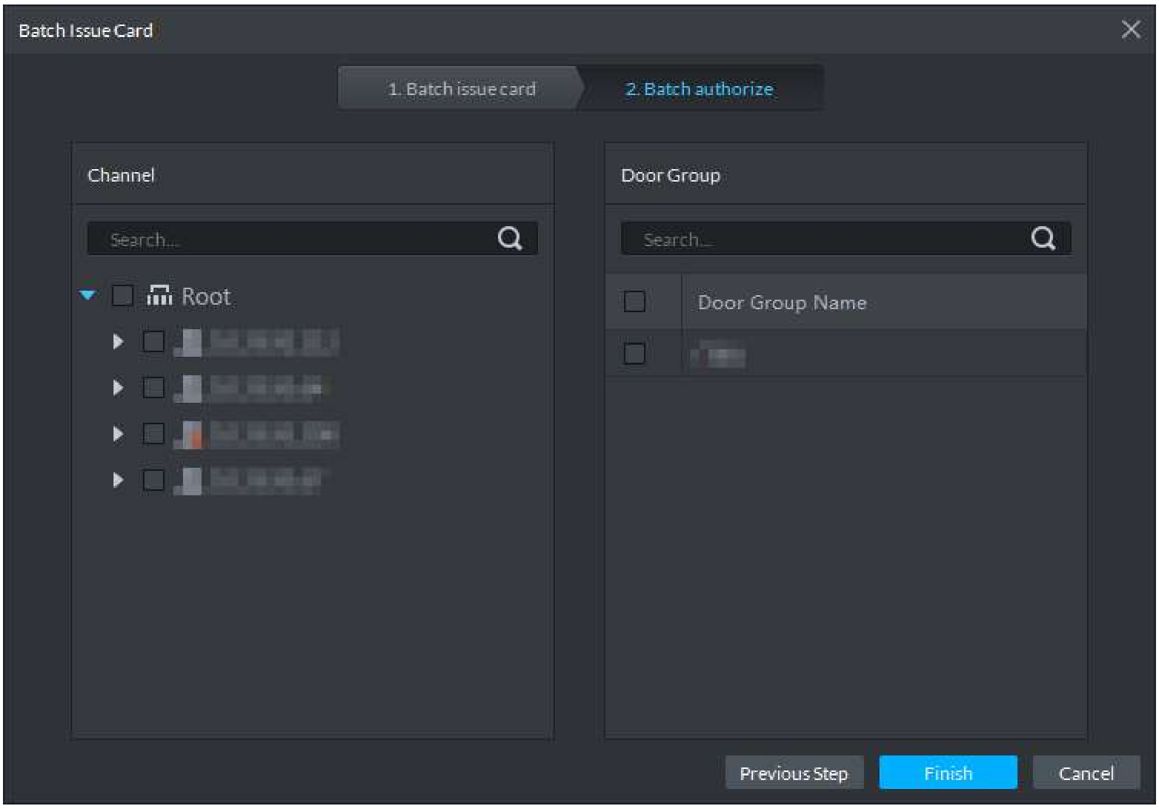
4) Select a person, set up the validity time and expiry time, and click **Issue Card**.

5) Repeat the steps until all personnel get their cards.

6) Click **Next Step**.

The **Batch authorize** interface is displayed. See Figure 5-214.

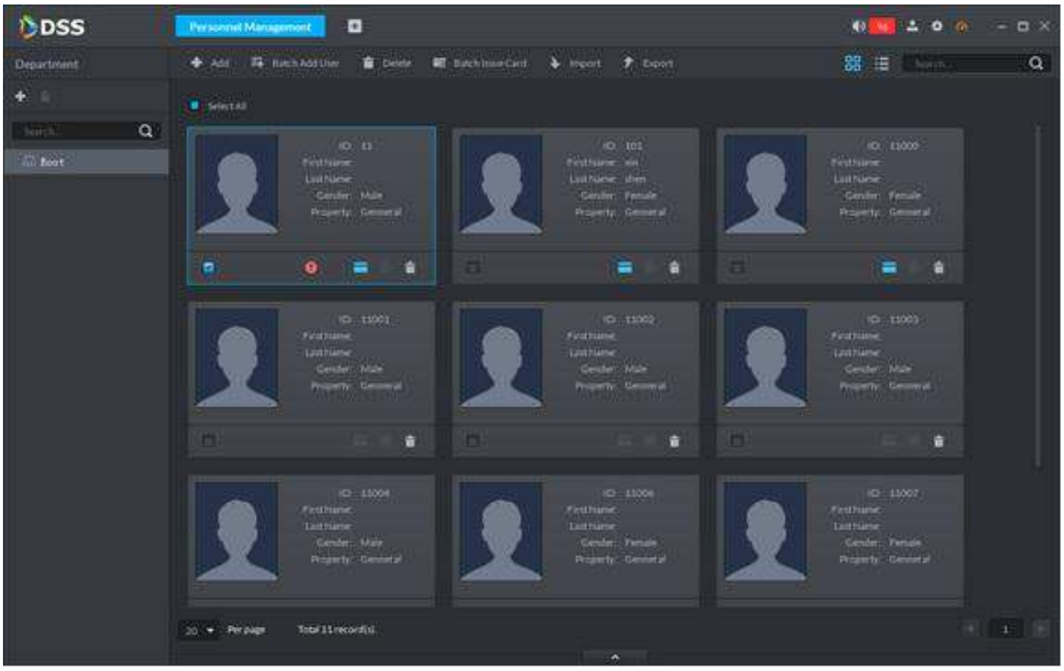
Figure 5-214 Batch authorize



Step 5 Select the access control channels or door groups to which the personnel have access, and click **Finish**.

Step 6 The interface displays the card issuing results. See Figure 5-215. The card icon changes into blue, as ▬ and it means that you have issued a card to the person.

Figure 5-215 Issuing card result



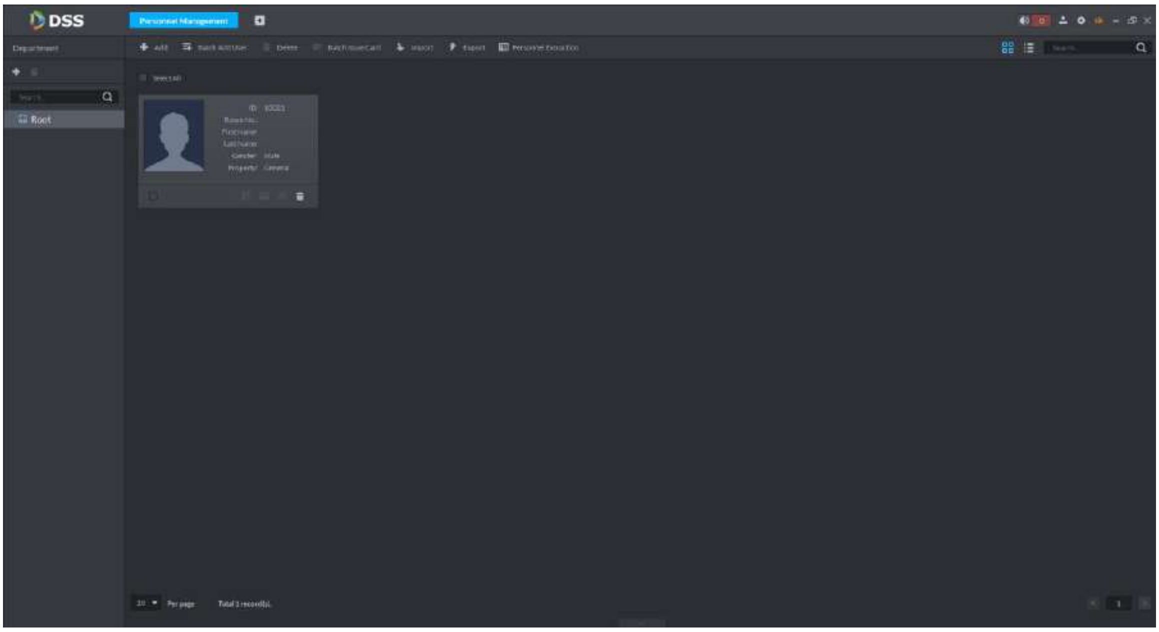
5.15.6 Personnel Extraction

Extract personnel info from access control and synchronize it to the platform.

Step 1 Click ⊞ and select **Personnel Management** on the homepage.

The interface of **Personnel Management** is displayed. See Figure 5-216.

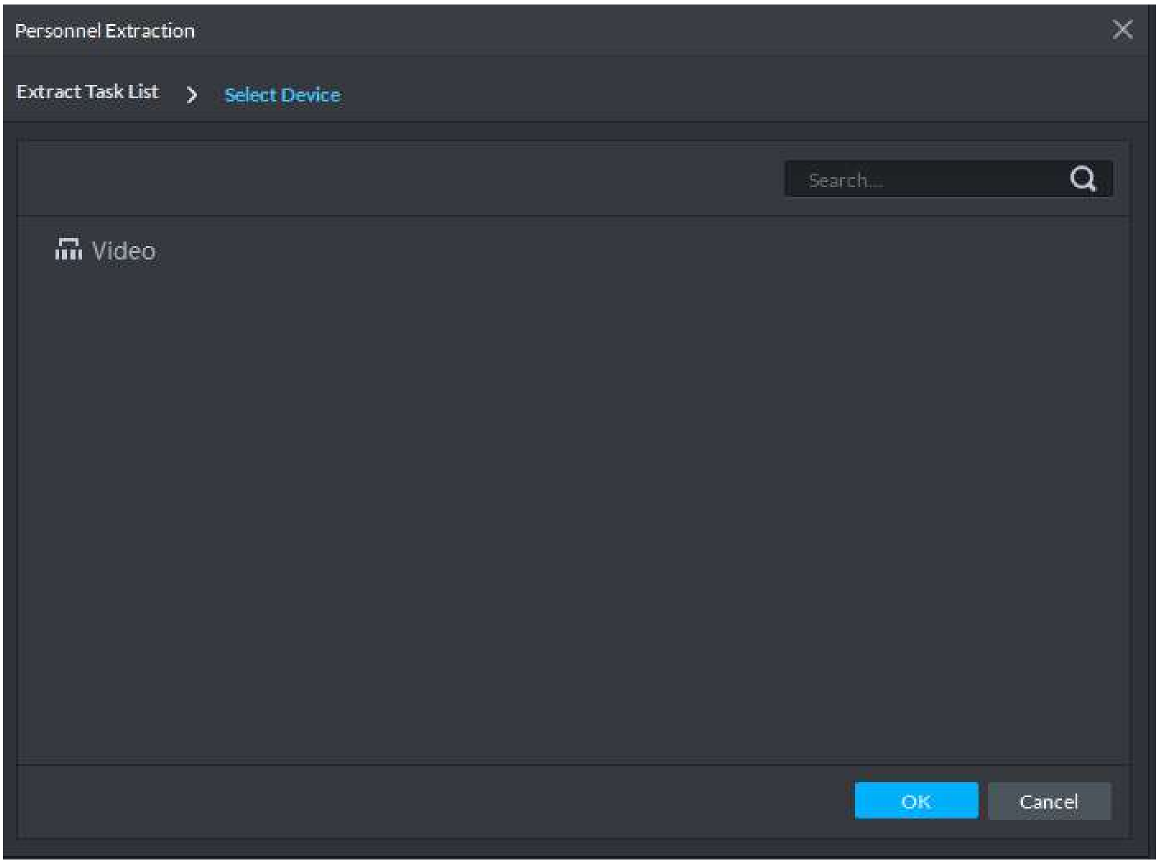
Figure 5-216 Personnel management



Step 2 Click **Personnel Extraction**.

The interface is displayed. See Figure 5-217.

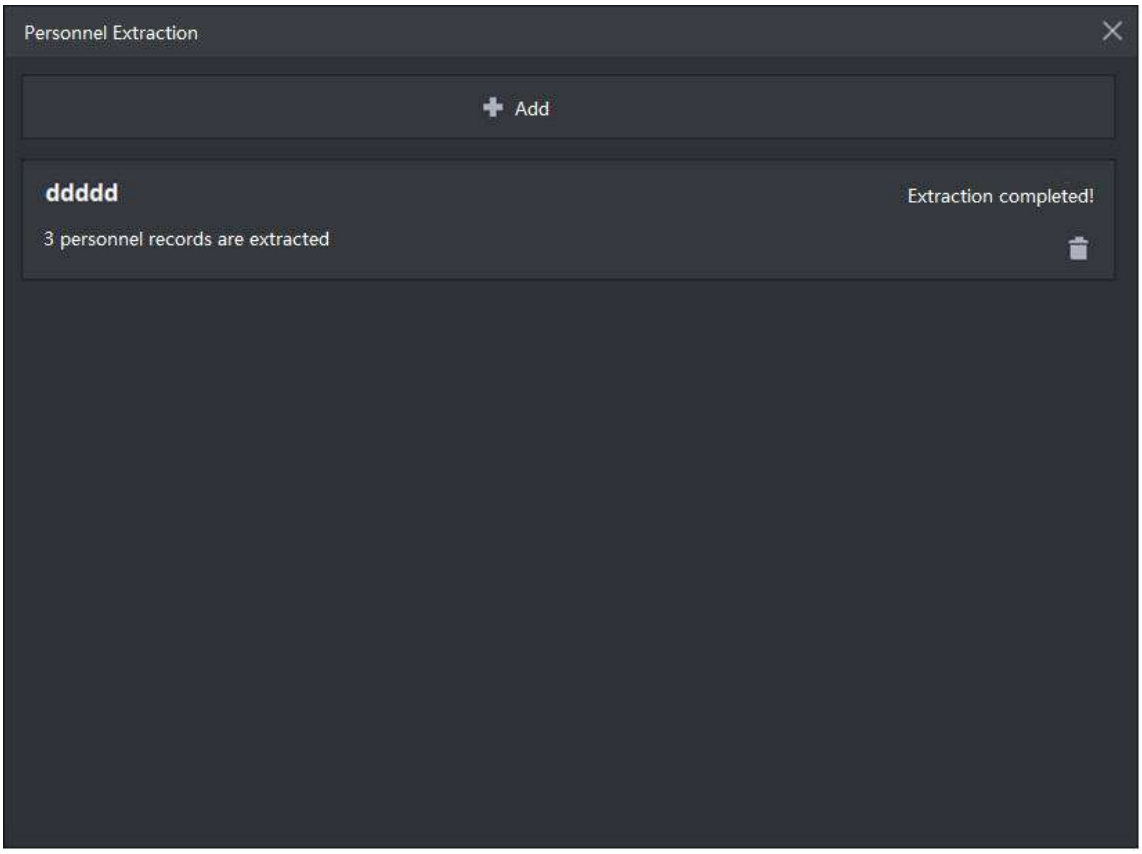
Figure 5-217 Personnel extraction



Step 3 Select access control device and click **OK**.

The extraction result is displayed. See Figure 5-218.

Figure 5-218 Personnel extraction result



ddddd

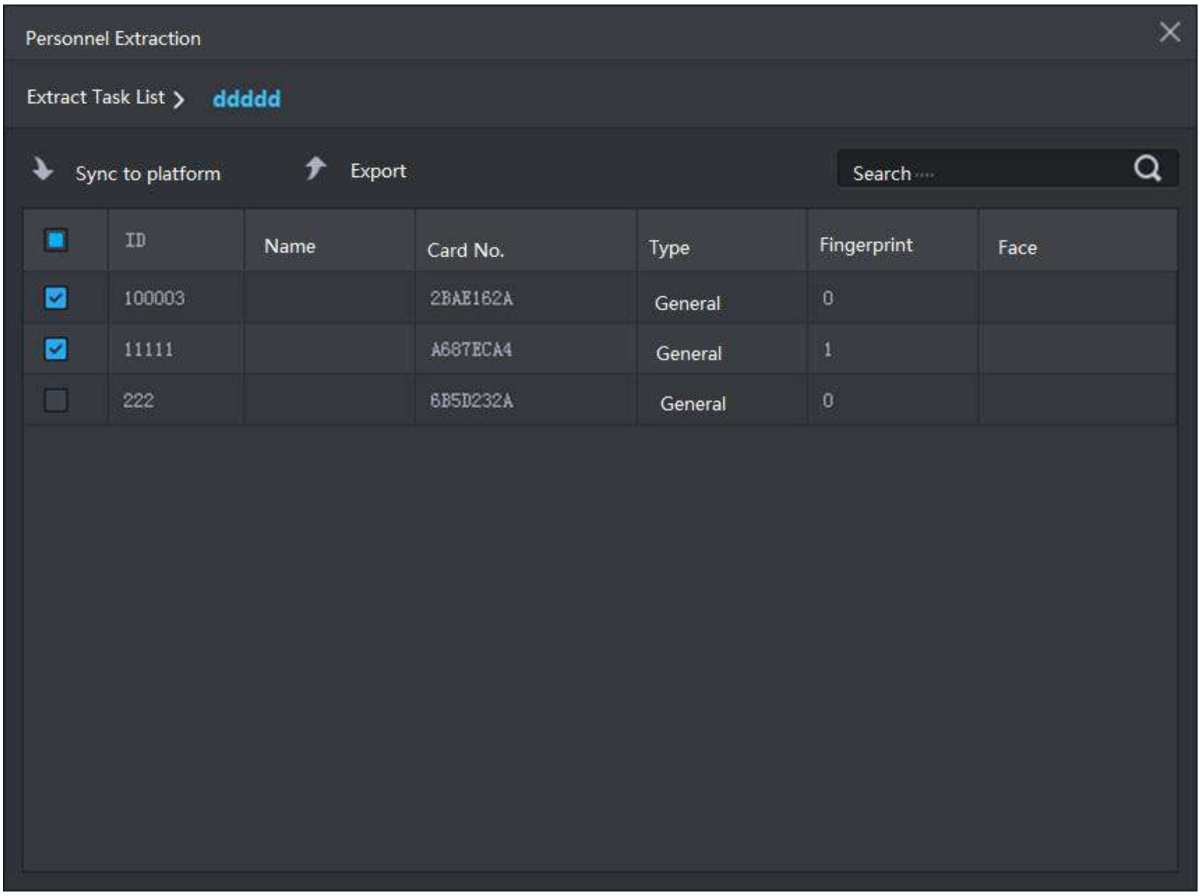
Extraction completed!

3 personnel records are extracted

Step 4 Double click the record.

The system displays the information of extracted personnel. See Figure 5-219.

Figure 5-219 Extracted personnel detail



■	ID	Name	Card No.	Type	Fingerprint	Face
☑	100003		2BAE162A	General	0	
☑	11111		A687ECA4	General	1	
□	222		6B5D232A	General	0	

Step 5 Select personnel, and click **Sync to Platform**.

Add the personnel to the list.

Select personnel, click Export and save personnel info to local PC.

5.15.7 Generate Path

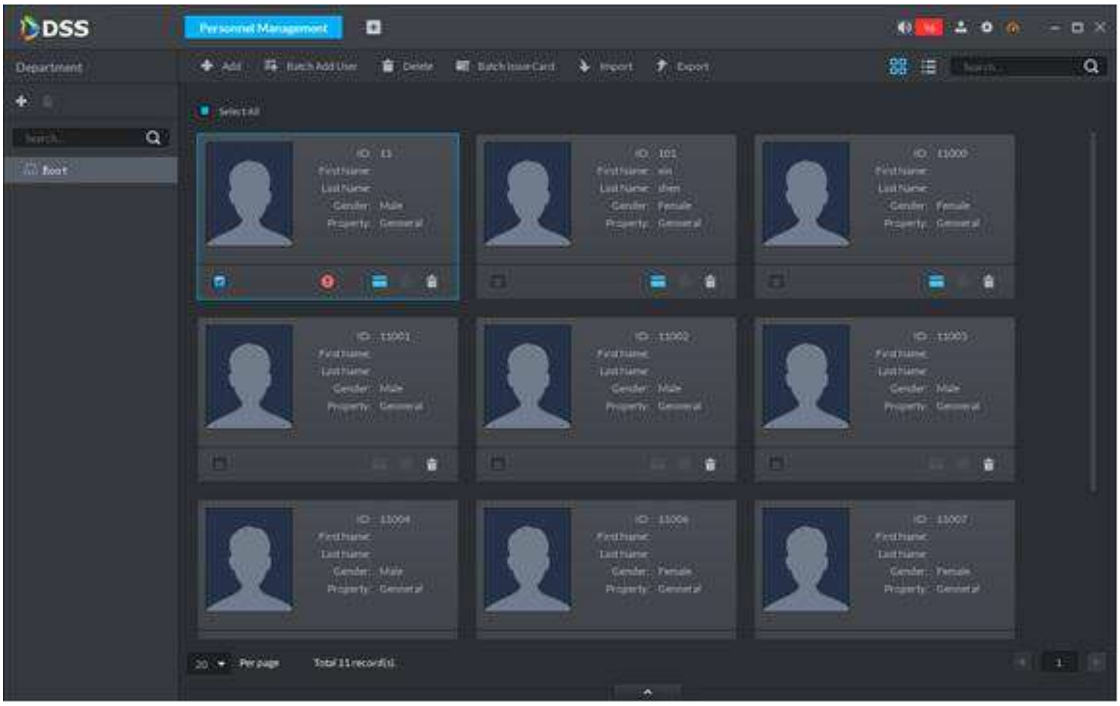
You can check all door unlocking records by personnel and generate a path.

To view the generated path, you have to drag the access control device to the map for display first. See Configure Maps for detailed steps.

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

The **Personnel Management** interface is displayed. See Figure 5-220.

Figure 5-220 Personel list



ID: 11
First Name:
Last Name:
Gender: Male
Property: General

ID: 101
First Name: xin
Last Name: shen
Gender: Female
Property: General

ID: 11000
First Name:
Last Name:
Gender: Female
Property: General

ID: 11001
First Name:
Last Name:
Gender: Male
Property: General

ID: 11002
First Name:
Last Name:
Gender: Male
Property: General

ID: 11003
First Name:
Last Name:
Gender: Male
Property: General

ID: 11004
First Name:
Last Name:
Gender: Male
Property: General

ID: 11006
First Name:
Last Name:
Gender: Female
Property: General

ID: 11007
First Name:
Last Name:
Gender: Female
Property: General

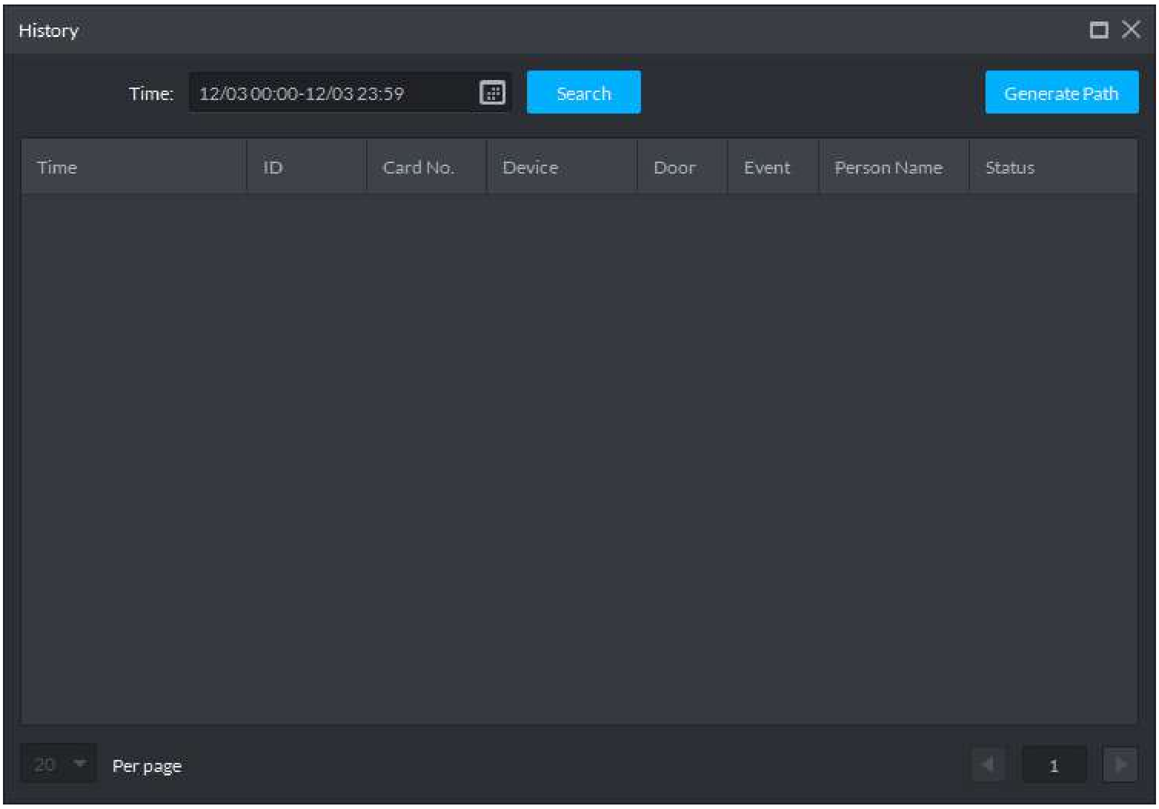
20 Per page Total 11 record(s).

1

Step 2 Click ▭ or ▯ of the person.

Step 3 The **History** interface is displayed. See Figure 5-221.

Figure 5-221 History record



Time: 12/03 00:00-12/03 23:59

Time	ID	Card No.	Device	Door	Event	Person Name	Status

20 Per page 1

Step 4 Set up time for the search and click **Search**.

The system displays the search results.

Step 5 Click **Generate Path**.

The system displays the map interface to show the activity path of the person.

Step 6 Click **Export**, and drag the mouse on the interface to select a region. Follow the instructions on the interface and save it in the form of picture to a local disk.

5.16 Access Control

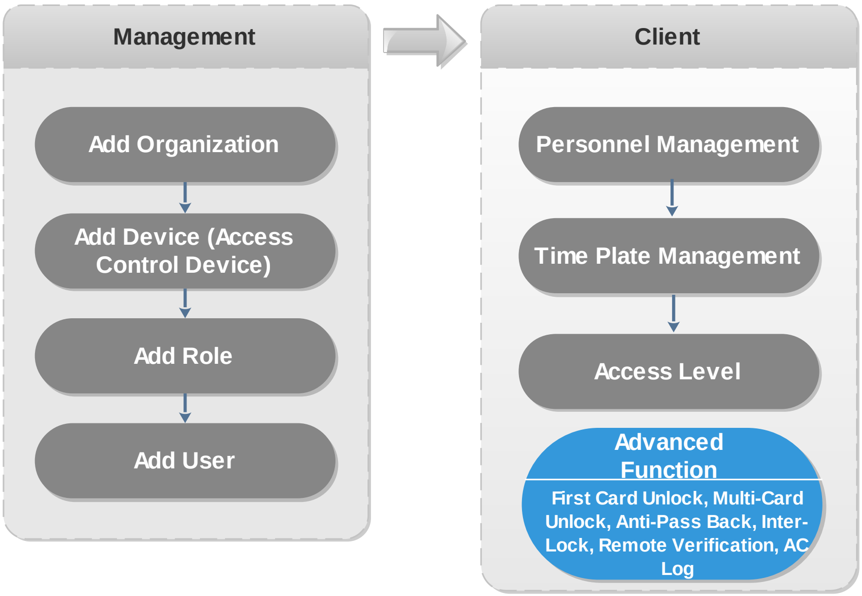
After adding access control devices on platform, you can control the door locking/unlocking on Pro, view videos and events related to the access control channel, and configure advanced access control functions, such as First Card Unlock and Multi-card Unlock.

5.16.1 Preparations

- You have added ACS on the platform's administrator end and bound resources. See 4.5 for specific steps.
- You have added personnel. See 5.15 Personnel Management for detailed steps.

For the access control procedures, see Figure 5-222.

Figure 5-222 Access control business flow


Management
Add Organization
Add Device (Access Control Device)
Add Role
Add User
Client
Personnel Management
Time Plate Management
Access Level
Advanced Function
First Card Unlock, Multi-Card Unlock, Anti-Pass Back, Inter-Lock, Remote Verification, AC Log

5.16.2 Console

On the console, you can control unlocking and locking of the access control channel, view linked videos and events, and enter the Door Config interface.

5.16.2.1 Configure Door Information

You can configure Door Status, NO/NC Period, Alarm Enable, Unlock Length and more.

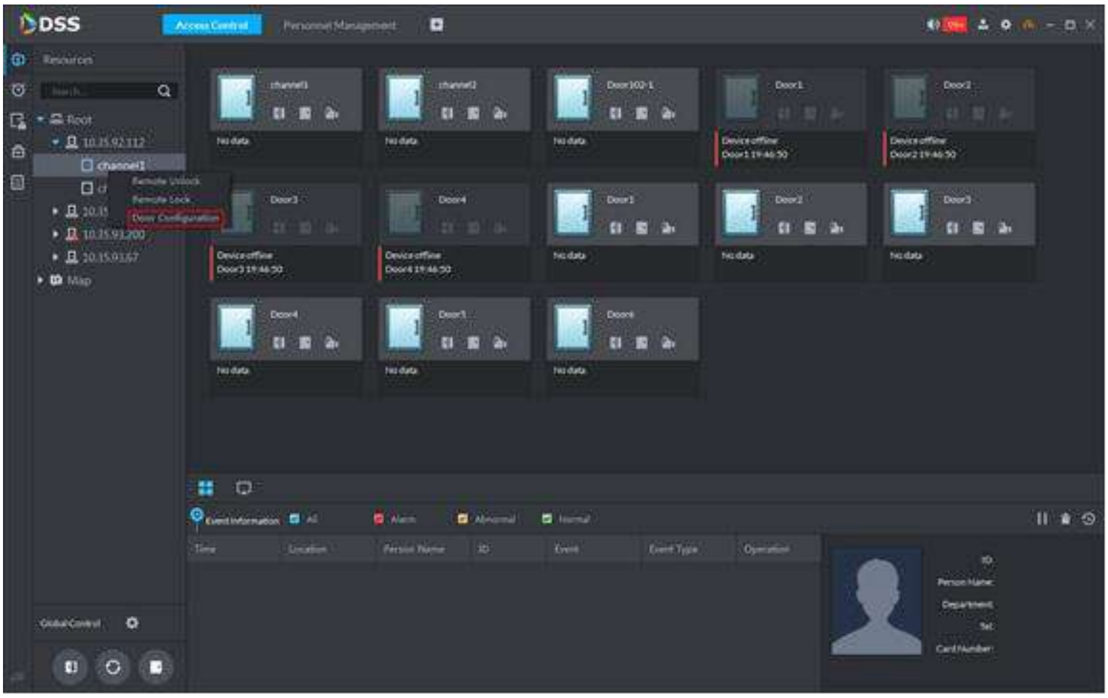
Step 1 Click ⊞. On the **Homepage** interface, select **Access Control**.

The **Access Control** interface is displayed.

Step 2 Click .

The **Console** interface is displayed. See Figure 5-223.

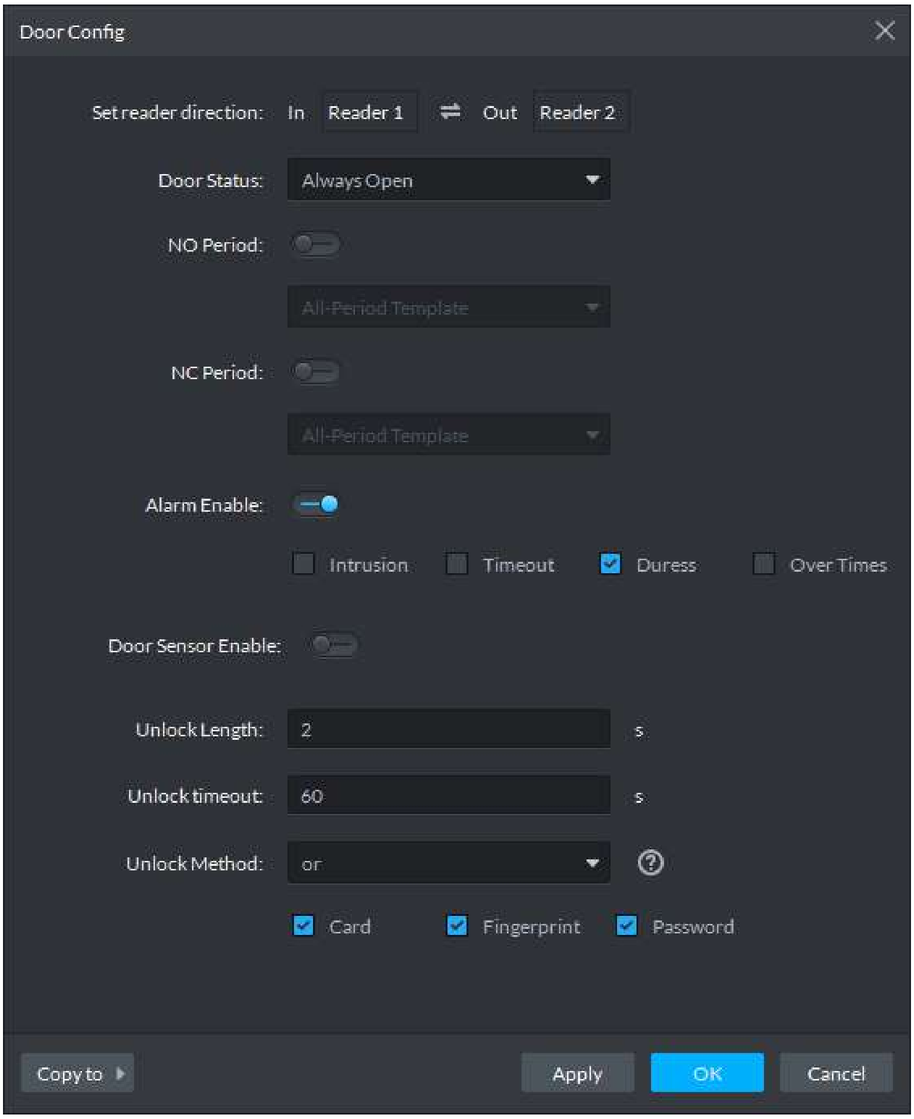
Figure 5-223 Console



Step 3 On the left side of the interface, right-click an access control channel in the device tree. In the popup menu, select **Door Configuration**.

Step 4 The **Door Config** interface is displayed. See Figure 5-224.

Figure 5-224 Door config



Set reader direction: In Reader 1 ⇄ Out Reader 2

Door Status: Always Open

NO Period: All-Period Template

NC Period: All-Period Template

Alarm Enable:

□ Intrusion □ Timeout ☑ Duress □ Over Times

Door Sensor Enable:

Unlock Length: 2 s

Unlock timeout: 60 s

Unlock Method: or

☑ Card ☑ Fingerprint ☑ Password

Step 5 Configure door information and click **OK**. For details of the parameters, see Table 5-38.

The screenshots might be different for different access control devices connected. The actual interfaces shall prevail.

Table 5-38 Door config description

Parameter	Description
Set reader direction	Indicates the in/out reader based on the wiring of ACS.
Door Status	Sets the access control status to Normal, Always Open, or Always Close.
NO Period	If enabled, you can set up a period during which the door is always open.
NC Period	If enabled, you can set up a period during which the door is always close.

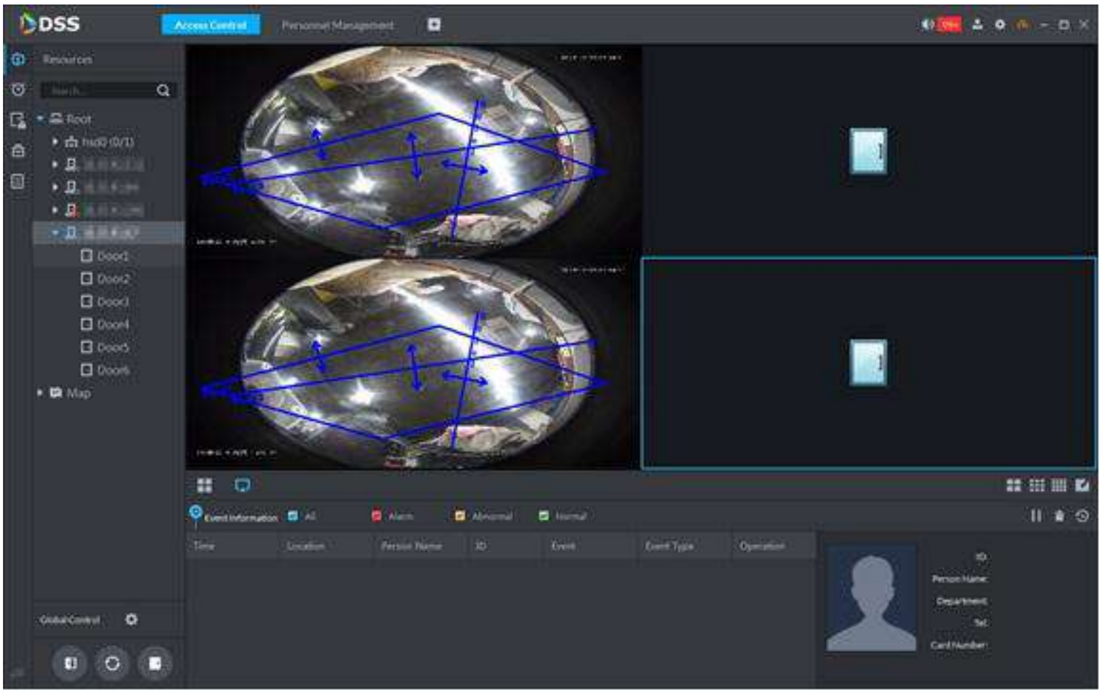
Parameter	Description
Alarm Enable	● If the door is opened not as intended, the door sensor is enabled and triggers an intrusion alarm. ● Entry with the Duress Card, Duress Password, or Duress Fingerprint triggers a duress alarm. ● Unlock duration exceeding the **Unlock timeout** triggers a timeout alarm. ● Swiping an illegal card for more than five times triggers a malicious alarm.
Door Sensor Enable	Enables the door sensor. The intrusion alarm and timeout alarm take effect only when door sensor is enabled.
Unlock Length	Sets up the duration of door unlocking. The door is automatically locked when the duration is over.
Unlock timeout	Unlock duration exceeding the **Unlock timeout** triggers a timeout alarm.
Unlock Method	You can use any one of the methods, card, fingerprint, face, and password, or any of their combinations to unlock the door.
Inter-door Lock	Indicates whether to enable Inter-door Lock.
Malicious Alarm	Swiping an unauthorized card for five times continuously within 50s triggers a malicious alarm. In the next 50s, every swipe of the card triggers a same alarm.

5.16.2.2 View Videos Bound to Channels

When adding access control devices, if you have already bound a video channel to the channel, you can preview the real-time videos of the bound video channels on the console. To bind video channels, see **4.5.5 Binding Resource.**

- On the right side of the console interface, click 📹 in the access control channel list. The system displays videos in real time. See Figure 5-225.
- Click 🖥 on the console interface. The system displays the video interface. Drag the access control channel on the left side of the screen to the preview interface on the right side. The system displays videos in real time. See Figure 5-225.

Figure 5-225 Link channel video



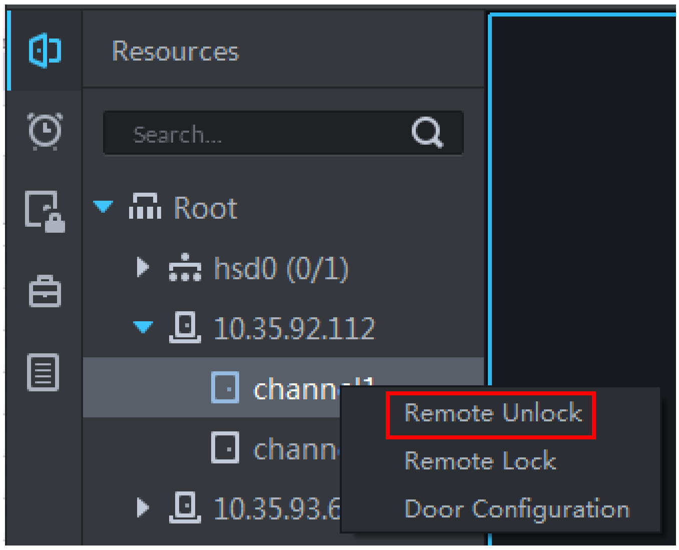
5.16.2.3 Manual Unlock

In addition to Always Open or linked unlock in specified periods, the console also supports unlocking by manually controlling the access control channel. After unlock, the door automatically locks up after a specified time period (5s by default, and 10s in this example) set up in Door Config.

You can unlock the door in the following ways:

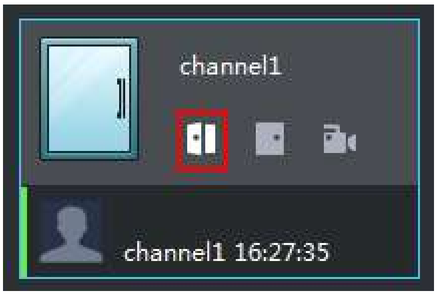
- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Unlock** in the popup menu. See Figure 5-226. After unlocking, the door status in the access control channel list on the right side of the interface changes to open, as.

Figure 5-226 Unlock(1)



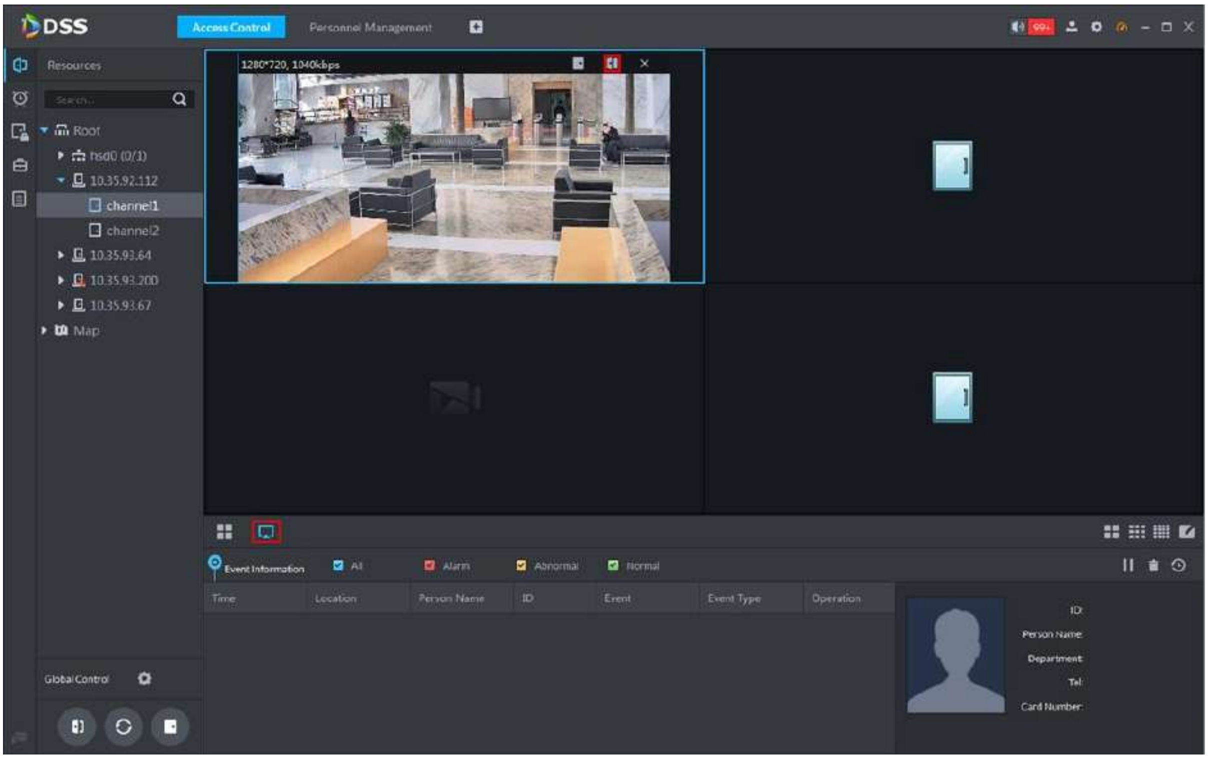
- Click on the door channel interface to unlock the door. See Figure 5-227. After unlocking, the door status in the access control channel list on the right side of the interface changes to open, as

Figure 5-227 Unlock(2)



- When viewing videos bound to the channel, click on the video interface to unlock the door. See Figure 5-228.

Figure 5-228 Unlock(3)



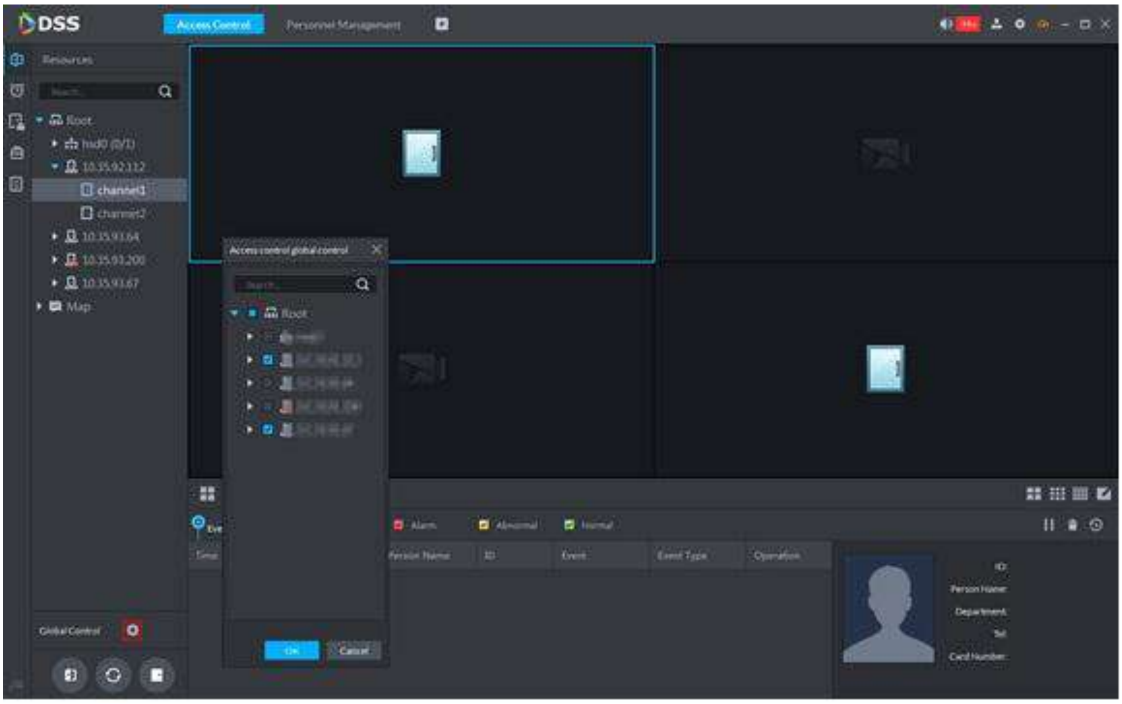
- Temporary Always Open of multiple doors

  Select a door channel through global control and you can set the door to be Always Open. Recovery to normal status after unlocking requires manual operations.

Step 1 Click on the bottom left of the console interface of the Access Control module.

Step 2 The **Access control global control** interface is displayed. See Figure 5-229.

Figure 5-229 Global control



Step 3 Select an access control channel to be set to Always Open via global control, and click **OK**.

Step 4 Click **Always Open** on the bottom left of the interface.

The **Password Verification** interface is displayed.

Step 5 Input current user's password, and click **OK**.

Step 6 All the doors of the selected access control channels are set to Always Open. The status of all the doors in the access control channel list on the right side of the interface changes to open, as . The interface control changes from **Always Open** to **Recover**.

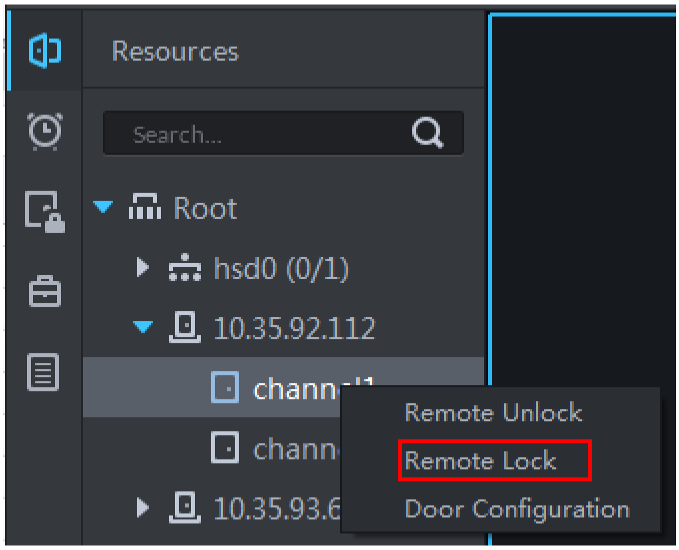
Click **Recover** and the doors return to normal status.

