DSS General Surveillance Management Center

User's Manual

V1.0.5

Foreword

General

This manual (hereinafter referred to as the "Manual") introduces the configurations and operations of the DSS general surveillance management center (hereinafter referred to as the "Device" or "System") and client operations.

Model

DSS4004-S2

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.5	Deleted content about hot spare.	August 2021
V1.0.4	Deleted sensitive elements.	November 2020
V1.0.3	Deleted POS, attendance management, visit appointment, and face track.	June 2020
V1.0.2	• Added contents of alarm controller, entrance, smart track and POS. • Optimized attendance management, and access control chapters. • Deleted FTP content.	June 2019

Version	Revision Content	Release Time
V1.0.1	Optimized the chapter of ANPR. Surveillance, added the chapters of Attendance Management and Flow Analysis.	November 2018
V1.0.0	First Release.	August 2018

Privacy Protection Notice

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

About the Manual

- The Manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

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 Product Positioning

This product is designed for medium-small project. It is suitable for single-server deployment of simple, easy and reliable VMS, to provide video surveillance for medium-small projects. It needs to integrate access control and VDP device organizations in order to provide solutions. It is widely used for residence, supermarket, factory, casino and other scenarios.

1.2 Highlights

- GPU decoding, meantime support preview of more HD cameras.
- Vector graph design, perfect support over 4K display.
- Both administrator and operator use the client with powerful control experience.
- Within LAN, auto search device in different network segment and show device list. One-click to add management. Save deployment time effectively.
- Mobile phone APP. Realize access anytime when you are not there.
- Auto and manual backup of database. Quickly recover when system error occurs.
- Lock record, permanent storage of important record footage, without being overwritten.

2 Configuration and Operation

The configuration system is used for system update, system self-check and system parameter configuration including network parameters, basic parameters, and security parameters.

⚠

Make sure you have got the server before configuring it.

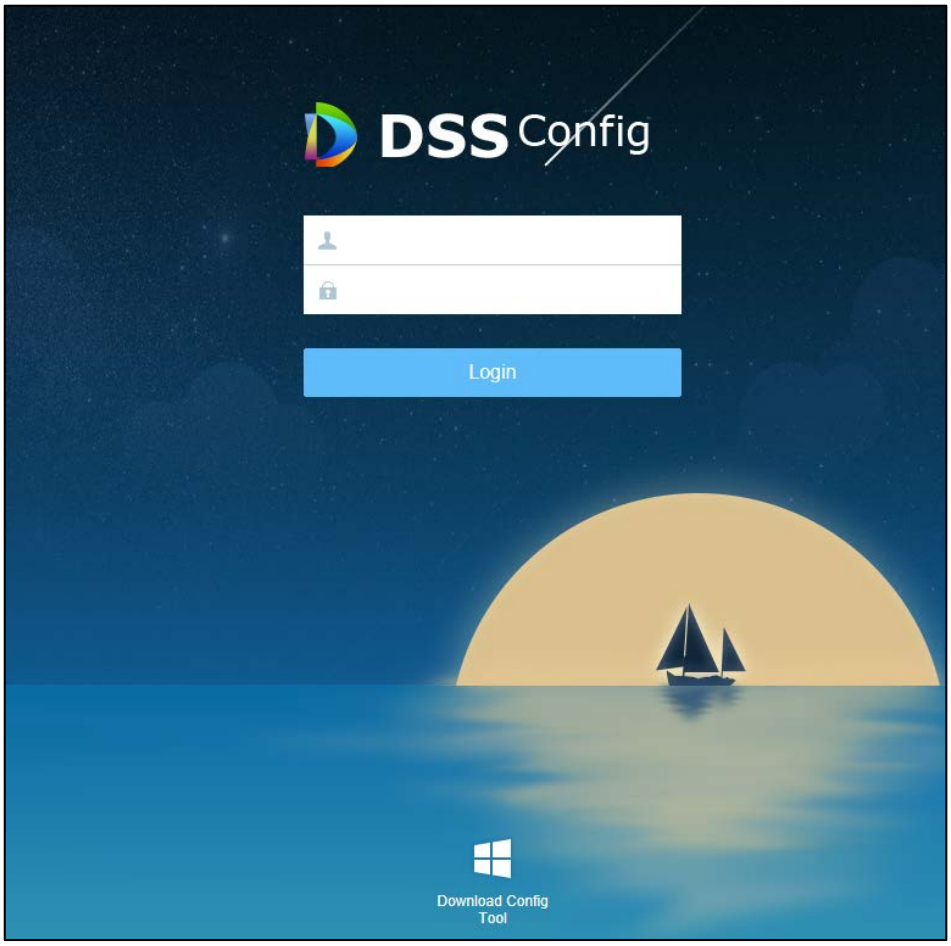
2.1 Login and Initialization

⚠

Make sure your PC is in the network segment with the server. If not, modify PC IP. The default IP of the server is 192.168.1.108.

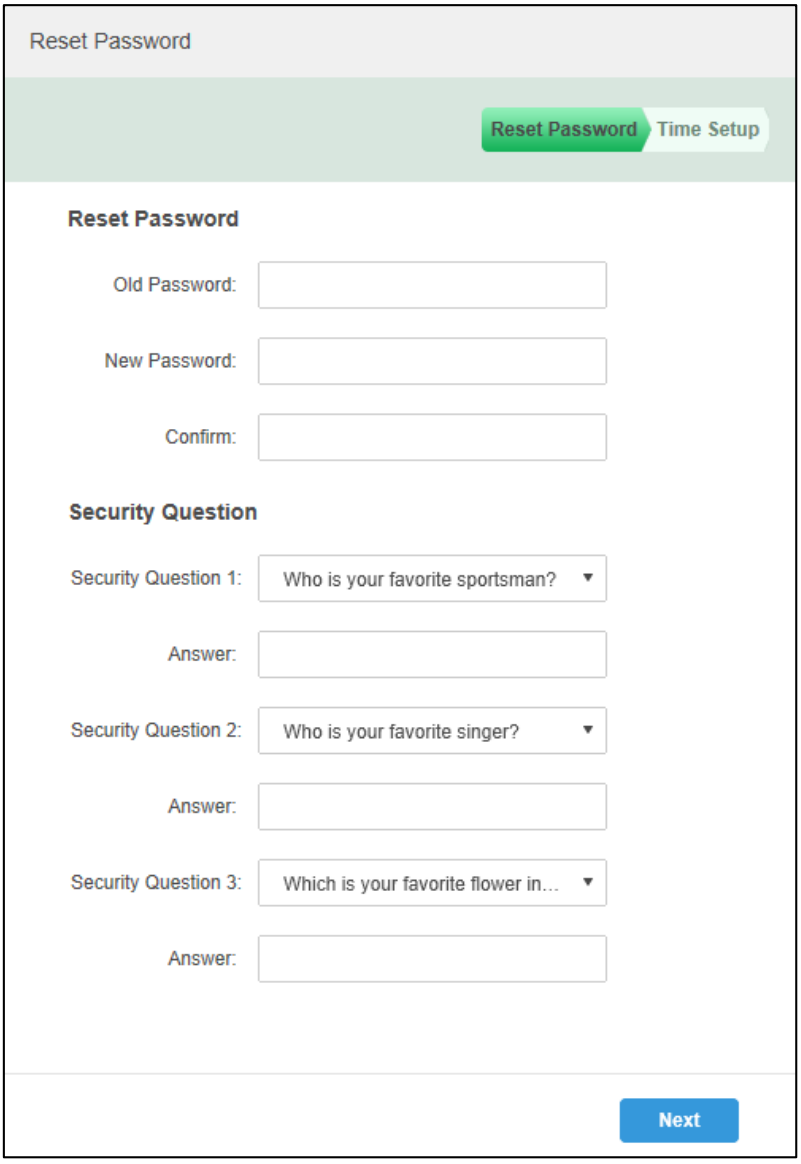
Step 1 Enter "DSS IP address/config" in the browser address bar and press **Enter**.
The system login interface is displayed. See Figure 2-1.

Figure 2-1 Login the system



Step 2 Enter username and password. The default username is admin and password 123456.
The password resetting interface is displayed. See Figure 2-2.

Figure 2-2 Reset password



Step 3 Enter the original password and then the new one, and set three security questions.

Step 4 Click **OK** to finish.

The server reboots. Wait and log in again.

2.2 Quick Guide

The quick guide leads you through network configuration, and port mapping.

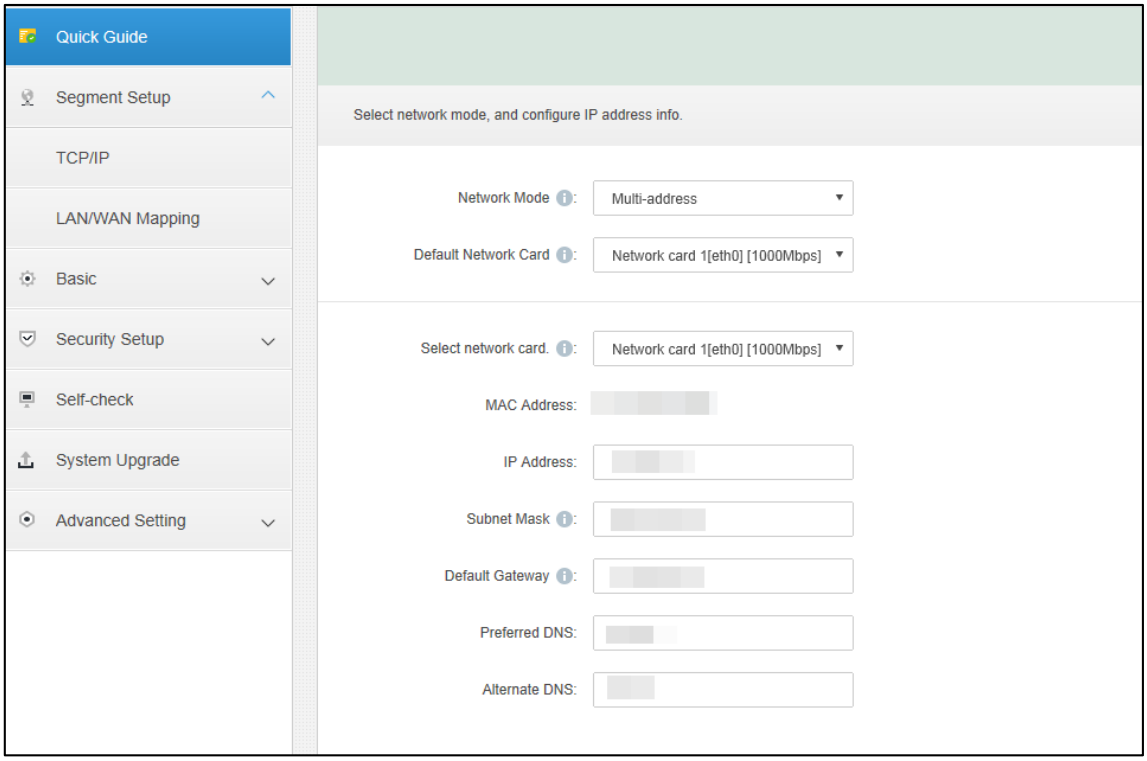
2.2.1 Network Card Config

Select network mode and set IP parameters.

Step 1 Click **Quick Guide** in the homepage.

The network card config interface is displayed. See Figure 2-3.

Figure 2-3 Network card config



Step 2 Configure network card parameters. See Table 2-1.

Table 2-1 Network card parameters

Parameter	Description
Network Mode	● Multi-address Multiple network card (hereinafter referred to as NIC) mode. You can configure different network segments for multiple NICs. This mode is suitable for scenarios that require high network reliability. For example, it can be used in ISCSI storage expansion solution. When setting ISCSI storage expansion, NIC 1 can be used for communication, NIC 2 is reserved and NIC 3 and NIC 4 can be used for ISCSI storage. ● Fault-tolerant Multiple NICs share one IP. Normally, one of them works. When the working NIC is fails, another one will automatically take over job to ensure network stability. ● Load Balancing Multiple NICs share one IP and work at the same time to share the network load, providing greater network capacity than the single NIC mode. When one of them fails, the network load will be re-distributed among the rest NICs to ensure network stability. ● Link Aggregation Bind NIC for network communication. All bound NICs work at the same time and share network load. For example, bind two NICs and set multi-address for the other two NICS. Then the server has three IPs. The bandwidth of the two bound NICs is 2K and the other two are 2K respectively. This is applicable to stream forwarding, not storage.
Add Network Card	When the network mode is fault tolerance, load balance or link aggregation,

Parameter	Description
	you need to add network card. Select NIC to bind. You can bind 2 NICs as needed.
Default Network Card	Select default NIC. This NIC will be used as a default NIC to forward data package between non-consecutive network segments such as WAN or public network.
Select Network Card	After NIC is selected or added, its information will be displayed.
MAC Address	Displays the MAC address of the server.
IP Address	After selecting NIC, you can set its IP address, subnet mask, default gateway and DNS server address.
Subnet Mask	
Default Gateway	
Preferred DNS	
Alternate DNS	

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

Click **Skip** to enter the LAN/WAN mapping interface without saving configuration.

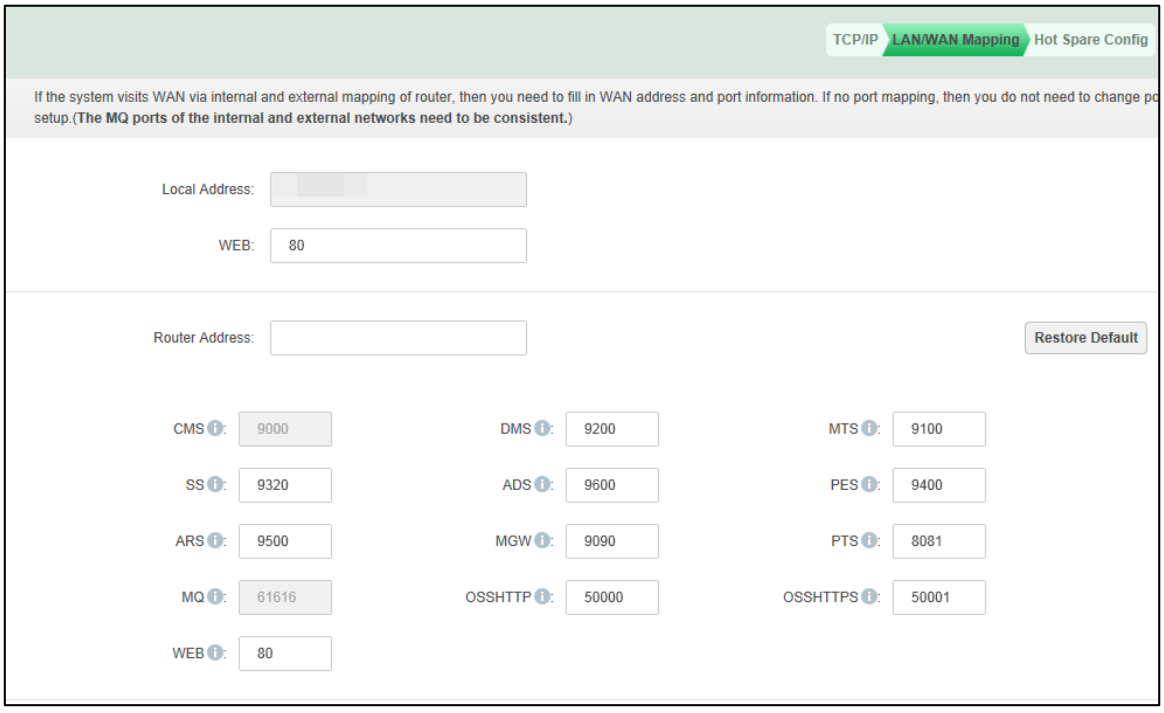
2.2.2 LAN/WAN Mapping

Realize communication with public network by port mapping.

Step 1 Click **Quick Guide** and then click **Skip**.

The interface of **LAN/WAN Mapping** is displayed. See Figure 2-4.

Figure 2-4 LAN/WAN Mapping



Step 2 Set WAN address and port info. See Table 2-2.

Table 2-2 Parameters

Parameter	Description
IP Address	Set DSS platform IP address.

Parameter	Description
Web Service Port	Web service port is 80 by default. If not, you need to visit Web by inputting IP: Port in the browser's address bar. For example, if the port is 81, enter http://192.168.1.35:81/config to visit the config system.
Router Address	Set WAN IP for router.
CMS	Central management service. It manages server registration and signal dispatching. The port is 9010 by default.
SS	Storage service. It manages recording storage, video search and playback. The port is 9320 by default.
ARS	Active registration service. It is responsible for listening and login of active registration device and getting and forwarding stream to MTS. The port is 9500 by default.
MQ	MQ service. It is responsible for message interaction. The port is 61616 by default.
DMS	Device management service. It is responsible for logging in to encoders, receiving and forwarding alarm and sending time sync command. The port is 9200 by default.
ADS	Alarm distribution service. It is responsible for distributing alarm to different objects according to alarm plan. The port is 9600 by default/
MGW	Media gateway. It is responsible for sending MTS address to decoder. The port is 9090 by default.
WEB	Web program service. It is responsible for configuration at administrator end, providing web service interface and providing built-in functions of client. The port is 9100 by default.
MTS	Streaming media distribution service. It is responsible for distributing audio/video stream from front-end device to SS, client and decoder. The port is 9100 by default.
PES	Power environment monitoring service. It is responsible for managing MCD (including alarm host, radar and access controller). The port is 9400 by default.
PTS	Picture transfer service. It is responsible for receiving, storing and transferring pictures.
OSSHTTP	Picture storage service. It is responsible for receiving, storing and transferring common pictures. The port is 50000 by default.
OSSHTTPS	Picture storage service. It is responsible for receiving, storing and transferring common pictures. It is safer than OSSHTTPS. The port is 50001 by default.

2.3 Segment Setup

Set NIC and port mapping. See"2.2.1 Network Card Config" and"2.2.2 LAN/WAN Mapping."

2.4 Basic Config

2.4.1 Managing Account

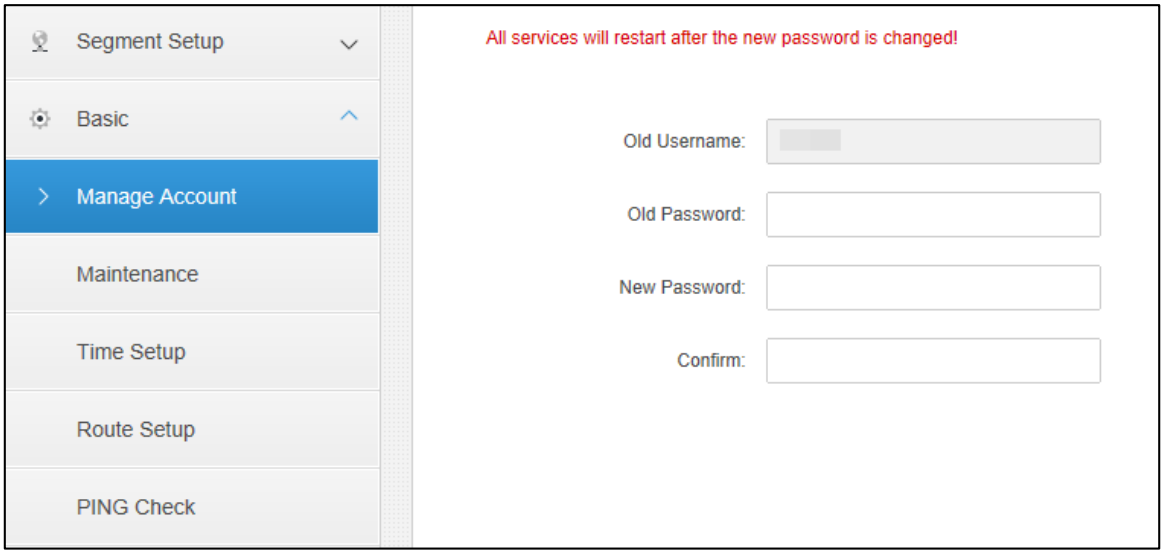
Modify admin password.

Modifying password will reboot all services. Confirm whether all services have rebooted successfully after reboot.

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

The interface of **Manage Account** is displayed. See Figure 2-5.

Figure 2-5 Manage account



Step 2 Input the original password and new password and then confirm password.

Step 3 Click **Apply**.

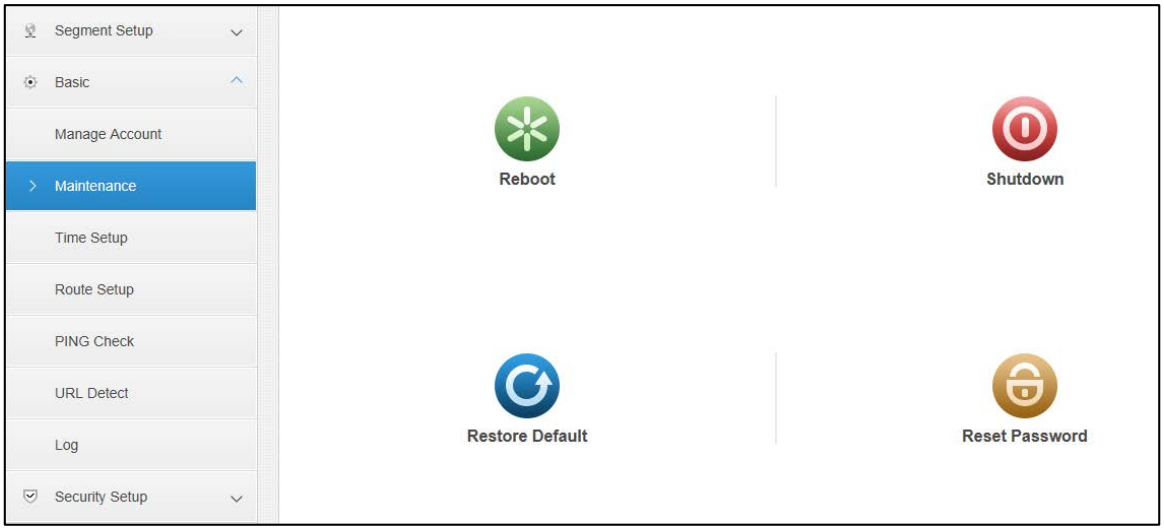
2.4.2 Maintenance

Reboot device, turn off device, restore device to factory settings and reset passwords of the config system user and Linux system root user.

Step 1 Select **Basic > Maintenance**.

The interface of **Maintenance** is displayed. See Figure 2-6.

Figure 2-6 Maintenance



Step 2 Select and click the following buttons as needed.

- Reboot: reboot server
- Shutdown: turn off server
- Restore Default: restore to factory settings
- Reset Password: restore the config system password to 123456

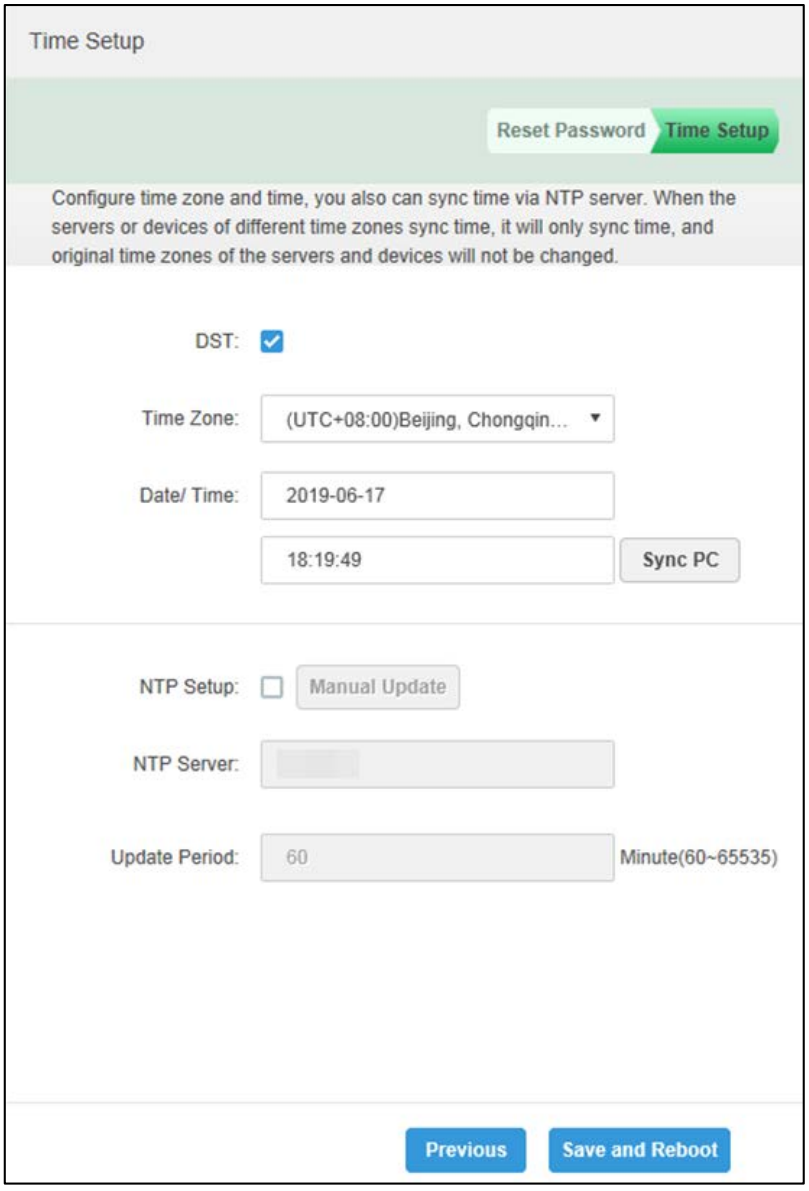
2.4.3 Time Setup

Set server time zone and time.

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

The interface of **Time Setu**p is displayed. See Figure 2-7.

Figure 2-7 Time setup



Step 2 Set time parameters. See Table 2-3.

Table 2-3 Time parameters

Parameter	Description
DST	Select DST to enable DST (Daylight Saving Time).
Time Zone	Select time zone of the server.
Date/Time	System provides two ways to set date and time. ● Click the box to select date and time. ● Click **Sync P**C to sync PC time with system time.
Sync PC	
NTP Setup	Select **NTP Setup** to enable NTP time sync.
NTP Server	Input NTP server domain or IP and click **Manual Update** to sync time.
Manual Update	
Update Period	Time interval of time sync between NTP server and platform server. The maximum interval is 65535 minutes.

Step 3 Click **Apply**.

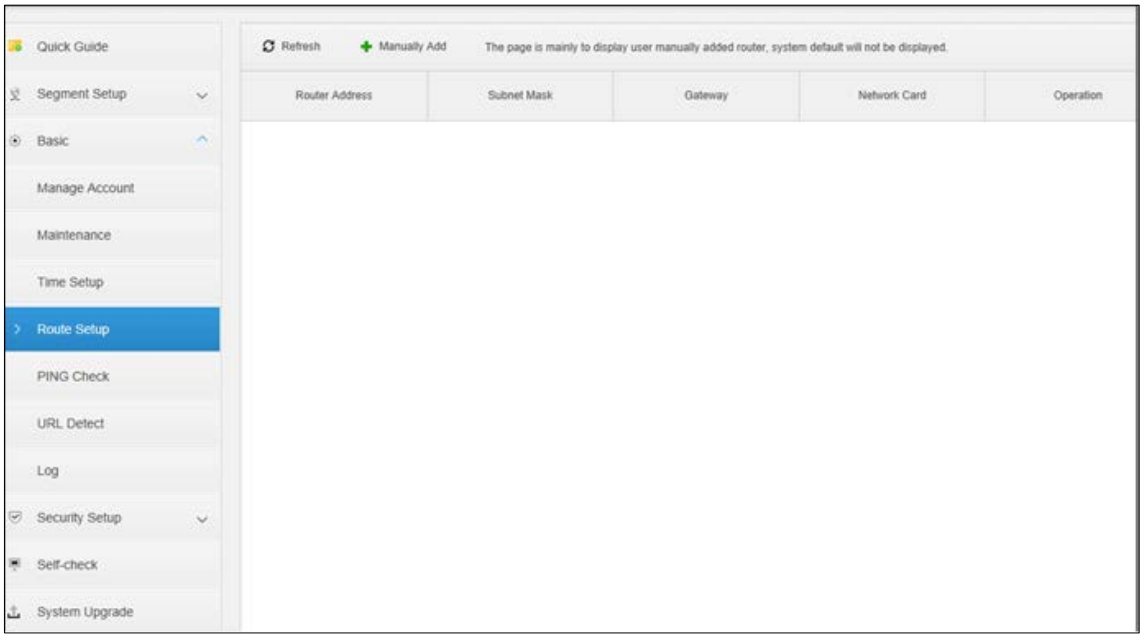
2.4.4 Route Setup

Configure static route for WAN/LAN access.

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

The interface of **Route Setup** is displayed. See Figure 2-8.

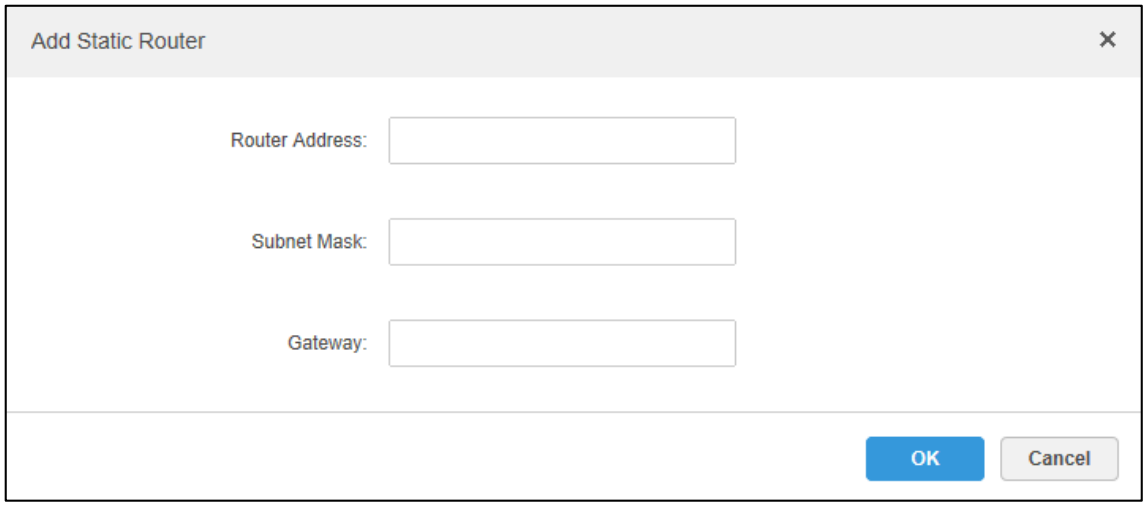
Figure 2-8 Route setup



Step 2 Click **Manually Add**.

The interface of **Add Static Router** is displayed. See Figure 2-9.

Figure 2-9 Add static router



Step 3 Input router IP, subnet mask and default gateway.

Step 4 Click **OK**.

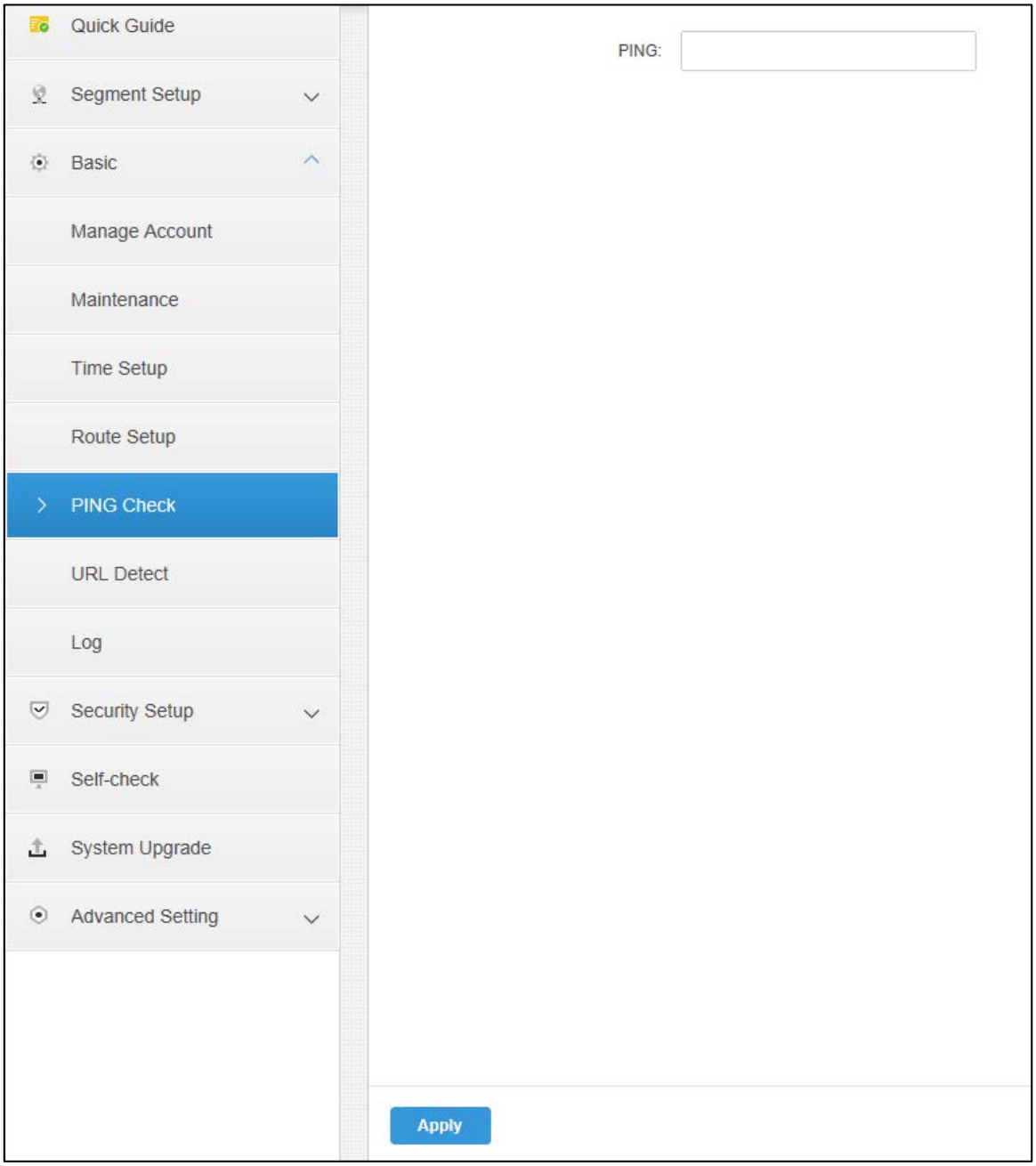
2.4.5 PING Check

Detect network connection status between platform and the input IP.

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

The interface of **PING Check** is displayed. See Figure 2-10.

Figure 2-10 PING check



Step 2 Enter IP address. Click **Apply** to start to detect the connection status between platform and the input IP.

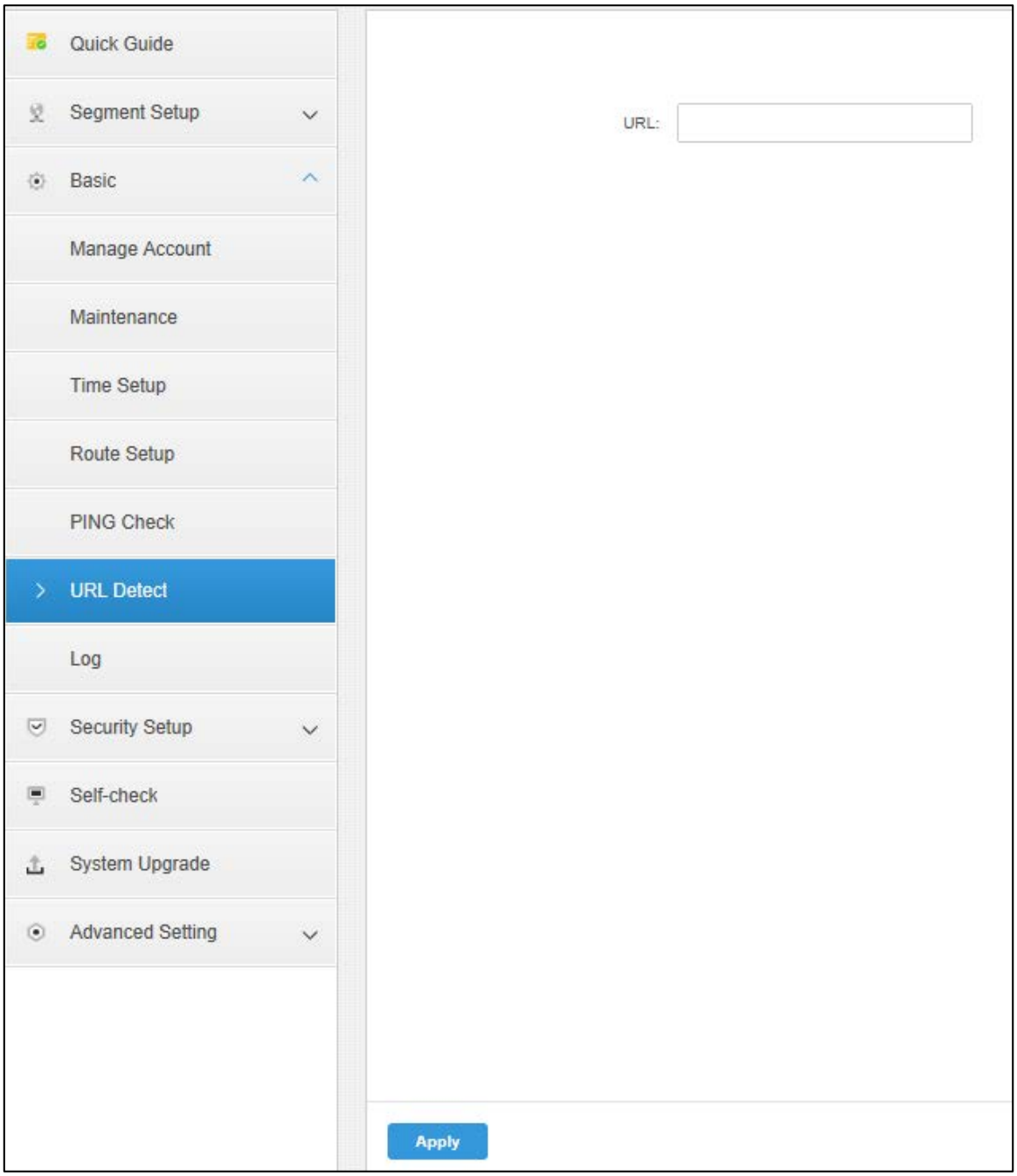
2.4.6 URL Detect

Test network connection status between platform and the input URL.

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

The interface of **URL Detect** is displayed. See Figure 2-11.

Figure 2-11 URL detect



Step 2 Enter url and click **Apply.**

Start to detect connection status.

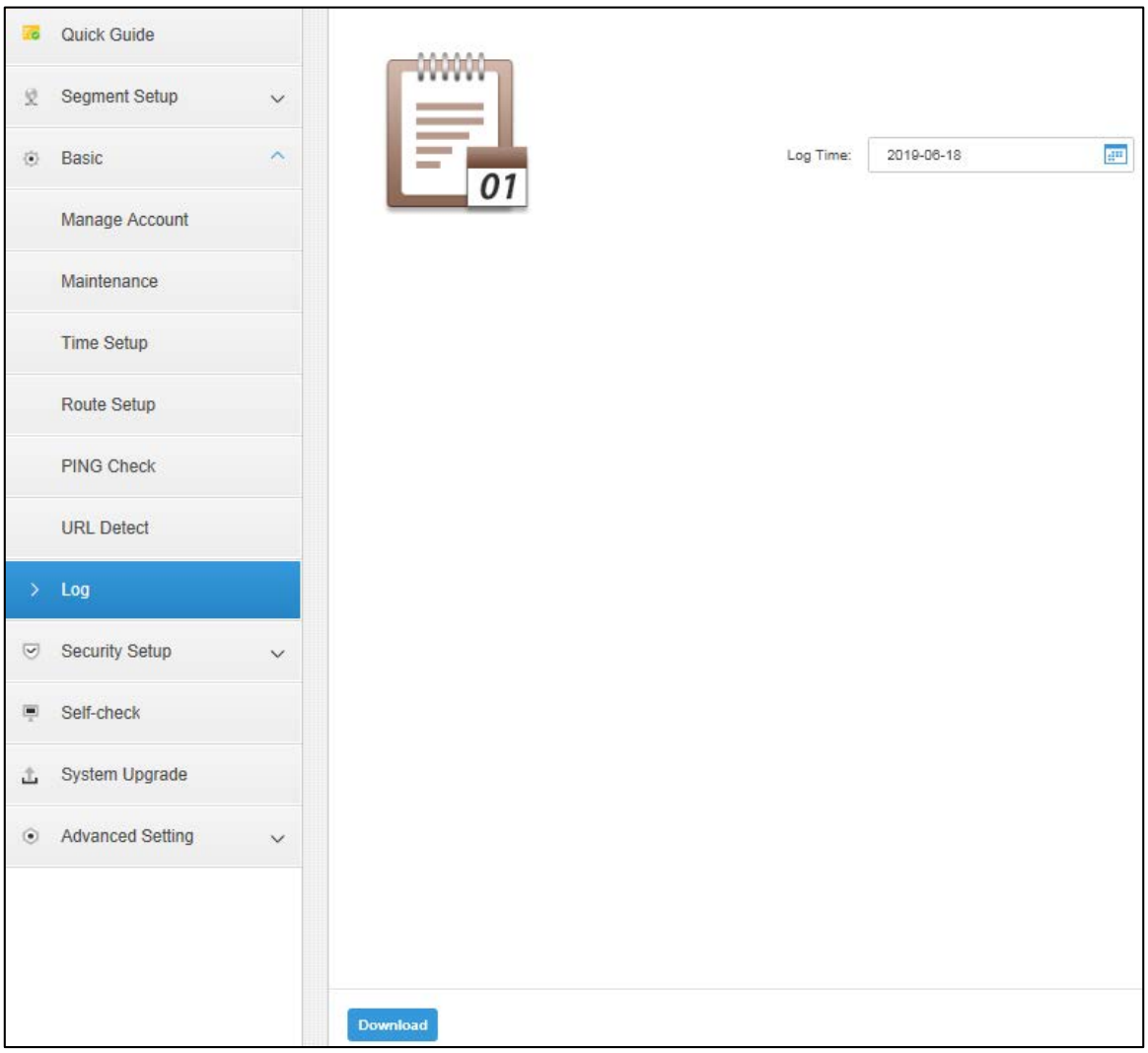
2.4.7 Log

Download log of services such as CMS, DMS, MTS, and SS.

Step 1 Click **Log.**

The interface of **Log** is displayed. See Figure 2-12.

Figure 2-12 Log



Step 2 Select date, and click **Download.**

2.5 Security Setup

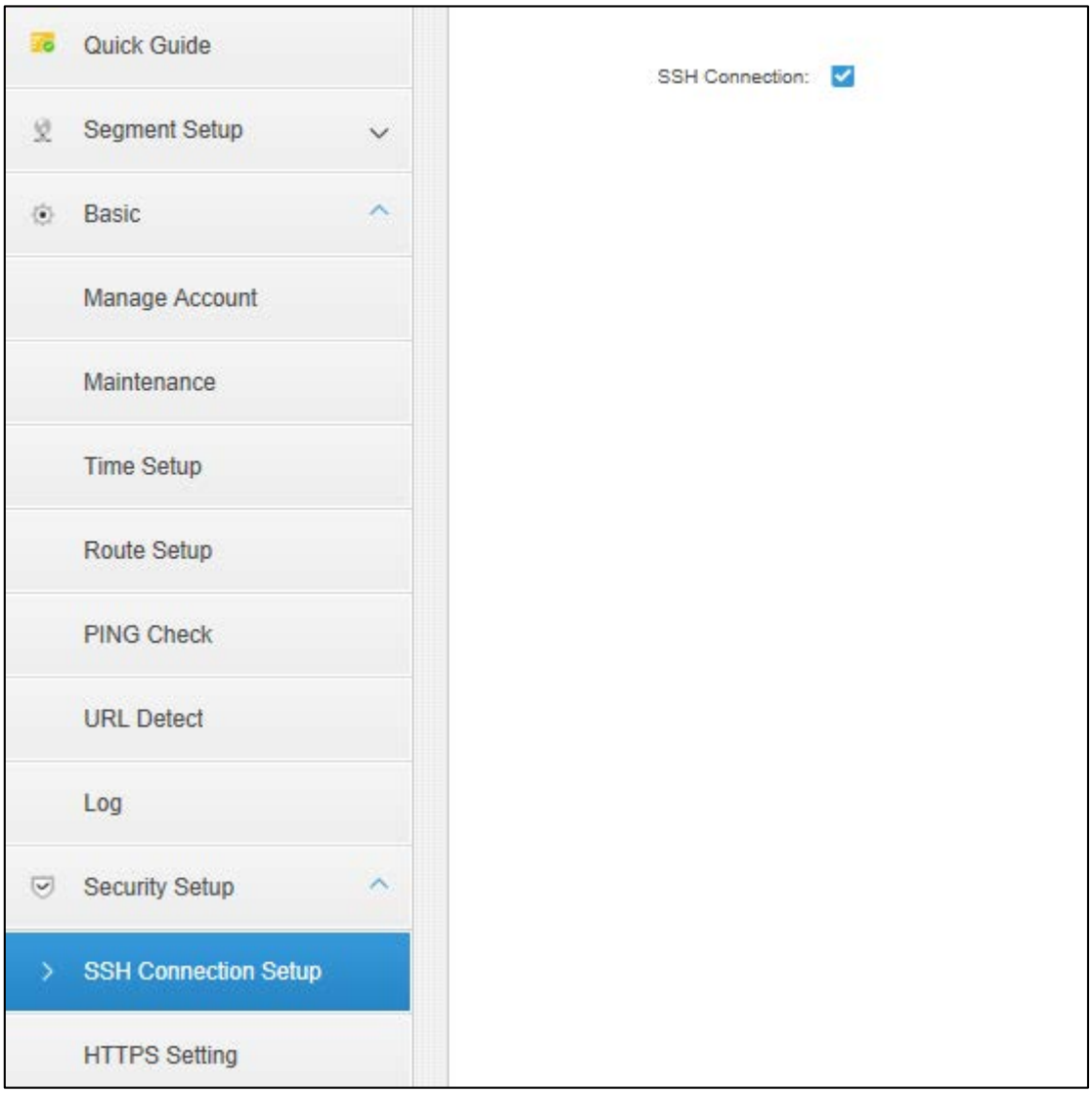
2.5.1 SSH Connection Setup

After SSH is enabled, the commissioning terminal can log in the platform by SSH protocol.

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

The interface of **SSH Connection Setup** is displayed. See Figure 2-13.

Figure 2-13 SSH connection



Step 2 Select **SSH Connection** to apply.

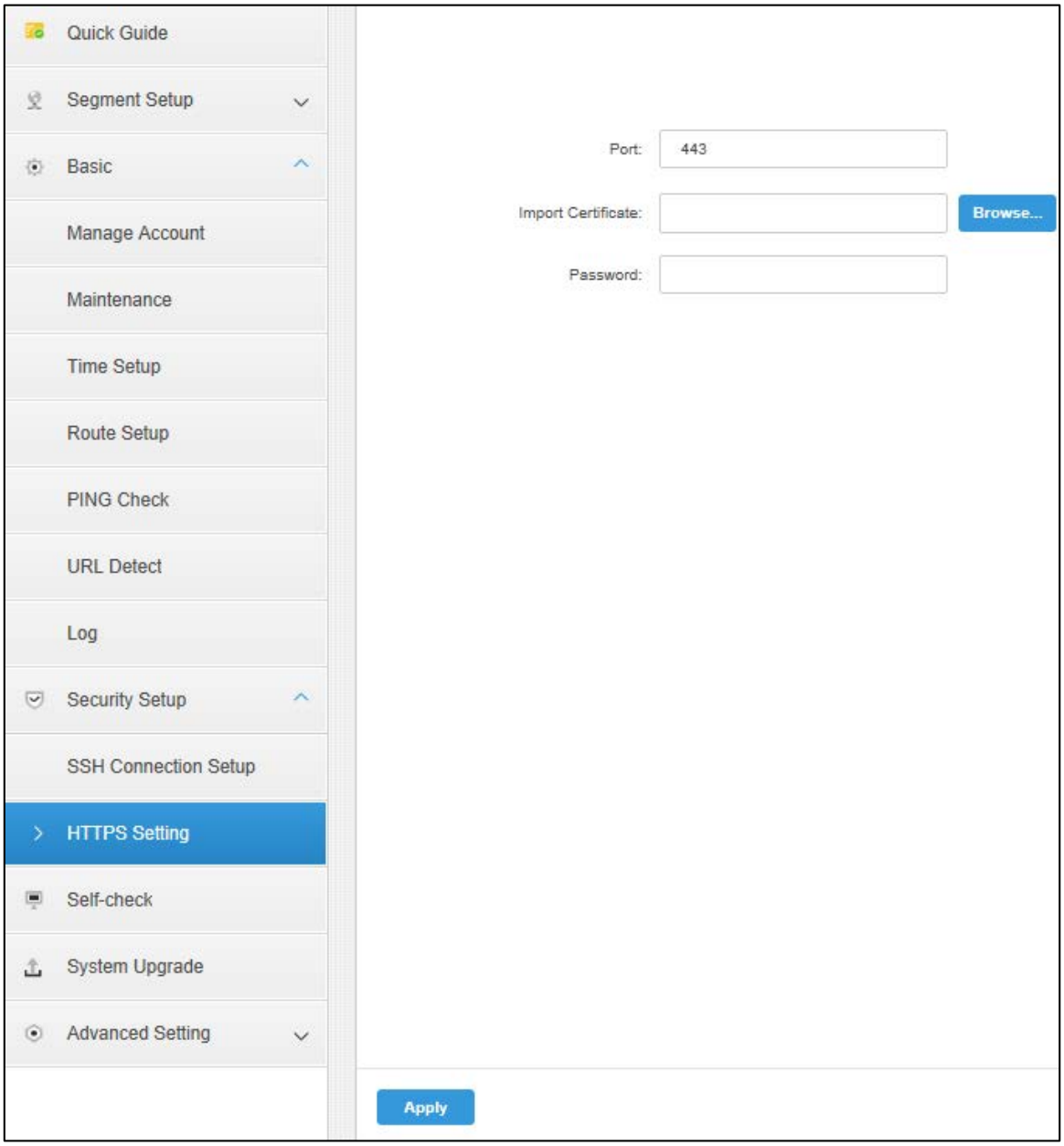
2.5.2 Configuring HTTPS

After HTTPS is configured, PC can log in platform by HTTPS. Communication data security is ensured in the meanwhile.

Step 1 Select **Basic > HTTPS Config**.

The interface of **HTTPS Config** is displayed. See Figure 2-14.

Figure 2-14 Configuring HTTPS



Step 2 Input port number (443 by default), import credential and input password.

If the default port number is modified, you need to input the new port number when visiting the platform or logging in client.

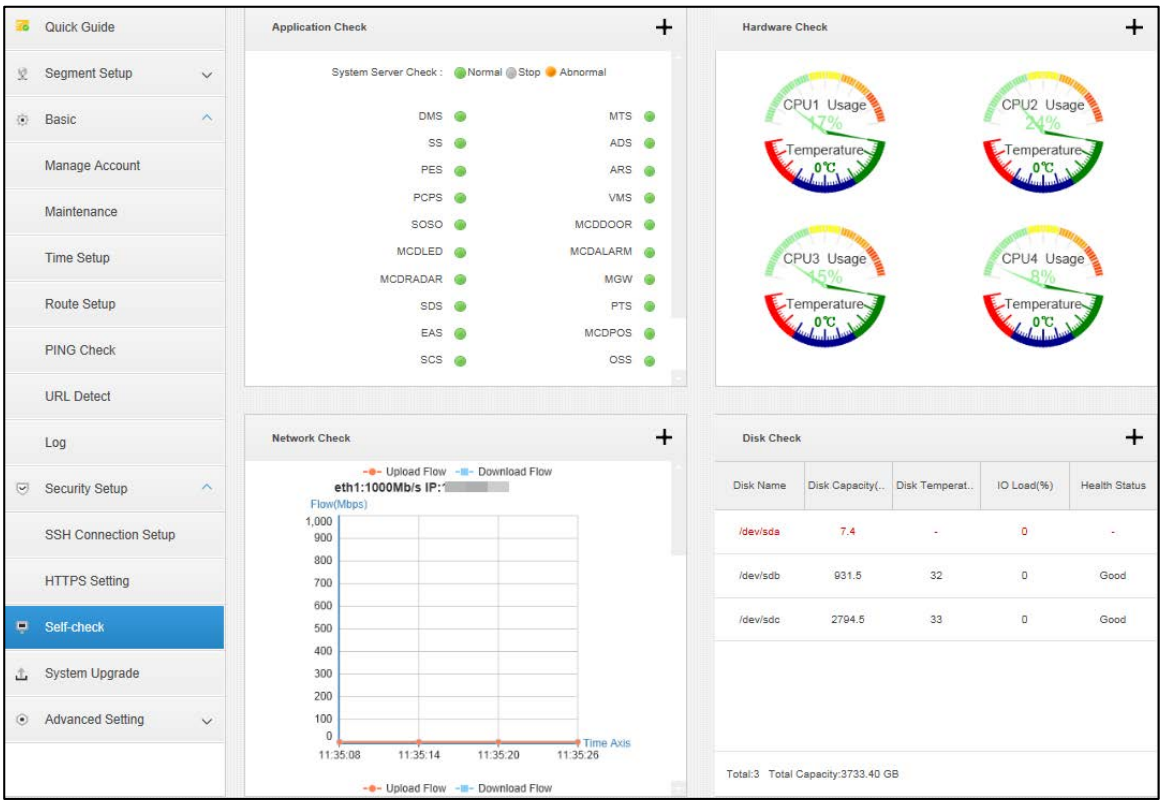
Step 3 Click **Apply** to finish.

2.6 Self-Check

Check health status of applications, CPU, network and disk.

Step 1 Click **Self-Check**. The interface of results is displayed. See Figure 2-15.

Figure 2-15 Self-check



Step 2 Click + at top right of each module or click  at top left. The detailed results are displayed. See Figure 2-16, Figure 2-17, Figure 2-18, and Figure 2-19.

Figure 2-16 Application check result

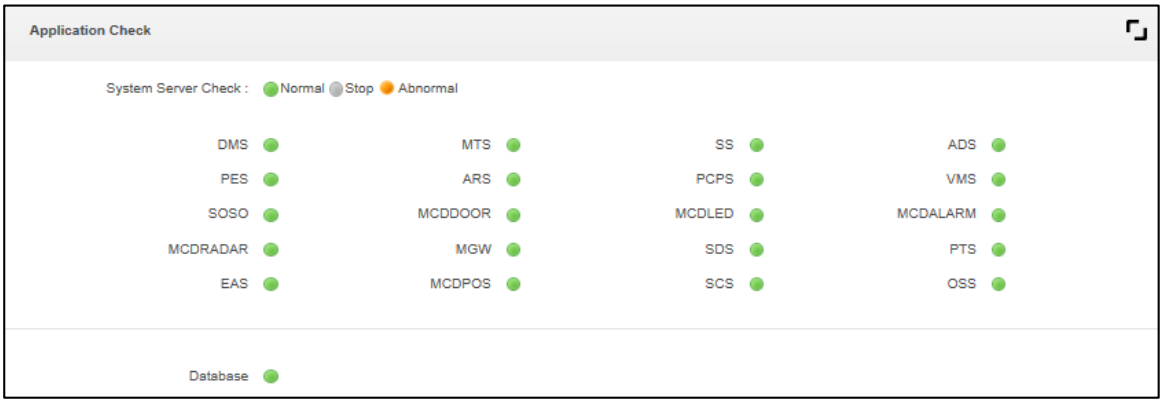


Figure 2-17 CPU check result

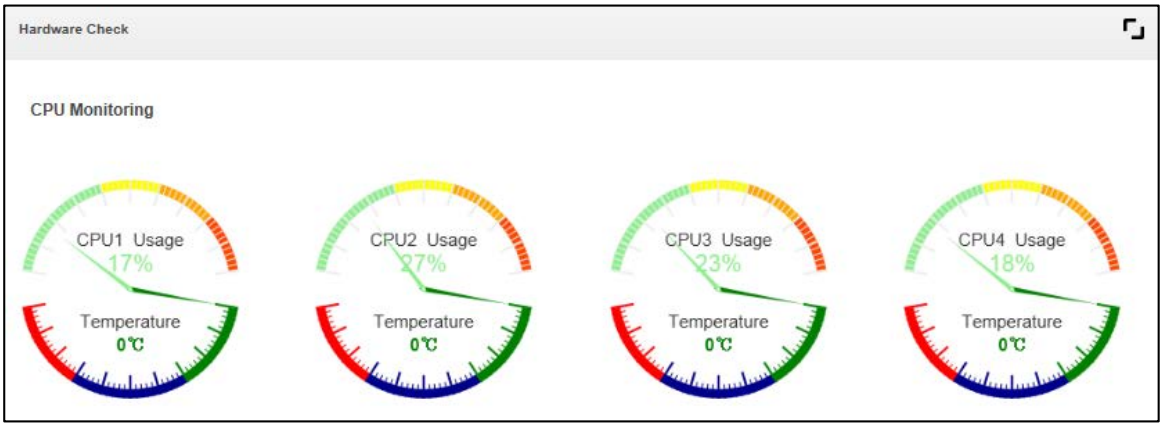


Figure 2-18 Network port check result

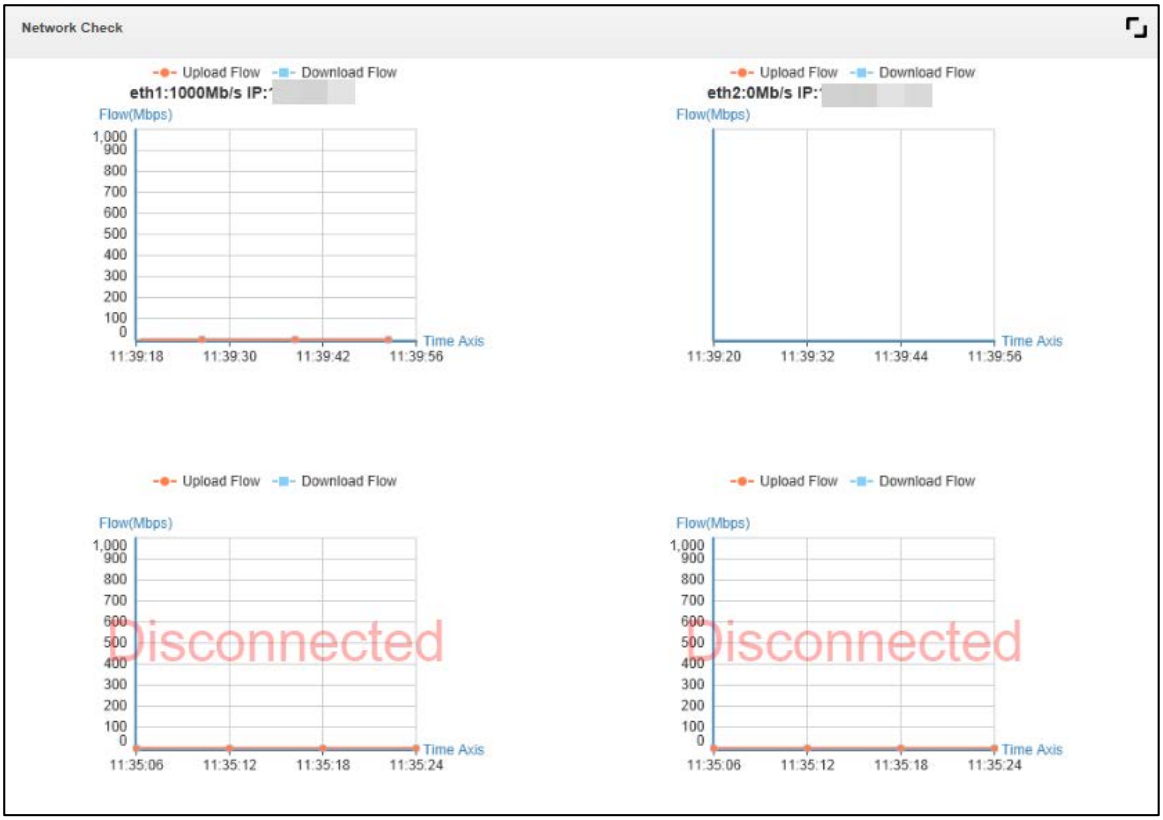
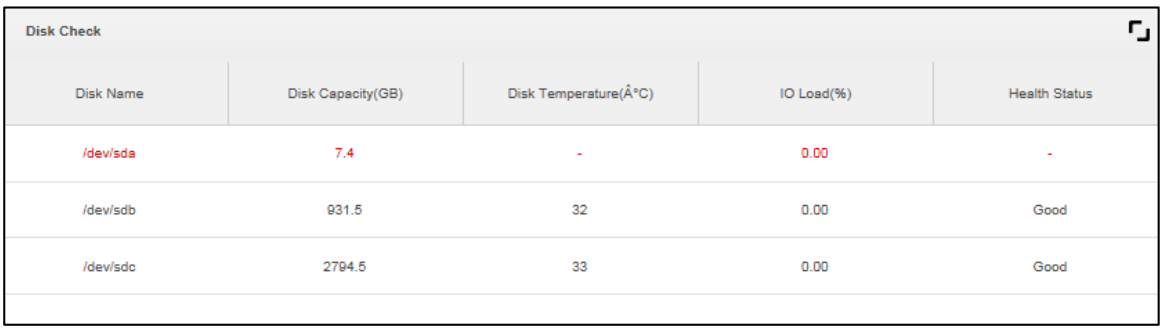


Figure 2-19 Disk check result



Disk Name	Disk Capacity(GB)	Disk Temperature(Â°C)	IO Load(%)	Health Status
/dev/sda	7.4	-	0.00	-
/dev/sdb	931.5	32	0.00	Good
/dev/sdc	2794.5	33	0.00	Good

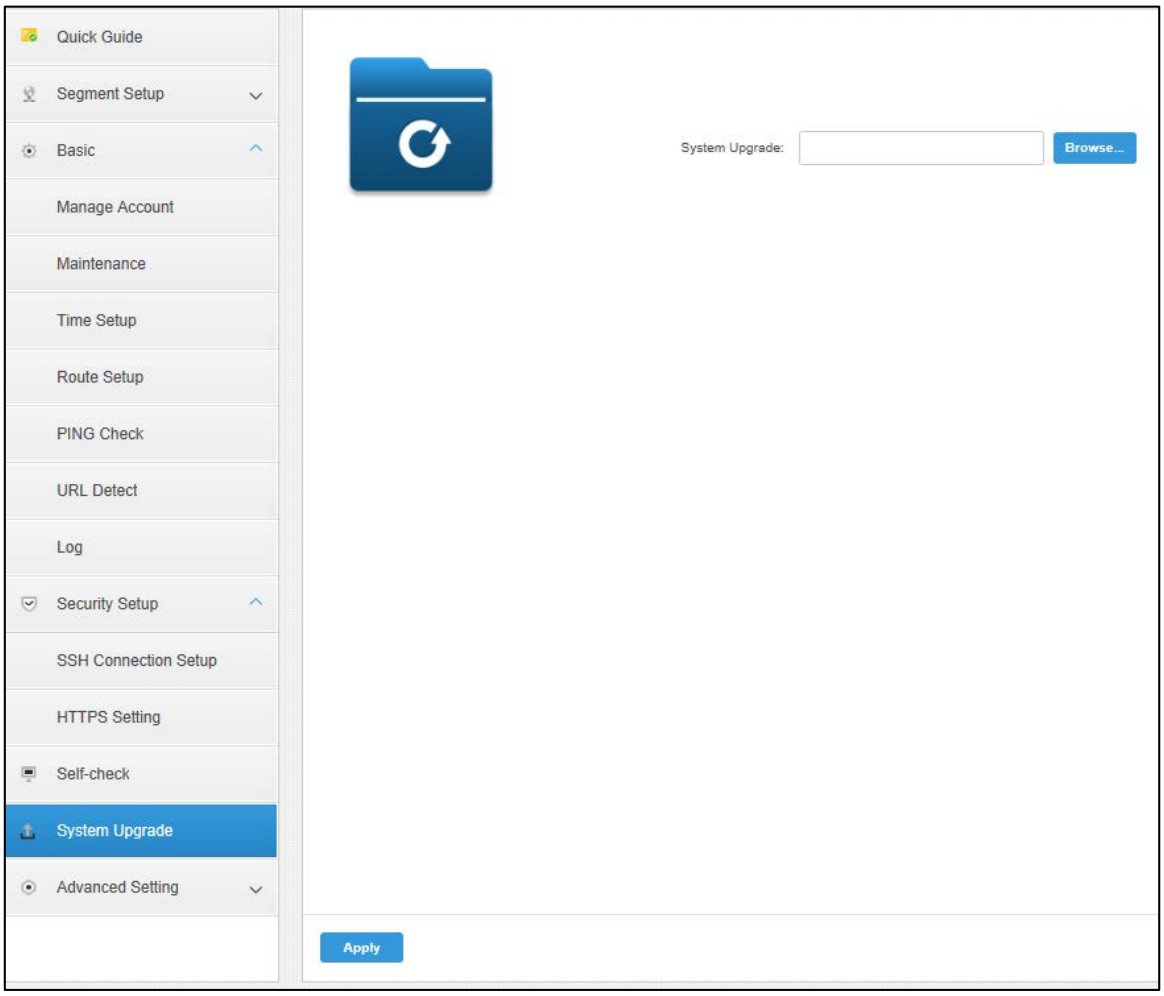
2.7 System Upgrade

Support WEB one-key upgrade and upgrading by tool.

Step 1 Click **System Upgrade**.

The interface of **System Upgrade** is displayed. See Figure 2-20.

Figure 2-20 Firmware upgrade



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

Step 3 Click **Apply** to start upgrade.

- When upgrading by Config Tool, you need to input platform IP address. The username and password are the same as that of the config system. The port is 3800.
- Click **Download Config Tool** in the login interface to download config tool.

3 Installing Client

3.1 Installing Client

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

3.1.1 PC Client

3.1.1.1 PC Config Requirement

For config requirement of PC where DSS Client is installed, see Table 3-1.

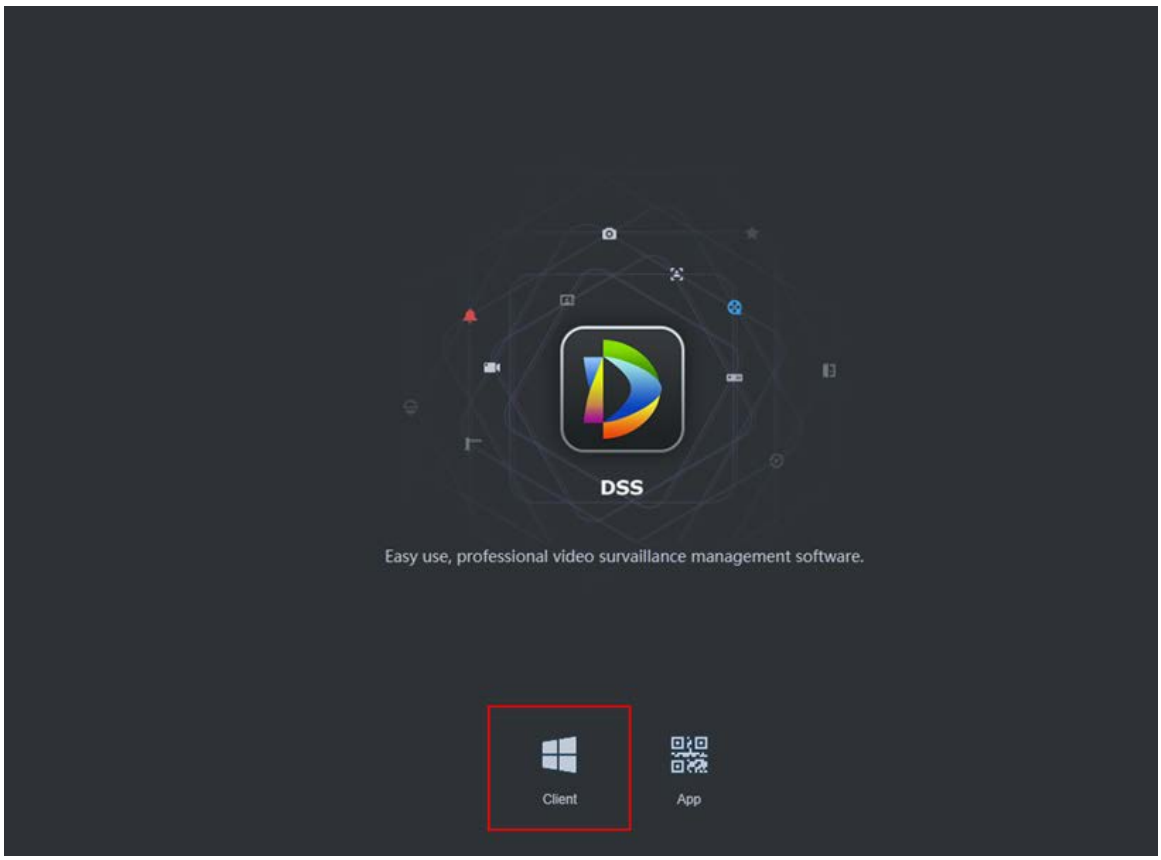
Table 3-1 Config requirement

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

3.1.1.2 Download and Install

Step 1 Enter server IP address into browser, click **Enter**.
The interface of downloading client is displayed. See Figure 3-1.

Figure 3-1 Download client



Step 1 Double click , run or download client according to interface prompt. For more download details, see Table 3-2.

Table 3-2 Download operation

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

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

Figure 3-2 Confirm agreement

Step 3 Select **I have read and agree the DSS agreement**, click **Next**.

The interface of installation path is displayed. See Figure 3-3.

Figure 3-3 Select installation path

Step 4 Click **Browse** and select installation path, click **Install**.

The installation takes about 2-3 minutes. The interface is shown in Figure 3-4 after installation is completed.

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

Figure 3-4 Installation completed

3.1.2 Mobile Phone APP

Currently mobile APP can be installed on IOS or Android.

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

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

The interface of downloading client is displayed. See Figure 3-5.

Figure 3-5 Mobile APP QR code

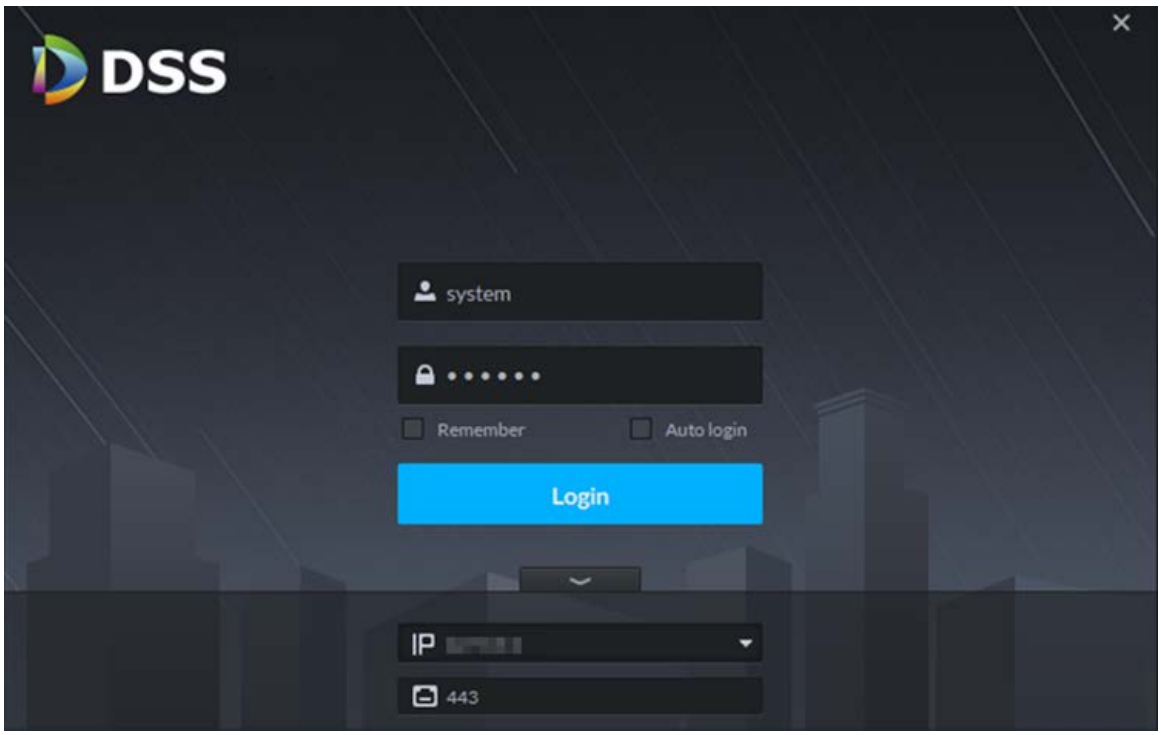
Step 2 Move the mouse to App, use mobile phone to scan corresponding QR code, then acquire and install APP according to prompt.

3.2 Initialization Config

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

Step 1 Double click on server desktop, or click Run on the interface after program is installed. The client login interface is displayed. See Figure 3-6.

Figure 3-6 Client login interface



Step 2 Enter username and password.

The default username and password is system, 123456 respectively.

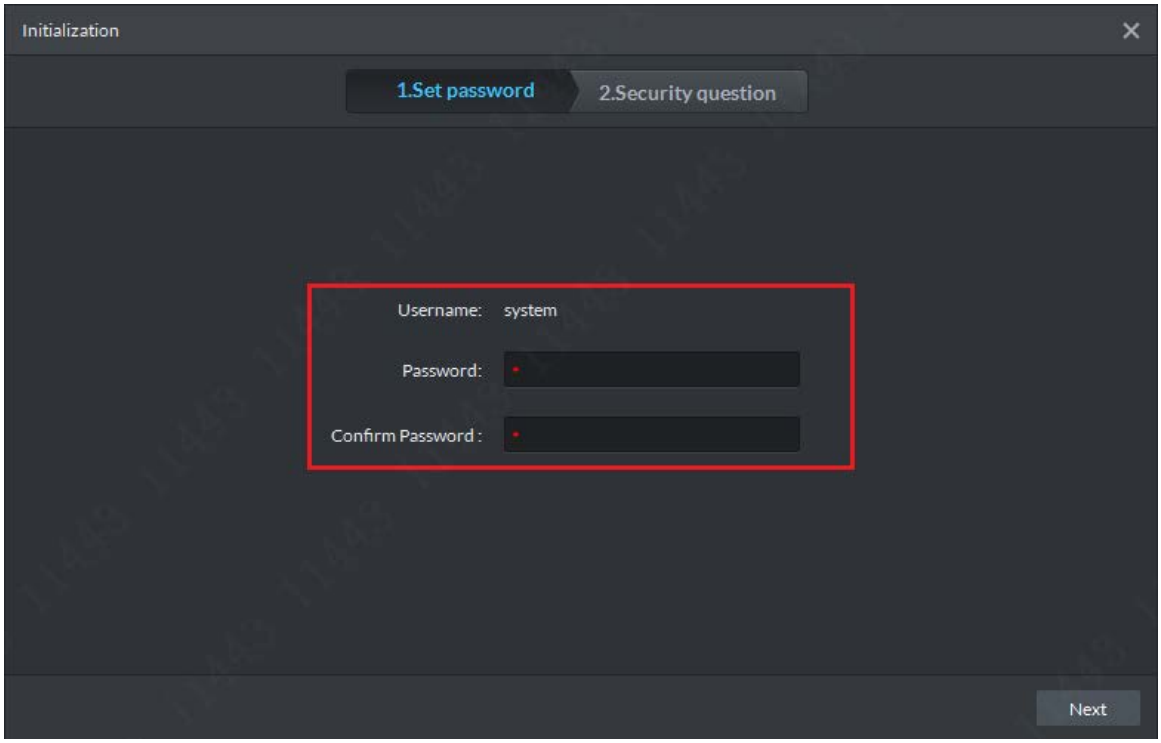
Step 3 Click [redacted], enter server IP address and HTTPS port number.

HTTPS port number is 441 by default.

Step 4 Click **Login**.

The interface of **Set Password** is displayed. See Figure 3-7.

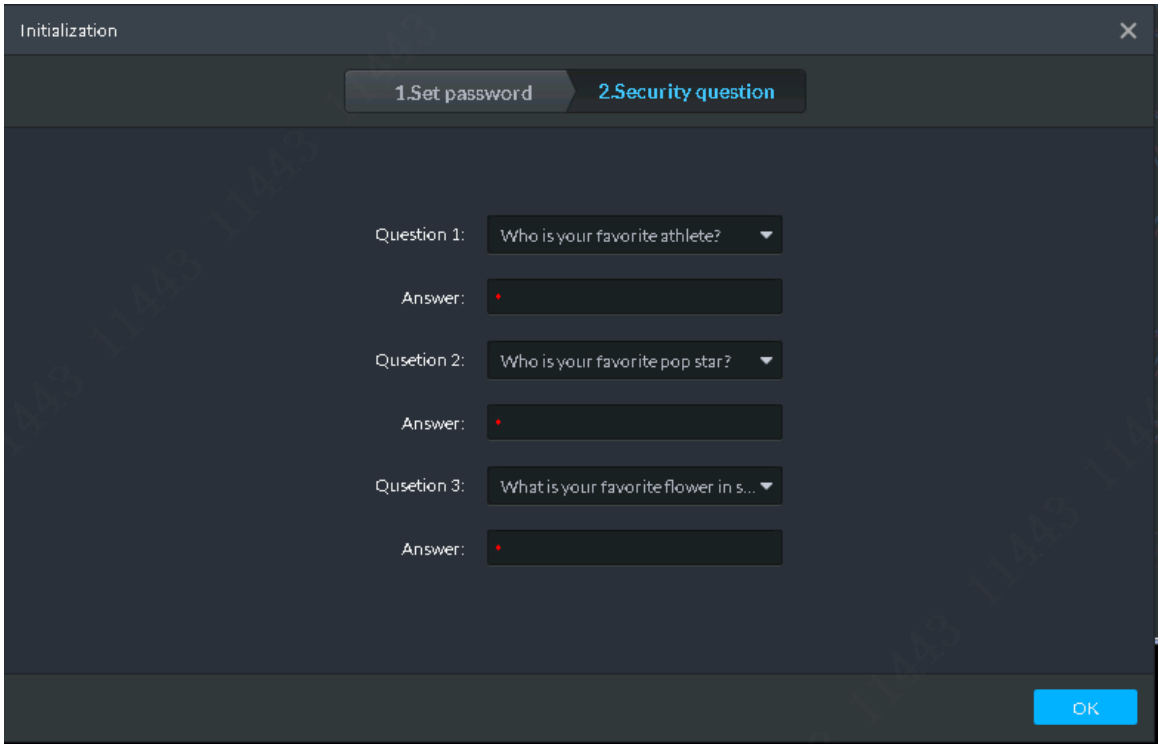
Figure 3-7 Set password



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

The **Security Question** interface is displayed. See Figure 3-8.

Figure 3-8 Security question



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

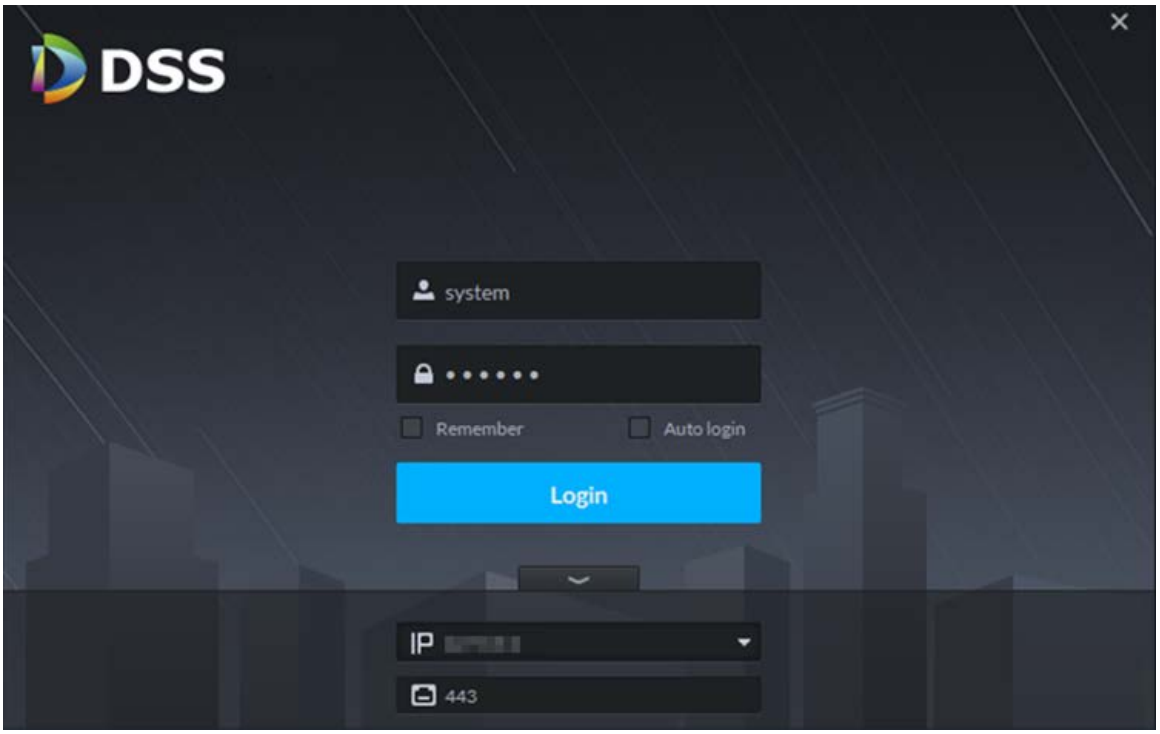
3.3 Logging in Client

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

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

The client login interface is displayed. See Figure 3-9.

Figure 3-9 Client login interface



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

The **Homepage** interface is displayed. See Figure 3-10. For homepage description, see Table 3-3.

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

Figure 3-10 Client homepage

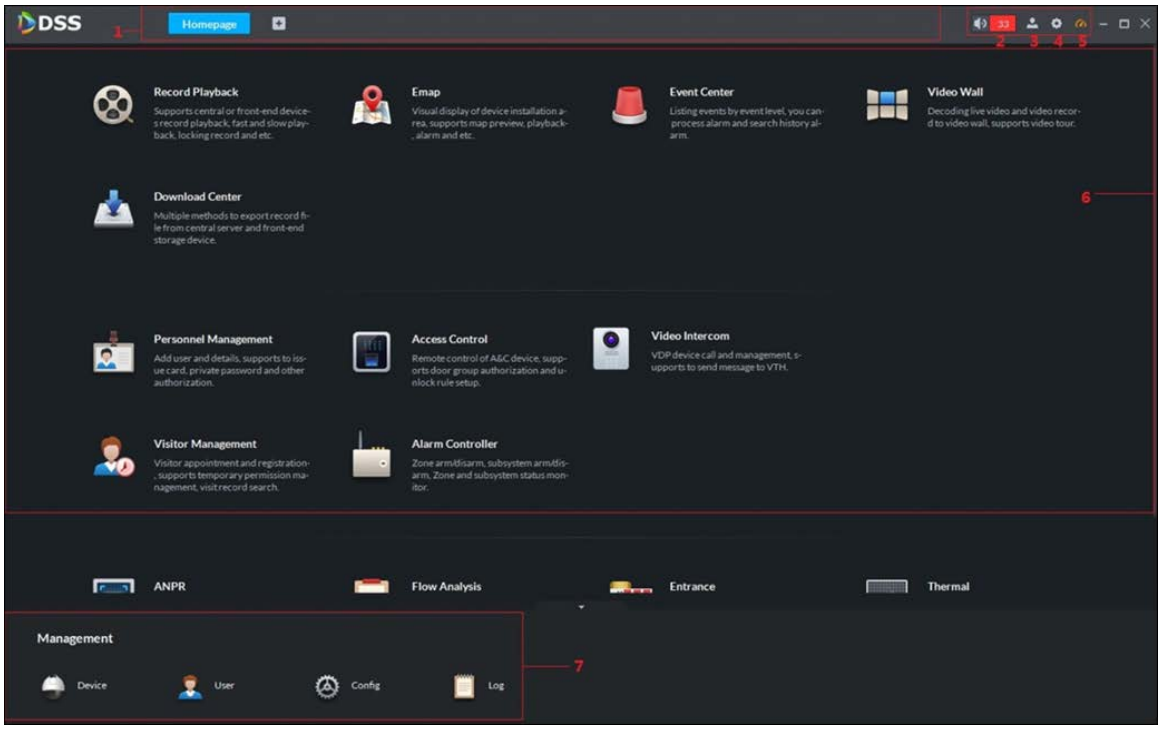


Table 3-3 Client homepage description

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

No.	Name	Description
4	Config	Click the icon and you can make settings, such as basic setting, video setting, video playback, snapshot setting, record, alarm and shortcut button.
5	System Status	Click the icon and you can view the status of server network, CPU and memory.
6	Function	Display live preview, video playback, map, event center, video wall, download center, user management, access control and plate recognition. You can click corresponding function to enter.
7	Management	Display device management, user management, config management and log management. Click to enter corresponding management page. Click  and you can hide the section.

4 Operation Guide

4.1 Basic Config

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

4.1.1 System Setting

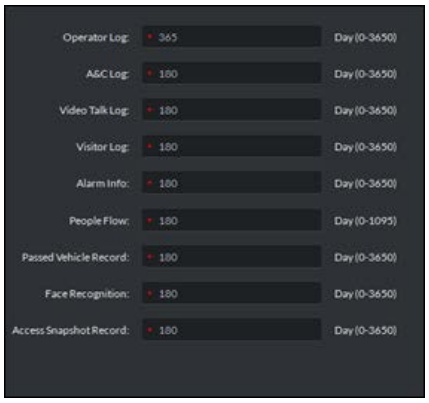
4.1.1.1 Setting Message Storage

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

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

1) On the client homepage, click **Config**.
   The **Config** interface is displayed.
2) Click **Message Storage**.
   The **Message Storage** interface is displayed. See Figure 4-1.

Figure 4-1 Message storage



Step 2 Set storage duration log.

Step 3 Click **OK**.
The config is saved and takes effect.

4.1.1.2 Time Sync

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

4.1.1.2.1 Auto Time Sync

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

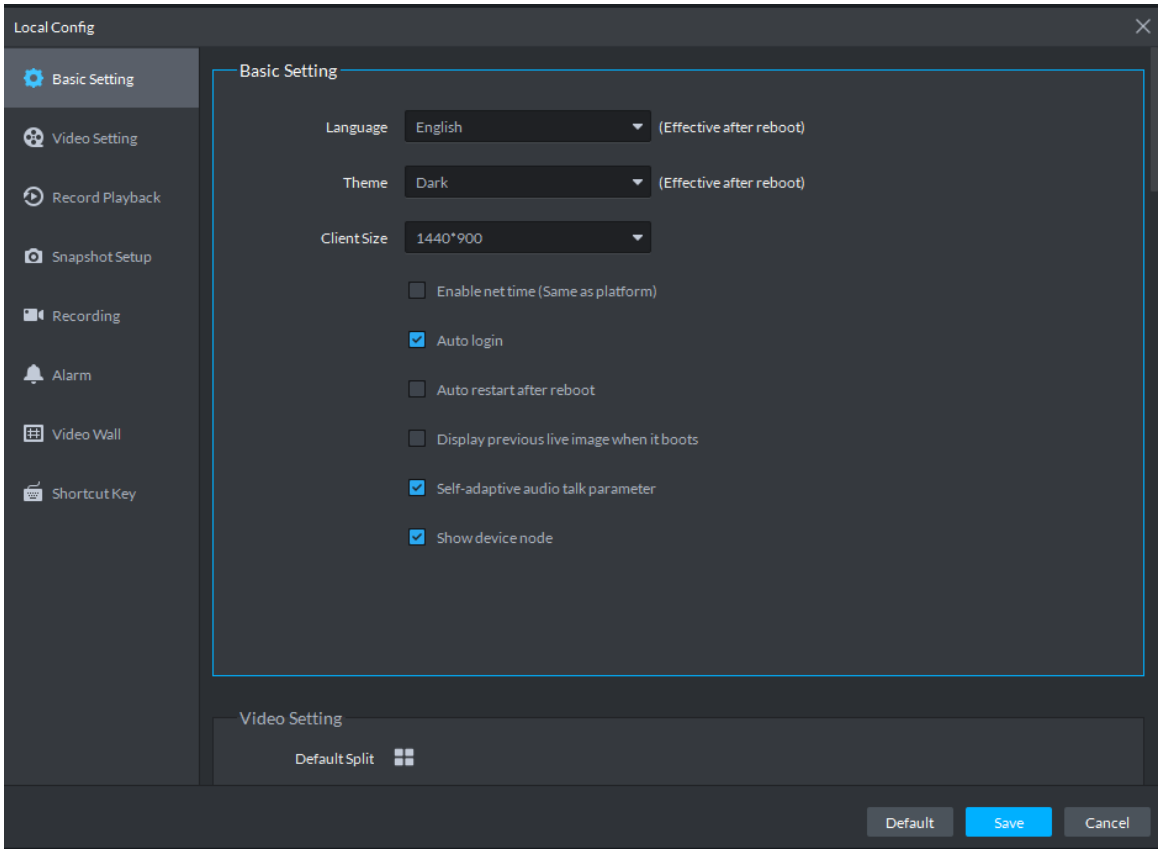
Step 1 (Optional) Enable time sync on local config of client.

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

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

The interface of **Local Config** is displayed. See Figure 4-2.

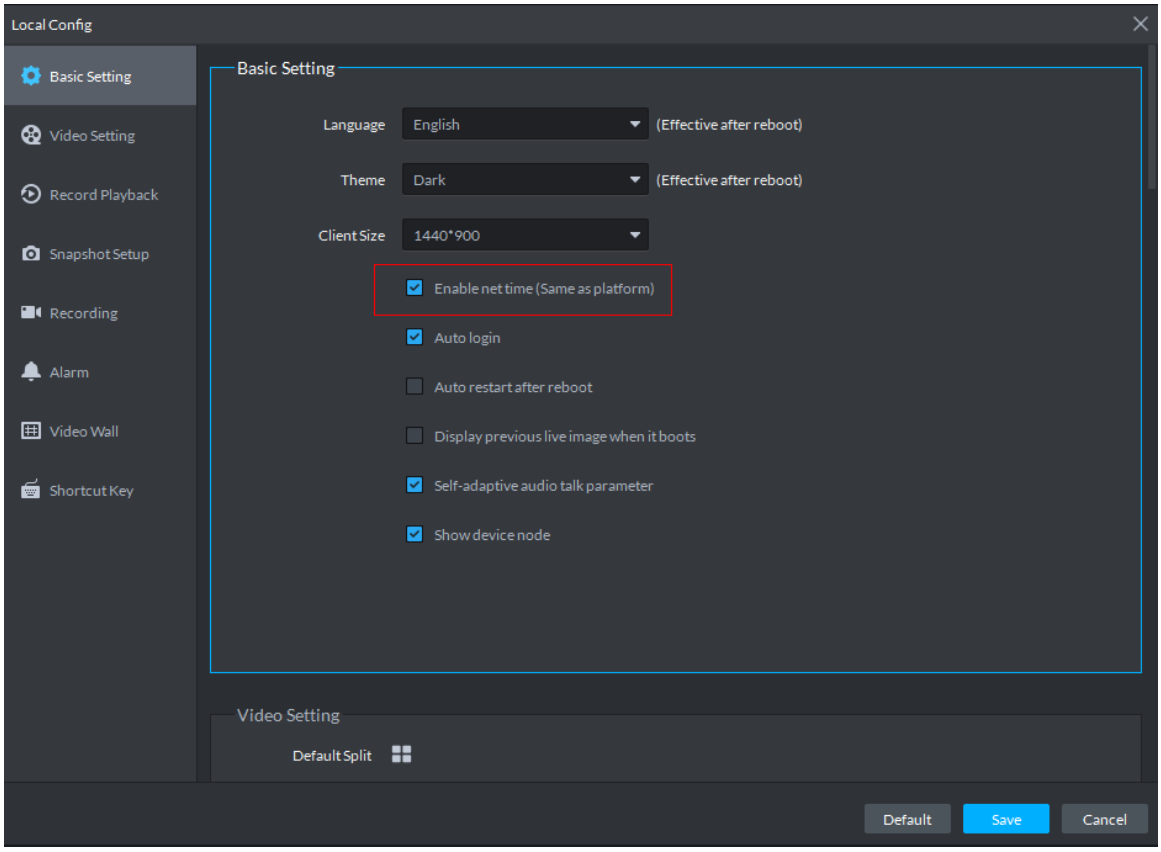
Figure 4-2 Local config



2) Click the tab of **Basic Config**.

The **Basic Config** interface is displayed. See Figure 4-3.

Figure 4-3 Enable net time



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

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

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

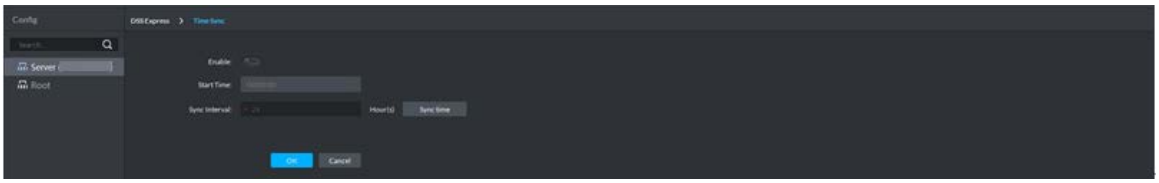
1) On client homepage, click **Config**.

The **Config** interface is displayed.

2) Click **Time Sync**.

The interface of **Time Sync** is displayed. See Figure 4-4.

Figure 4-4 Time sync



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

The icon becomes  and auto time sync is enabled.

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

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

4.1.1.2.2 Manual Time Sync

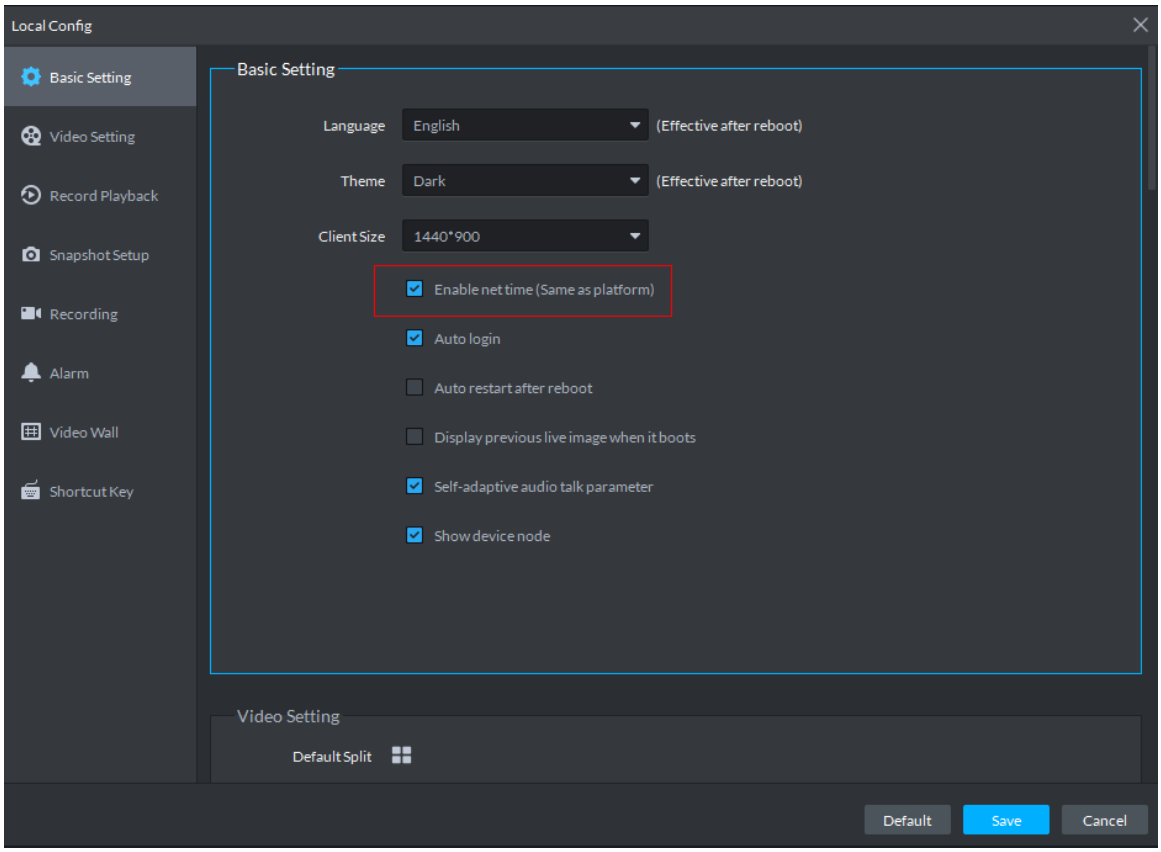
Start time sync request manually, and the system responds to request immediately.

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

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

1) Click on upper right corner of client interface.
   The interface of **Local Config** is displayed.
2) Click the tab of **Basic Setting**.
   The interface of **Basic Setting** is displayed. See Figure 4-5.

Figure 4-5 Enable client time sync



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

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

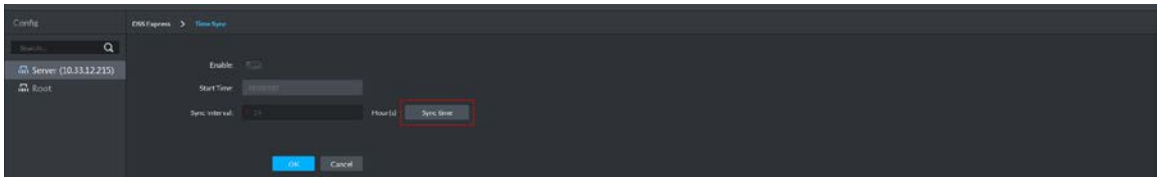
Step 2 Enter config interface of **Time Sync**.

1) On client homepage, click **Config**.
   The **Config** interface is displayed.
2) Click **Time Sync**.
   The interface of **Time Sync** is displayed. See Figure 4-4.

Step 3 Click **Sync Time**. See Figure 4-6.

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

Figure 4-6 Sync time



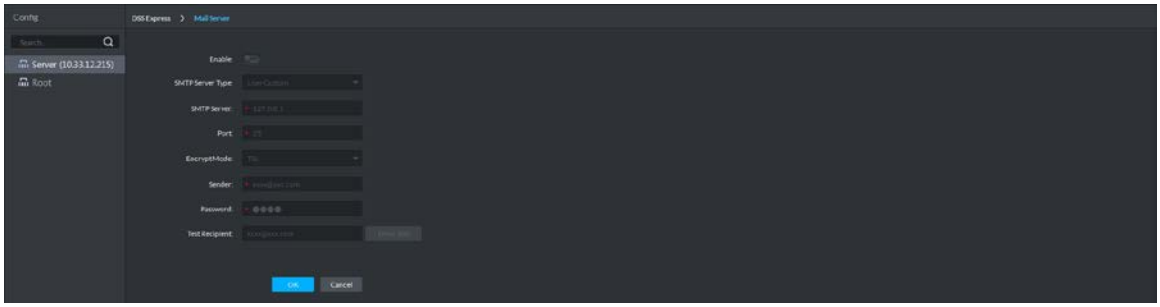
4.1.1.3 Setting Email

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

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

1) Click **Config** on the client homepage.
   The **Config** interface is displayed.
2) Click **Email**.
   The **Mail Server** interface is displayed. See Figure 4-7.

Figure 4-7 Email server



Step 2 Click  , and enable email.

The icon becomes  and the function is enabled.

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

TSL encryption method is highly recommended.

4.1.1.4 Setting Storage Space

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

4.1.1.4.1 Setting Local Storage Disk

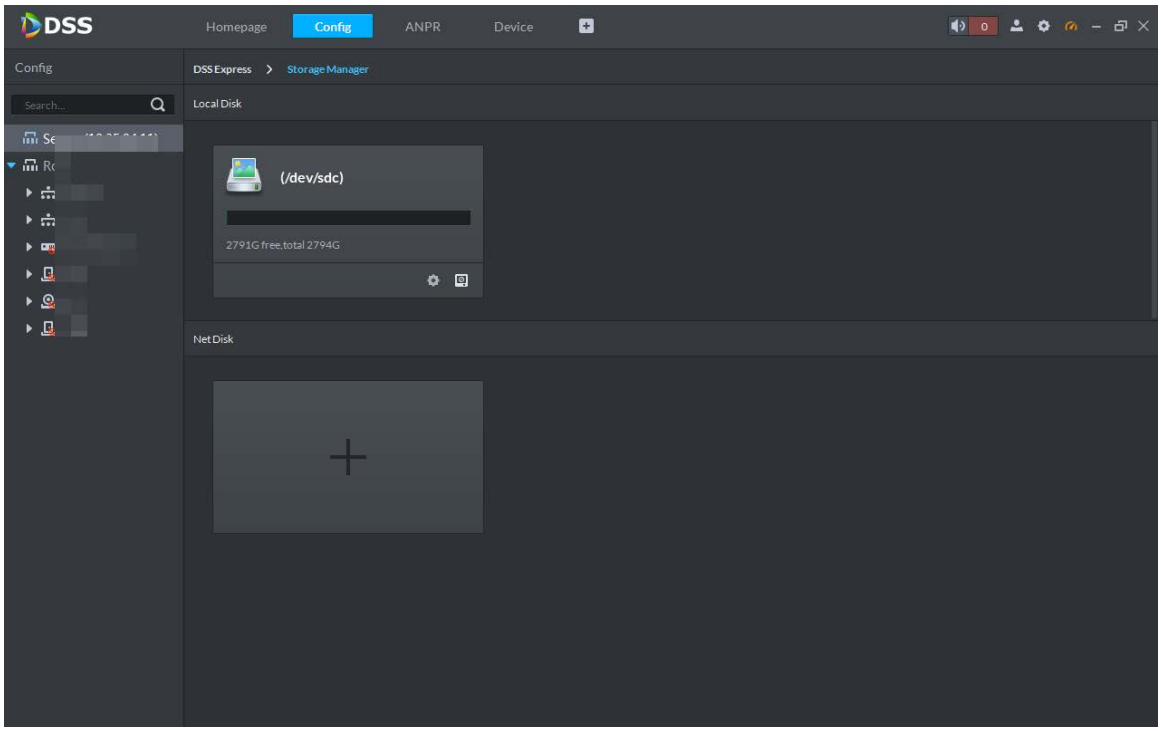
The system automatically detects storage space of all the disks in the system, and creates exclusive space for platform, used to store videos, general pictures and ANPR pictures.

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

1) Click **Config** on the client homepage.
   The interface of **Config** is displayed.
2) Click **Storage**.

The **Storage Manager** Interface is displayed; the system automatically detects disk info of server (Disk info of non PC client). See Figure 4-8.

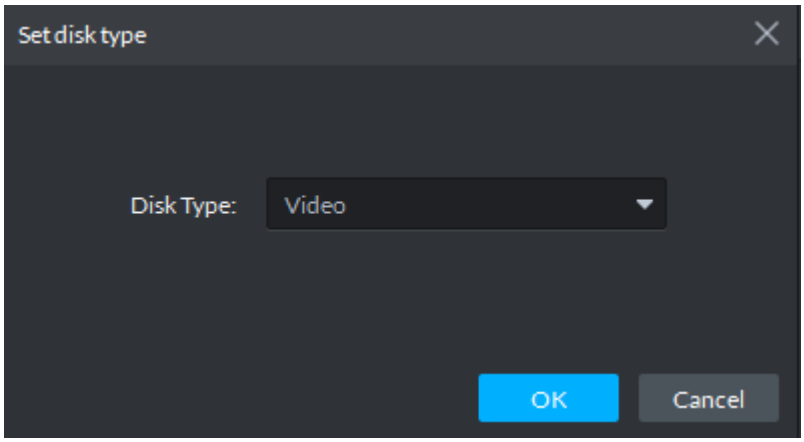
Figure 4-8 Storage manager



Step 2 Click  .

The system pops out the dialog of **Set disk type**.

Figure 4-9 Set disk type



Step 3 Set storage space type, and click **OK**.

Platform exclusive storage space is created on the disk.

- Storage space type includes video, general picture and ANPR picture. Video disk is used to store video, ANPR picture disk is used to store ANPR snapshot, general picture is used to store all snapshots except ANPR pictures.
- Click  to format disk.Disk formatting will delete all data in the disk. Please take care to carry out this operation.

4.1.1.4.2 Setting Network Disk

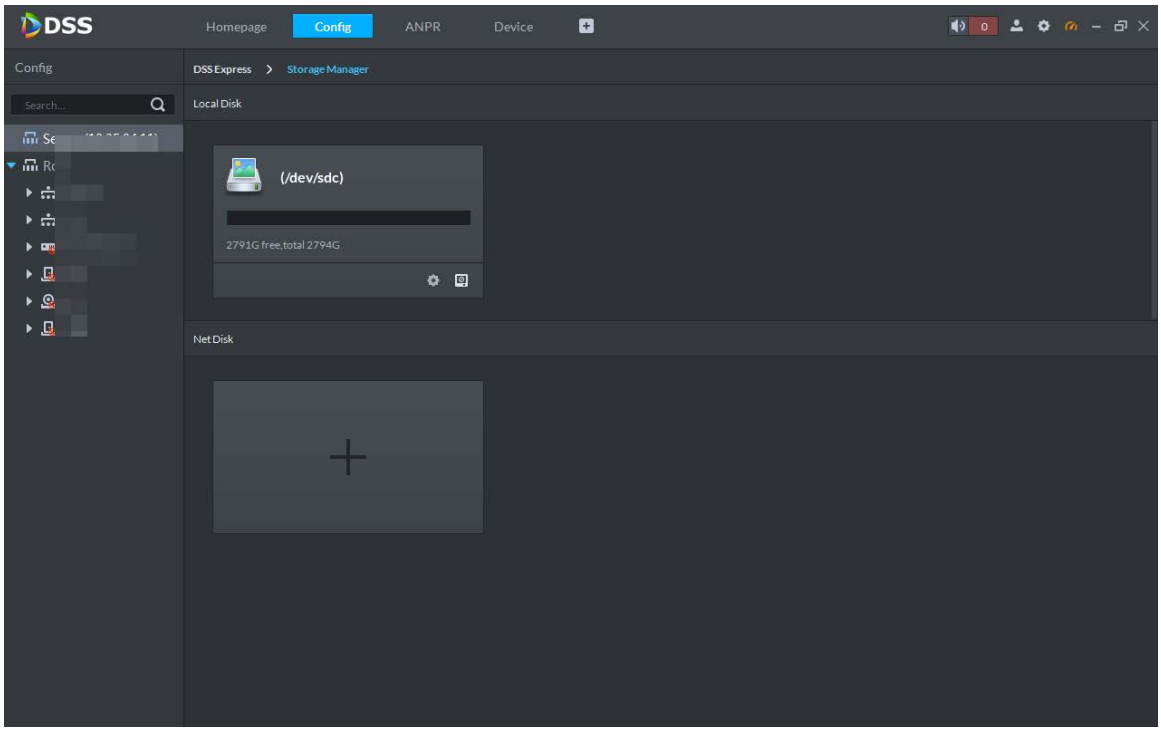
If network storage device exists in networking, you can create platform's exclusive storage space on network storage device, used to store video and ANPR pictures.

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

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

1) Click **Config** on the client homepage.
   The **Config** interface is displayed.
2) Click **Storage**.
   The **Storage Manager** interface is displayed. See Figure 4-10.

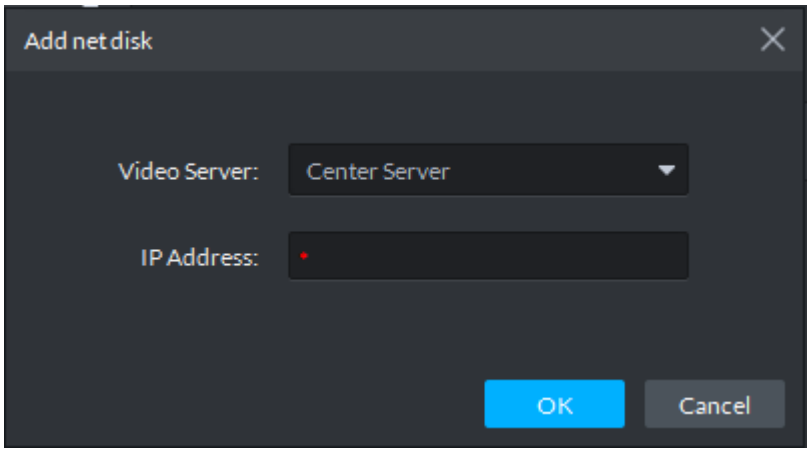
Figure 4-10 Storage manager



Step 2 Click  .

The system pops out the interface of **Add Network Disk**. See Figure 4-11.

Figure 4-11 Fill in IP



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

See Figure 4-12 for the adding result, green means remaining space, red means used space which can be overwritten.