5.16.2.4 Manual Lock

In addition to Always Close or linked lock in specified periods, the console also supports locking by manually controlling the access control channel. You can lock the door in the following ways:

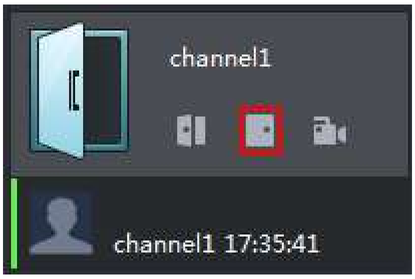
- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Lock** in the popup menu. See Figure 5-230. After locking, the door status in the access control channel list on the right side of the interface changes to closed, as .

Figure 5-230 Lock(1)



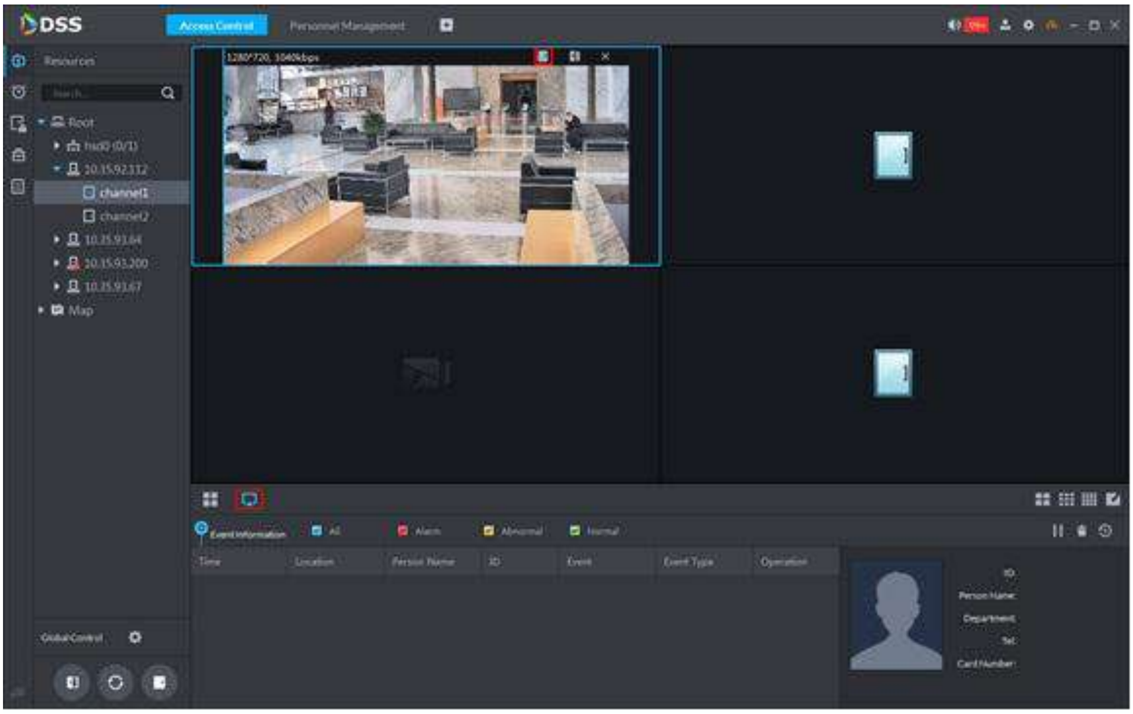
- Click on the door channel interface to lock the door. See Figure 5-231. After locking, the door status in the access control channel list on the right side of the interface changes to closed, as.

Figure 5-231 Lock(2)



- When viewing videos bound to the channel, click on the video screen to lock the door. See Figure 5-232.

Figure 5-232 Lock(3)



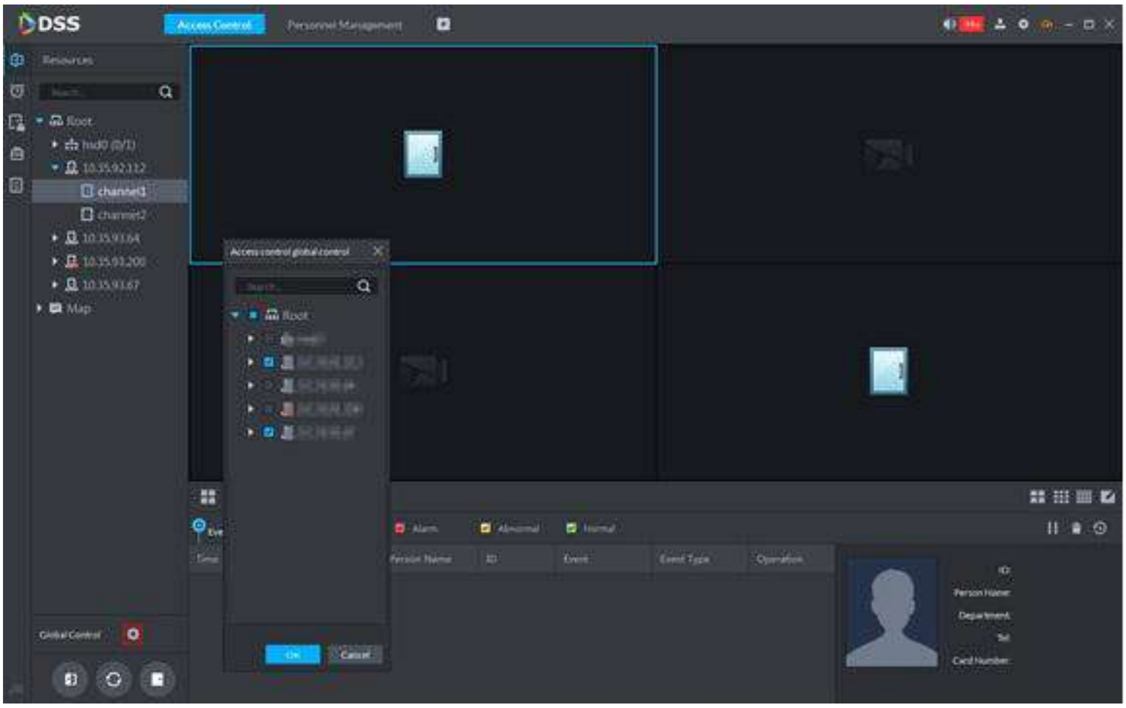
- Temporary Always Open of multiple doors

  Select a door channel through global control and you can set the door to be Always Close. Recovery to normal status after locking requires manual operations.

Step 1 Click ⚙ on the bottom left of the console interface of the Access Control module.

Step 2 The **Access control global control** interface is displayed. See Figure 5-233.

Figure 5-233 Global control



Step 3 Select an access control channel to be set to Always Close via global control, and click **OK**.

Step 4 Click **Always Close** on the bottom left of the interface.

The **Password Verification** interface is displayed.

Step 5 Input current user's password, and click **OK**.

Step 6 All the doors of the selected access control channels are set to Always Close. The status of all the doors in the access control channel list on the right side of the interface changes to closed, as . The interface control changes from **Always Close** to **Recover**.

Click **Recover** and the doors return to normal status.

5.16.2.5 View Event Details

Supports viewing details of the events reported on door locking and unlocking, including: Event Info, Live View, Snapshot, and Recording.

- Live View is only available when a video channel is bound to the access control channel. To bind video channels, see Bind Resources.
- When snapshot and video recording require configuring event management, access control-related alarm devices are linked with the camera.
- The console displays all event information except for locking related info, including unlock, duress unlock, invalid swipe.

Step 1 In the event list below the console interface, click next to the event records.

Step 2 The **ACS Event Info** interface is displayed. See Figure 5-234. See Table 5-39 for more descriptions on the controls.

Figure 5-234 Event info

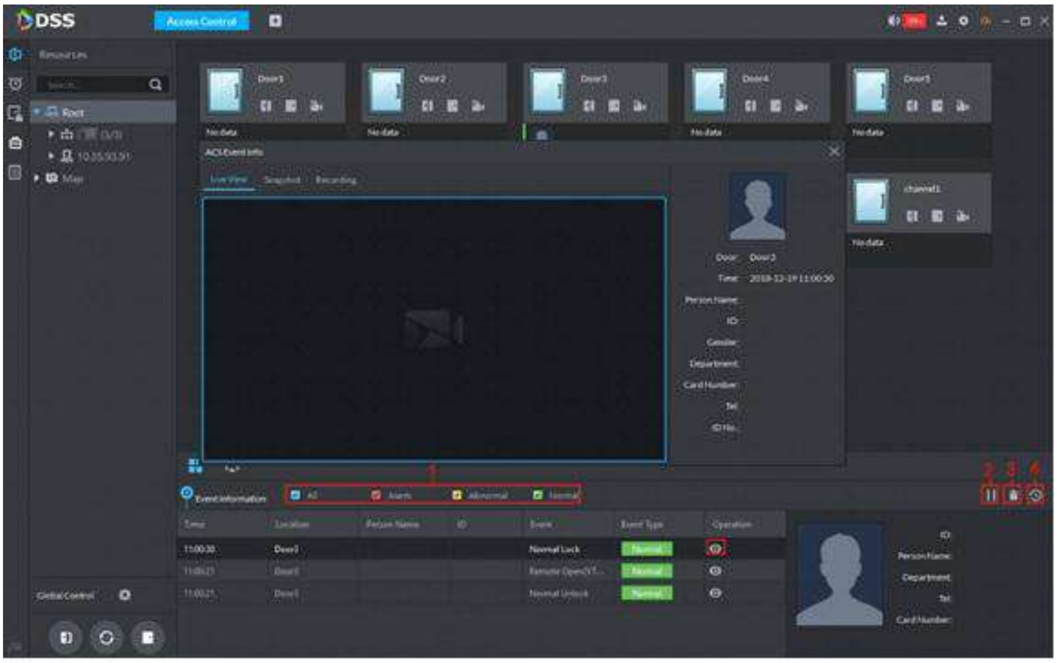


Table 5-39 Operation description

No.	Description
1	You can choose to view the events of certain event types. For instance, if you select **Normal**, the list only displays **normal** events.

No.	Description
2	● Click ⏸ to stop displaying reported event information. In this case, the interface no longer displays the reported new events. After clicking, the button changes to ▶. ● Click ▶ to start refreshing reported event information. The interface does not display events during the stopping period. After clicking, the button changes to ⏸.
3	Clearing the events from the current event list, does not delete them from the log.
4	Click to jump to the **A&C Log** interface.

Step 3 Click the corresponding tab to view the live view, snapshots, and video recordings of the linked video channel.

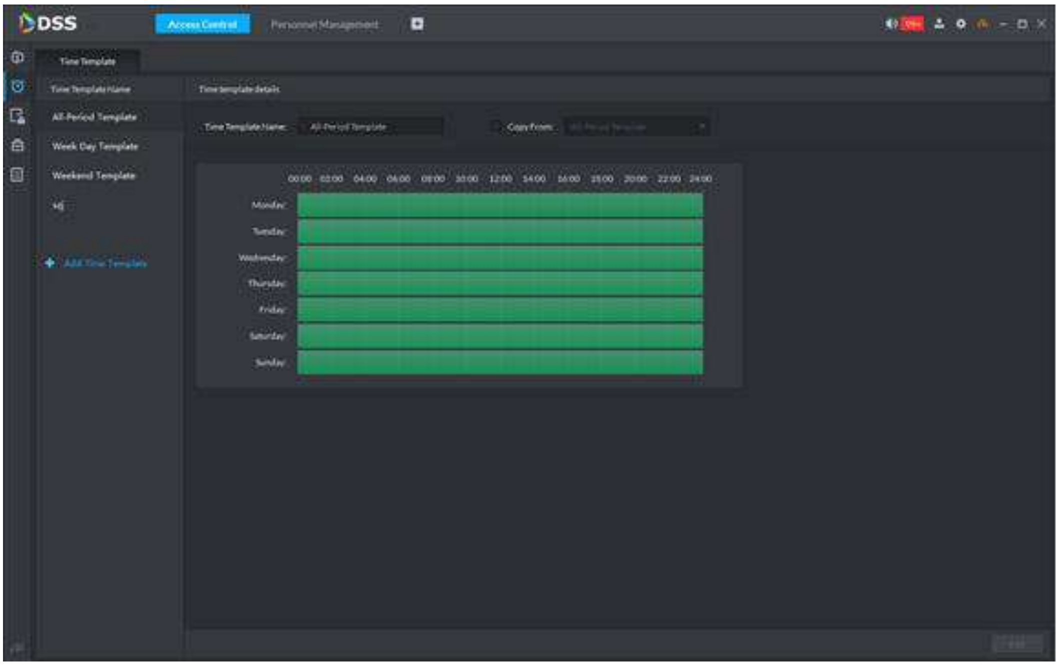
5.16.3 Setting Time Template

You can apply various unlock strategies in the time template. For example, you can use First Card Unlock in the selected time template.

Step 1 On the **Access Control** interface, click ⏰.

Step 2 The **Time Template** interface is displayed. See Figure 5-235.

Figure 5-235 Time template

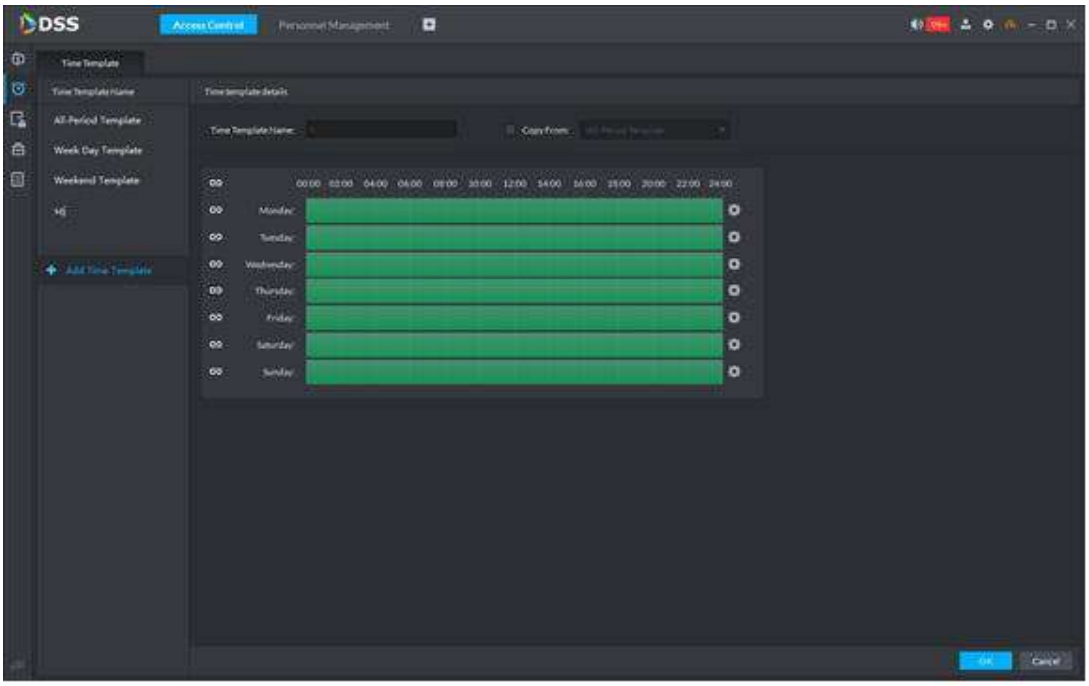


Time Template Name: All-Period Template

Step 3 Click Add Time Template.

The **Time template details** interface is displayed. See Figure 5-236.

Figure 5-236 Time template detail



Step 4 Set up **Time Template Name** and the required time period, and click **OK**.

Select **Copy From** and the copied template, and you can use the time periods of the copied template. In this way, you can quickly configure the time periods by modifying the ones of the copied template.

Methods to set up the time period:

- Method I: Press and hold the left button of the mouse. Over the time periods not selected, the mouse displays as a pen, and you can drag the mouse on the setting interface to select a time period. Over the selected time periods, the mouse displays as an eraser, and you can erase selected time periods with it.

  Click the icons ⛓ in front of multiple week numbers one by one and the icons change to ⛓. In this way, you can configure the time periods corresponding to the week numbers. You can quickly select all the week numbers by clicking ⛓ on the top.

- Method II: Click ⚙ and set up the time periods in the popup interface. You can set up six time periods at most.

Step 5 After setting up, the time templates display in the list on the left side.

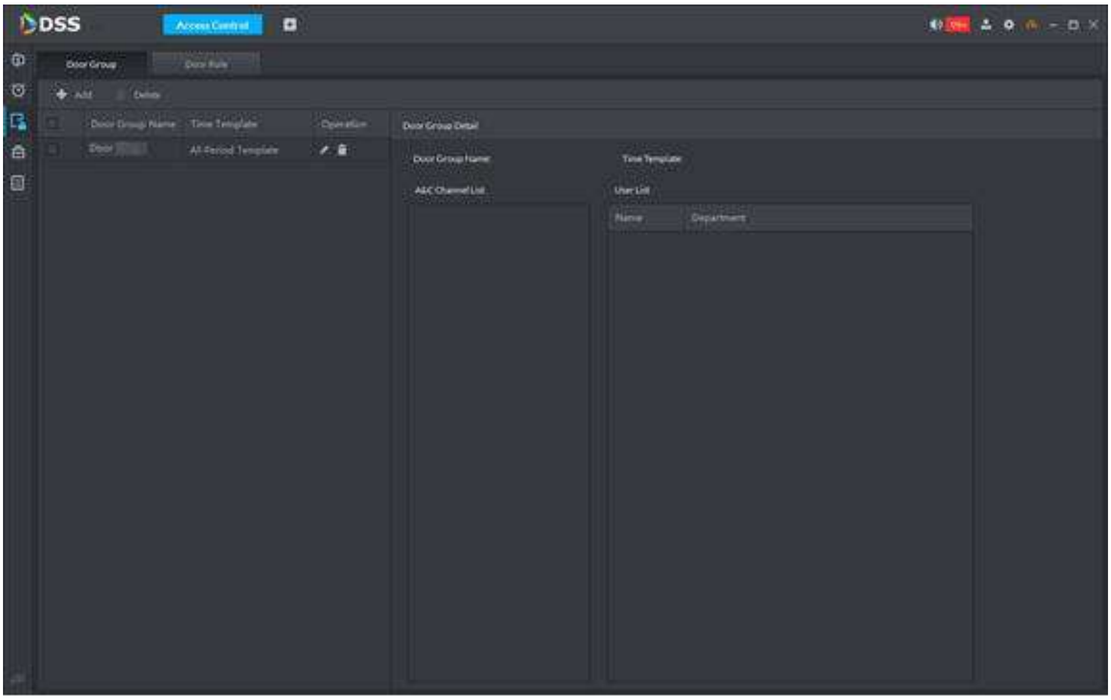
5.16.4 Setting Door Group Permissions

If you manage the doors by groups, you can quickly grant users with the authorizations to unlock the doors in a specific group.

Step 1 On the **Access Control** interface, click 🔒.

Step 2 The **Access Level** interface is displayed. See Figure 5-237.

Figure 5-237 Access level



Door Group Name	Time Template	Operation
Door	All-Period Template	

Name	Department

Step 3 Create door groups.

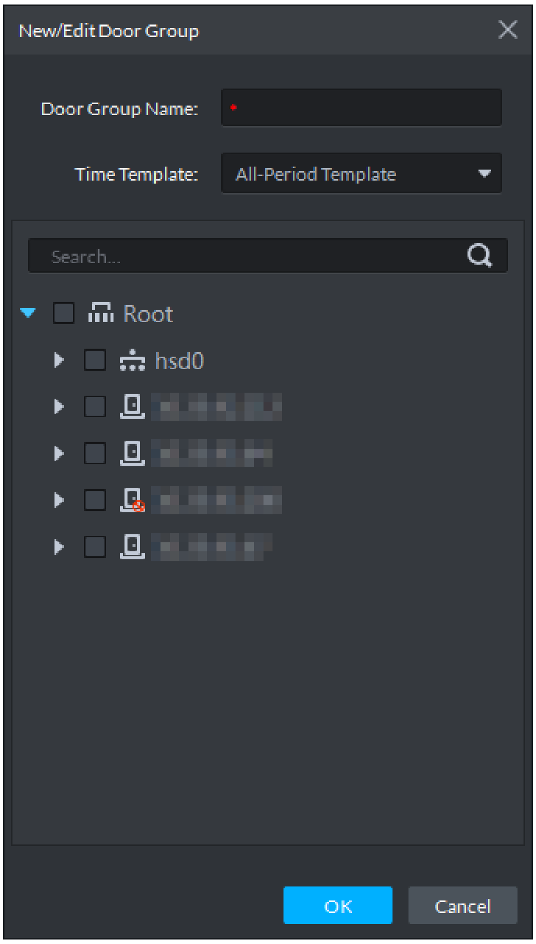
1) Click the **Door Group** tab.

   The **Door Group** interface is displayed.

2) Click **Add**.

   The **New/Edit Door Group** interface is displayed. See Figure 5-238.

Figure 5-238 New/edit door group



New/Edit Door Group

Door Group Name: *

Time Template: All-Period Template

3) Input **Door Group Name**, select **Time Template** and an access control channel, and click **OK**.

   After selecting the time template and access control channel, you can only use the time periods of the selected time template and the selected access control channel when granting authorizations to users. The interface displays the information of the newly created door groups.

Step 4 Authorize users.

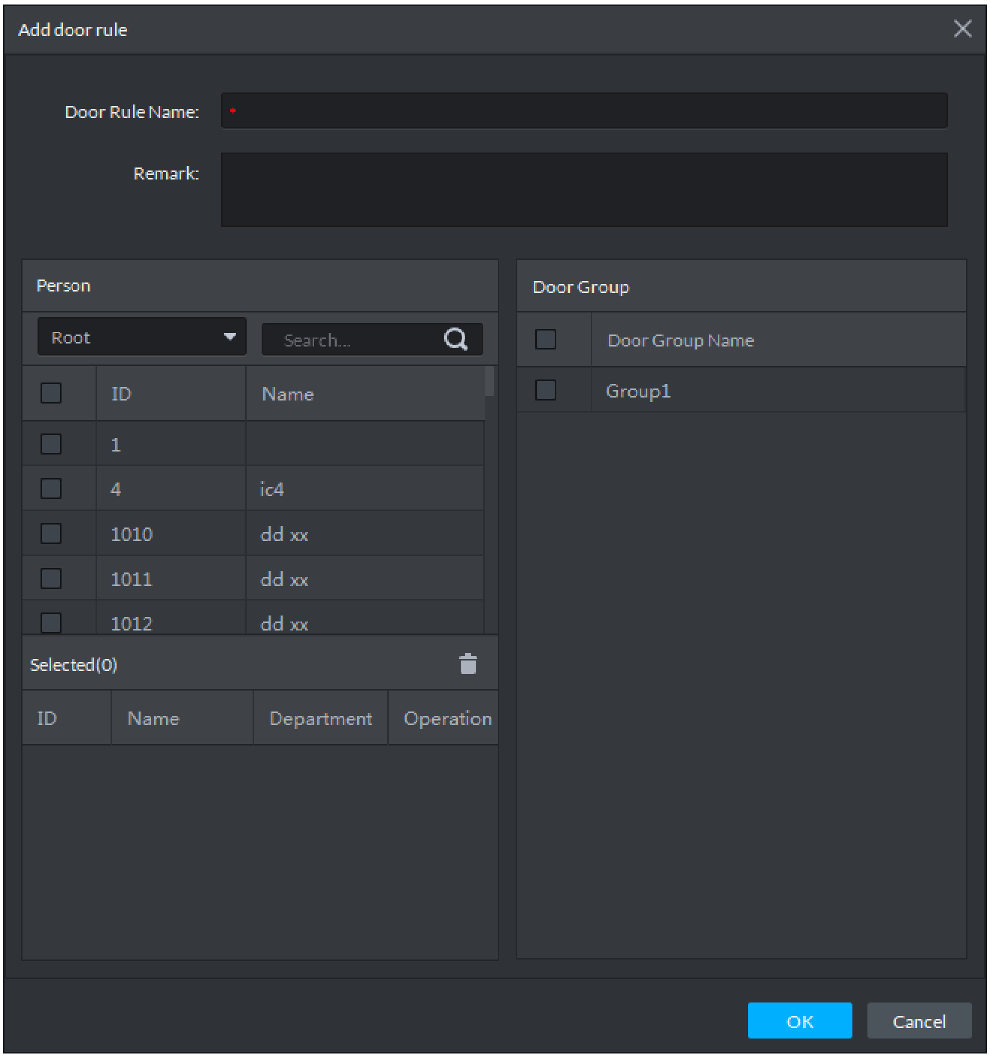
1) Click the **Door Rule** tab.

   The **Door Rule** interface is displayed.

2) Click **Add**.

   The **Add door rule** interface is displayed. See Figure 5-239.

Figure 5-239 Add door rule



□	ID	Name
□	1	
□	4	ic4
□	1010	dd xx
□	1011	dd xx
□	1012	dd xx

ID	Name	Department	Operation

□	Door Group Name
□	Group1

3) Input **Door Rule Name**, select **Person** and **Door Group**, and click **OK**. The interface displays the authorization information.

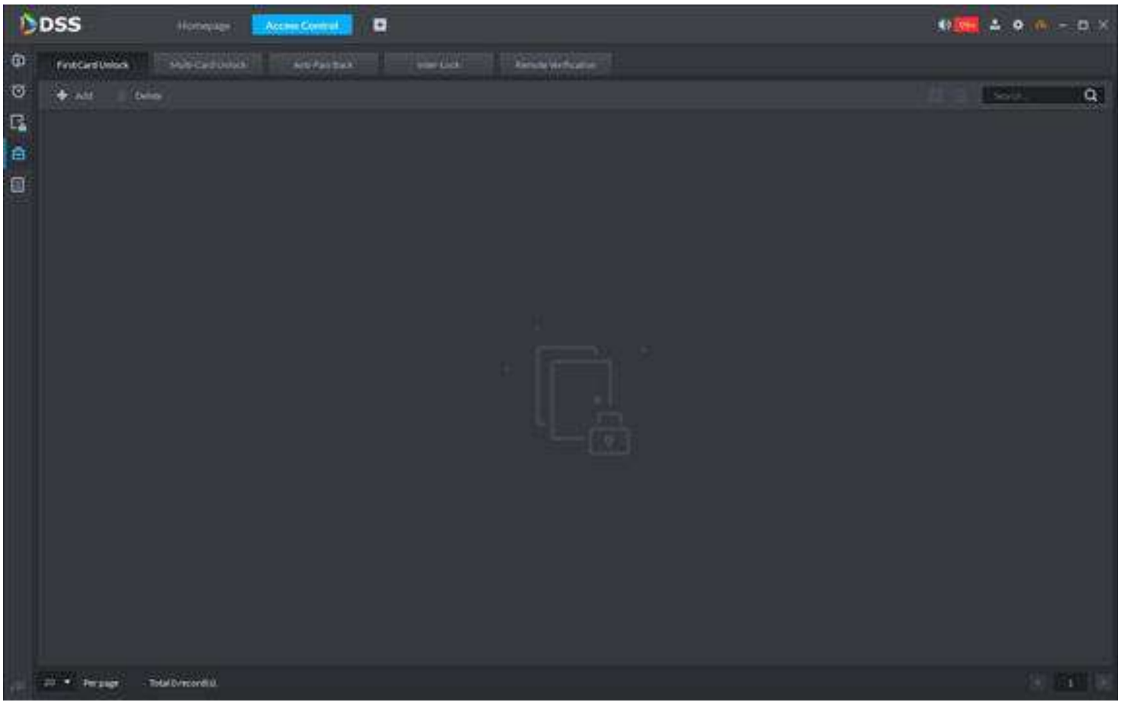
5.16.5 First Card Unlock

Only after the specified first-card user swipes the card every day can other users unlock the door with their cards. You can set up multiple first cards. Only after any one of the users swipes the first card can other users without first cards unlock the door with their cards.

Step 1 On the **Access Control** interface, click .

Step 2 The **Advanced Function** interface is displayed. See Figure 5-240.

Figure 5-240 Advanced function



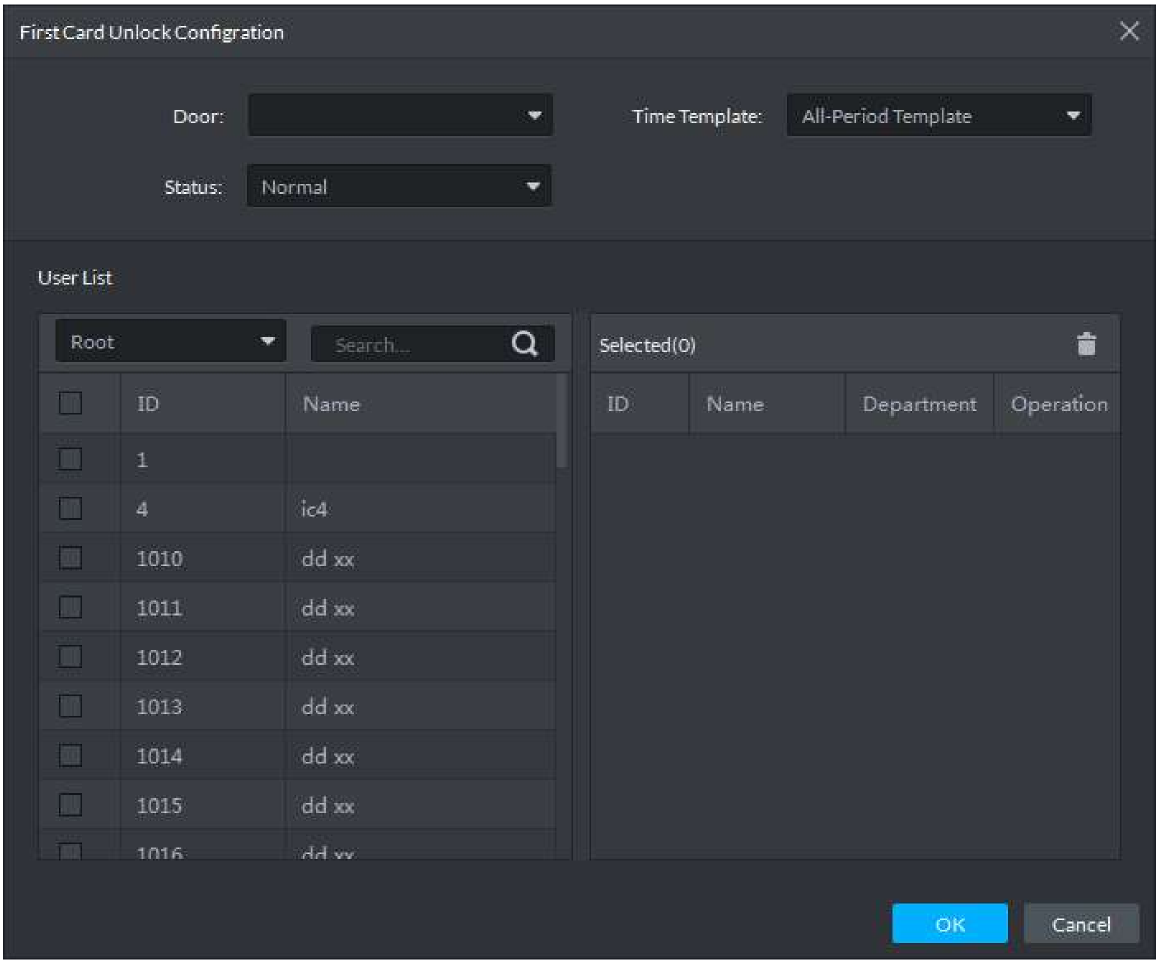
Step 3 Click the First Card Unlock tab.

The **First Card Unlock** interface is displayed.

Step 4 Click **Add**.

The **First Card Unlock Configuration** interface is displayed. See Figure 5-241.

Figure 5-241 First card unlock config



First Card Unlock Configration

Door:

Time Template: All-Period Template

Status: Normal

User List

Root

Search...

□	ID	Name
□	1	
□	4	ic4
□	1010	dd xx
□	1011	dd xx
□	1012	dd xx
□	1013	dd xx
□	1014	dd xx
□	1015	dd xx
□	1016	dd xx

Selected(0)

ID	Name	Department	Operation

OK

Cancel

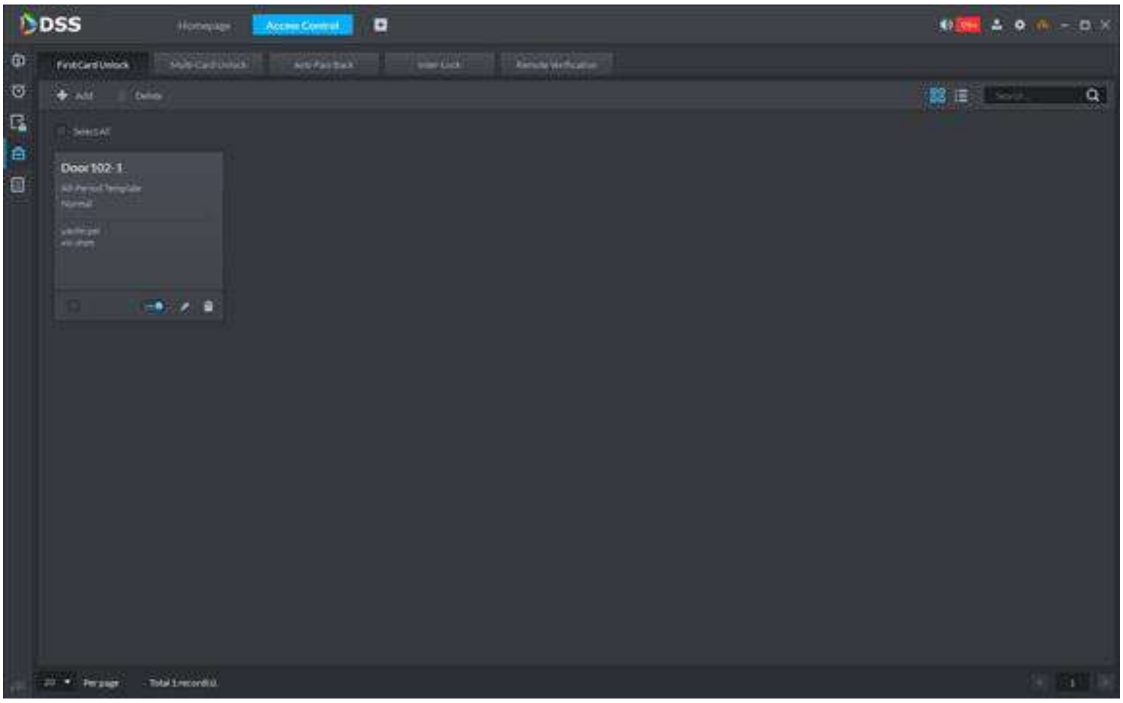
Step 5 Configure the First Card Unlock parameters and click **OK**. For details of the parameters, see Table 5-40.

Step 6 The system displays the First Card Unlock information. See Figure 5-242. First Card Unlock is enabled by default.

Table 5-40 First card unlock parameter description

Parameter	Description
Door	You can select the target access control channel to configure the first card unlock.
Time Template	First Card Unlock is valid in the time period of the selected time template.
Status	After First Card Unlock is enabled, the door is in either the Normal mode or Always Open mode.
User	You can select the user to hold the first card. Supports selecting a number of users to hold first cards. Any one of them swiping the first card means first card unlock is done.

Figure 5-242 First card info list



Step 7 Click ○.

Step 8 The icon changing into ● indicates First Card Unlock is enabled.

5.16.6 Multi-Card Unlock

In this mode, multiple groups of users have to swipe cards for an access control channel in an established sequence to unlock the door.

- One group can have up to 64 users.
- With Multi-Card Unlock enabled for an access control channel, it supports up to four groups of users being on site at the same time for verification. The total number of users can be 64 at most, with up to five valid users.

Step 1 On the **Access Control** interface, click.

The **Advanced Function** interface is displayed.

Step 2 Click the **Multi-Card Unlock** tab.

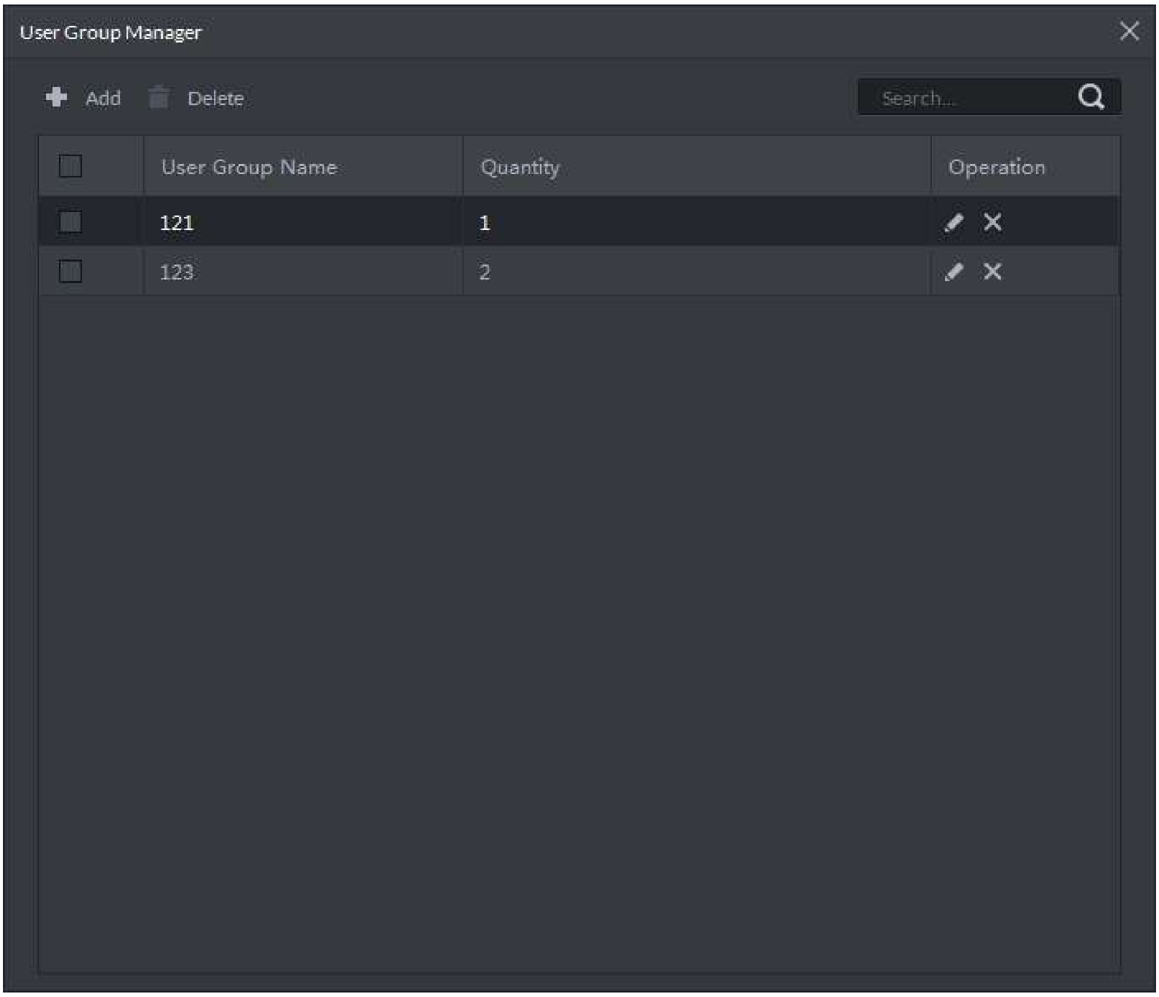
The **Multi-Card Unlock** interface is displayed.

Step 3 Add user group.

1) Click **Person Group**.

The **User Group Manager** interface is displayed. See Figure 5-243.

Figure 5-243 User group manager



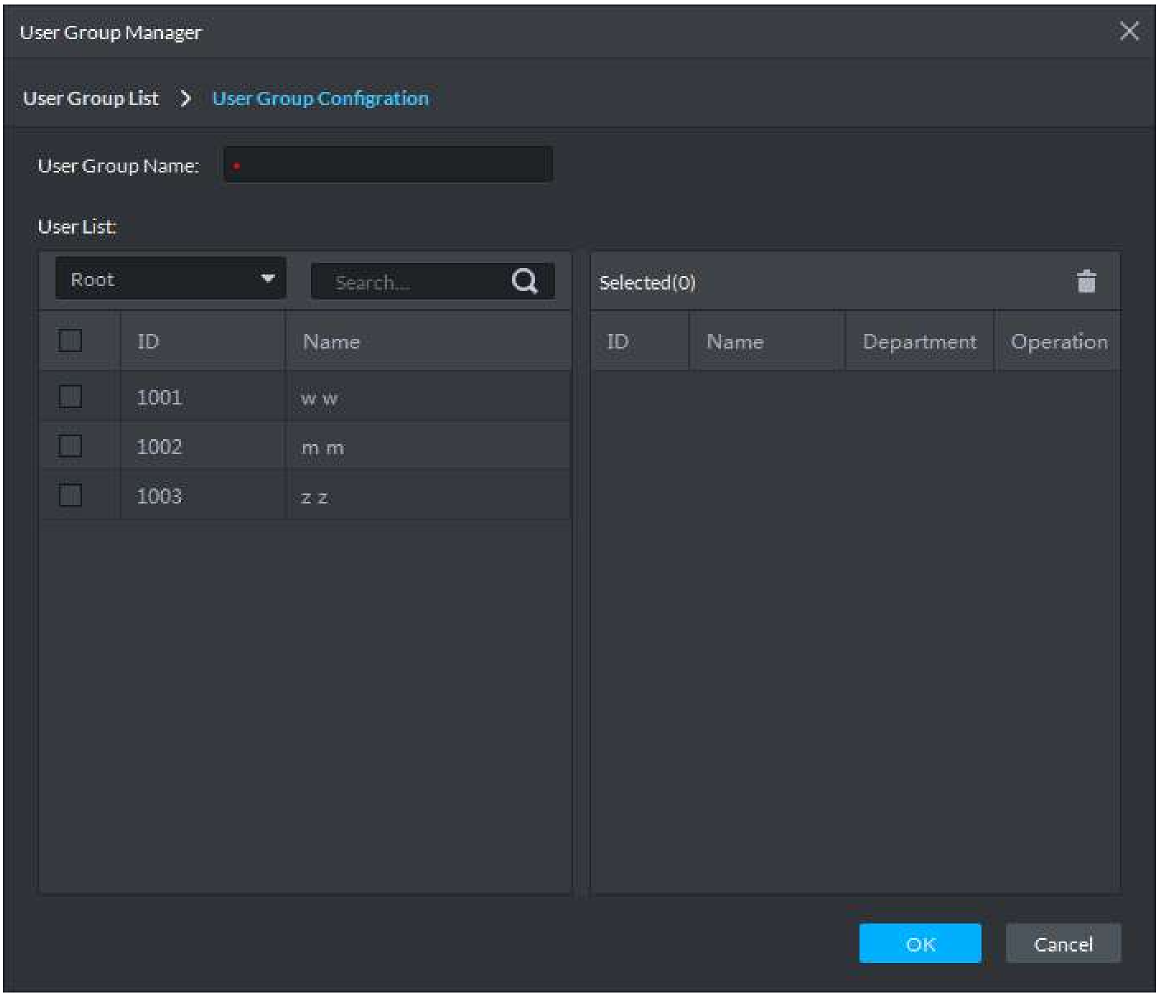
User Group Manager

□	User Group Name	Quantity	Operation
□	121	1	✎ ✕
□	123	2	✎ ✕

2) Click **Add**.

The **User Group Manager** interface is displayed. See Figure 5-244.

Figure 5-244 User group config



□	ID	Name
□	1001	w w
□	1002	m m
□	1003	z z

ID	Name	Department	Operation

3) Set up **User Group Name**. Select users from **User List** and click **OK**. You can select up to 64 users.

   The system displays the user group information.

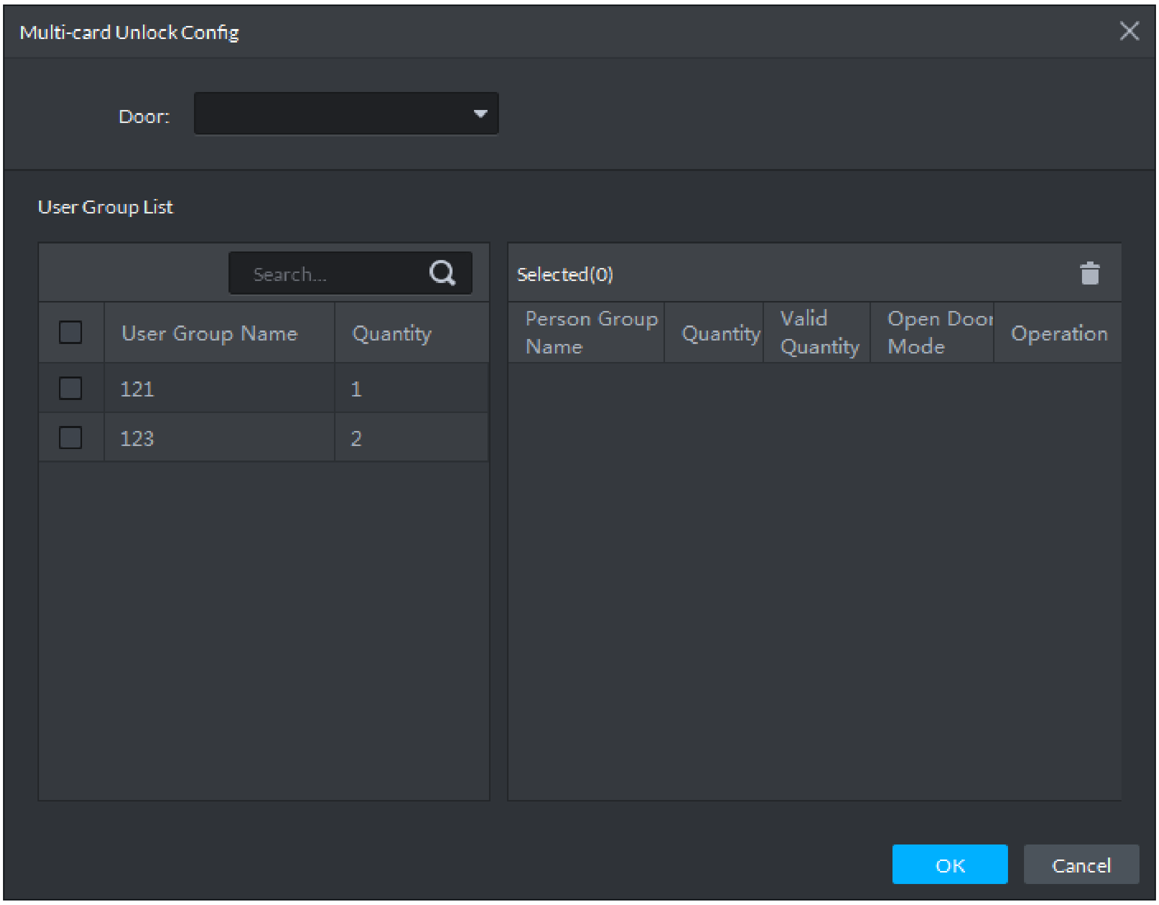
4) Click ☒ in the upper right corner of the **User Group Manager** interface.

Step 4 Config Multi-Card Unlock.

1) Click **Add**.

   The **Multi-card Unlock Config** interface is displayed. See Figure 5-245.

Figure 5-245 Multi-card unlock config



□	User Group Name	Quantity
□	121	1
□	123	2

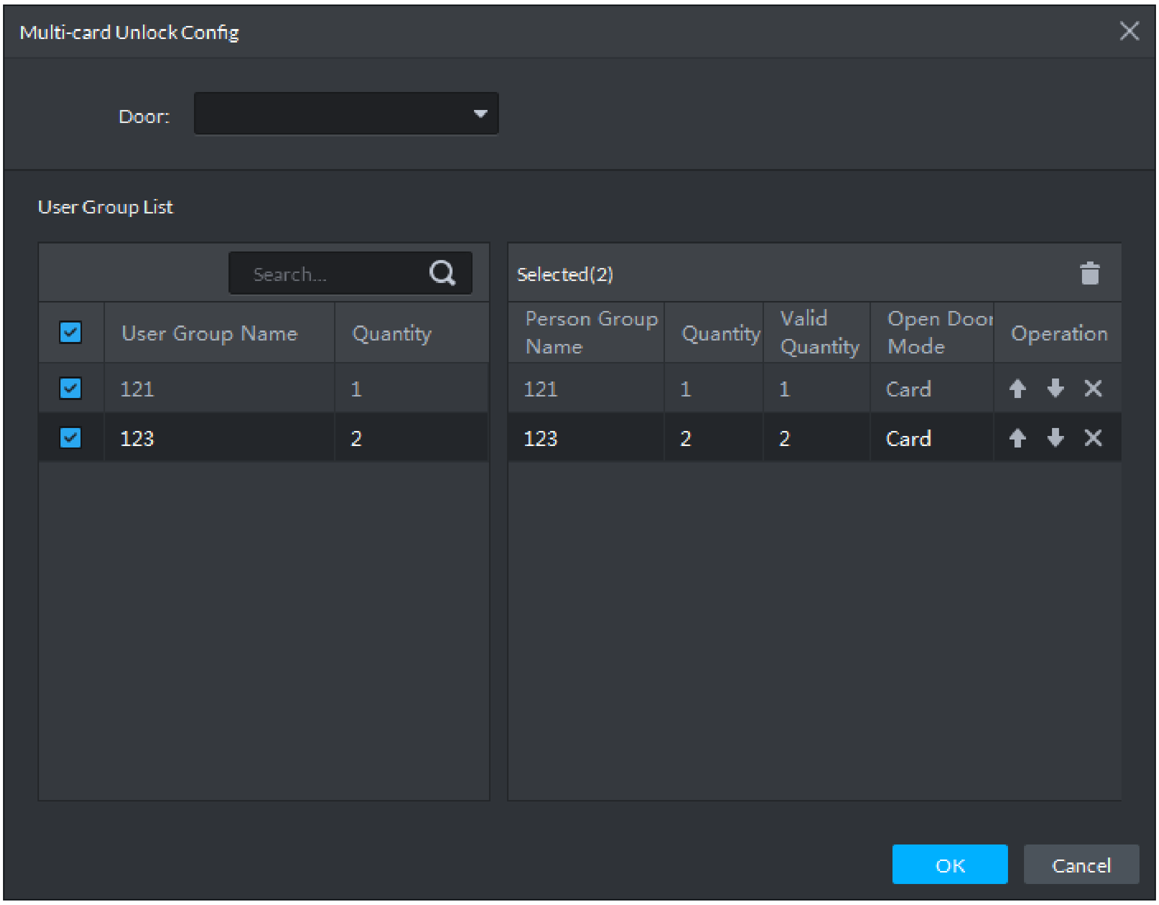
Person Group Name	Quantity	Valid Quantity	Open Door Mode	Operation

2) Select the door to set up Multi-Card Unlock.

3) Select the user group. You can select up to four groups.

The system displays the user group information. See Figure 5-246.

Figure 5-246 Select person group



Multi-card Unlock Config

Door:

User Group List

Search...

☑	User Group Name	Quantity
☑	121	1
☑	123	2

Selected(2)

Person Group Name	Quantity	Valid Quantity	Open Door Mode	Operation
121	1	1	Card	↑ ↓ ✕
123	2	2	Card	↑ ↓ ✕

4) Fill in the **Valid Quantity** for each group to be on site and the **Open Door Mode**.

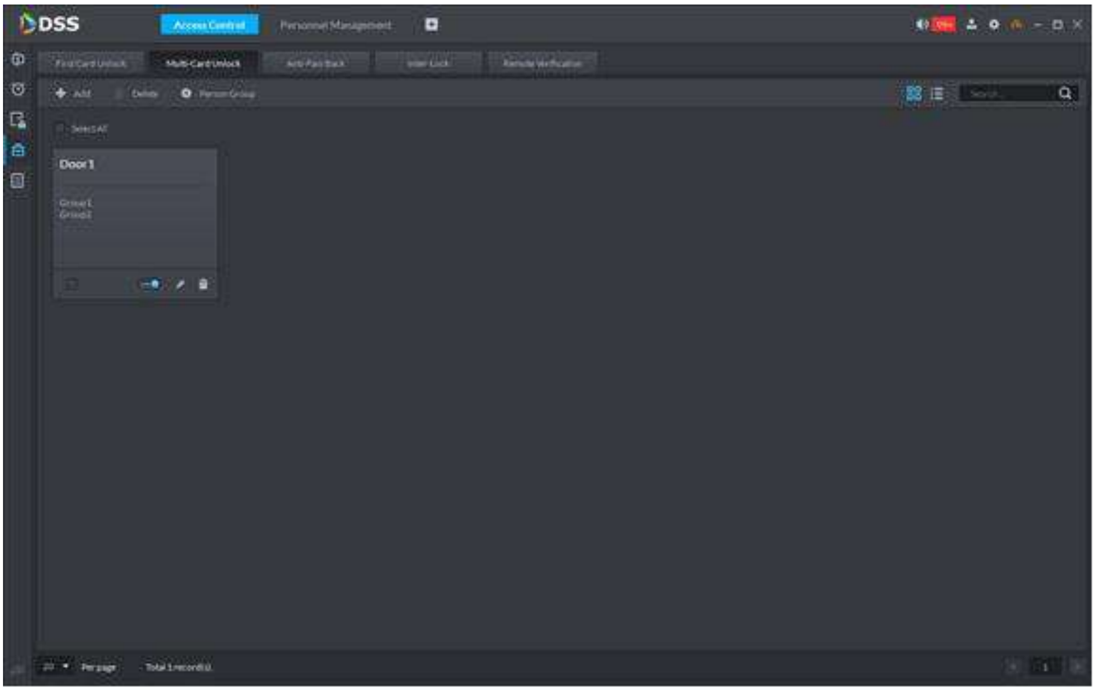
   Click ⬆ or ⬇ to adjust the user sequence for each group to unlock the door.

   The valid quantity refers to the number of users in each group that must be on site to swipe their cards.

5) Click **OK**.

   The system displays the Multi-Card Unlock information. See Figure 5-247.

Figure 5-247 Multi-card unlock



6) Click .

Step 5 The icon changing into indicates Multi-Card Unlock is enabled.

5.16.7 Anti-Pass Back

The Anti-Pass Back feature refers to that a user entering through a door group by verification must exit from the same door group by verification. One entry swipe must have a matching exit swipe. A non-verified user following a verified one to enter cannot pass the verification when taking exit; a non-verified user following a verified one to exit cannot pass verification when taking entry again. The door cannot be unlocked by swiping cards until the reset period on the A&C Central Controller expires.

Step 1 On the **Access Control** interface, click .

The **Advanced Function** interface is displayed.

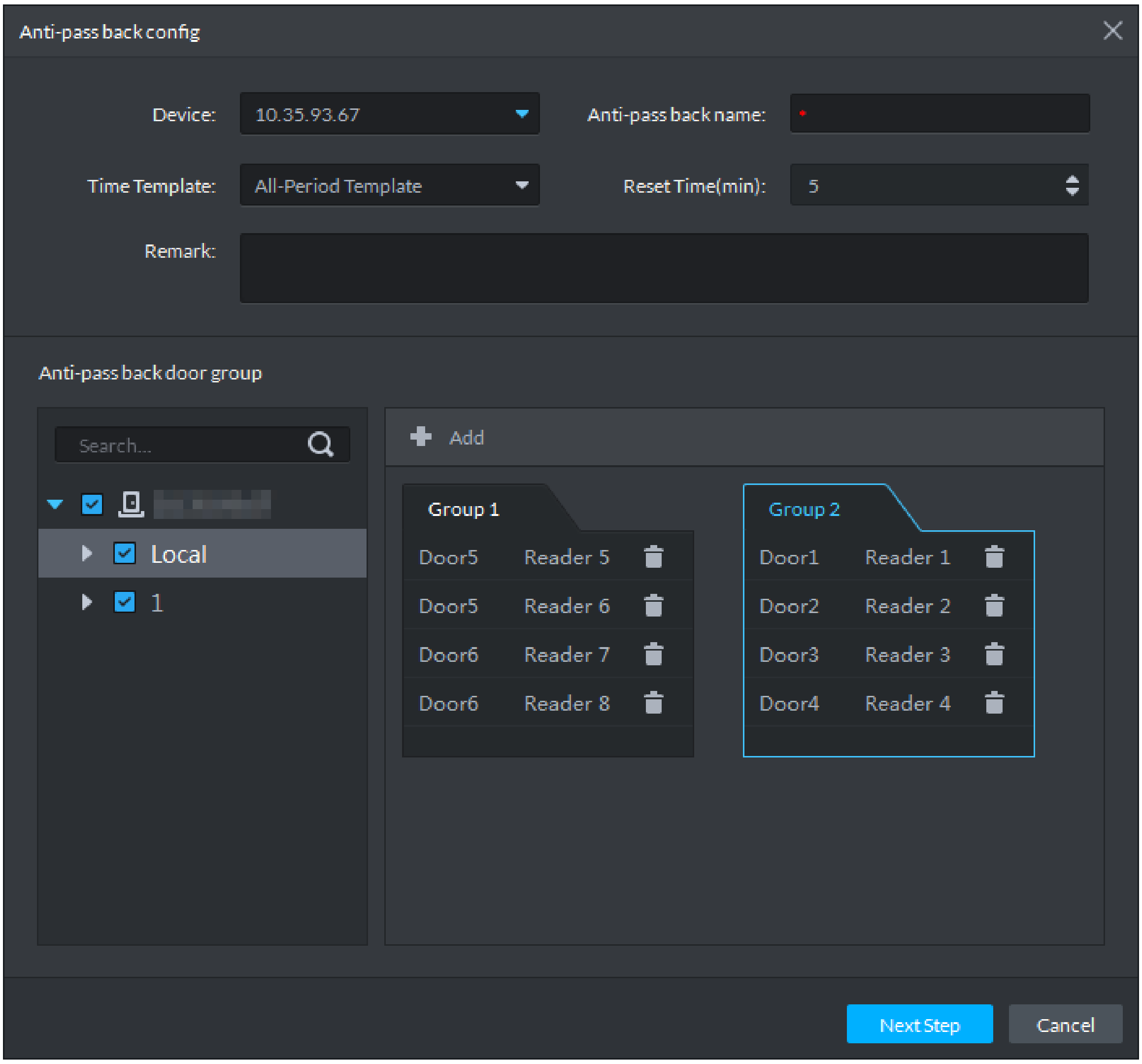
Step 2 Click the **Anti-Pass Back** tab.

The **Anti-Pass Back** interface is displayed.

Step 3 Click **Add**.

The **Anti-pass back config** interface is displayed. See Figure 5-248.

Figure 5-248 Anti-pass back config



Anti-pass back config

Device: 10.35.93.67

Anti-pass back name: *

Time Template: All-Period Template

Reset Time(min): 5

Remark:

Anti-pass back door group

Group 1

Door5	Reader 5
Door5	Reader 6
Door6	Reader 7
Door6	Reader 8

Group 2

Door1	Reader 1
Door2	Reader 2
Door3	Reader 3
Door4	Reader 4

Step 4 Configure the anti-pass back parameters and click **Next Step**. For details of the parameters, see Table 5-41.

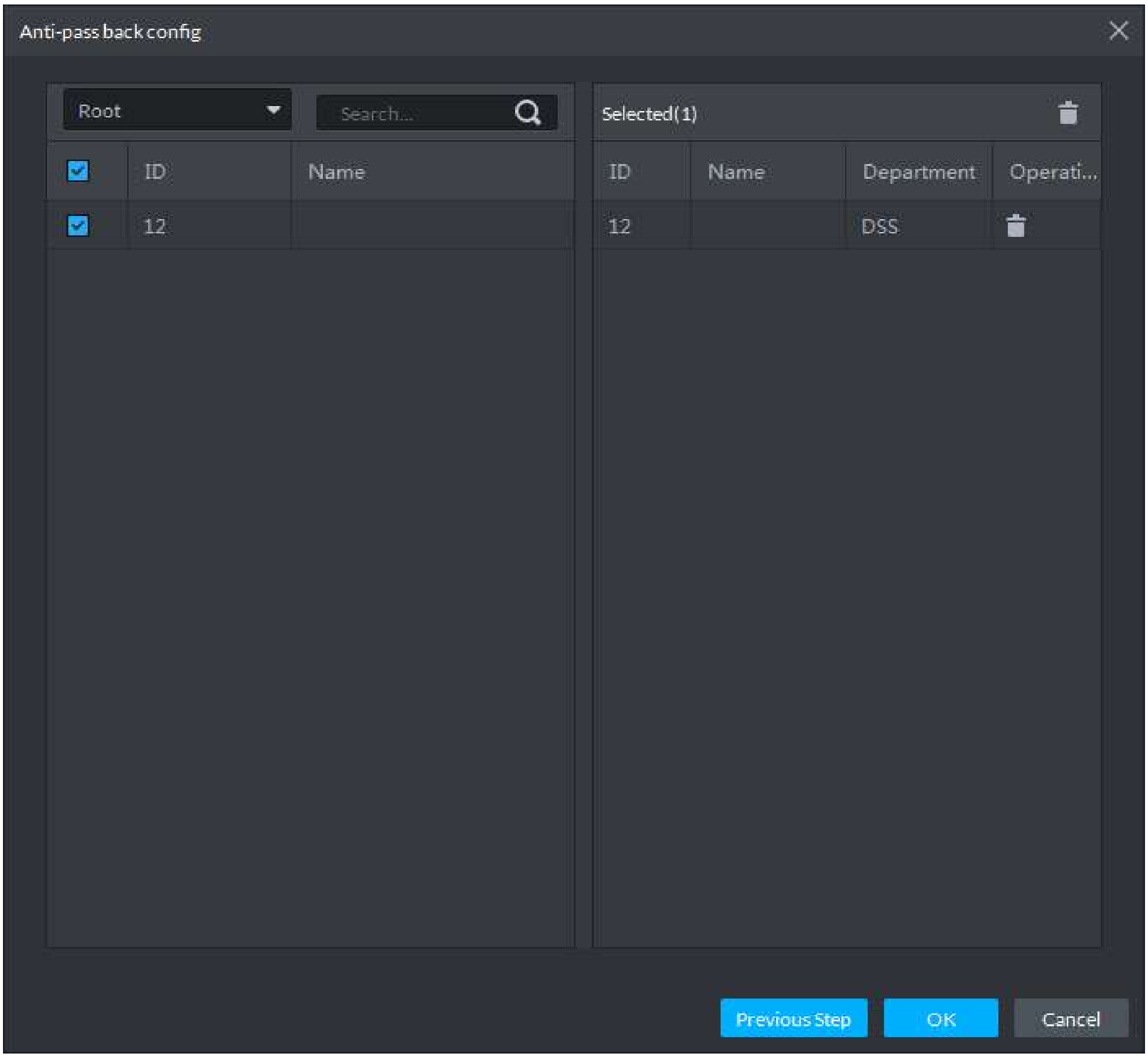
Step 5 The system displays the user selection information. See Figure 5-249.

Table 5-41 Anti-pass back parameter description

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Device</td><td colspan="2">You can select the device to configure the anti-pass back rules.</td></tr>
<tr><td>Anti-pass back name</td><td colspan="2">You can customize the name of an anti-pass back rule.</td></tr>
<tr><td>Reset Time(min)</td><td>The access card becomes invalid if an anti-pass back rule is violated.
The reset time is the invalidity duration.</td><td rowspan="4">📖
When the selected device is a multi-door controller, you must set up these</td></tr>
<tr><td>Time Template</td><td>You can select the time periods to implement the anti-pass back rules.</td></tr>
<tr><td>Remark</td><td>Note info.</td></tr>
<tr><td>Group X
📖
X is a number.</td><td>The group sequence here is the sequence for swiping cards. You can add up to 16 readers for each group. Each group can swipe cards on any of the readers.</td></tr>
</table>

Parameter	Description	
		parameters.

Figure 5-249 Select user


Anti-pass back config

Root

Search...

☑	ID	Name
☑	12	

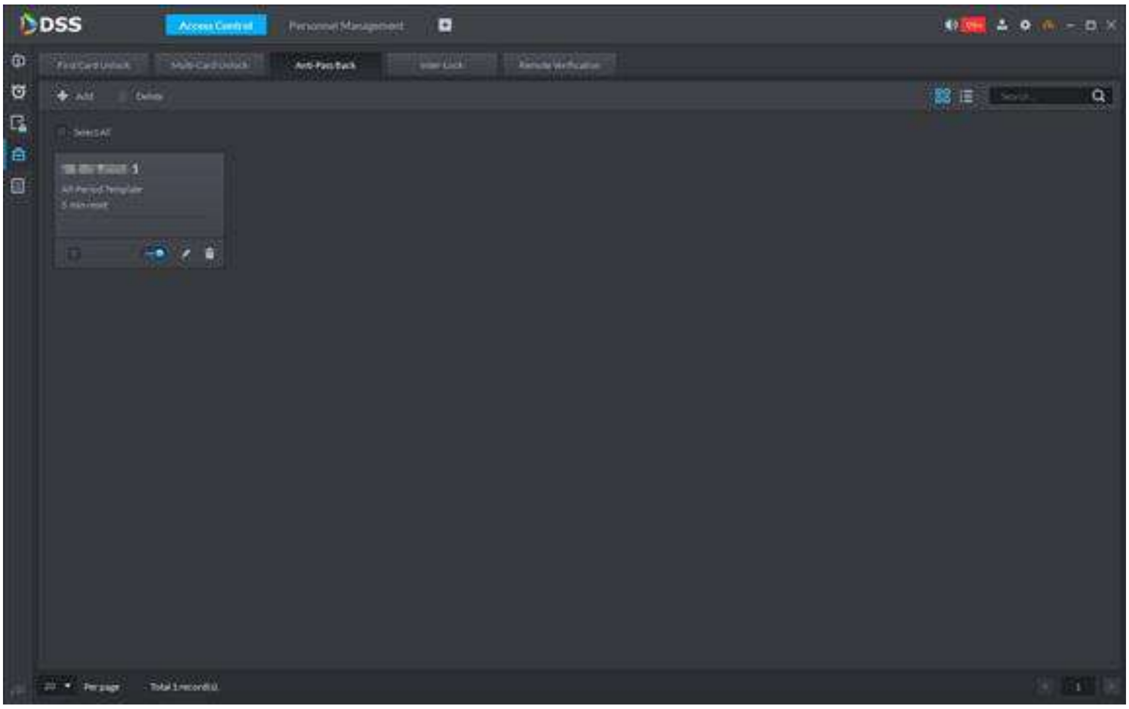
Selected(1)

ID	Name	Department	Operati...
12		DSS	🗑

Step 6 Select users and click **OK**.

Step 7 The system displays the anti-pass back information. See Figure 5-250.

Figure 5-250 Anti-pass back list



Step 8 Click.

Step 9 The icon changing into indicates Anti-Pass Back is enabled.

5.16.8 Inter-door Lock

A regular access controller employs inter-lock within the group. When one of the access control channels is opened, other corresponding channels are closed. To open one of the access control channels (under normal access control), other corresponding access control channels must be closed; otherwise the door cannot be unlocked. The A&C Central Controller employs inter-group inter-lock, where the access control channels are independent of the inter-lock and can all be opened. However, whenever an access control channel in a group is opened, no channels of other groups can be opened. The configuration steps in this chapter are for an A&C Central Controller.

Step 1 On the **Access Control** interface, click.

The **Advanced Function** interface is displayed.

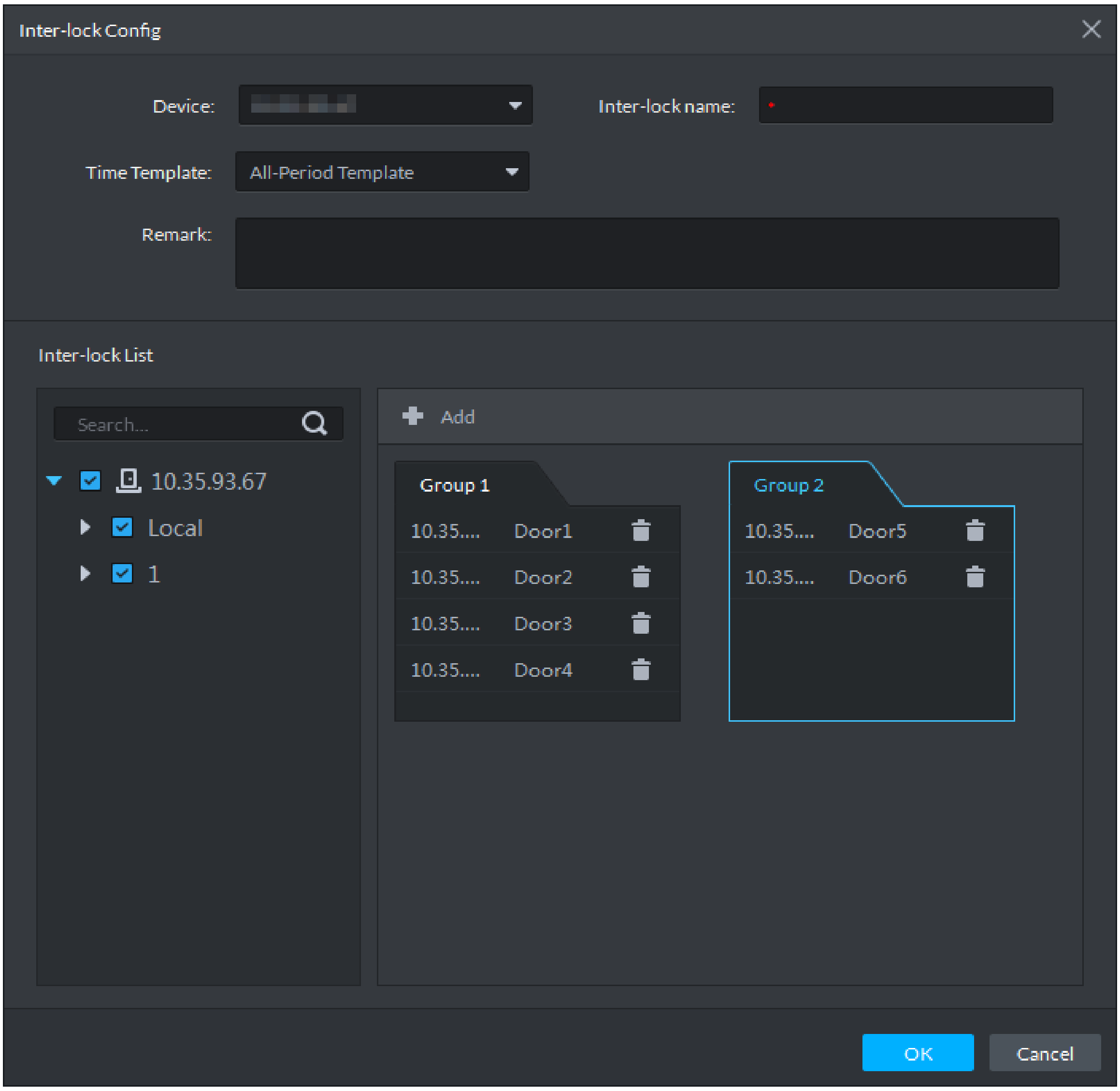
Step 2 Click the **Inter-Lock** tab.

The **Inter-Lock** interface is displayed.

Step 3 Click **Add**.

The **Inter-lock Config** interface is displayed. See Figure 5-251.

Figure 5-251 Inter-lock config



Device: [redacted]

Inter-lock name: *

Time Template: All-Period Template

Remark:

- ☑ 10.35.93.67
  - ☑ Local
  - ☑ 1

Group 1	
10.35....	Door1
10.35....	Door2
10.35....	Door3
10.35....	Door4

Group 2	
10.35....	Door5
10.35....	Door6

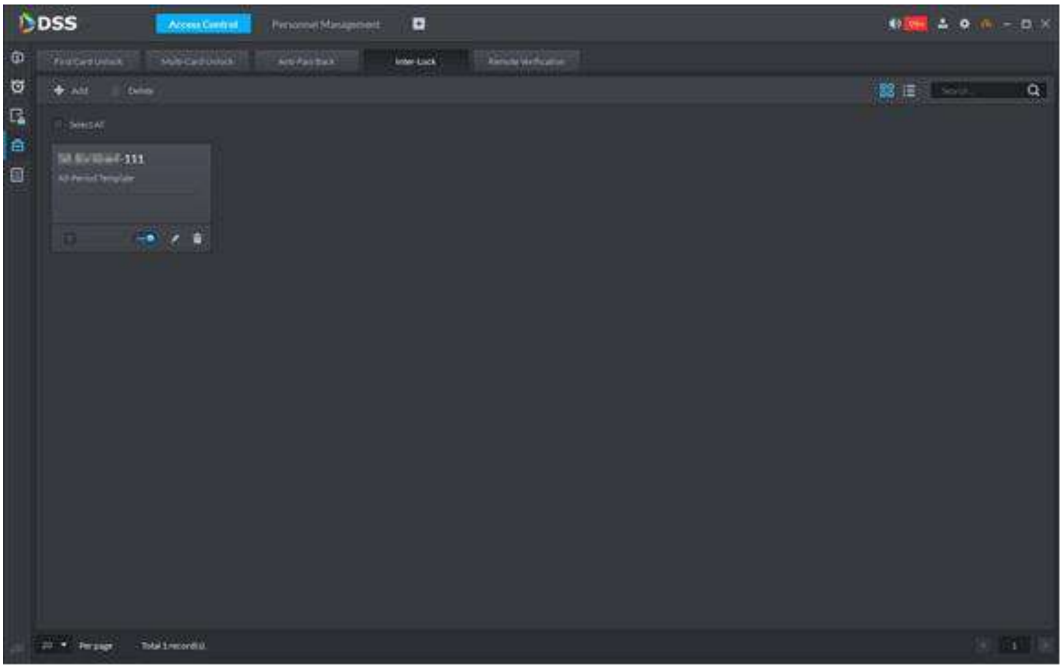
Step 4 Configure inter-lock parameters and click **OK**. For details of the parameters, see Table 5-42.

Step 5 The system displays the inter-lock information. See Figure 5-252.

Table 5-42 Inter-lock parameter description

Parameter	**Description**	
Device	You can select the device to set up inter-lock.	
Inter-lock name	You can customize the name of the inter-lock rule.	
Time Template	You can select the time period to implement inter-lock.	📖 When the selected device is a multi-door controller, you must set up these parameters.
Remark	Note info.	
Group X 📖 X is a number.	You can set up inter-lock across different door groups. If a door in Group 1 is opened, no doors can be opened in Group 2 until all doors in Group 1 are closed. Supports up to 16 door groups, with up to 16 doors in each group.	

Figure 5-252 Inter-lock list



Step 6 Click.

Step 7 The icon changing into indicates Inter-Lock is enabled.

5.16.9 Remote Verification

For devices with remote verification, when users unlock the doors with card, fingerprint, or password in the specified time period, it must be confirmed on the platform client before the access controller can be opened.

Step 1 On the **Access Control** interface, click.

The **Advanced Function** interface is displayed.

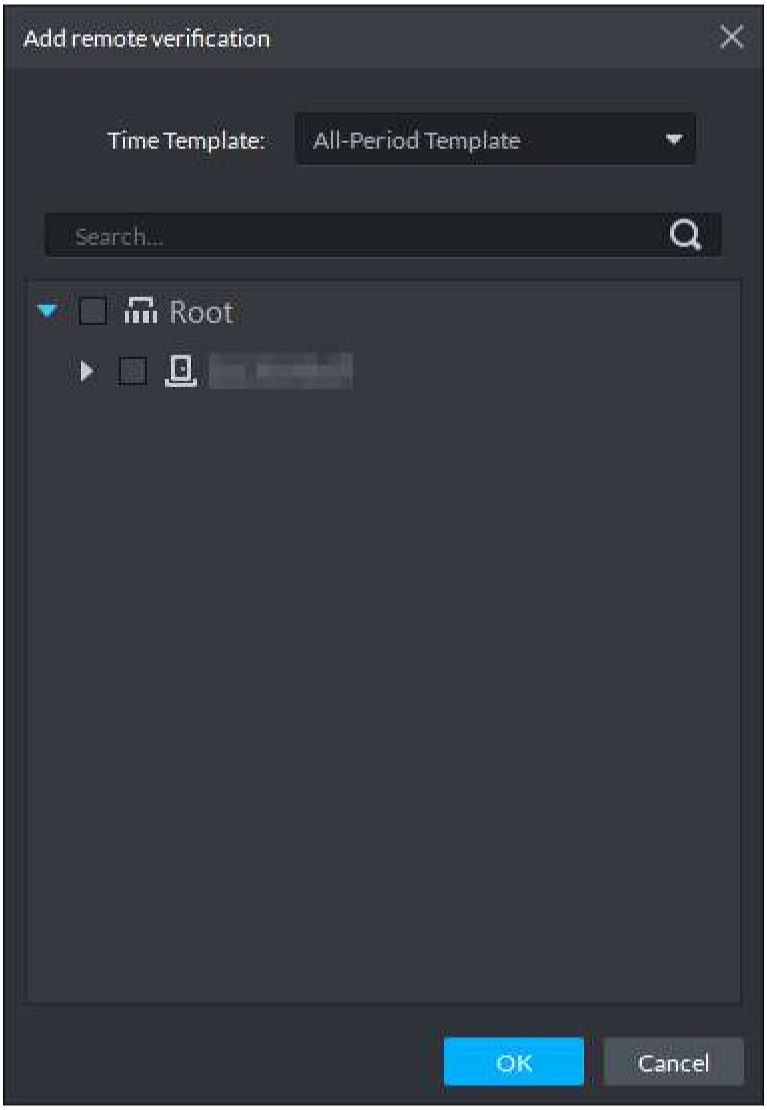
Step 2 Click the Remote Verification tab.

The **Remote Verification** interface is displayed.

Step 3 Click **Add**.

The **Add remote verification** interface is displayed. See Figure 5-253.

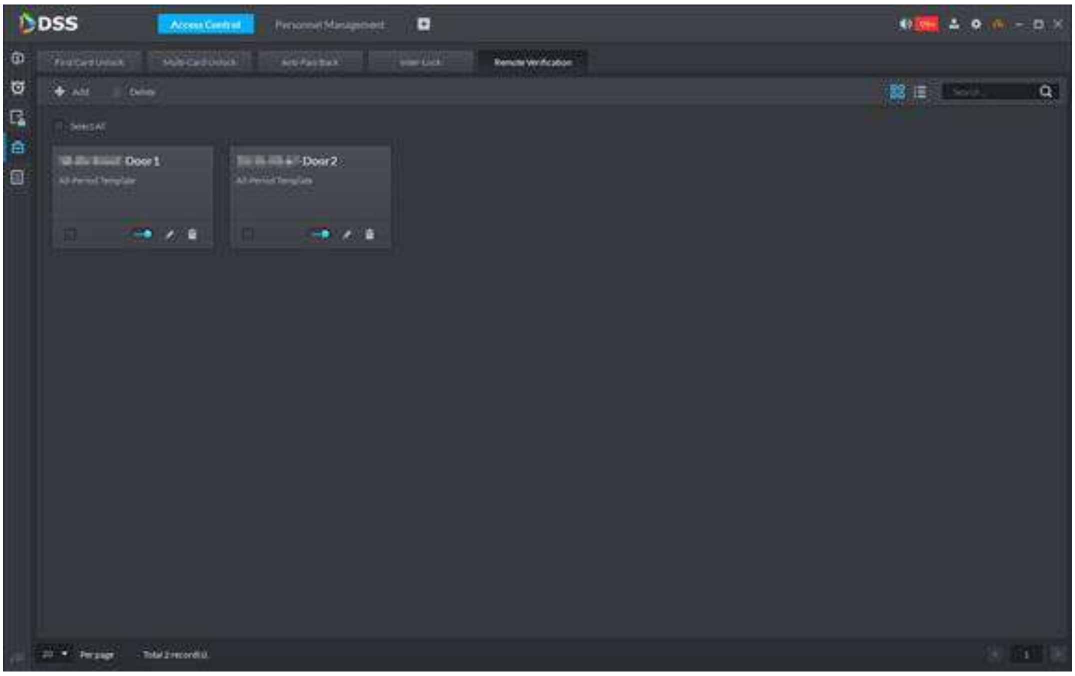
Figure 5-253 Add remote verification



Step 4 Select **Time Template** and access control channel, and click **OK**.

The system displays the remote verification information. See Figure 5-254.

Figure 5-254 Remote verification list



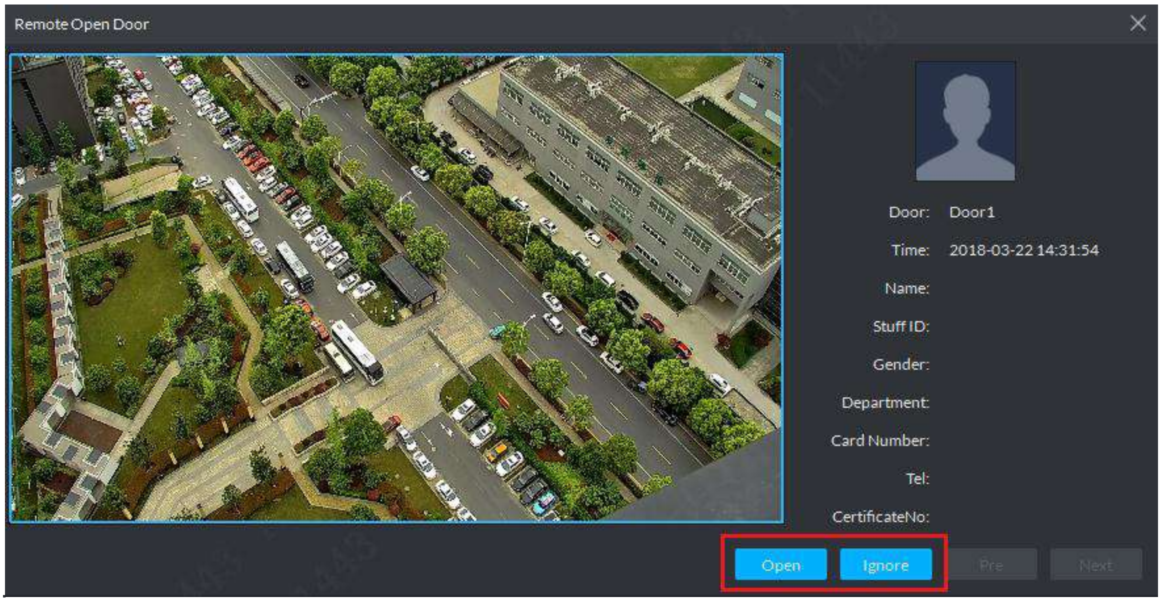
Step 5 Click.

The icon changing into indicates First Card Unlock is enabled.

Step 6 After the setup, door unlocking by card, fingerprint, or password that takes place in the corresponding access control channel triggers a popup on the client. See Figure 5-255.

Step 7 You can choose to unlock the door or ignore it by clicking the corresponding button, and the popup automatically disappears.

Figure 5-255 Remote open door



Door: Door1
Time: 2018-03-22 14:31:54
Name:
Stuff ID:
Gender:
Department:
Card Number:
Tel:
CertificateNo:

5.16.10 Searching A&C Log

You can search reported A&C log and device local log.

5.16.10.1 Searching Log on Platform

You can view the access control log by the following two methods:

- Click on the console to jump to the access control logo search interface, and set up search criteria to search for corresponding log info. See Figure 5-256 and Figure 5-257. Click Export in the top right corner of the interface and save the exported log to a local disk.

- Go to the Access Control module from the Homepage on the client, and click to go to the access control log search interface. See Figure 5-257. Click **Export** in the top right corner of the interface and save the exported log to a local disk.

Figure 5-256 Search A&C log(1)

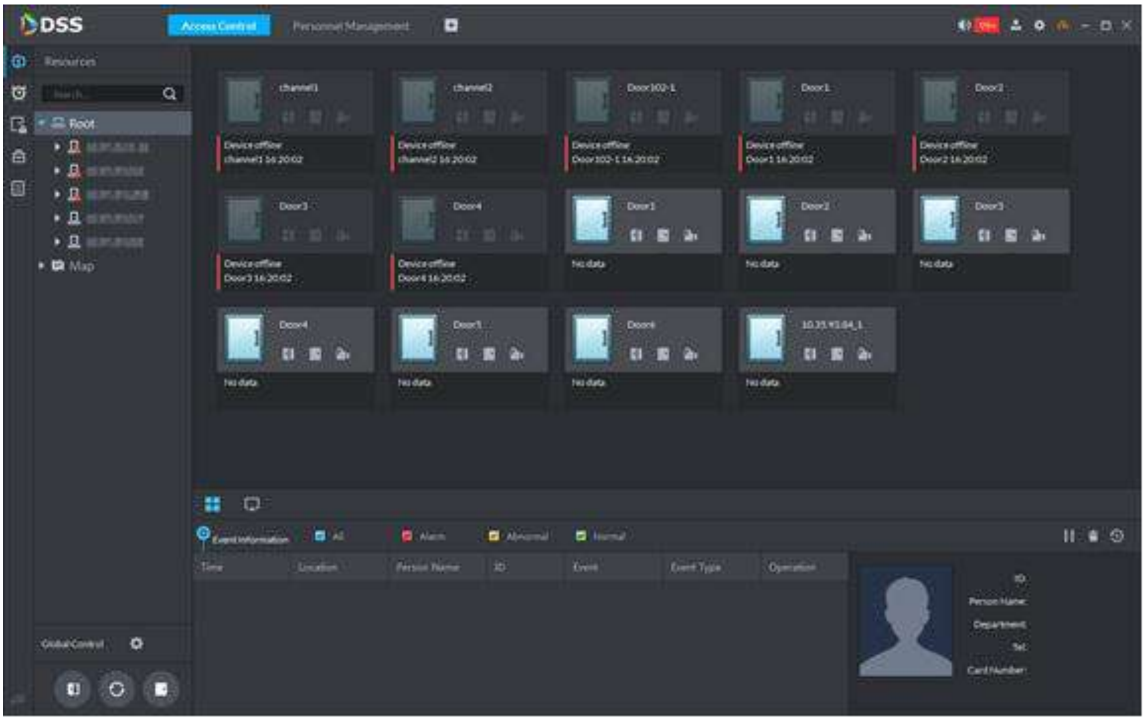
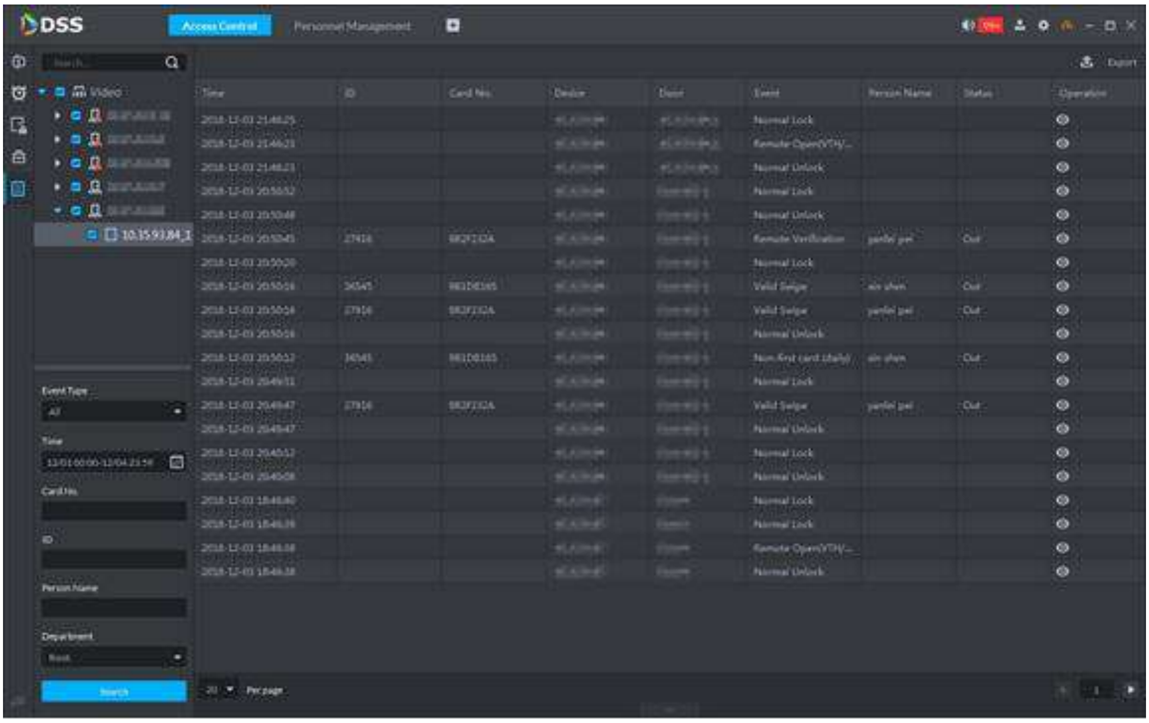


Figure 5-257 Search A&C log(2)



Time	ID	Card No.	Device	Door	Event	Person Name	Status	Operation
2018-12-03 21:46:25			[redacted]	[redacted]	Normal Lock			👁
2018-12-03 21:46:23			[redacted]	[redacted]	Remote Open(VTH/...			👁
2018-12-03 21:46:21			[redacted]	[redacted]	Normal Unlock			👁
2018-12-03 20:50:52			[redacted]	[redacted]	Normal Lock			👁
2018-12-03 20:50:48			[redacted]	[redacted]	Normal Unlock			👁
2018-12-03 20:50:45	27416	6B2F132A	[redacted]	[redacted]	Remote Verification	yanfei pei	Out	👁
2018-12-03 20:50:20			[redacted]	[redacted]	Normal Lock			👁
2018-12-03 20:50:16	36545	9B1D8165	[redacted]	[redacted]	Valid Swipe	xin shen	Out	👁
2018-12-03 20:50:16	27416	6B2F132A	[redacted]	[redacted]	Valid Swipe	yanfei pei	Out	👁
2018-12-03 20:50:16			[redacted]	[redacted]	Normal Unlock			👁
2018-12-03 20:50:12	36545	9B1D8165	[redacted]	[redacted]	Non-first card (daily)	xin shen	Out	👁
2018-12-03 20:49:51			[redacted]	[redacted]	Normal Lock			👁
2018-12-03 20:49:47	27416	6B2F132A	[redacted]	[redacted]	Valid Swipe	yanfei pei	Out	👁
2018-12-03 20:49:47			[redacted]	[redacted]	Normal Unlock			👁
2018-12-03 20:40:52			[redacted]	[redacted]	Normal Lock			👁
2018-12-03 20:40:08			[redacted]	[redacted]	Normal Unlock			👁
2018-12-03 18:46:40			[redacted]	[redacted]	Normal Lock			👁
2018-12-03 18:46:39			[redacted]	[redacted]	Normal Lock			👁
2018-12-03 18:46:38			[redacted]	[redacted]	Remote Open(VTH/...			👁
2018-12-03 18:46:38			[redacted]	[redacted]	Normal Unlock			👁

5.16.10.2 Extracting Log during Device Offline

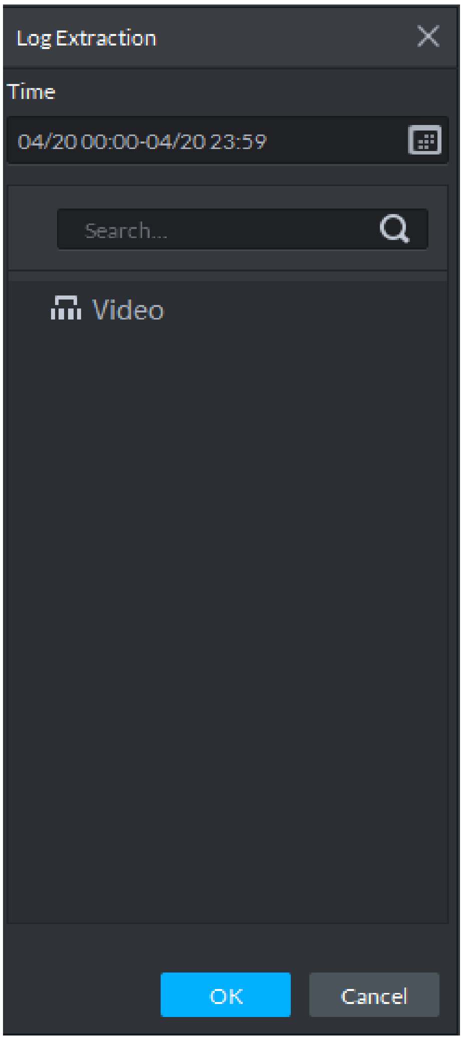
You can extract offline A&C log to platform when the device is offline.

Step 1 Click ▤ on the interface of **Access Control**.

The system displays the interface of **A&C Log**.

Step 2 Click Extract Record on the upper right corner of the interface.

Figure 5-258 Log extraction



Log Extraction

Time

04/20 00:00-04/20 23:59

Step 3 Click ▦ to set extraction time.

Step 4 Click ▶ to display access control device and select channel.

Step 5 Click **OK.**

The system displays the extracted A&C log.

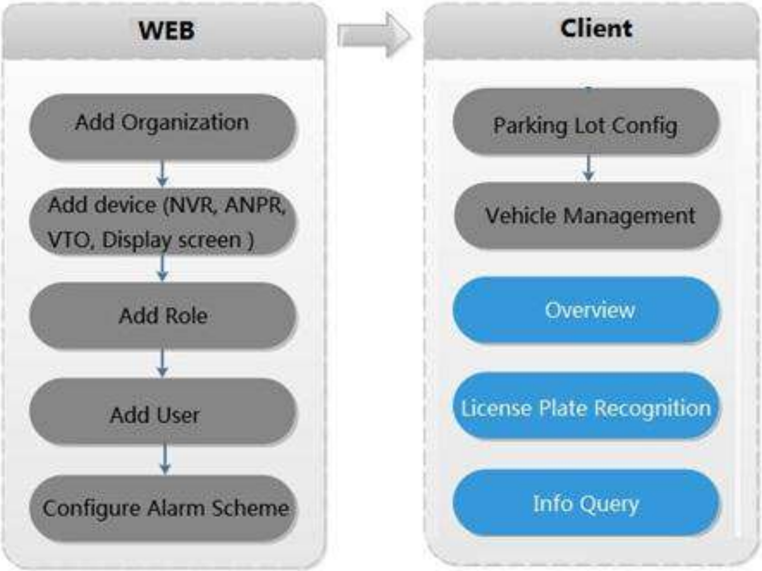
5.17 Entrance

Integrate entrance module, realize entrance and exit recognition barrier unlock, remaining parking space info display, blacklist vehicle alarm, message search and other functions. When it fails to recognize vehicle by entrance, then it can unlock by VTO password, swipe card to unlock, fingerprint unlock and unlock by face recognition to open barrier. The supported VTO unlock mode is based on the performance of accessed VTO.

5.17.1 Preparation

The flow diagram of entrance is shown in Figure 5-259.

Figure 5-259 Business flow



5.17.2 Adding Device

To use a new device, select **User Management** > **User** on WEB, enter **User** interface, and edit user to make him or her have access to device, otherwise the device cannot be used.

5.17.2.1 Adding ANPR Camera

ANPR camera is used to recognize license plate and vehicle info.

- Please make sure ANPR camera is fully configured before adding, such as initialization config an IP modification.
- The device category is **ANPR Device**.

Step 1 Add encoder ANPR, for more details, refer to "4.5 Adding Device"**.**

Modify device type.

1) On the **Device** interface of Web, click ✎ of added ANPR camera. See Figure 5-260. The device displays the interface of **Edit Device**. See Figure 5-261.

Figure 5-260 Device

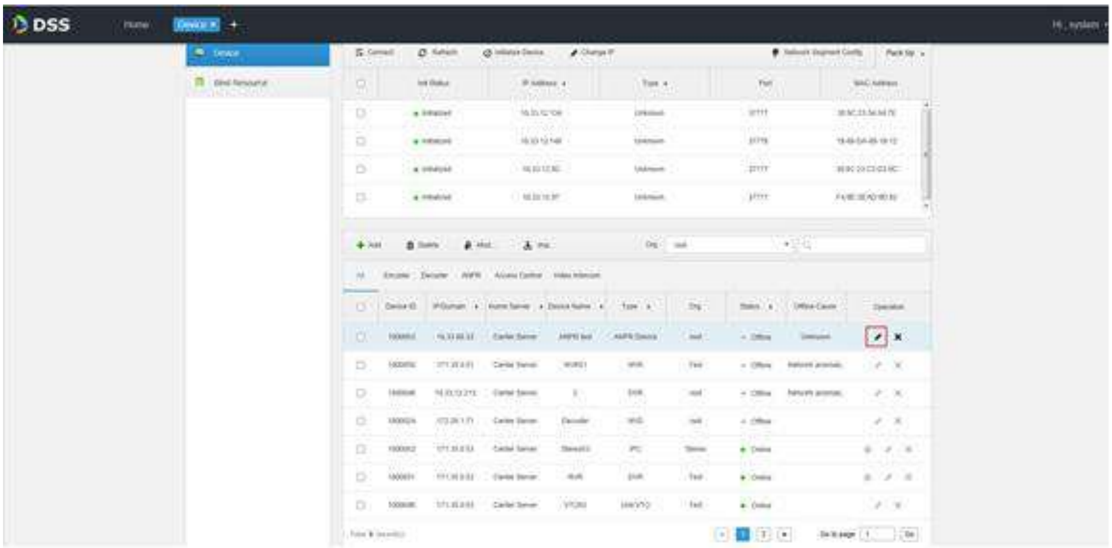
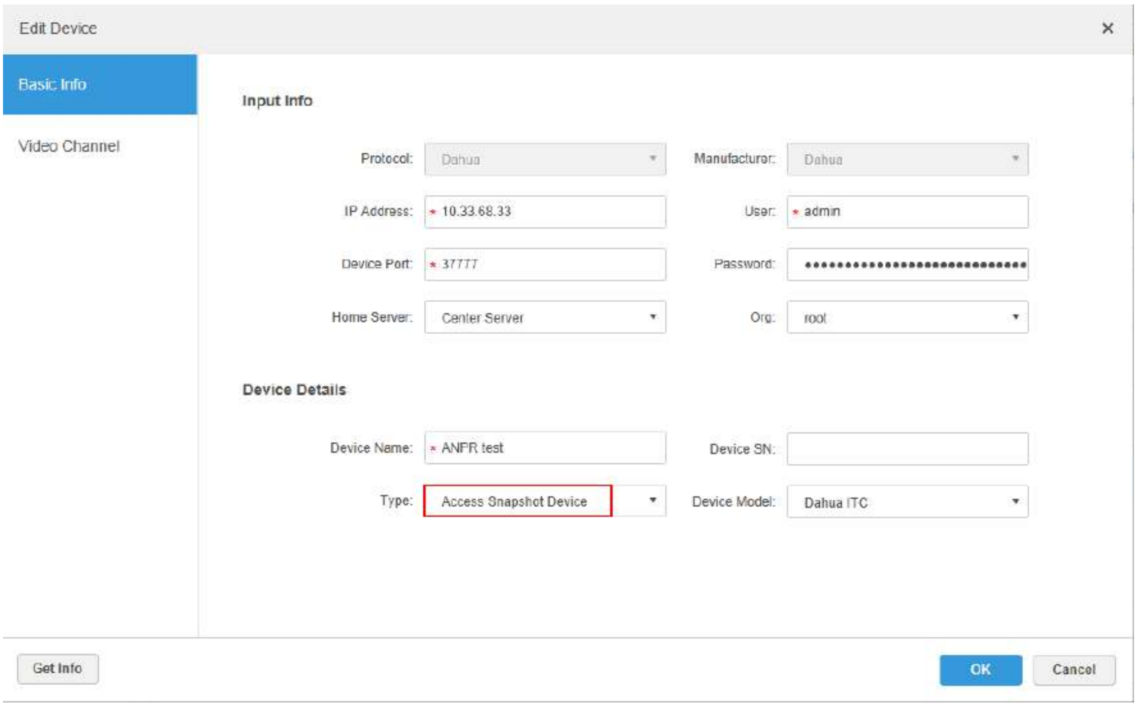


Figure 5-261 Edit device


Edit Device

Basic Info

Video Channel

Input Info

Protocol: Dahua

Manufacturer: Dahua

IP Address: * 10.33.68.33

User: * admin

Device Port: * 37777

Password: ••••••••••••••••••••••••••••

Home Server: Center Server

Org: root

Device Details

Device Name: * ANPR test

Device SN:

Type: Access Snapshot Device

Device Model: Dahua ITC

Get Info

OK

Cancel

2) Set type as **Access Snapshot Device**.