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

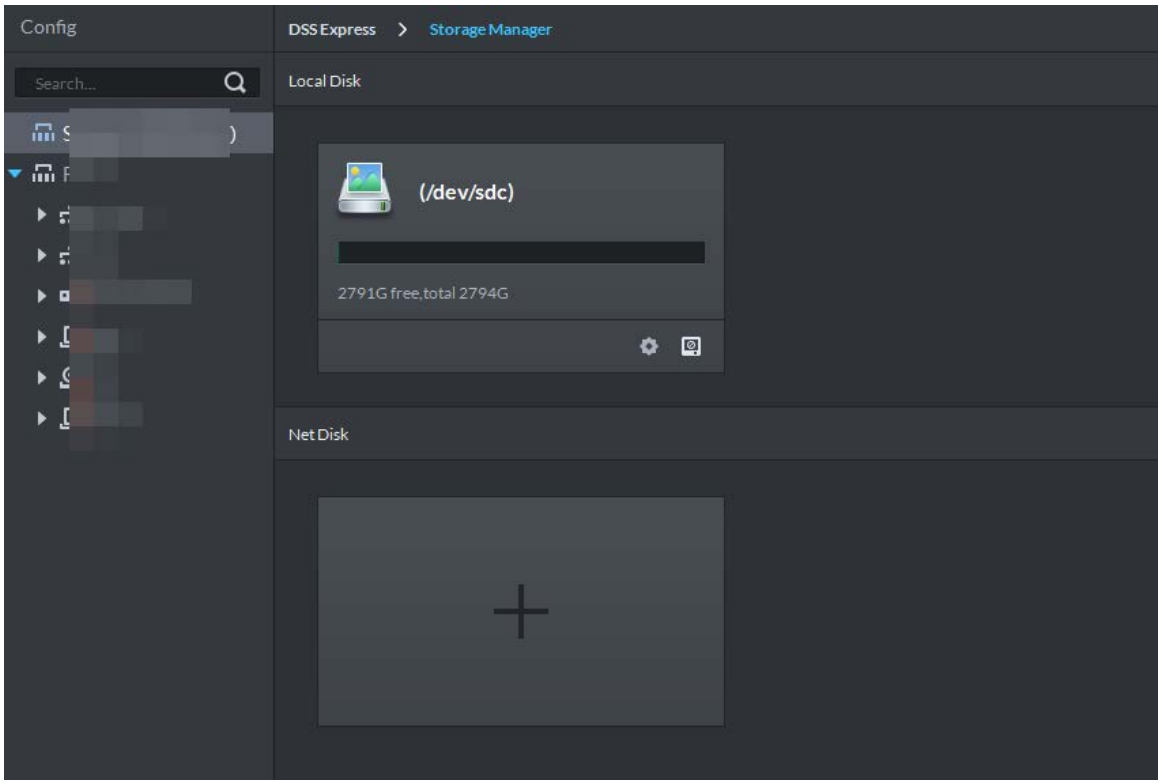
- Click and modify storage space type of disk, including video and ANPR picture.

  Video disk is used to store video, ANPR picture disk is used to store ANPR snapshot. If you need to store ANPR device snapshot, storage space type must be set as ANPR picture.

- Click and take the network disk used by other devices. Please make sure other device has stopped recording or snapshot before being taken, otherwise it will cause video or picture loss.

- Click and delete network disk. Please make sure recording or snapshot has stopped before being deleted, otherwise it will cause video or picture loss.

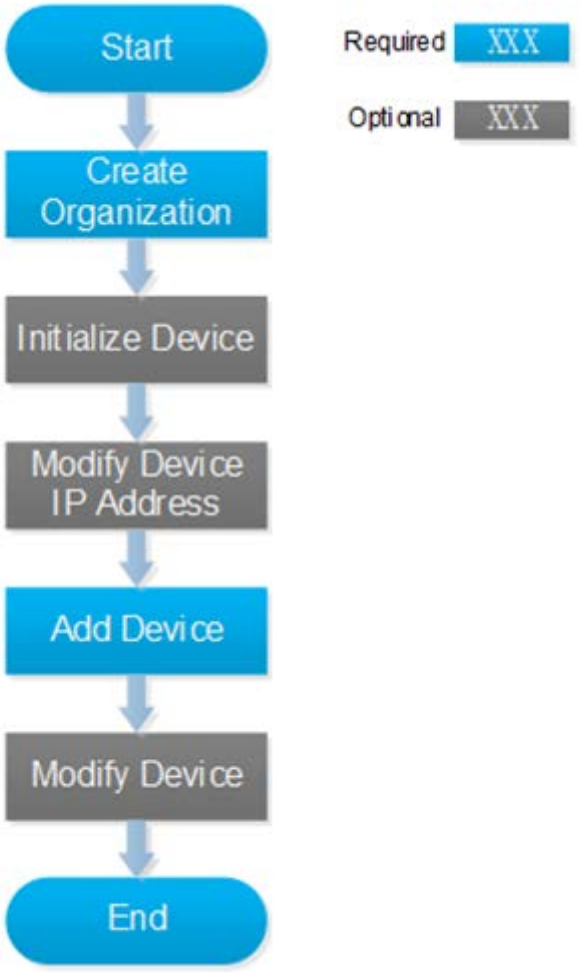
Figure 4-12 Network disk



4.1.2 Managing Device

After device is added on the server, you can operate device remotely by server. The flow of device management is shown in Figure 4-13.

Figure 4-13 Device management flow



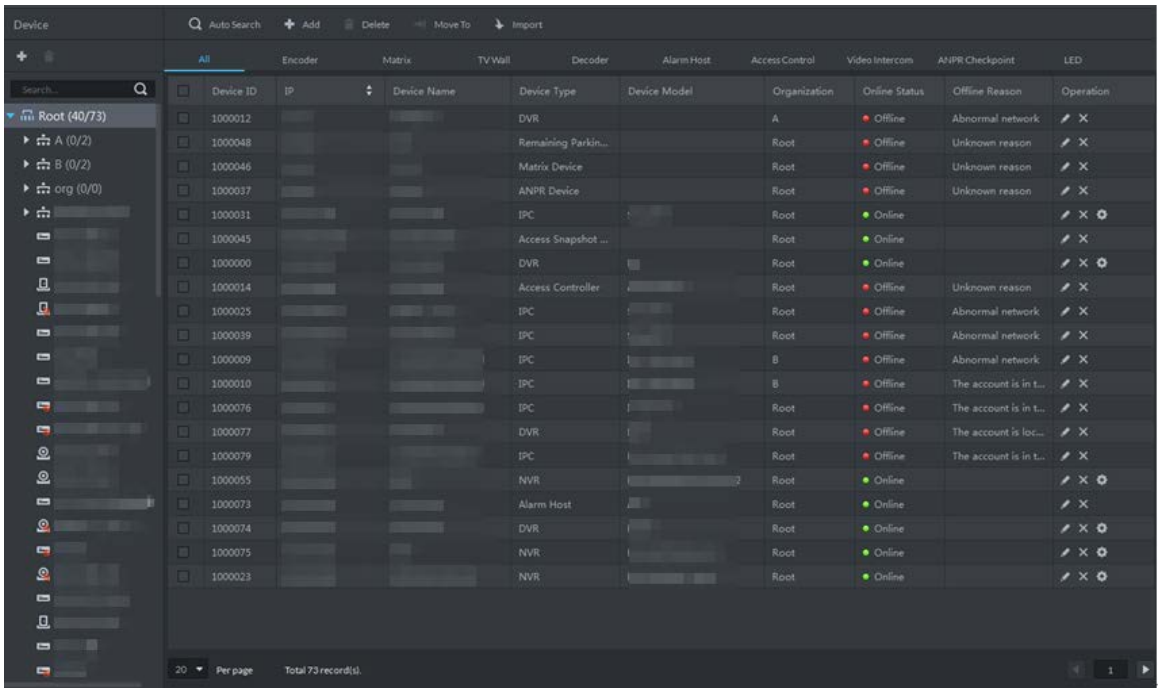
4.1.2.1 Creating Organization

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

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

The **Device** interface is displayed. See Figure 4-14. The device is online if online status is green. Device is offline if online status is red.

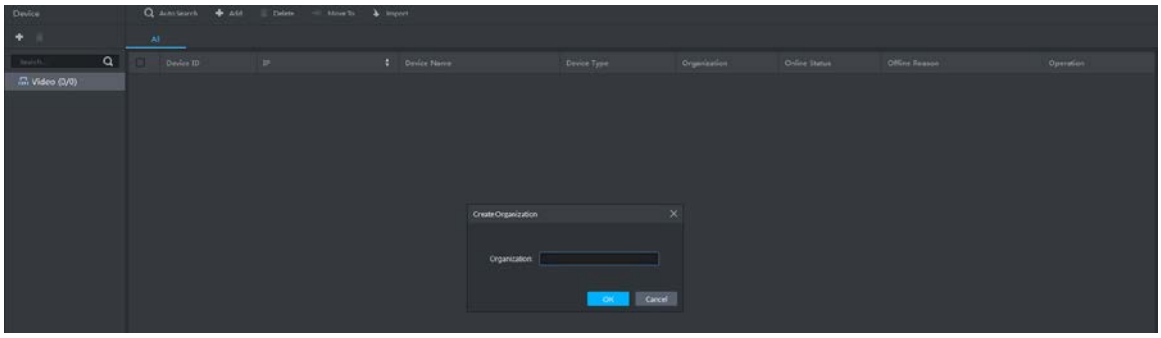
Figure 4-14 Device



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

The interface of **Create Organization** is displayed. See Figure 4-15.

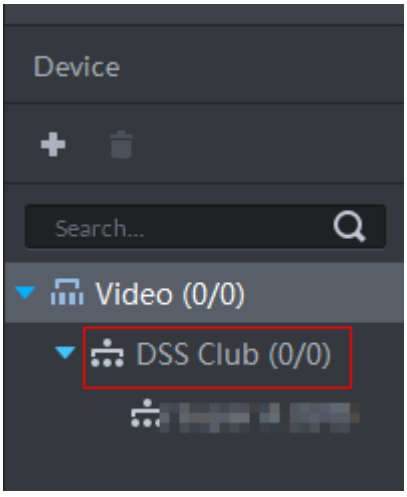
Figure 4-15 Create organization



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

The info of added organization is displayed. See Figure 4-16.

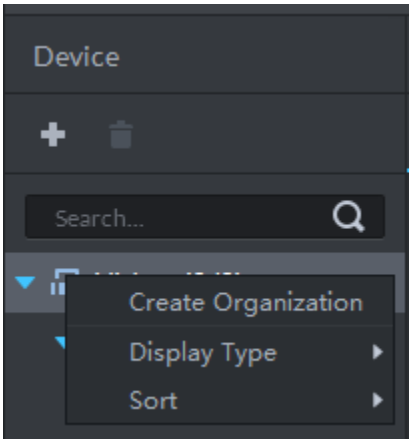
Figure 4-16 Organization list



More operations of organization are shown as follows:

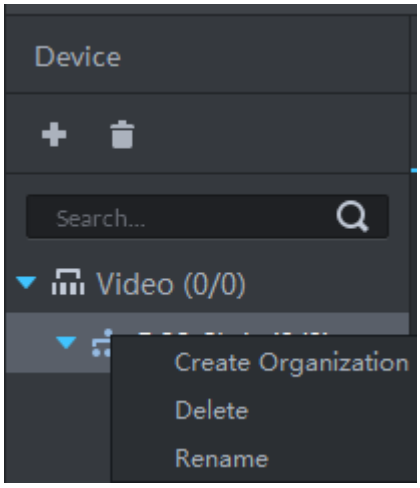
- Root node supports creating subordinate organization; Set display type means setting device display by name or IP; Set sort means setting sort mode of all devices and organizations under root node, including ascending, descending and default order. See Figure 4-17.

Figure 4-17 Root node operation



- Child node organization supports creating subordinate child node organization; delete and rename organization. See Figure 4-18.

Figure 4-18 Child node organization



4.1.2.2 Initializing Device

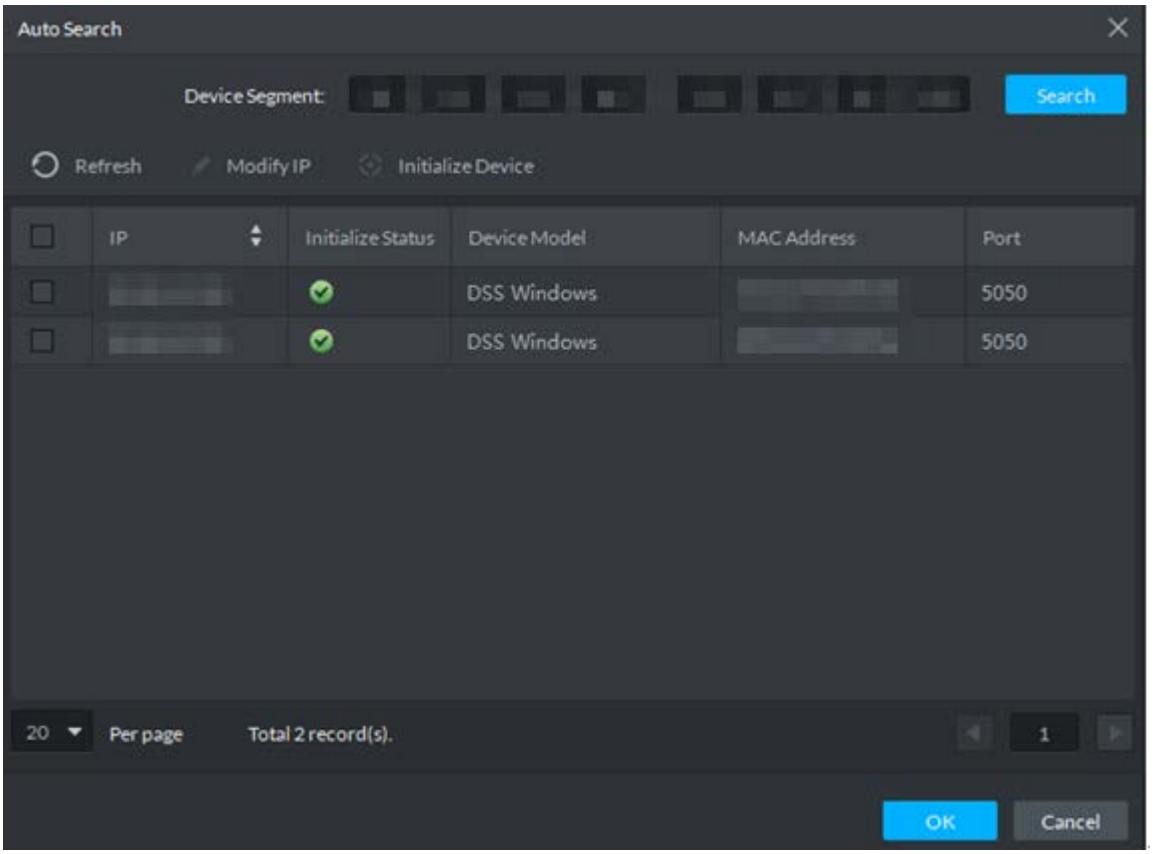
The device is required to configure admin account password and security questions after being delivered out of factory; otherwise, it cannot be used normally. The platform supports initializing device remotely.

Step 1 Click **Device** on the client homepage.
The **Device** interface is displayed.

Step 2 Click Auto Search.
The **Auto Search** interface is displayed.

Step 3 Enter start IP and end IP, click **Search**.
The search results are displayed.

Figure 4-19 Search result

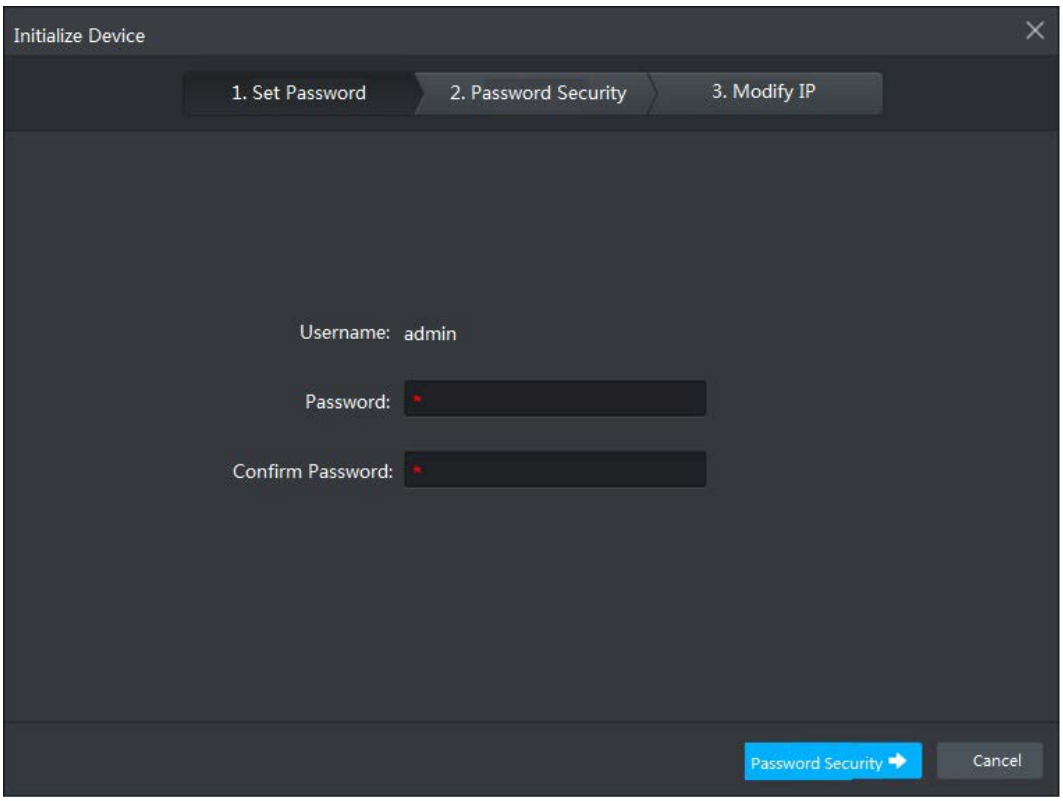


Step 4 Select an uninitialized device, click **Initialize Device**.

The **Set Password** is displayed. See Figure 4-20.

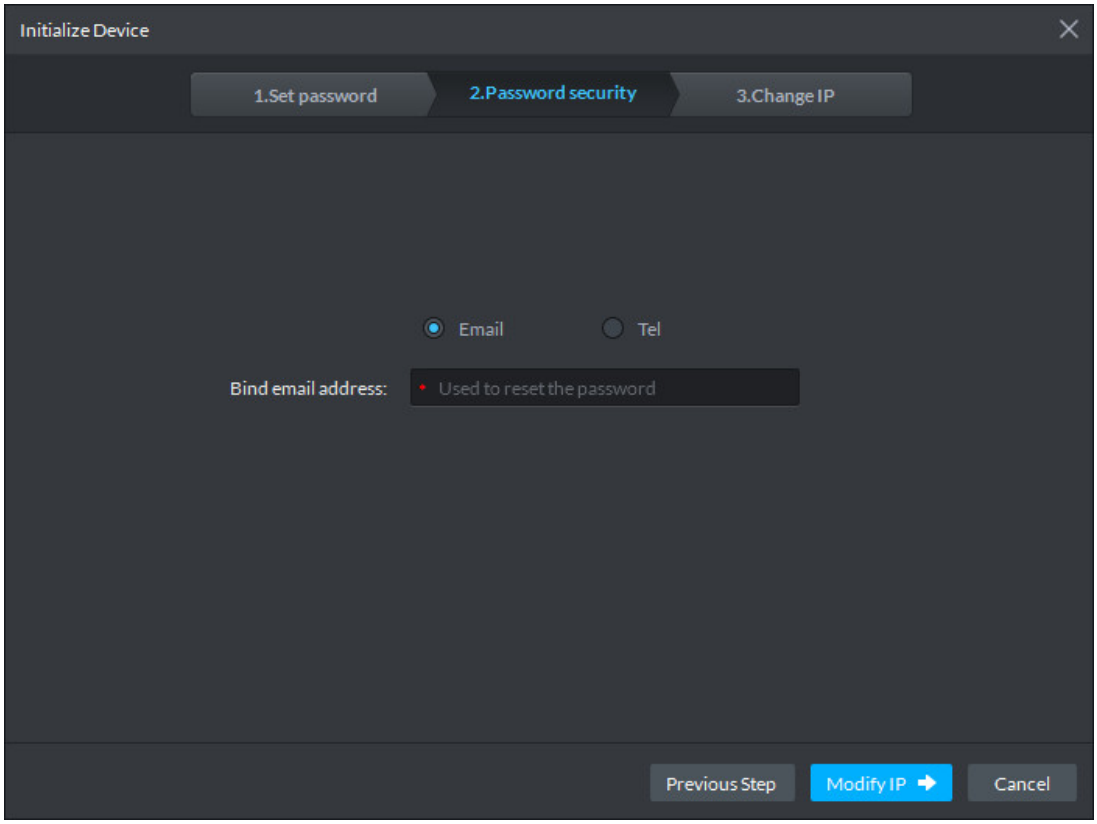
Several devices can be initialized together.

Figure 4-20 Set password



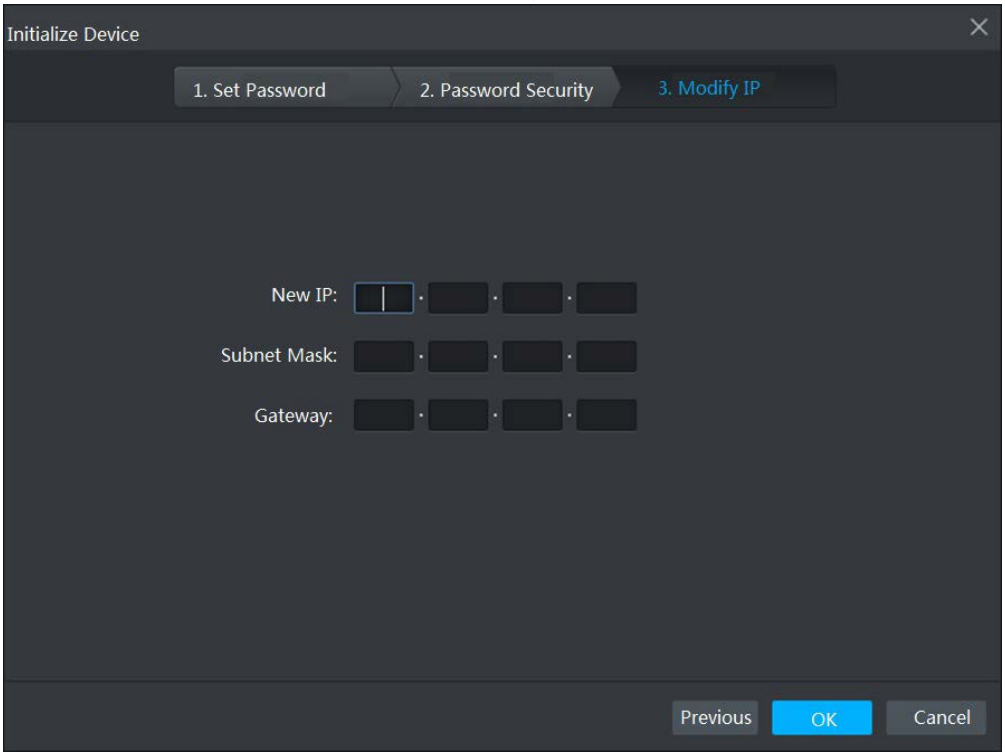
Step 5 Enter password, click **Password Security**. See Figure 4-21.

Figure 4-21 Password security



Step 6 Select email or phone, enter corresponding email address or phone number, click **Modify IP**. The **Modify IP** interface is displayed. See Figure 4-22.

Figure 4-22 Modify IP



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

4.1.2.3 Modifying Device IP Address

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

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

The **Device** interface is displayed.

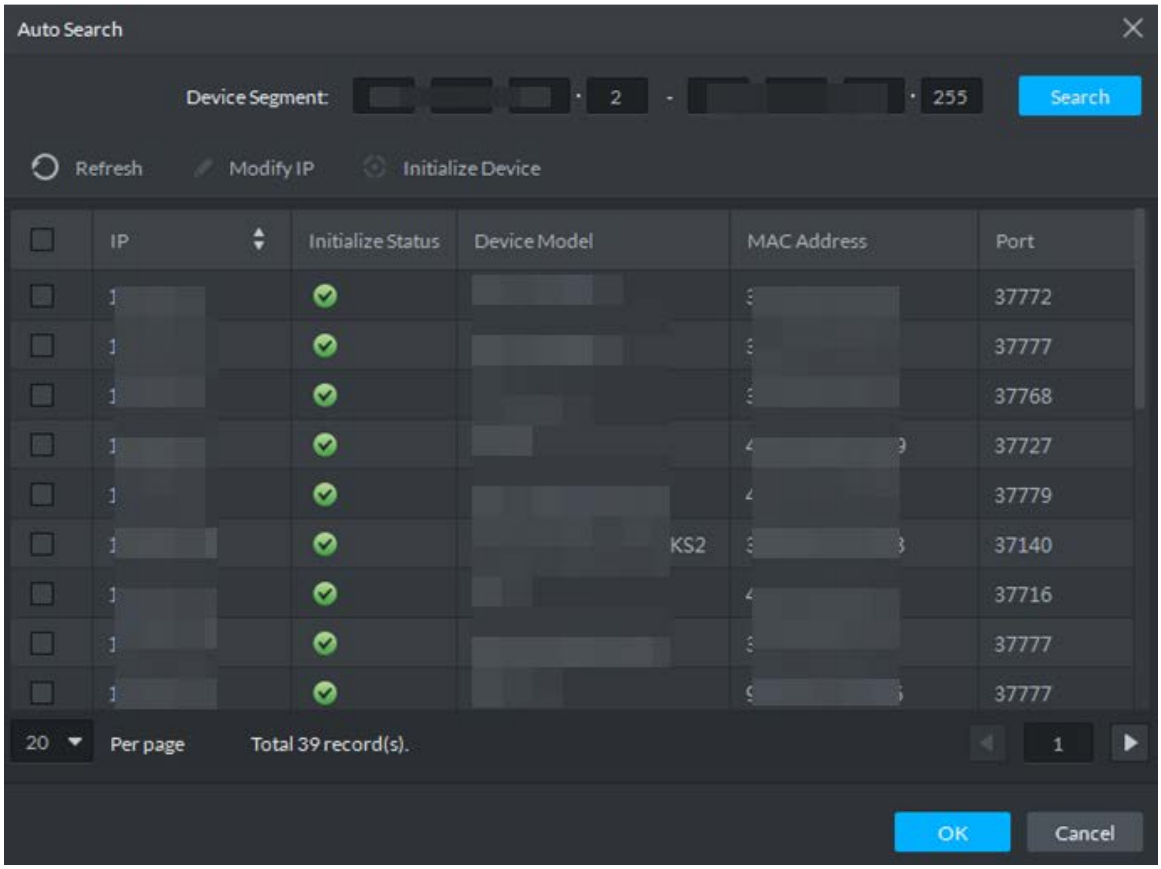
Step 2 Click Auto Search.

The **Auto Search** interface is displayed.

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

The search result is displayed. See Figure 4-23.

Figure 4-23 Search result



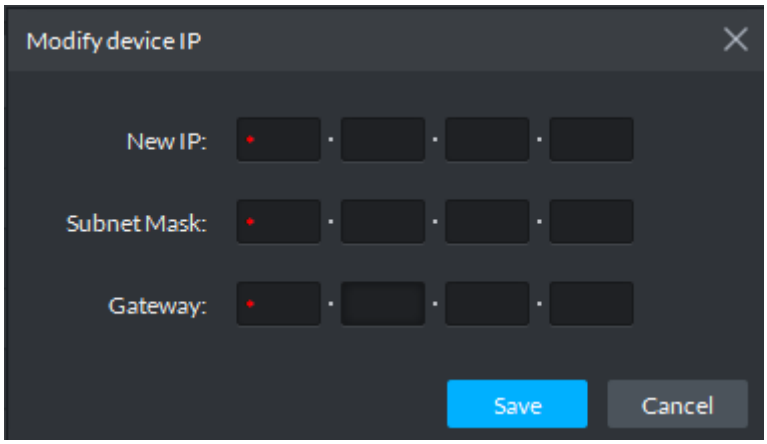
Step 4 Select device whose IP address needs to be modified, click **Modify IP**.

The interface of **Modify Device IP** is displayed.

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

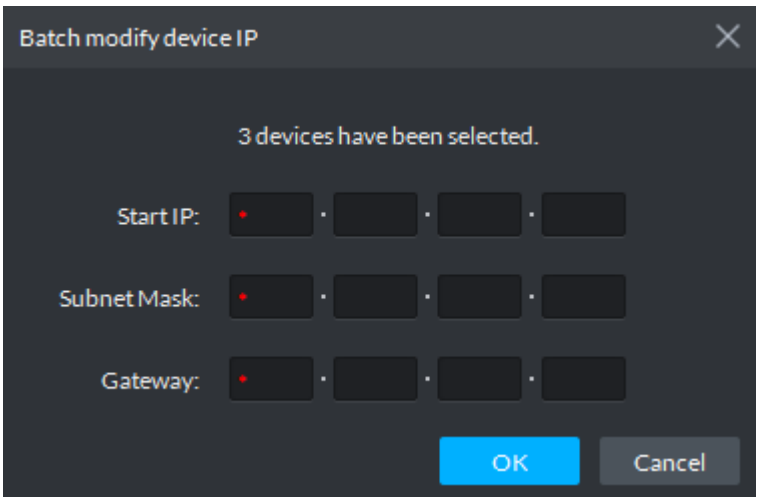
- When you select one device, the system pops out the **Modify Device IP** dialog box. See Figure 4-24.

Figure 4-24 Singly modify device IP



- When you select several devices, the system pops out the dialog box of **Batch Modify Device IP**. See Figure 4-25.

Figure 4-25 Batch modify device IP



Step 6 Set new IP address or start IP, subnet mask and gateway.
Modify in batches, IP address increases by 1 sequentially.

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

4.1.2.4 Adding Device

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

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

4.1.2.4.1 Searching and Adding Device

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

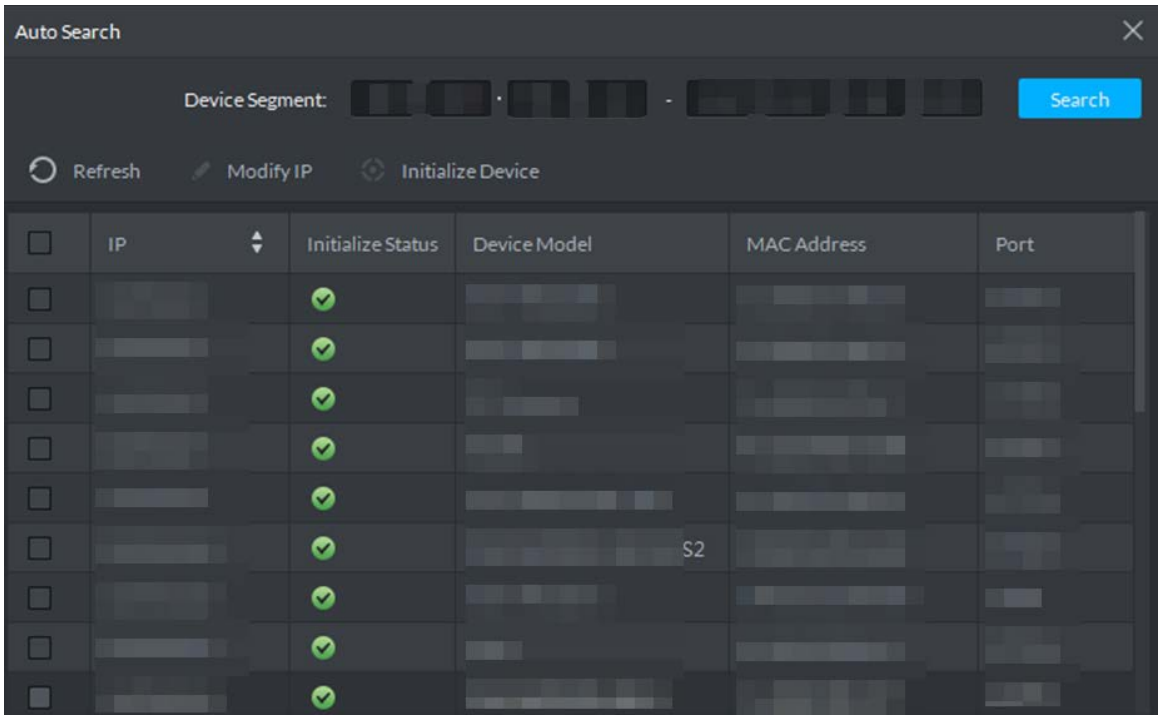
Step 1 Click **Device** on the client homepage.
The **Device** interface is displayed.

Step 2 Click Auto Search.

The interface of **Auto Search** is displayed. See Figure 4-26. The system searches the device with the same segment as server by default.

- Click **Refresh** to refresh device info.
- Select a device, click Modify IP and modify device IP address. For details, see"4.1.2.3 Modifying Device IP Address."
- Select uninitialized device, click **Initialize Device** and initialize device. For details, see"4.1.2.2 Initializing Device."

Figure 4-26 Auto search device



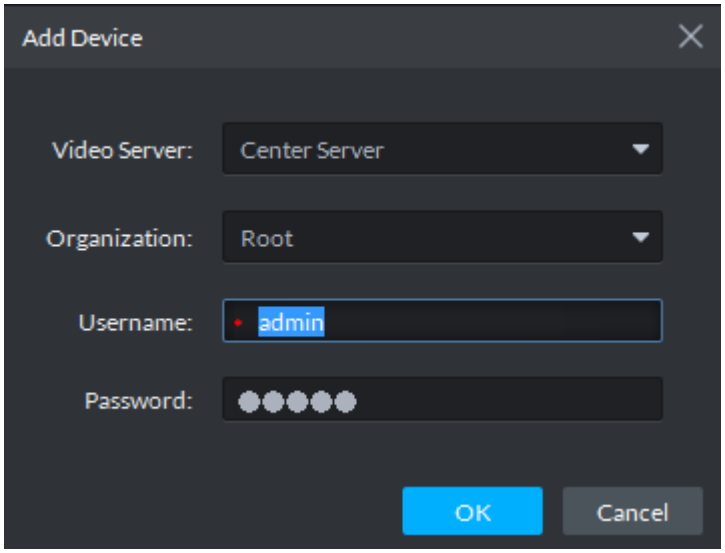
Step 3 Enter searched start IP and end IP, click **Search**.

The search results are displayed.

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

The interface of **Add Device** is displayed. See Figure 4-27.

Figure 4-27 Add Device



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

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

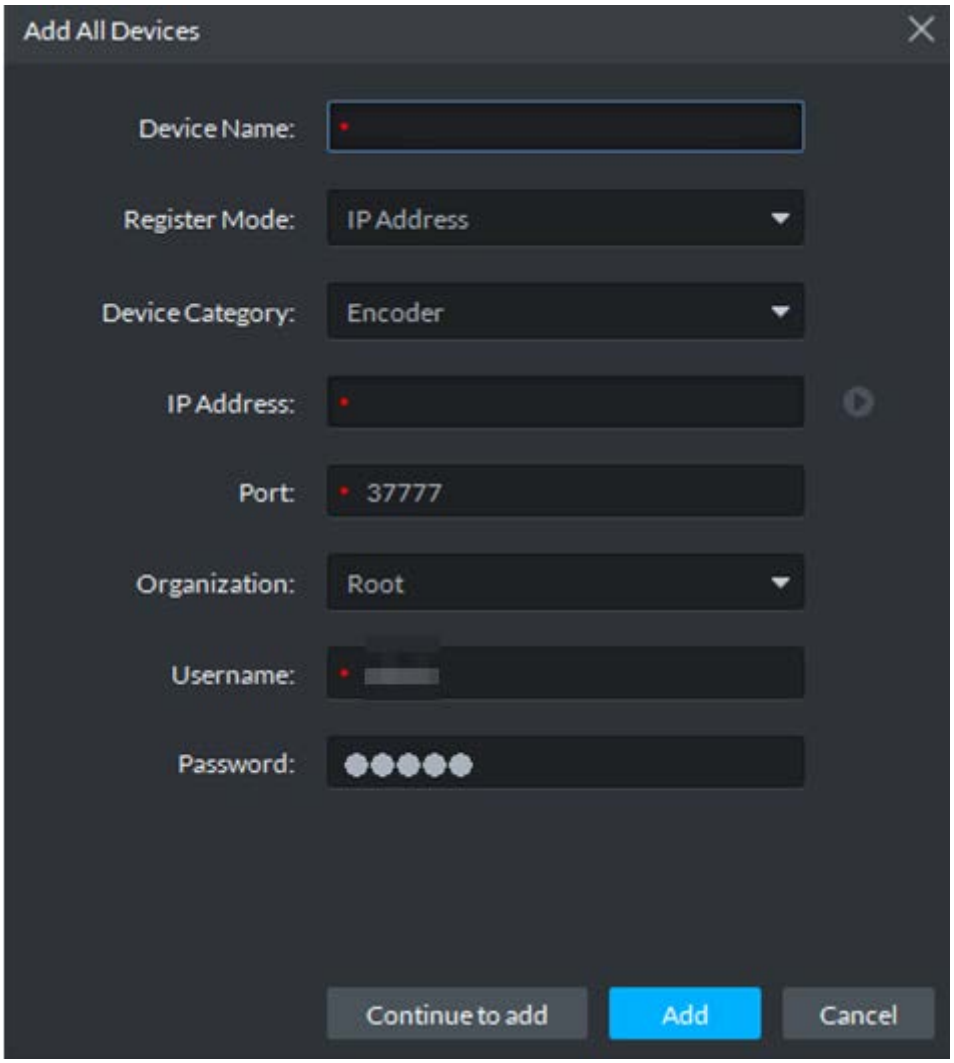
4.1.2.4.2 Adding Device Manually

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

Step 1 Click **Device** on the client homepage.
The **Device** interface is displayed.

Step 2 Click **Add**.
The interface of **Add All Devices** is displayed. See Figure 4-28.

Figure 4-28 Manually add device



Step 3 Set parameters, for more details, refer to Table 4-1.

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

Table 4-1 Parameter description

Parameter	Description
Device Category	Select according to the type of added device, currently support adding access control, encoder, decoder, video wall, ANPR, matrix, LED, alarm host and video intercom.
Register Mode	Support registration by following methods: ● IP address Add device to platform by adding device IP. ● Onvif If device enables Onvif protocol, then you can add device to platform by Onvif protocol. Generally it can be used when adding third-party device.

Parameter	Description
Port	TCP protocol communication provides service port, and keeps it in accordance with added device.
Organization	Select organization node of added device.
IP Address	When register by IP address or Onvif mode, set the IP address of added device.
SN	When register by serial number mode, set the serial number of added device.
Username	Enter login username and password of added device.
Password	
Decode mode	Select according to the decode mode of added device: ● Pull Decoder extracts stream from platform by url address, the decode mode of device is pull. ● Direct Decoder extracts stream directly from encoder, the decode mode is direct for device, under this mode; you need to add decoder IP address when trusted list is added by device. ● Push VMS pushes stream directly to decoder, currently only support NVD without combination screen, the mode is not supported by matrix, video wall or NVD under combination mode.
Support Combination	Select when added device supports combination.
Picture Server	Select storage location of picture reported by ANPR.
LED Type	Support added LED including general screen and free parking screen, select corresponding device type according to the accessed device.

Step 4 Click **Add**.

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

4.1.2.4.3 Importing Device

If the video intercom template already exists and its information is complete, you can quickly add device to platform by importing existing file or account.

Import Local File

Import video intercom template file, and add device to the platform quickly.

Please contact technical support for video intercom template.

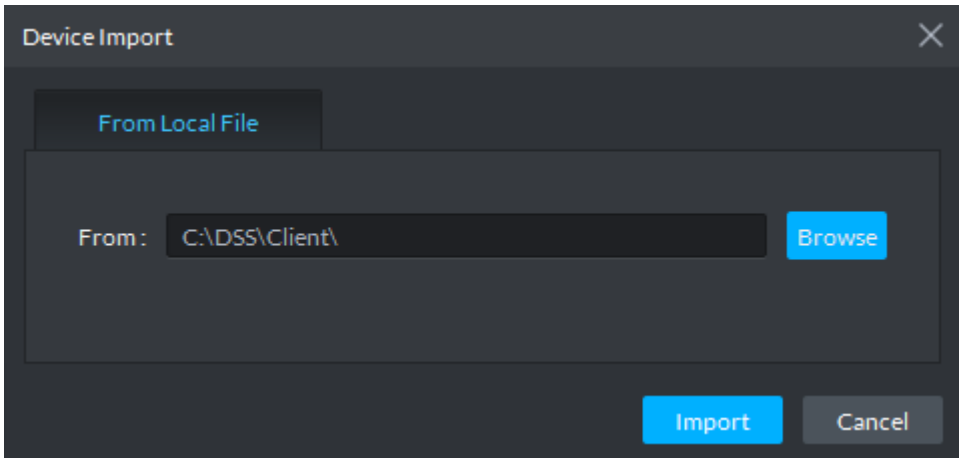
Step 1 Click **Device** on the client homepage.

The **Device** interface is displayed.

Step 2 Click **Import**.

The **Device Import** interface is displayed. See Figure 4-29.

Figure 4-29 Import from local file



Step 3 Click **Browse**, select device info file and click **Import**.
The system shows import results.

4.1.2.5 Editing Device

4.1.2.5.1 Modifying Device Info

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

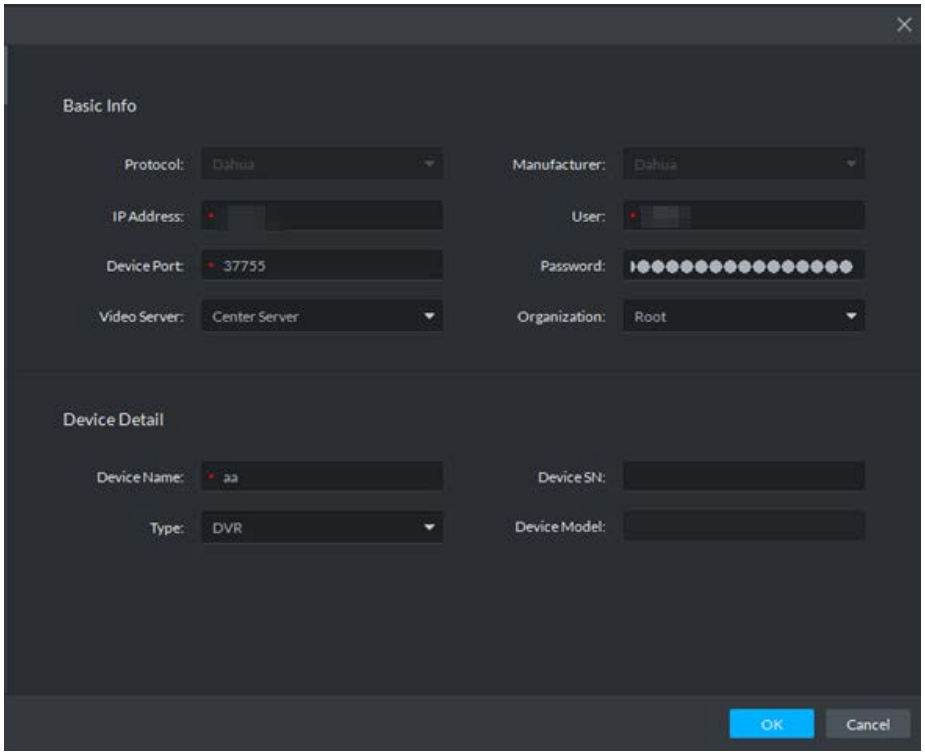
- Please modify device according to the following method if you want to modify info except device IP address, port number, user and password.

Step 1 Click **Device** on the client homepage.
The **Device** interface is displayed.

Step 2 Click  next to device list.

The **Edit Device** interface is displayed. See Figure 4-30.

Figure 4-30 Edit device



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

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

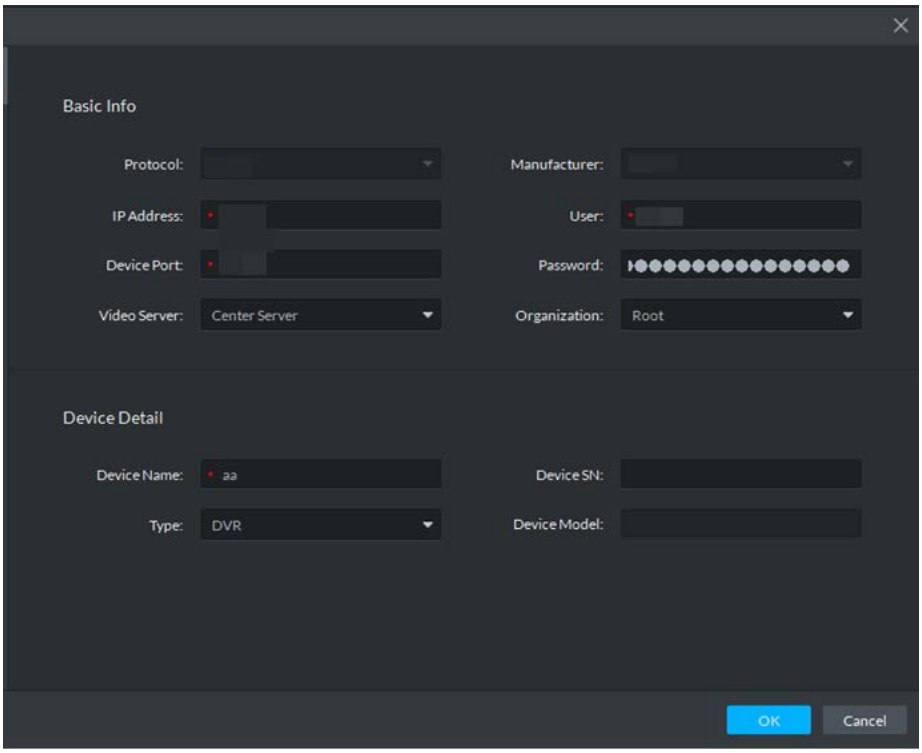
Step 1 Click **Device** on the client homepage.

The **Device** interface is displayed.

Step 2 Click  next to the device list.

The **Edit Device** interface is displayed. See Figure 4-31.

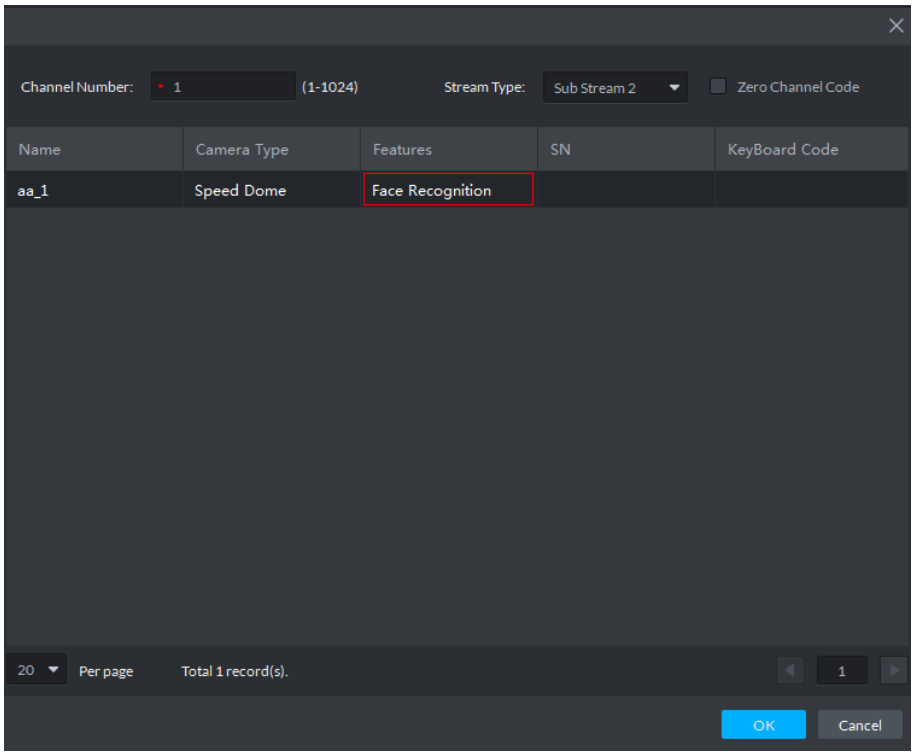
Figure 4-31 Modify device basic info



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

Step 4 Click **Video Channel** tab, modify channel number and stream type, and see Figure 4-32. You need to enable corresponding intelligent function if the added device owns intelligent functions. For example, the added camera is face recognition camera, the camera is required to detect face, and then you need to set **Features** as **Face Recognition**.

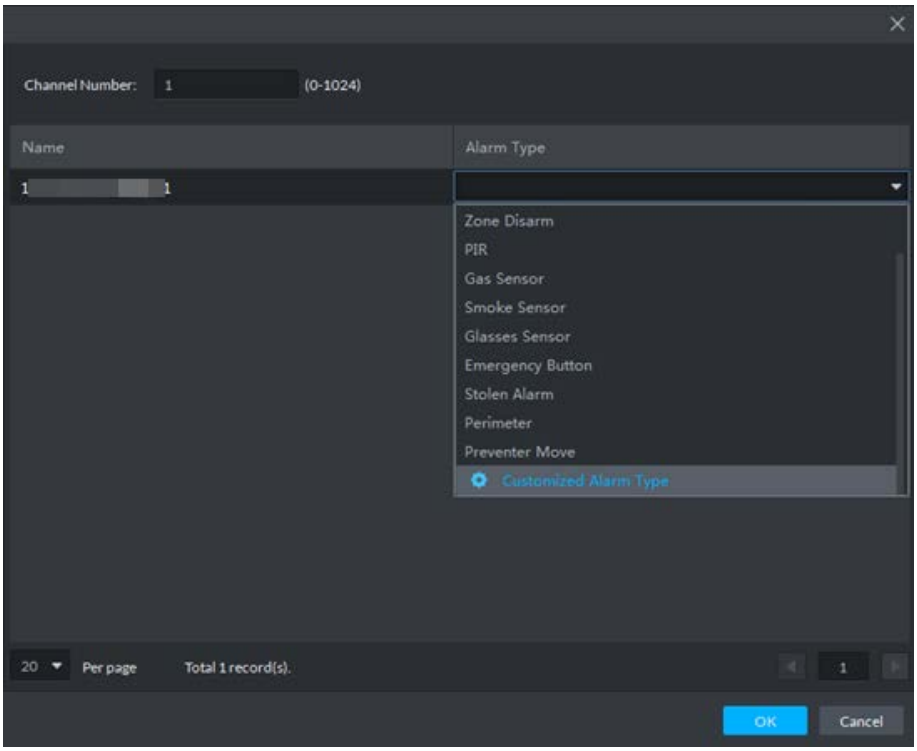
Figure 4-32 Video channel



Step 5 Click **Alarm Input Channel** tab and modify alarm input channel number. See Figure 4-33. Alarm type supports custom. Select **Customized Alarm Type** from the drop-down box of

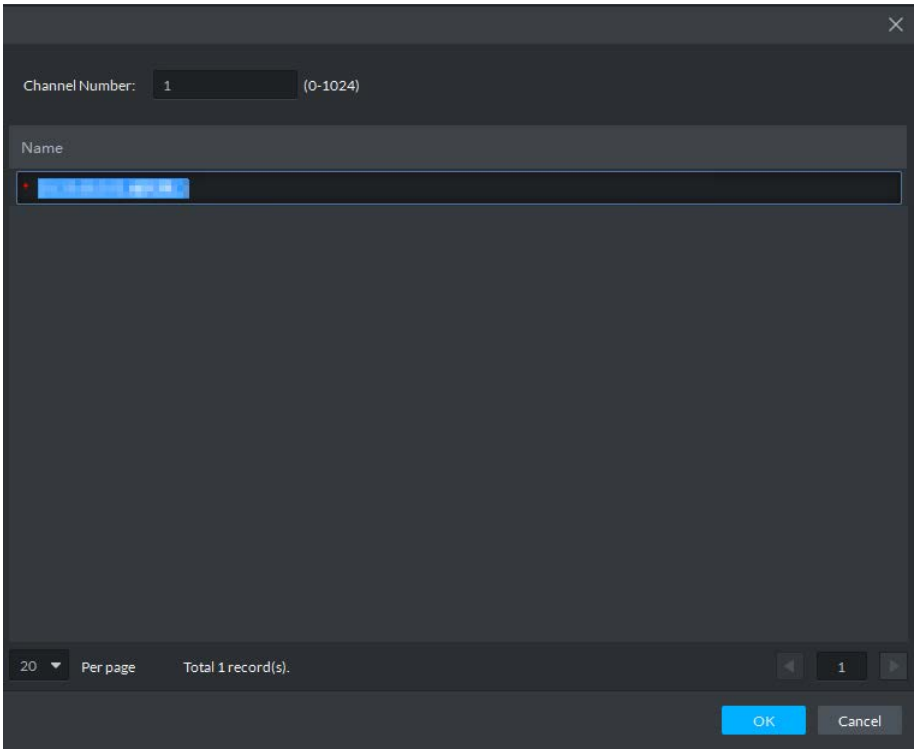
Alarm Type, set needed alarm type, used to quickly identify alarm. After config, on the event config interface, you can configure corresponding alarm event for corresponding alarm input.

Figure 4-33 Alarm input channel



Step 6 Click **Alarm Output Channel** tab, modify device alarm output channel number, and double click to modify corresponding channel name. See Figure 4-34.

Figure 4-34 Alarm output channel



Step 7 Click **OK**.

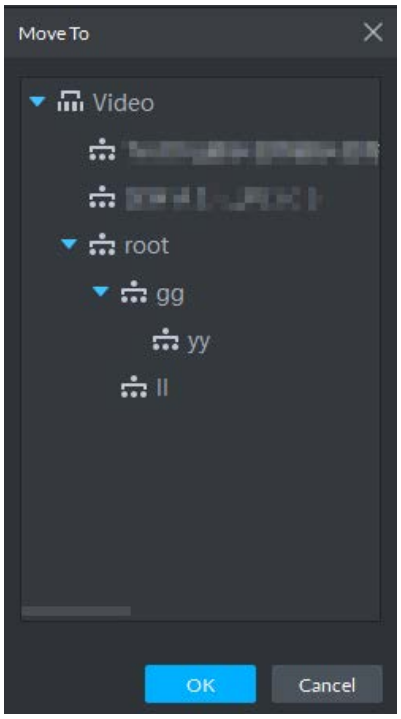
4.1.2.5.2 Modifying Device's Organization

You can move device from one organization to another.

Step 1 Click **Device** on the client homepage.
The **Device** interface is displayed.

Step 2 Select the device to be moved, click **Move To**.
The **Move To** interface is displayed. See Figure 4-35.

Figure 4-35 Move device



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

4.1.3 Adding User

4.1.3.1 Adding Basic User

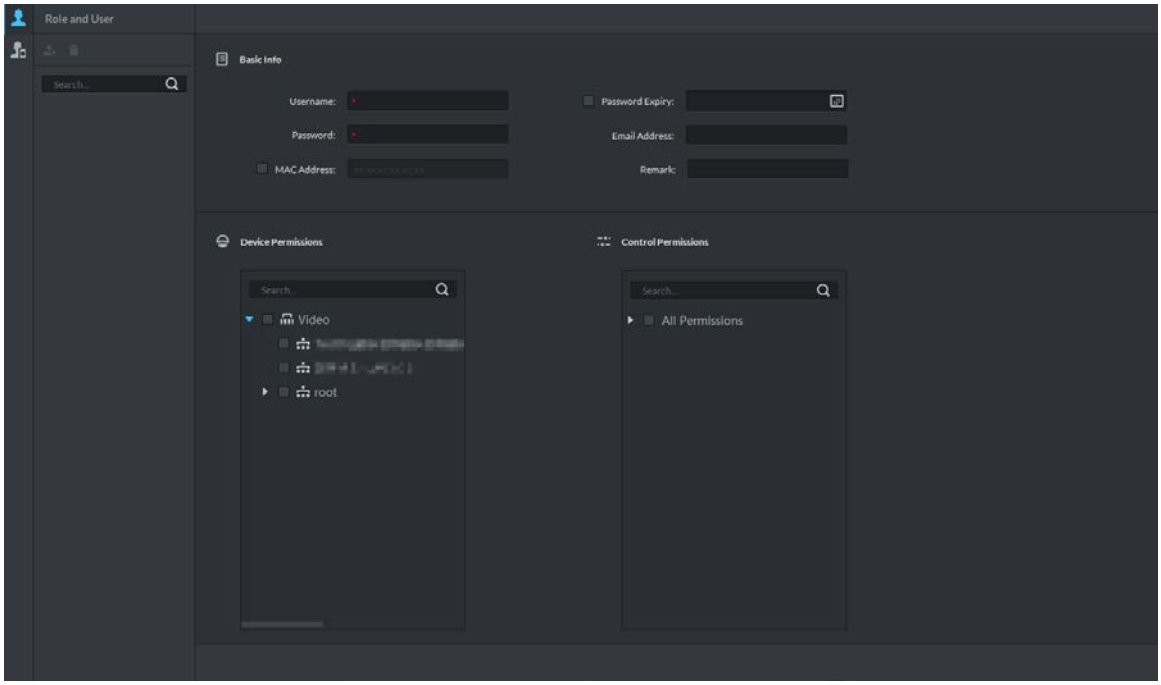
Create users with different permissions for platform and make sure the platform is safe. The platform provides three types of user, including administrator, advanced user and general user, different users have different permissions. Each type of user can adjust permission within certain permission range.

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

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

Step 1 Click **User** on the client homepage.
The **User** interface is displayed. See Figure 4-36.

Figure 4-36 User



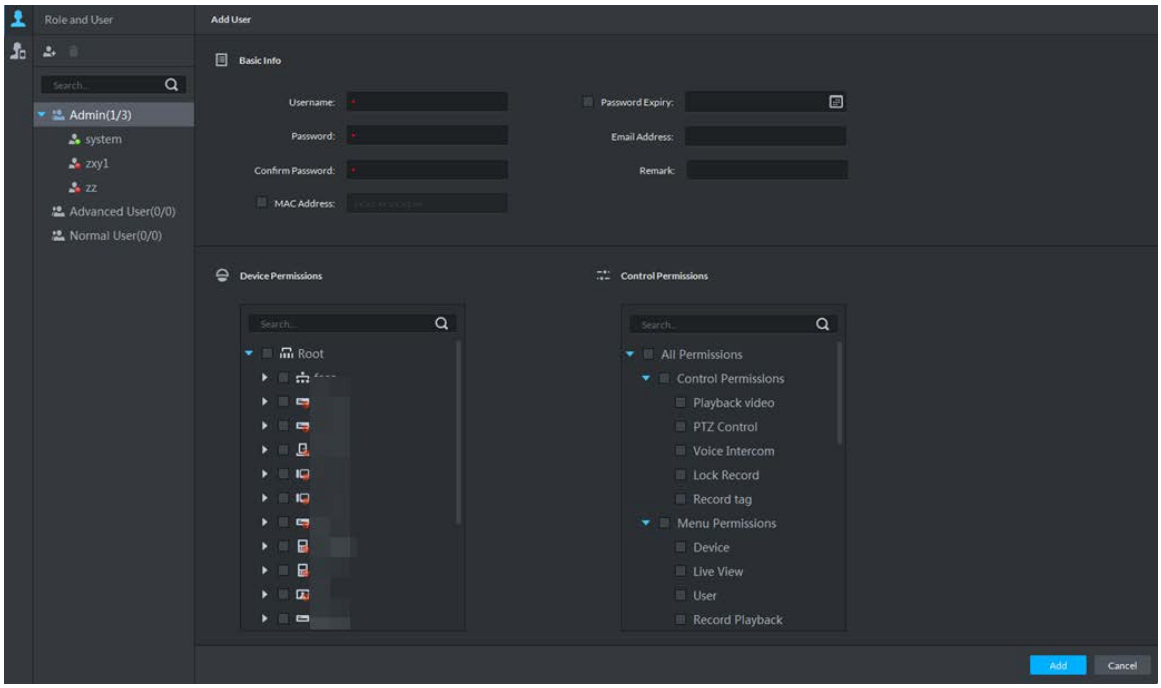
Step 2 Click  .

The **User** interface is displayed.

Step 3 Select user type from the left list, click  .

The **Add User** interface is displayed. See Figure 4-37.

Figure 4-37 Add user



Step 4 Set user info, select device and permission that can be used by user, click **Add**.

4.1.3.2 Managing APP User

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

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

Click  on the **User** interface. The APP User interface is displayed, and shows info of all registered APP users. See Figure 4-38. For operation details, see Table 4-2.

Figure 4-38 Enter APP user interface

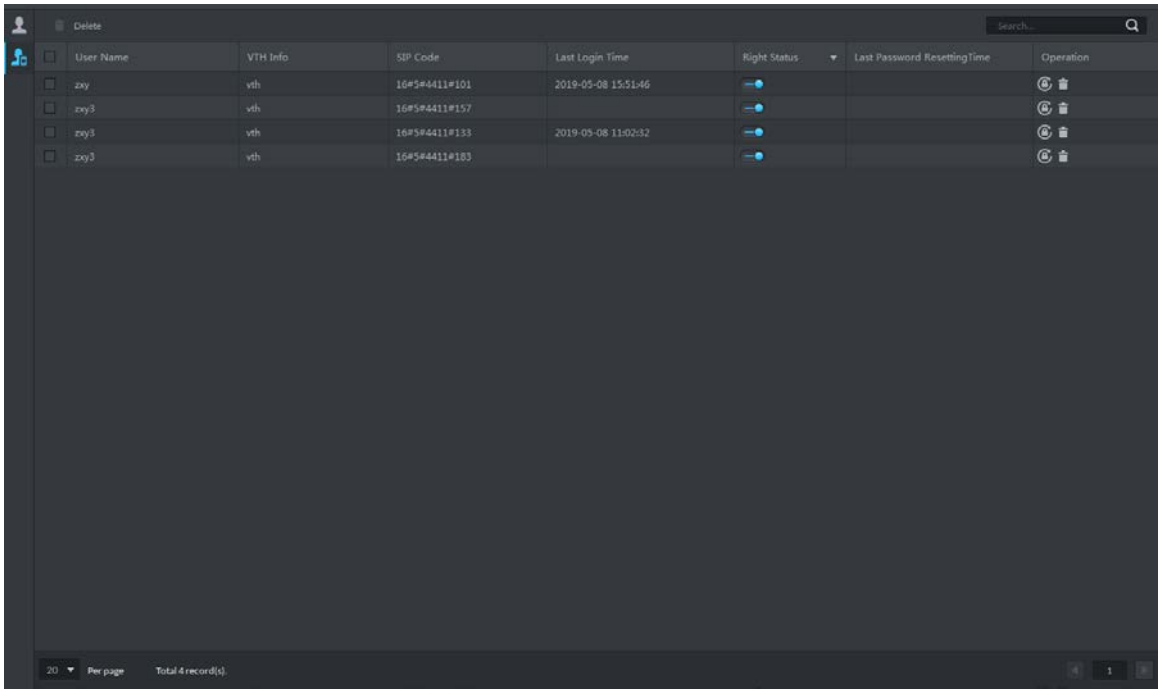


Table 4-2 Operation description

Operation	Description
Freeze APP User	After APP user is freezed, APP user cannot log in within 600s. ON means normal, OFF means freeze, both can be mutually switched. The account can also be freezed if password attempts exceed 5 by APP user.
Modify APP User Login Password	Click and enter new password the interface of **Reset Password**, click **OK**. Password length is 8~16 characters, must include number and letter. means showin password; means enabling password protection and hiding password. Click icon to switch mutually.
Delete APP User	Click next to APP user or select APP user, you can select several users, click **Delete** and delete users according to prompt on interface.

4.1.4 Setting Alarm Event

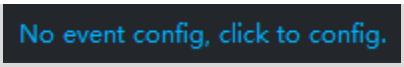
Device reports all alarm messages. Alarm messages can be responded only when the platform configures corresponding alarm linkage scheme. Linkage actions are shown as follows when responding to alarm.

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

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

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

Step 1 Click **Config** on the client homepage.
The **Config** interface is displayed.

Step 2 Select device or device channel from left device tree, click **Event Config**. See Figure 4-39.
The **Event** interface is displayed. See Figure 4-40.
Select root node on the left device tree, device event config is displayed on the right. If no config, click 

or  and enter config interface.

Figure 4-39 Config

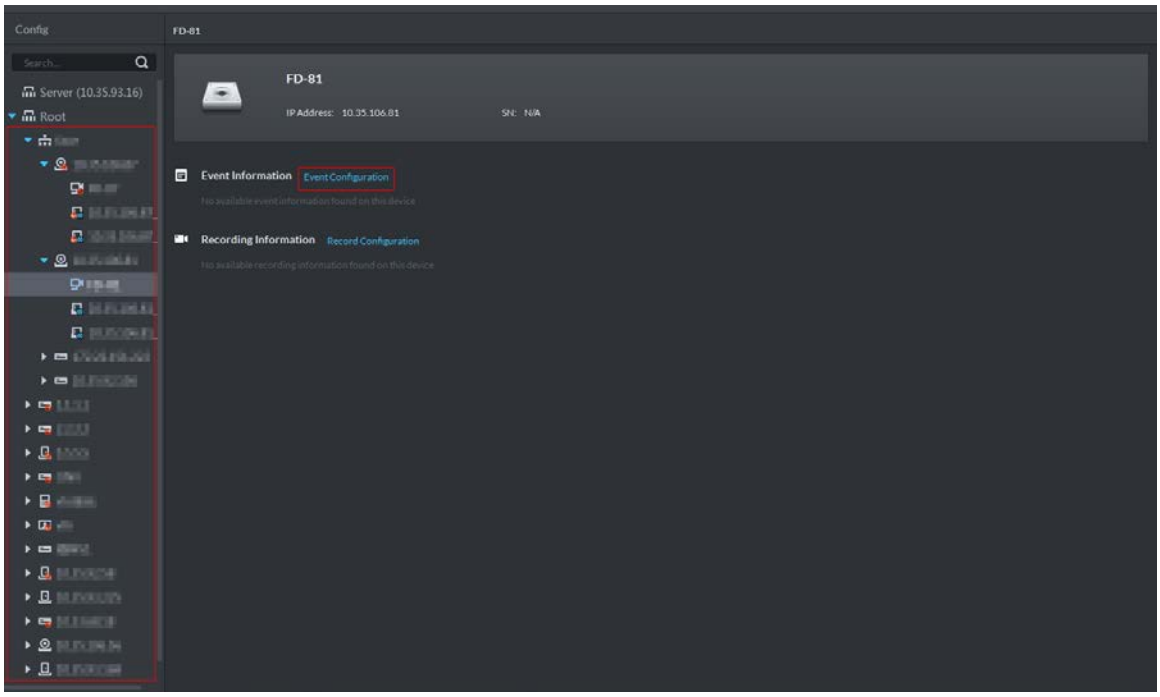
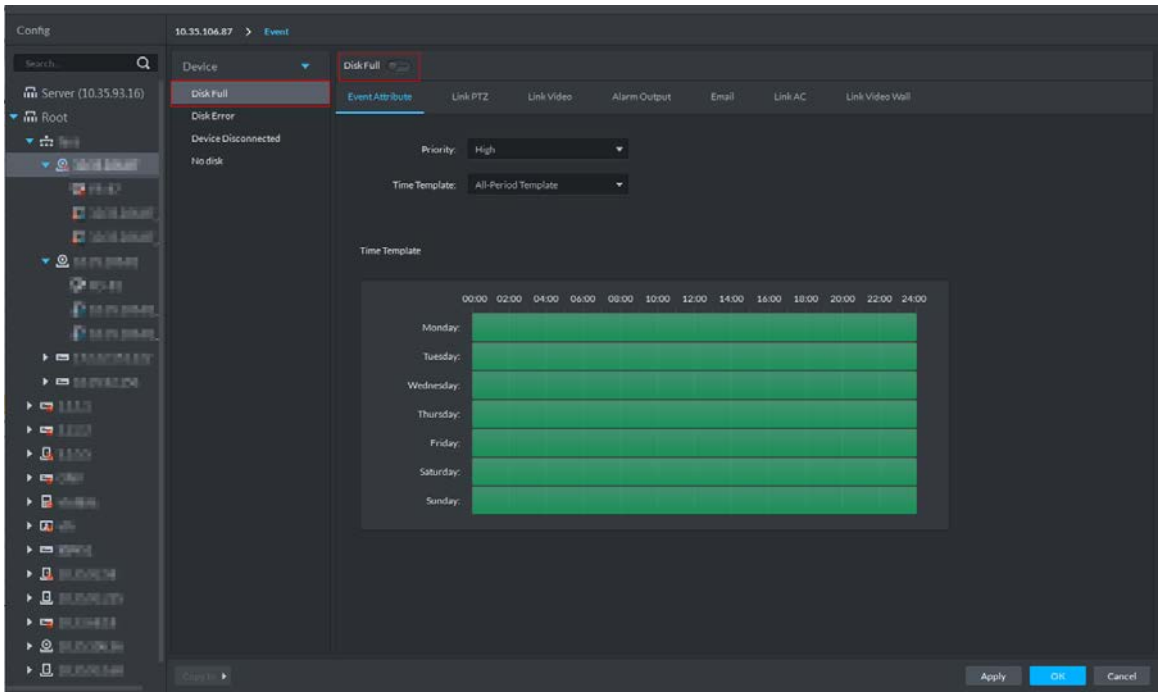


Figure 4-40 Event



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

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

Step 4 Set event attribute

Include setting alarm event priority and effective period of event.

- Set Event Attribute

1) Click Event Attribute tab.

The **Event Attribute** interface is displayed. See Figure 4-40.

2) Select priority.
Priority is only used to recognize alarm message.

3) Select time template, you need to configure again if default time template fails to meet requirement.
After selected, the time info set by time template is displayed below.

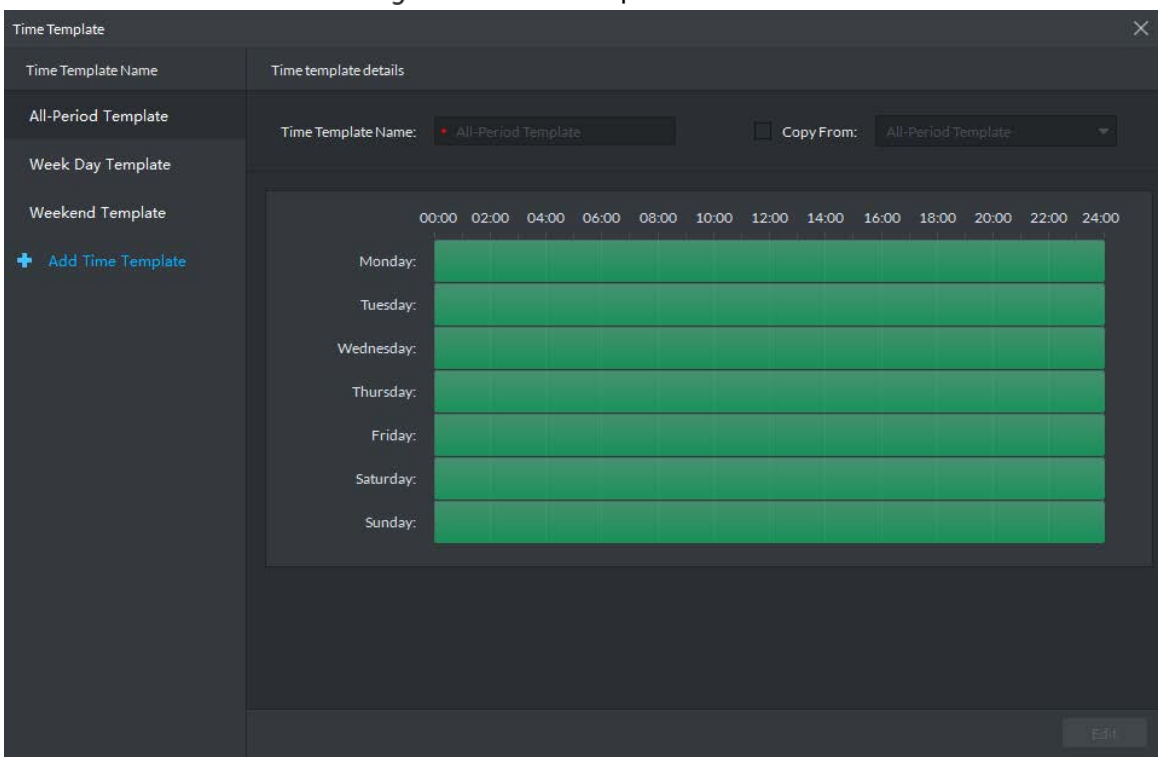
- Set Time Template

Default time templates include all-period template, week day template and weekend template. If the default template fails to meet requirement, please add new template according to the following steps.

1) Click Event Attribute tab.
The **Event Attribute** interface is displayed. See Figure 4-40.

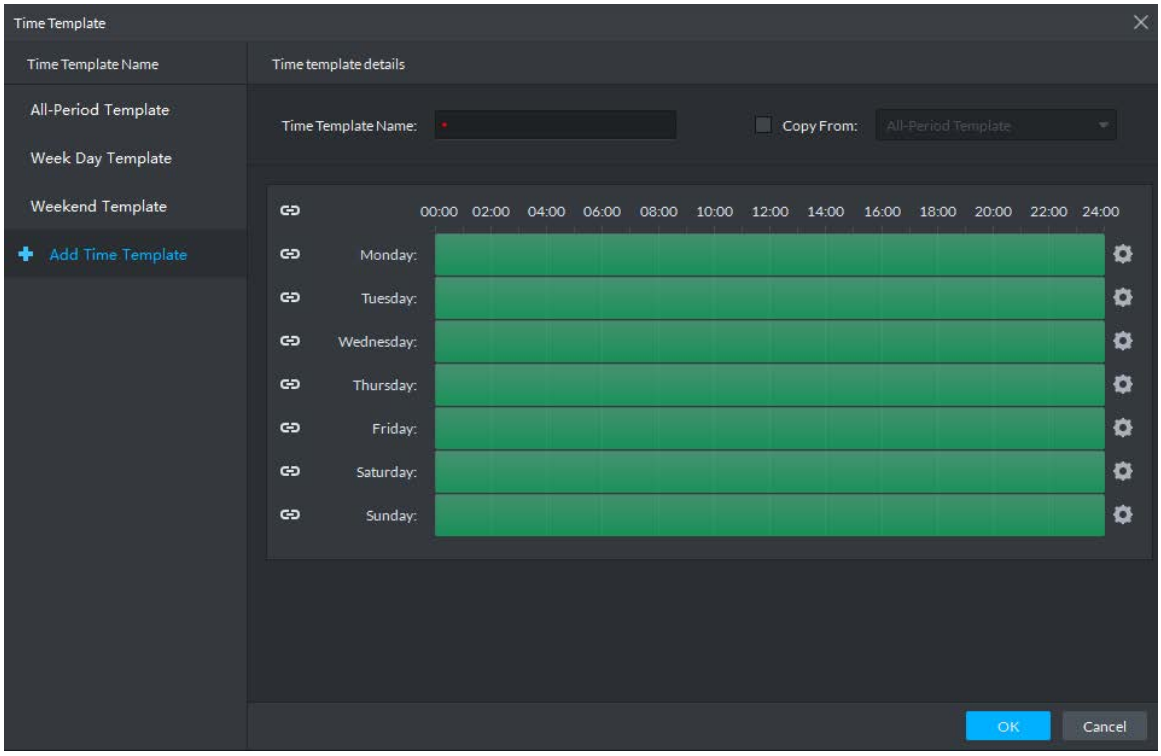
2) Click Time Template and select **Manage Time Template**.
The **Time Template** interface is displayed. See Figure 4-41.

Figure 4-41 Time template



3) Click Add Time Template.
The **Time Template Details** interface is displayed. See Figure 4-42.

Figure 4-42 Add time template



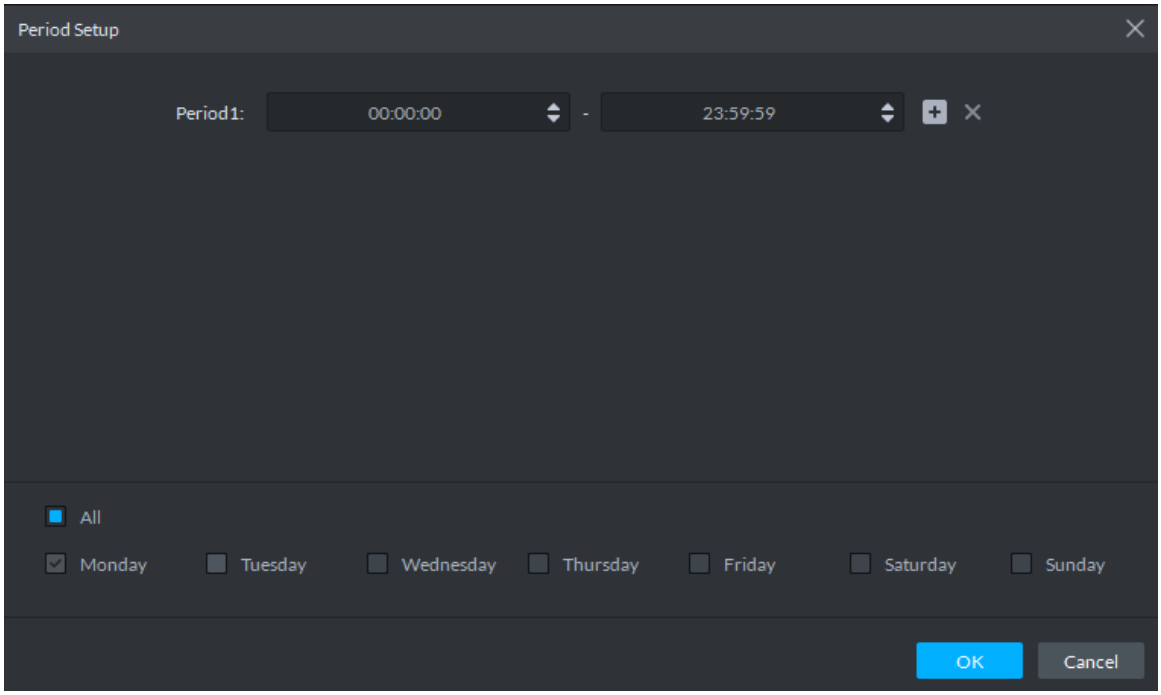
4) Enter time template name, and set time by three following methods.

◇ Select **Copy**, select existed default template, and copy time directly from default template.

◇ Use mouse and drag time line, if time is set, then eraser is displayed, and erase the time of location where you drag; if time is not set, then pen is displayed, and add time of dragged location.

◇ Click  , set period and week, click  and add several periods, click  to delete time. Click OK after setting is completed, save and return to the interface of Time Template Details. See Figure 4-43.

Figure 4-43 Period setup



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

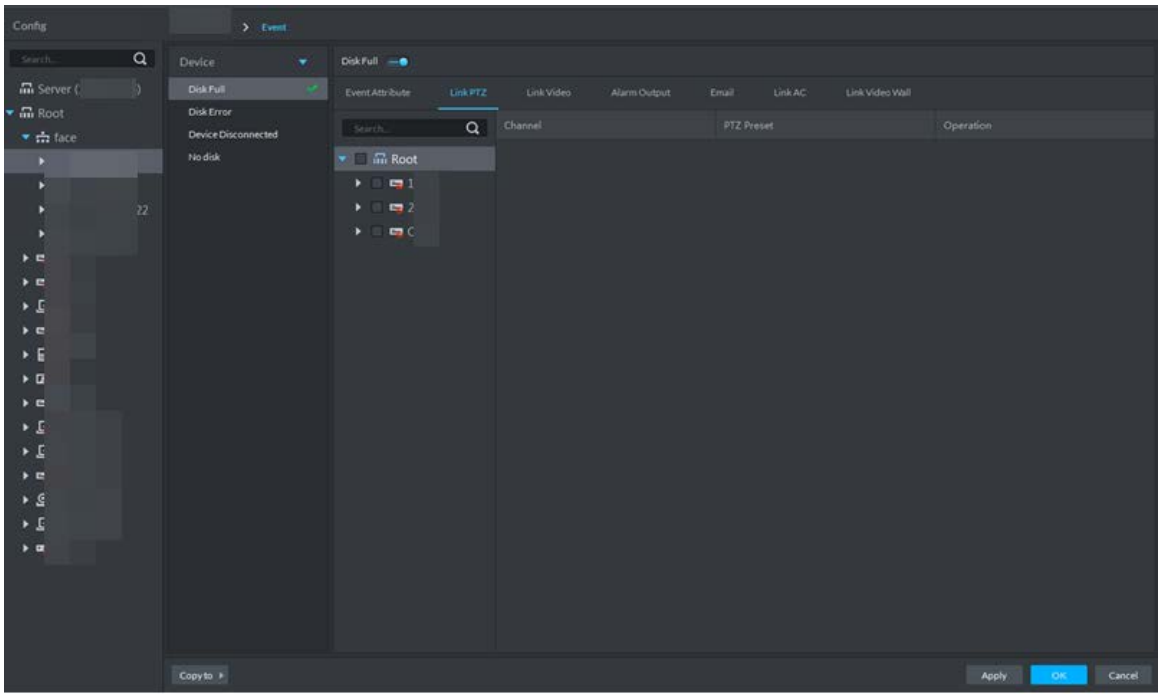
Step 5 Link PTZ.

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

1) Click **Link PTZ** tab.

The **Link PTZ** interface is displayed. See Figure 4-44.

Figure 4-44 Link PTZ



2) Select PTZ device from device tree.

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

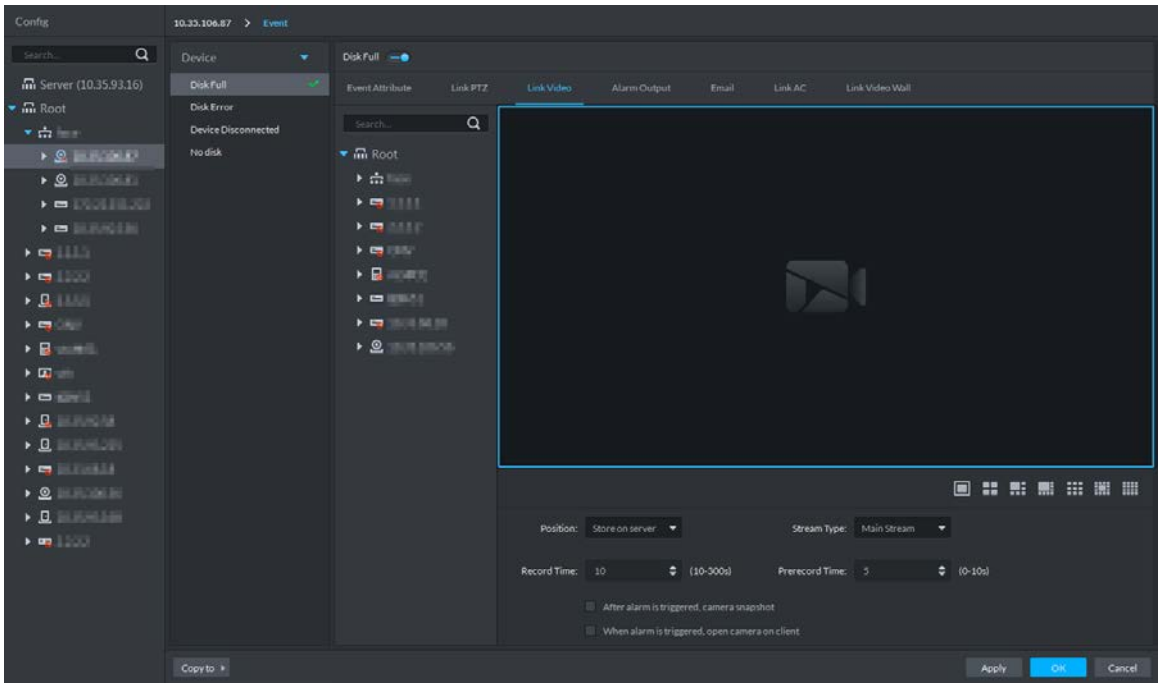
Step 6 Link Video.

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

1) Click **Link Video** tab.

The **Link Video** interface is displayed. See Figure 4-45.

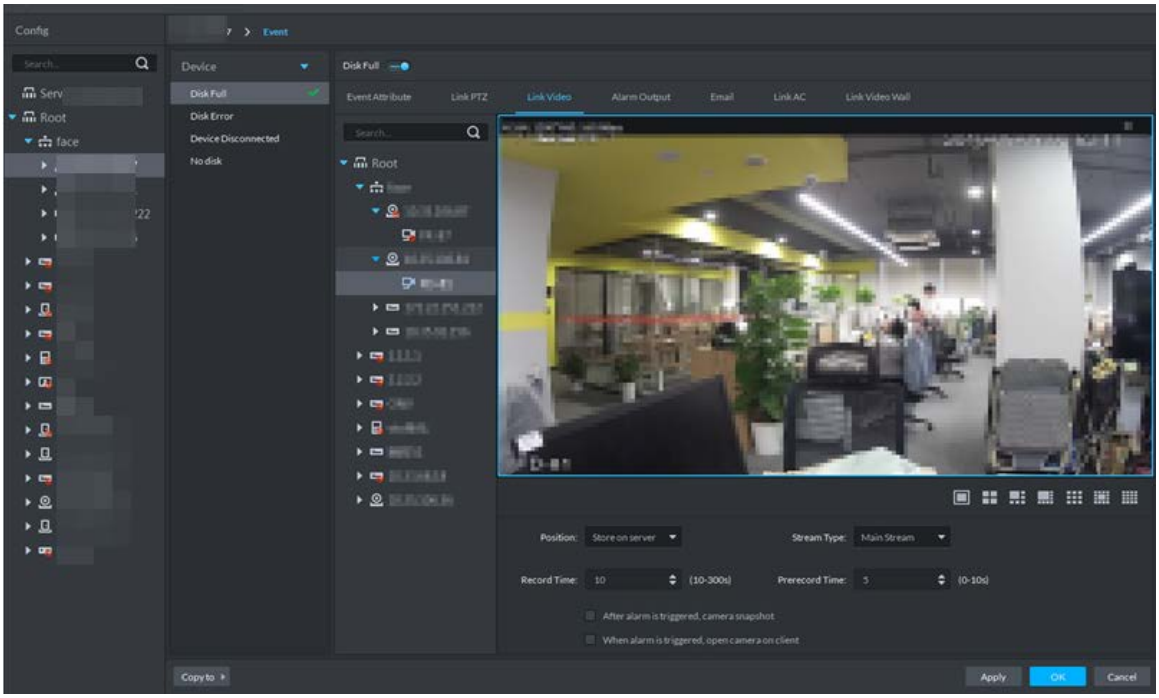
Figure 4-45 Link video



2) Select window, drag the linked device to the window, and see Figure 4-46.

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

Figure 4-46 Bind device channel



3) Set linked parameters. For more details, see Table 4-3.

Table 4-3 Link video parameter

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

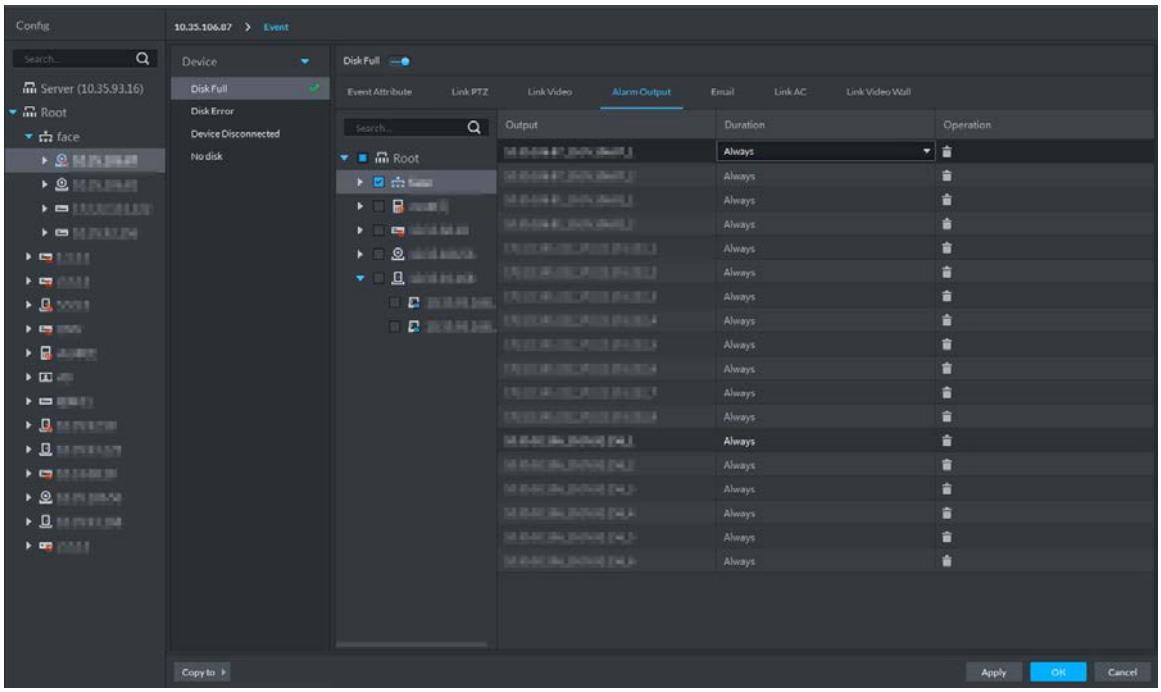
Step 7 Link Alarm Output.

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

1) Click Alarm Output tab.

The **Alarm Output** interface is displayed. See Figure 4-47.

Figure 4-47 Alarm output



2) Select alarm output device.

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

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

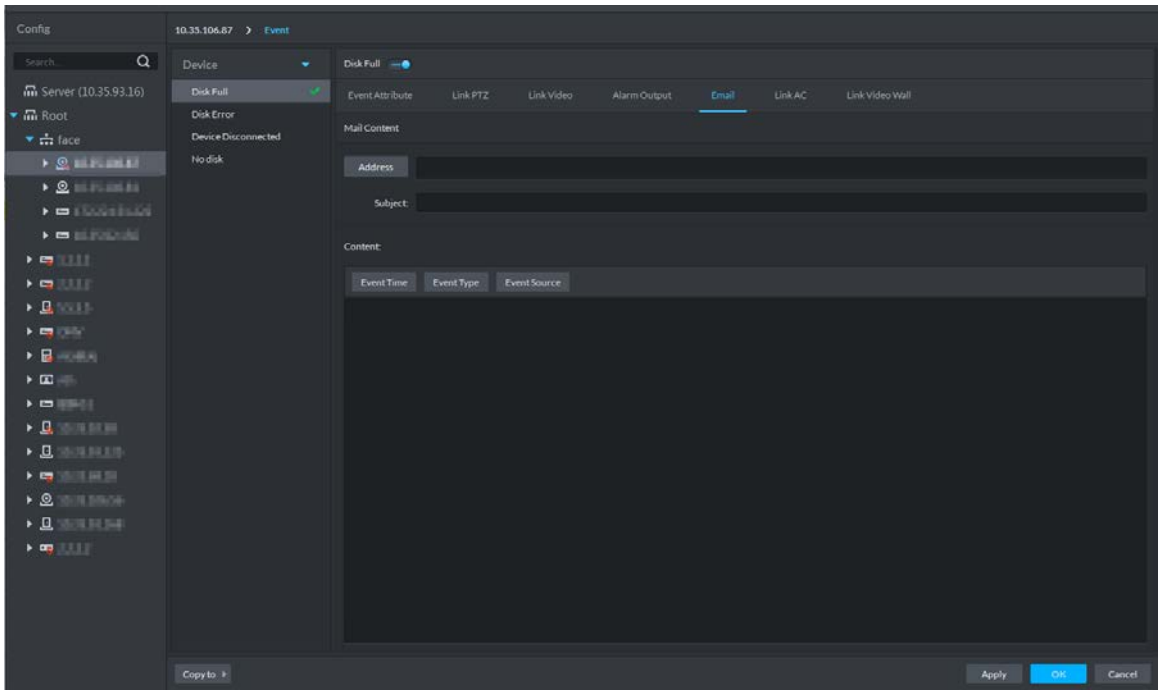
Step 8 Link Email.

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

1) Click **Email**.

The **Email** interface is displayed. See Figure 4-48.

Figure 4-48 Email



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

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

3) Enter email subject.

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

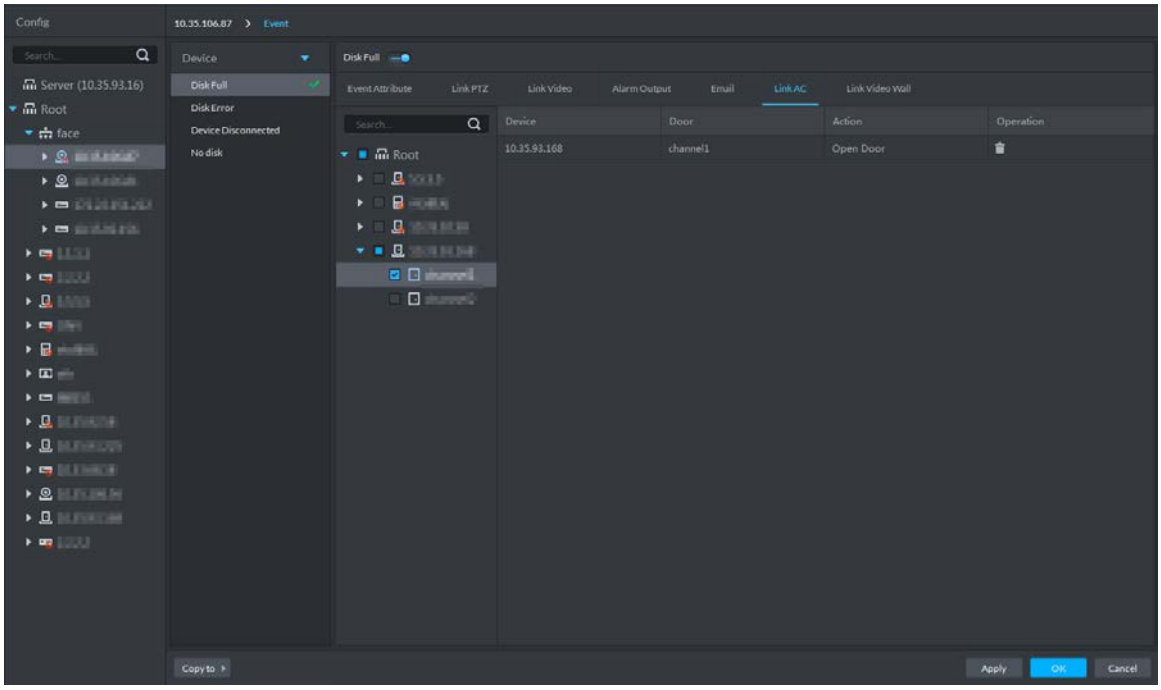
Step 9 Link Access Control

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

1) Click **Link AC** tab.

The **Link AC** interface is displayed. See Figure 4-49.

Figure 4-49 Link AC



2) Select channel of access control.

3) Select linkage action of the access control channel in the right list.

Support four types of action, open door, close door, always open and always close.

- ◇ Open door: Link to open door when alarm event is triggered.
- ◇ Close door: Link to close door when alarm event is triggered.
- ◇ Always open: Linked door is always open when alarm event is triggered.
- ◇ Always close: Linked door is always close when alarm event is triggered.

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

Step 10 Link Video Wall.

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

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

1) Click Link Video Wall tab.

The **Link Video Wall** interface is displayed.

2) Select video wall channel from the middle device list.

The info of linking video wall is displayed. See Figure 4-50.

If video wall window is not configured, click **OK** on the prompt box, configure window on the video wall config interface, and see Figure 4-50.

Figure 4-50 Link video wall

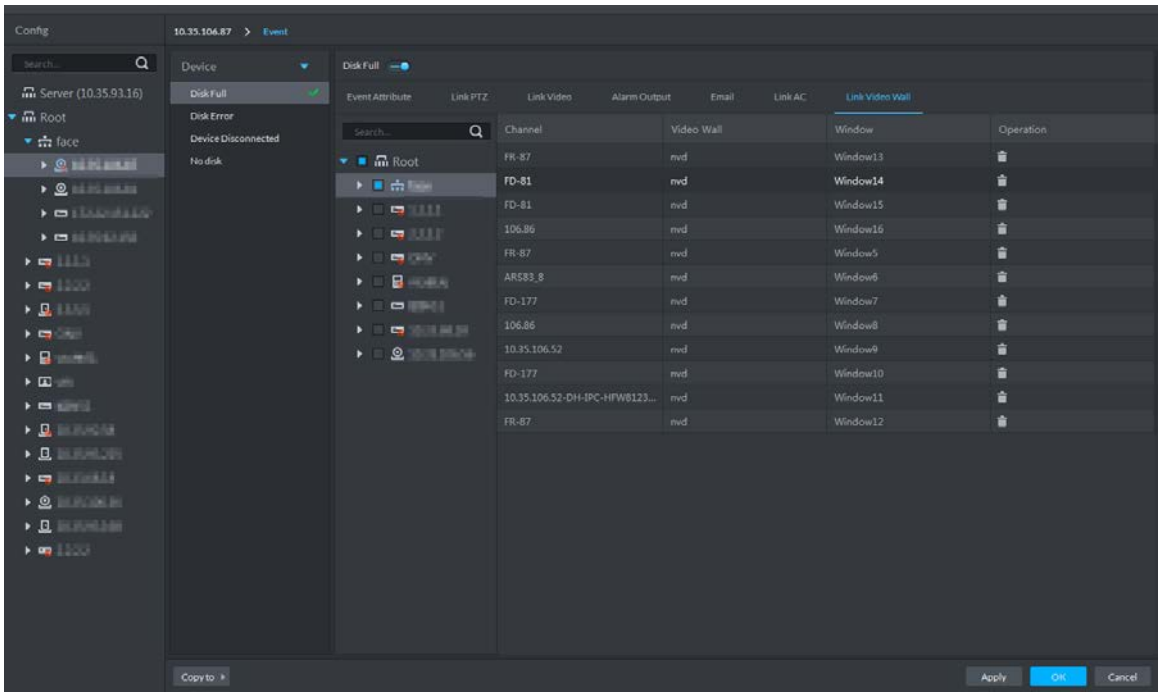
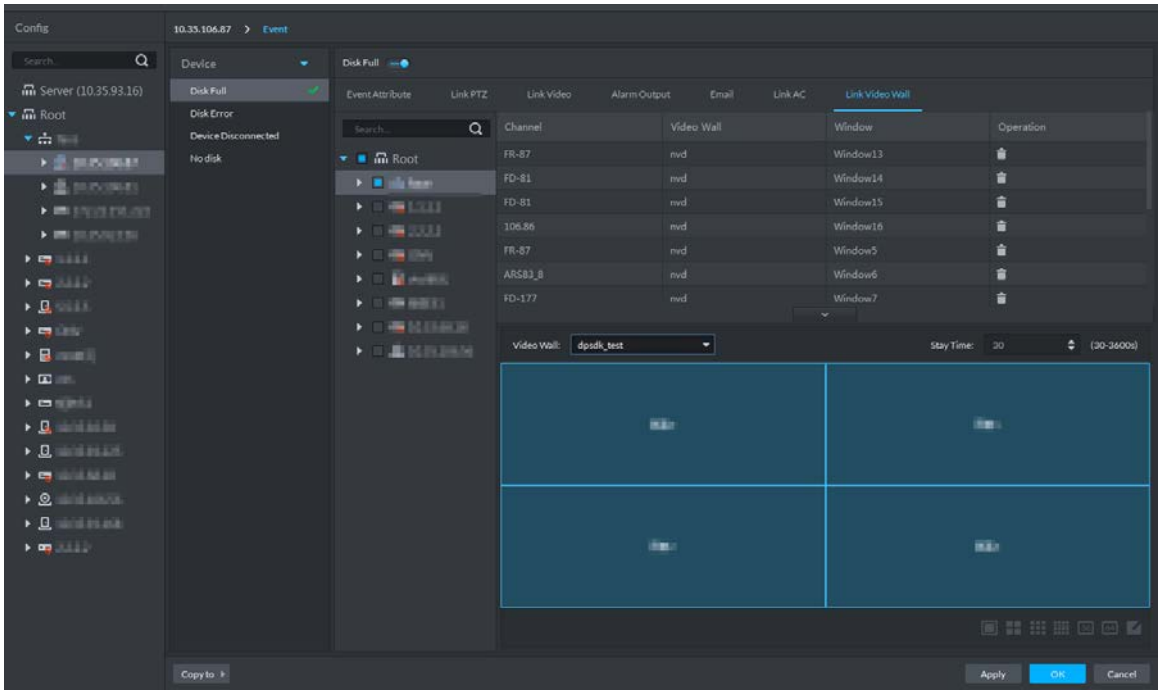


Figure 4-51 Configure video wall window.



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

If you want to configure new window, select New Window from the drop-down box. See Figure 4-50.

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

4.1.5 Setting Record Plan

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

⚠

For storage space config, refer to"4.1.1.4 Setting Storage Space." Following risks may exist if not configured.

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

Step 1 Click **Config** on the client homepage.
The **Config** interface is displayed.

Step 2 From the device tree on the left, select device channel, and click **Record Configuration**. See Figure 4-52.
The **Record** interface is displayed. See Figure 4-53.

Figure 4-52 Enter record config interface

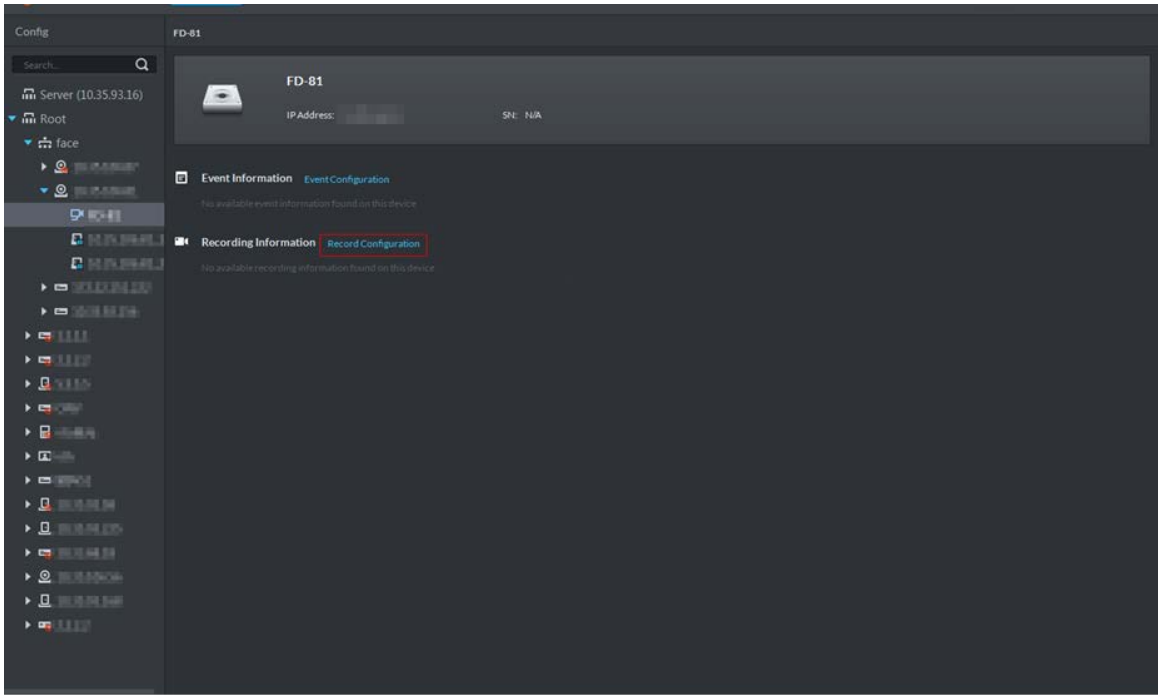
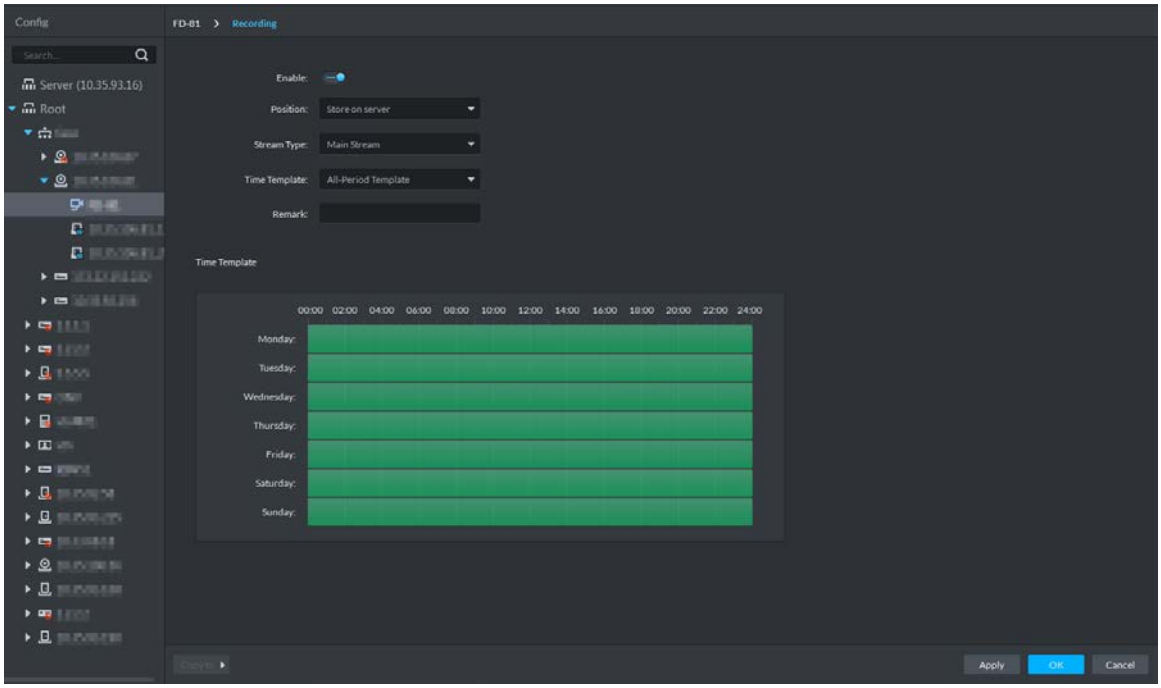


Figure 4-53 Record



Step 3 Click  .

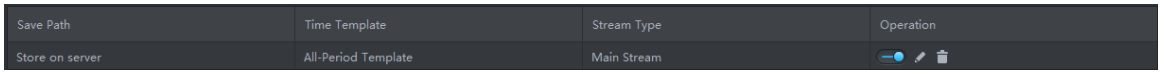
The icon is switched to  , enable record plan.

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

The default time template is provided by system, if requirement is not met, then you can cteate new template.

Step 5 Click **OK**, complete record plan config, and see Figure 4-54.

Figure 4-54 Record info



4.1.6 Configuring Emap

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

4.1.6.1 Adding Map

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

The **Emap** interface is displayed. See Figure 4-55 and Figure 4-56.