3) Click **OK** and complete config.

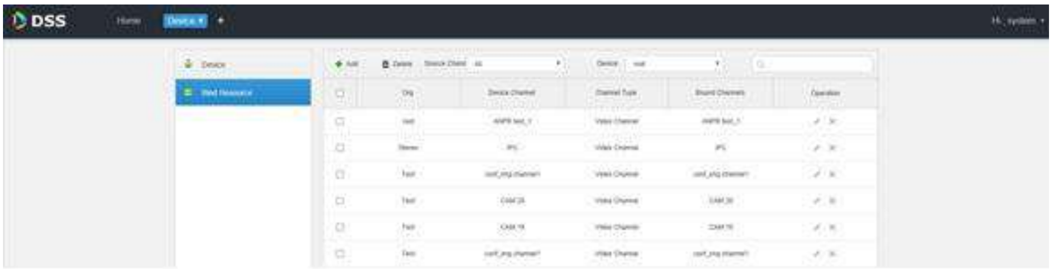
Step 2 Bind Resource

If there is camera installed at the entrance to view entrance panoramic picture, support binding ANPR and video camera. You can view realtime video image from license plate recognition. You can view video of bound camera.

1) Click **Bind Resource** tab on the interface of **Device**.

The system displays the interface of **Bind Resource**. See Figure 5-262.

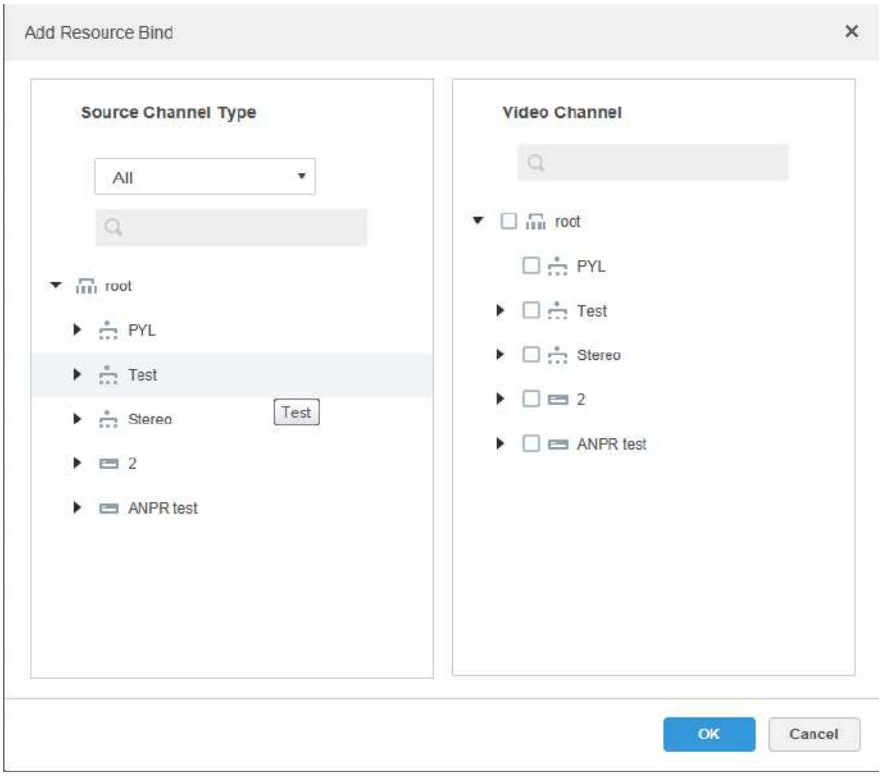
Figure 5-262 Bind resource



2) Click **Add**.

The system displays the interface of **Add Resource Bind**. See Figure 5-263.

Figure 5-263 Add resource bind



3) Select ANPR from the list of **Source Channel Type**, and select video camera from the list of **Video Channel**.

4) Click **OK** and complete config.

5.17.2.2 Adding NVR

NVR is used to connect ANPR camera and DSS, and realize data transmission.

- Please make sure NVR is fully configured before adding. For example, modify IP address, add remote device.
- NVR device category is Encoder.

Step 1 Add encoder **NVR**, for detailed operation; refer to "4.5 Adding Device".

Step 2 Modify device capacity set.

1) Click ✎ of added NVR on the **Device** interface on Web. See Figure 5-264.

The system displays the interface of **Edit Device**. See Figure 5-265.

Figure 5-264 Device

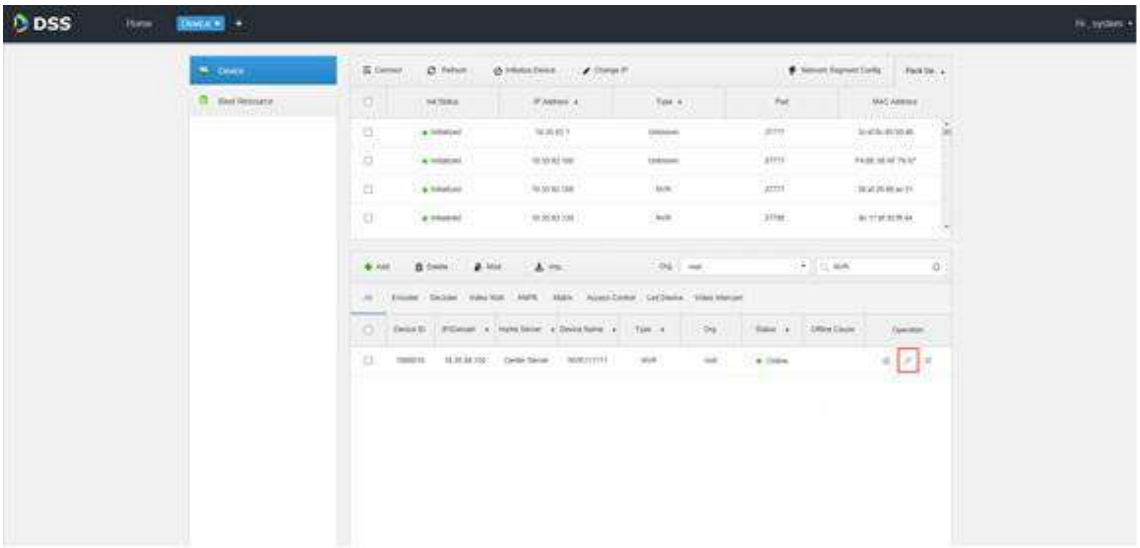
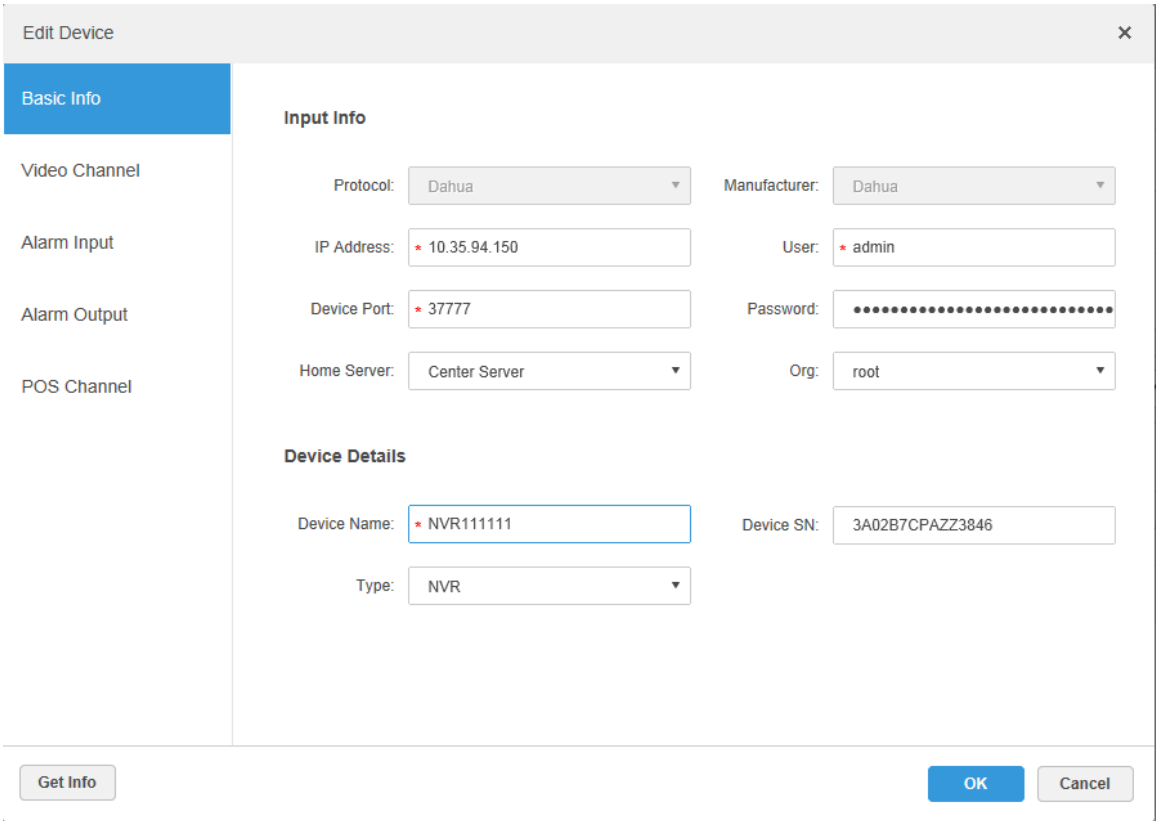


Figure 5-265 Edit device



Edit Device ×

Basic Info

Video Channel

Alarm Input

Alarm Output

POS Channel

Input Info

Protocol:	Dahua	Manufacturer:	Dahua
IP Address:	* 10.35.94.150	User:	* admin
Device Port:	* 37777	Password:	•••••••••••••••••••••••••••
Home Server:	Center Server	Org:	root

Device Details

Device Name:	* NVR111111	Device SN:	3A02B7CPAZZ3846
Type:	NVR		

Get Info

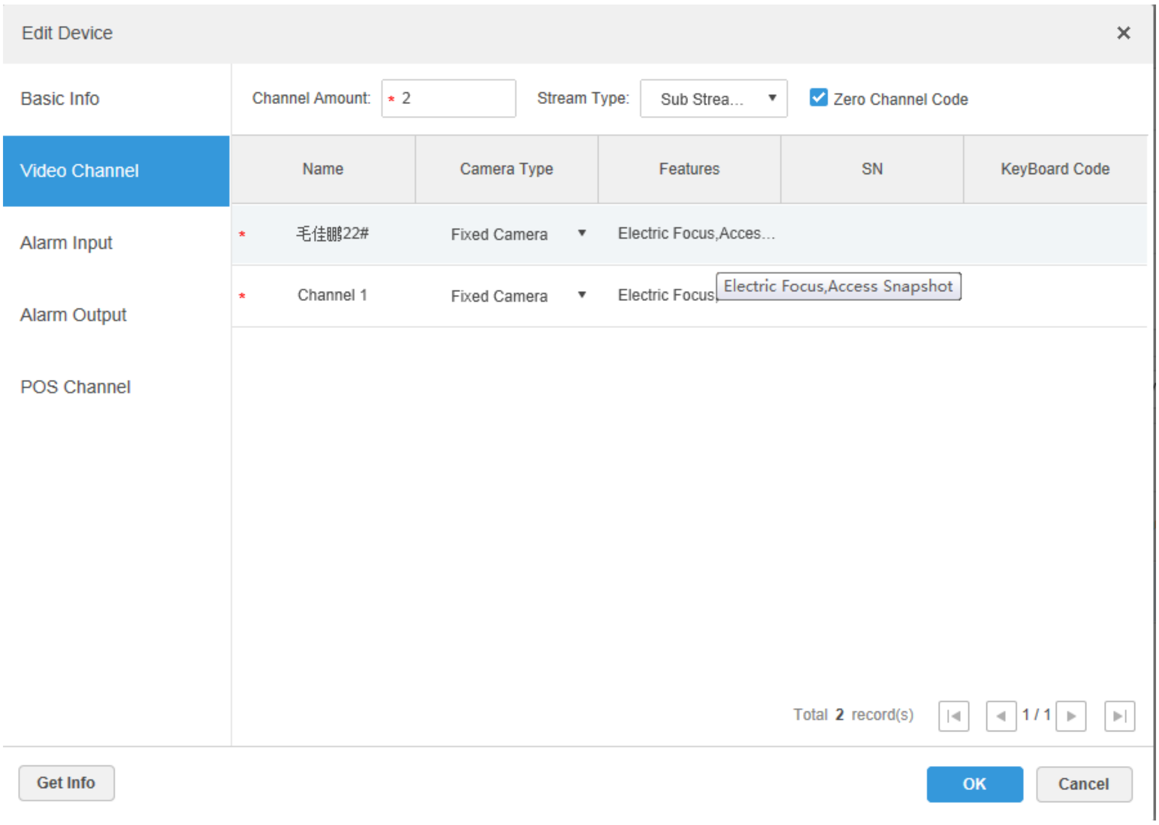
OK

Cancel

2) Click the tab of Video Channel, set features as **Access Snapshot**. See Figure 5-266.

The feature of all the bound ANPR device channel is set as **Access Snapshot**.

Figure 5-266 Video channel



Edit Device ×

Basic Info

Video Channel

Alarm Input

Alarm Output

POS Channel

Channel Amount: * 2 Stream Type: Sub Strea... ▼ ☑ Zero Channel Code

	Name	Camera Type	Features	SN	KeyBoard Code
*	毛佳鹏22#	Fixed Camera ▼	Electric Focus,Acces...		
*	Channel 1	Fixed Camera ▼	Electric Focus Electric Focus,Access Snapshot		

Total 2 record(s) 1 / 1

Get Info OK Cancel

3) Click **OK** and complete config.

5.17.2.3 Adding Remaining Parking Screen

Collect the data of vehicle entrance and exit from ANPR camera; make statistics of parking space quantity, then parking space quantity will be displayed on the screen. Currently the supported brands of remaining parking screen include Dahua and Jiuzhou.

- Please make sure remaining parking space is completely configured before adding. For example, modify IP address.
- The device category of remaining parking screen is **LED Device**.

Step 1 Add remaining parking screen, for detailed operation, refer to "4.5 Adding Device"**.**

Step 2 Modify the information of remaining parking screen.

1) Click ✏ of added remaining parking screen on the Device interface. See Figure 5-267.

The system displays the interface of Edit LED Device. See Figure 5-268

Figure 5-267 Device

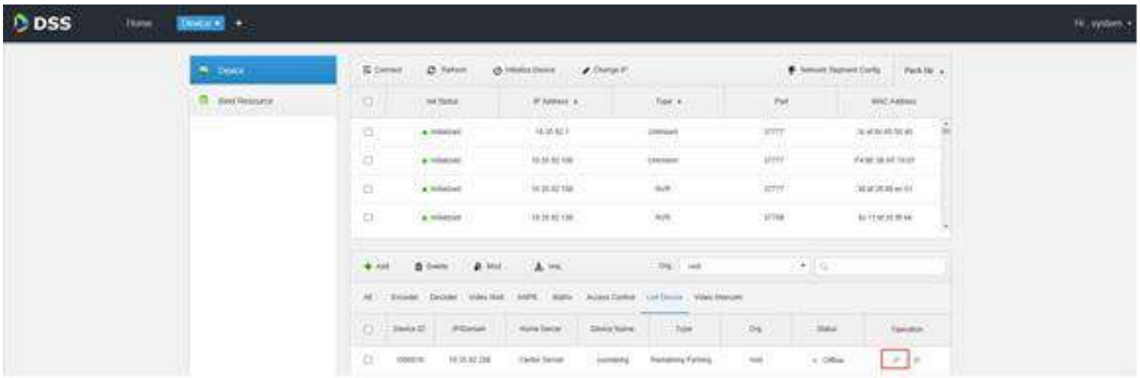
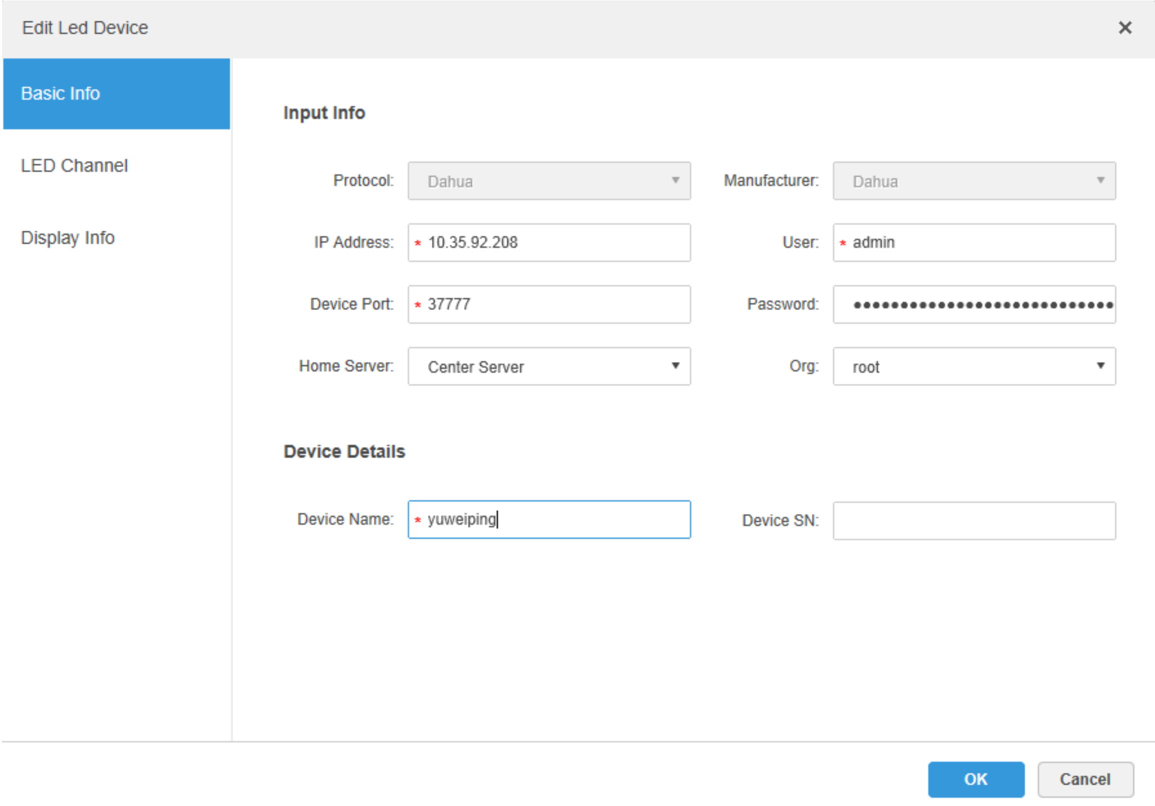


Figure 5-268 Edit device


Edit Led Device ×

Basic Info

LED Channel

Display Info

Input Info

Protocol:	Dahua	Manufacturer:	Dahua
IP Address:	* 10.35.92.208	User:	* admin
Device Port:	* 37777	Password:	••••••••••••••••••••••••••
Home Server:	Center Server	Org:	root

Device Details

Device Name:	* yuweiping	Device SN:	

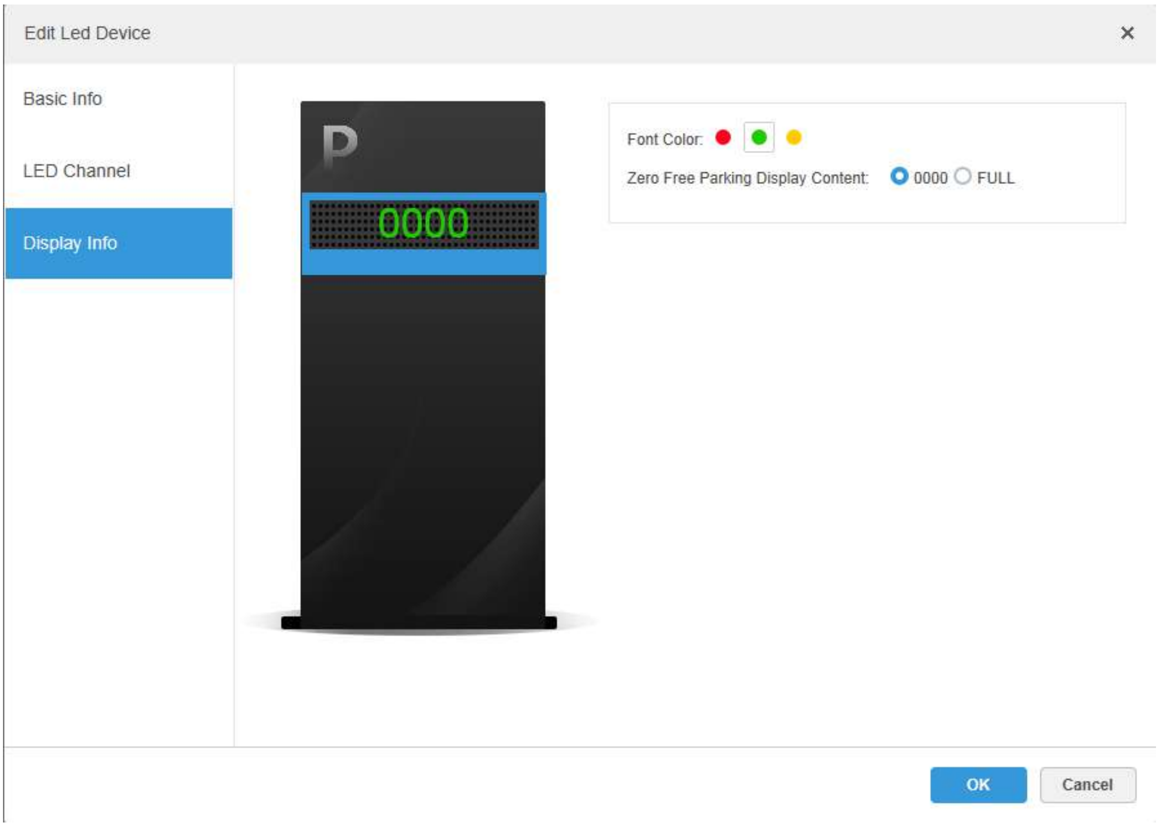
OK Cancel

2) Click the tab of **Display Info**, select **Font Color** and **Zero Free Parking Display Content**. See Figure 5-269.

Font color is the color of the words displayed on the screen; Zero free parking display content is the information displayed on the screen when there is no parking space available.

3) Click **OK** to complete config.

Figure 5-269 Display info



Edit Led Device

Font Color: 🟥 🟩 🟨

Zero Free Parking Display Content: ● 0000 ○ FULL

5.17.3 Configuring Alarm Scheme

Related alarm schemes of entrance include:

- License plate recognition

  When ANPR device recognizes license plate, it will be reported to DSS by NVR, alarm is triggered on DSS, and extract video before and after license plate recognition happens from NVR, save it on the server installed on DSS. Default record time is 20s, 10s before and 10s after alarm is triggered.

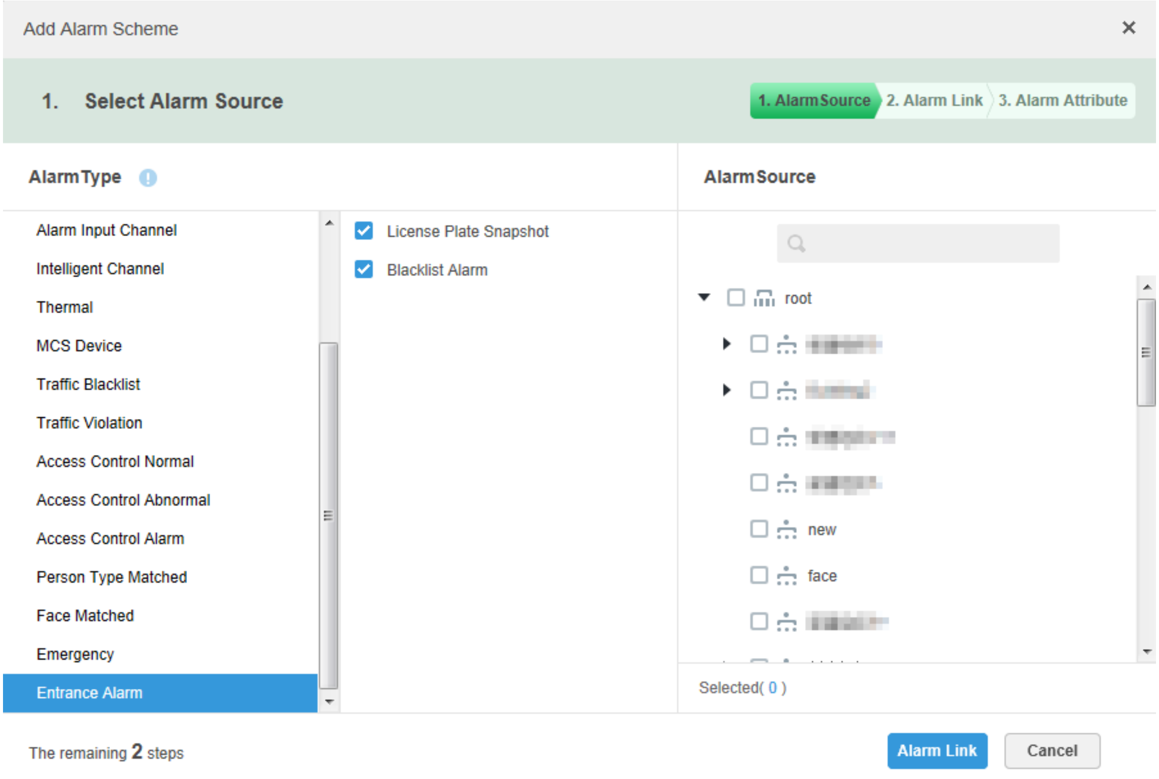
- Blacklist Alarm

  Mark some plate number as blacklist vehicle, compare the plate number reported by ANPR device with the plate number of blacklist vehicle. It triggers alarm when plate number in the vehicle blacklist is detected.

  Refer to "5.17.5 Vehicle Management" for more details.

Add entrance alarm scheme on the **Event** interface of Web. See Figure 5-270. Refer to "4.7 Configuring Event" for more details.

Figure 5-270 Add alarm scheme



Add Alarm Scheme

1. Select Alarm Source

Alarm Type

- Alarm Input Channel
- Intelligent Channel
- Thermal
- MCS Device
- Traffic Blacklist
- Traffic Violation
- Access Control Normal
- Access Control Abnormal
- Access Control Alarm
- Person Type Matched
- Face Matched
- Emergency
- Entrance Alarm

☑ License Plate Snapshot

☑ Blacklist Alarm

Alarm Source

□ root

□ new

□ face

Selected(0)

The remaining 2 steps

5.17.4 Configuring Parking Lot

Parking lot config includes setting parking space quantity, release situation and other information. Bind ANPR device channel and use it to recognize vehicles, bound VTO is used to recognize people.

Step 1 Click ⊞ and select **Entrance** on the **Homepage** interface.

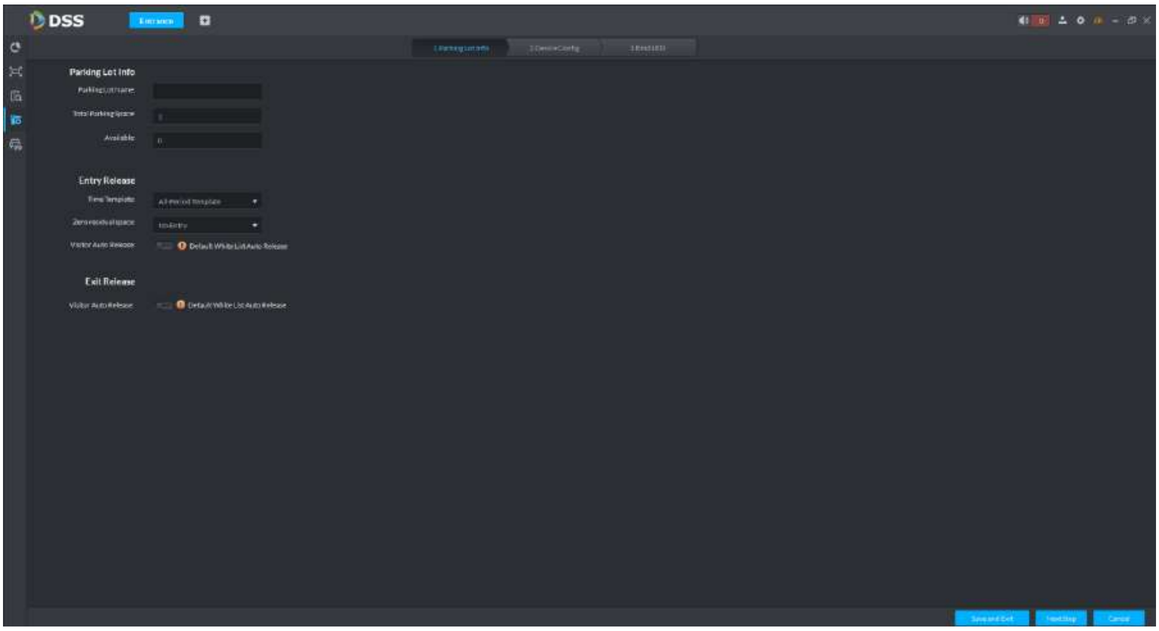
The system displays the interface of **Entrance**.

Step 2 Click .

The system displays the interface of **Parking Lot Config**.

Step 3 Configure parking lot information. See Figure 5-271. Refer to Table 5-43 for more parameter details.

Figure 5-271 Parking lot info



Parking Lot Info

Parking Lot Name

Total Parking Space 0

Available 0

Entry Release

Time Template All-Period Template

Zero residual space No Entry

Visitor Auto Release Default White List Auto Release

Exit Release

Visitor Auto Release Default White List Auto Release

Table 5-43 Parking lot

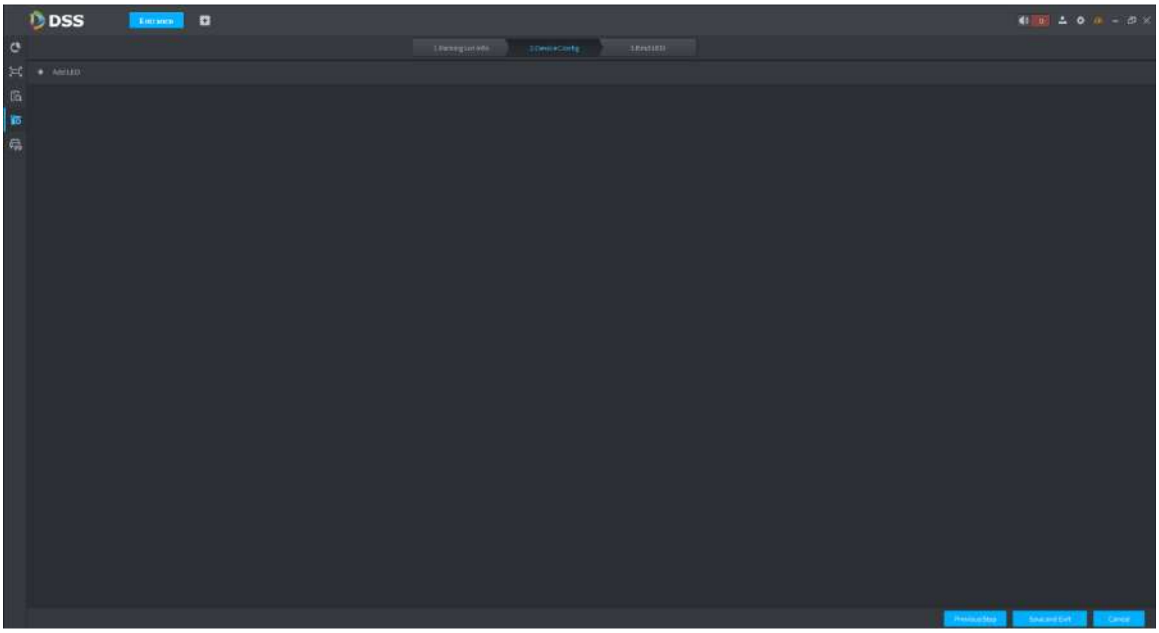
Parameter		Description
Parking lot info	Name	Parking lot name, used to recognize different areas.
	Total parking space	Total available parking space of the area.
	Available	Available parking lot quantity when configuring parking lot.
Entry Release	Time template	Select the time template which conforms to entry release. If default template fails to meet the requirement, you can select **Manage Time Template** to set custom time template. Default templates include: ● All-period template: 00:00 to 24:00 daily. ● Weekday template: 00:00 to 24:00 Mon to Fri ● Weekend template: 00:00 to 24:00 Sat and Sun
	Zero residual space	Release option when remaining space is zero. ● No entry. Any vehicle is not allowed to enter. ● All Any vehicle is allowed to enter. ● Whitelist Whitelist vehicles include several vehicle types, such as no group, general and VIP. Only three types of vehicle above are allowed to enter when remaining space is zero. ● VIP Only VIP vehicle is allowed to enter when remaining space is zero. Vehicle type should be set during vehicle management.

Parameter		Description
	Visitor auto release	Vehicles not registered on DSS are considered as visitor. Confirm whether the barrier opens automatically when visitor enters the parking lot. If yes, click , and the icon changes to . Otherwise, it remains , and the barrier will not automatically open when visitor wants to enter the parking lot.
Exit Release	Visitor auto release	Those which are not registered on DSS are considered as visitor vehicles. Confirm if it unlocks barrier automatically when visitor vehicle exits according scenario design. If it is required to release, and then click , the icon displays as . Otherwise, it remains as , and it will not unlock barrier to release when visitor wants to exit parking lot.

Step 4 Click **Next.**

The system displays the interface of **Device Config.** See Figure 5-272

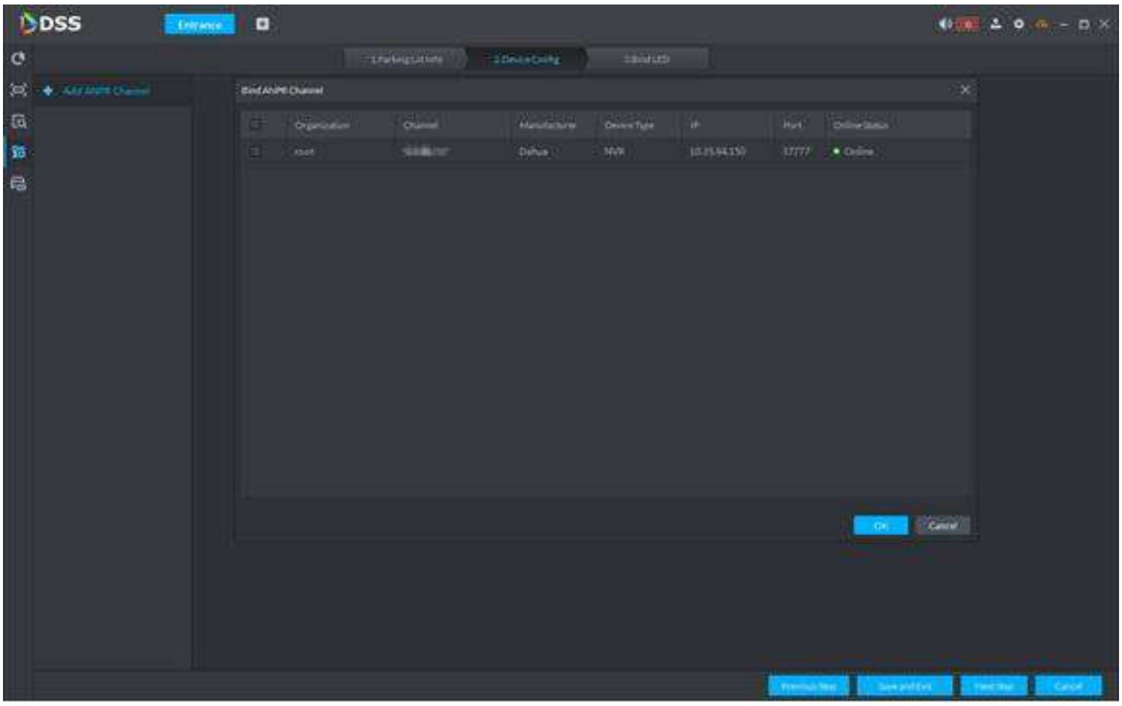
Figure 5-272 Device config



Step 5 Add ANPR device.

1) Click **Add ANPR Channel** and you can select all the ANPR devices deployed at entrance and exit of the parking lot on the interface. See Figure 5-273.

Figure 5-273 Add ANPR device

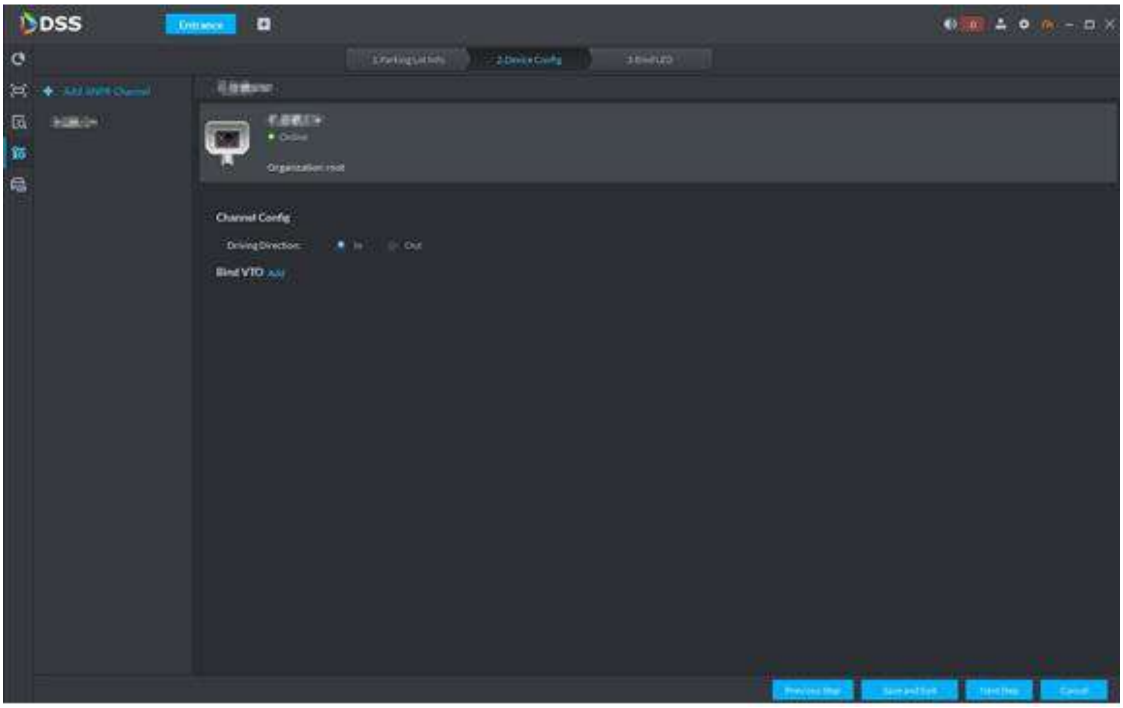


□	Organization	Channel	Manufacture	Device Type	IP	Port	Online Status
□	root	[redacted]	Dahua	NVR	10.15.94.150	37777	● Online

2) Click **OK**.

The system displays the information of added ANPR device. See Figure 5-274.

Figure 5-274 ANPR device info



[redacted]

● Online

Organization: root

Channel Config

Driving Direction: ● In ○ Out

Bind VTO Add

3) Select ANPR device from device list in sequence, and set corresponding driving direction. The default driving direction is **In**.

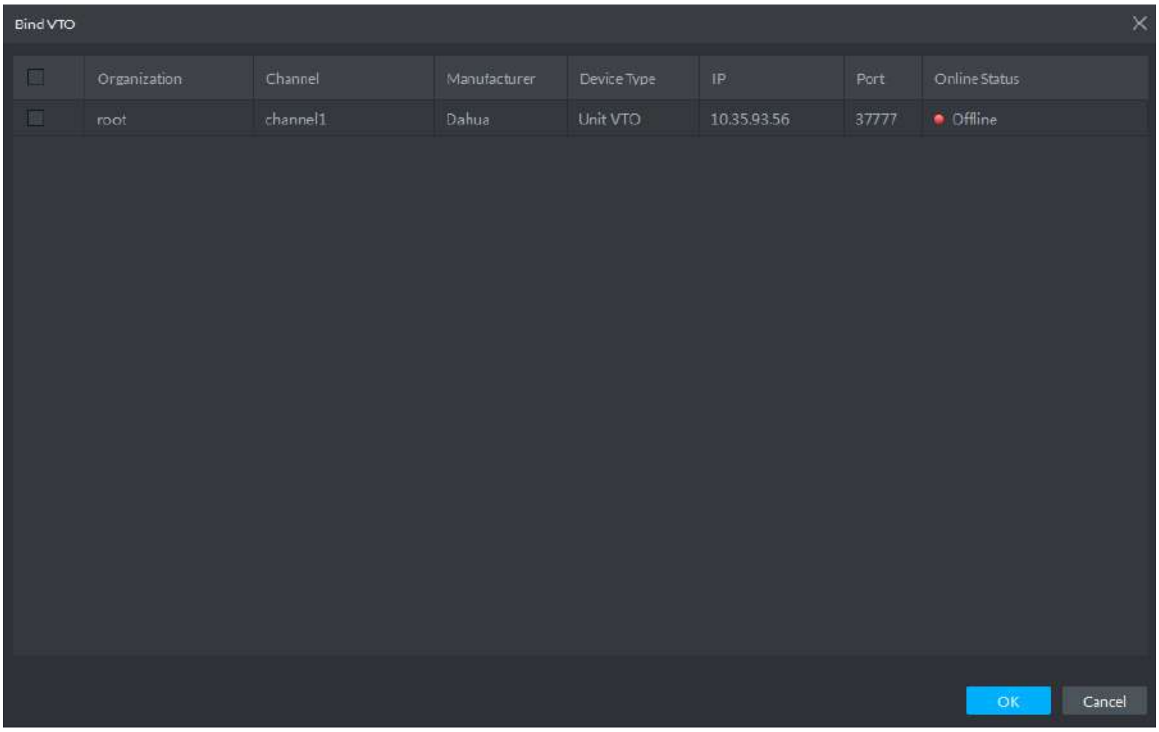
Step 6 Bind VTO device.

VTO device is used to recognize people, and open barrier. Please skip this step if there is no VTO in the networking.

1) Click **Add** next to **Bind VTO**.

The system displays the interface of **Bind VTO**. See Figure 5-275.

Figure 5-275 Bind VTO



□	Organization	Channel	Manufacturer	Device Type	IP	Port	Online Status
□	root	channel1	Dahua	Unit VTO	10.35.93.56	37777	● Offline

2) Select the VTO that is deployed next to barrier, and click OK.

The interface displays the VTO information.

Step 7 Click **Next**.

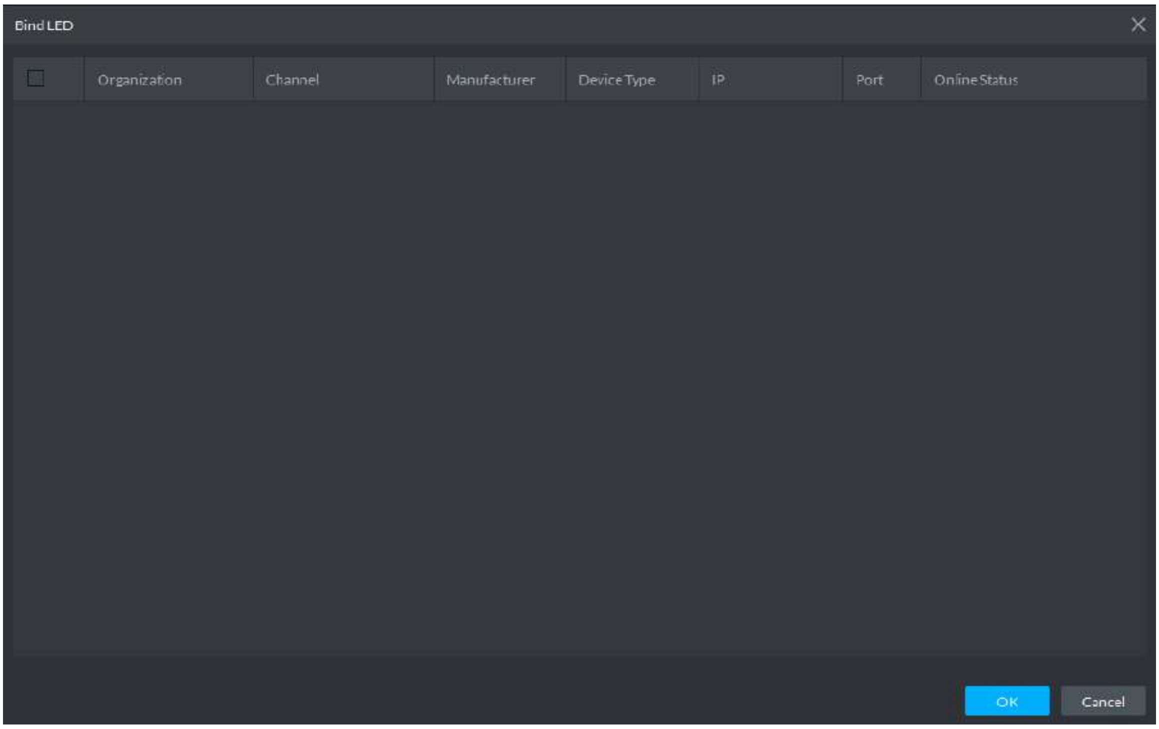
The system displays Bind LED.

Step 8 Add LED.

1) Click **Add LED**.

The system displays the interface of **Bind LED**. See Figure 5-276.

Figure 5-276 Bind LED



□	Organization	Channel	Manufacturer	Device Type	IP	Port	Online Status

2) Select all the LED of the parking lot and click OK.

The system displays the information of LED.

5.17.5 Vehicle Management

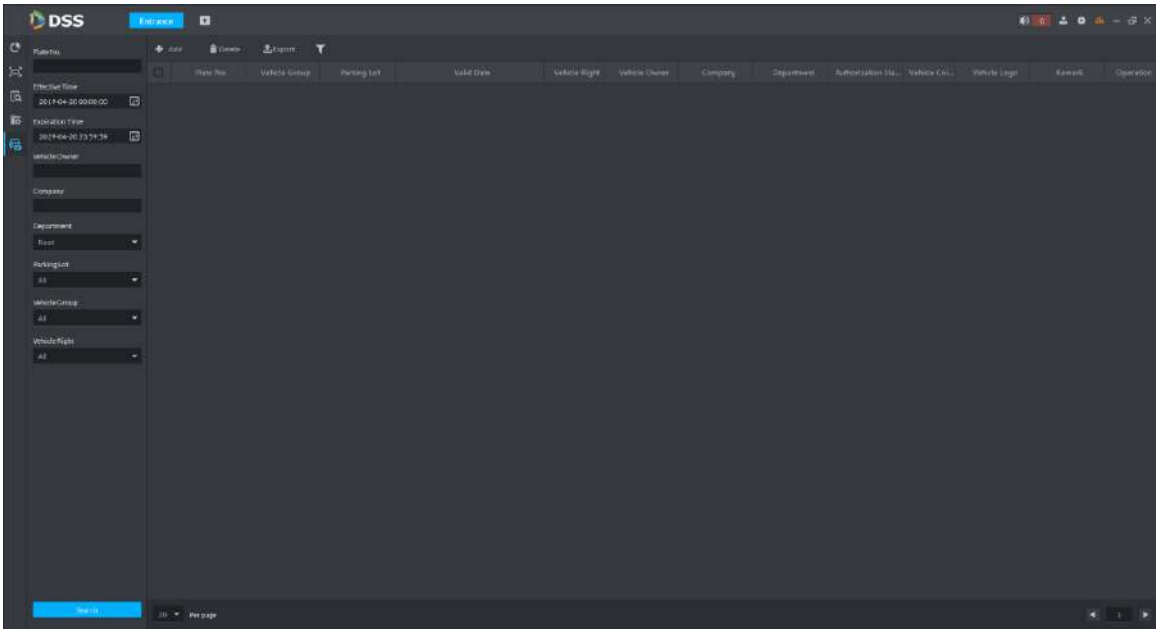
Vehicle info management includes vehicle type, department, related personnel and release ANPR, which are used as judgment basis to confirm if the vehicle can enter some area. Vehicle management can synchronize added vehicle info from personnel management module.

Step 1 Click on the interface of **Entrance**.

The system displays the interface of Vehicle Management. See Figure 5-277.

You can set serach condition, click **Search** and the system displays vehicle info. Including vehicle information added on personnel management module.

Figure 5-277 Vehicle management



Step 2 Click **Add**.

The system displays the interface of **Add**. See Figure 5-278.

Figure 5-278 Add vehicle

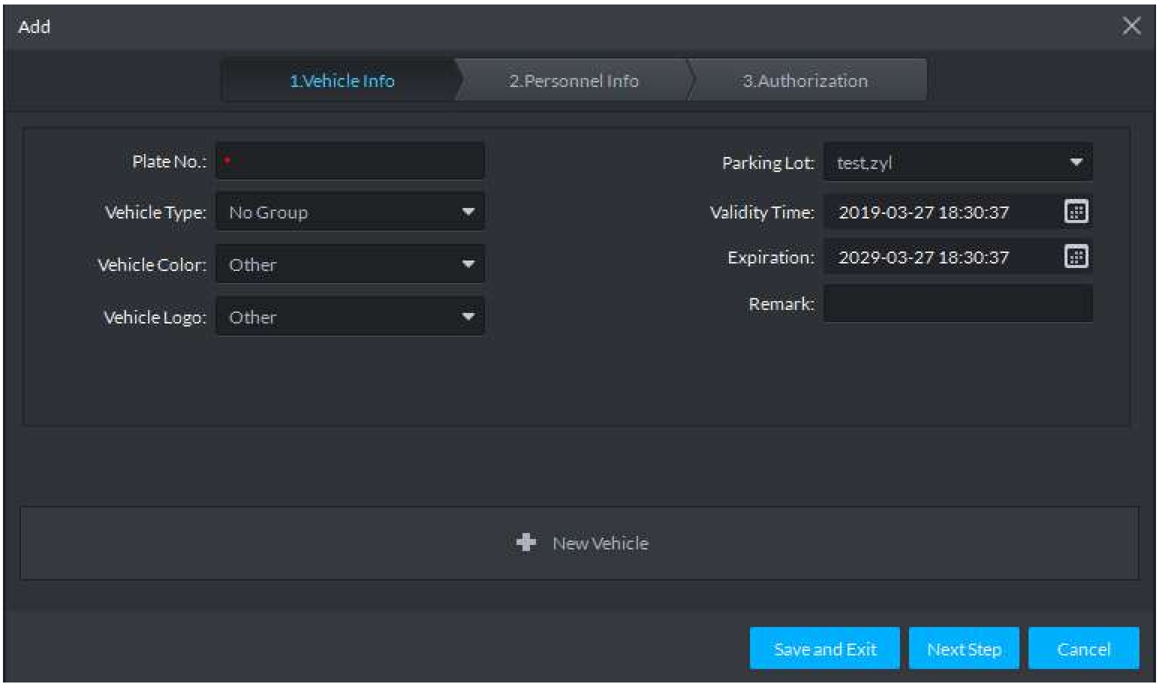


Plate No.: *

Vehicle Type: No Group

Vehicle Color: Other

Vehicle Logo: Other

Parking Lot: test.zyl

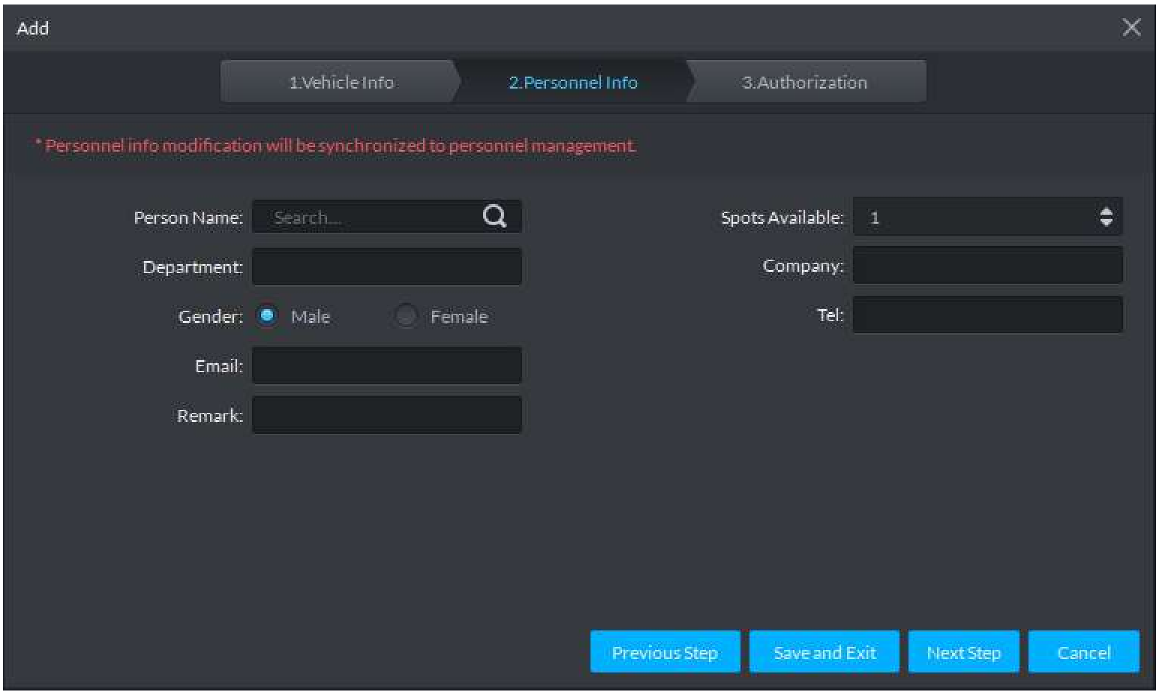
Validity Time: 2019-03-27 18:30:37

Expiration: 2029-03-27 18:30:37

Remark:

Step 3 Click the tab of **Vehicle Info** and add vehicle info, click **Next** and the system display the interface of **Personnel Info**. Refer to Figure 5-279. Refer to Table 5-44 for parameter details.

Figure 5-279 Personnel info



* Personnel info modification will be synchronized to personnel management.

Person Name: Search...

Department:

Gender: ● Male ○ Female

Email:

Remark:

Spots Available: 1

Company:

Tel:

Table 5-44 Vehicle info

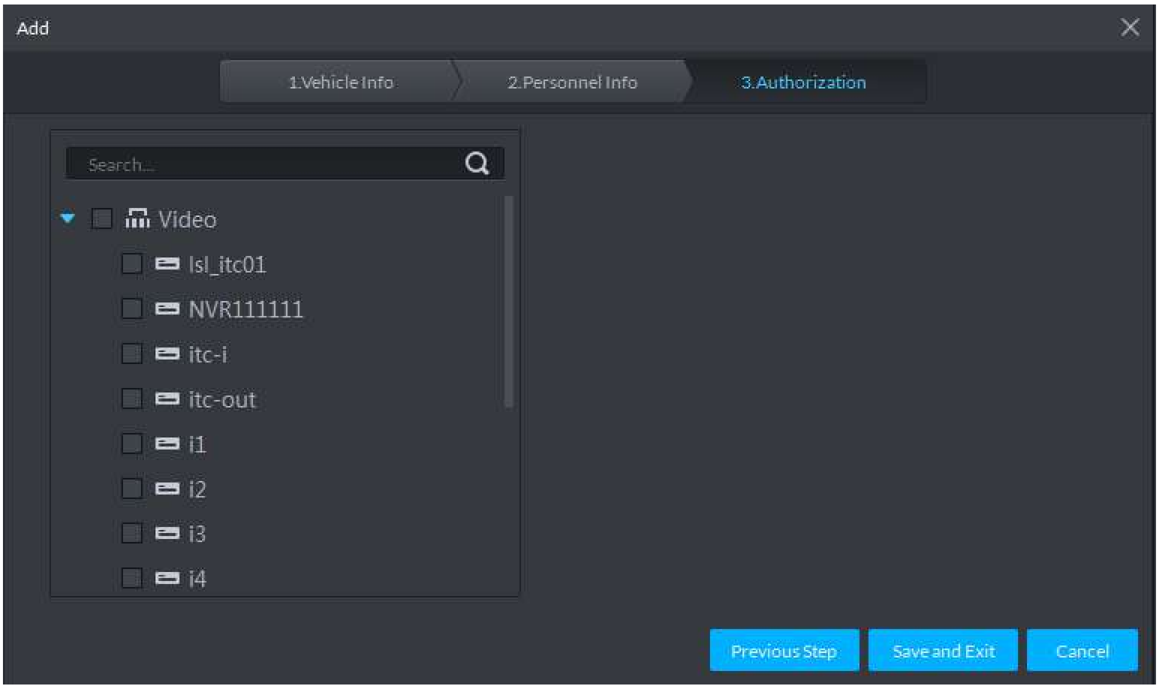
Parameter	Description
Plate No.	The plate number of added vehicle.
Vehicle Type	Include no group, general, VIP and blacklist. The first three types make up whitelist. If blacklist alarm scheme is set, then set vehicle type as blacklist, it will trigger alarm when vehicle is recognized.

Parameter	Description
Vehicle Color	Vehicle color of added vehicle. You can set **Not Recognized** if vehicle color cannot be recognized. If the color is beyond the selected range, then you can set is as **Other**.
Vehicle Logo	Main vehicle logos on the market.
Parking Lot	Area where vehicle belongs (required)
Validity Time	Validity period of added vehicle.
Expiration	
New Vehicle	If there are several vehicles, then click the button to add continuously. One person can add up to 5 vehicles.

Step 4 Set vehicle related personnel info, click **Next**.

The system displays the Authorization interface. See Figure 5-280.

Figure 5-280 Authorization



Step 5 Select all the ANPR devices that allow entrance and exit of the parkling lot, click **Save and Exit**. Synchronize vehicle info to corresponding ANPR device; make sure the ANPR device can make judgment if it has to release the vehicle even if ANPR device is disconnected to DSS platform.

5.17.6 Overview

View the free parking ratio of current parking area; make statistics over realtime quantiy and on-site vehicle quantity, view quantity of entrance and exit vehicle within some period.

Click ◔ on the Entrance interface. The system displays the interface of Overview. See Figure 5-281. Refer to Table 5-45 for parameter details.

Figure 5-281 Overview

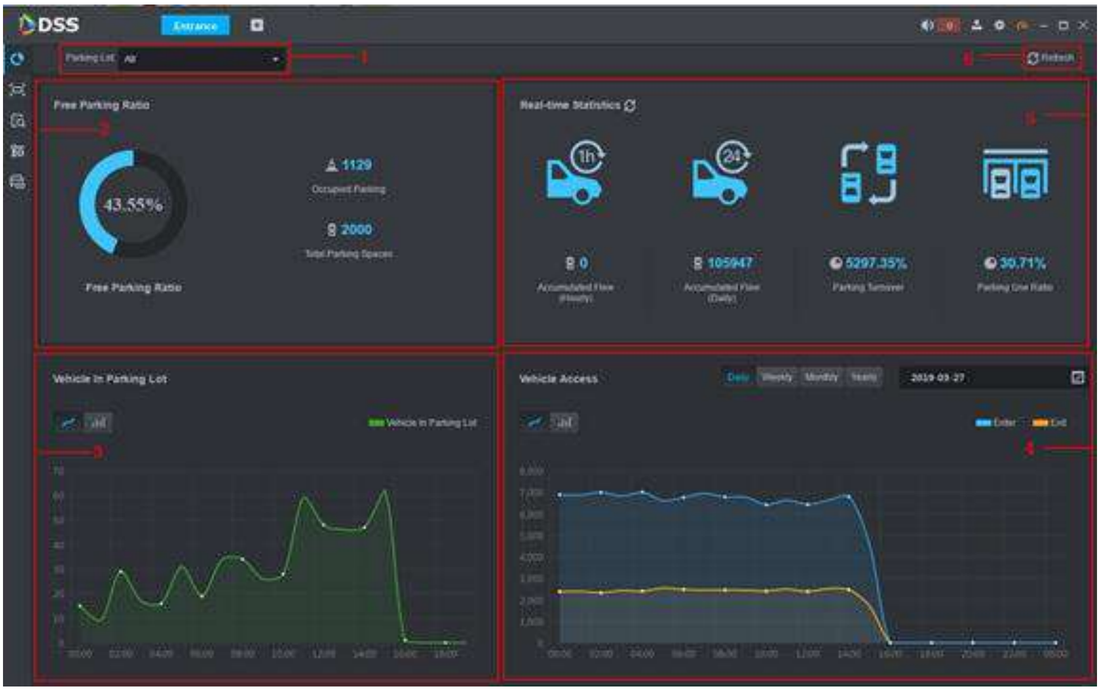


Table 5-45 Vehicle info overview

SN	Description
1	Interface displays the information of selected area; refer to other items for included content.
2	Display total parking spaces, occupied parking and free parking ratio of the selected parking lot.
3	Select occupied parking space quantity of selected area, the result can be displayed by line chart or bar chart. Move mouse on the image and displays corresponding time and occupied parking lot quantity.
4	Select vehicle access quantity of some period, supports day, week, month and year. Select time after period is selected; the system displays vehicle access quantity of selected period within the area. Blue means entered vehicle while orange means exited vehicle. The result can be displays by line chart or bar chart. Move the mouse on the image and display corresponding time and occupied parking space quantity.

SN	Description
5	Display following data. 1. Accumulated vehicle flow (hourly) Vehicle flow within current hour (for example, it is 8:42, and then it will make statistics about vehicle flow between 8:00 and 8:42). 2. Accumulated vehicle flow (Daily) Vehicle flow of the day (Start statistics from 00:00) 3. Parking turnover The bigger the parking turnover is, the shorter the vehicle stays in the parking lot, and then parking space reuse ratio is higher. If it is a paid parking lot, then it will make more money. 4. Parking Use Ratio The bigger the parking use ratio is, the average time of vehicle parking is longer.
6	Auto refresh overview info every 5 minutes. Click **Refresh** to sync realtime data.

5.17.7 License Plate Recognition

Click on the Entrance interface. The system displays the interface of License Plate Recognition. See Figure 5-282. Refer to Table 5-46 for more parameter details.

Figure 5-282 License plate recognition

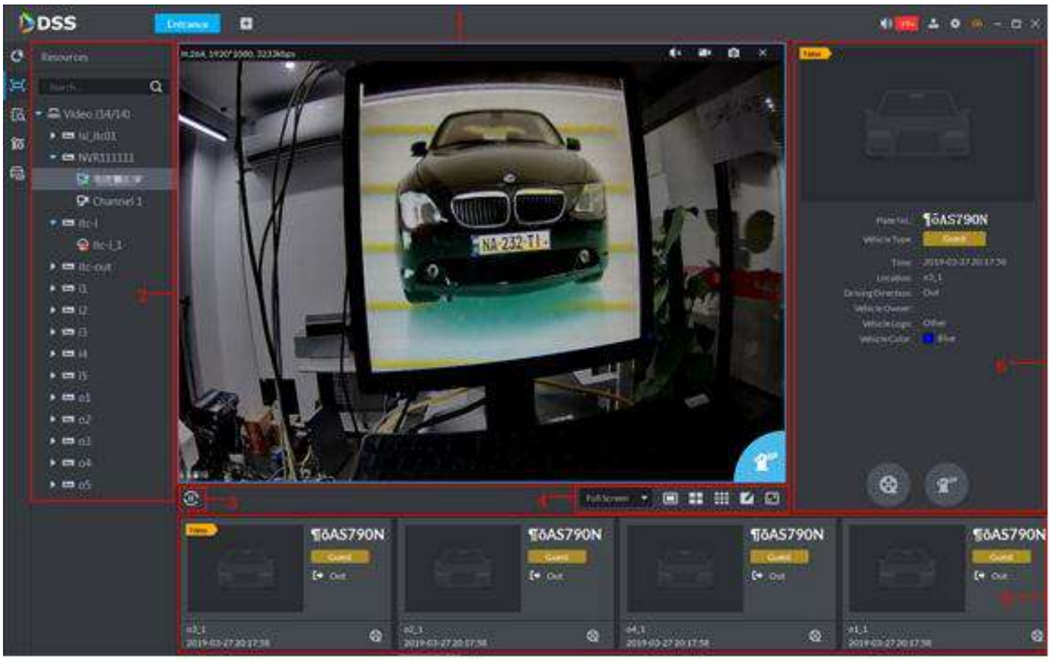


Plate No.: ¶6AS790N
Vehicle Type: Guest
Time: 2019-03-27 20:17:38
Location: o3_1
Driving Direction: Out
Vehicle Owner:
Vehicle Logo: Other
Vehicle Color: Blue

Table 5-46 LPR interface description

SN	Description
1	Realtime image display area. Select window, and double click video channel bound by ANPR in the device list, or drag the video channel bound by ANPR to window, and the interface displays realtime image. Move the mouse on the image, interface displays unlock button, click it to unlock barrier.
2	Device list. Display ANPR device and bound video channel.
3	Click the icon and it becomes ▶ and the interface will no longer ANPR recognition info. Click ▶ and the icon becomes, the interface will update realtime ANPR recognition info.
4	1. Full Screen ▾, set height and width ratio of video window, it plays video by two modes which are original scale and full screen. 2. , used to set image split mode, which includes 1 split, 4 splits and 9 splits, or click and customize split mode. 3. , switch video window to **Full Screen** mode. If you want to exit **Full Screen**, you can also press ESC button or right click to select **Exit Full Screen**.
5	Display latest 4 snapshots of LPR. More details as follows. 1. Double click and display snapshot details, vehicle info, snapshot panoramic picture and vehicle matting. 2. Click and view video of linked channel.
6	Display license plate snapshot and vehicle which need to be released manually. More operation as follows. 1. Click and unlock barrier to release vehicle. 2. Click and view video of linked channel.

5.17.8 Info Query

Search accessed vehicle, on-site vehicle and snapshot record.

Step 1 Click on the **Entrance** interface.

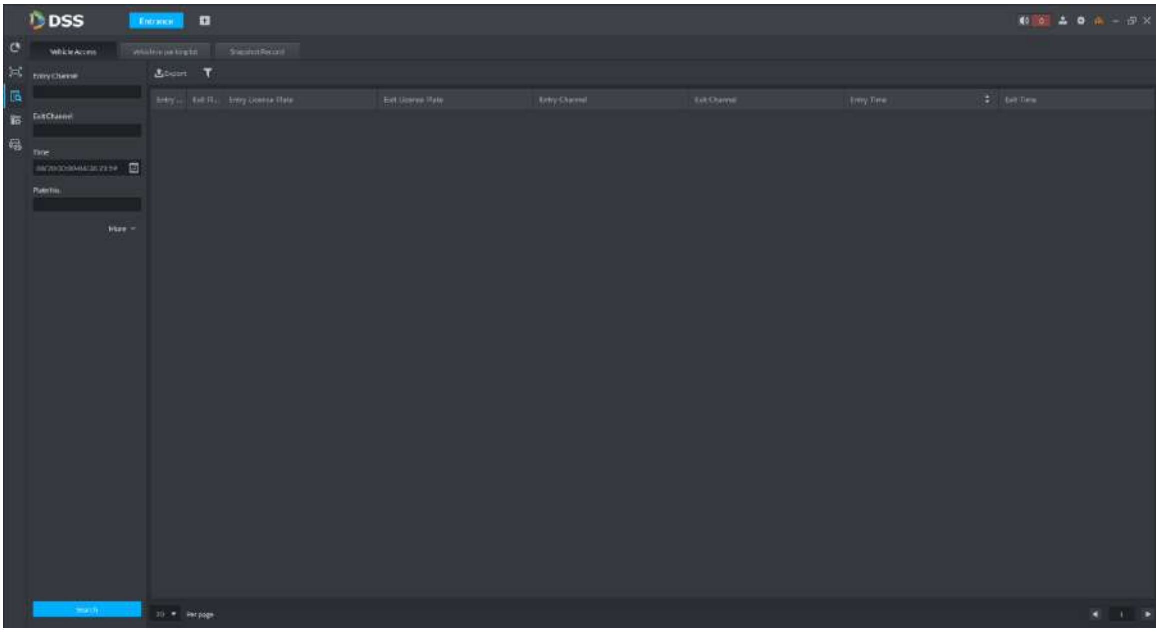
The system displays the interface of **Info Query**.

Step 2 Search vehicle in and out information.

1) Click the tab of **Vehicle Access**.

The system displays the interface of **Vehicle Access**. See Figure 5-283.

Figure 5-283 Vehicle access



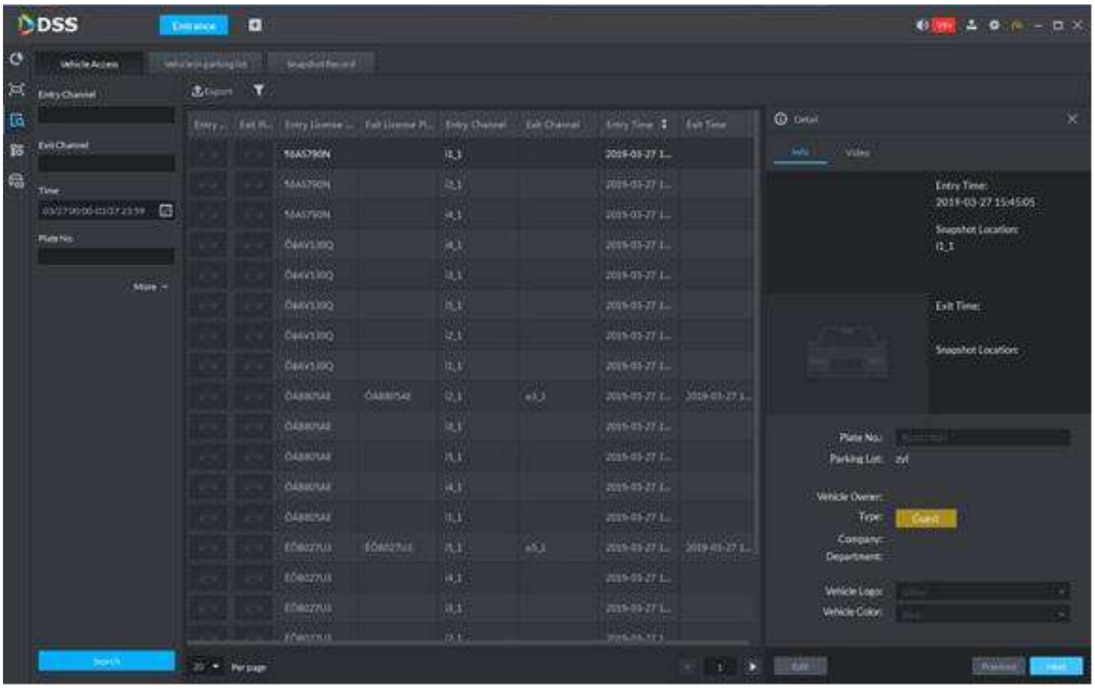
Entry ...	Exit Pi...	Entry License Plate	Exit License Plate	Entry Channel	Exit Channel	Entry Time	Exit Time

2) Set search condition, click Search.

The system displays search results. See Figure 5-284.

Click **More** and you can search by vehicle owner, department and vehicle type.

Figure 5-284 Vehicle access info



Entry ...	Exit Pi...	Entry License ...	Exit License Pl...	Entry Channel	Exit Channel	Entry Time	Exit Time
		56A5790N		i1_1		2019-03-27 1...	
		56A5790N		i2_1		2019-03-27 1...	
		56A5790N		i4_1		2019-03-27 1...	
		Ö4AV130Q		i4_1		2019-03-27 1...	
		Ö4AV130Q		i3_1		2019-03-27 1...	
		Ö4AV130Q		i5_1		2019-03-27 1...	
		Ö4AV130Q		i2_1		2019-03-27 1...	
		Ö4AV130Q		i1_1		2019-03-27 1...	
		ÖA8807A8	ÖA8807A8	i2_1	e3_1	2019-03-27 1...	2019-03-27 1...
		ÖA8807A8		i3_1		2019-03-27 1...	
		ÖA8807A8		i5_1		2019-03-27 1...	
		ÖA8807A8		i4_1		2019-03-27 1...	
		ÖA8807A8		i1_1		2019-03-27 1...	
		ÉÖ8027U3	ÉÖ8027U3	i5_1	e5_1	2019-03-27 1...	2019-03-27 1...
		ÉÖ8027U3		i4_1		2019-03-27 1...	
		ÉÖ8027U3		i3_1		2019-03-27 1...	

Entry Time:
2019-03-27 15:45:05
Snapshot Location:
i1_1

Exit Time:

Snapshot Location:

Plate No.:
Parking Lot: zyl

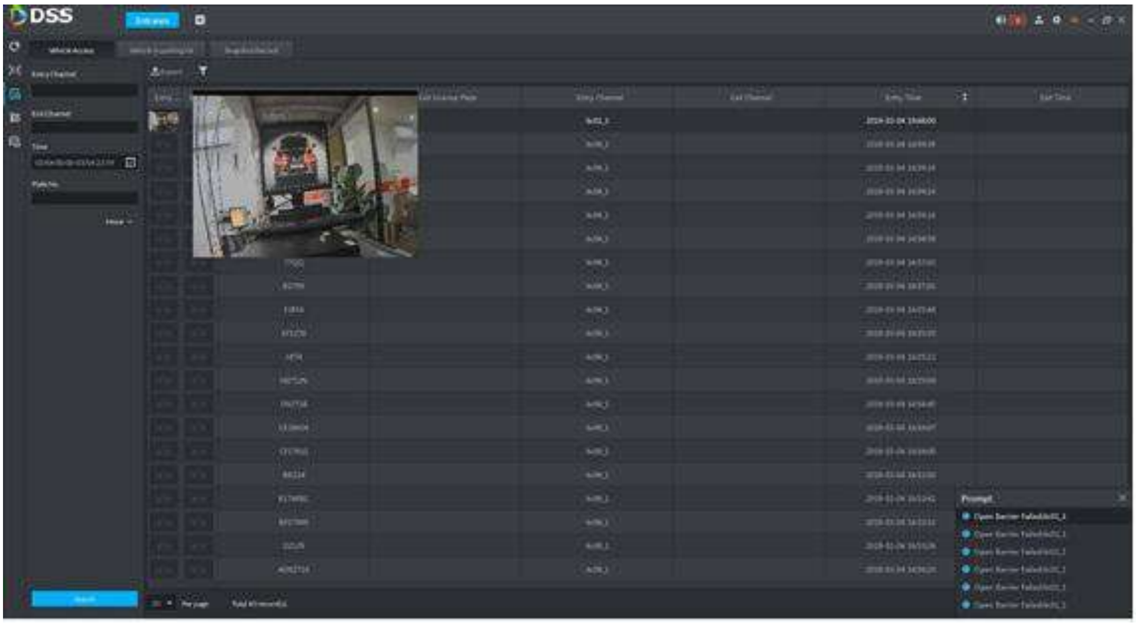
Vehicle Owner:
Type: Guest
Company:
Department:

Vehicle Logo:
Vehicle Color:

3) The related operations of vehicle access are as follows.

◇ Move the mouse to the recorded entry picture or exit picture, and the system will display a bigger picture. See Figure 5-285.

Figure 5-285 Vehicle bigger picture



◇ Double click the record, and detailed info is displayed on the right of interface. See Figure 5-286. Double click the picture in the Info, display big picture, drag green box and the big picture will be displayed in the lower right corner. See Figure 5-287. Click **Edit** to modify vehicle info, click **OK** to save config. Click **Video** to view linked video.

Figure 5-286 Vehicle detail(1)

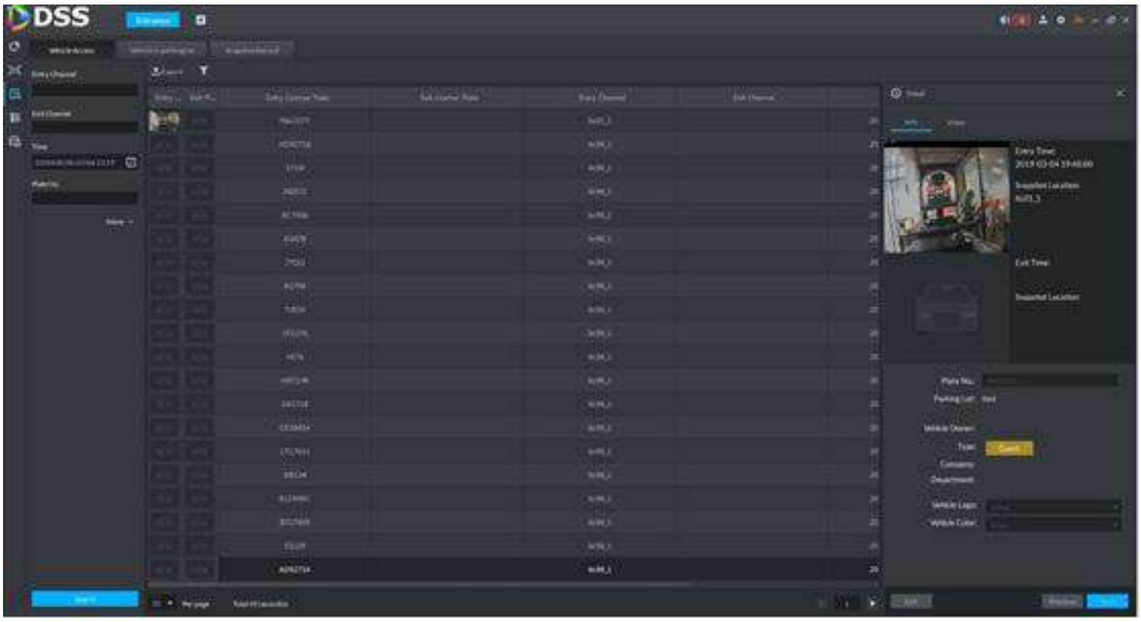
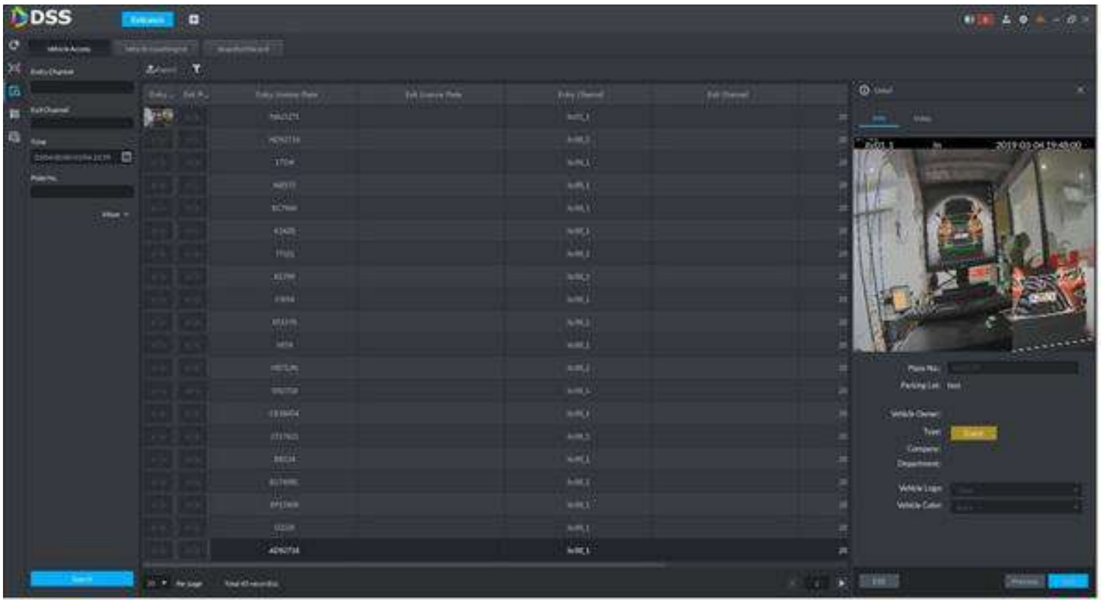


Figure 5-287 Vehicle detail(2)



◇ Export info. Click **Export** to export all the searched vehicle access info.

◇ Set info display item. Click and select display item.

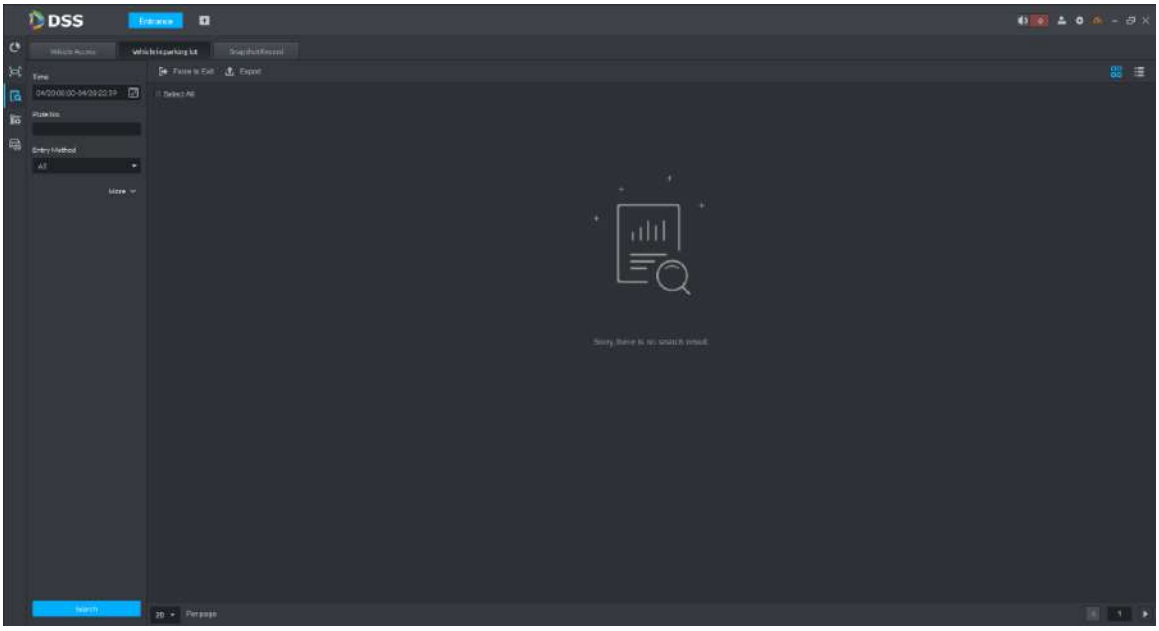
◇ Click **Next** and display next info detail. Click **Previous** and display previous info detail.

Step 3 Search on-site vehicle.

1) Click the tab of Vehicle in parking lot.

The system displays the interface of **Vehicle in Parking Lot**. See Figure 5-288.

Figure 5-288 Vehicle in parking lot

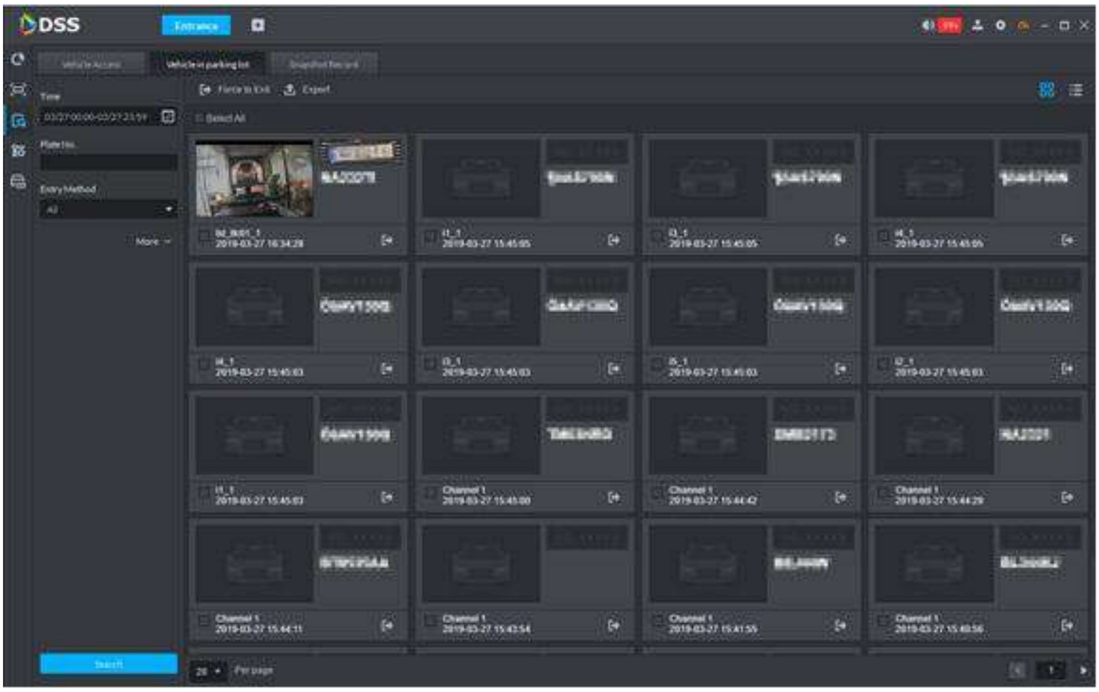


2) Set search condition, Click **Search**.

The system displays the search results. See Figure 5-289.

Click **More** and you can search info via vehicle owner, department and vehicle type.

Figure 5-289 Vehicle in parking lot



3) Related operations of vehicle in and out are as follows.

◇ If the vehicle is confirmed not to be in the area, then click to select information (several items supported), click Force to Exit or ⇥, make sure the vehicle exits by Pro.

◇ Export information. Click Export and export all the information of on-site vehicles that can be searched.

◇ Set info display item. Click ▼ and select display item.

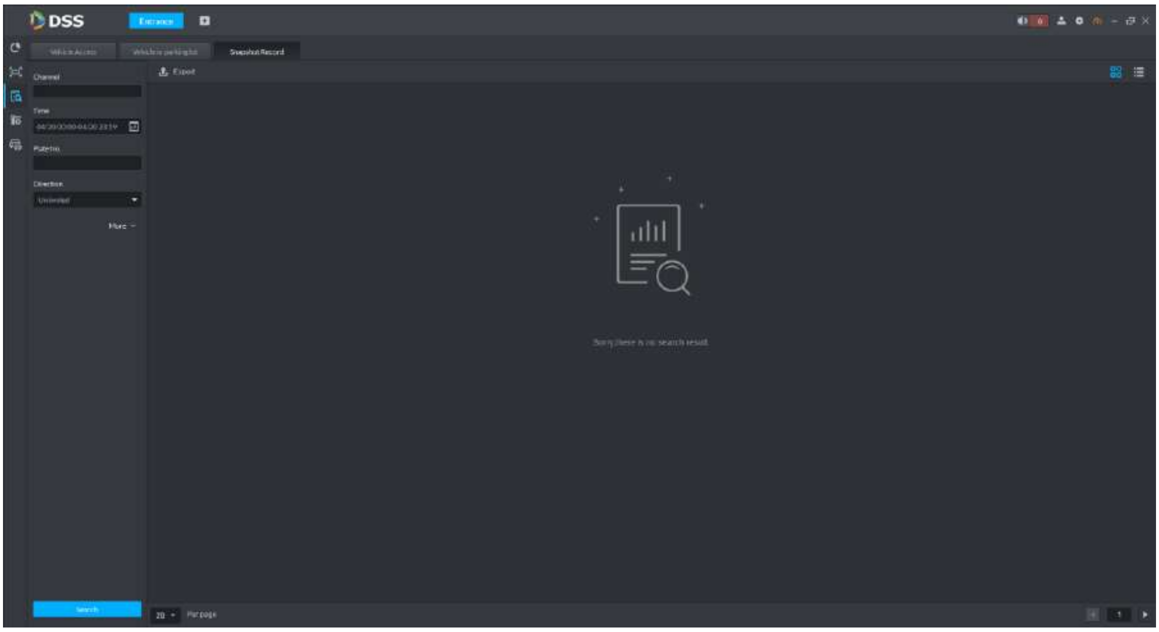
◇ Click view mode (⊞) or list mode (☰) to select different display mode.

Step 4 Search Snapshot Record

1) Click the tab of **Snapshot Record**.

The system displays the interface of **Snapshot Record**. See Figure 5-290.

Figure 5-290 Vehicle snapshot



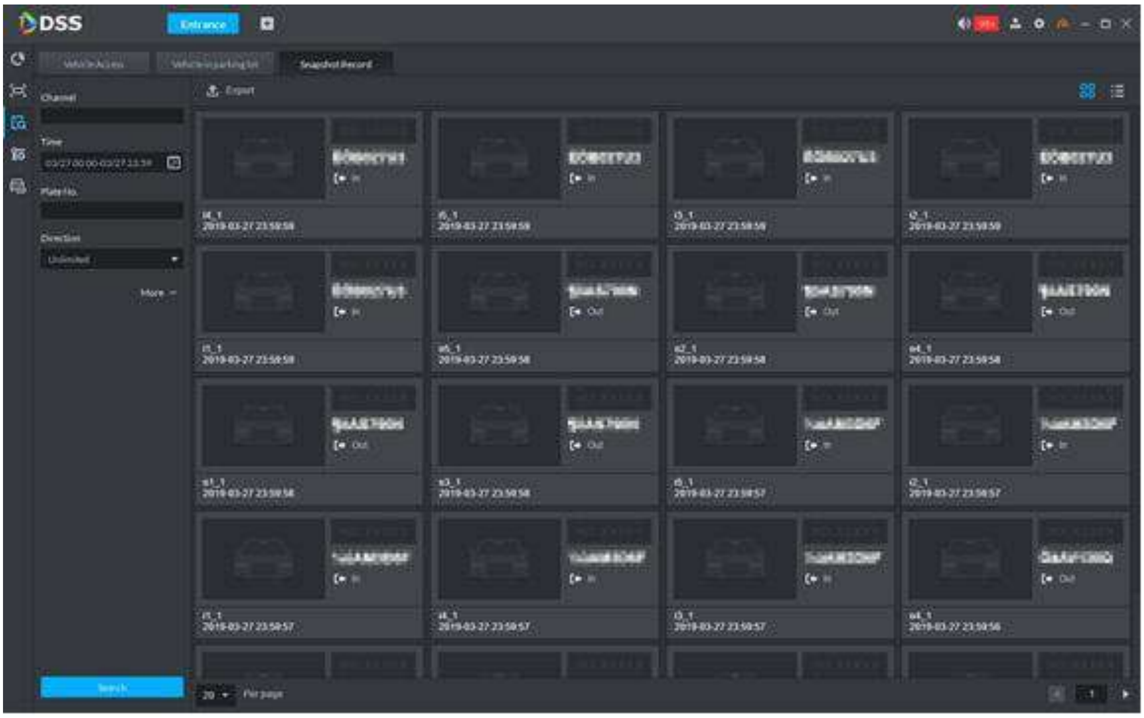
Sorry, there is no search result.

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

The system displays search results. See Figure 5-291.

Click **More** and you can search info via vehicle owner, department and vehicle type.

Figure 5-291 Vehicle snapshot



3) Related operations of vehicle snapshot are as follows.

◇ Export info. Click Export to export all the info of on-site vehicles that can be searched.

◇ Click view mode (⊞) or list mode (☰) and select different display modes.

5.18 Video Intercom

After integrating video talk module and adding video intercom device, you can realize device talk, realtime monitoring and issuing info.

5.18.1 Preparations

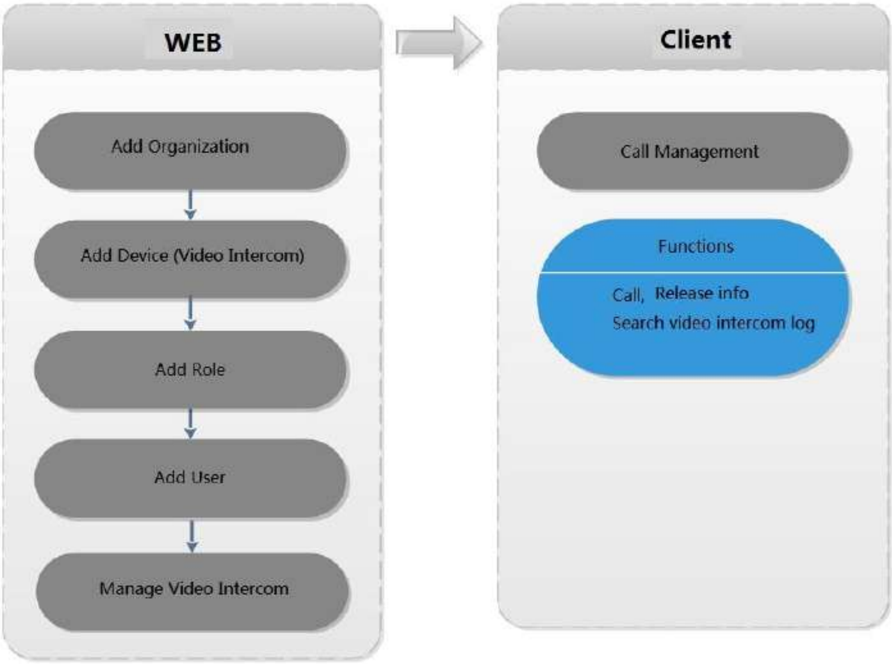
- The video intercom device is already configured before configuring video talk function in DSS platform. For detailed config, refer to user manual.
- Complete video intercom management on Web; refer to "4.12 Video Intercom Management" for more details.
- Add video talk devices such as unit VTO, VTH and fence VTO. Set Device Category as Video Intercom. Refer to "4.5 Adding Device" for more details.

📖

- Add VTH and it will create personnel automatically, extract room number and generate fixed personnel according to VTH SIP; room number can be used as personnel ID. Go to **Personnel Management** and you can view and edit.
- Device will not actively push info to Pro if device config is modified during operation. You need to enter the device modification interface and manually acquire device info.

See Figure 5-292 for video intercom config diagram.

Figure 5-292 Business flow



5.18.2 Call Management

Create device group, management group and relation group respectively; realize mutual call in the specific group. Only default system account supports the function.

⚠

Click ⟲ on the interface of device group, management group or relation group, the system will restore management group and relation group to original status.

5.18.2.1 Device Group Config

It can realize mutual call only when VTO and VTH are added into the same device group. Pro will automatically generate corresponding device group when VTO, verifying VTO and fence station are added to Pro.

- Add VTO and automatically generate a device group, add VTH of the unit into the group, and realize mutual call between VTH and VTO within the group.
- Add verifying VTO and automatically generate a device group, add it to the group together with the VTH of the same room, and realize mutual call between VTH and verifying VTO within the group.
- Add fence station and automatically generate a device group, add all the VTH into the group. Realize mutual call between fence station and all the VTH.
- Add VTH, if the VTH is automatically connected to unit VTO, verifying VTO, fence station, and then it will be automatically added to the device group, and realize mutual call among unit VTO, verifying VTO or fence station.

📖

Call between VTH is not restricted by device group; mutual call can be realized among VTH in different device groups.

5.18.2.2 Adding Management Group

Management group is to make groups for administrators, and realize relation binding of one to one, one to many or many to many. Administrators include Pro administrator and VTS. If there is default management group, VTS will be automatically added to management group when it is added.