Figure 4-55 Emap-first use

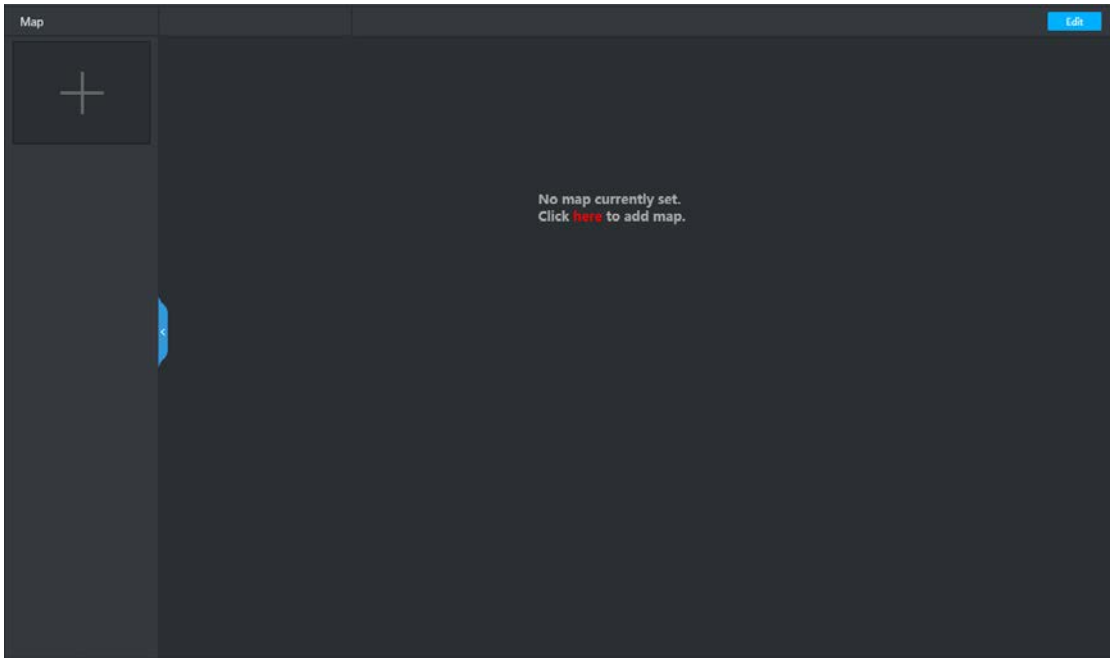
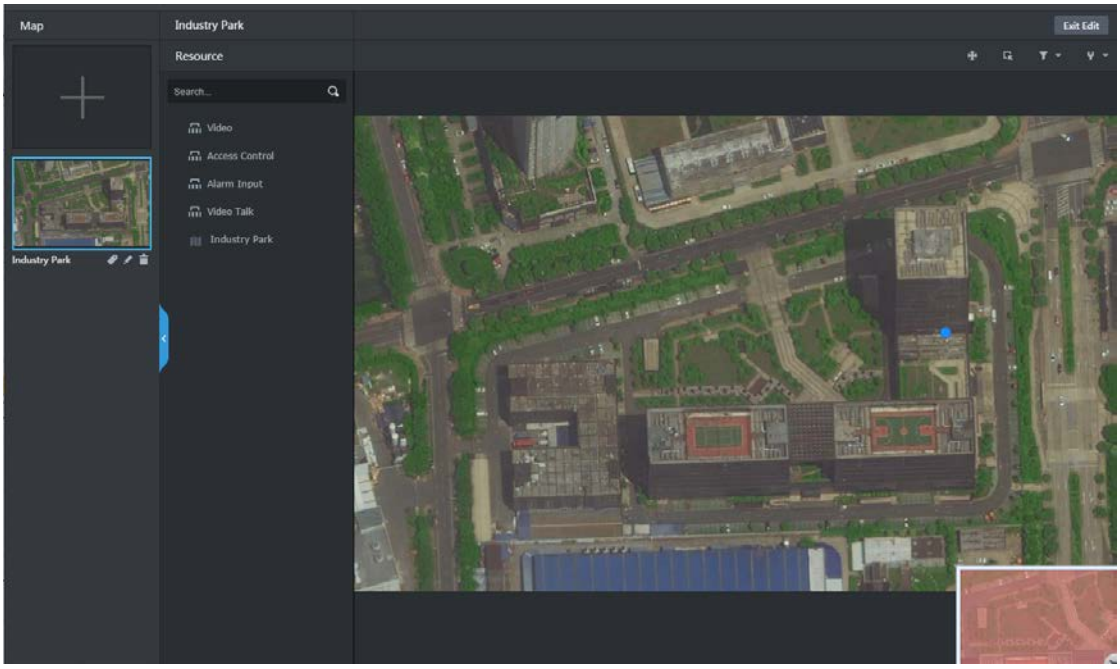


Figure 4-56 Emap-non first use

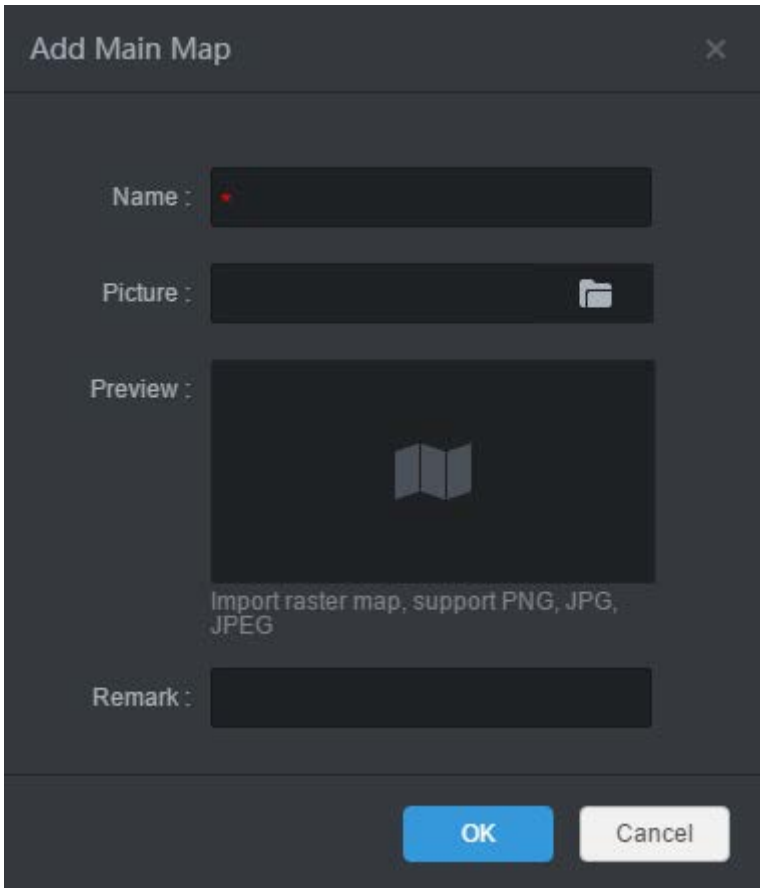


Step 2 Add main map.

1) Click Here for the first use, click + on the left if not use for the first time.

The **Add Main Map** interface is displayed. See Figure 4-57.

Figure 4-57 Add main map



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

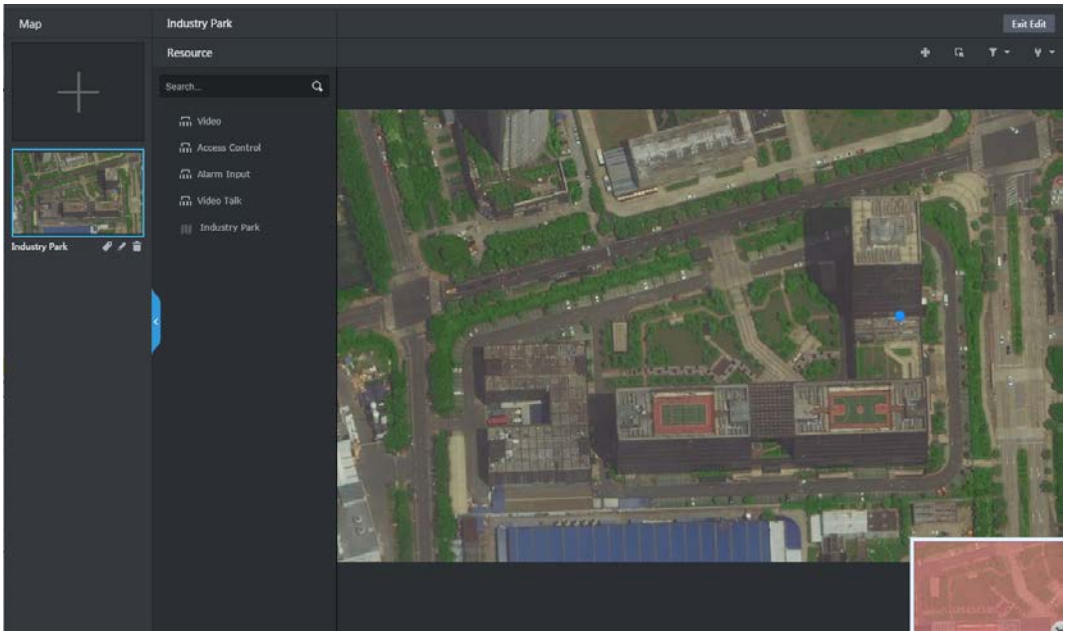
After the picture is selected, selected pictures are displayed on the **Preview** area.

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

3) Click **OK**.

The map is imported to platform. See Figure 4-58.

Figure 4-58 Added map



4) Click  under the map, set it as main map, yellow mark is displayed on the left upper corner. See Figure 4-59.

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

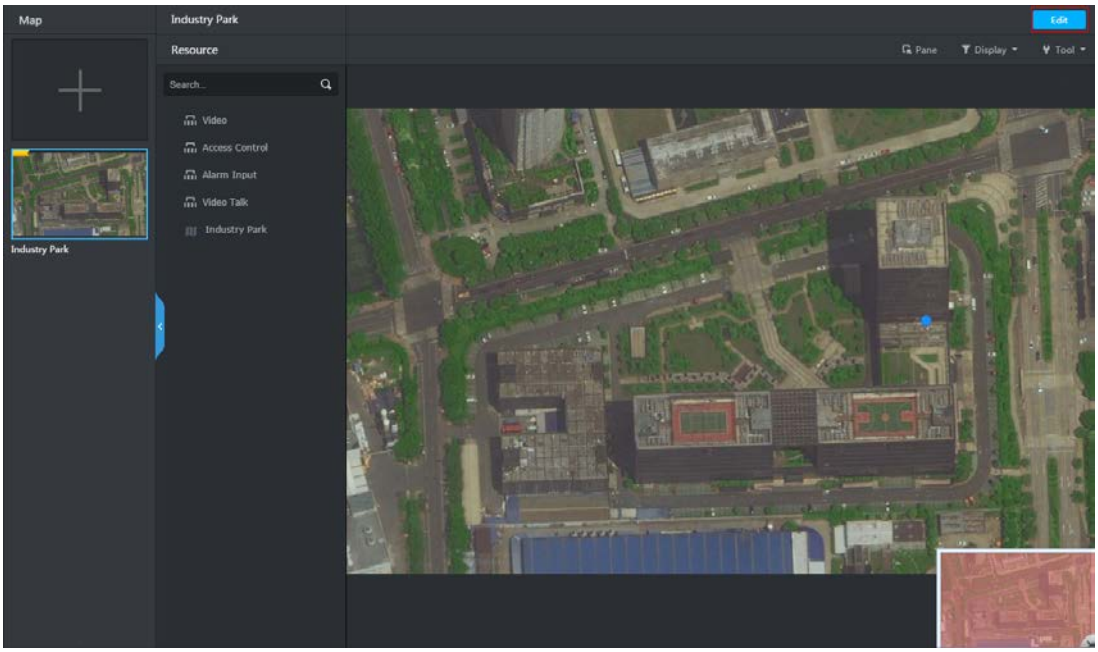
Figure 4-59 Set main map

Step 3 Add hot zone in the map list.

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

1) Click map in the list, open the map, and see Figure 4-60.

Figure 4-60 Open map

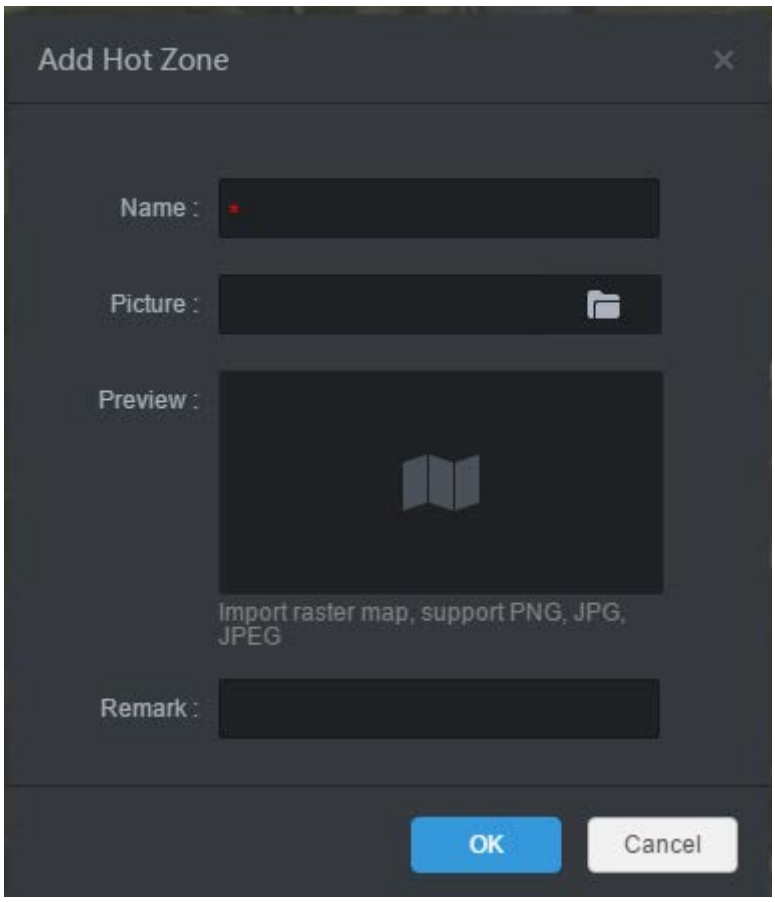


2) Open map, click **Edit** on the upper right corner, and then you can edit the map.

3) Click  , the mouse becomes map icon, select location on the map and click **Add**.

The **Add Hot Zone** interface is displayed. See Figure 4-61.

Figure 4-61 Add hot zone



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

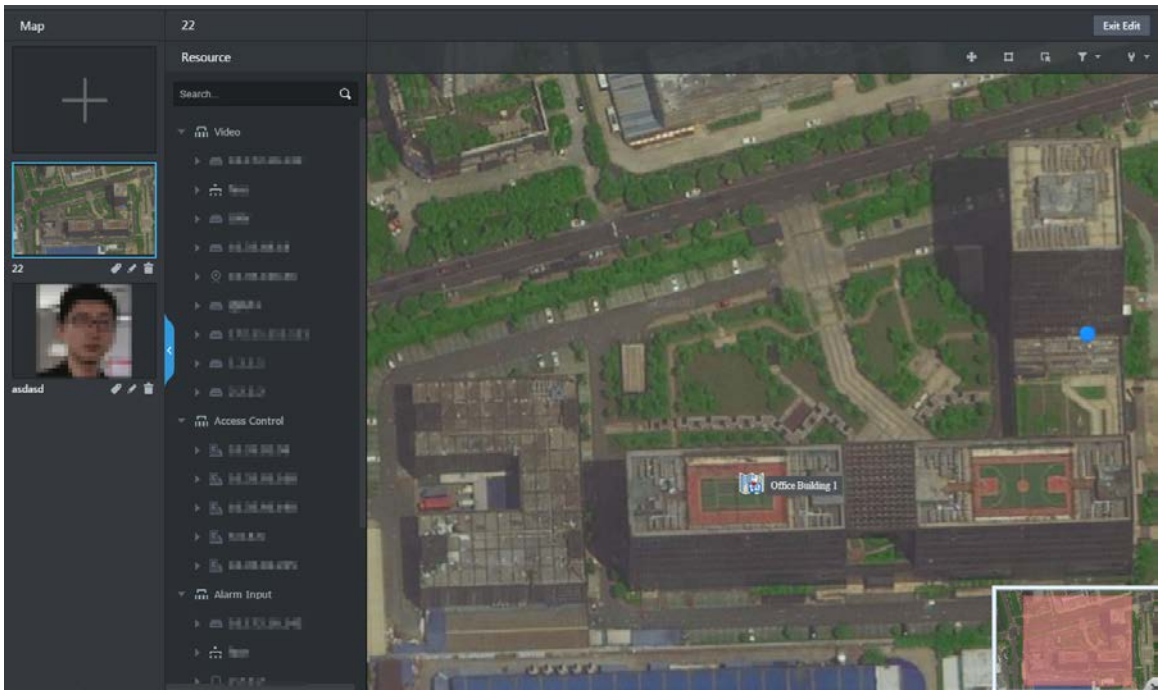
- The format of imported raster map supports PNG, JPG and JPEG.
- After adding the picture, it is displayed on the preview area.

5) Click **OK**.

Hot zone is added. See Figure 4-62. Left list displays map levels, right map displays hot zone icon.

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

Figure 4-62 Hot zone added

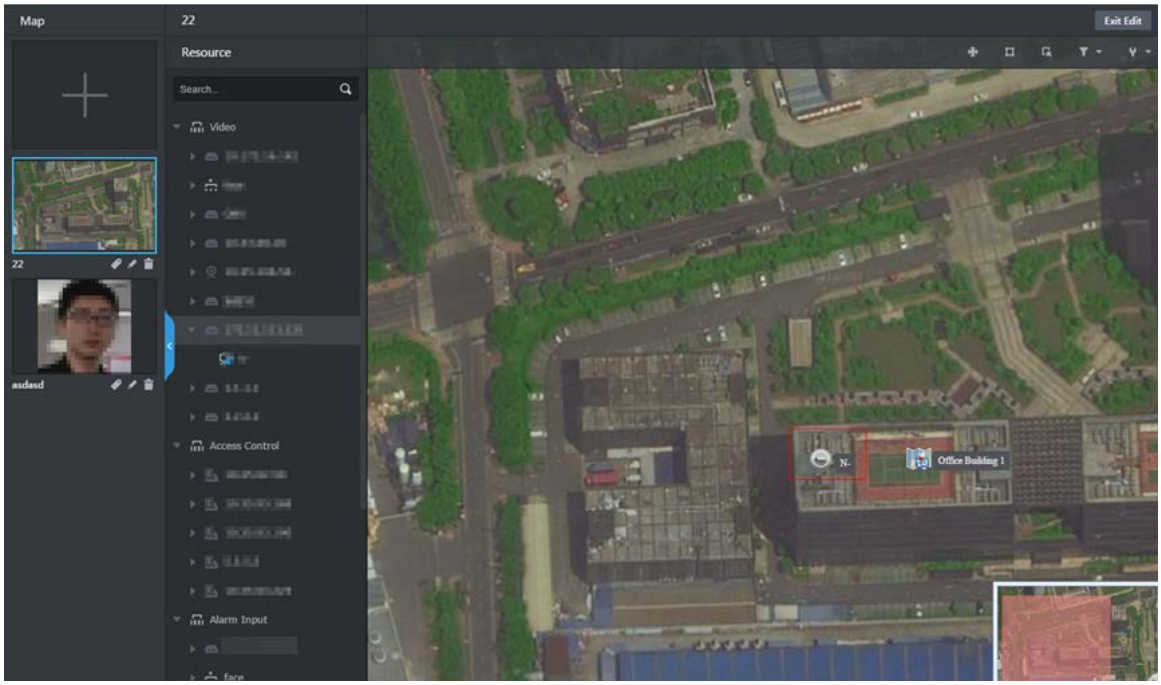


Step 4 Drag device channel onto the map for display.

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

1) Click the map in the list, and open the map. See Figure 4-60.
2) Click **Edit** on the upper right corner.
   The map can be edited.
3) Select device channel from the resource list in the middle, drag to the proper location on the map. See Figure 4-63.

Figure 4-63 Add device channel



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

4.1.6.2 Viewing Map

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

The **Emap** interface is displayed.

Step 2 Click map in the list.

The system opens map. See Figure 4-64. For interface description, see Table 4-4.

Figure 4-64 Map

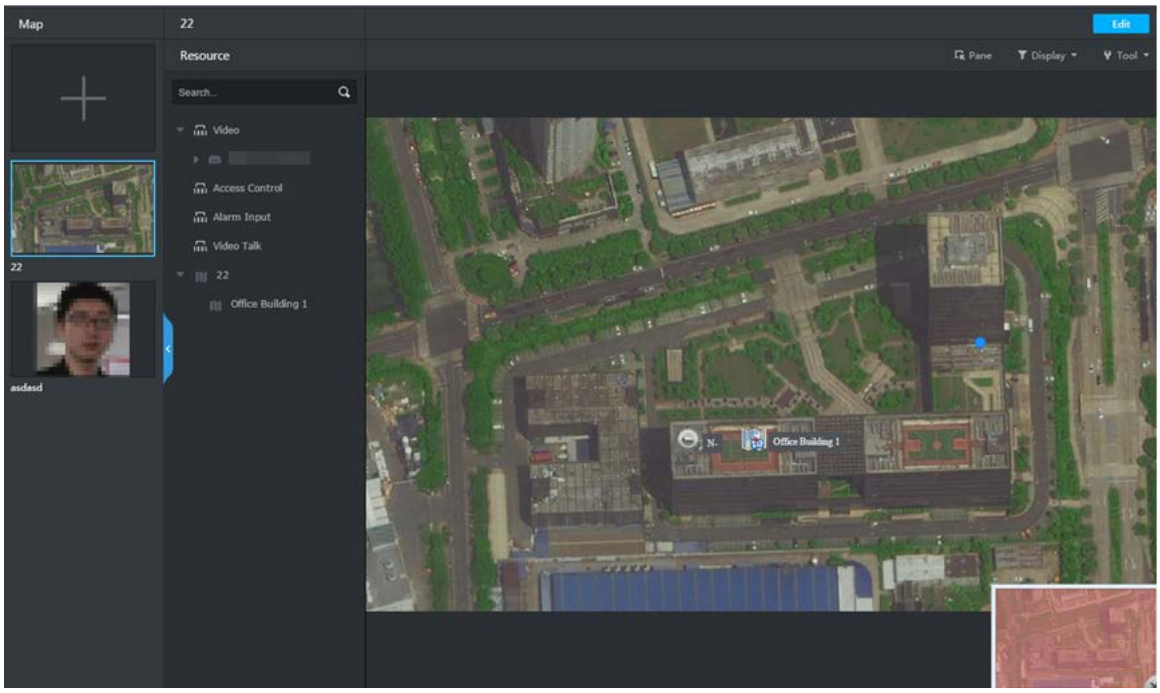


Table 4-4 Interface function description

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

Following operations are supported on the map:

- View channels on map

  Double click channel from the left device tree, and then you can view the channel position on the map.

  ◇ Roll the mouse on the map and you can zoom in or out map.

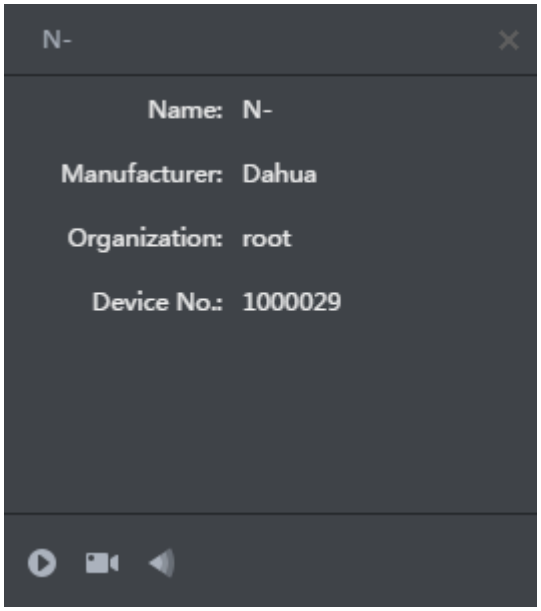
  ◇ If the picture is too big to be completely displayed, you can drag the red module on the lower right corner to display by mouse.

- View channel details

Click the channel on the map. The system displays device number, name, manufacturer and organization. See Figure 4-65.

Different devices may have different channel details and operations.

Figure 4-65 Channel info



- View channel video

  Click  and open channel video.
- View playback

  Click  and realize video playback.
- View visible range

  Click  and view visible range.
- Edit map

  Click **Edit** on the upper right corner, the map can be edited. See Figure 4-66. For operations, see Table 4-5.

Figure 4-66 Edit map

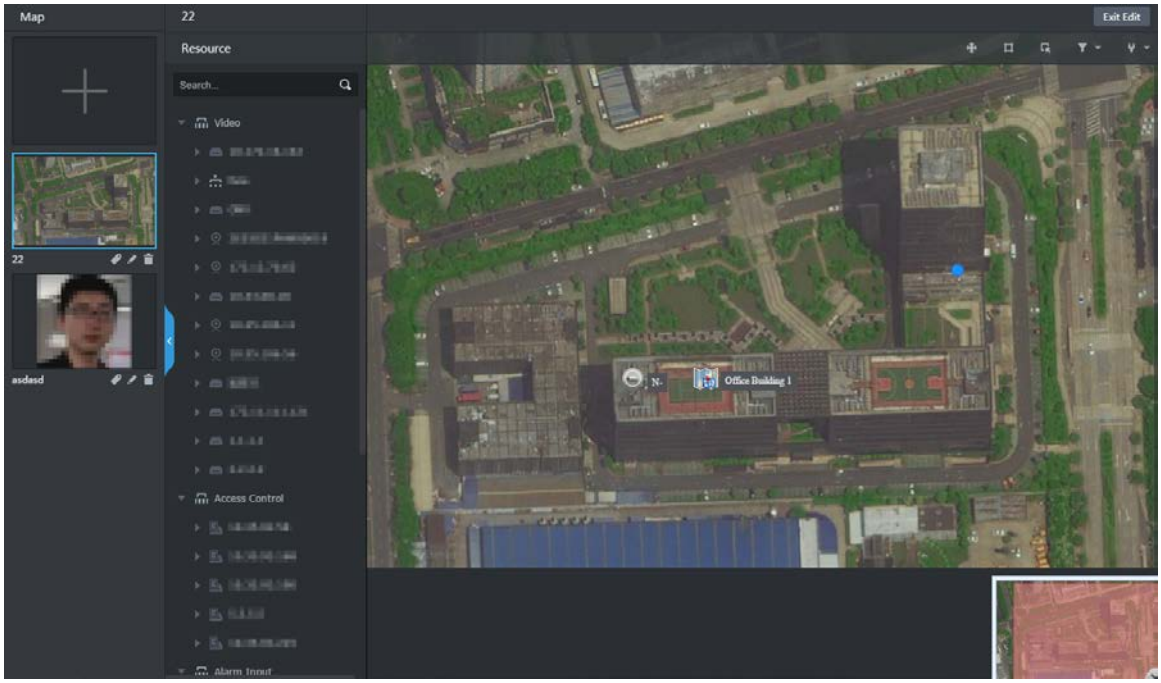


Table 4-5 Operation description

Icon	Function	Description
	Move device	Click the icon and it becomes blue, you can drag the device on map and change its position. Click again to exit move status
	Add hot zone	Refer to 4.1.6.1 Adding Map Step 3 Add hot zone in the map list.
	Select device	Click the icon and it becomes blue, select an area on the map and it will display device list within the area. Select device, click corresponding icon, and then you can preview view, playback video and delete the device.
	Display device	Filter by device type, only kept device type is displayed on the map.
	Mark or reset	Include mark and reset. ● Mark: Mark on the map. ● Reset: Restore the map to default position.

4.2 Local Config

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

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

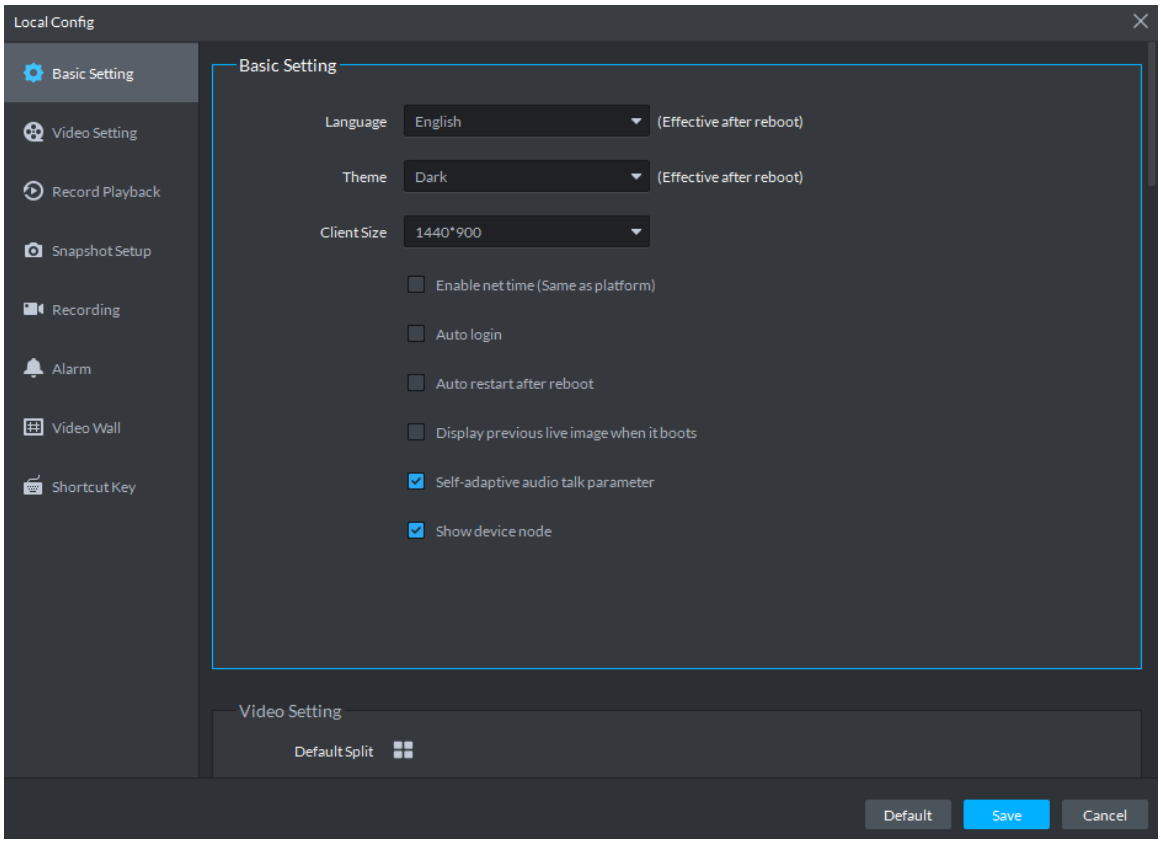
4.2.1 Setting Basic Parameter

Set client language, client size and sync time.

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

The **Local Config** interface is displayed. See Figure 4-67

Figure 4-67 Local config



Step 2 Click **Basic Setting** tab, set basic parameters, and see Figure 4-67. For parameter description, see Table 4-6.

Table 4-6 Basic parameter description

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

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

Step 3 Click **Save**.

4.2.2 Setting Real-time Video Parameter

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

Step 1 Click on the upper right corner of client interface.
The **Local Config** interface is displayed.

Step 2 Click **Video Setting** tab, set parameters, and see Figure 4-68. For parameter details, see Table 4-7.

Figure 4-68 Video setting

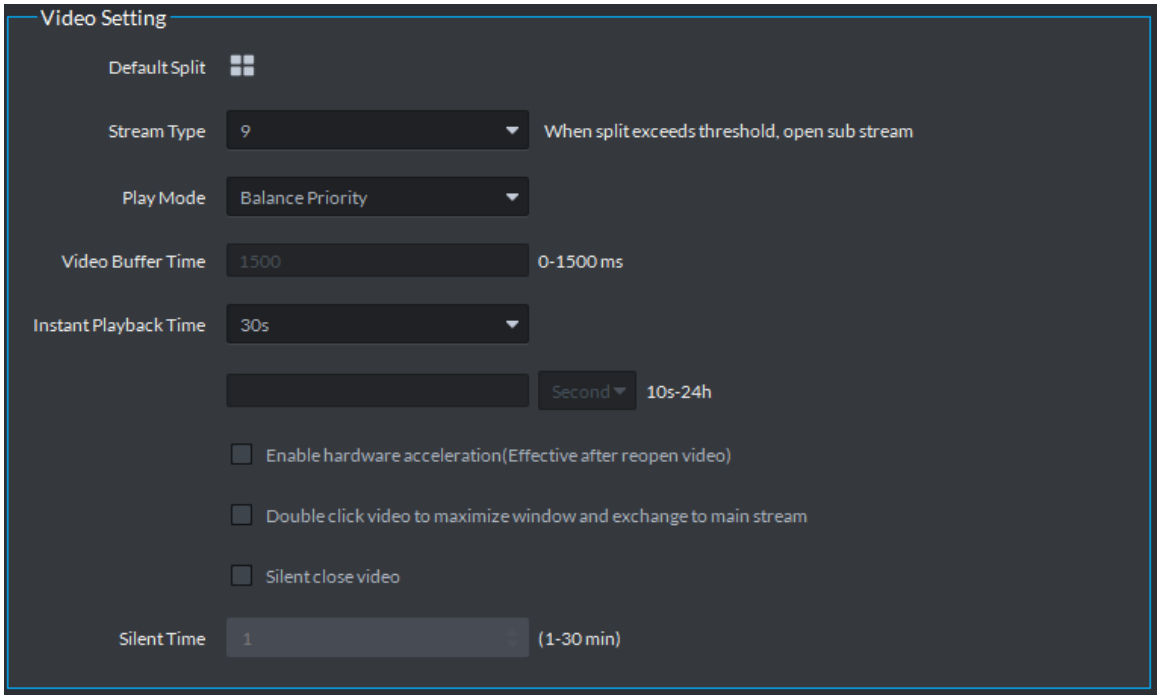


Table 4-7 Video setting parameter description

Parameter	Description
Default Split	Set split mode of the video window.
Stream type	Defines bit stream type for video transmission. With main bit stream as default, the auxiliary bit stream will be used when number of window splits is greater than the value selected here.
Play Mode	Play mode to be selected as required, including Real Time Priority, Fluency Priority, Balance Priority, as well as user-defined modes.
Video buffer time	Set video buffer time. It is only valid when play mode is customized.
Instant playback time	Select instant playback time and then click Instant playback on the Live view interface, you can view the record of current period.
Enable hardware acceleration	Check the box to enable the function. Use hardware module to enhance acceleration features.
Double click video to maximize window and exchange to main stream	Check the box to enable the function.
Silent close video	After being enabled, if the time of no operation for the Live interface exceeds the set value, the system will close Live automatically.

Step 3 Click **Save**.

4.2.3 Setting Record Playback

Set video window split mode and record stream type.

Step 1 Click on upper right corner of client interface.
The **Local Config** interface is displayed.

Step 2 Click **Record Playback** tab, set parameters, and see Figure 4-69. For details, refer to Table 4-8.

Figure 4-69 Record playback

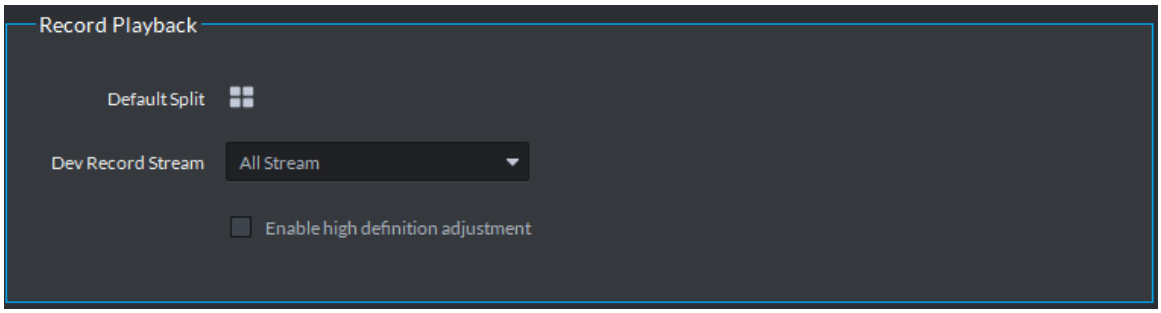


Table 4-8 Record playback parameter description

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 3 Click **Save**.

4.2.4 Setting Snapshot

Set snapshot save format, path and naming rule.

Step 1 Click on upper right corner of client interface.
The **Local Config** interface is displayed.

Step 2 Click **Snapshot Setup** tab, set snapshot format and save path. See Figure 4-70. For parameter details, see Table 4-9.

Figure 4-70 Snapshot setting

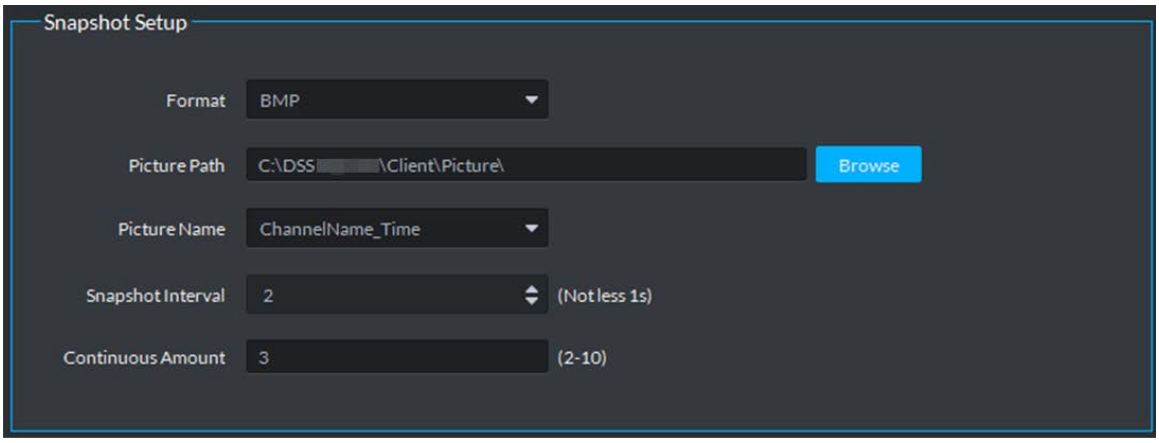


Table 4-9 Snapshot setting parameter description

Parameter	Description
Format	Set snapshot image format.

Parameter	Description
Picture path	Set snapshot storage path.
Picture name	Select picture name rule.
Snapshot interval	Set snapshot interval. System snapshot once after the specified period.
Continuous amount	Snapshot amount at each time.

Step 3 Click **Save**.

4.2.5 Setting Recording Parameter

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

Step 1 Click on upper right corner of client interface.
The **Local Config** interface is displayed.

Step 2 Click **Recording** tab, set record path and save path. See Figure 4-71. For parameter details, see Table 4-10.

Figure 4-71 Recording

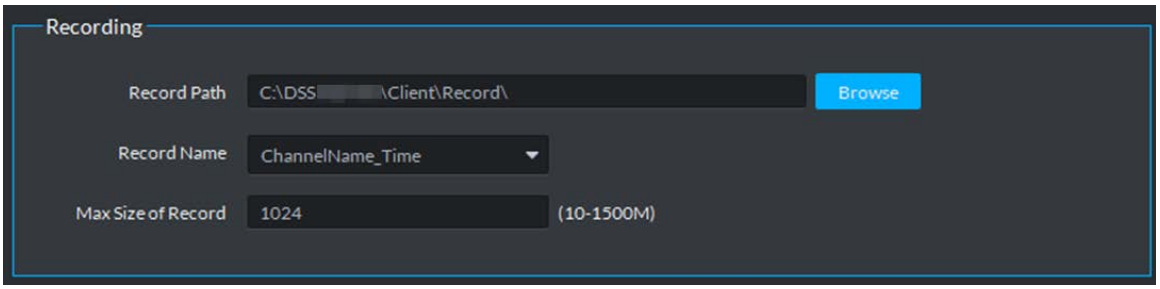


Table 4-10 Recording parameter description

Parameters	Description
Record path	Set record storage path.
Record name	Set record file name rule.
Max. record size	Set record file size.

Step 3 Click **Save**.

4.2.6 Setting Alarm Parameter

Set alarm type, sound path and video opening type.

Step 1 Click on upper right corner of client interface.
The **Local Config** interface is displayed.

Step 2 Click **Alarm** tab, set client alarm type. See Figure 4-72.

Figure 4-72 Alarm

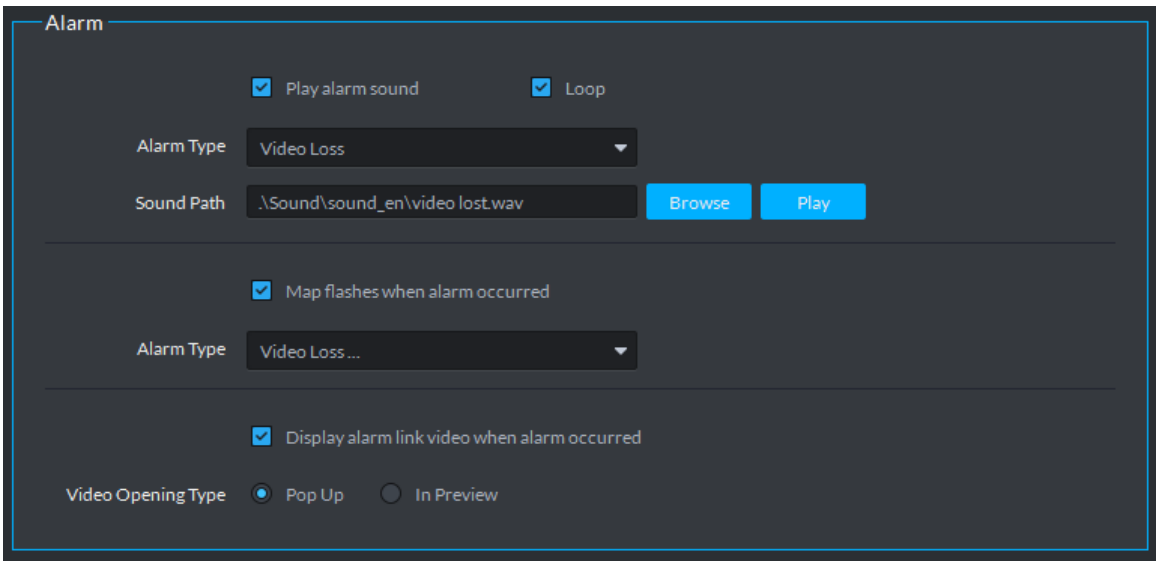


Table 4-11 Alarm parameter description

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

Step 3 Click **Save**.

4.2.7 Setting Video Wall

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

Click **Video Wall** and set parameters. See Figure 4-73. For parameter details, see Table 4-12.

Figure 4-73 Video wall

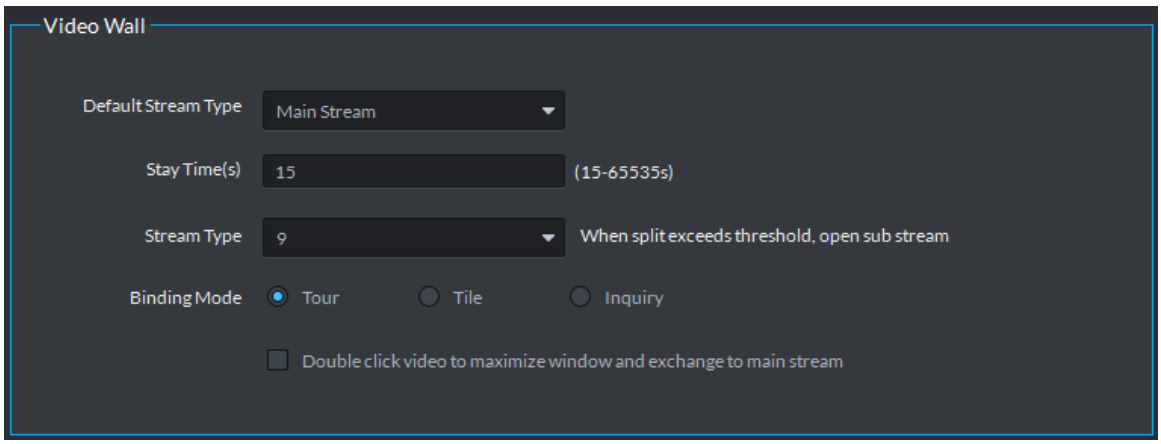


Table 4-12 Video wall parameter description

Parameter	Description
Stream type	When split exceeds threshold, open substream.
Binding mode	● Tour: Device nodes are displayed on 1 window by tour. ● Tile: Device nodes are aredisplayed on windows of current screen by tile. ● Inquiry: When dragging the device nodes to the window, the systems prompts whether tour or tile.
Double click video to maximize window and exchange to main stream	Double-click the video screen to maximize the window, and the stream change to main stream.

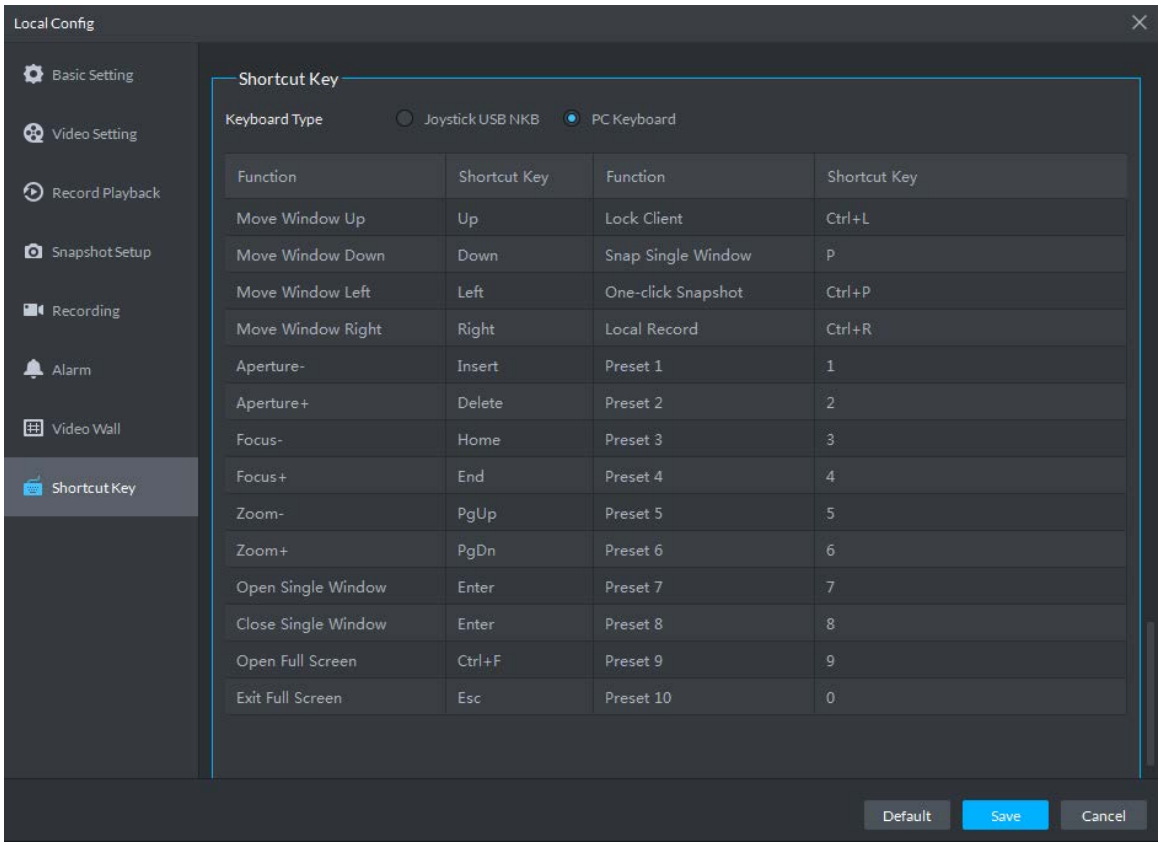
4.2.8 Setting Shortcut Key

Set client shortcut key and control client quickly.

Step 1 Click on upper right corner of client interface.
The **Local Config** interface is displayed.

Step 2 Click **Shortcut Key** tab, check PC keyboard or shortcut key of USB keyboard. See Figure 4-74.

Figure 4-74 Shortcut key



Step 3 Click **Save**.

4.3 Live View

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

4.3.1 Entering Live View Interface

On client homepage, click **Live View**. The **Live View** interface is displayed. See Figure 4-75. For interface description, see Table 4-13.

Figure 4-75 Live view

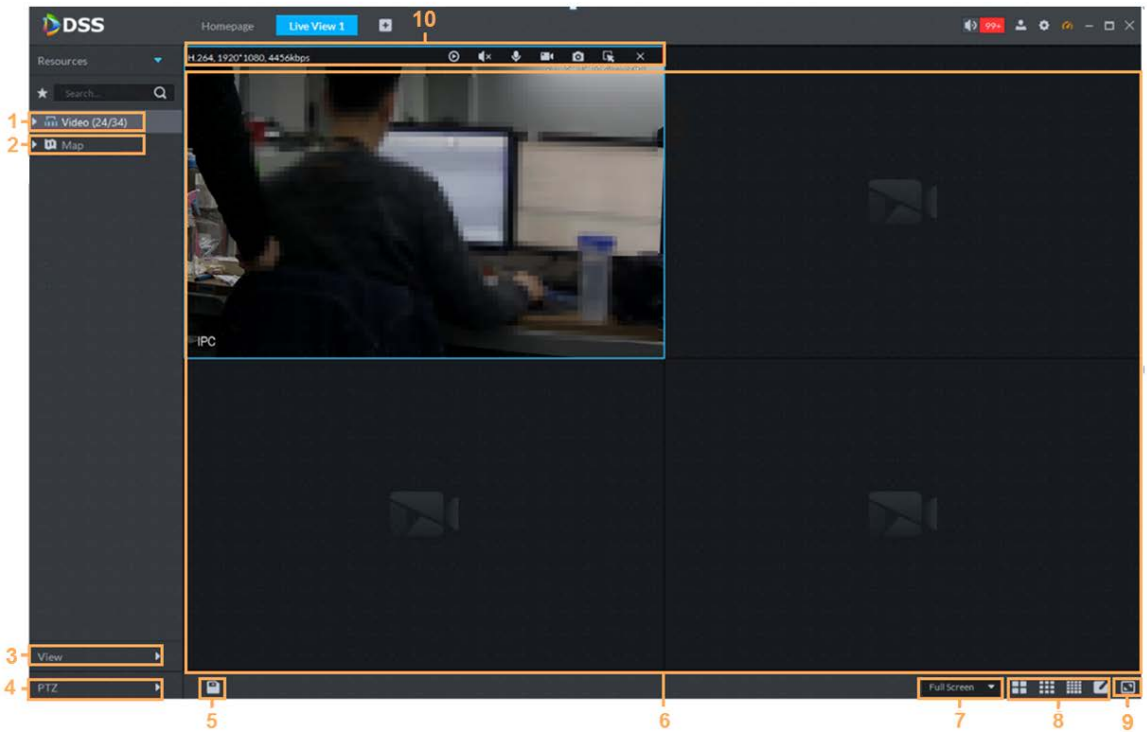


Table 4-13 Live view interface description

No.	Parameter	Description
1	Resources	• Click ☆ and enter favorite. • You can search device or channel in Search... according to device name or channel name. • Display device list. If you enable **Show Device Node** in **Local Config** > **Basic Setting**, then the device tree displays device and its channels, or you can disable it and display all the device channels.
2	Map	Display added map, double click to open map, select device and support live view and cancel alarm.
3	View	Display created view list.
4	PTZ	For detailed operation of PTZ, refer to"4.3.5 Setting PTZ."
5	Save View	Record live video window split and window play. Save as preview plan for quick call. For detailed operation, see"4.3.8 View."
6	Video Play Window	Display live view image. Move the mouse to the video window which is being displayed; scroll the mouse to zoom in or out video. Right click and refer to"4.3.2 Enabling Live View."
7	Display Mode	Select height and width ratio of video window, you can play video by actual ratio or full window.
8	Image Split Mode	Used to set image split mode, support 1, 4, 6, 8, 9, 13, 16, 20, 25, 36 and 64, or click ✎ and customize split mode.

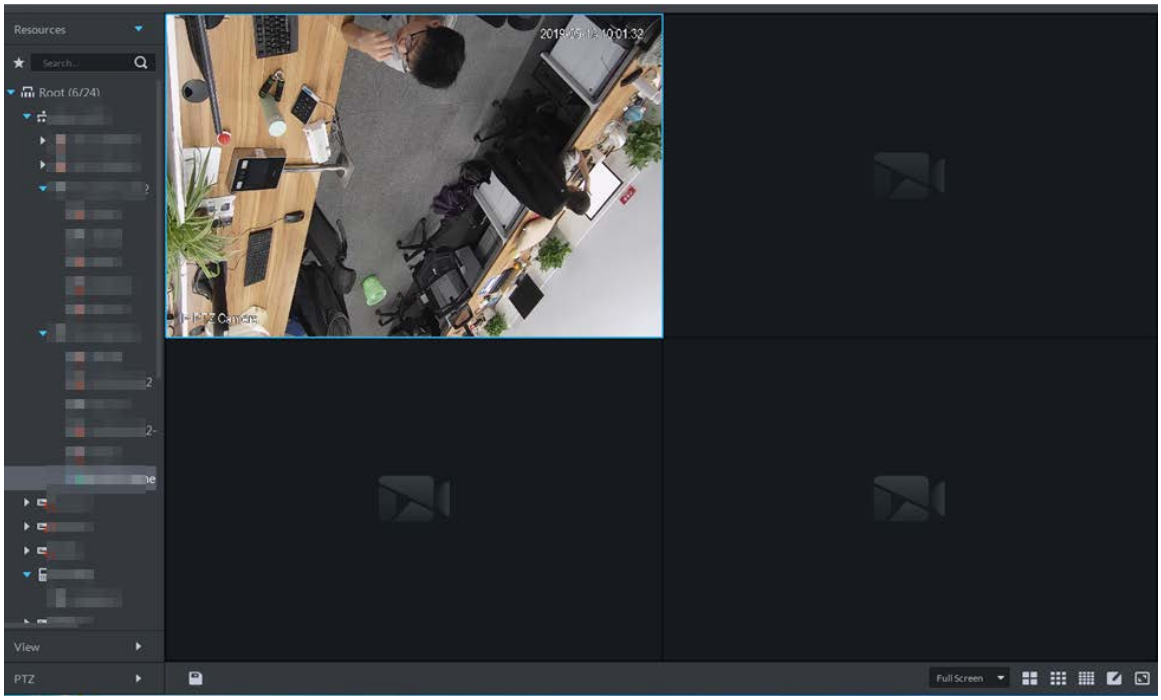
No.	Parameter	Description
9	Full Screen	Switch video window to **Full Screen** mode. If you want to exit **Full Screen**, you can press Esc button or right click and select **Exit Full Screen**.
10	Stream and Shortcut	Display encode format, stream and shortcut operation. For detailed operation, see"4.3.2 Enabling Live View."

4.3.2 Enabling Live View

Select channel or device from device list on the **Live View** interface, double click or drag to video window. The system plays realtime video. See Figure 4-76.

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

Figure 4-76 Enable live view



Related operations of live view are shown as follows:

- Move the mouse to video window, shortcut operation menu is displayed on upper right corner of the window. See Figure 4-77. For detailed description, see Table 4-14.