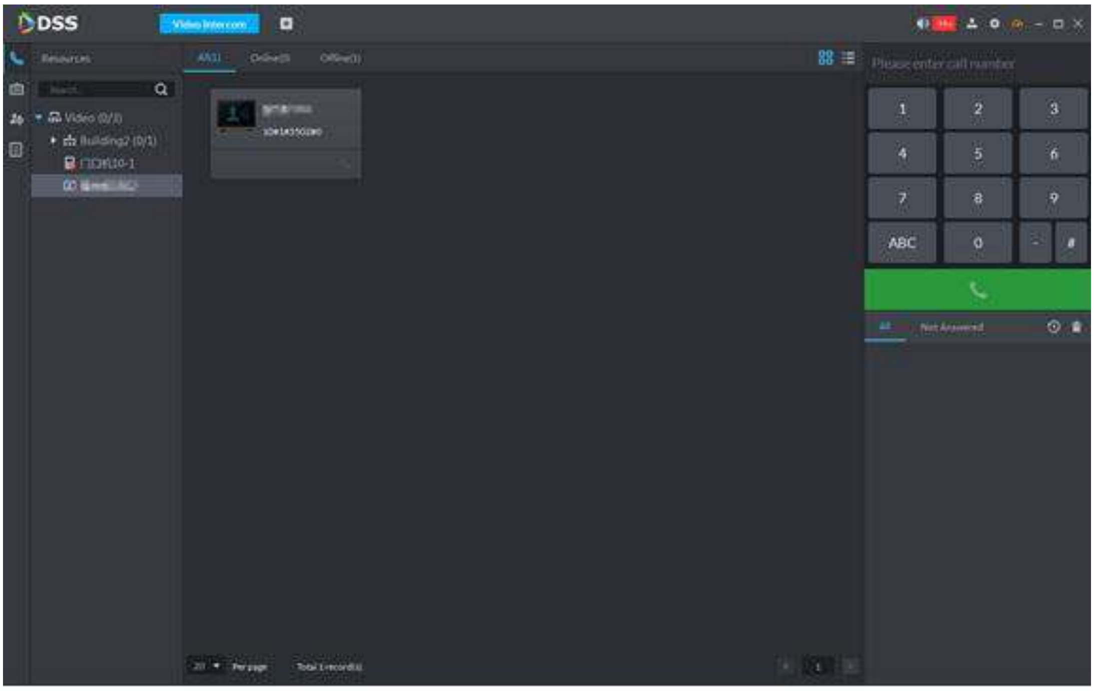
⚠

- Before configuring management group, it needs to create user, select video intercom menu permission and device permission, and add new users into management group.
- Use system user to configure group relation, need to switch to new user for login. If system logs onto many devices, then it cannot be used as administrator.

Step 1 Click ⊞ and select **Video Intercom** on the interface of **Homepage**.

The system displays the interface of **Video Intercom**. See Figure 5-293.

Figure 5-293 Video intercom



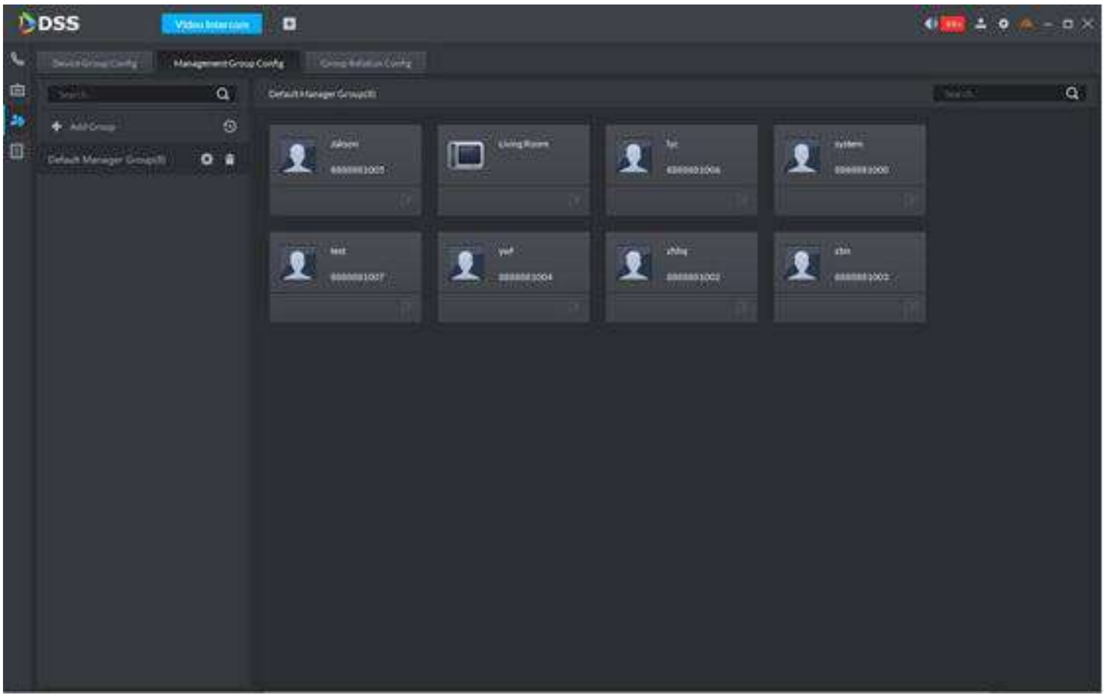
Step 2 Click.

The system displays the interface of **Call Management**.

Step 3 Click **Management Group Config**.

The system displays the interface of **Management Group Config**. See Figure 5-294.

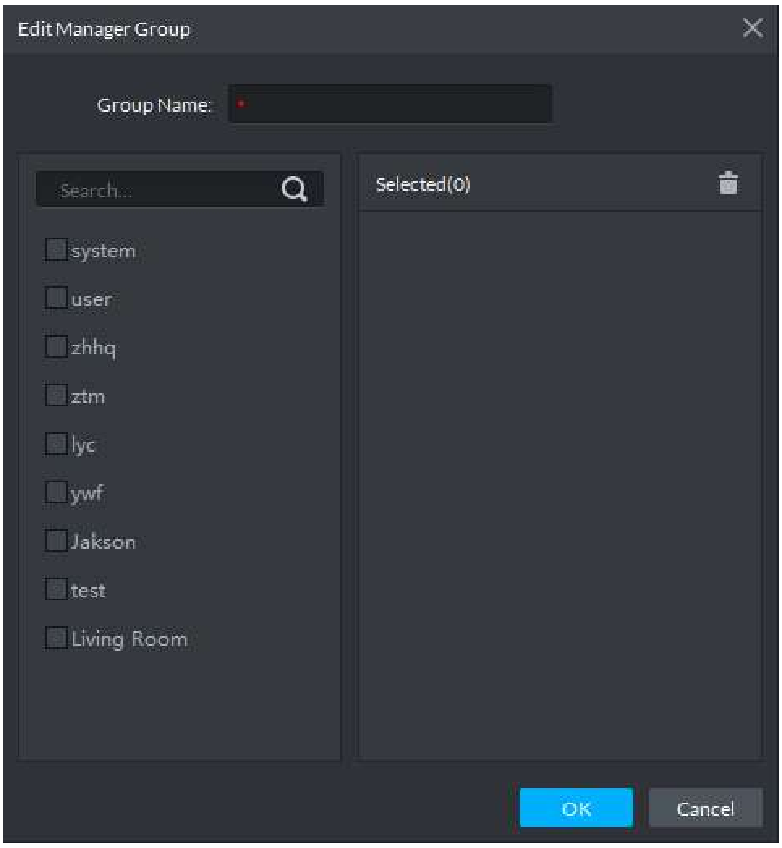
Figure 5-294 Call management



Step 4 Click **Add Group**.

The system displays the interface of **Edit Manager Group**. See Figure 5-295.

Figure 5-295 Edit management group



Edit Manager Group

Group Name: *

Search...

□ system

□ user

□ zhhq

□ ztm

□ lyc

□ ywf

□ Jakson

□ test

□ Living Room

Selected(0)

OK | Cancel

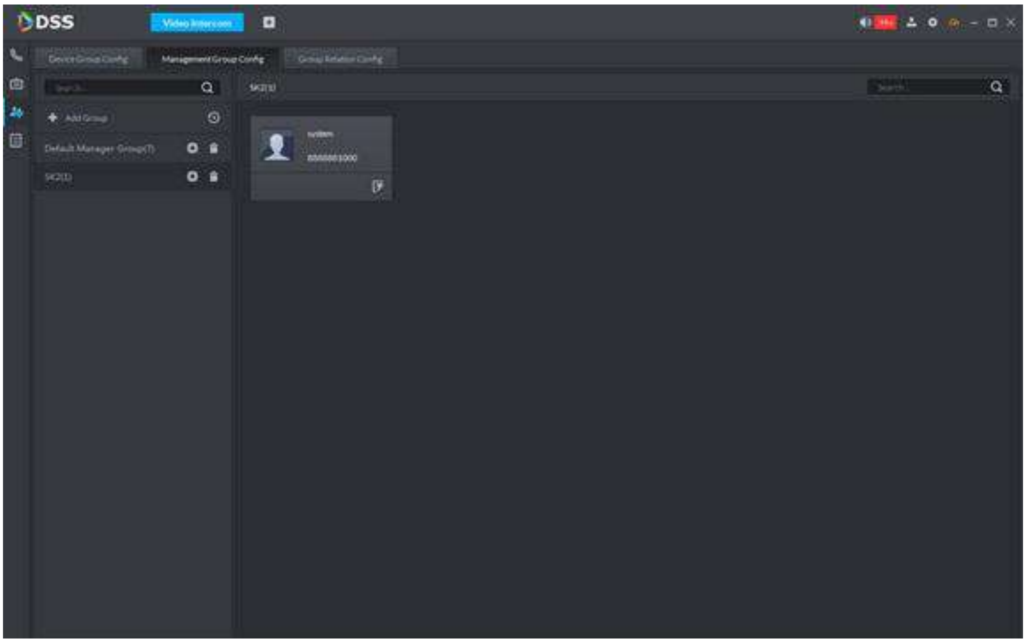
Step 5 Enter group name, select administrator account or VTS, and click **OK**.

The added management group is displayed in the list. See Figure 5-296.

The members in management group support following operation.

- Transfer members, click and move the member to the group.
- Manage group members, click to add or delete group member.

Figure 5-296 Management group



5.18.2.3 Group Relation Config

Relation group config means adding both device group and management group to the same relation group, making then related. Realize VTO or VTH only calling administration or VTS within the relation group.

There are two situations for relation binding

- Device group only binds one management group

  Any device in the group can call administration with one click, all the bound administrators within the management group will generate ring bell. At this moment, all other ring bell will stop as long as there is on administrator answers. The device call request can be rejected as long as all the administrators reject to answer.

- Device group binds several management groups

  There is priority among several management groups. When any device in the group calls administrator with one click, and all the online administrators of management group with highest priority will generate ring bell. If none of these administrators answer, then it will call next management group. The interval between two calls is 30s; it can skip up to one management group. If neither of two groups answer, then the device prompts call overtime, no response.

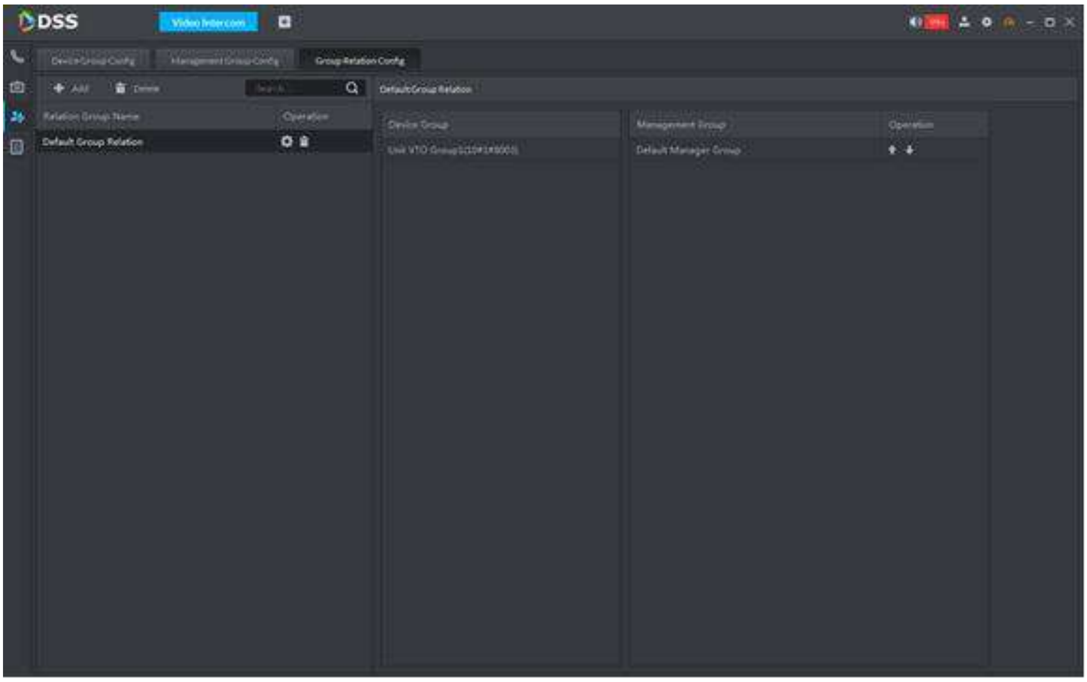
Step 1 Click on the interface of **Video Intercom**.

The system displays the interface of **Relation Group Config**.

Step 2 Click the tab of **Relation Group Config**.

The system displays the interface of **Relation Group Config**. See Figure 5-297.

Figure 5-297 Group relation config



Relation Group Name	Operation
Default Group Relation	

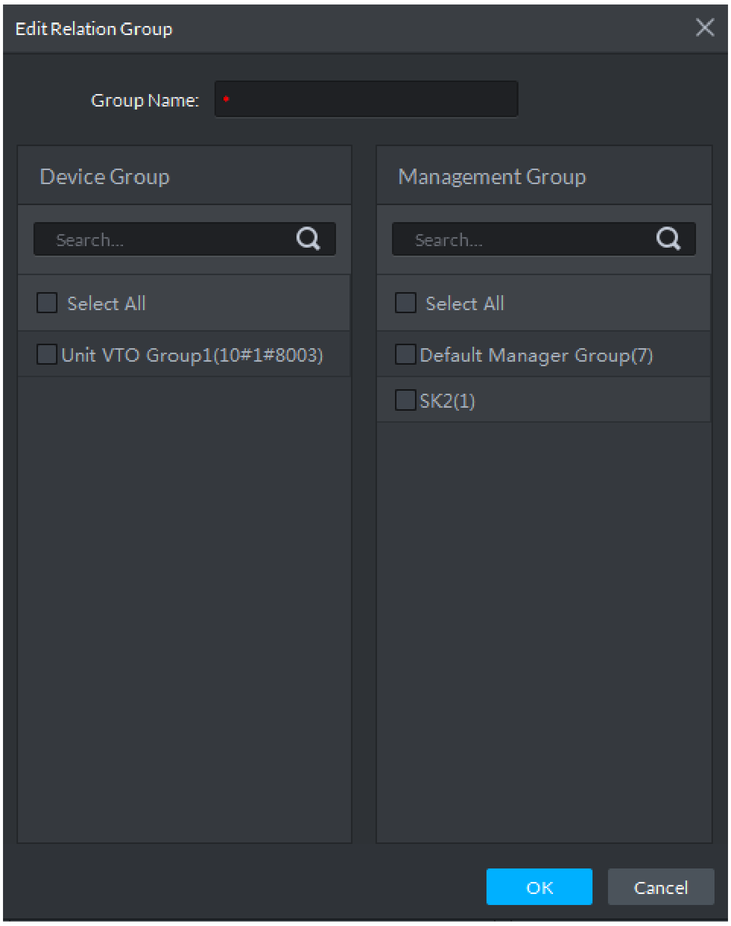
Device Group
Unit VTO Group1(10#1#000)

Management Group	Operation
Default Manager Group	↑ ↓

Step 3 Click **Add**.

The system displays the interface of **Edit Relation Group**. See Figure 5-298.

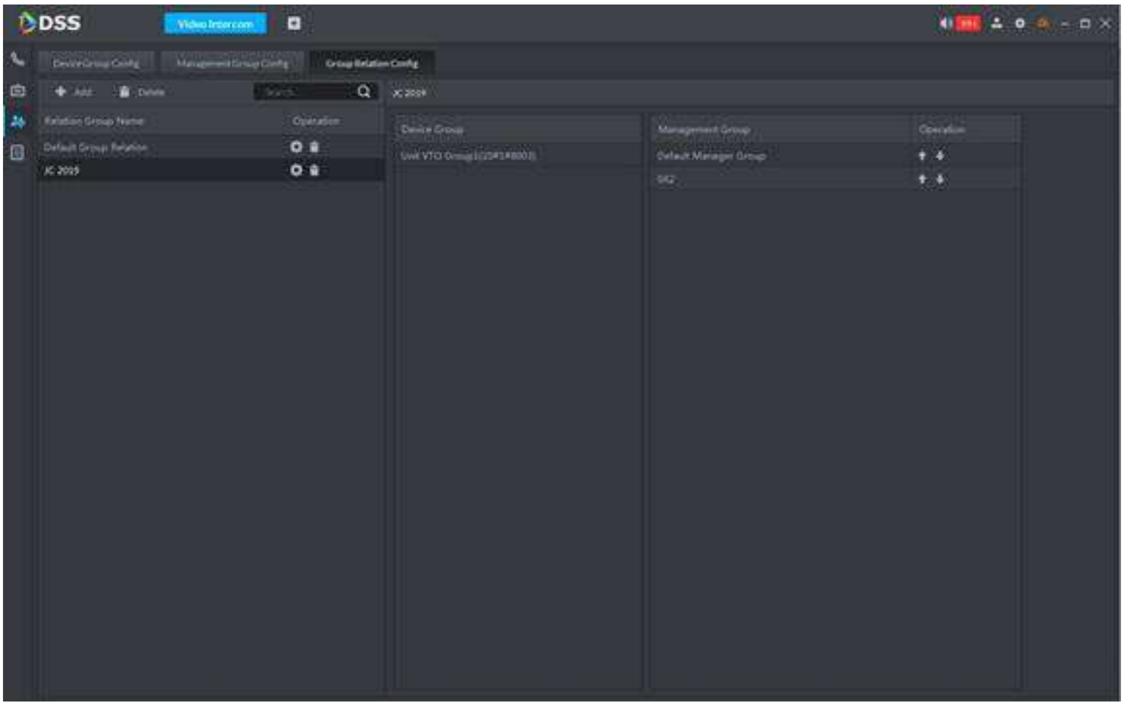
Figure 5-298



Step 4 Enter name, select device group and management group, Click **OK**.

Added relation group is displayed in the list. See Figure 5-299. If there are several relation groups, you can click ⬆ or ⬇ to adjust priority level. When there is call, the online administrators with high priority will generate ring bell first.

Figure 5-299 Edit relation group



Relation Group Name	Operation
Default Group Relation	
JC 2019	

Device Group
Unit VTO Group1(10#1#8001)

Management Group	Operation
Default Manager Group	
GQ	

5.18.3 Video Intercom Application

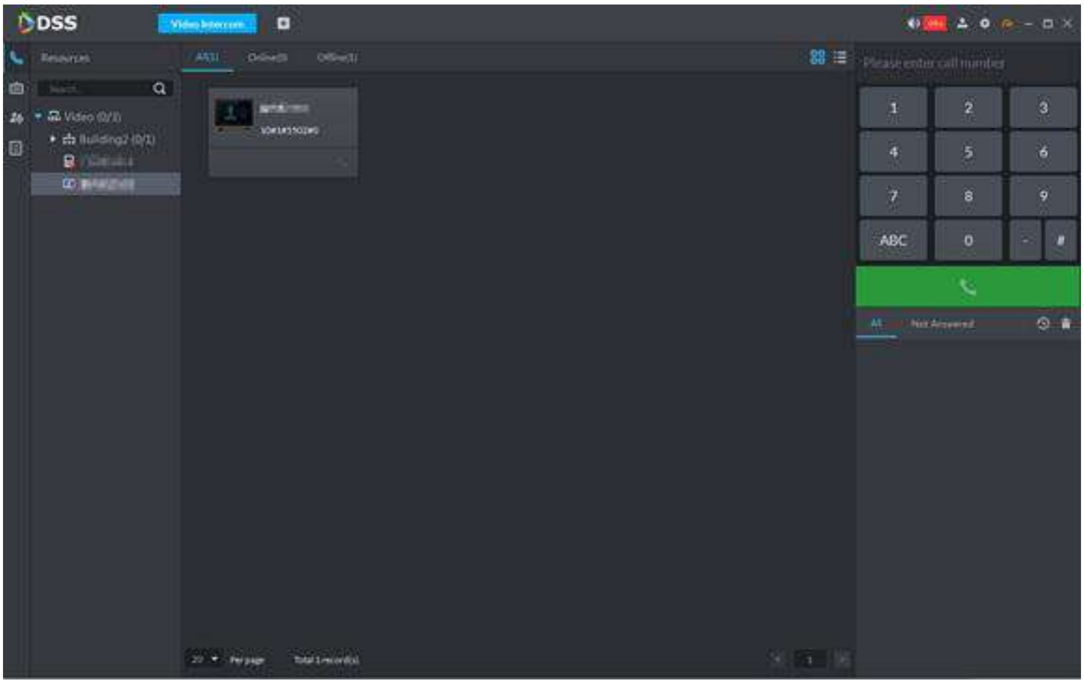
5.18.3.1 Call Center

Realize call among Pro, VTO and VTH.

Step 1 Click ☎ on the interface of **Video Intercom**.

The system displays the interface of **Call Center**. See Figure 5-300

Figure 5-300 Call center



Step 2 You can call VTO and VTH on the interface of **Call Center**.

- Pro Call VTO

Select VTO in the device list; click corresponding ▶ of VTO and call VTO. The system pops out call interface and realize video talk. See Figure 5-301. Following operations are support during call.

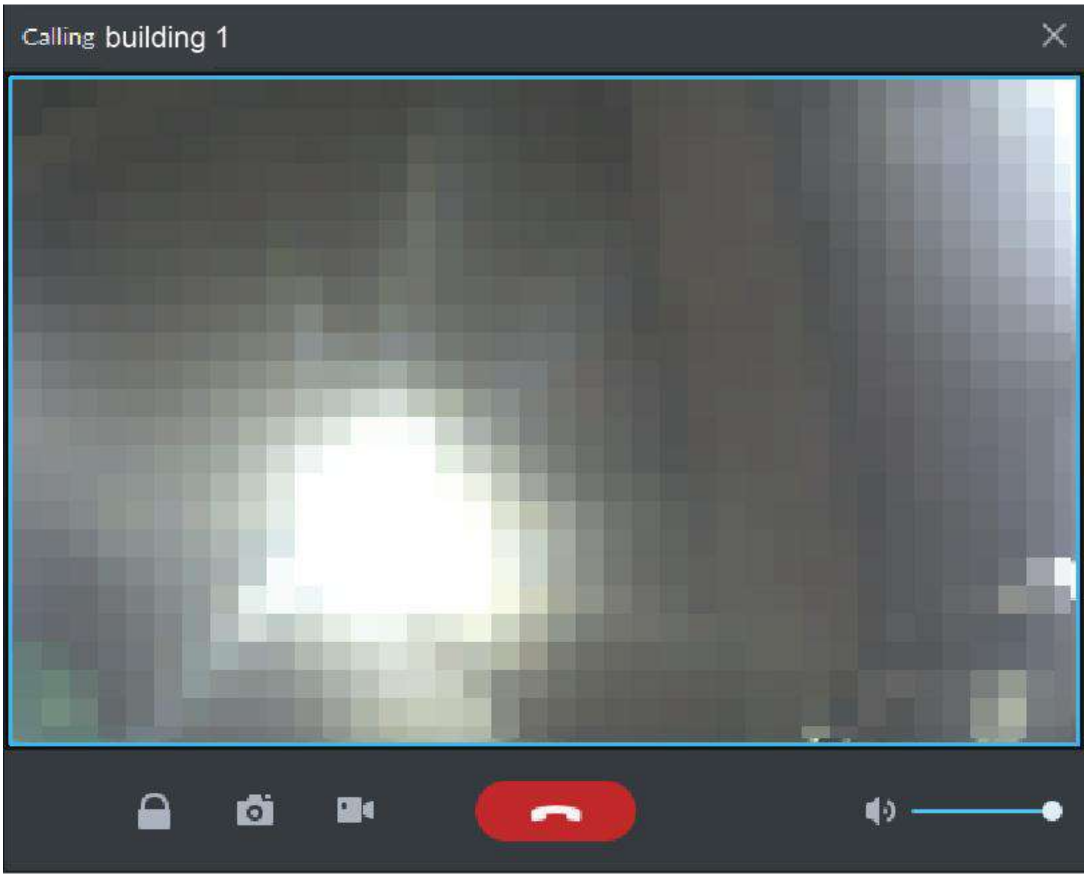
◇ 🔒, if VTO is connected to lock, click the icon to unlock.

◇ 📷, click the icon to capture picture, the snapshot is saved into the default directory installed by client. If you need to modify the save path of snapshot, refer to "5.2 Local Configuration" for more details.

◇ 📹, click the icon to start record, click again to stop record. The video is saved in default path installed by client. If you need to modify the save path, refer to "5.2 Local Configuration" for more details.

◇ ☎, click the icon to hang up.

Figure 5-301 Call VTO



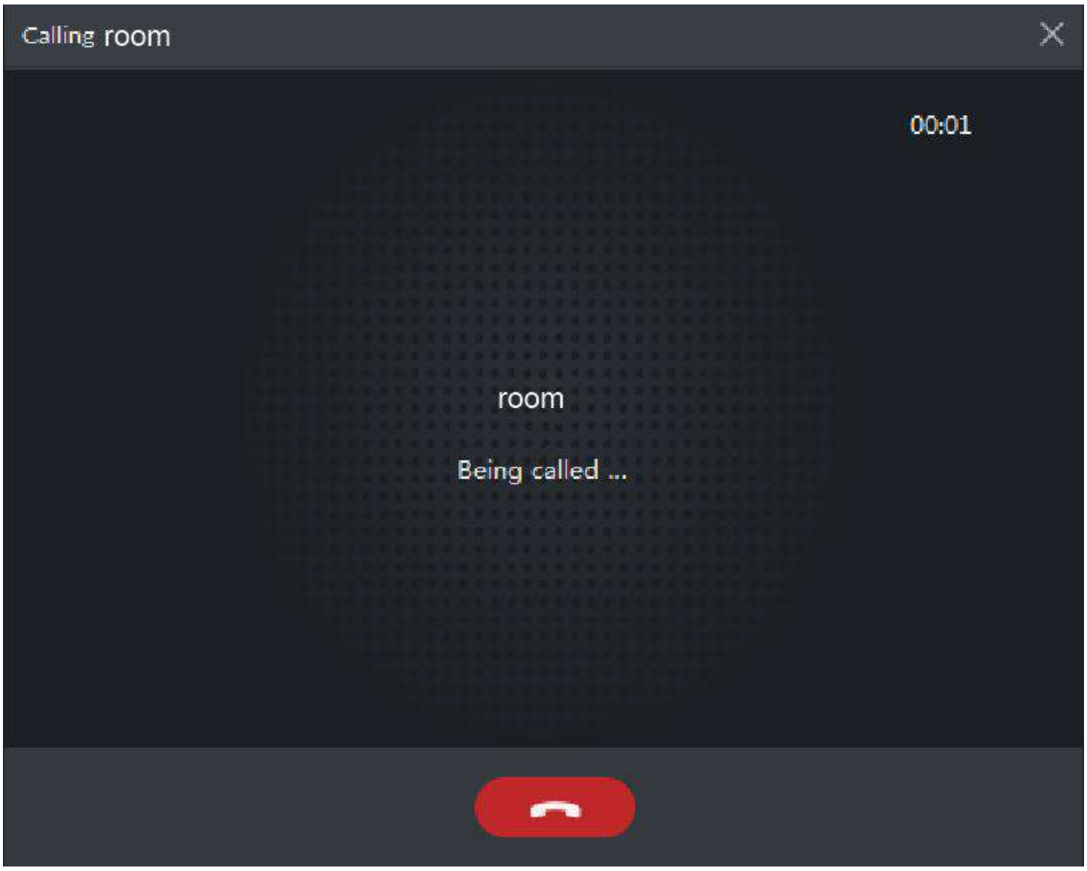
- Pro Call VTH

Select VTH from the device list, click ☎ on the VTH or dial corresponding VTH on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait …**, see Figure 5-302. There are two modes for answering the call.

◇ Answer by VTH, bidirectional talk between client and VTH. Press ☎ to hang up when you answer the call.

- ◇ If VTH fails to answer over 30s, busy or hang up directly, then it means the callee is busy.

Figure 5-302 Call VTH



room

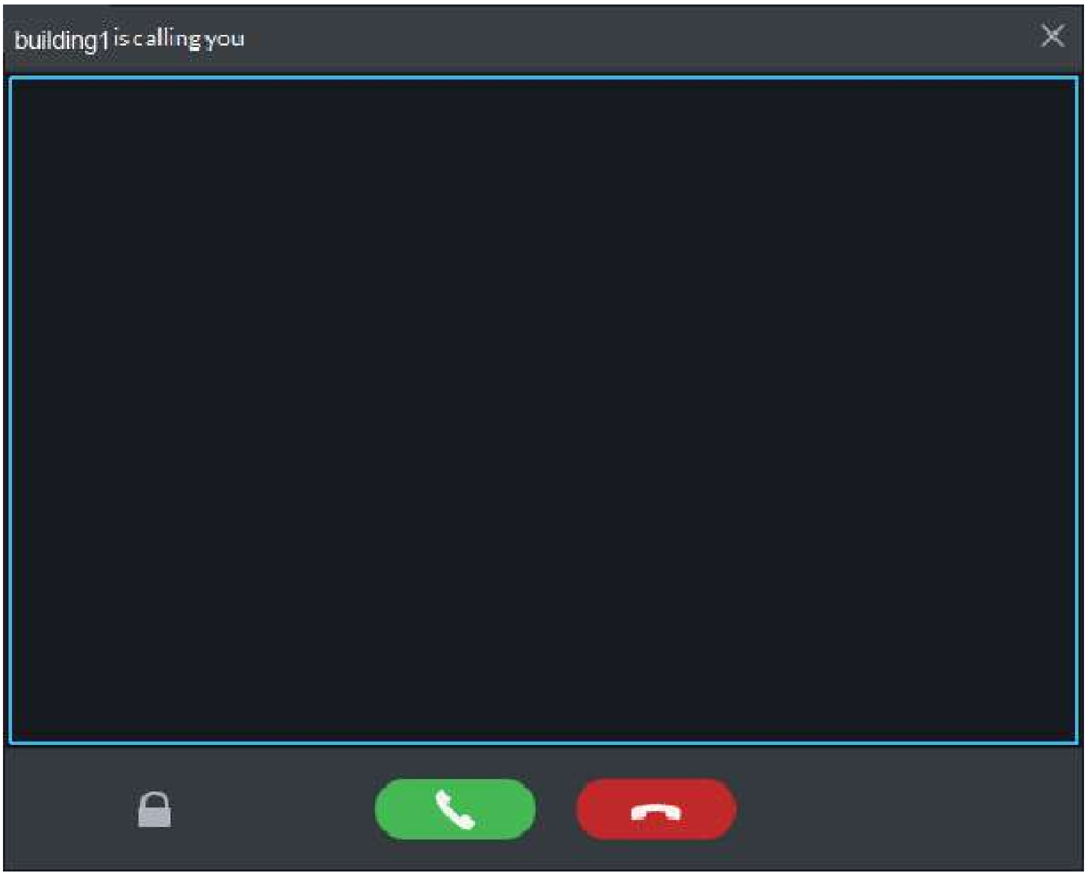
Being called ...

- VTO Call Pro

  VTO calls platform, client pops up the dialog box of VTO calling. See Figure 5-303.

  - ◇ 🔒, if VTO is connected to lock, click the icon to unlock.
  - ◇ 📞, click the icon, answer VTO, realize mutual call after connected.
  - ◇ 🟥, click the icon to hang up.

Figure 5-303 VTO calls platform



building1 is calling you

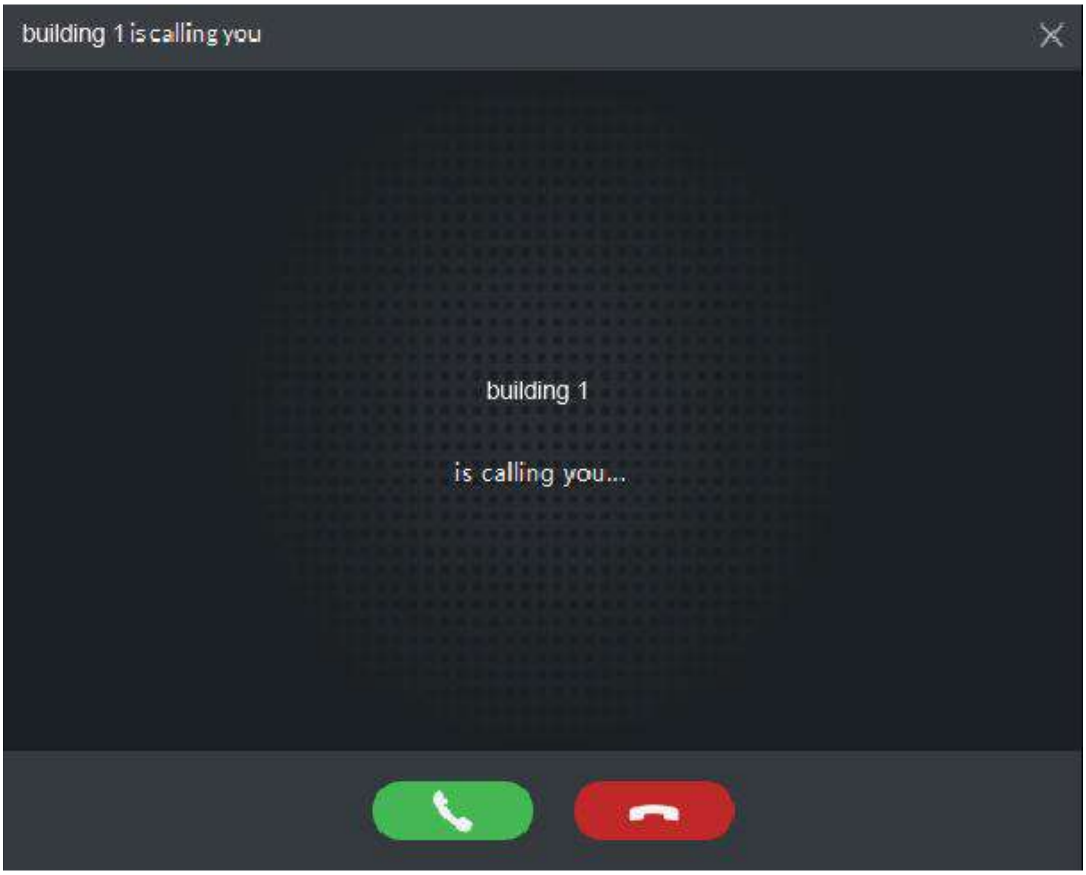
- If VTH is calling platform

The client pops out the dialog box of VTH calling. See Figure 5-304. Click 🟩 and realize talk with VTH.

◇ 🟩, click the icon and answer VTO, realize mutual talk after connected.

◇ 🟥, click the icon and hang up.

Figure 5-304 VTH calling platform



building 1 is calling you

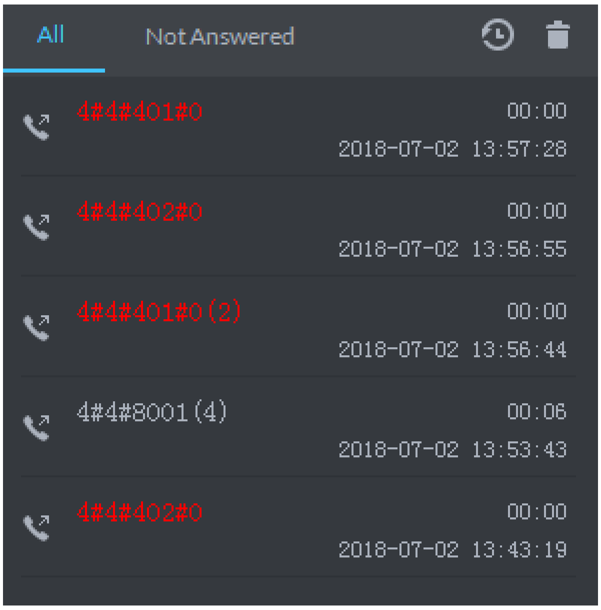
building 1

is calling you...

- Call via call record

  All the call records are displayed in the **Call Record** in the lower right corner of the interface of **Video Intercom**. See Figure 5-305. Move the mouse to the record, click ☎ and call back.

Figure 5-305 Call record



4#4#401#0 00:00
2018-07-02 13:57:28

4#4#402#0 00:00
2018-07-02 13:56:55

4#4#401#0 (2) 00:00
2018-07-02 13:56:44

4#4#8001 (4) 00:06
2018-07-02 13:53:43

4#4#402#0 00:00
2018-07-02 13:43:19

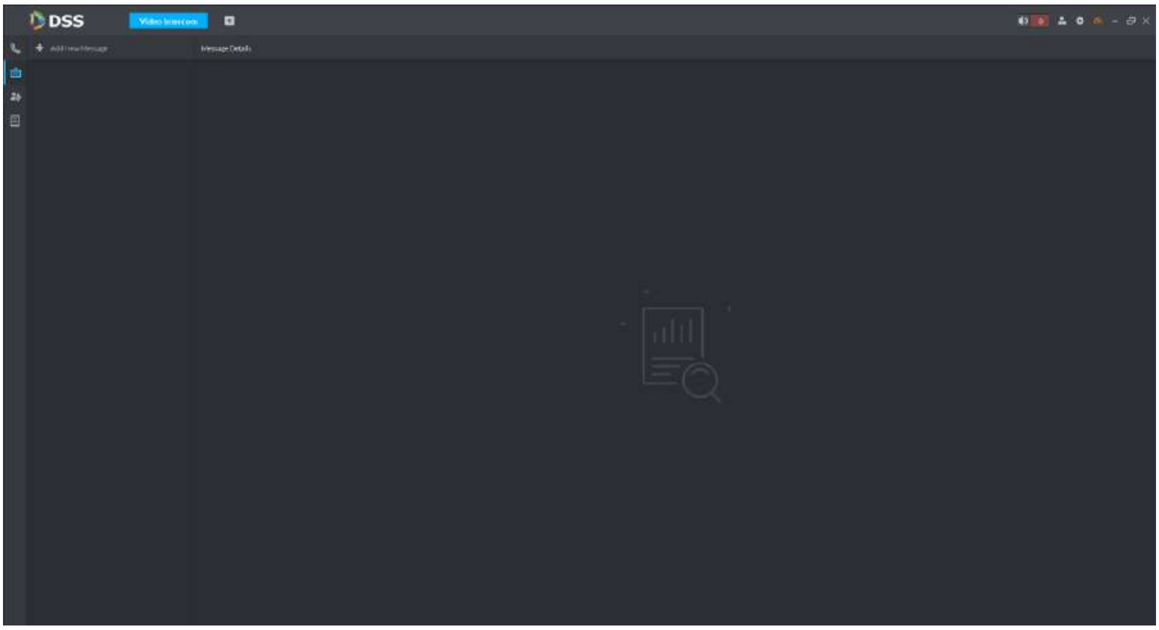
5.18.3.2 Release Info

Send message to designated VTO.

Step 1 Click on the interface of **Video Intercom**.

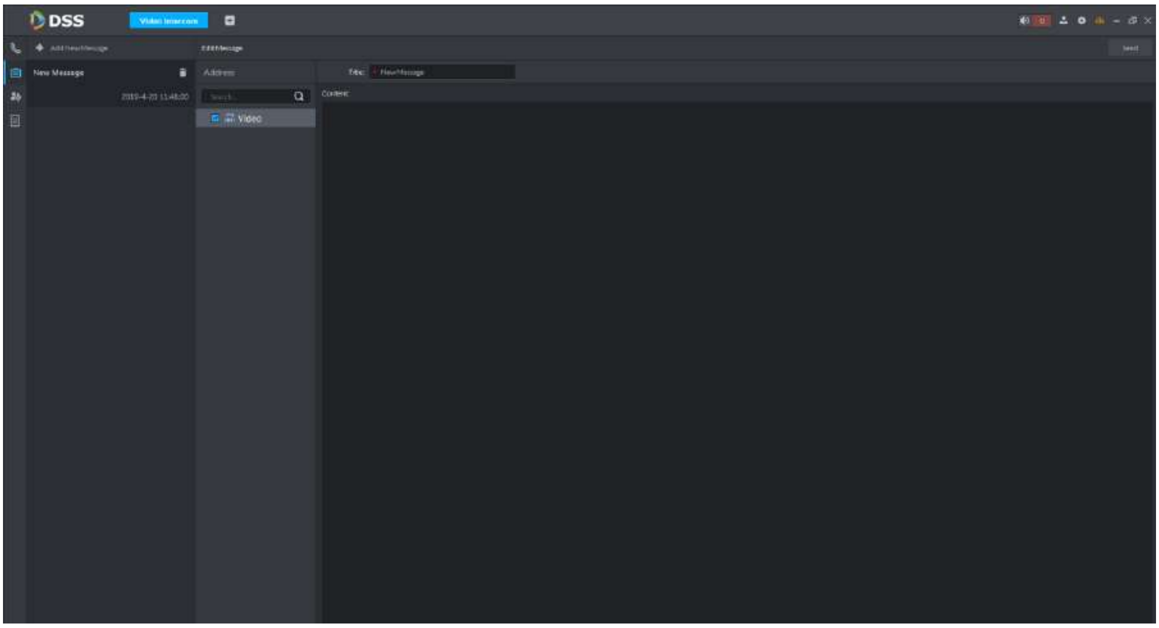
The system displays the interface of **Release Info**. See Figure 5-306.

Figure 5-306 Release information(1)



Step 2 Click **Add New Message**, select VTH and add release info. See Figure 5-307.

Figure 5-307 Release information(2)



Step 3 Click **Send**.

The VTH will receive the message after it is sent successfully.

5.18.3.3 Search Video Intercom Log

View log records and you can trace recorded calls.

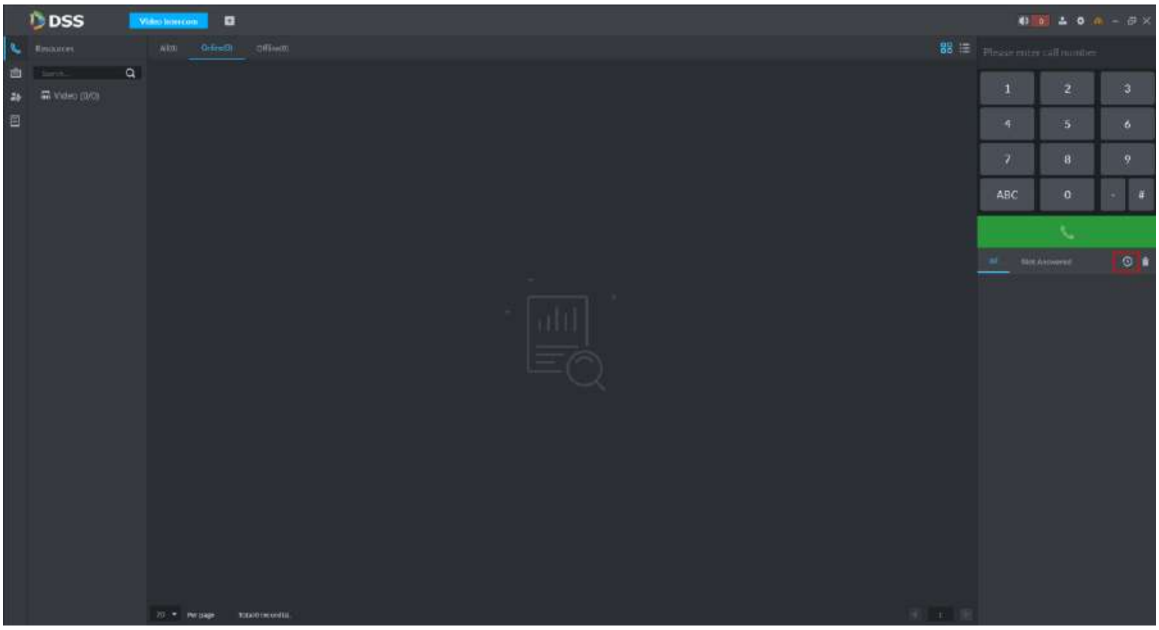
Step 1 Enter the interface of video intercom log.

The system supports following two ways to enter.

Click on the interface of **Video Intercom**.

Click ⧉ and enter console on the interface of **Video Intercom**. See Figure 5-308

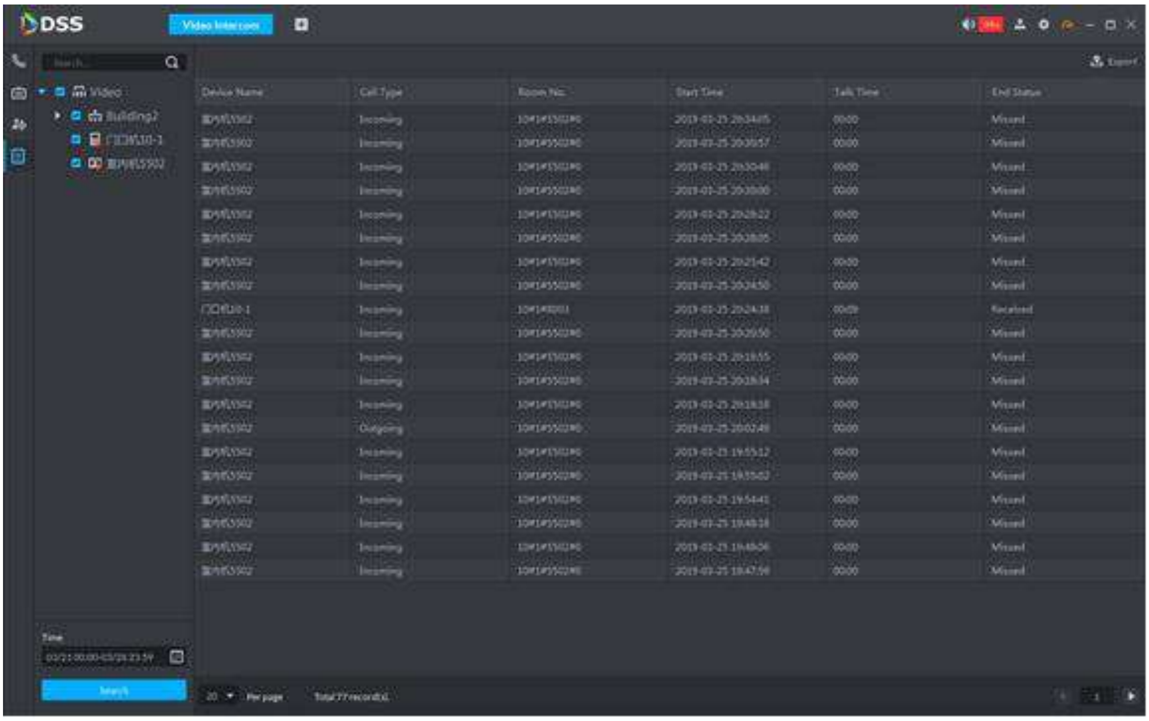
Figure 5-308 Video intercom log interface



Step 2 Set conditons, click **Search**.

The system displays the log info. See Figure 5-309

Figure 5-309 Search log



Device Name	Call Type	Room No.	Start Time	Talk Time	End Status
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:34:05	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:30:57	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:30:48	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:30:00	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:28:22	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:28:05	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:21:42	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:24:50	00:00	Missed
门口机10-1	Incoming	10#1#0001	2019-03-25 20:24:18	00:09	Received
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:20:50	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:19:55	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:18:34	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 20:18:18	00:00	Missed
室内机5502	Outgoing	10#1#5502#0	2019-03-25 20:02:48	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 19:55:12	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 19:55:02	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 19:54:41	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 19:48:18	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 19:48:06	00:00	Missed
室内机5502	Incoming	10#1#5502#0	2019-03-25 19:47:56	00:00	Missed

Step 3 Click **Export** and the logs will be saved locally according to system prompt.

5.19 Attendance Management

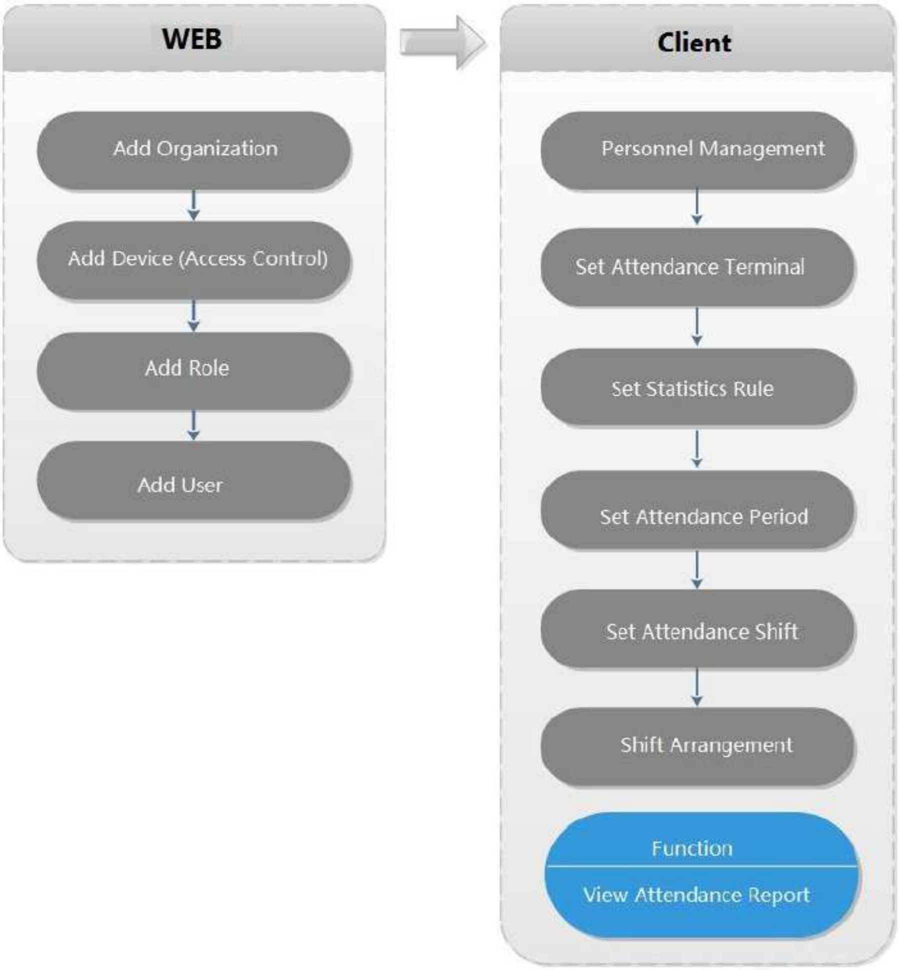
Integrate attendance module, add access control device, manage and configure attendance by Pro, view attendance data.

5.19.1 Preparations before Operation

- Access control is already added on Web, and bound with resource. For details, refer to "4.5 Adding Device".
- Personnel are already added. For details, refer to "5.15 Personnel Management".

See Figure 5-310 for attendance management flow.

Figure 5-310 Business flow



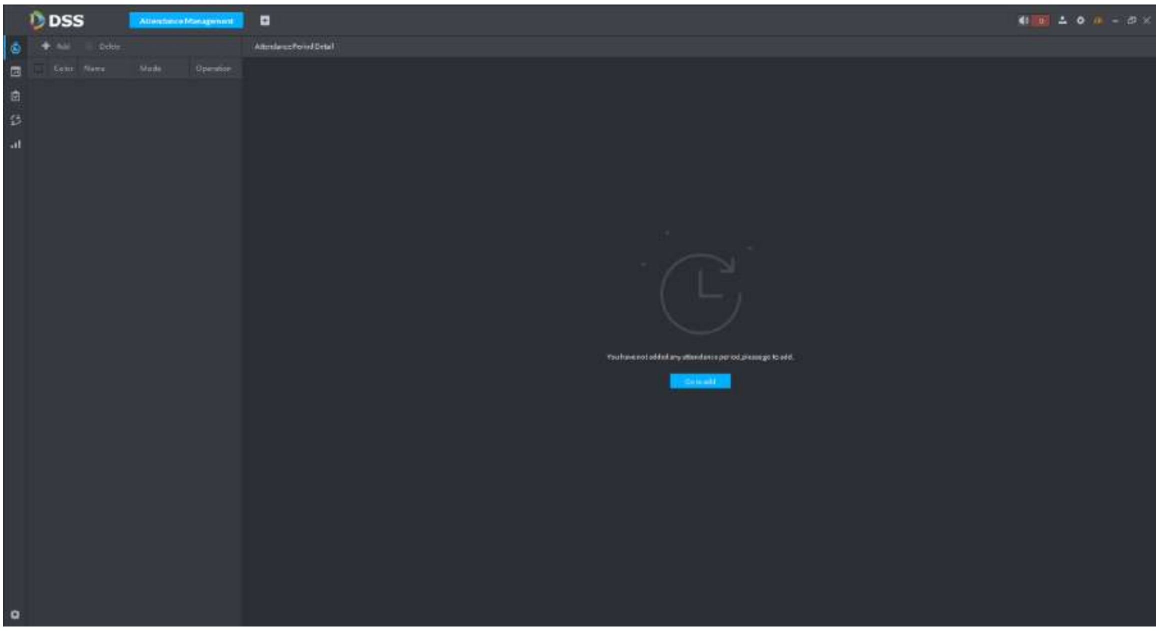
5.19.2 Setting Attendance Terminal

Make sure access control is used as attendance device, used to punch card, record attendance info and upload attendance data.

Step 1 Click ⊞ and select **Attendance Mangement** on the interface of **Homepage**.

The system displays the interface of **Attendance Management**. See Figure 5-311.

Figure 5-311 Attendance management

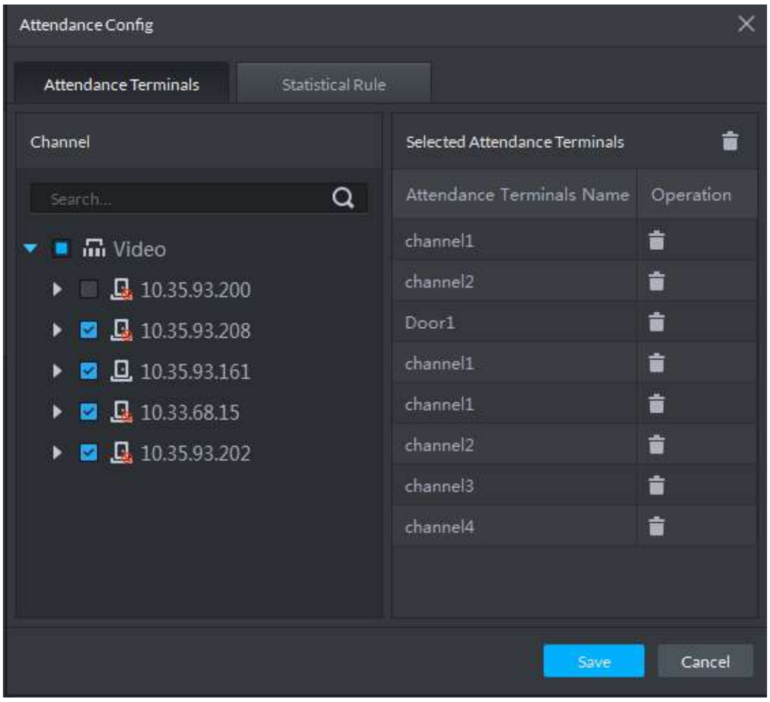


You have not added any attendance period, please go to add.

Step 2 Click ⚙ on the lower left corner of the interface, select **Attendance Terminal**.

The system displays the interface of **Attendance Terminal**. See Figure 5-312.

Figure 5-312 Attendance terminal setting



- ■ Video
  - □ 10.35.93.200
  - ☑ 10.35.93.208
  - ☑ 10.35.93.161
  - ☑ 10.33.68.15
  - ☑ 10.35.93.202

Selected Attendance Terminals

Attendance Terminals Name	Operation
channel1	🗑
channel2	🗑
Door1	🗑
channel1	🗑
channel1	🗑
channel2	🗑
channel3	🗑
channel4	🗑

Step 3 Select access control channel from the left list, click **Save**.

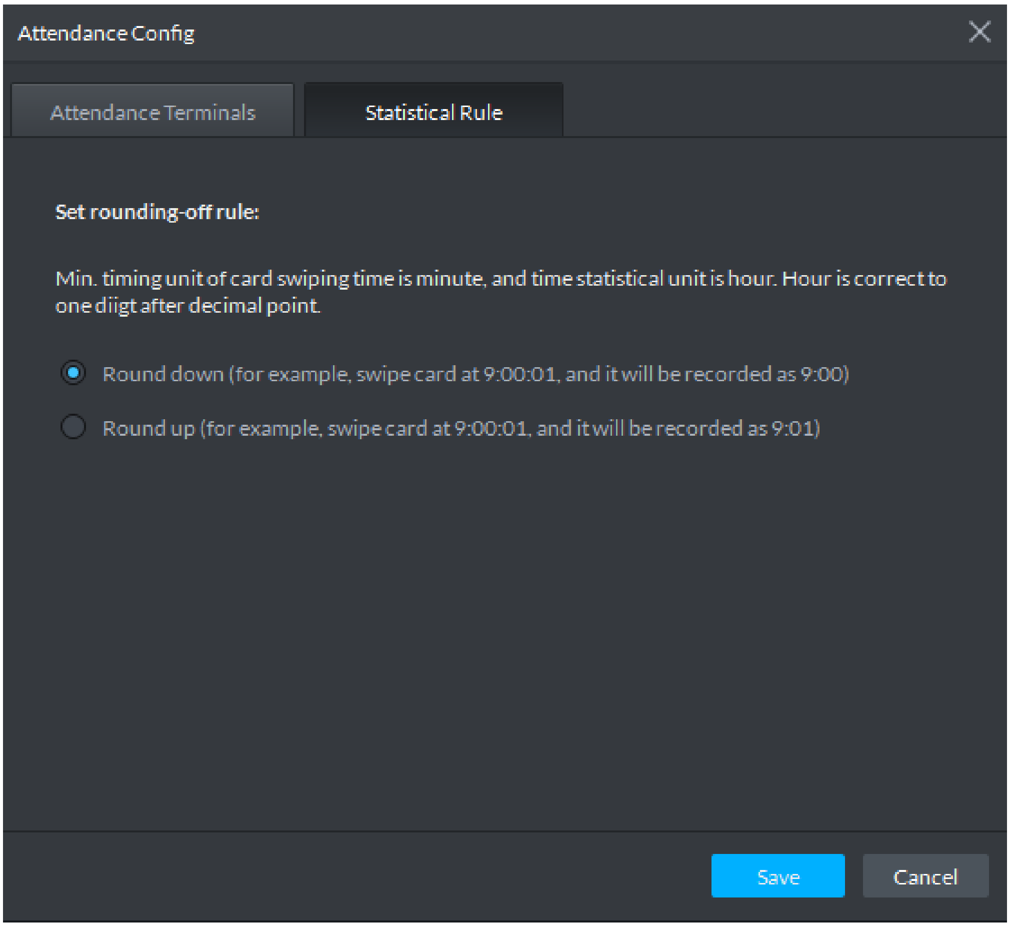
You can find needed device by search function, the system supports fast search.

5.19.3 Setting Statistics Rule

Minimun timing unit of swiping card is minute, the satistics rule of dealing with second is round up and round down. For example, swipe card at 09:00:01, if the rule is set as round down, then the time of swiping card is 09:00; if the rule is set as round up, then the time of swiping card is 09:01.

Click ⚙ at the lower left corner on the interface of **Attendance Management**, select **Statistics Rule**. The interface of **Statistical Rule** is displayed. See Figure 5-313

Figure 5-313 Setting statistics rule



Set rounding-off rule:

Min. timing unit of card swiping time is minute, and time statistical unit is hour. Hour is correct to one diigt after decimal point.

● Round down (for example, swipe card at 9:00:01, and it will be recorded as 9:00)

○ Round up (for example, swipe card at 9:00:01, and it will be recorded as 9:01)

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

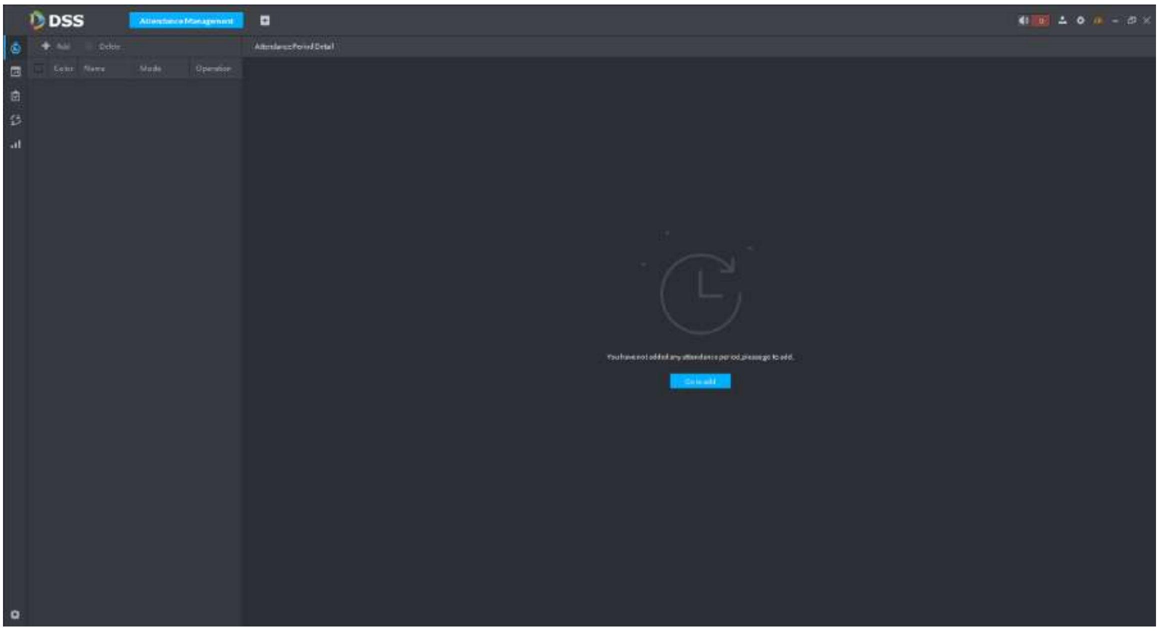
5.19.4 Setting Attendance Period

Set attendance period, which can be used as time evidence to judge if people attend, late or leave early.

Step 1 Click ⏱ on the interface of **Attendance Management**.

The interface of **Attendance Management** is displayed. See Figure 5-314.

Figure 5-314



You have not added any attendance period, please go to add.

Go to add

Step 2 Click on top left corner of the interface.

The new attendance period interface is displayed.

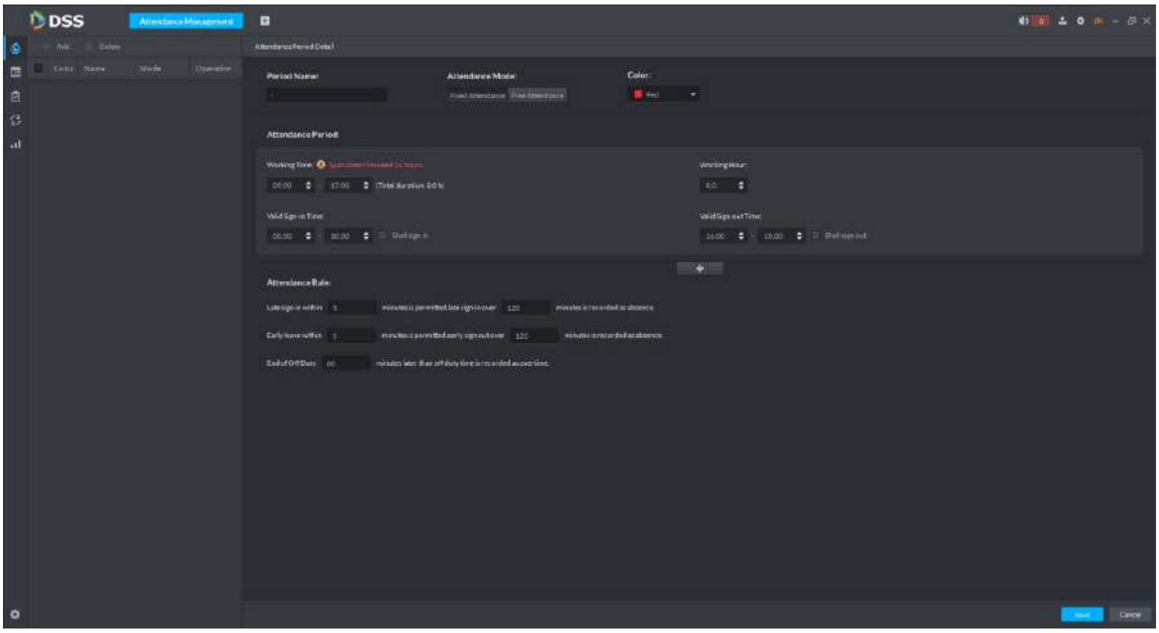
Step 3 Set parameters of attendance period.

The priority of rules set by platform is higher than that of the device itself.

There are two types of attendance according to different attendance mode and different config.

Fixed attendance requires you to sign in and sign out within the designated period. For config details, see Figure 5-315 and Figure 5-316. For parameter details, see Table 5-47.

Figure 5-315 Attendance period(1)



Period Name:

Attendance Mode: Fixed Attendance Free Attendance

Color: 🟥 Red

Attendance Period

Working Time: 00:00 - 17:00 (Total duration: 8.0 h)

Working Hour: 8.0

Valid Sign-in Time: 00:00 - 10:00 □ Shall sign in

Valid Sign-out Time: 16:00 - 18:00 □ Shall sign out

Attendance Rule:

Late sign in within 5 minutes is permitted, late sign in over 120 minutes is recorded as absence.

Early leave within 5 minutes is permitted, early sign out over 120 minutes is recorded as absence.

End of Off Duty 60 minutes later than off duty time is recorded as overtime.

Figure 5-316 Attendance period(2)

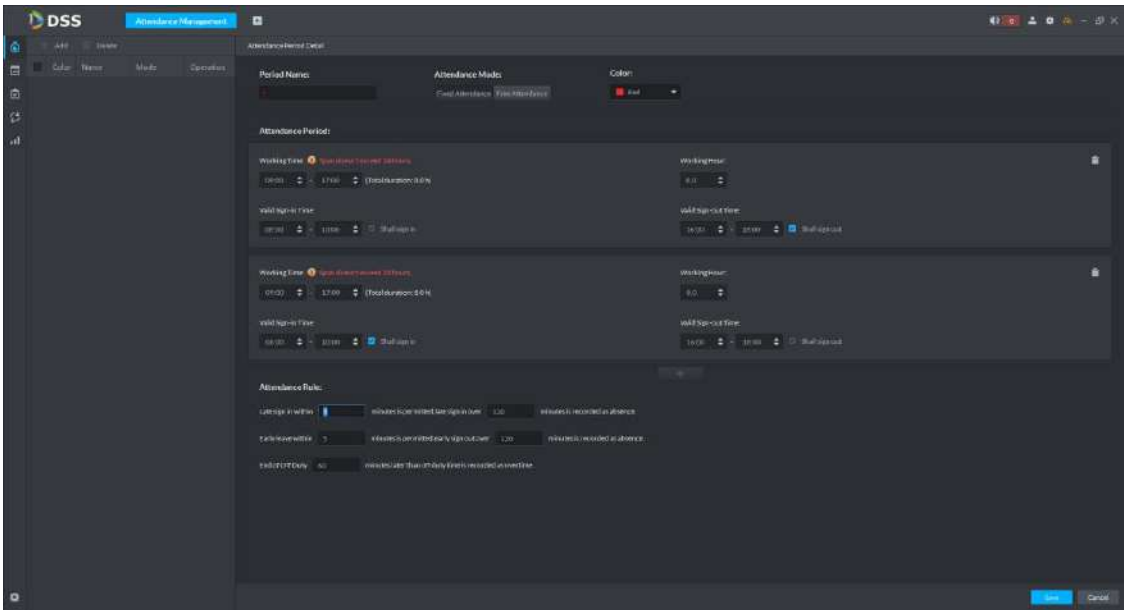


Table 5-47 Fixed attendance description

Parameter	Description
Period name	Custom period name, used to recognize period, such as early shift and night shift.
Color	Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly recognize shift information.
Attendance mode	Set as **Fixed Attendance**.
Working time	Set corresponding working hour of period. Attendance time supports cross-day, but not exceeds 24 hours. One attendance period supports max two types of attendance time. 📖 ● If attendance time needs to be split into twice, such as morning and afternoon, then it needs to click ➕, set second working time and sign-in sign-out period. ● If you set two types of attendance time, then it needs to sign in and sign out accoriding to the configured attendance time, which can be considered as normal attendance.
Working hour	Please fill in according to actual situation.
Valid sign-in time	If working time is set from 09:00-18:00, then valid sign-in time can be set as 08:00-10:00, valid sign-out time can be set as 16:00-18:00. Config rules are as follows: ● The start time of valid sign-in time is earlier than or equal to start working time (09:00), the end time of valid sign-in time should be later than start working time (09:00), earlier than start time of valid sign-out time. If there are several sign-in records within valid sign-in time, then the earliest record is
Valid sign-out time	

Parameter	Description
	considered as sign-in time. ● The start time of valid sign-out time is later than the end time of valid sign-in time, earlier than end working time (18:00), the end sing-in time of valid sign-out time is later than or equal to end working time (18:00). If there are several sign-out records within valid sign-out time, then the earliest record is considered as sign-out time.
Shall sign in	If you set two working time, then the second working time can cancel sign in, you don’t have to sign in when you work at the second working time, and the start time of working time can be used as sign-in time.
Shall sign out	If you set two working time, then the first working time can cancel sign in, you don’t have to sign out when you finish work at the second working time, and the end time of working time can be used as sign-out time.
Work sign-in over _minutes recorded as late	Define the rules of late, absence and early leave. Suppose set **Work sign-in over__minutes recorded as late** as 5 minutes; **Late sign-in over _minutes recorded as absence** is set as 60 minutes**; Off duty _ minutes in advance recorded as early leave** is set as 10 minutes; **Early leave exceeds_ minutes recorded as absebce** is set as 30 minutes. Details are as follows. ● Late When work sign-in is later than start time of working time, and 5 minutes< period ≤60 minutes, then it is recorded as late. ● Early leave When off duty sign-out time is earlier than end time of working time, and 10 minutes< period ≤30 minutes, then it is recorded as early leave. ● Absence When work sign-in time is later than start time of working time, and period > 60 minutes, then it is recorded as absence. When off duty sign-out time is earlier than end time of working time, and period> 30 minutes, then it is recorded as absence.
Late sign-in over _minutes recorded as absence	
Off duty_ minutes in advance recorded as early leave	
Early leave exceeds_ minutes recorded as absebce	
Off duty sign-out over_minutes recorded as overtime	Define overtime rule. Suppose **Off duty sign-out over__minutes recorded as overtime** is set as 120 minutes, off duty sign-out time is later than end time of working time, and period >120 minutes, then it is recorded as overtime, overtime period is **Period – 120 minutes**.

Free Attendance, you are required to sign in and sign out within the specific period. See Figure 5-317. For parameter details, see Table 5-48.

Figure 5-317 Free attendance

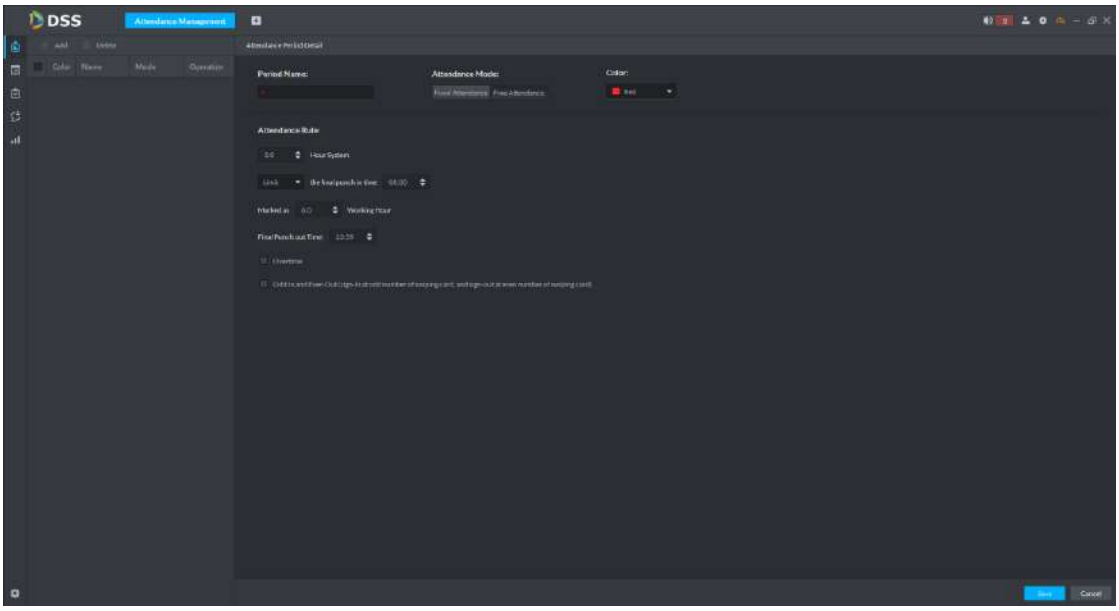


Table 5-48 Free attendance parameter description

Parameter	Description
Period name	Custom period name, used to recognize period, such as flexible attendance.
Attendance mode	Set as **Free Attendance**.
Color	Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly recognize shift information.
Hour system	Set how many hours you have to work a day. For example, if you set 8, then it means you are required to work 8 hours.
Final punch in time	Set if it restricts latest punch in time; sign in after restricted time is recorded as late.
Mark as_working hour	Fill in working hout according to actual situation.
Final punch out time	You are required to sign out before the designated time, otherwise no sign out is recorded.
Overtime	Working over__ hours is recorded as overtime. For example, working hour is 8 hours a day, and if you work overtime for 2.5 hours, then it is recorded as overtime, then you can set 10.5 here.
Work over_hours recorded as overtime	
Odd in even out	Swipe card at odd number is recorded as sign in. For example, the first card swiping is sign in. Swipe card at even number is recorded as sign out. For example, the second card swiping is sign out. It is recorded as twice punch card when the interval of continuous twice card swiping is bigger than the threshold.
Continuous twice card swiping interval≥_minutes	

Step 4 Click **Save** and save period config.

If attendance period is already applied to attendance shift, then before deleting attendance period, first enter the interface of **Attendance Shift**, modify attendance shift, and delete attendance period before removing application of the attendance period.

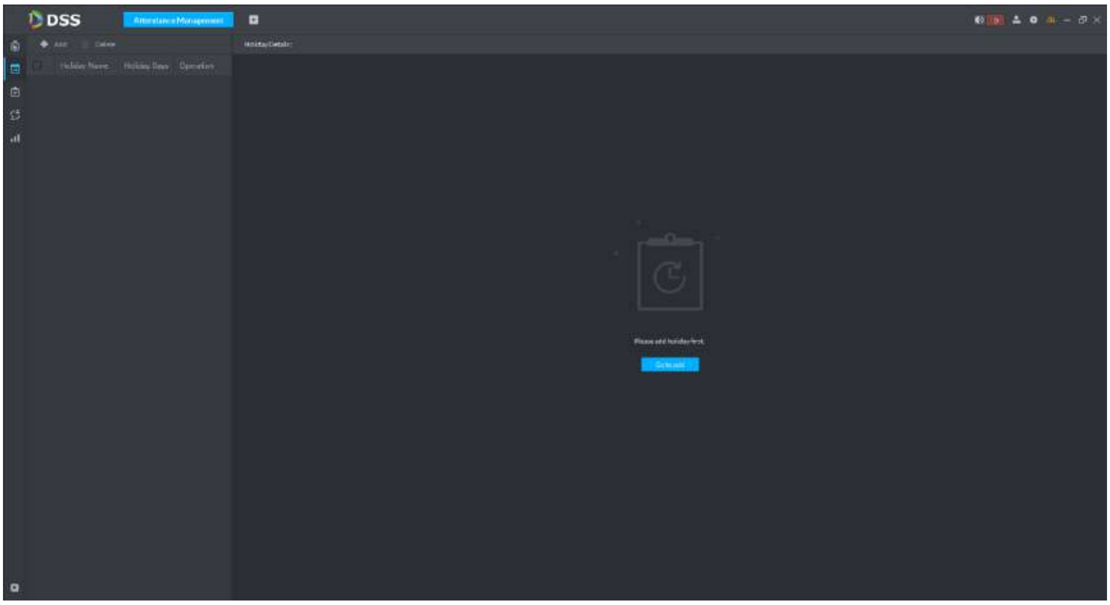
5.19.5 Setting Holiday

Set holiday time, used to judge overtime type during attendance statistics.

Step 1 Click ▦ on the interface of **Attendance Management**.

The interface of **Holiday Management** is displayed. See Figure 5-318.

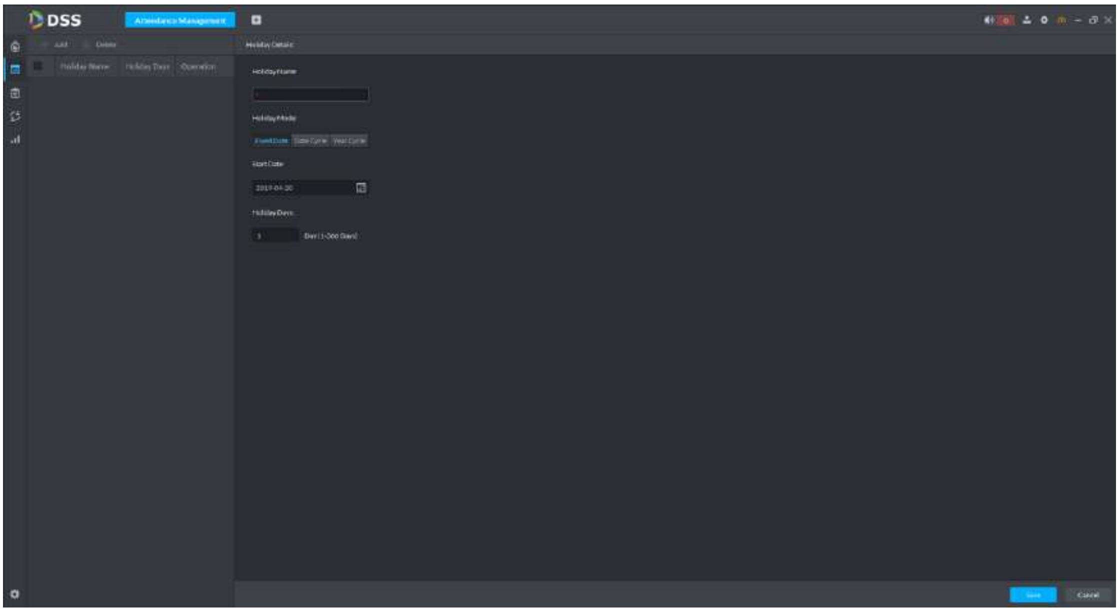
Figure 5-318 Holiday management



Step 2 Click ✚ on the upper left corner of the interface.

The add holiday interface is displayed. See Figure 5-319.

Figure 5-319 Add holiday



Step 3 Set holiday details, three modes available. See Table 5-49 for more parameter details.

Table 5-49 Holiday mode parameter description

Holiday mode	Description
Fixed Date	Set some specific date as holiday. For example, set June 7, 2019 (Dragon Boat Festival) as holiday, and lasts for 1 day, then set **Start Date** as June 7, 2019 and **Holiday Days** as 1.
Date Cycle	If the holiday is the fixed weekday of some week in some specific month, and it cycles according to year, which can be configured as data cycle. For example, if you want to set Mother's Day as holiday, and it lasts for 1 day, then you can set **Start Date** as the second Sunday in May, and **Holiday Days** as 1.
Year Cycle	If the holiday is fixed date and it cycles according to year, which can be configured as year cycle. For example, set New Year's Day as holiday, and it lasts for 1 day, then you can set **Start Date** as January 1 and **Holiday Days** as 1.

Step 4 Click **Save**.

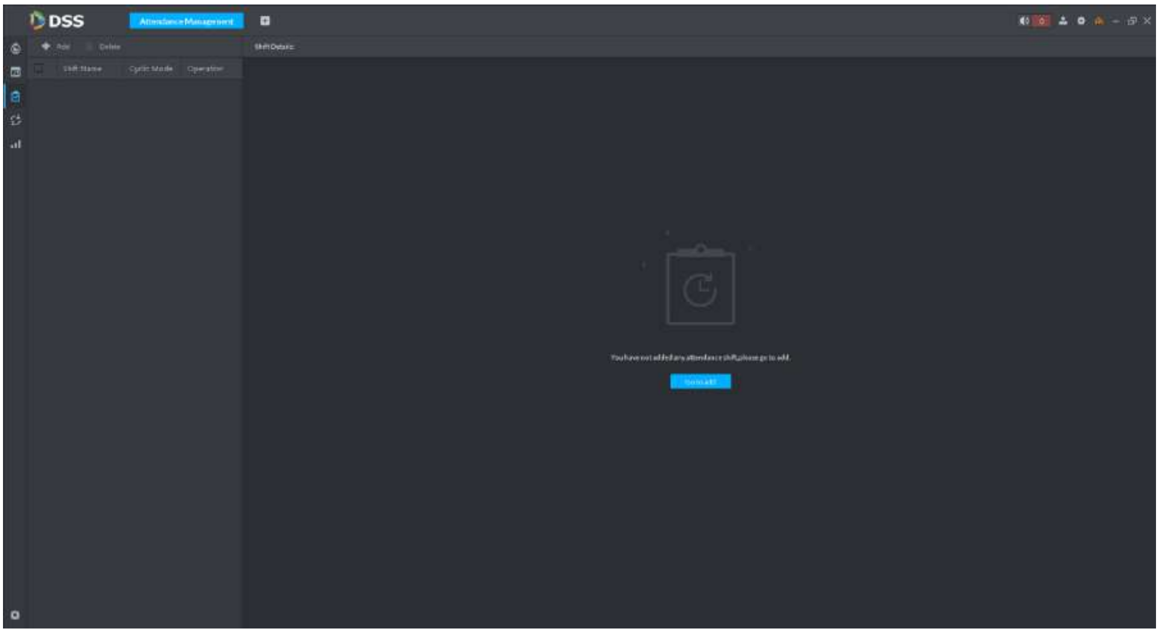
5.19.6 Setting Attendance Shift

Set attendance shift according to attendance period, used for department and personnel shift.

Step 1 Click ☑ on the interface of **Attendance Management**.

The interface of **Attendance Shift** is displayed. See Figure 5-320.

Figure 5-320 Attendance shift

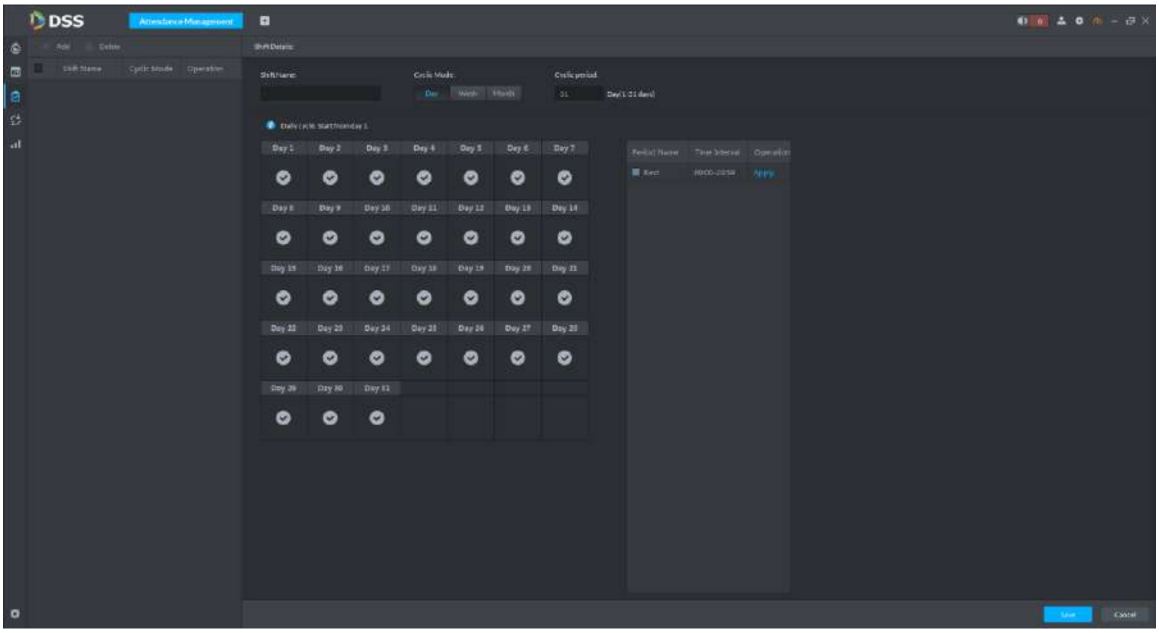


You have not added any attendance shift, please go to add.

Step 2 Click ✚ on the top left corner of the interface.

The add attendance shift interface is displayed. See Figure 5-321.

Figure 5-321 Attendance shift details(1)



Step 3 Set shift details, select date, click Apply and arrange attendance period for date. See Figure 5-322. For parameter details, see Table 5-50.

Figure 5-322 Attendance shift detail(2)

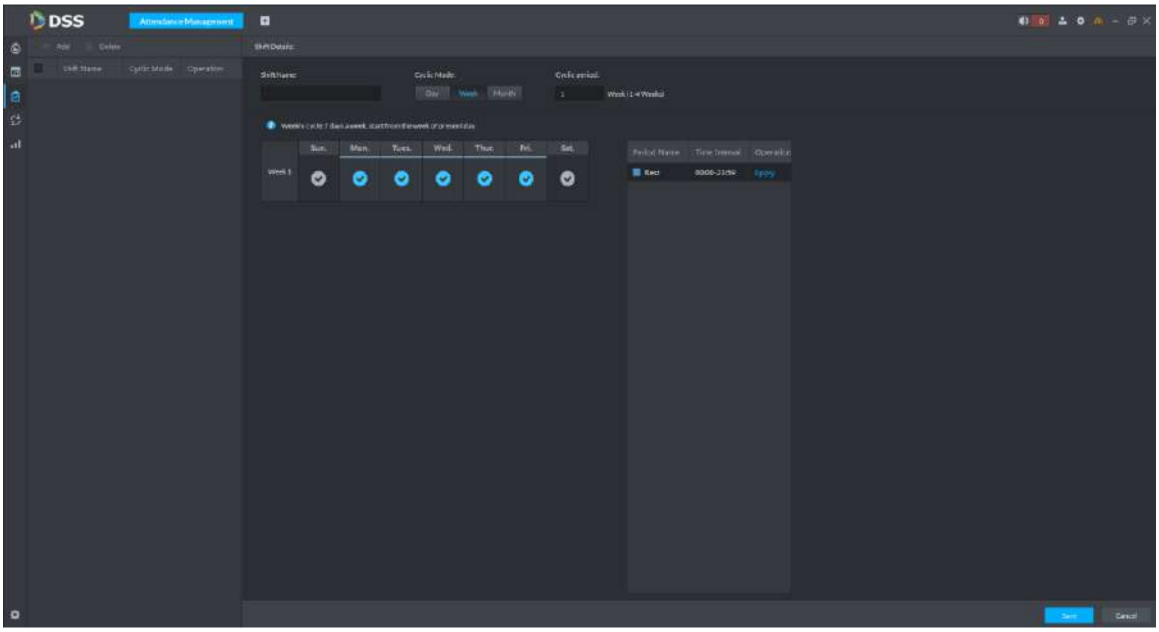


Table 5-50 Attendance shift parameter description

Parameter	Description
Shift name	Custom period name, used to recognize shift.
Cycle mode	Day: Start cycle from the first day, cycle period can be set as any number from 1 to 31 according to day. For example, if you set 2, then the cycle period is 2 days. Week: There are 7 days in a week by default, it starts cycle from

Parameter	Description
Cycle period	Sunday, and so Sunday is required to be set as the first day. Cycle period can be set as any number from 1 to 4. For example, if you set 2, then 2 weeks can be a cycle period. Month: There are 31 days in a month by default, it starts cycle from the current day (If the date does not exist, then it will be deleted during shift arrangement), cycle period can be set as any number from 1 to 3 according to month. For example, if you set 2, then 2 months can be a cycle period.

Step 4 Click **Save** to save shift config.

Delete in-use attendance shift: Enter the interface of **Personnel Shift Arrangement**, check if there are shifts need to be deleted for all personnel shifts, please delete after remove the relation.

5.19.7 Shift Management

Make shifts for personnel or department, meanwhile it makes temporary shift for personnel. The shift priority is temporary shift > holiday > personnel shift > department shift.

5.19.7.1 Personnel/Department Shift Arrangement

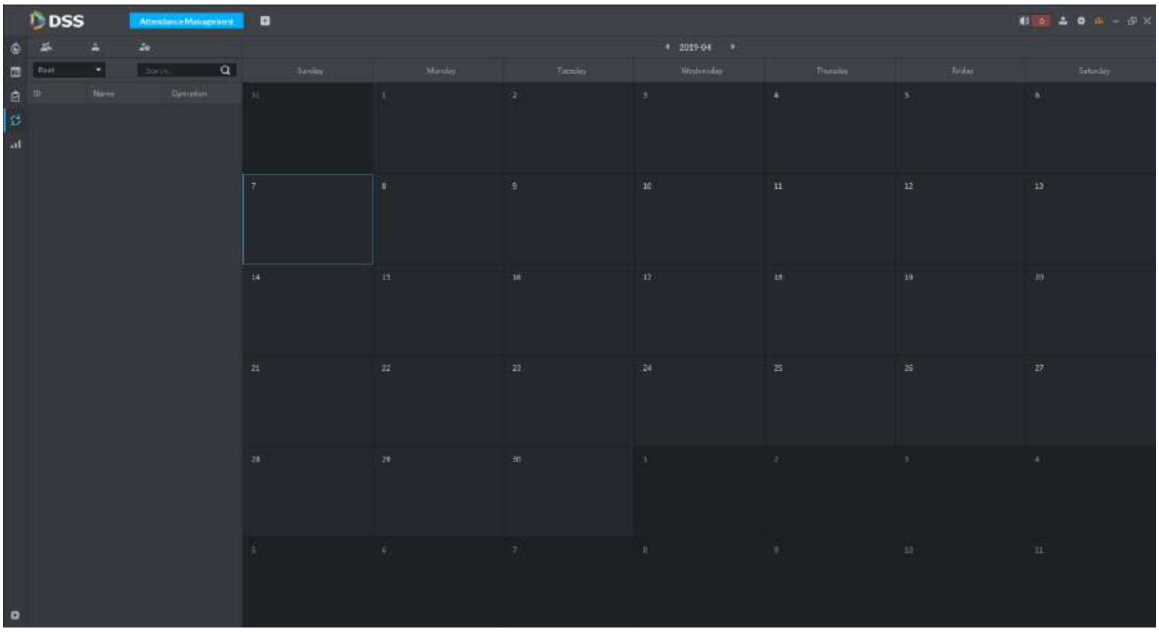
The operations over both personnel shift and department shift are similar, in this chapter; it takes personnel shift as an example to introduce config.

- If you configure department shift, then all the personnel of the department need to conform to the shift.
- If both personnel and department are configured with shift, then the latest personnel shift shall prevail. For example, after configuring the personnel shift, and the corresponding department is configured as well, then personnel shift is based on the latest department shift.
- If the department where new personnel belong is configured with shift, then the shift of new personnel should conform to department shift.

Step 1 Click on the interface of **Attendance Management**.

The interface of **Personnel Shift Arrangement** is displayed. See Figure 5-323

Figure 5-323 Personnel shift management

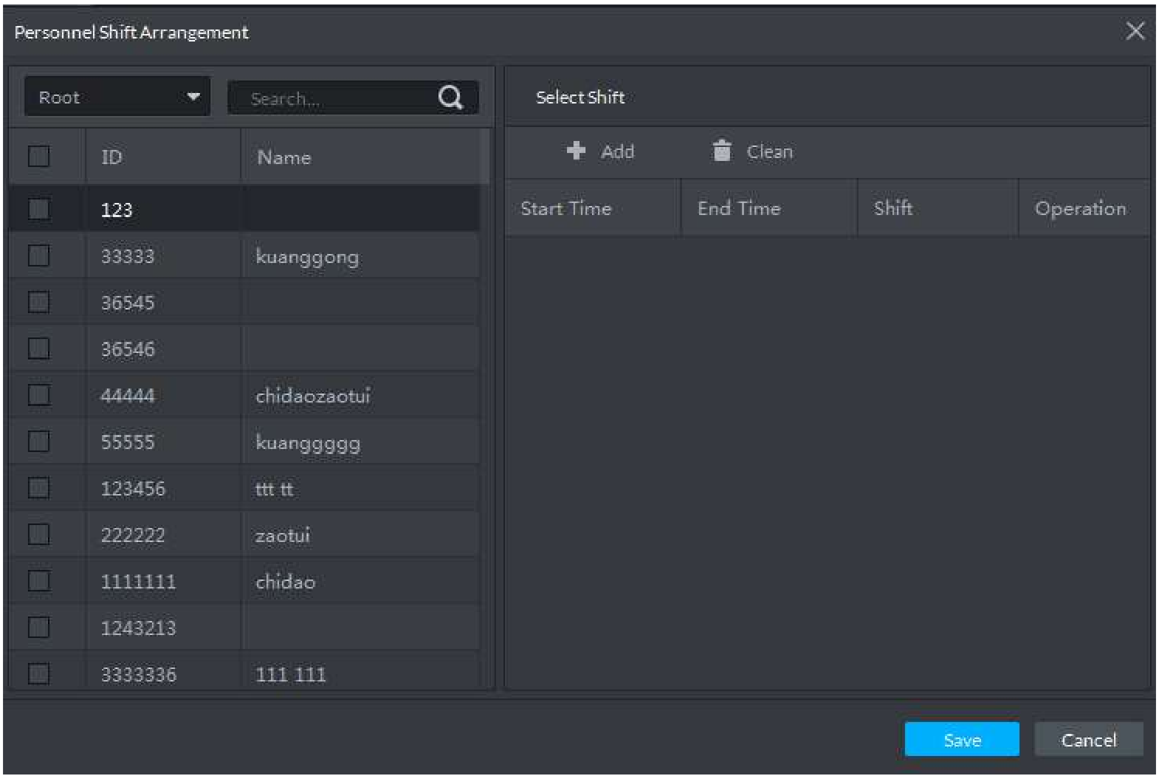


Step 2 Click on the top left corner of the interface.

The interface of **Personnel Shift Arrangement** is displayed. See Figure 5-324.

- If you need to configure shift for department, click on the top left corner and enter the interface of department shift arrangement. The following operation is the same as personnel shift arrangement.
- On the interface of personnel shift arrangement, select personnel and view the shift situation.
- Click next to the personnel and you can view the shift details.

Figure 5-324 Personnel shift

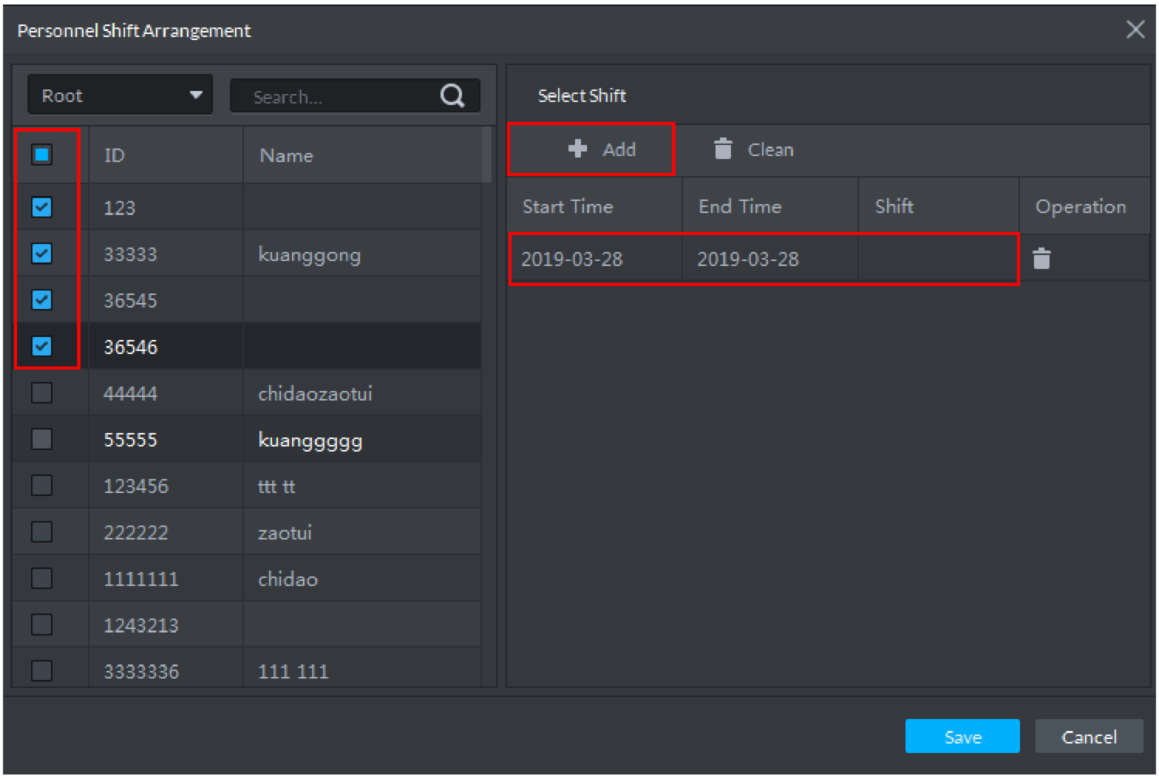


□	ID	Name
□	123	
□	33333	kuanggong
□	36545	
□	36546	
□	44444	chidaozaotui
□	55555	kuanggggg
□	123456	ttt tt
□	222222	zaotui
□	1111111	chidao
□	1243213	
□	3333336	111 111

Start Time	End Time	Shift	Operation

Step 3 Select shift personnel, click ➕ to add shift info. See Figure 5-325. For parameter details, see Table 5-51

Figure 5-325 Select shift



☑	ID	Name
☑	123	
☑	33333	kuanggong
☑	36545	
☑	36546	
□	44444	chidaozaotui
□	55555	kuanggggg
□	123456	ttt tt
□	222222	zaotui
□	1111111	chidao
□	1243213	
□	3333336	111 111

Start Time	End Time	Shift	Operation
2019-03-28	2019-03-28		🗑

Table 5-51 Shift parameter description

Parameter	Description
Start time	Set start date and end date of personnel shift. Click the

Parameter	Description
End time	column of **Start Time** and display calendar, select date and time, and then click **OK** to complete date setting
Shift	Select needed shifts. Shift range means all the attendance shifts set in **5.19.6 Setting Attendance Shift**

Step 4 Click **Save** to save personnel shift information.