Figure 4-77 Shortcut menu

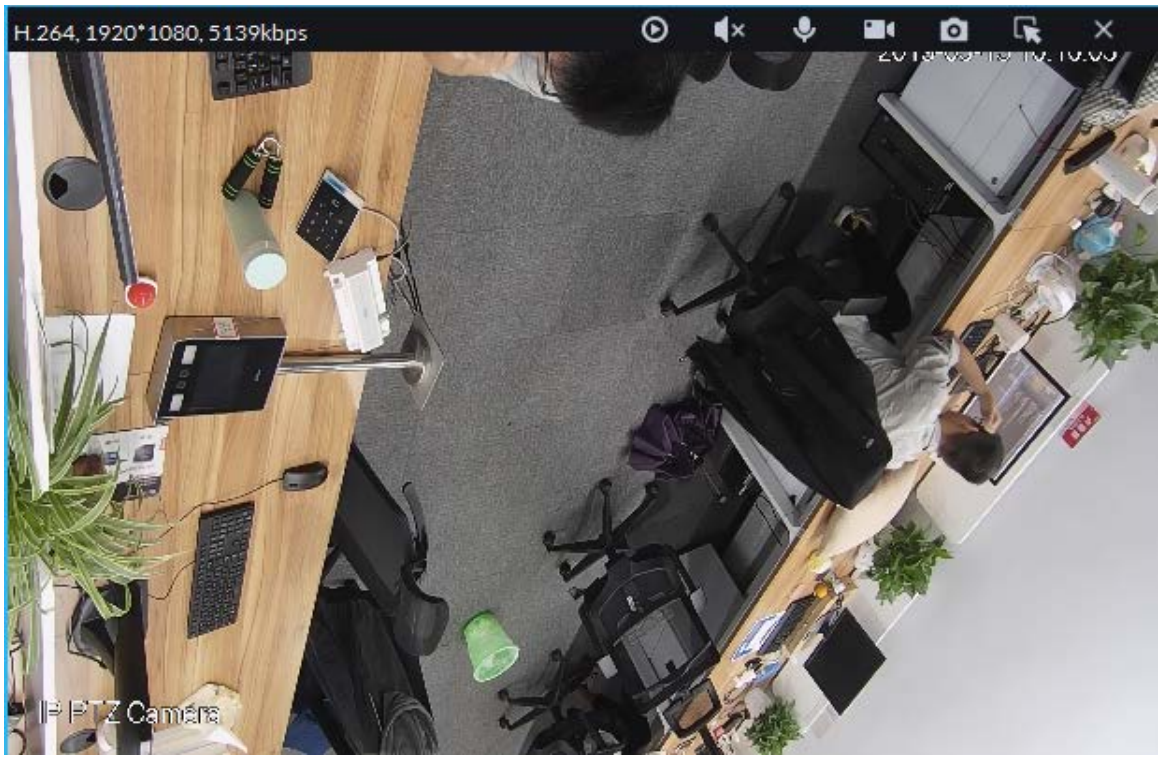


Table 4-14 Shortcut menu description

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.

- Right click live view window, display menu shown in Figure 4-78. For operation description, see Table 4-15.

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

Figure 4-78 Right click menu

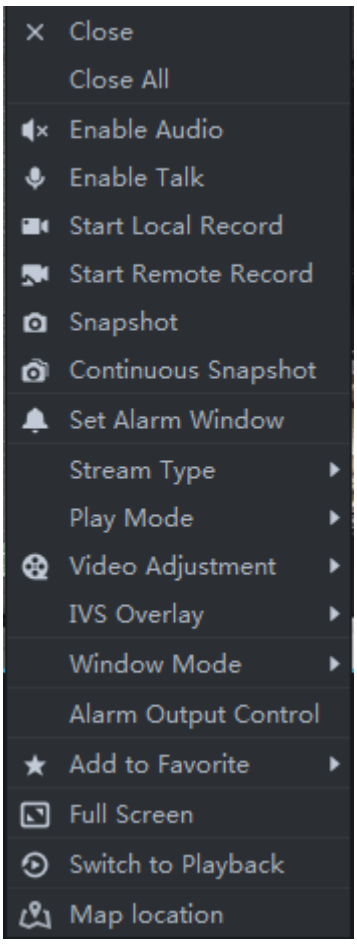


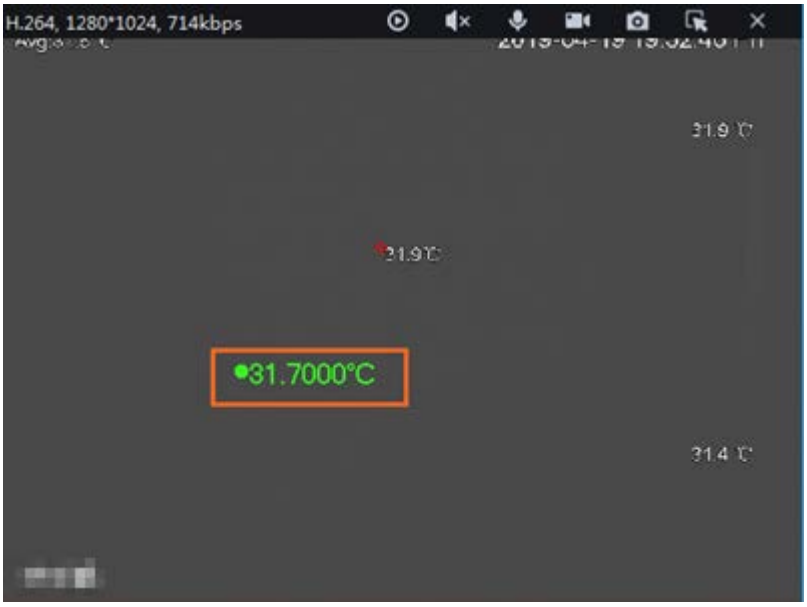
Table 4-15 Right click menu description

Parameters	Description
Close	Close active video window.
Close All	Close all video windows.
Enable Audio	Same as , to enable or disable camera audio.
Enable Talk	Same as , to enable or disable audio talk of corresponding device. Check Self-adaptive Audio Talk Parameters from Local Config > General; when audio talk is on, it will automatically adapt to various parameters without showing a pop-up box.
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
Stream Type	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.
Installation mode	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. For fisheye camera only.
Fisheye view mode	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. For fisheye camera only. When changing the video stream, the fisheye view mode keeps the configuration before the stream is changed.
Split mode	Support standard mode, 1+3 mode, 1+5 mode.
Alarm output control	It control alarm input/output.
Add To Favorites	You can add the active channel or all channels into Favorite.
Full Screen	Switch the video window to full screen mode. To exit full screen, double click video window, or right click to select exit full screen.
Switch to Playback	You can switch between live view interface and playback interface quickly, without going back to homepage first.
Map location	After enabling map location, a map that centers on the device will be displayed.

- If you preview thermal channel, move the mouse and lay it any position of the image, and then the platform displays realtime temperature of the position. See Figure 4-79.

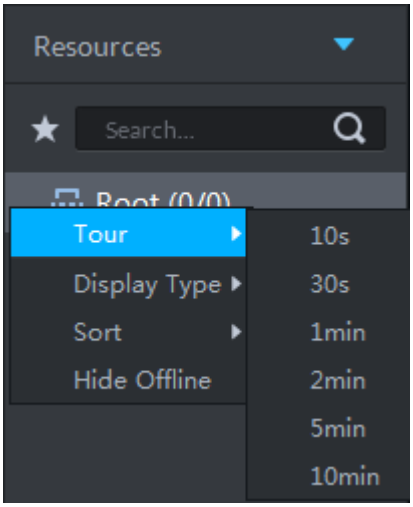
Figure 4-79 Spot temperature



4.3.3 Enabling Tour View

Right click device or organization in the device list on **Live View** interface, select **Tour** and set duration. See Figure 4-80. The system plays video image of all online channels in loop, click  or right click window to stop. Select **Stop Tour** if you want to.

Figure 4-80 Tour interface



4.3.4 Device Config

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

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

4.3.4.1 Configuring Camera Properties

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

4.3.4.1.1 Configuring Property Files

Step 1 On the **Preview** interface, right-click the video device and select **Device Config**. See Figure 4-81.

The **Device Config** interface is displayed. See Figure 4-82.

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

Figure 4-81 Entering device config

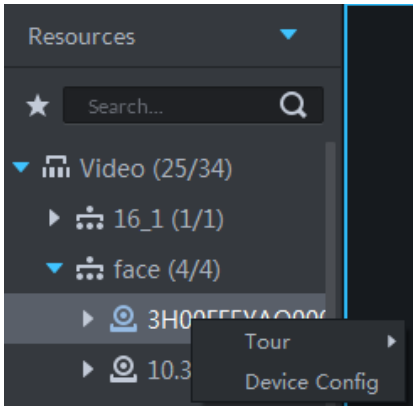
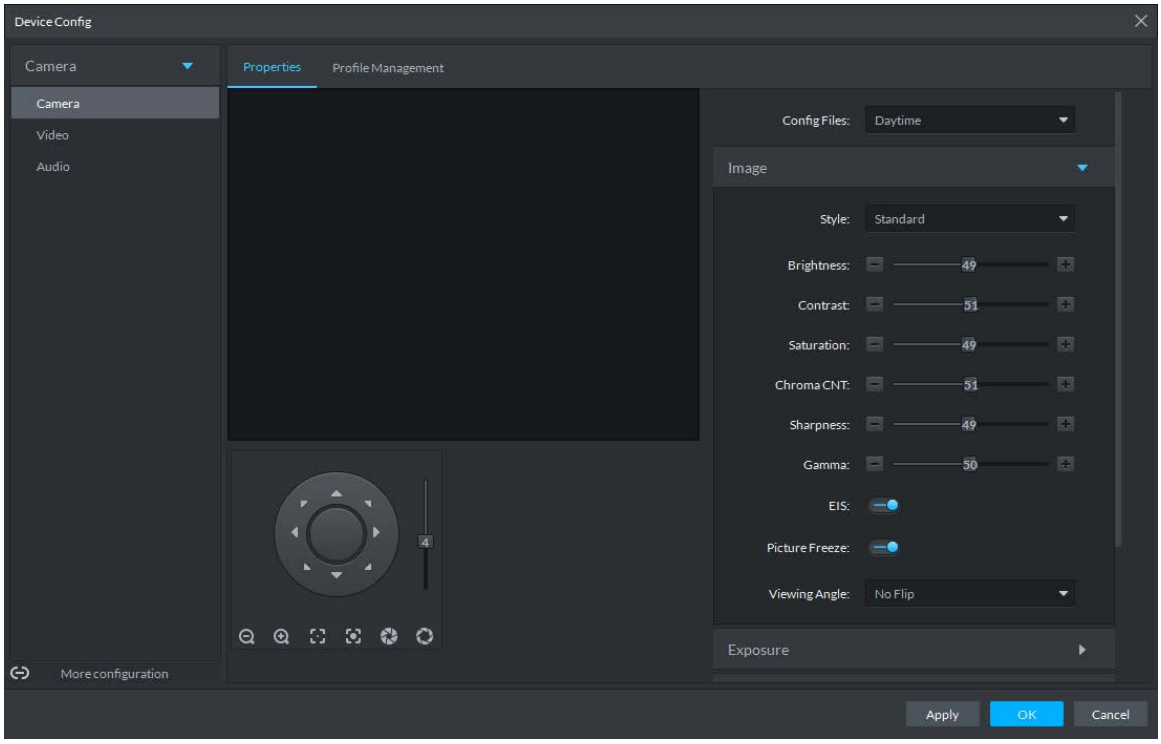


Figure 4-82 Device config



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

The **Properties** interface is displayed. See Figure 4-82.

Step 3 Select **Profile Management**.

Step 4 Click **Image**. See Figure 4-82. For details of the parameters, see Table 4-16.

Table 4-16 Image parameter description

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

Step 5 Click **Exposure** to set up relevant parameters. See Figure 4-83. For details of the parameters, see Table 4-17.

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

Figure 4-83 Exposure

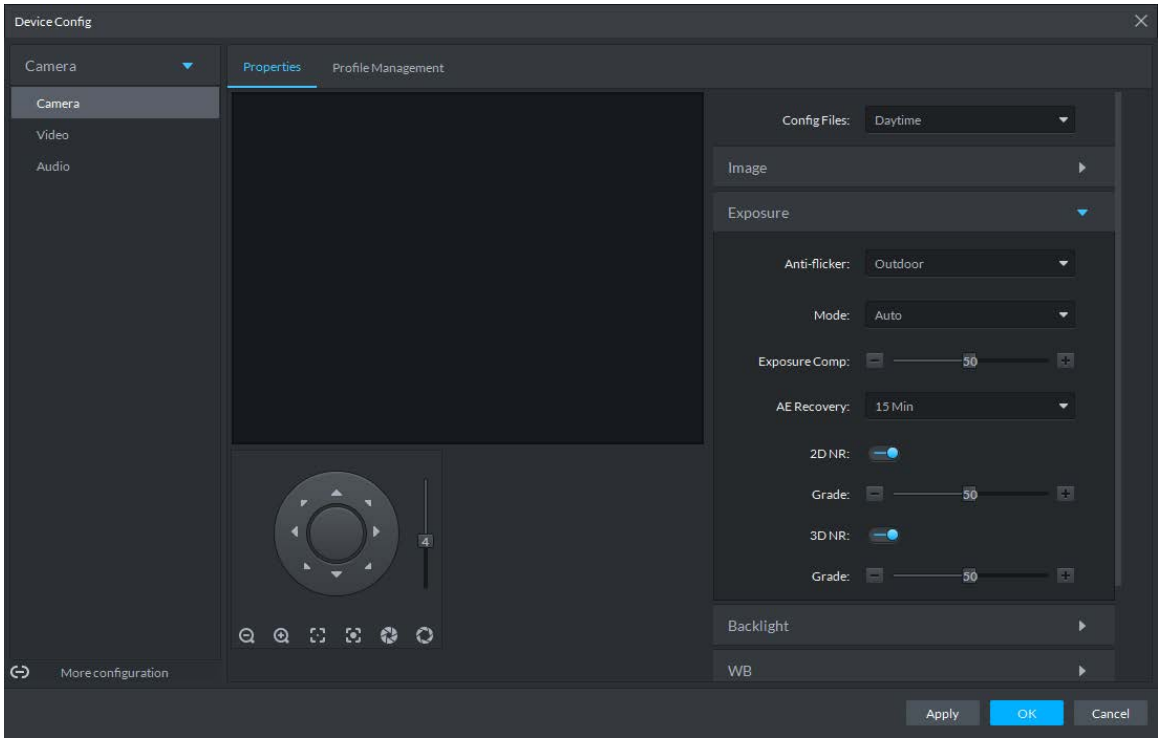


Table 4-17 Exposure parameter description

Parameter	Description
Anti-flicker	You can select from these three modes: 50Hz, 60Hz, or Outdoor. ● 50Hz: With the 50Hz household power supply, the mode can automatically adjust exposure based on the brightness of the scene to ensure that the image does not yield horizontal stripes. ● 60Hz: With the 60Hz household power supply, the mode can automatically adjust exposure based on the brightness of the scene to ensure that the image does not yield horizontal stripes. ● Outdoor: In an outdoor scenario, you can switch the exposure modes to achieve your target effect.
Mode	The following options are available for the different exposure modes of the camera: ● 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. ● 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.
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 4-84. For details of the parameters, see Table 4-18.

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

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

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

Figure 4-84 Backlight

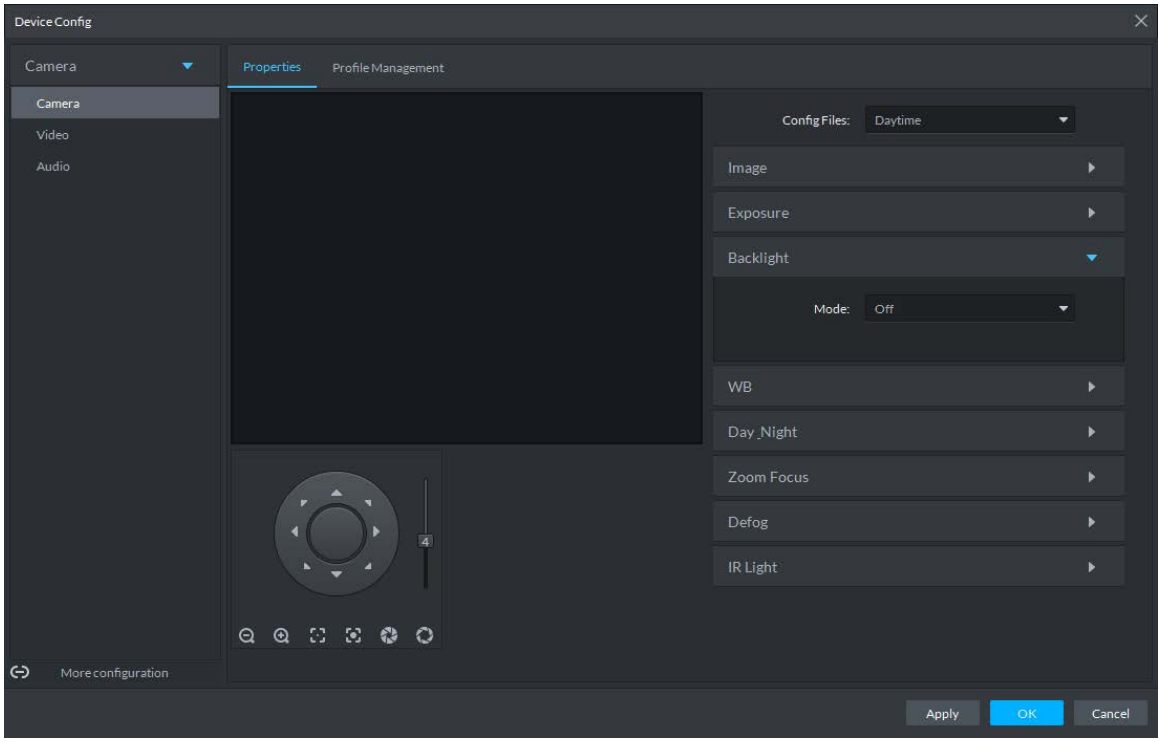


Table 4-18 Backlight mode description

Backlight mode	Description
SSA	The system adjusts image brightness automatically based on the environmental lighting conditions to show image details clearly.
Backlight Correction	You can select **Default** 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.
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 4-85. For details of the parameters, see Table 4-19.

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

Figure 4-85 WB

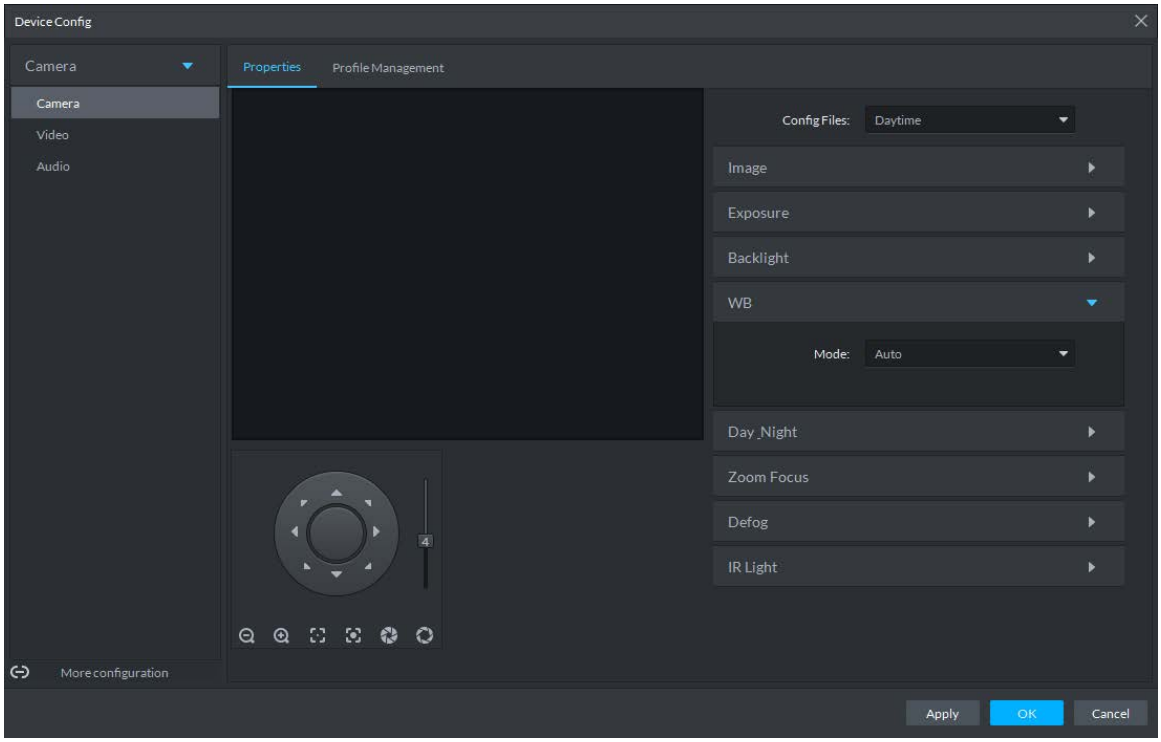


Table 4-19 WB mode description

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

Step 8 Click **Day & Night** to set up relevant parameters. See Figure 4-86. For details of the parameters, see Table 4-20.

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

Figure 4-86 Day/Night

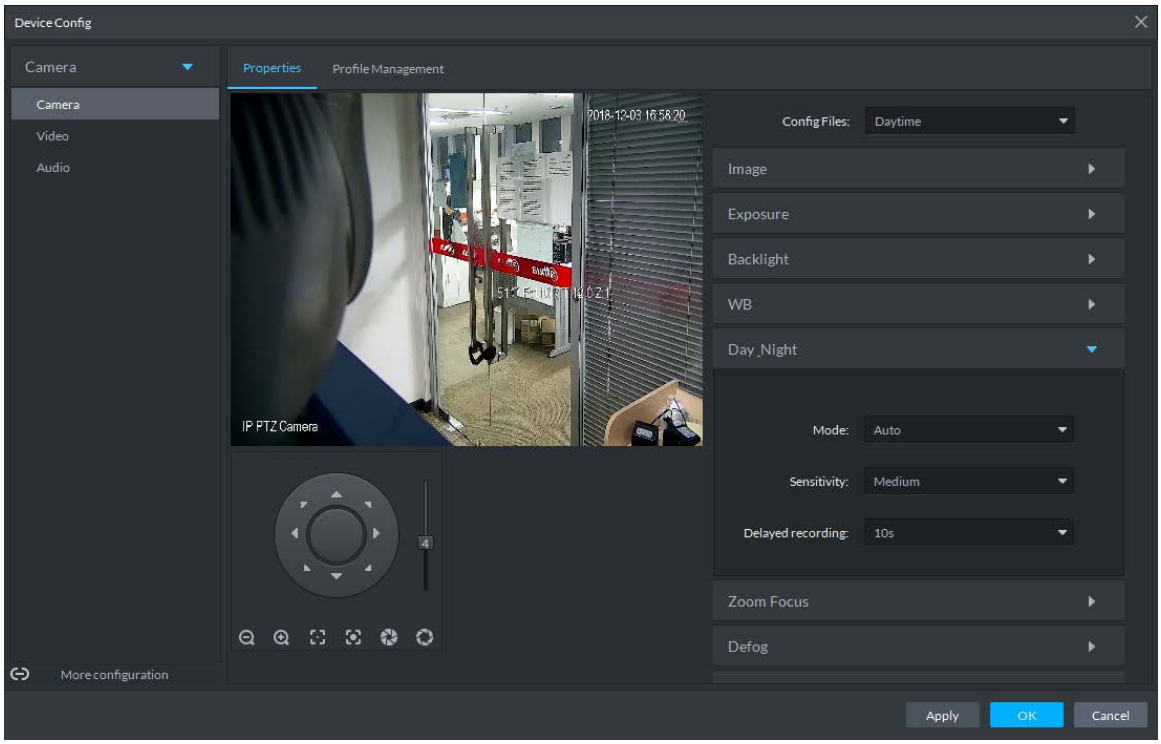


Table 4-20 Day/night mode parameter description

Parameter	Description
Mode	You can set up the image display of the camera to the Colored mode or the Black&White mode, including the following options: The **Day & Night** settings are independent from 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 4-87. For details of the parameters, see Table 4-21.

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

Figure 4-87 Defog

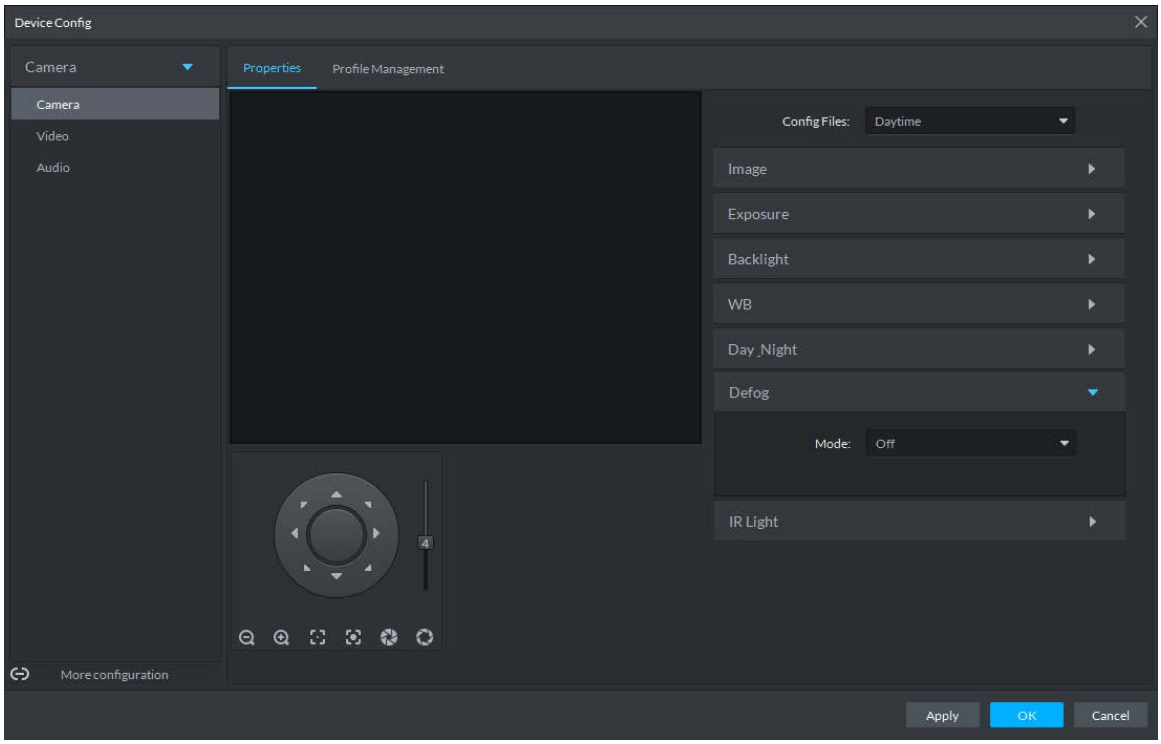


Table 4-21 Defog mode description

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

Step 10 Click **IR Light** to set up relevant parameters. See Figure 4-88. For details of the parameters, see Table 4-22.

Figure 4-88 IR light

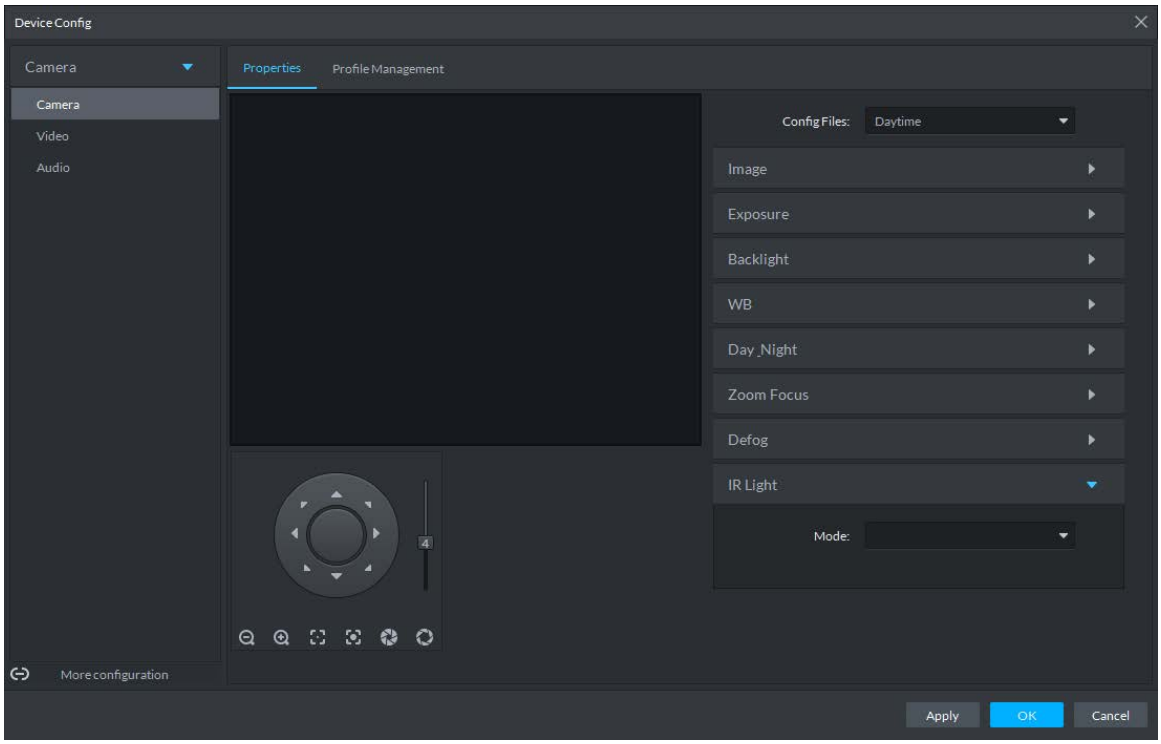


Table 4-22 IR light mode description

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

Step 11 Click **OK**.

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

4.3.4.1.2 Applying Config Files

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

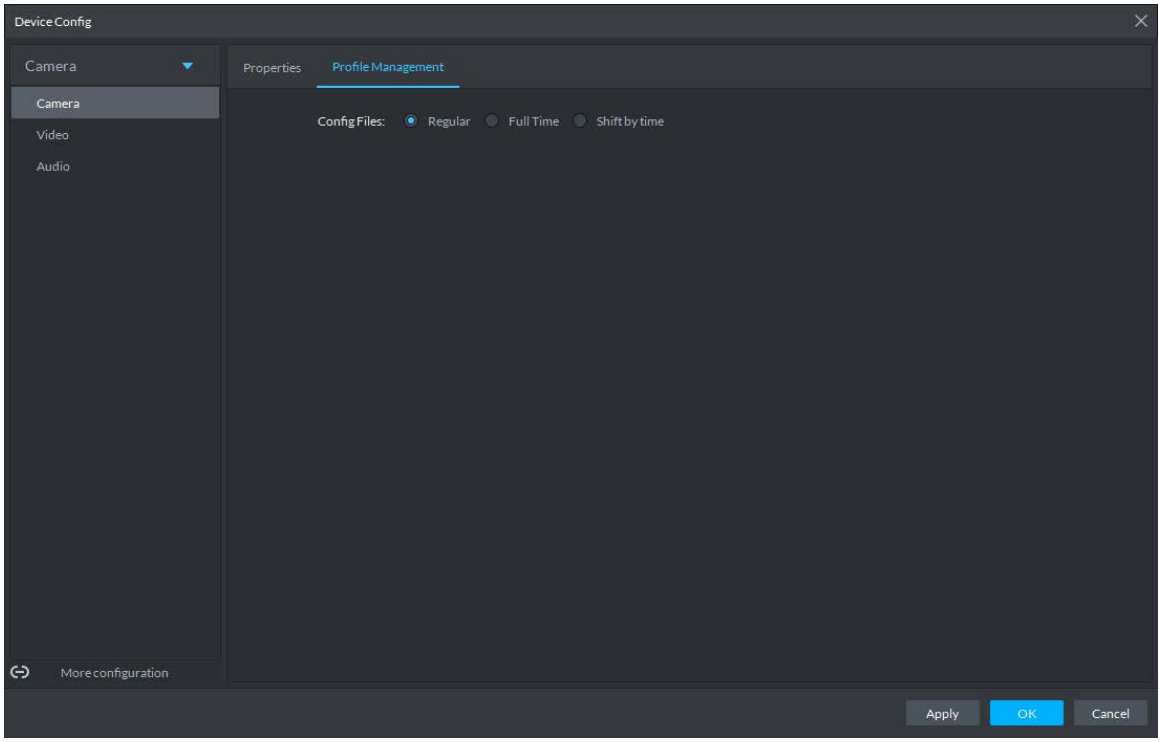
Step 1 Select **Camera > Camera > Properties > Profile Management**.

The **Profile Management** interface is displayed.

Step 2 Setting up config files.

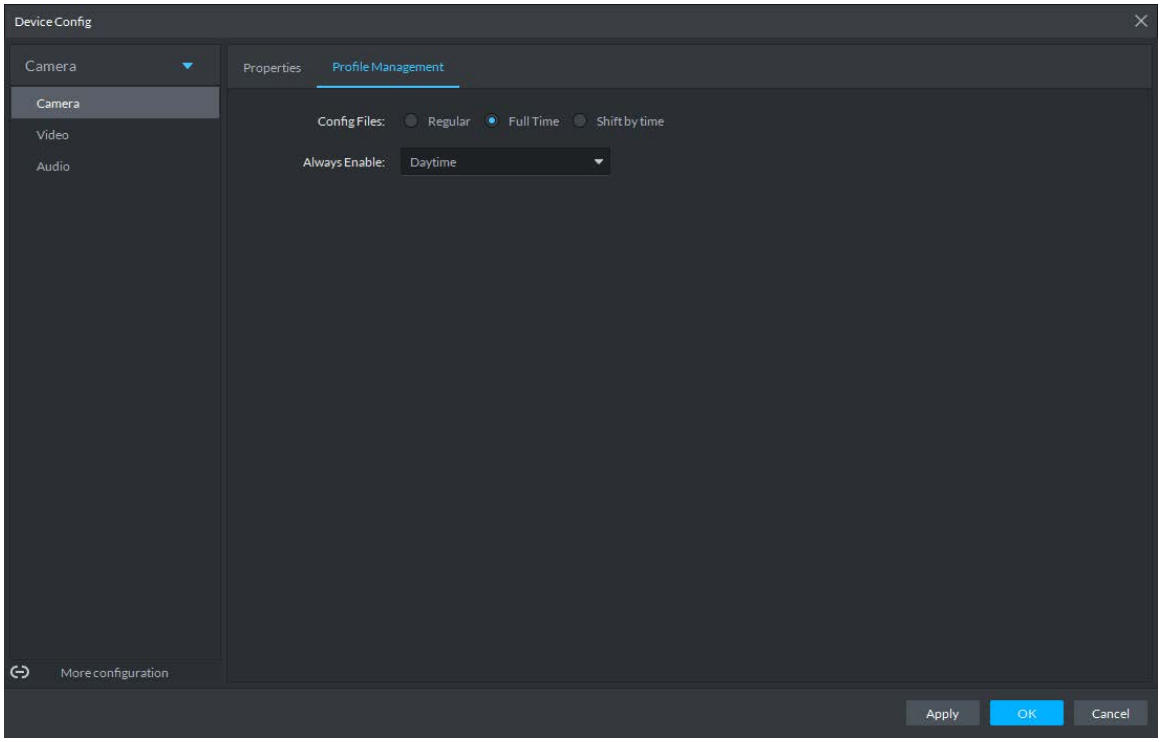
- When **Config Files** is set to **Regular**, the system monitors the objects as per regular configurations.

Figure 4-89 Regular



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

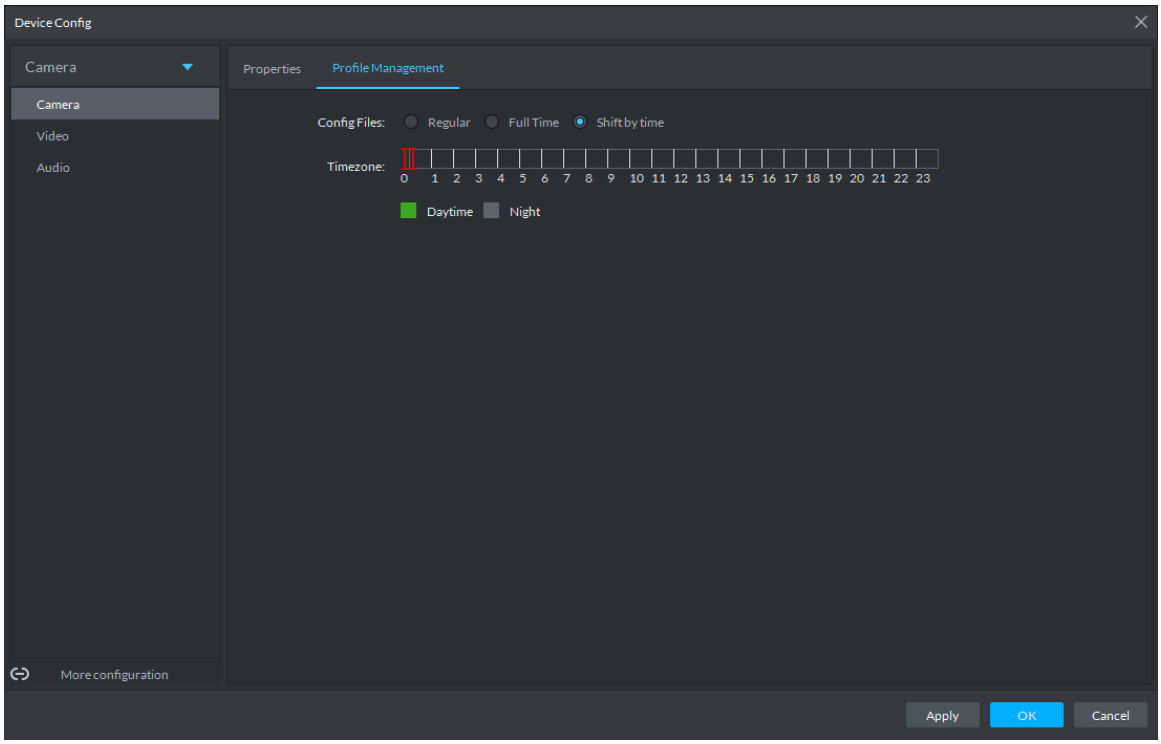
Figure 4-90 Full time



- When **Config Files** is set to **Shift by time**, you can drag the slider to set a period of time as daytime or night. For example, you can set 8:00–18:00 as daytime, 0:00–8:00 and

18:00–24:00 as night. The system monitors the objects in different time periods as per corresponding configurations.

Figure 4-91 Shift by time



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

4.3.4.2 Video

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

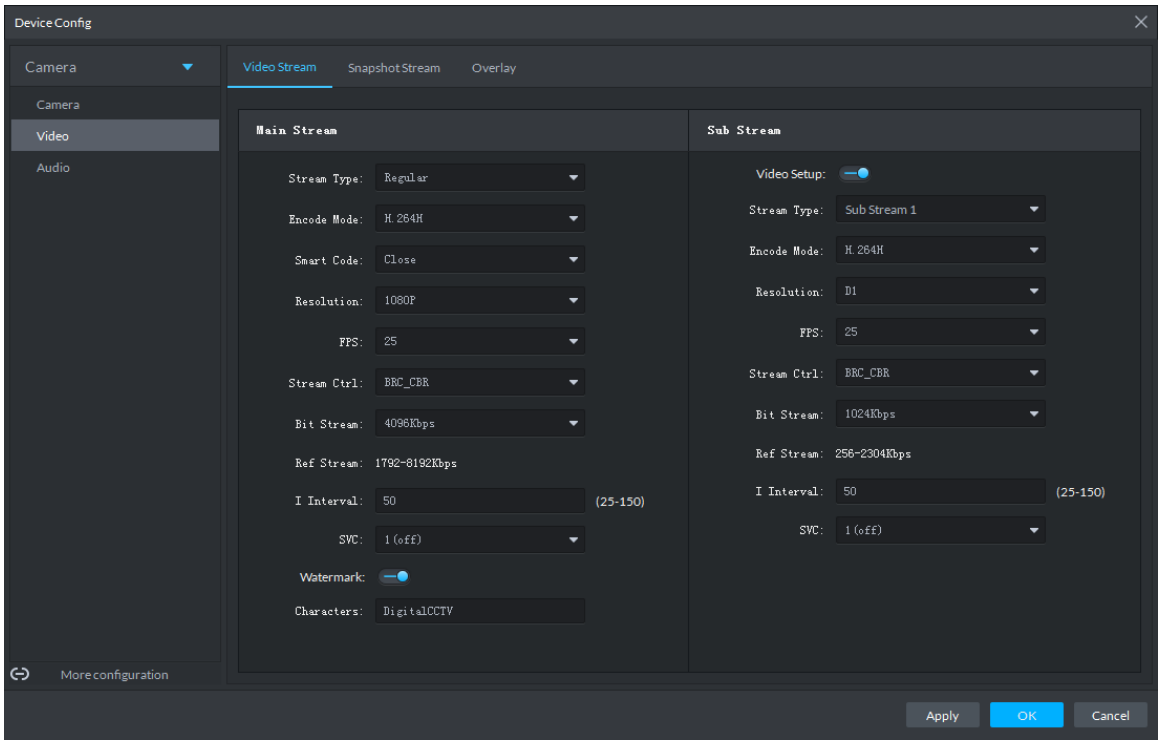
4.3.4.2.1 Video Stream

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

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

The **Video Stream** interface is displayed. See Figure 4-92.

Figure 4-92 Video stream



Step 2 To set up Video Stream, see Table 4-23 for the details of various parameters.

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

Table 4-23 Video stream parameter description

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

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

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

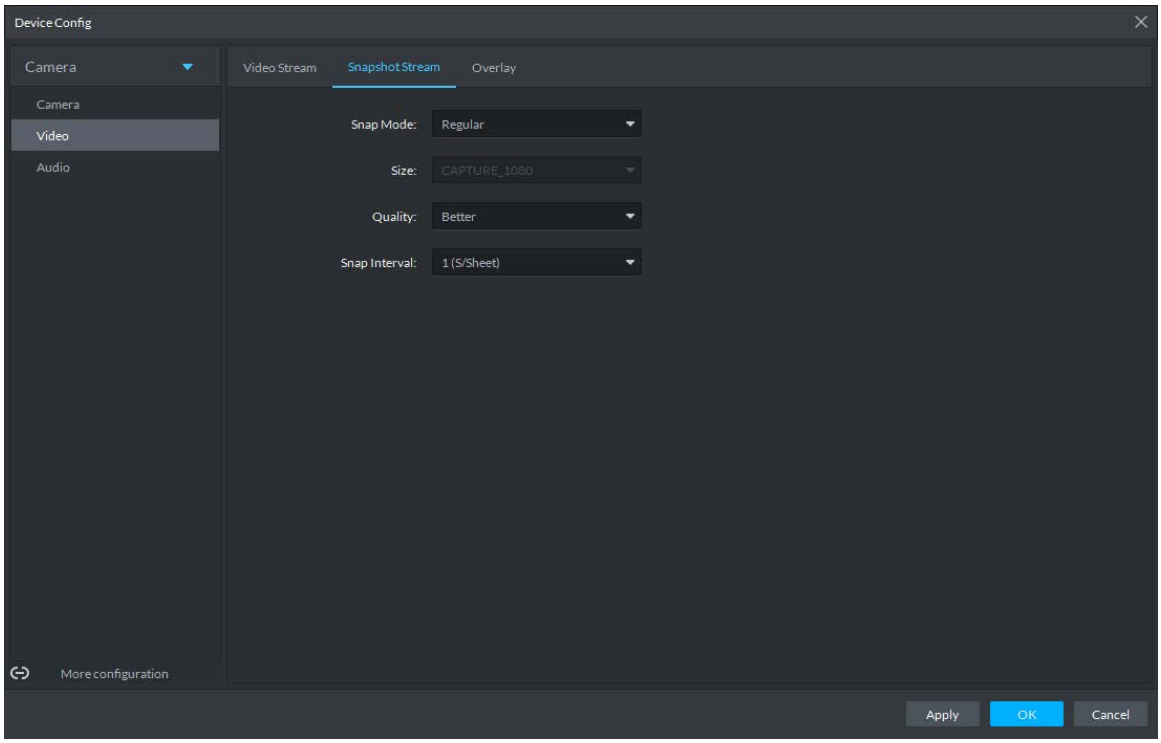
4.3.4.2.2 Snapshot Stream

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

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

The **Snapshot Stream** interface is displayed. See Figure 4-93.

Figure 4-93 Snapshot stream



Step 2 To set up Snapshot Stream, see Table 4-24 for the details of various parameters.

Table 4-24 Snapshot stream parameter description

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

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

4.3.4.2.3 Overlay

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

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

The **Overlay** interface is displayed.

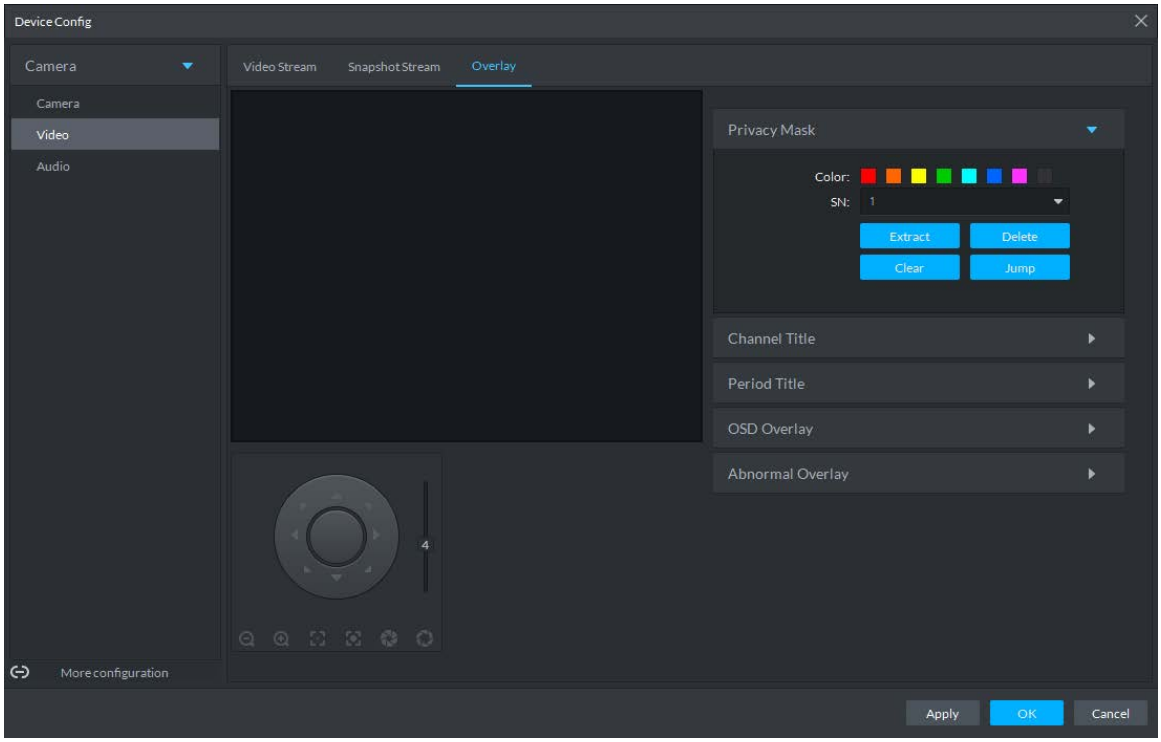
Step 2 (Optional) Set up **Privacy Mask**.

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

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

The **Privacy Mask** interface is displayed. See Figure 4-94.

Figure 4-94 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.

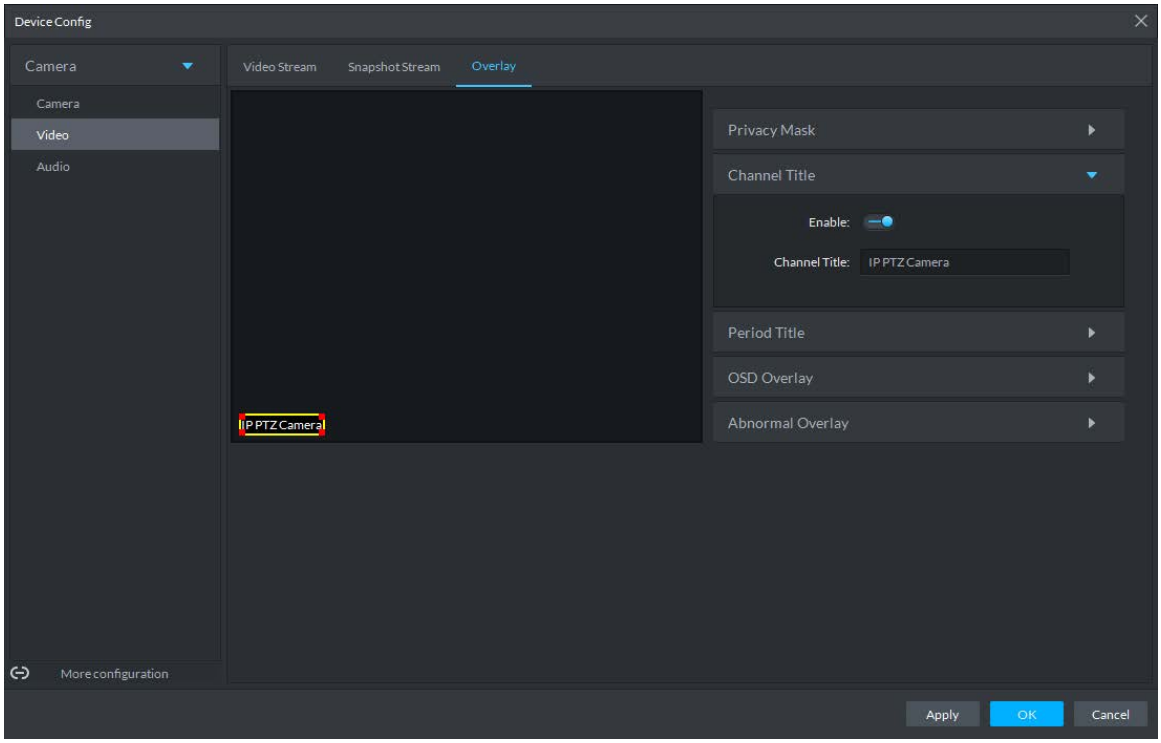
Step 3 (Optional) Set up Channel Title.

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 4-95.

Figure 4-95 Channel title



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

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

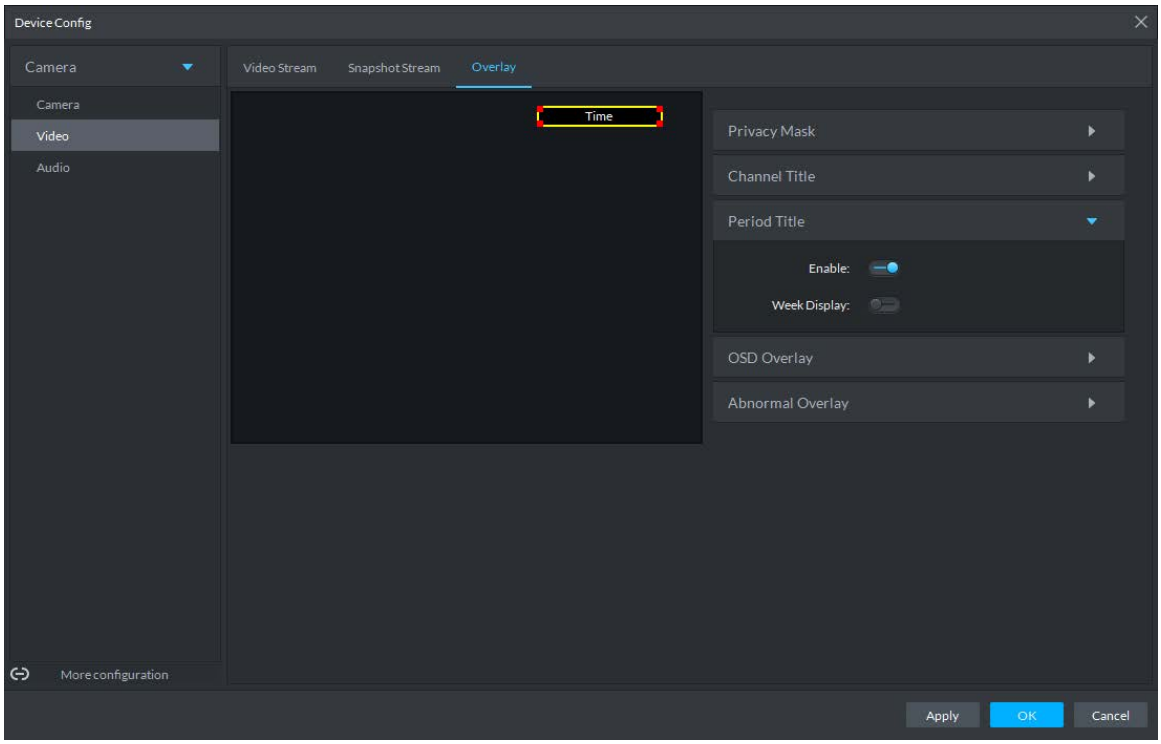
Step 4 (Optional) Set up **Period Title**.

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

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

   The **Period Title** interface is displayed. See Figure 4-96.

Figure 4-96 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.

4.3.4.3 Audio

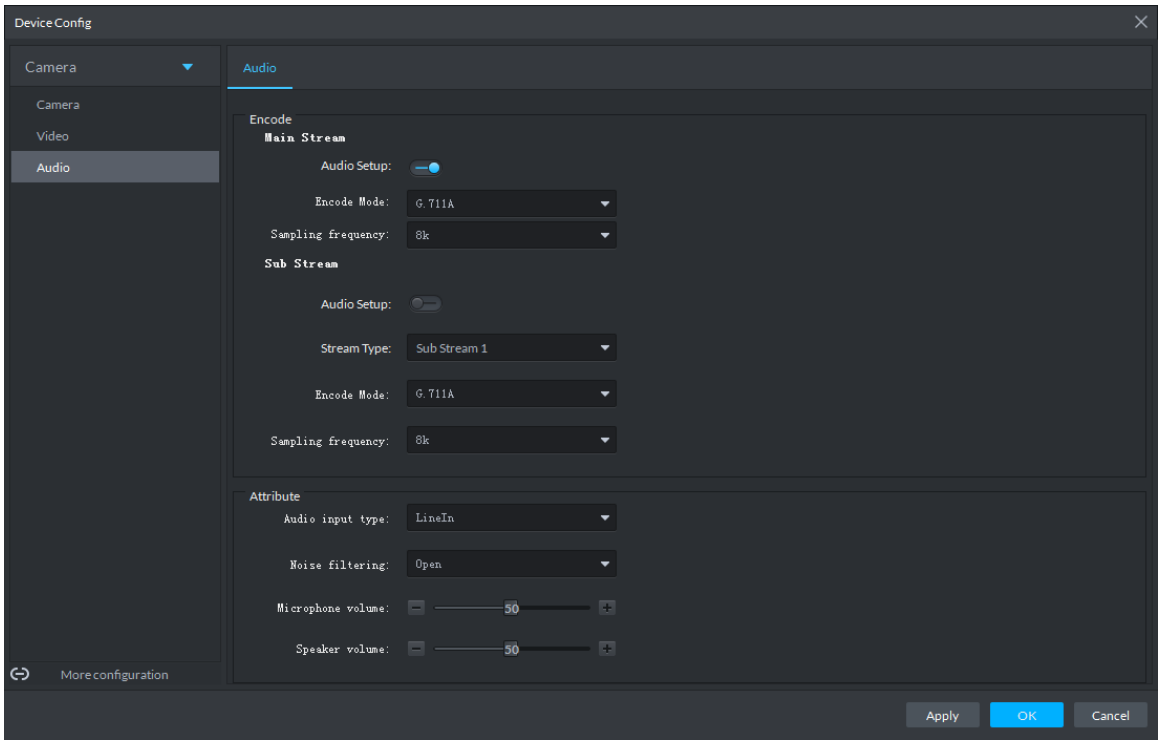
You can set some audio parameters such as Encode Mode, Sampling frequency, Audio input type, Noise filtering.

Some devices do not support audio functions.

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

The **Audio** interface is displayed. See Figure 4-97.

Figure 4-97 Audio



Step 2 To set up audio parameters, see Table 4-25 for details.

Table 4-25 Audio parameter description

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

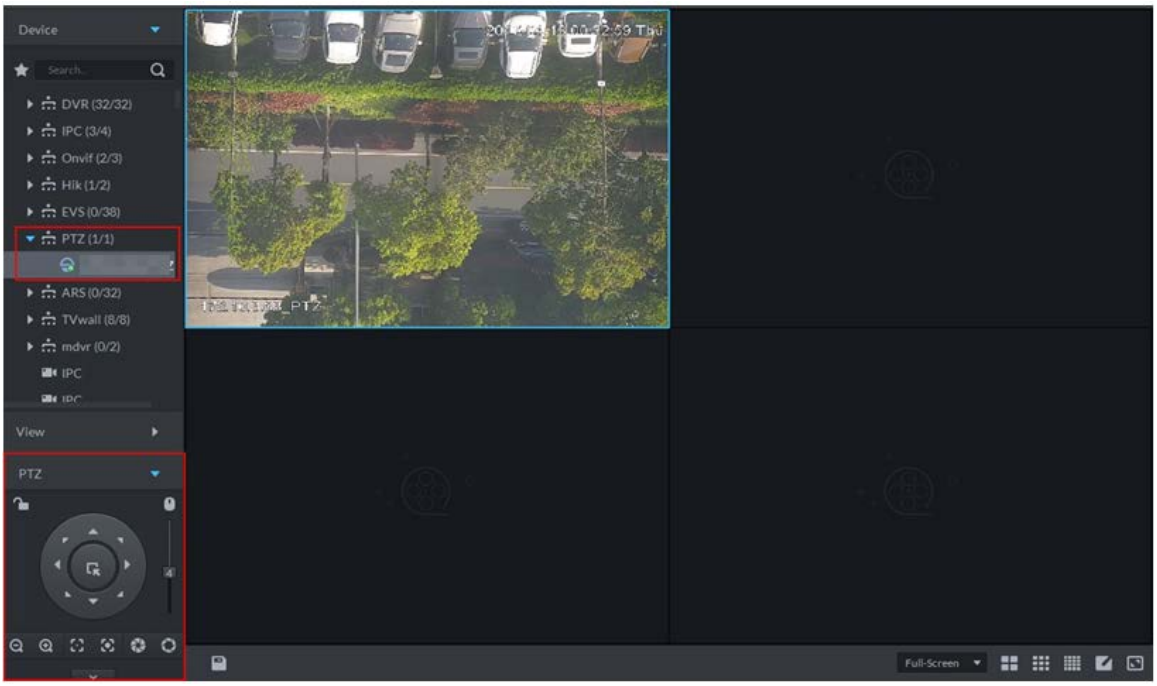
Step 3 Click **OK** to save the configurations.

4.3.5 Setting PTZ

4.3.5.1 PTZ Operation Interface

Step 4 On Preview interface, open video from the PTZ camera, you can see PTZ operation interface on the left. See Figure 4-98.

Figure 4-98 Live view



Step 5 Click  at the bottom of the interface to operate. See Figure 4-99.

Figure 4-99 PTZ

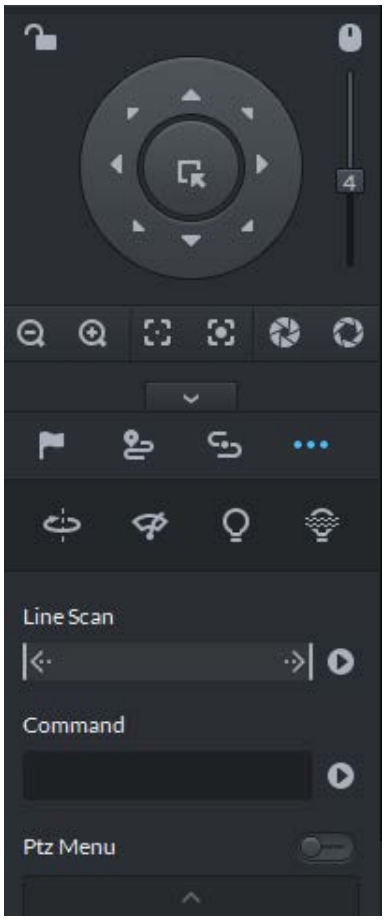


Table 4-26 PTZ operation description

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.
	From top to the bottom to adjust rotation speed of PTZ, to set the step size chosen from 1 to 8.
	Zoom, to control zoom operation of speed dome.
	Focus, to adjust focus.
	Aperture, to adjust brightness.
 	Set preset, tour, pattern, scan, rotation, wiper, light, IR light function, etc. Refer to"4.3.5.2 PTZ Settings " for more information.

4.3.5.2 PTZ Settings

4.3.5.2.1 Configuring Preset

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

Step 6 Click direction key of the PTZ to rotate the camera to the needed place.

Step 7 Click  .

Step 8 Place mouse over 1 and click  .

Step 9 Input preset point SN, and click  .

Adding preset point completed.

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

4.3.5.2.2 Configuring Tour

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

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

Step 1 Click  .

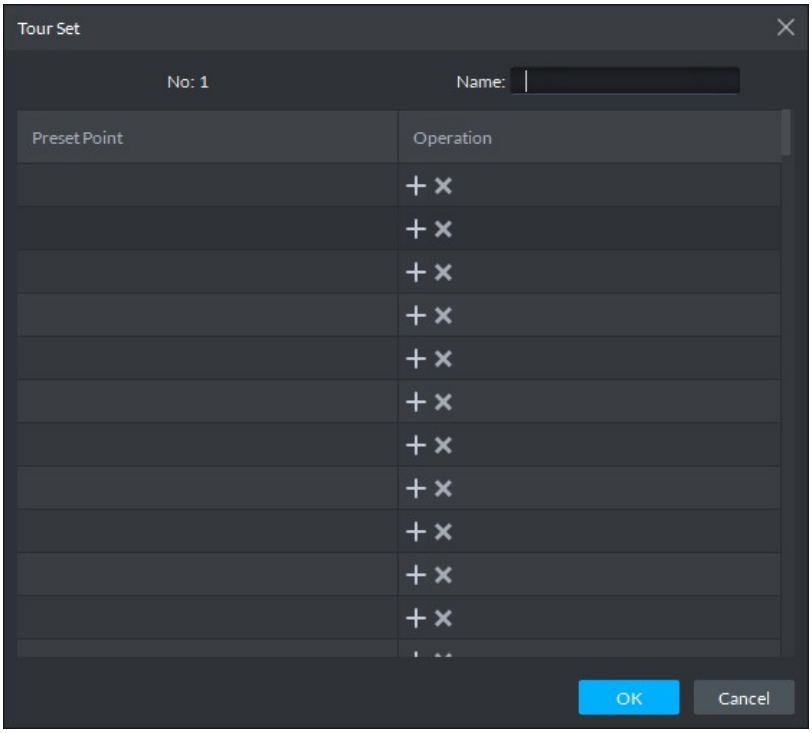
Step 2 Place mouse over 1 and click  .

New tour dialogue box pops up.

Step 3 Input name, and click Operation bar  .

Choose preset points from the dropdown list on the left. See Figure 4-100.

Figure 4-100 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.

4.3.5.2.3 Configuring Pattern

Pattern is equivalent to a record process.

Step 1 Click .

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

Step 3 Click to complete pattern setup.

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

4.3.5.2.4 Configuring Scan

Step 1 Click .

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

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

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

4.3.5.2.5 Enable/Disable Pan

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

4.3.5.2.6 Enable/Disable wiper

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

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

4.3.5.2.7 Enable/Disable light

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

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

4.3.5.2.8 Enable/Disable IR light

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

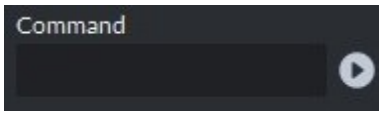
4.3.5.2.9 Configuring custom commands

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 4-101.

Figure 4-101 Command



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

4.3.5.2.10 PTZ Menu

Step 1 Click .

The PTZ menu is shown as in Figure 4-102.

Figure 4-102 Menu

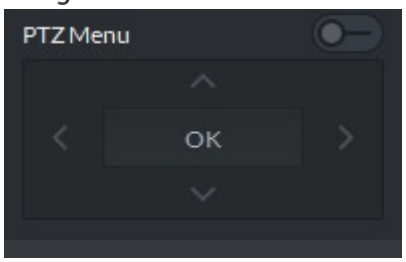


Table 4-27 PTZ menu parameter description

Parameters	Description
/	Up/down button. Move the cursor to the corresponding item.
/	Left/right. Move the cursor to set parameters.
	Click to enable PTZ menu function. The main menu is displayed 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 4-103.

Figure 4-103 Display main menu interface

Table 4-28 Main menu parameter description

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

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

4.3.6 Smart Track

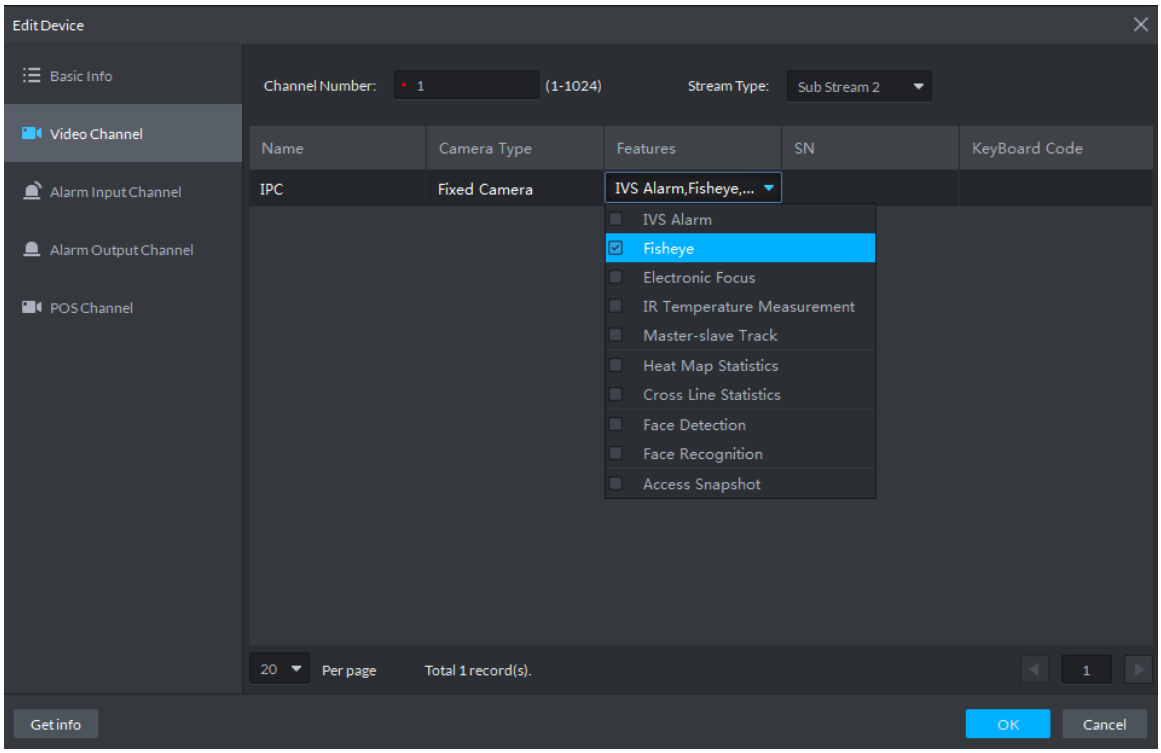
DSS Client supports smart track which links fisheye speed dome to general speed dome to better control each monitoring position.

4.3.6.1 Adding Device

Step 1 Add fisheye and speed dome. For more details, see"4.1.2.4 Adding Device ."

Step 2 On **Device** interface, click next to the fisheye device, then you can modify the device features as **Fisheye**. See Figure 4-104.

Figure 4-104 Fisheye device



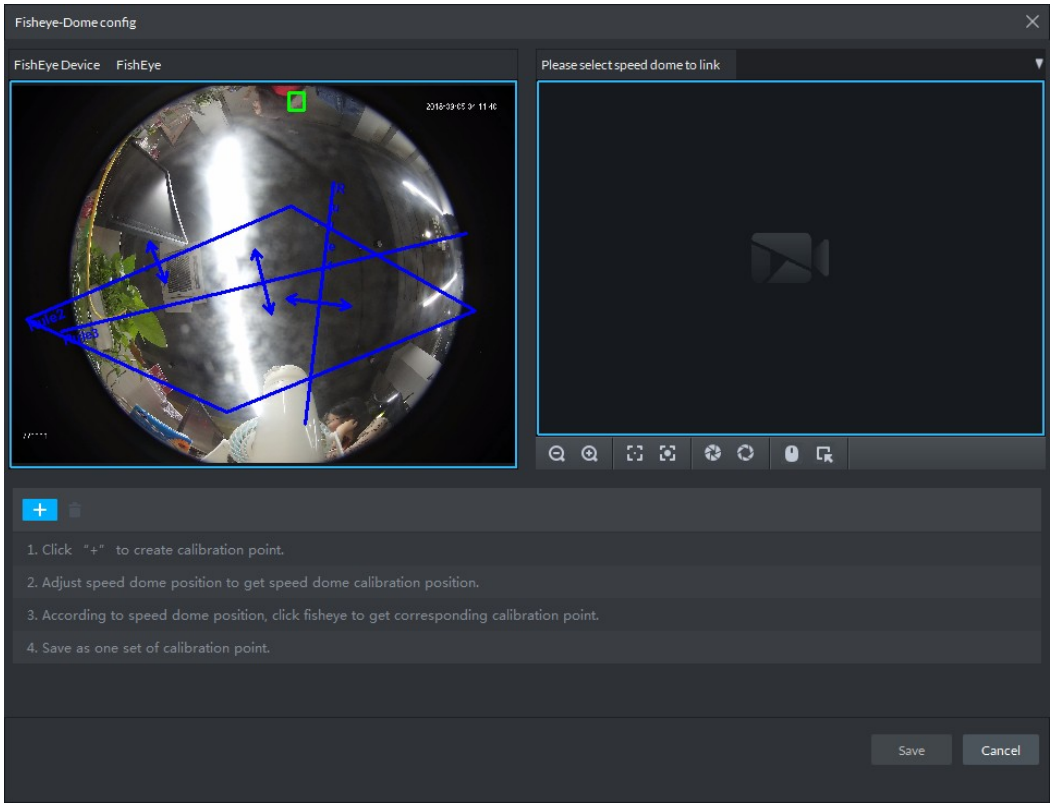
4.3.6.2 Adding Smart Track Config

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

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

The **Smart track** interface is displayed. See Figure 4-105.

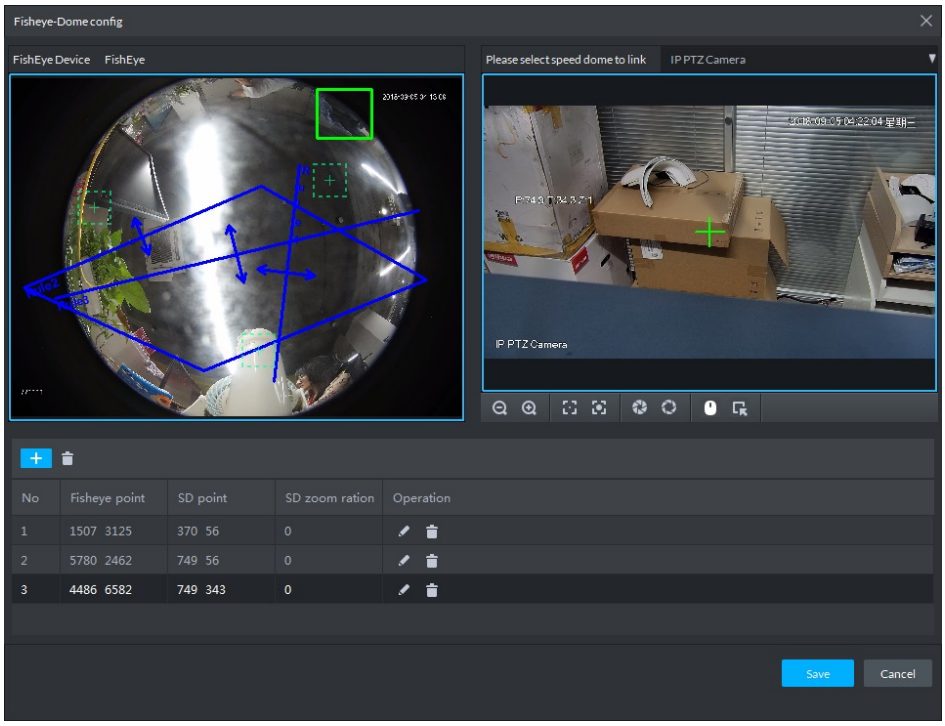
Figure 4-105 Smart track config



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

Step 3 Click + and then move the ⊕ of the fisheye on the right to select a position. Click 🖱 on the general PTZ camera to find the position. Adjust the PTZ camera to find the position and move the PTZ to the center position (The green cross on the image). See Figure 4-106.

Figure 4-106 Configure calibration point



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

Step 4 Click to save the calibration point.

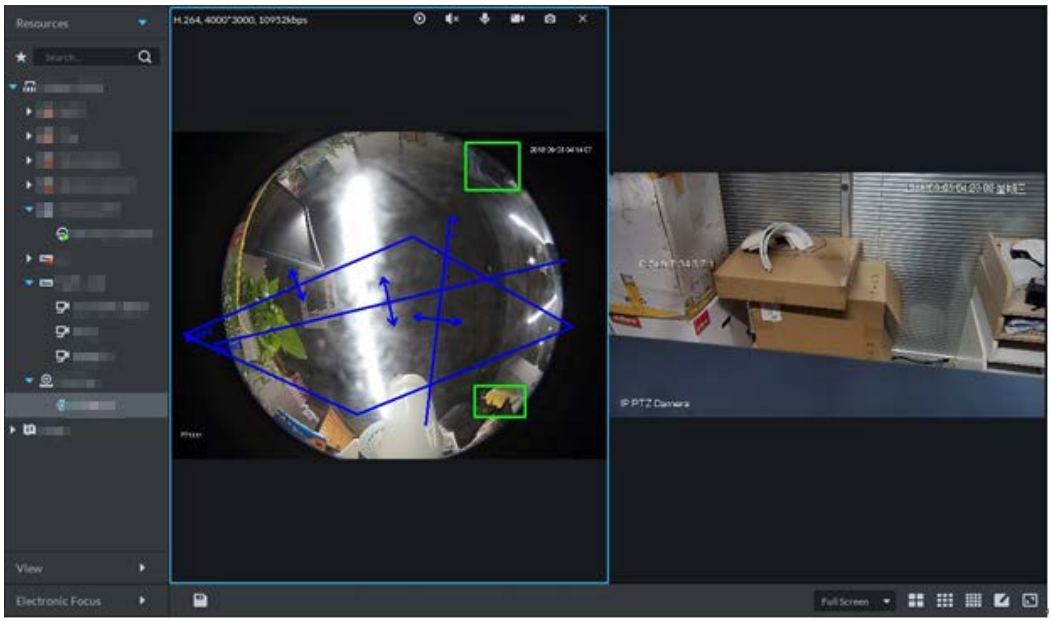
Refer to above steps to add at least three calibration points. These three points shall not be on the same straight line.

Step 5 Click **Save**.

4.3.6.3 Enabling Smark Track Function

Step 1 Select the fisheye device on the device tree and then right click to select **Smart Track**. See Figure 4-107.

Figure 4-107 Smart track



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

4.3.7 Smart Track

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

To add independent bullet camera and PTZ camera, you need to define bullet and PTZ camera using config tool in advance. See config tool manual for details.

4.3.7.1 Preparations

Step 1 Before implementing smart track (bullet + PTZ camera), it needs to add bullet and PTZ camera from **Device**. For detailed steps, refer to"4.1.2.4 Adding Device."

Step 2 Click after adding bullet, and select **Main Sub Track**. Tracking function can be realized after configuring main sub track.

Step 3 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.

4.3.7.2 Configuring Smart Track Linkage

For separate bullet camera and PTZ camera, or integrated device, you need to calibrate and link the bullet camera and PTZ camera.

Calibrating camera:

- Single-sensor bullet camera

Select two views to calibrate. Mark 4 coordinates in each view.

- Multi-sensor bullet camera

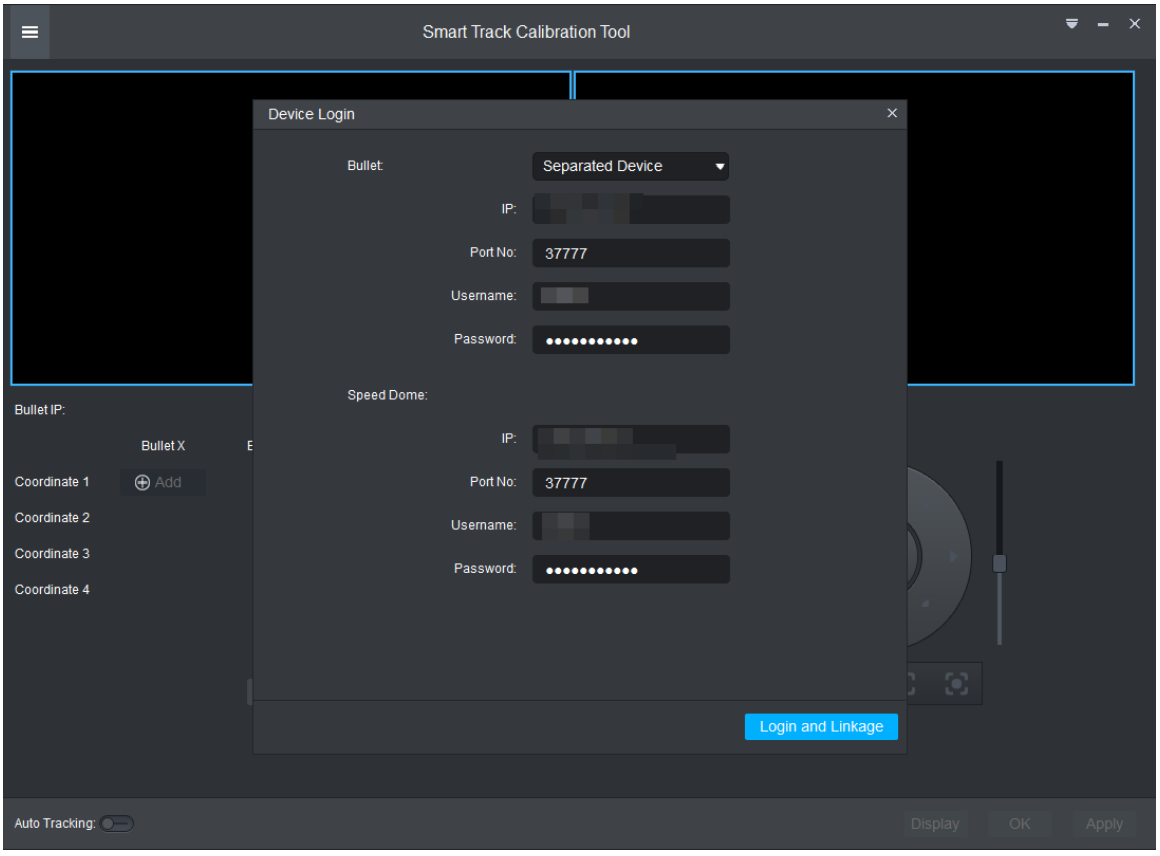
  Calibrate one view for each sensor. Mark 4 coordinates in each view.

Step 1 Right-click the bullet camera in the resrouce tree of **Live View** interface and select **Main-sub config**.

Step 2 Configure bullet camera and PTZ camera.

- Separate cameras: parameters are different between the two cameras. The bullet camera parameters have been configured in Figure 4-108. Fill in PTZ camera parameters as required.
- Integrated device: login parameters are the same between the two cameras. You do not need to fill in other parameters.

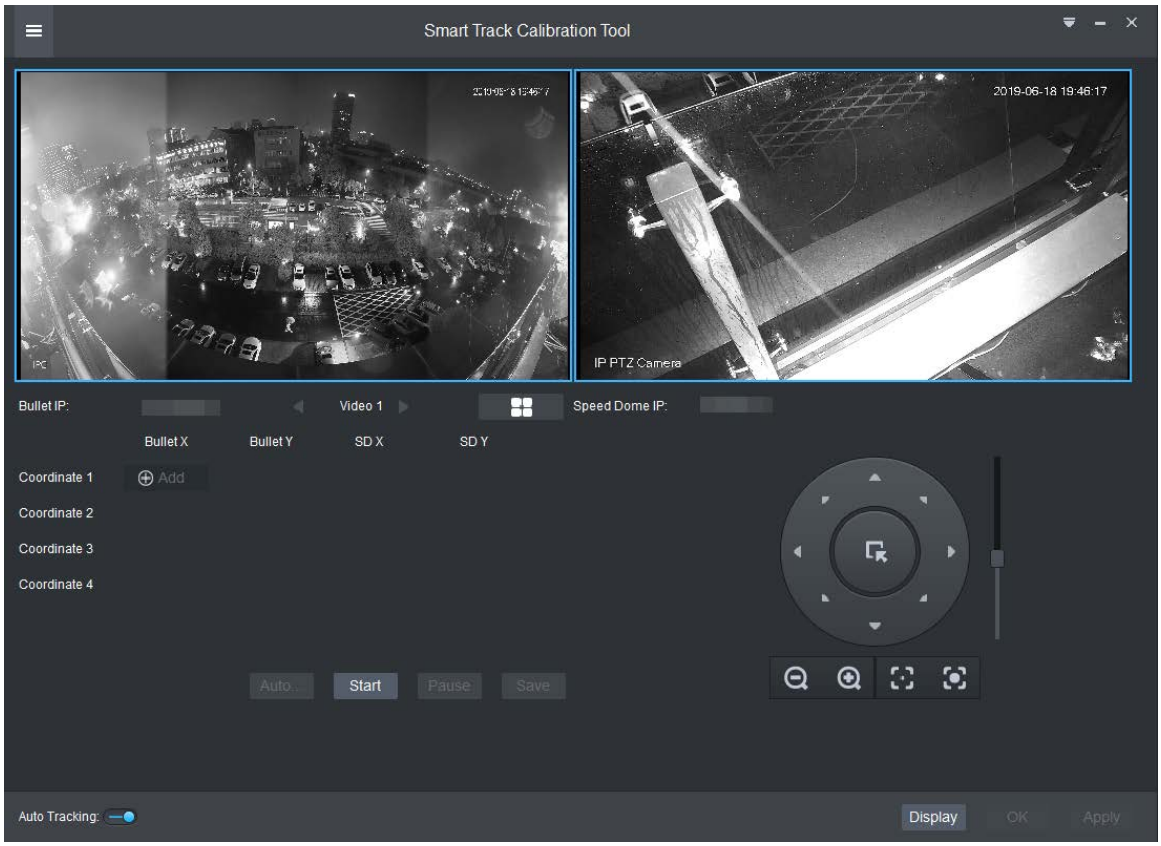
Figure 4-108 Device login



Step 3 Click **Login** and **Linkage**.

The **Smart Track Calibration Tool** interface displays. See Figure 4-109.

Figure 4-109 Smart track calibration tool



Step 4 Use the PTZ control buttons to adjust the view on the right until it is similar with the left view.

Step 5 Click **Start**.

To ensure accuracy, PTZ buttons are disabled during the calibrating operation. If needed, you can click Pause to enable the buttons. When you have finished PTZ operation, you can click **Start** to continue calibrating.

Step 6 Calibrate coordinates.

1) Click **Add** behind **Coordinate 1** and then two frames appear in the bullet camera view. Move the frames to similar positions. Frame center coordinates appear in the four value frames behind **Coordinate 1**.
2) Click **Add** to complete calibrating the other three coordinates.
3) Click **Save**.
4) Click **OK**.
   - ◇ If the bullet camera is multi-sensor, system will display calibrating interface of the next sensor.
   - ◇ If the bullet camera is single-sensor, system will display the calibrating interface of the second four-coordinate group.
5) Go on and complete the rest coordinates.
   For multi-sensor camera, you need to calibrate each sensor; for single-sensor camera, you need to complete calibrating two four-coordinate groups. The **Apply** button is activated when finishing calibrating all coordinates.
6) Click **Apply**.

4.3.7.3 Applying Smart Track

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

4.3.7.3.1 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 4-110. Click the red spot on the bullet image, and the PTZ central point will move to the corresponding location automatically.

Figure 4-110 Manual positioning

Before Positioning

After Positioning

4.3.7.3.2 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.

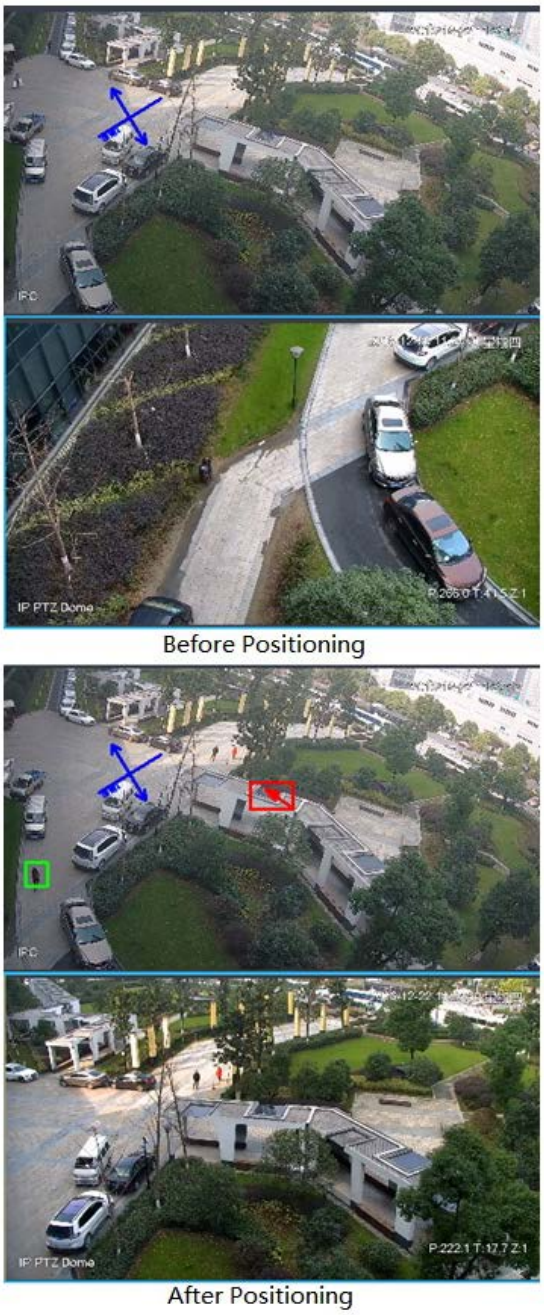
- Draw rectangular box from upper left to lower right, zoom in after being positioned by PTZ camera. See Figure 4-111.
- Draw rectangular box from lower right to upper left; zoom out after being positioned by PTZ camera. See Figure 4-112.

Figure 4-111 3D positioning (Zoom in after positioning)

Before Positioning

After Positioning

Figure 4-112 3D positioning (Zoom out after positioning)



4.3.7.3.3 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 4-113 Manual track

Before Tracking

After Tracking

4.3.7.3.4 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 4-114 and Figure 4-115.

Figure 4-114 Auto track

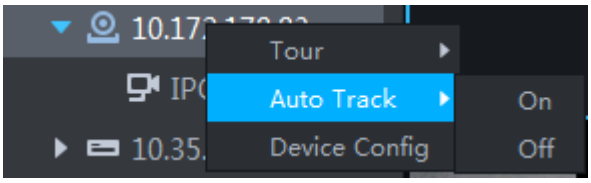


Figure 4-115 Auto track

Before Tracking

After Tracking

4.3.7.3.5 Preset Return

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

4.3.8 View

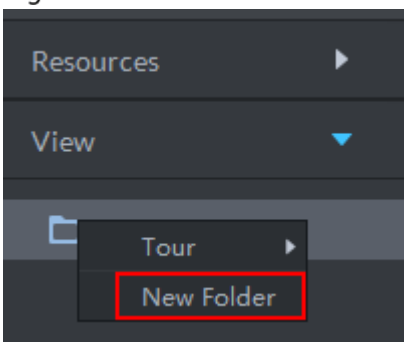
4.3.8.1 Creating View

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

Step 1 Create groupd.

1) Click **View** tab on the **Live View** interface.
2) Right click **View**, select **New Folder**, and see Figure 4-116.
   The **New Folder** interface is displayed.

Figure 4-116 New folder

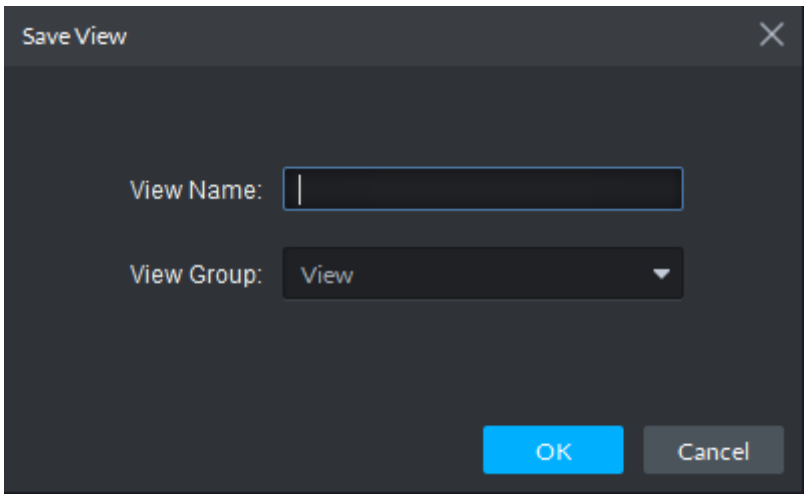


3) Enter folder name, click **OK**.
   All new groups are displayed under view.

Step 2 Create view.

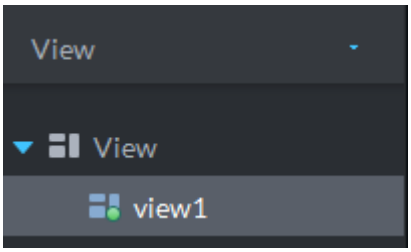
1) On **Live View** interface, click  according to your needs.
   The **Save View** interface is displayed. See Figure 4-117.

Figure 4-117 Save view



2) Enter **View Name**, select **View Group** and click **OK**.
   New view is created under view group. See Figure 4-118.

Figure 4-118 Generate view



4.3.8.2 Previewing View

- Live view

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

- Tour

  On Live View interface, right click view group or root node, select **Tour** and tour period. See Figure 4-119. The system tours according to view group or root node; see Figure 4-120. Click  to stop tour.

Figure 4-119 Entering video tour interface

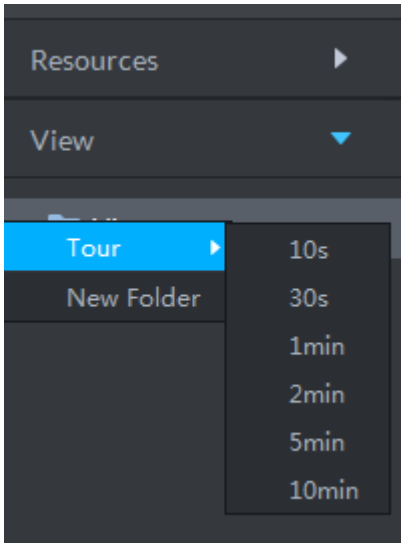


Figure 4-120 View tour

4.3.9 Favorites

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

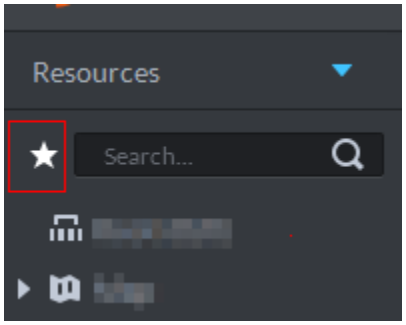
4.3.9.1 Creating Favorites

Step 1 Create favorites.

1) On **Live View** interface, click . See Figure 4-121.

The favorites list is displayed.

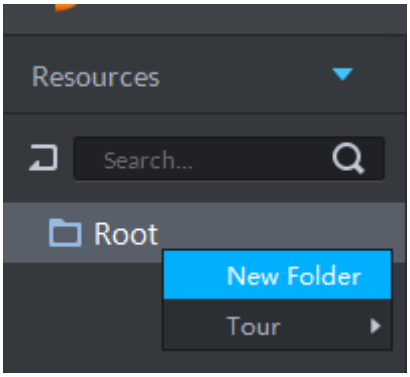
Figure 4-121 Enter favorites list



2) Right click root node or created favorites, select **New Folder**. See Figure 4-122.

The **Create Folder** interface is displayed.

Figure 4-122 Favorites list



3) Enter folder name, click **OK**.

Selected root node or favorites generates lower-level favorites.

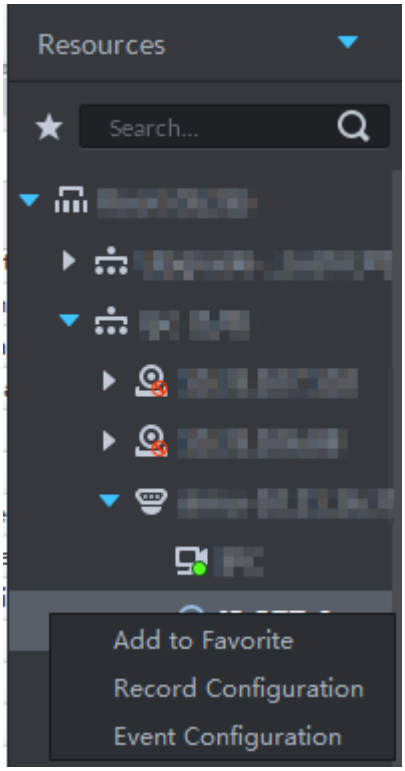
4) Click  .

The system returns to device list.

Step 2 Favorite channel.

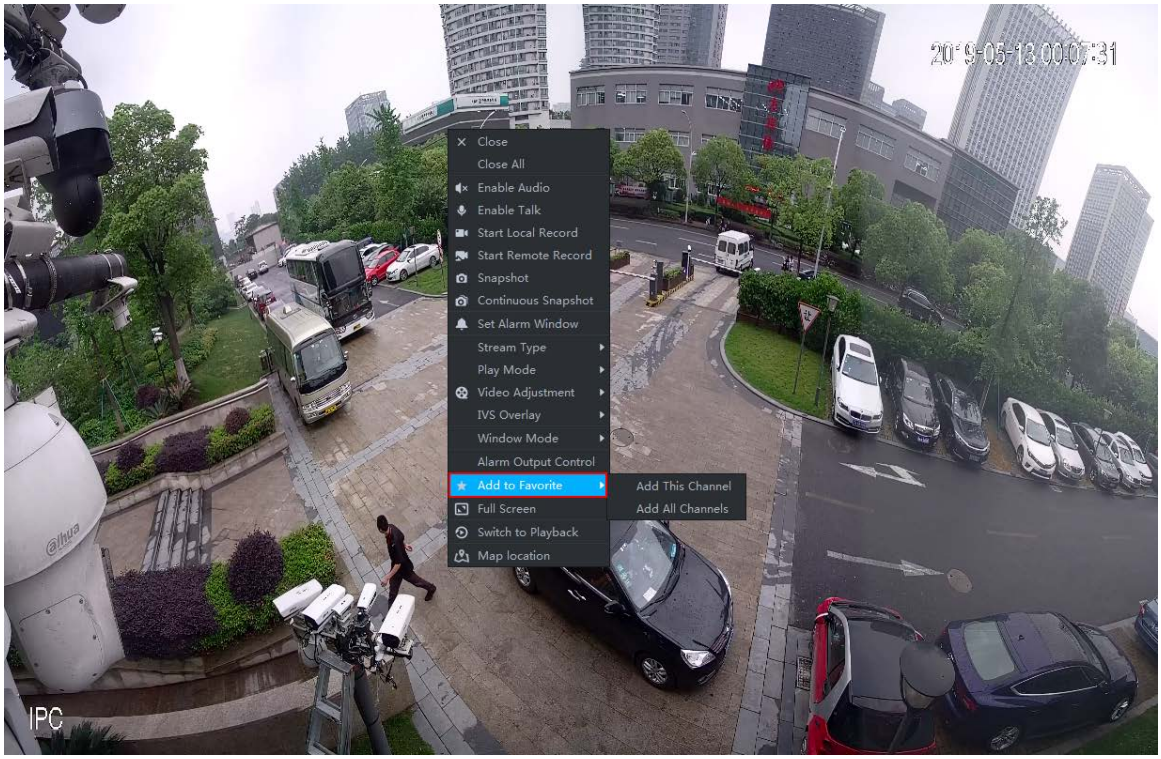
- In the device list on **Live View** interface, right click channel, select **Add to Favorites**, and add the channel to favorite according to system prompt. See Figure 4-123.

Figure 4-123 Favorite channel (1)



- On **Live View** interface, right click the window with live view, and select **Add to favorite**, add it to favorite according to system prompt. See Figure 4-124.

Figure 4-124 Favorite channel (2)



4.3.9.2 Viewing Favorites

- Live view

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

- Tour

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

4.3.10 Region of Interest (RoI)

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

On **Live View** interface, right click the window under live view, select **Split Mode**, and see Figure 4-125. The split image is displayed. For example, select 1+3 mode. See Figure 4-126.

Figure 4-125 Split mode

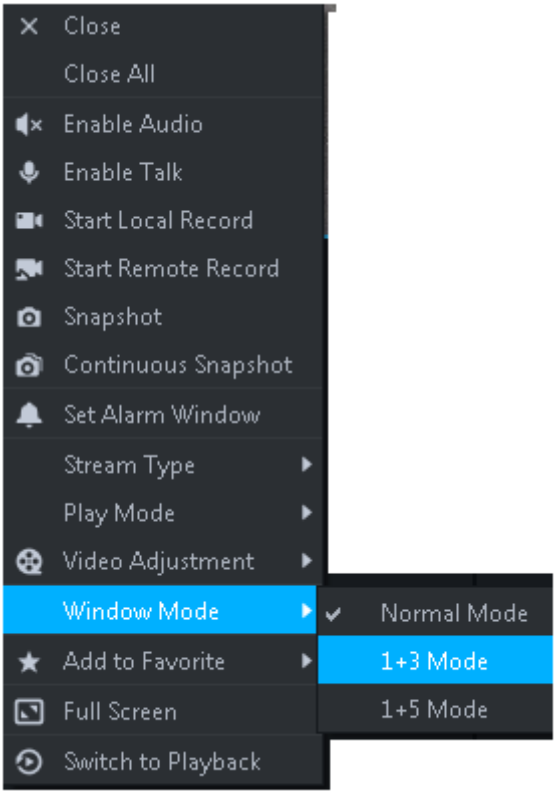
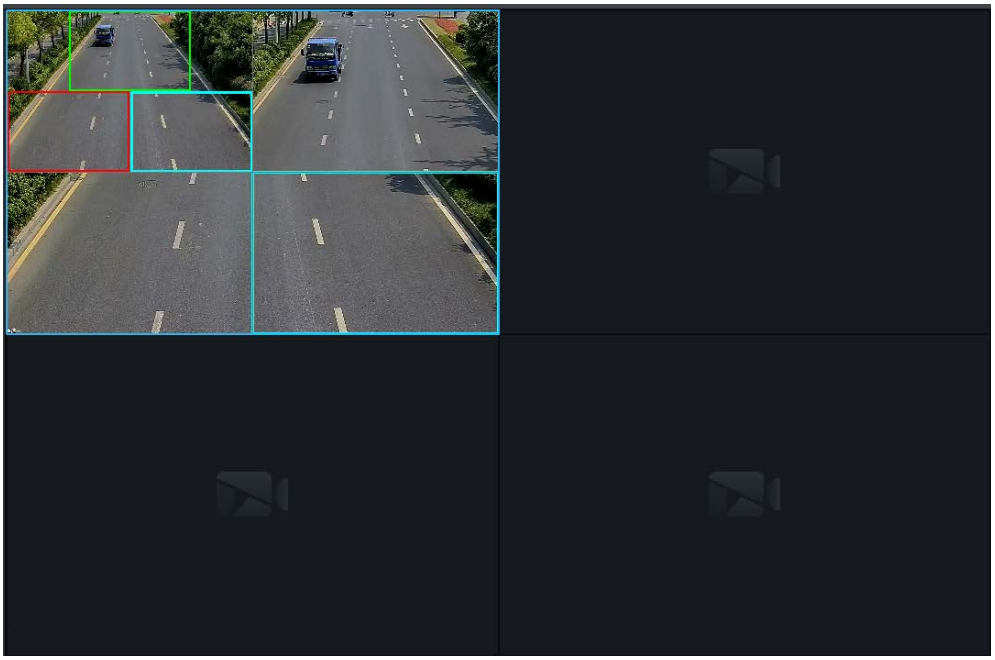


Figure 4-126 1+3 mode



4.4 Record Playback

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

If neither device nor platform is configured with record plan, then you can search no video. If you want to configure platform record plan, refer to"4.1.5 Setting Record Plan" for more details.

4.4.1 Entering Record Playback Interface

On client homepage, click **Record Playback**. The **Record Playback** interface is displayed. For interface description, see Table 4-29.

Figure 4-127 Recording playback interface

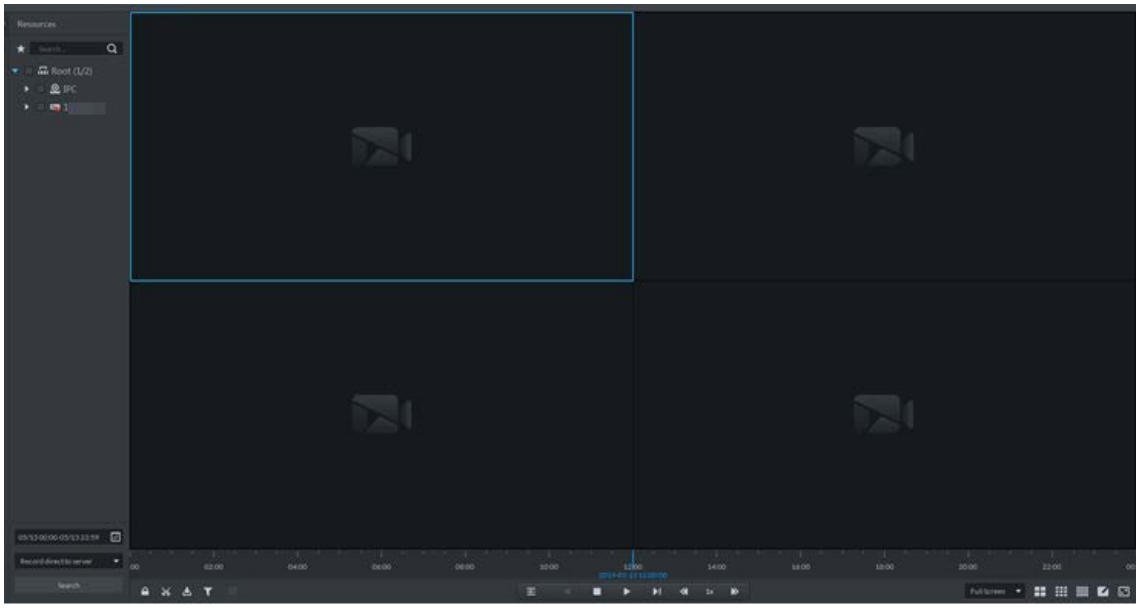


Table 4-29 Record playback icon description

Icon	Description
	Lock the video stored on server within some period of designated channel. Locked video will not be overwritten when disk is full.
	Cut video
	Download video
	Filter video according to record type.
	Make dynamic detection analysis over some area of the record image, it only replays the video with dynamic image in the detection area.
	Playback record files of the same period from different channels on selected windows.
	Stop/pause playback
/	Frame by frame playback/frame by frame backward.
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.

4.4.2 Playback Video

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

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

Step 2 Select window with video, click .

The corresponding window plays video of the channel. See Figure 4-128. For operation description, see Table 4-30.

Figure 4-128 Playback video

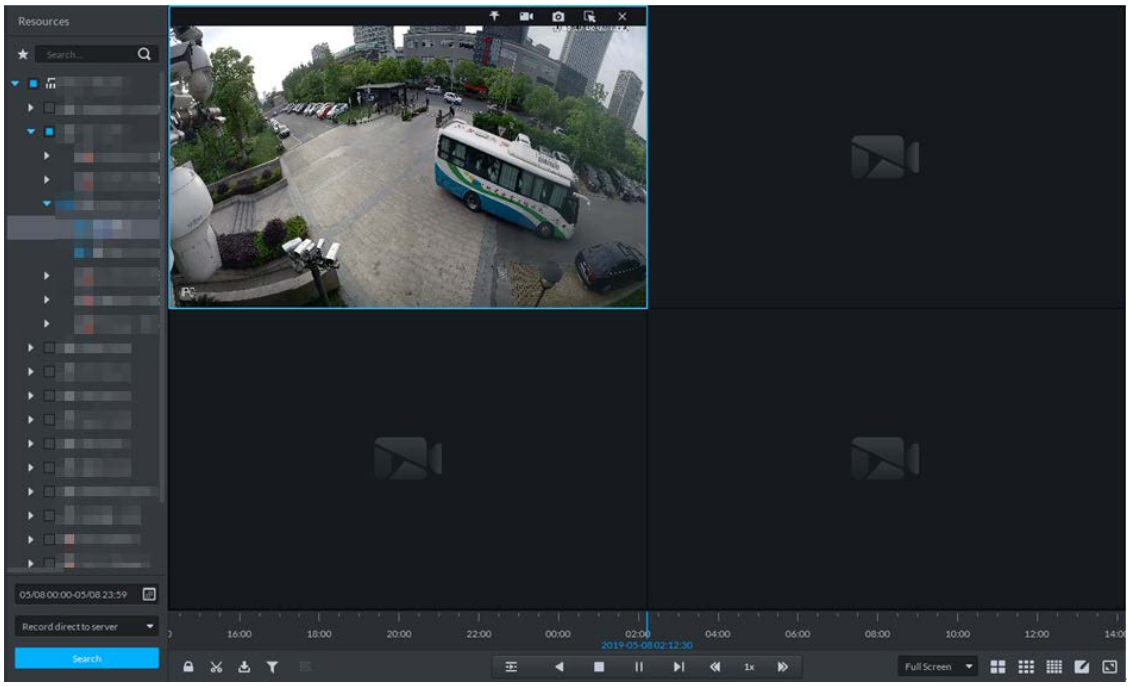


Table 4-30 Shortcut menu description

Icon	Icon Name	Description
	Record Tagging	Mark the record if you are interested in, convenient for future search. For detailed operations, see"4.4.4 Tagging Record."
	Local Record	Click the icon and system begins to record audio and video of current video window, recording duration is displayed on the upper left corner of the window; click the icon again, stop record and store to local PC. The default save path is"C:\DSS\Client\Record\". If you want to modify save path, refer to"4.2.5 Setting Recording Parameter."
	Snapshot	Save the image in the form of snapshot (one snapshot for once). Default save path is"C:\DSS\Client\Picture\". If you need to modify save path, refer to"4.2.4 Setting Snapshot."
	Zoom in	Select and zoom in regionally, you can scroll the mouse to zoom in or out.
	Close	Click the icon to close video.

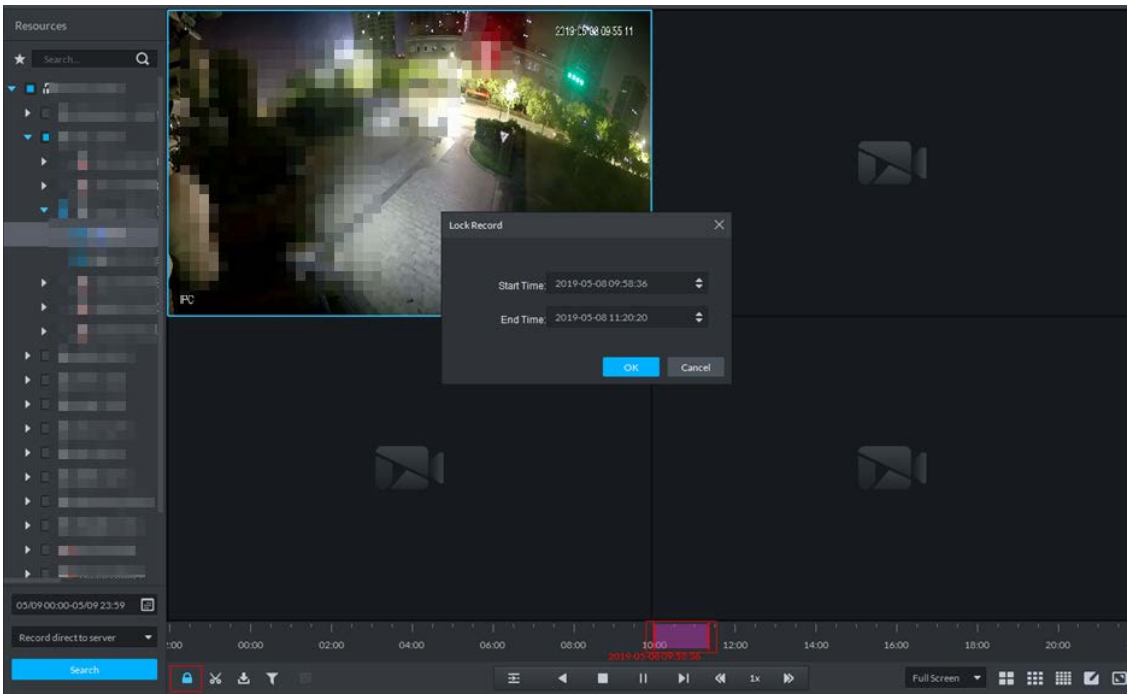
4.4.3 Locking Record

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

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

Step 2 Click at the bottom of the **Record Playback** interface (make sure the window has the record). The system pops out **Lock Record** interface. See Figure 4-129.