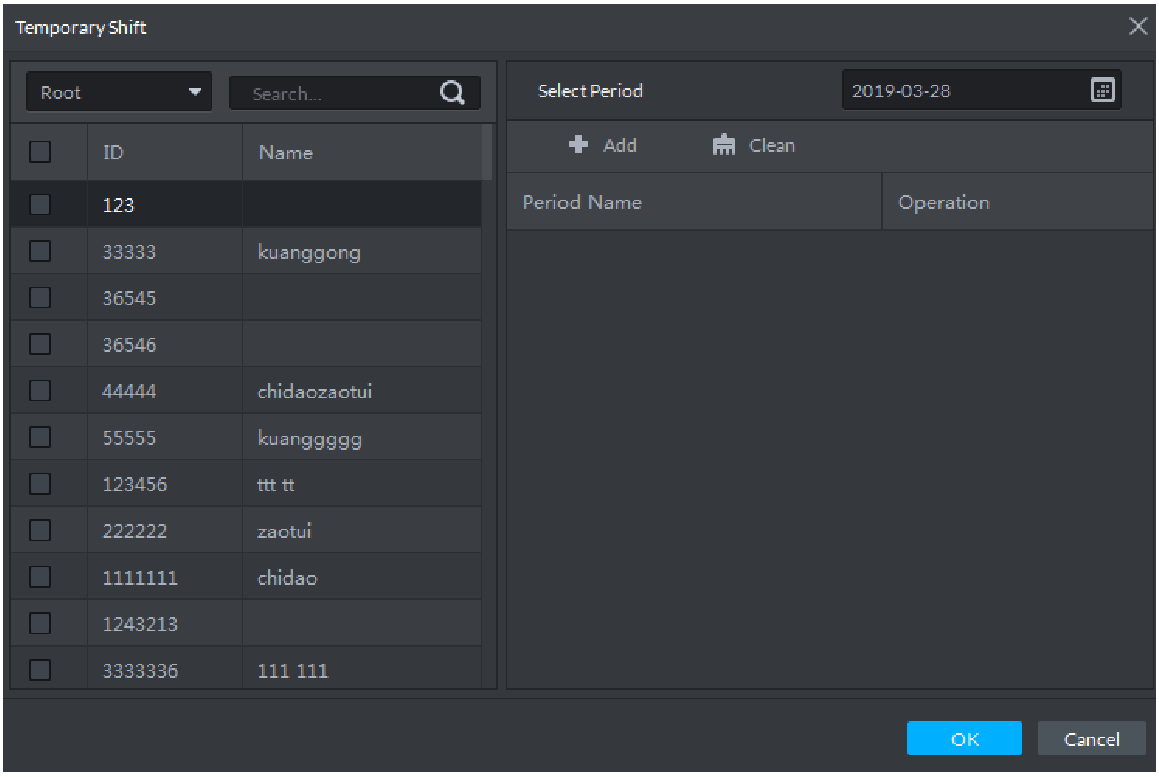
5.19.7.2 Temporary Shift

Temporary shift is needed when work changes temporarily.

Step 1 Click on the interface of Attendance Management or select personnel on the right, double click date on the left.

The interface of Temporary Shift is displayed. See Figure 5-326.

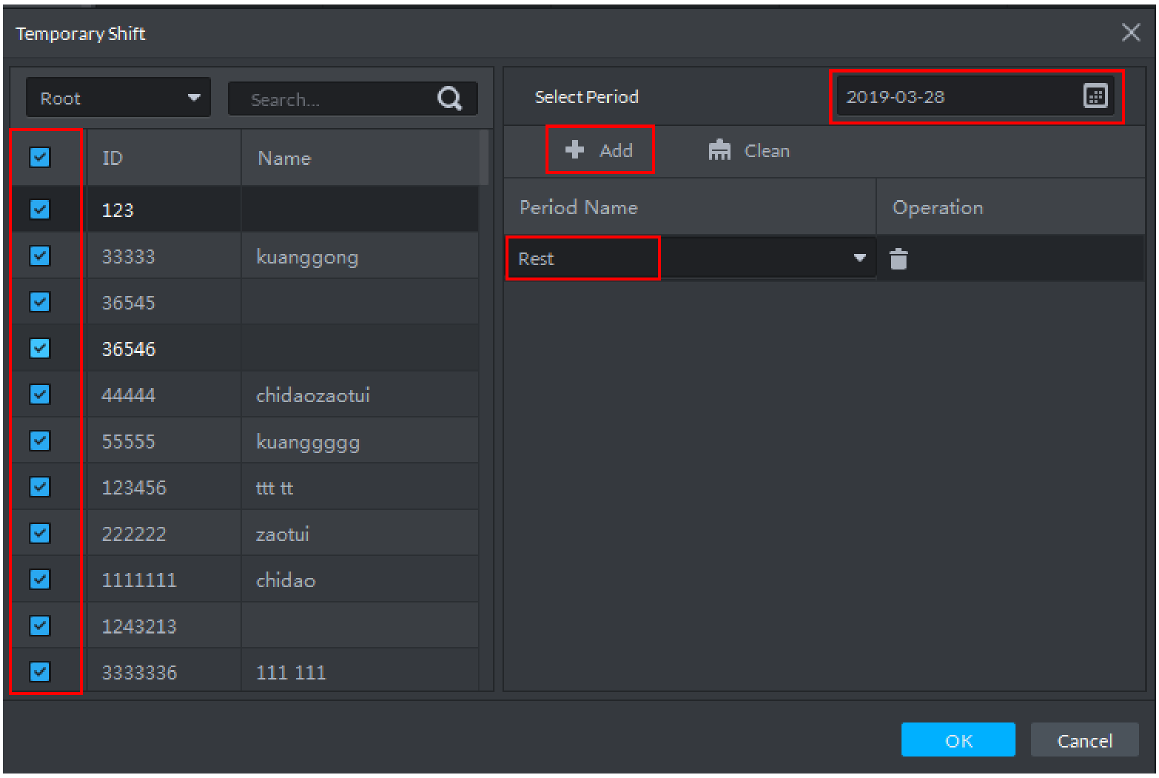
Figure 5-326 Temporary shift



□	ID	Name
□	123	
□	33333	kuanggong
□	36545	
□	36546	
□	44444	chidaozaotui
□	55555	kuanggggg
□	123456	ttt tt
□	222222	zaotui
□	1111111	chidao
□	1243213	
□	3333336	111 111

Step 2 Select personnel and date, click ✚ and select temporary attendance period. See Figure 5-327.You can add max. 2 attendance periods and 1 free attendance period.

Figure 5-327 Temporary shift



Select Period 2019-03-28

☑	ID	Name
☑	123	
☑	33333	kuanggong
☑	36545	
☑	36546	
☑	44444	chidaozaotui
☑	55555	kuanggggg
☑	123456	ttt tt
☑	222222	zaotui
☑	1111111	chidao
☑	1243213	
☑	3333336	111 111

Period Name	Operation
Rest	

Step 3 Click **OK** and save shift information.

Temporary shift can be deleted, right click the date which is configured with temporary shift, and delete temporary shift according to system prompt.

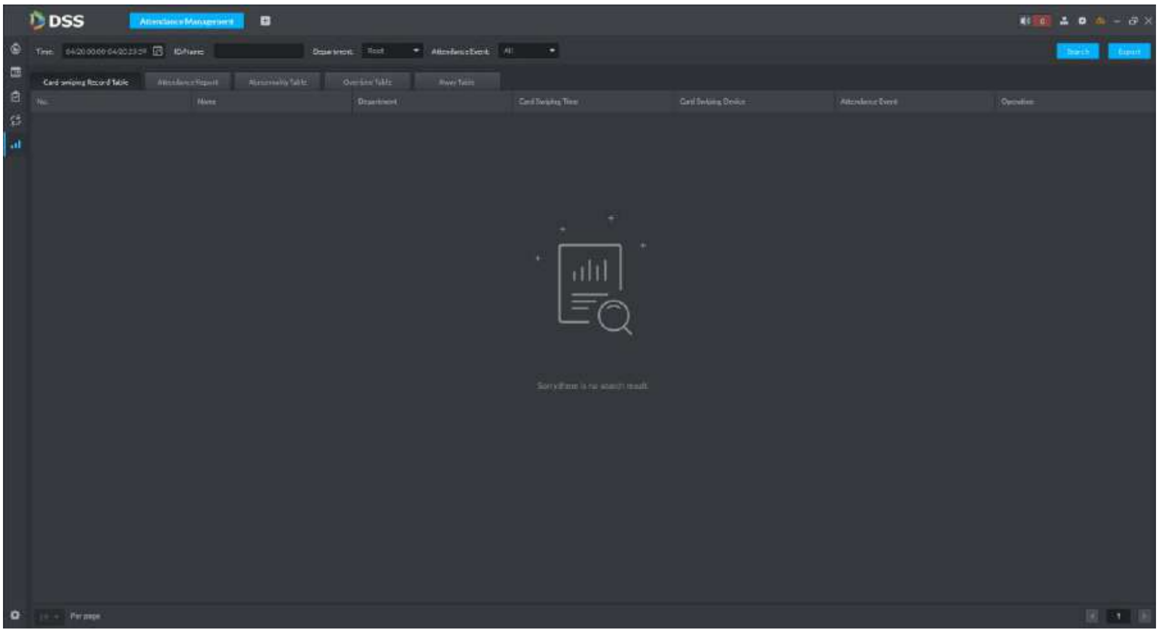
5.19.8 Viewing Attendance Report

View attendance data, displayed in the form of report, including card swiping record table, attendance report, abnormity table, overtime table and away table.

Step 1 Click on the interface of **Attendance Management**.

The interface of **Attendance Report** is displayed. See Figure 5-328.

Figure 5-328 Attendance report



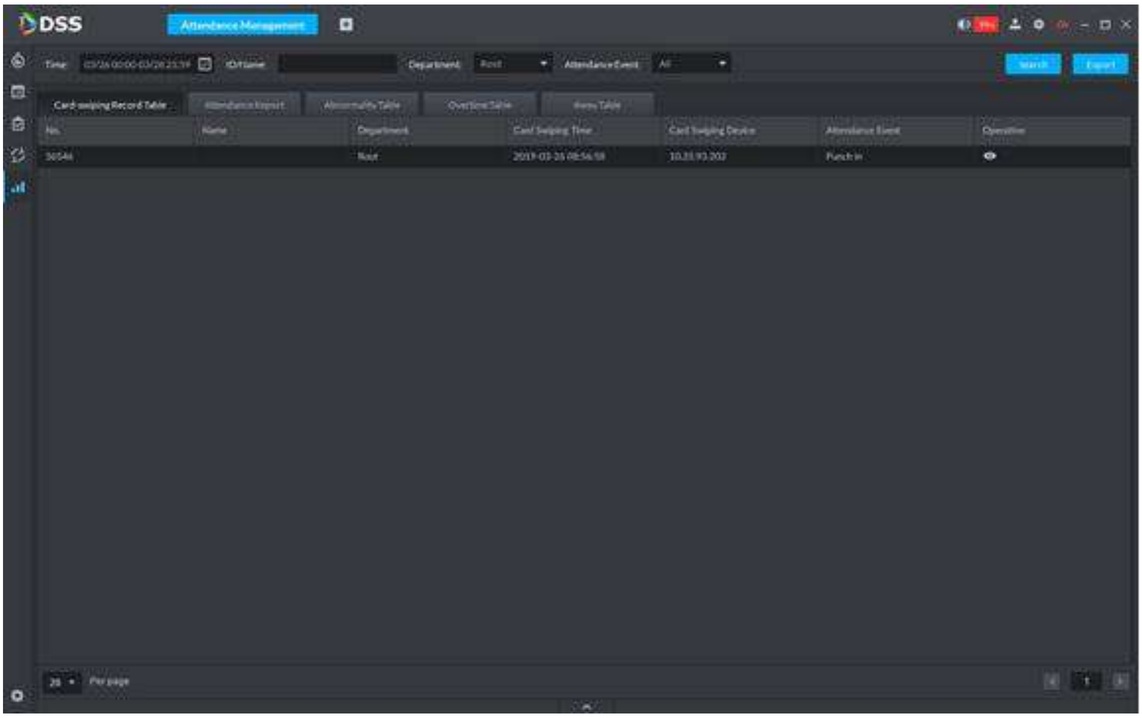
No.	Name	Department	Card Swiping Time	Card Swiping Device	Attendance Event	Operation

<u>Step 2</u> Click corresponding tab, set serach condition, click Search.

The search result is displayed, exported by excel and saved locally, it can export up to 10,000 records.

- Card swiping record table is shown in Figure 5-329. Click 👁 and view more details of the person who swipes card.

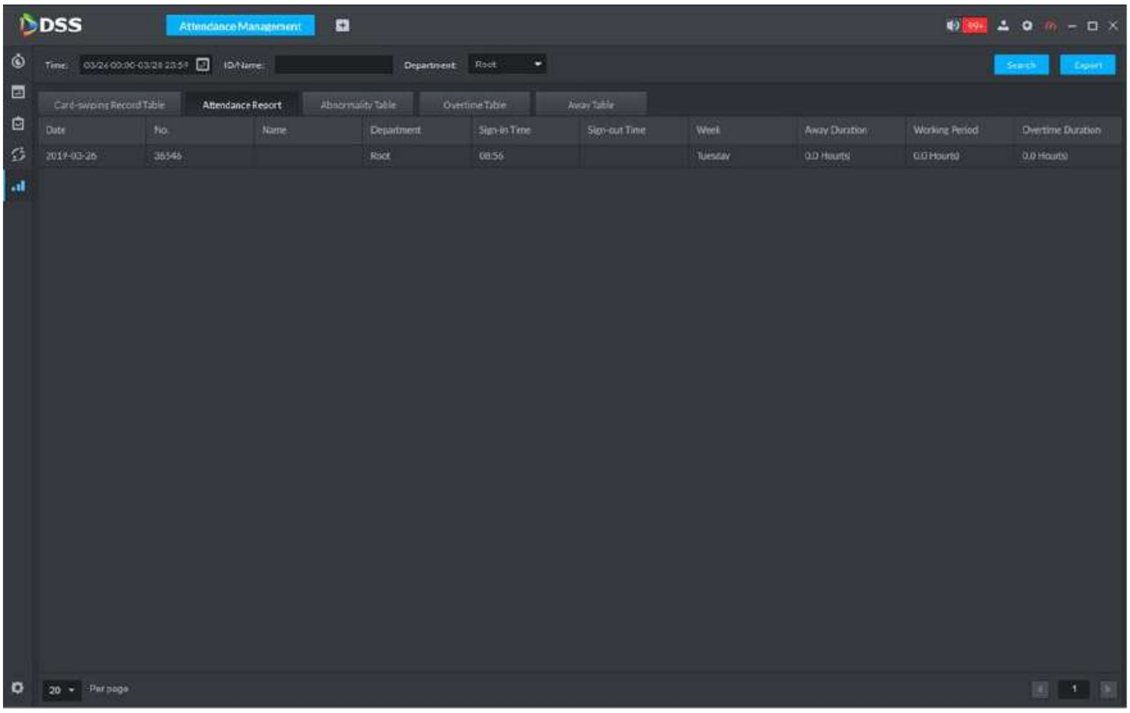
Figure 5-329 Card swiping record



No.	Name	Department	Card Swiping Time	Card Swiping Device	Attendance Event	Operation
36546		Root	2019-03-26 08:56:58	10.33.93.202	Punch in	👁

- See Figure 5-330 for attendance report.

Figure 5-330 Attendance report



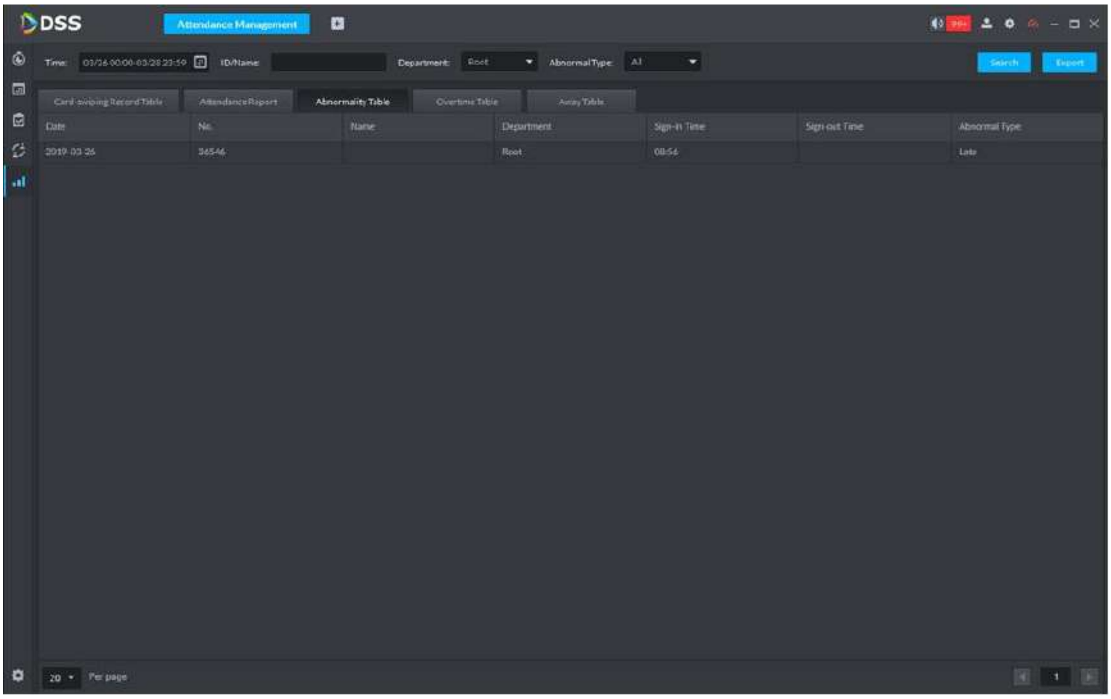
Time: 03/26 00:00-03/28 23:59 ID/Name: Department: Root

Date	No.	Name	Department	Sign-in Time	Sign-out Time	Week	Away Duration	Working Period	Overtime Duration
2019-03-26	36546		Root	08:56		Tuesday	0.0 Hour(s)	0.0 Hour(s)	0.0 Hour(s)

20 Per page

- See Figure 5-331 for abnormality table.

Figure 5-331 Abnormality table



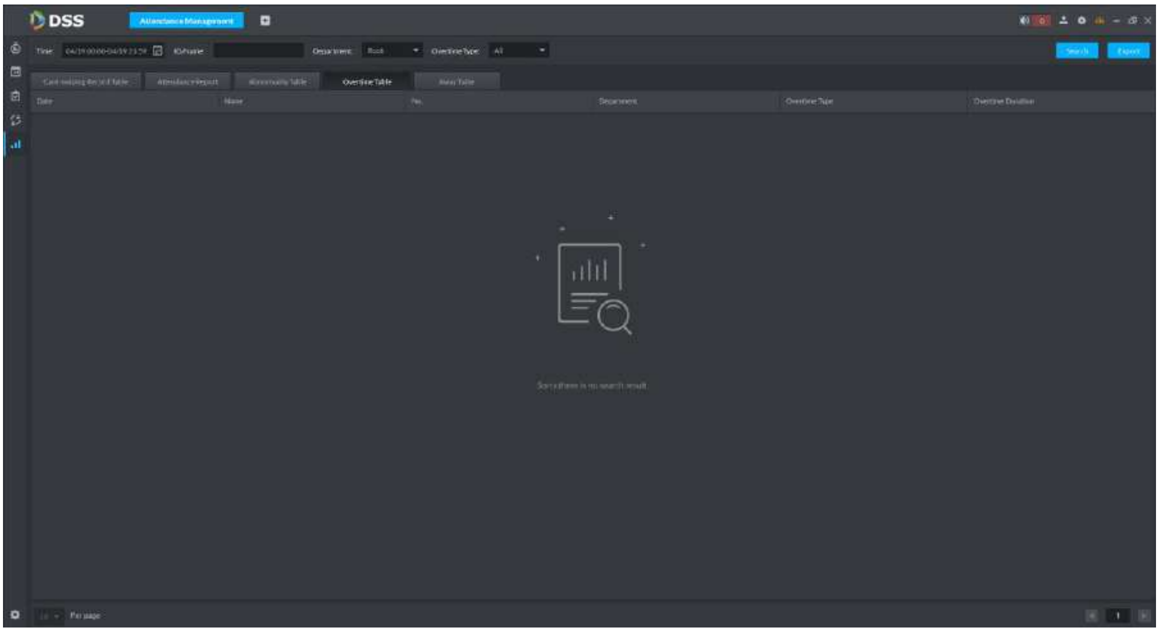
Time: 03/26 00:00-03/28 23:59 ID/Name: Department: Root Abnormal Type: All

Date	No.	Name	Department	Sign-in Time	Sign-out Time	Abnormal Type
2019-03-26	36546		Root	08:56		Late

20 Per page

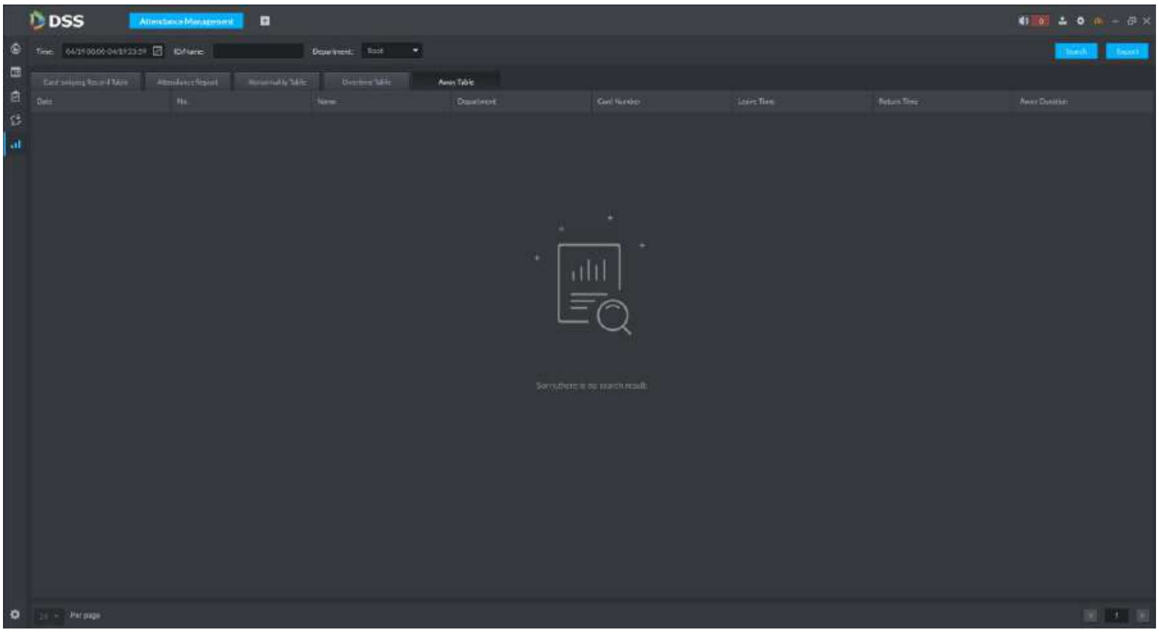
- See Figure 5-332 for overtime table.

Figure 5-332 Overtime table



- See Figure 5-333 for away table.

Figure 5-333 Away table



5.20 Time Synchronization

5.20.1 Device Time Synchronization

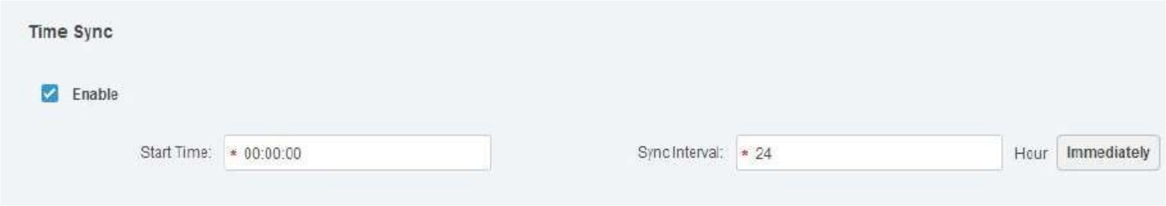
Device time synchronization is to synchronize front-end device time with platform server. The platform server time is the basic time. DSS platform supports devices of Dahua, and ONVIF protocol to synchronize time. It supports auto time synchronization function and manual time synchronization function. 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.

5.20.1.1 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 5-334.

Figure 5-334 Enable time sync



Time Sync

☑ Enable

Start Time: * 00:00:00

Sync Interval: * 24 Hour

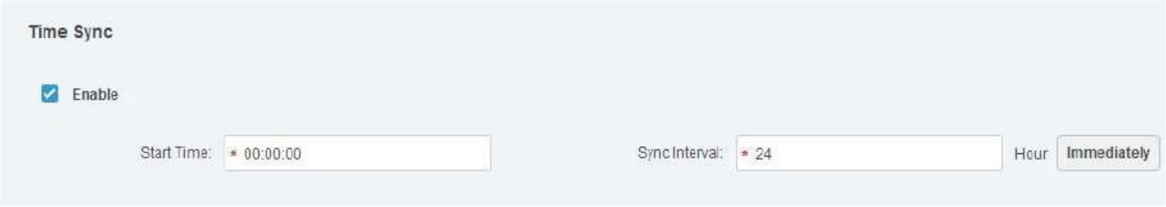
Step 3 Click Save to save configuration information.

5.20.1.2 Manual Sync Time

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

Step 2 Click **Immediately.** See Figure 5-335.

Figure 5-335 Immediately



Time Sync

☑ Enable

Start Time: * 00:00:00

Sync Interval: * 24 Hour

5.20.2 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.

5.20.2.1 Auto Sync Time

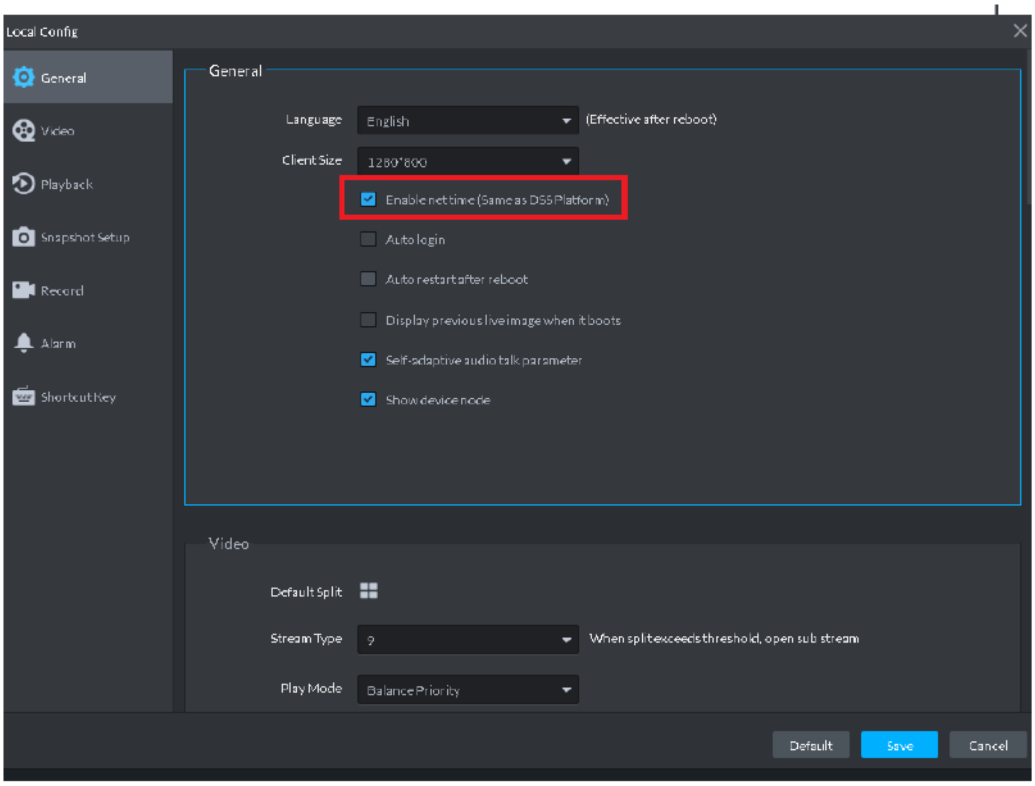
Step 1 Login DSS client.

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 5-336.

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 5-336 Enable net time



General

Language: English (Effective after reboot)

Client Size: 1280*800

☑ Enable net time (Same as DSS Platform)

□ Auto login

□ Auto restart after reboot

□ Display previous live image when it boots

☑ Self-adaptive audio talk parameter

☑ Show device node

Video

Default Split

Stream Type: 9 When split exceeds threshold, open sub stream

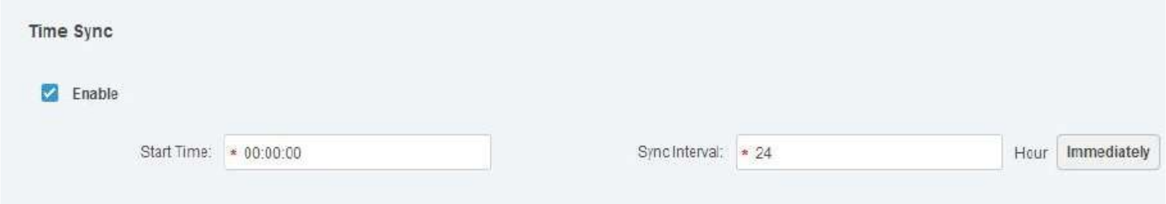
Play Mode: Balance Priority

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 5-337.

Figure 5-337 Enable device time sync



Time Sync

☑ Enable

Start Time: * 00:00:00

Sync Interval: * 24 Hour

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

5.20.2.2 Manual Time Sync

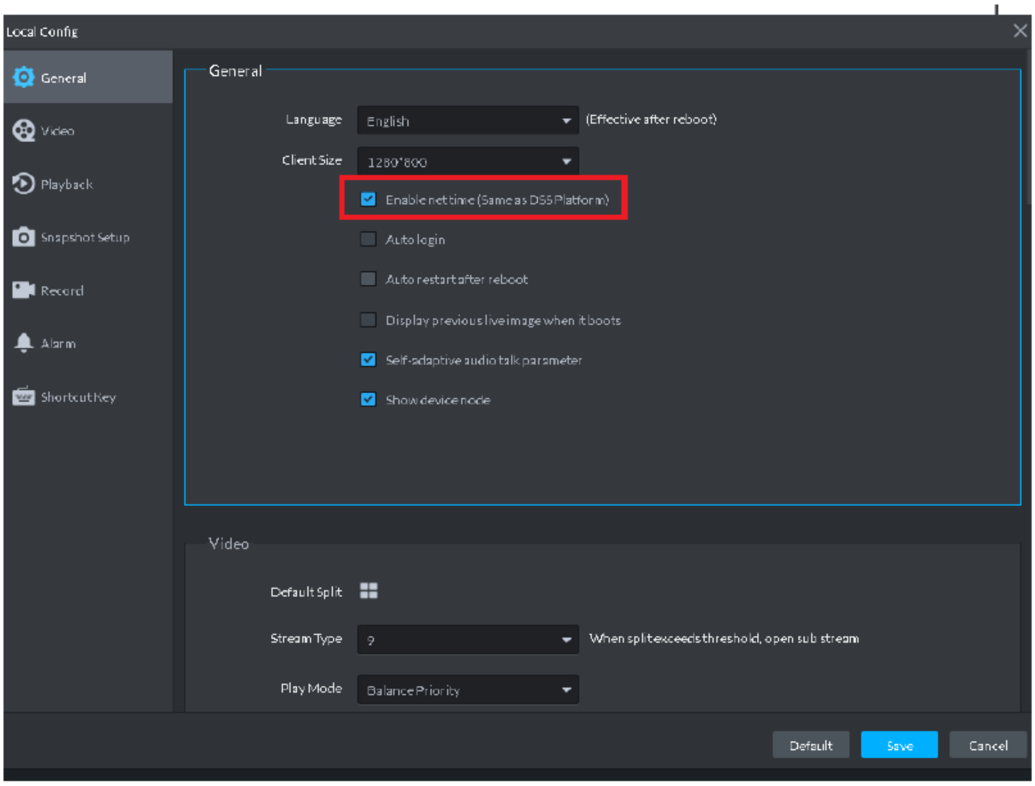
Step 1 Login DSS client.

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 5-338.

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 5-338 Enable client time sync



General

Language: English (Effective after reboot)

Client Size: 1280*800

☑ Enable net time (Same as DSS Platform)

□ Auto login

□ Auto restart after reboot

□ Display previous live image when it boots

☑ Self-adaptive audio talk parameter

☑ Show device node

Video

Default Split

Stream Type: 9 When split exceeds threshold, open sub stream

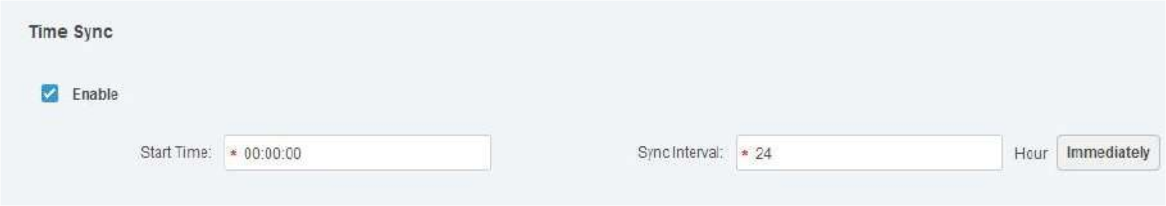
Play Mode: Balance Priority

Step 4 Click **Save**.

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

Step 6 Click **Immediately**. See Figure 5-339.

Figure 5-339 Immediately



Time Sync

☑ Enable

Start Time: * 00:00:00

Sync Interval: * 24 Hour

6 Update

Platform software version updates continuously, and it can improve product performance and extend more functions. You can update softerware accoding to requirement.

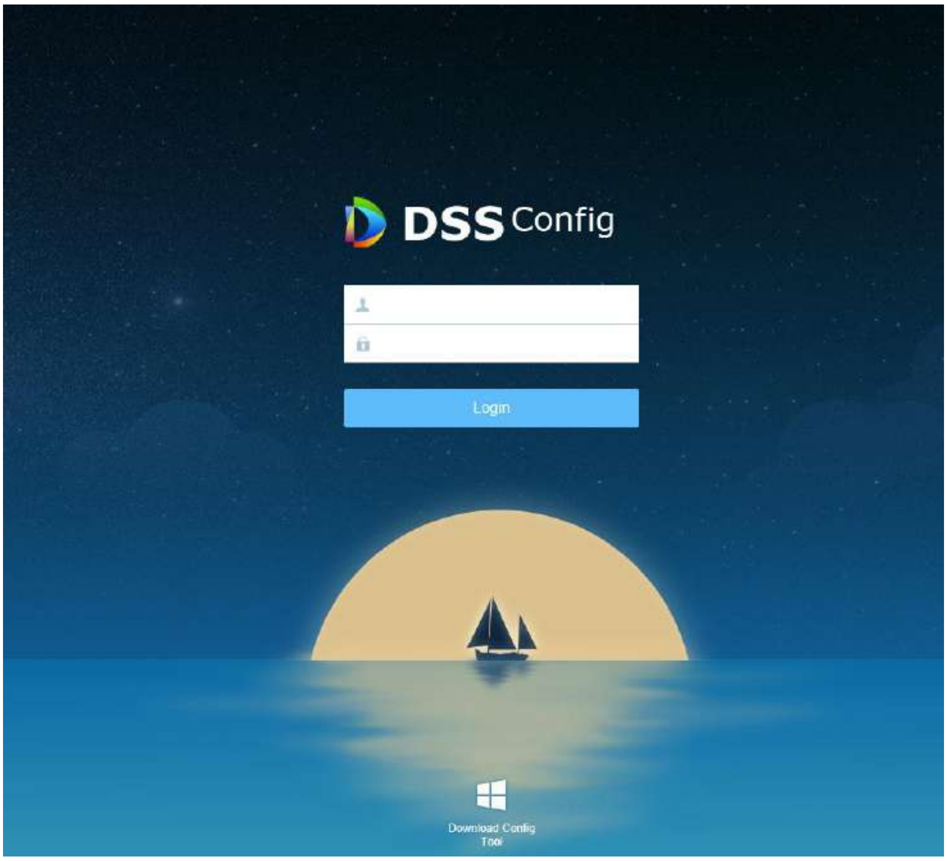
Please contact technical support for software package before update.

Step 1 Download and unzip config tool.

1) Enter **Platform IP address/config** into the browser and press **Enter**.

The system displays config system login interface. See Figure 6-1.

Figure 6-1 Log in config system



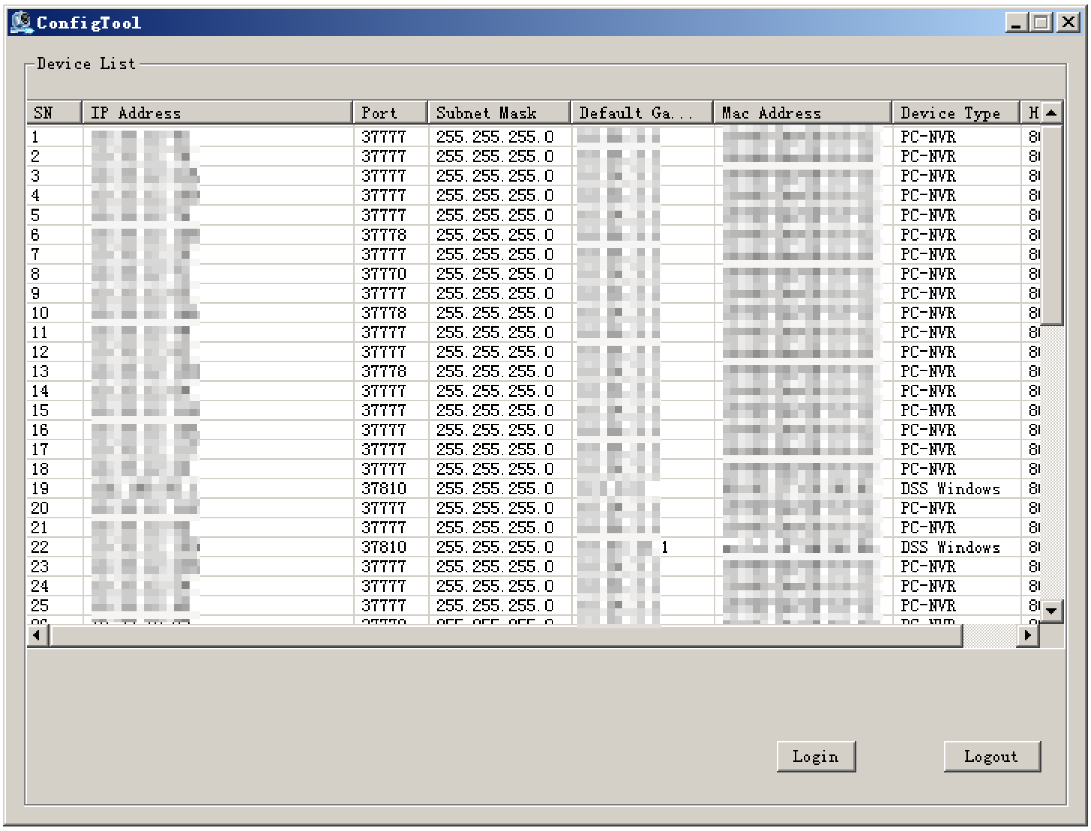
2) Click **Download Config Tool** and save it locally according to prompt.

3) Decompress ConfigTool.zip.

Step 2 Double click ConfigTool.exe.

The config tool login interface is displayed. See Figure 6-2.

Figure 6-2 Log in config system



ConfigTool

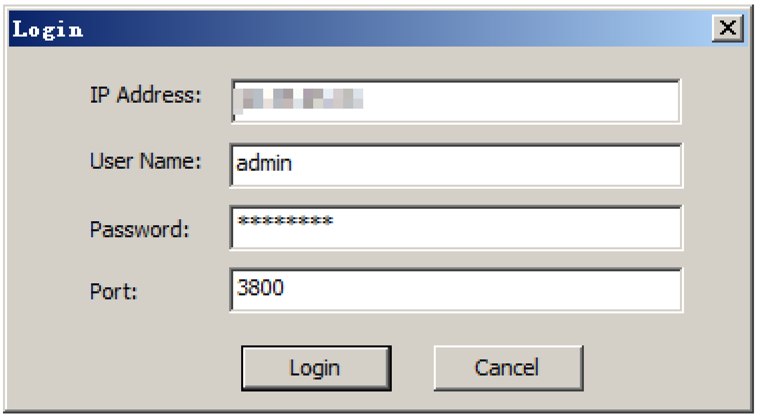
Device List

SN	IP Address	Port	Subnet Mask	Default Ga...	Mac Address	Device Type	H
1	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
2	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
3	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
4	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
5	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
6	[redacted]	37778	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
7	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
8	[redacted]	37770	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
9	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
10	[redacted]	37778	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
11	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
12	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
13	[redacted]	37778	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
14	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
15	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
16	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
17	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
18	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
19	[redacted]	37810	255.255.255.0	[redacted]	[redacted]	DSS Windows	8
20	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
21	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
22	[redacted]	37810	255.255.255.0	[redacted]	[redacted]	DSS Windows	8
23	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
24	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8
25	[redacted]	37777	255.255.255.0	[redacted]	[redacted]	PC-NVR	8

Step 3 Click **Login**.

The ConfigTool login interface is displayed. See Figure 6-3.

Figure 6-3 Config system login



Login

IP Address: [redacted]

User Name: admin

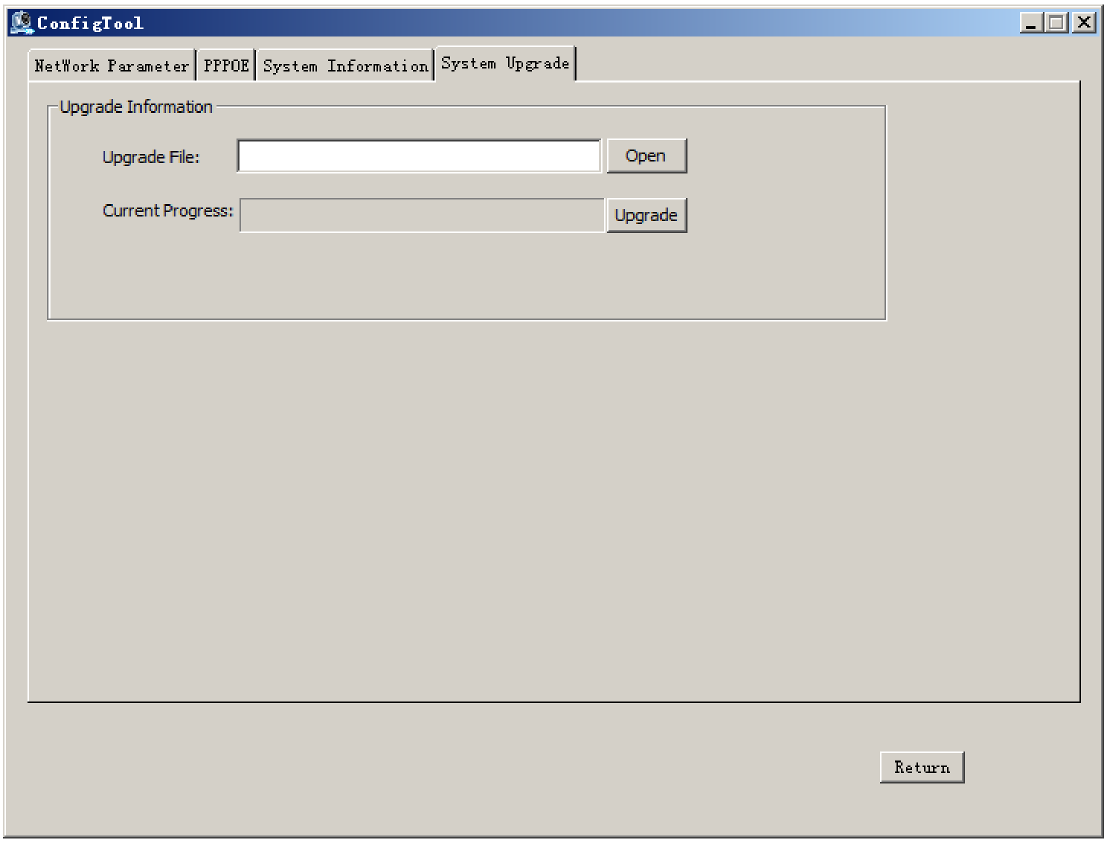
Password: *********

Port: 3800

Step 4 Enter platform IP address, username, password and port, and then click **Login**.

The update interface is displayed. See Figure 6-4.

Figure 6-4 Update



Step 5 Click **Open** and select update file.

Step 6 Click **Upgrade**.

The system displays upgrade progress. The server reboots automatically after upgrade is completed.

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

Appendix 2 RAID Introduction

RAID (Redundant Arrays of Independent Disks), is a type of technology that combines several independent disks (physical disk) according to different way and form a HDD group (logical disk), and then provides higher storage performance than single disk and provides the technology of data redundancy.

The way that forms different RAID is called RAID Level. There are several different RAID levels; each level owns different data protection, data availability and performance.

RAID Level

RAID Level	**Description**	**Min number of disks**
RAID 0	RAID0 consists of striping. Because striping distributes the contents of each file among all HDDs, reads and writes can be done concurrently. Its read and write speed is N times of single HDD (N is the number of disk that consists of RAID0). RAID0 provides no redundancy, and if one HDD fails then all data in the array is lost.	2
RAID 1	RAID1 is also called mirroring. Data is written identically to two HDDs, thus improving the system reliability and performance. Its read throughput approaches the sum of throughputs of every HDD in the set, and the write throughput is limited by the slowest HDD. At the same time, RAID has the lowest disk usage, only 50%.	2
RAID 5	It distributes data and parity information among the HDDs, and parity information and corresponding data are respectively backed up on different HDDs. Upon failure of a single HDD, subsequent data and parity information can be used to reconstruct the failed data to ensure data integrity.	3
RAID 6	A parity information HDD is added on the basis of RAID5. The two independent parity systems use different algorithms for enhanced reliability. No data will be lost when the two HDDs fail. But compared with RAID5, it needs to distribute larger space for parity information, so it performs worse in respect of write.	4
RAID 10	RAID10 is a combination of RAID1 and RAID0. It owns high read and write capabilities of RAID0, as well as high data protection and restorability of RAID1. But its HDD utilization is as low as RAID1.	4

RAID Capacity Calculation

CapacityN refers to the HDD with the minimum capacity in the set. The capacity shall be subject to the value on the web.

RAID Level	Total capacity of N HDDs
RAID 0	Total capacity of the HDDs in the set.
RAID 1	Min (capacityN)
RAID 5	(N-1)×min(capacityN)
RAID 6	(N-2)×min(capacityN)
RAID 10	(N/2)×min(capacityN)
RAID 50	(N-2)×min(capacityN)
RAID 60	(N-4)×min(capacityN)

Appendix 3 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123 and abc;
   - Do not use overlapped characters, such as 111 and aaa;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR and IP camera.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable equipment (such as USB flash disk and serial port).

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The equipment supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer’s IP address and the accompanying equipment’s IP address to the whitelist.

8. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. **Disable Unnecessary Services and Choose Secure Modes**

    If not needed, it is recommended to turn off some services such as SNMP, SMTP and UPnP to reduce risks.

    If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

    - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access mailbox server.
    - FTP: Choose SFTP, and set up strong passwords.
    - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

11. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

12. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. **Network Log**

    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.

- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.