Figure 4-129 Select lock time



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

4.4.4 Tagging Record

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

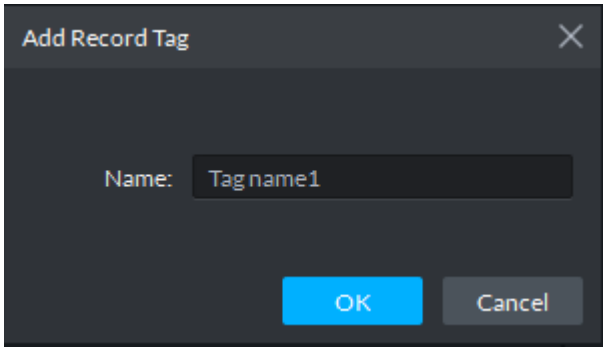
Step 1 On Record Playback interface, set search condition and search video.

Step 2 Select video, click  and play video.

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

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

Figure 4-130 Add record tag



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

4.4.5 Record Type Filter

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

Step 1 On **Record Playback** interface, click . See Figure 4-131.

The interface of **Record Type Filter** is displayed. See Figure 4-132.

Figure 4-131 Record type filter

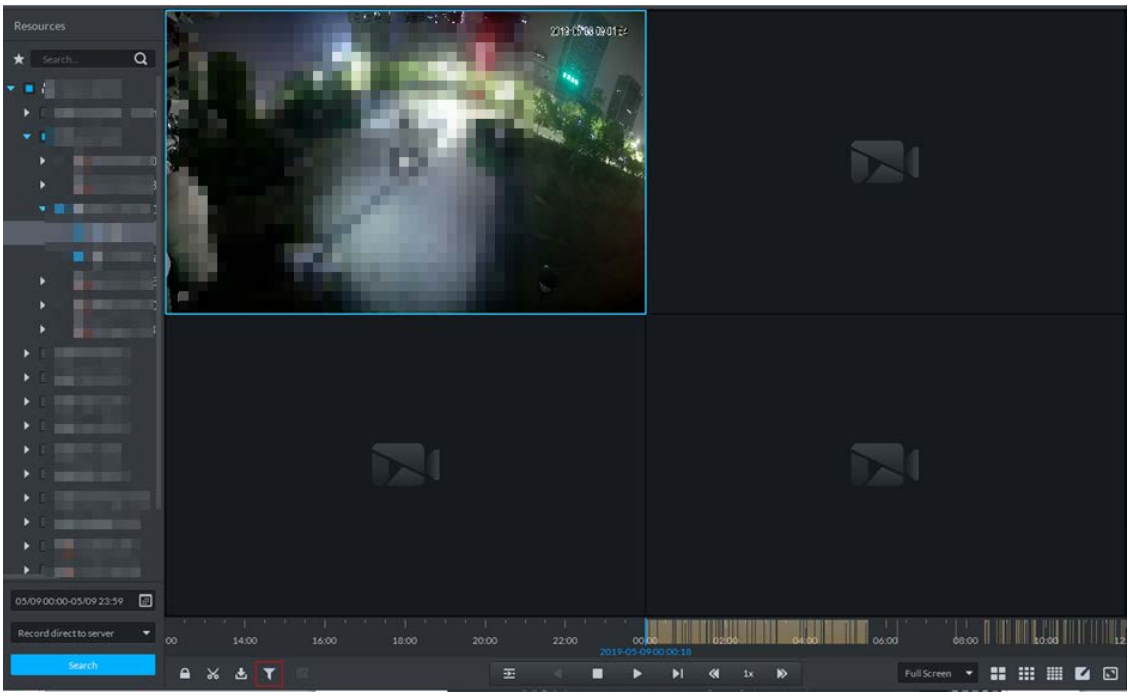
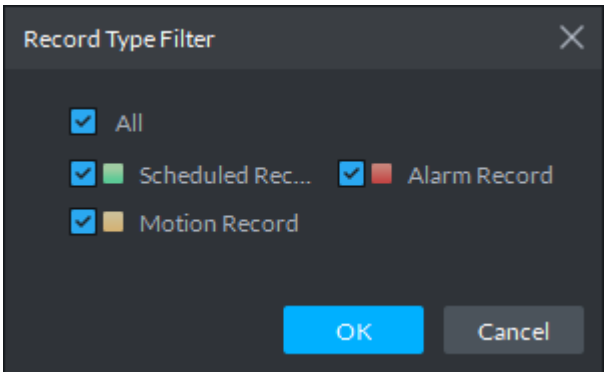


Figure 4-132 Record filter



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

The system only displays the video of selected type.

4.4.6 Clip Record

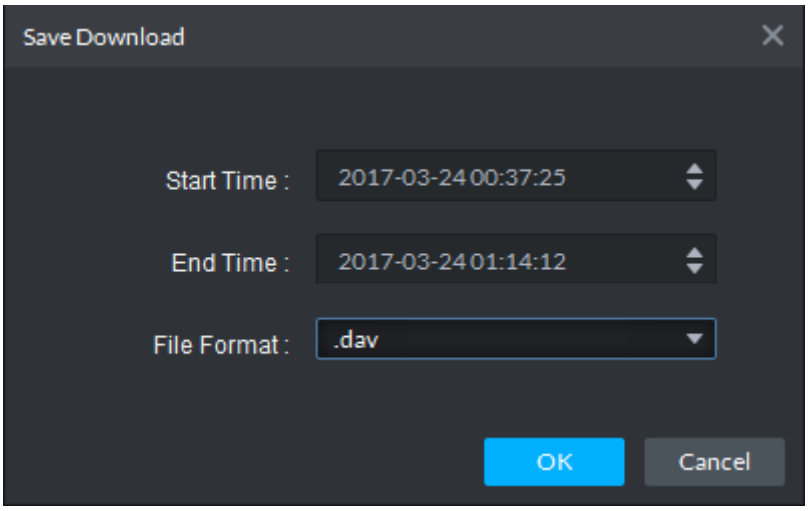
Step 1 On **Record Playback** interface, set search condition and search videos.

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

Step 3 During the timeline, click to start clip and then drag the mouse, click to stop clip.

The **Save Download** interface is displayed. See Figure 4-133.

Figure 4-133 Save download



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

4.4.7 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 4-134.
The interface of **Smart Search** is displayed. See Figure 4-135. 22×18 squares are displayed in the window.

Figure 4-134 Enable smart search

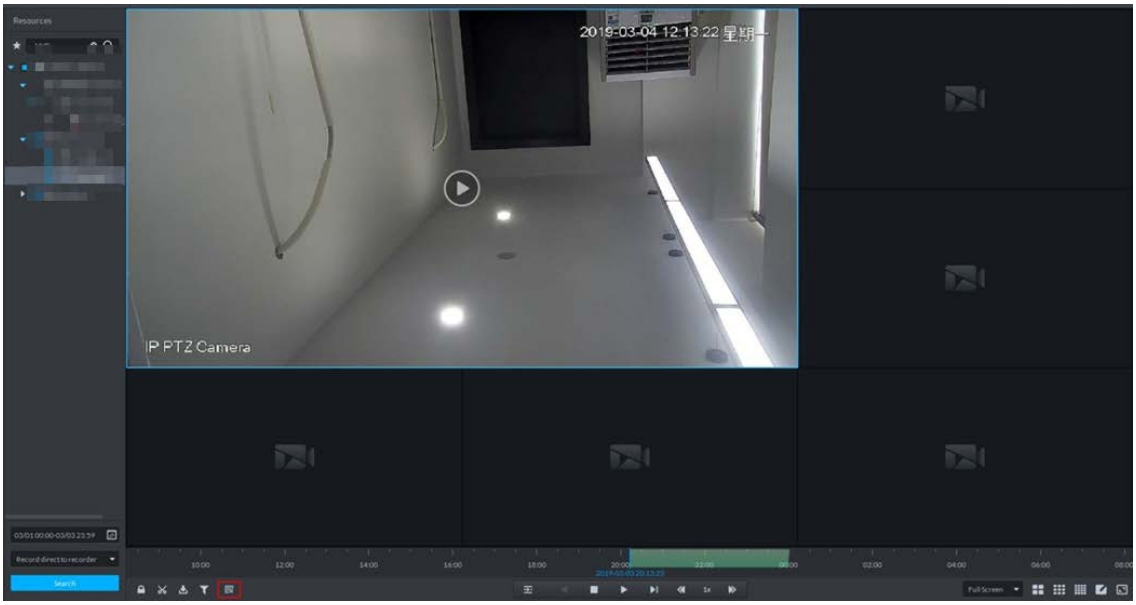
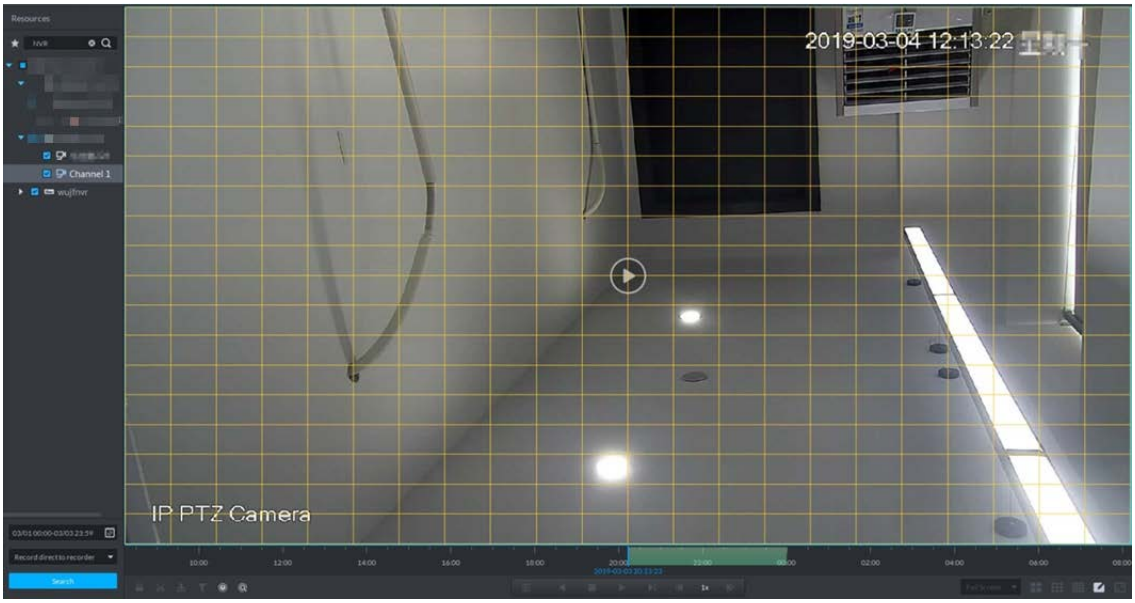


Figure 4-135 Smart search



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.

4.4.8 Downloading Record

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

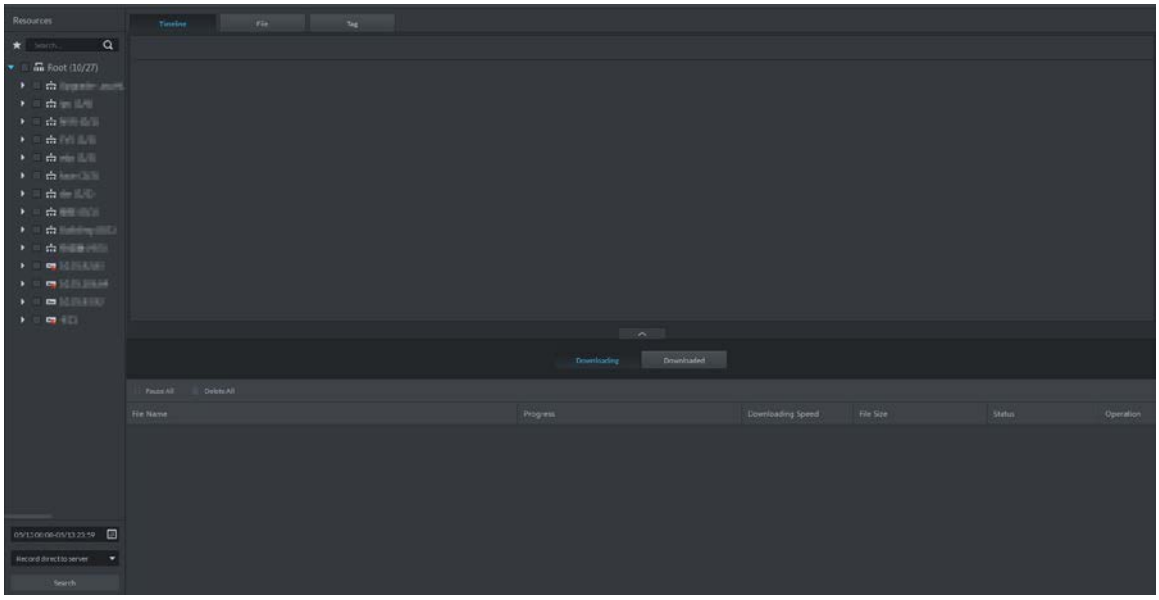
4.4.8.1 Timeline

Download video of some period for record file.

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

The **Download Center** interface is displayed. See Figure 4-136.

Figure 4-136 Download center



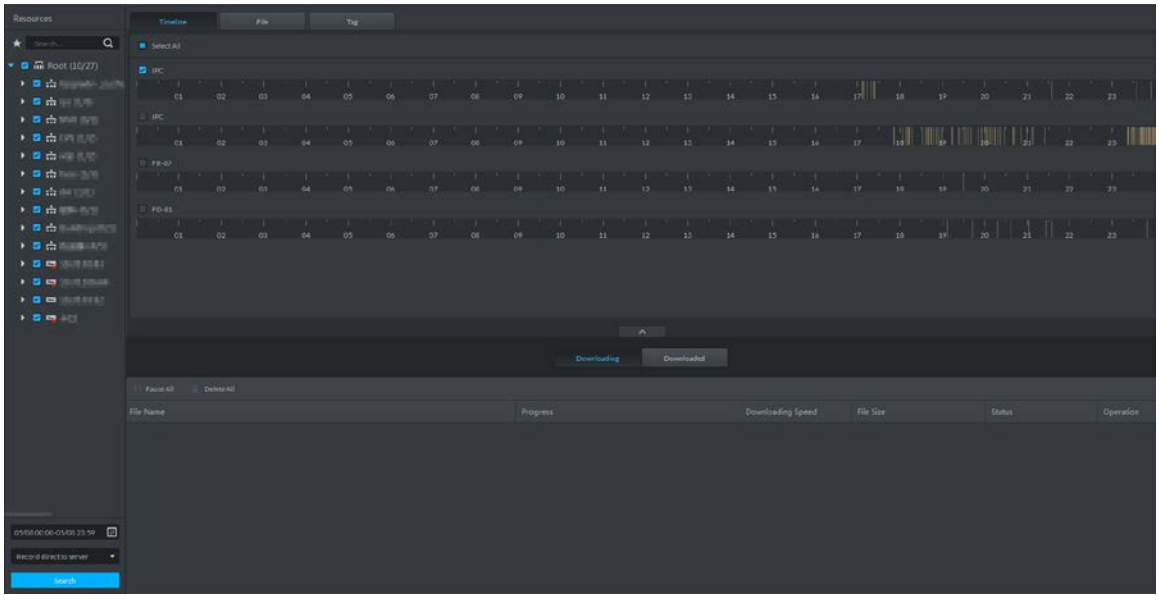
Step 2 Set search condition, click **Search**.

The search results is displayed.

Step 3 Click **Timeline** tab.

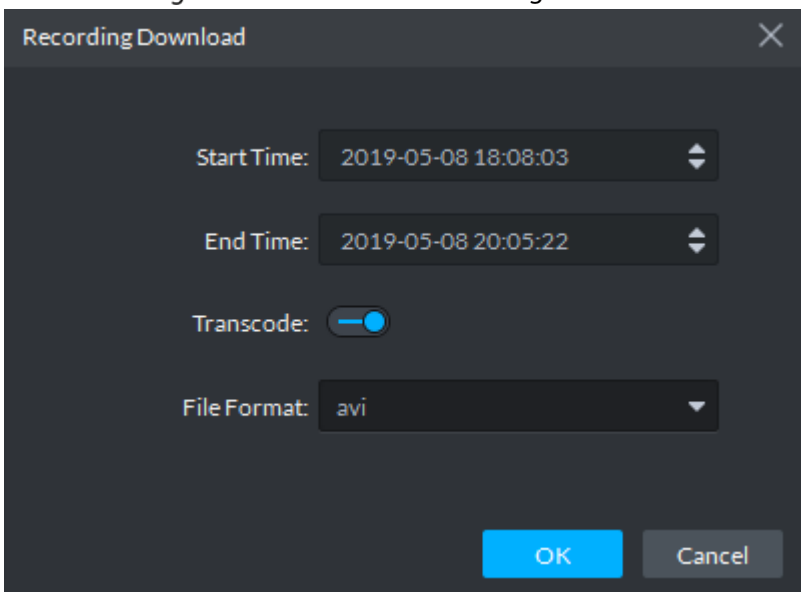
The search results in the form of timeline are displayed. See Figure 4-137.

Figure 4-137 Record search result



Step 4 Move the mouse to timeline, select start time and end time.

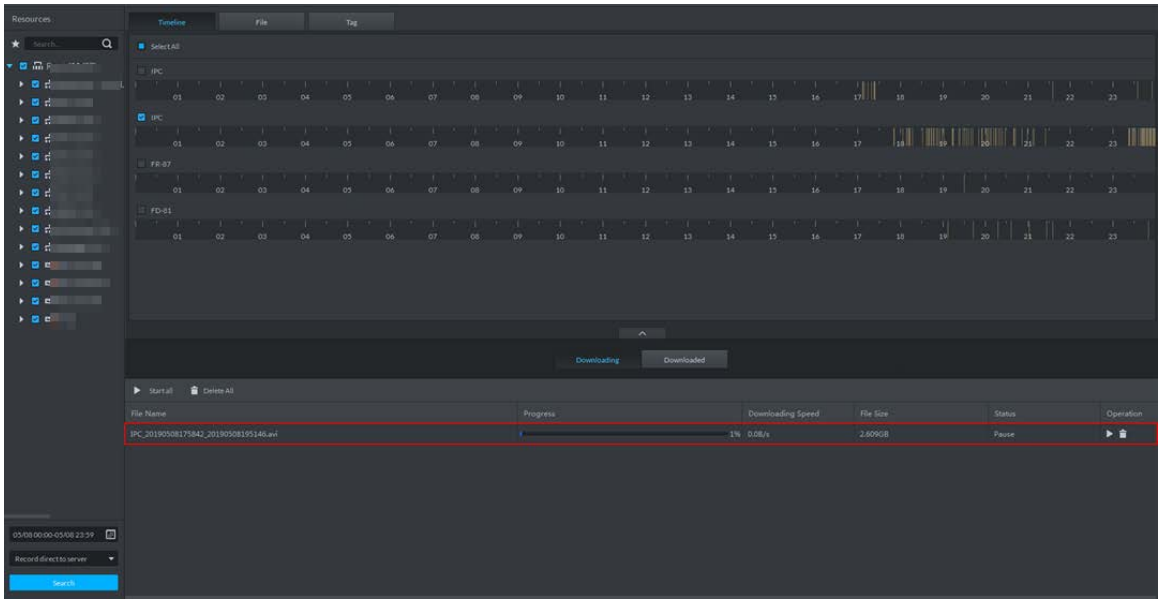
Figure 4-138 Download recording



Step 5 Confirm recording time, select file format, including dav, avi, mp4, flv and asf. Click **OK**.

The download progress is displayed. See Figure 4-139. You can pause, start and delete downloaded recording. A prompt task will pop out in the lower right corner of client. The downloaded tasks are displayed on the **Downloaded** interface.

Figure 4-139 Download progress



4.4.8.2 File

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

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

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

The **Download Center** interface is displayed.

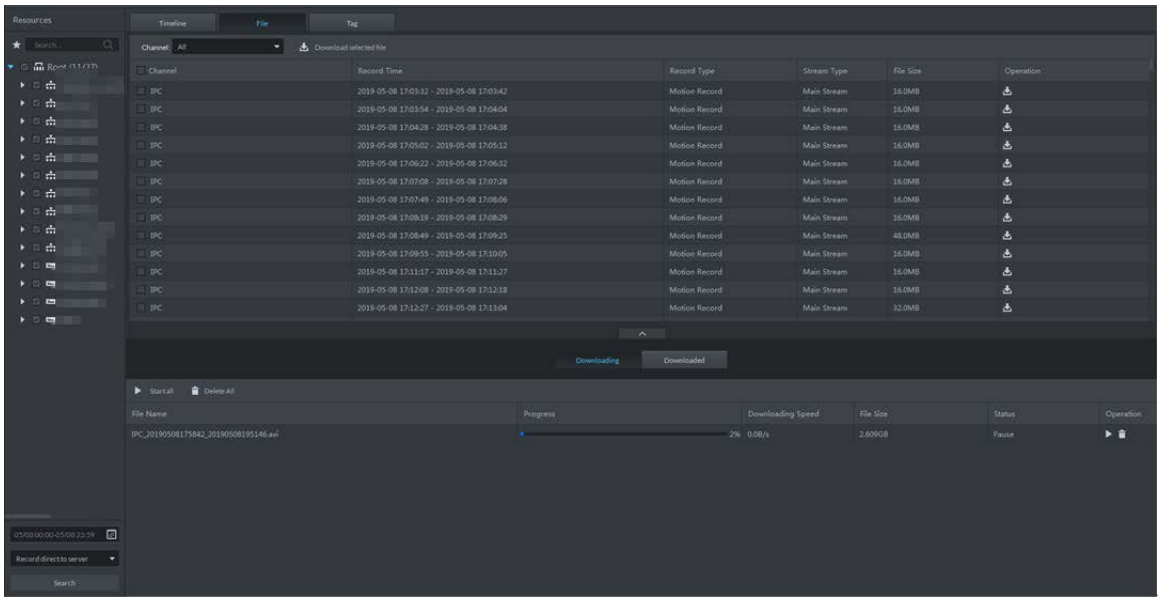
Step 2 Set search condition, click **Search**.

The search result is displayed.

Step 3 Click **File** tab.

The searched result is displayed in the form of file list. See Figure 4-140.

Figure 4-140 Record search result

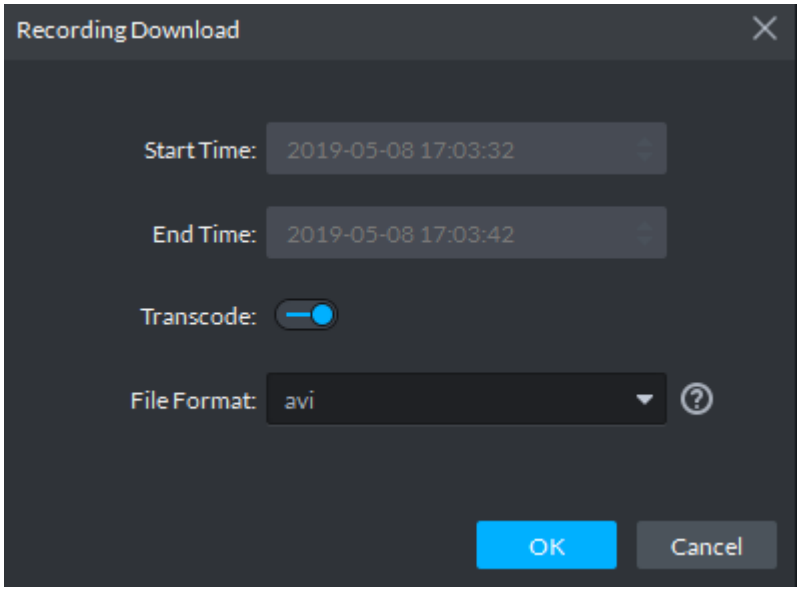


Step 4 Click in the back of file list.

The **Recording Download** interface is displayed. See Figure 4-141.

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

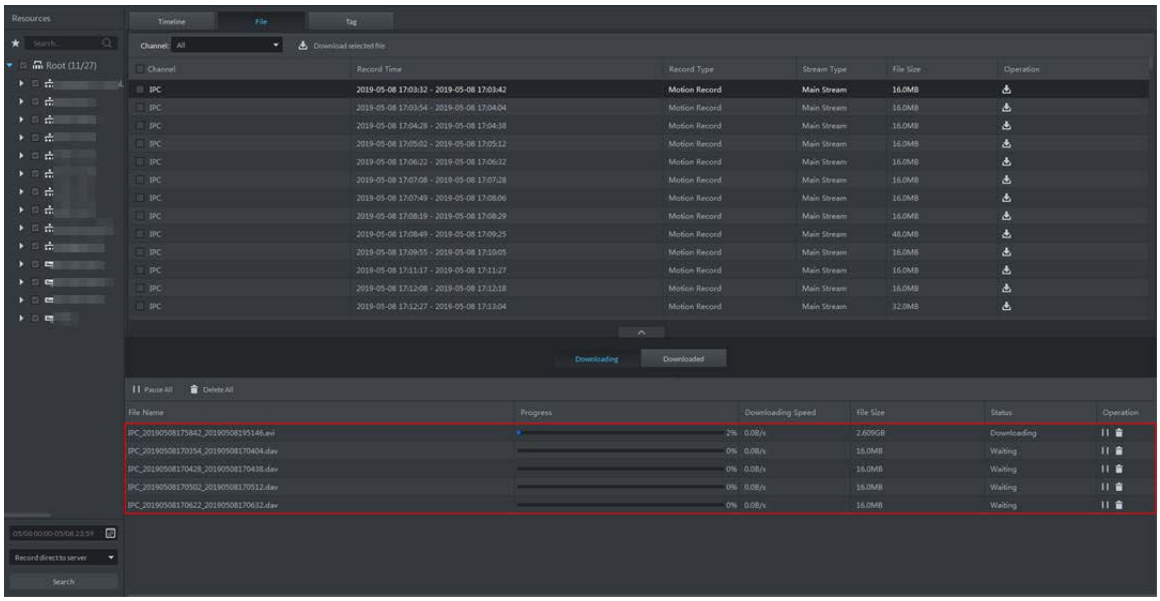
Figure 4-141 Recording download



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

The download progress is displayed. See Figure 4-142. You can pause, start and delete downloaded recording. A prompt task will pop out in the lower right corner of client. The downloaded tasks are displayed on the **Downloaded** interface.

Figure 4-142 Download progress



4.4.8.3 Tag

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

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

The **Download Center** interface is displayed.

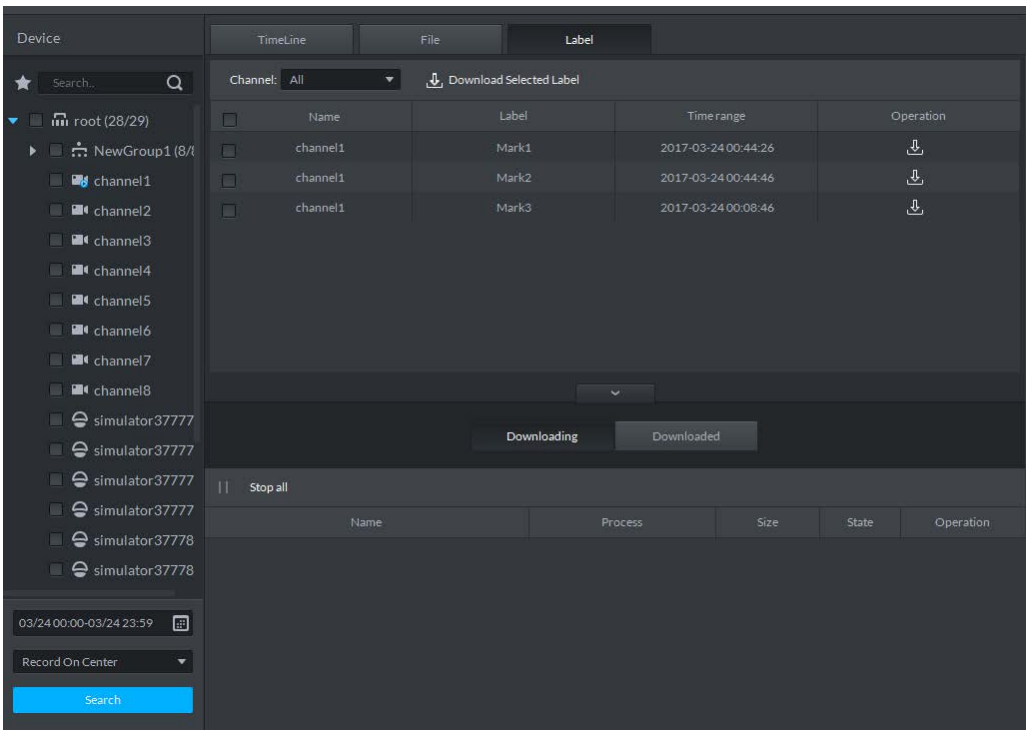
Step 2 Set search condition, click **Search**.

The searched results are displayed.

Step 3 Click **Tag** tab.

The tag file result is displayed. See Figure 4-143.

Figure 4-143 Record search result

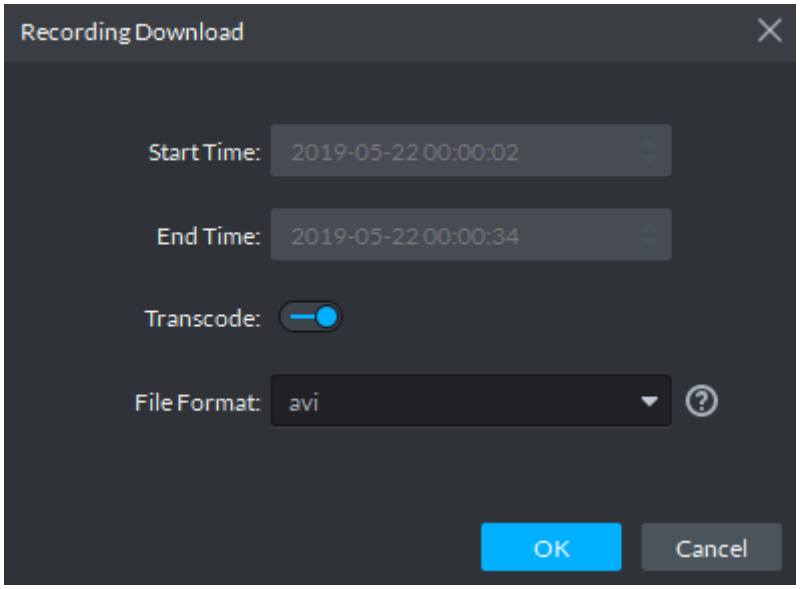


Step 4 Click  in the back of tag list.

The **Recording Download** interface is displayed. See Figure 4-144.

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

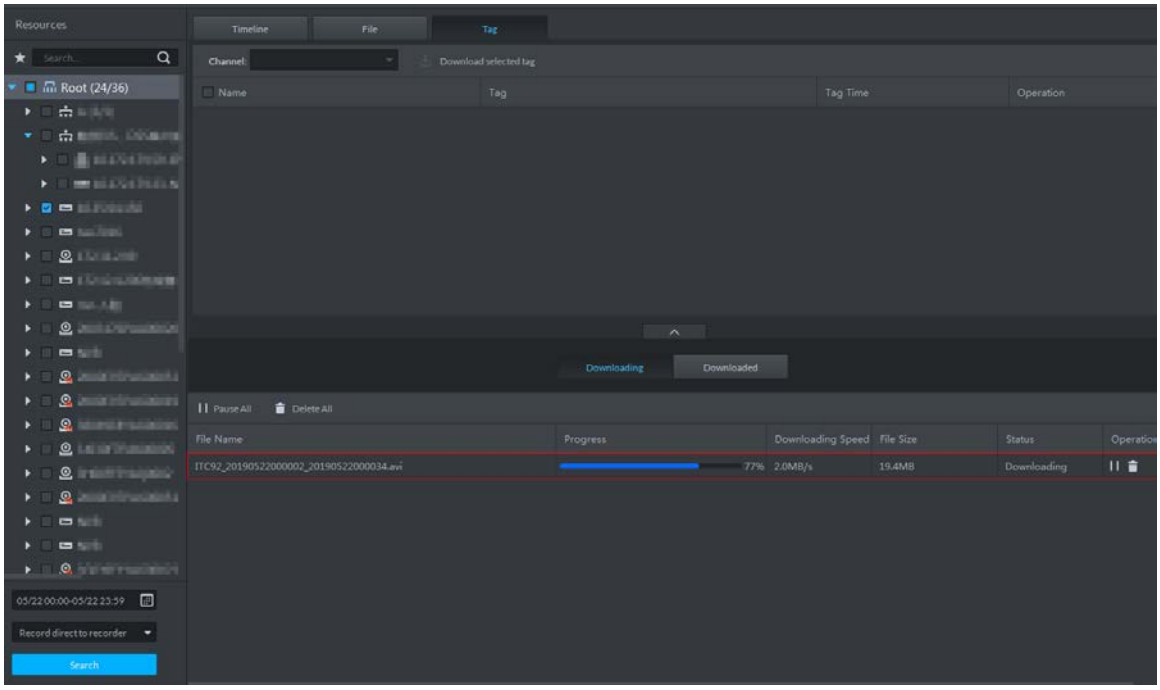
Figure 4-144 Recording download



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

The download progress is displayed. See Figure 4-142. You can pause, start and delete downloaded recording. A prompt task will pop out in the lower right corner of client. The downloaded tasks are displayed on the **Downloaded** interface.

Figure 4-145 Download progress



4.5 Event Center

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

For detailed operation of alarm event config, see"4.1.4 Setting Alarm Event."

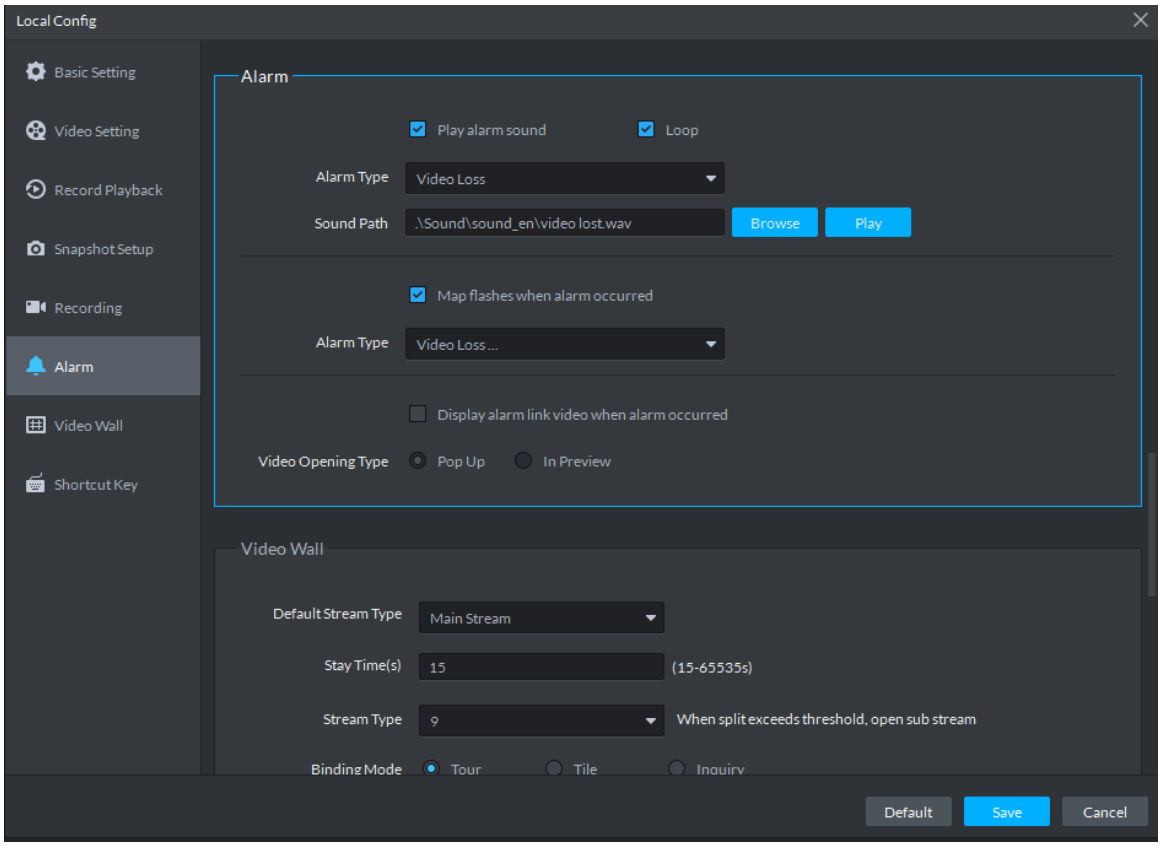
4.5.1 Setting Alarm Parameters

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

Step 1 Click at the top right corner on client interface.
The **Local Config** interface is displayed.

Step 2 Click **Alarm** tab.
The **Alarm** interface is displayed. See Figure 4-146.

Figure 4-146 Alarm



Step 3 Set alarm parameters and then click **Save**. Refer to Table 4-31 for detailed information.

Table 4-31 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	It is to select alarm audio file path.
Map flashes when alarm occurred	Check the box and then select alarm type. When the corresponding alarm occurs, the device on the emap can flash.
Display alarm link video when alarm occurred	Check the box, system automatically opens linkage video when an alarm occurs.
Display type	System automatically opens linkage video when an alarm occurs. You can view on the pop-up window or on the preview interface.

4.5.2 Searching and Processing Real-Time Alarm

After alarm is reported to client, users can claim alarm, view and confirm alarm, process alarm and register processed alarm. If alarm is claimed by user A, then other users cannot see the alarm record

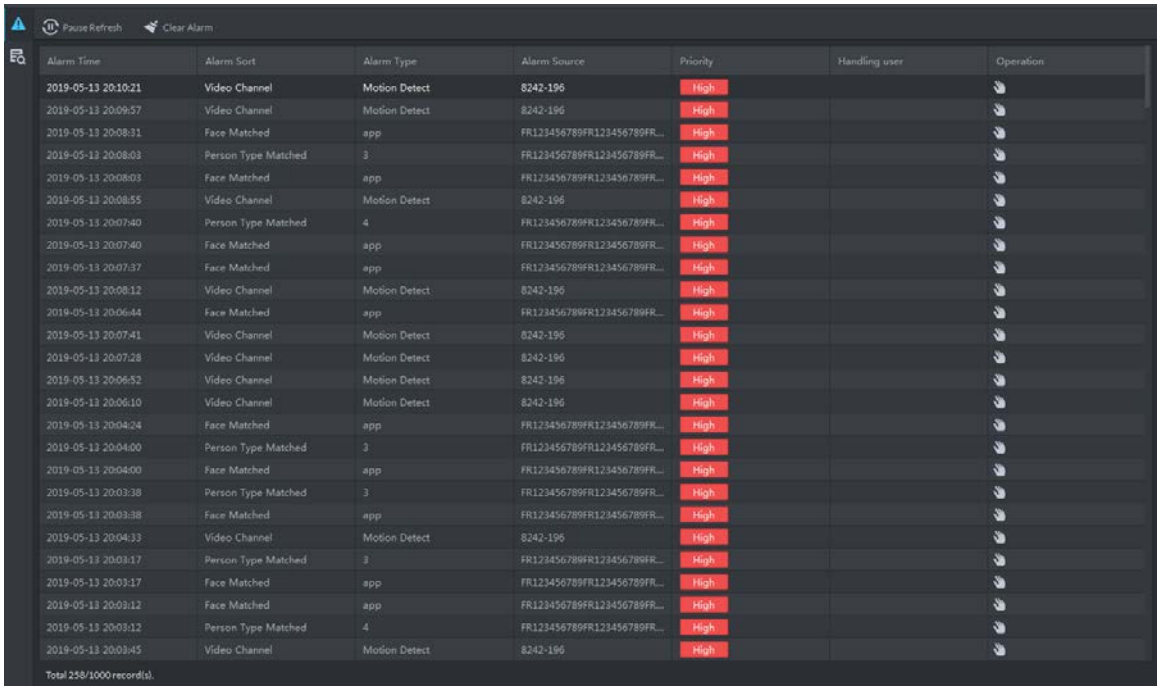
in real-time alarm. They can view the alarm details in histort alarm, but cannot deal with it. Client displays max 1000 realtime alarm messages.

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

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

The **Event Center** interface is displayed. See Figure 4-147.

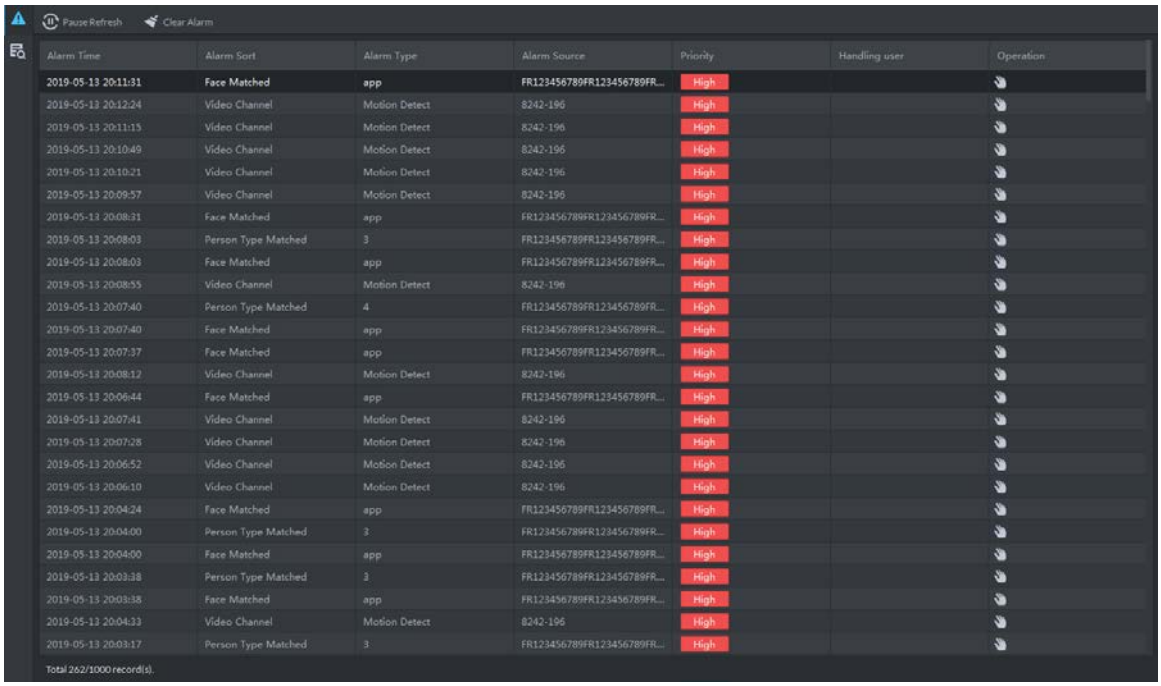
Figure 4-147 Event center



Step 2 Click 
.

The **Real-time Alarm** interface is displayed. See Figure 4-148.

Figure 4-148 Real-time alarm



- System refreshes to display real-time alarm by default. Click Pause Refresh to pause refresh, click Refresh to continue refresh.
- Click Clear Alarm and delete all alarms on real-time alarm interface, but not the data on server, you can still find it in history alarm.

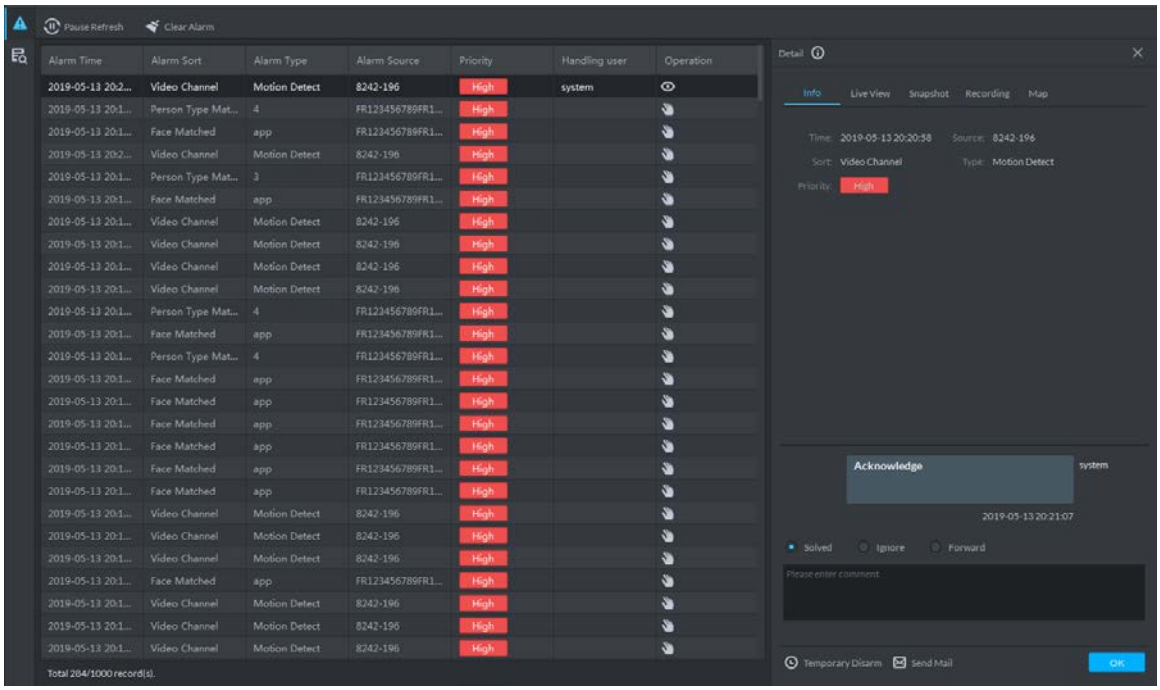
Step 3 Click of corresponding alarm.

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

Step 4 Click .

The alarm processing interface is displayed. See Figure 4-149.

Figure 4-149 Alarm processing



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

Step 6 Process alarm.

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

Step 7 Click **OK**.

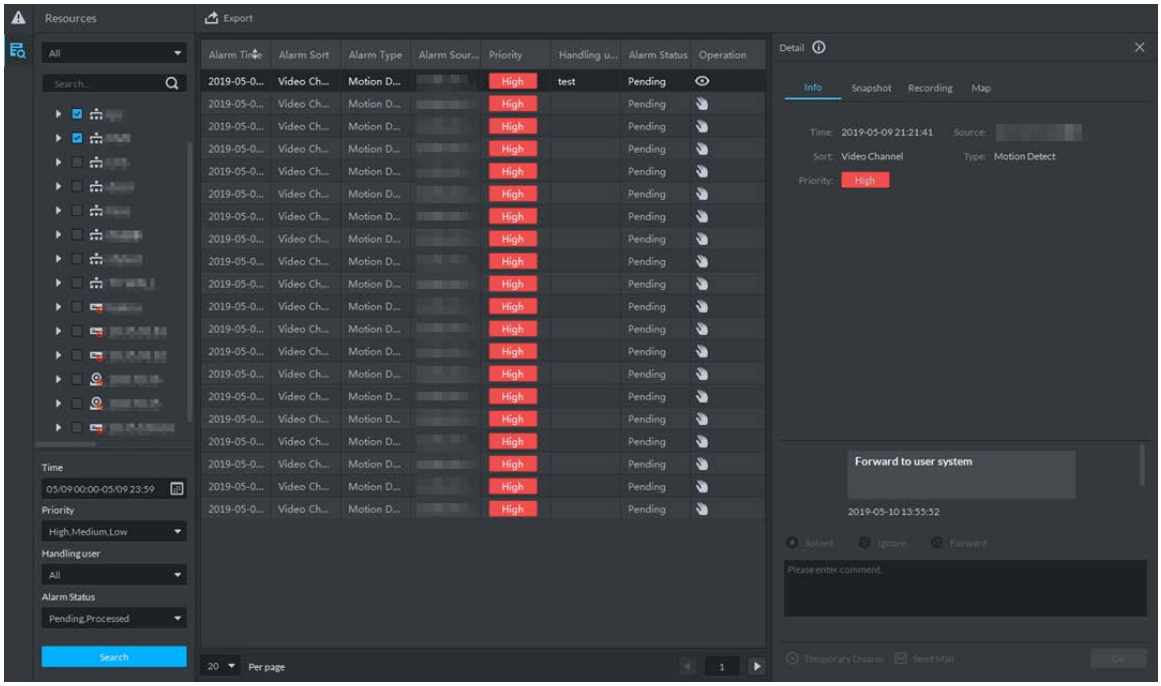
4.5.3 Searching and Processing History Alarm

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

, or click **Event Center** on client homepage.
The **Event Center** interface is displayed.

Step 2 Click  .
The **History Alarm** interface is displayed. See Figure 4-150.

Figure 4-150 Select alarm type



Step 3 Set search condition, click Search.
The result is displayed. You can only search alarm within one month.

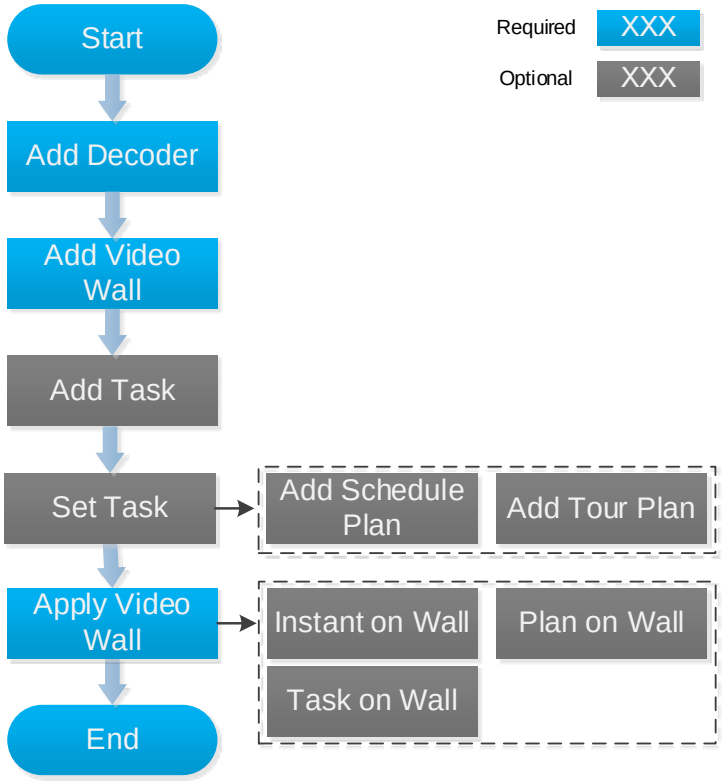
Step 4 View and process alarm. For operations, refer to"4.5.2 Searching and Processing Real-Time Alarm."

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

4.6 Video Wall

Decoder decodes video source, output image and display on video wall. The operation flow of video wall is shown in Figure 4-151.Video wall flow

Figure 4-151 Video wall flow



4.6.1 Adding Encoder

Add decoding devices; currently support decoder, matrix and video wall. For details, see"4.1.2.4 Adding Device."

4.6.2 Entering Video Wall Interface

On client homepage, click **Video Wall**. The **Video Wall** interface is displayed. See Figure 4-152. For interface description, see Table 4-32.

Figure 4-152 Video wall

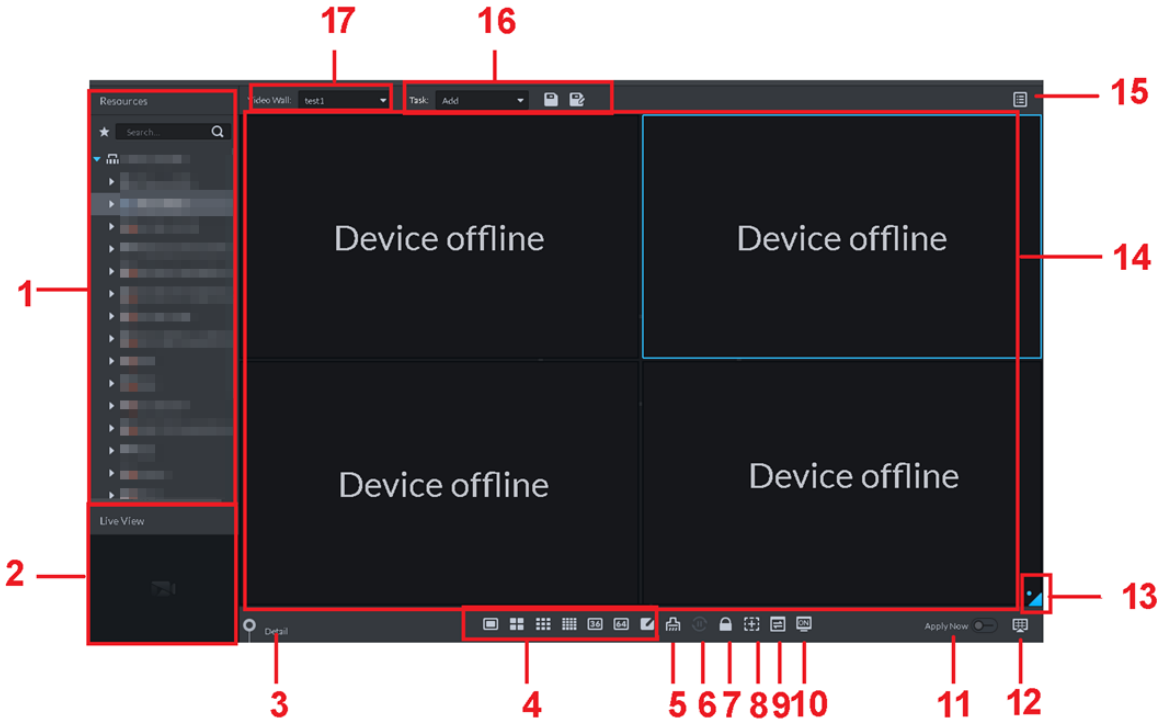


Table 4-32 Interface description

SN	Name	Function
1	Device tree	From **Local Config**> **General**, if you enable **Show device node**, device tree displays all channels of current device. If you cancel the box, system display all channels of all device. Click ★ to view the channels on the favorites folder. Search is supported by input device name or channel name in 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, modify signal interval on current channel when tour. ● Click Stream column or , modify video bit stream.
4	Window split	Set window split mode.
5	Clear	Clear information on all screens.

SN	Name	Function
6	Start/stop all tours	Start or stop all tours.
7	Lock window	Click to lock the window. You cannot operate on the locked window.
8	Add box	You can click to add a box, and click again to cancel box.
9	Back display	View current layout
10	Screen On/Off	In Screen On mode, the system will automatically display the video after configuring the tasks.
9	Apply now	If you enable the function, system automatically outputs the video to the wall after you set the task.
10	Decode to wall	Click to manually output the video to the wall.
11	Eagle eye	View current video wall layout
12	Video wall	Video wall area.
13	Video wall task	Set schedule task and tour task. Refer to"4.6.5 Setting Video Wall Plan" for detailed information.
14	Task management pane	Add, save delete task.
15	Video wall selection	Select a video wall to configure.

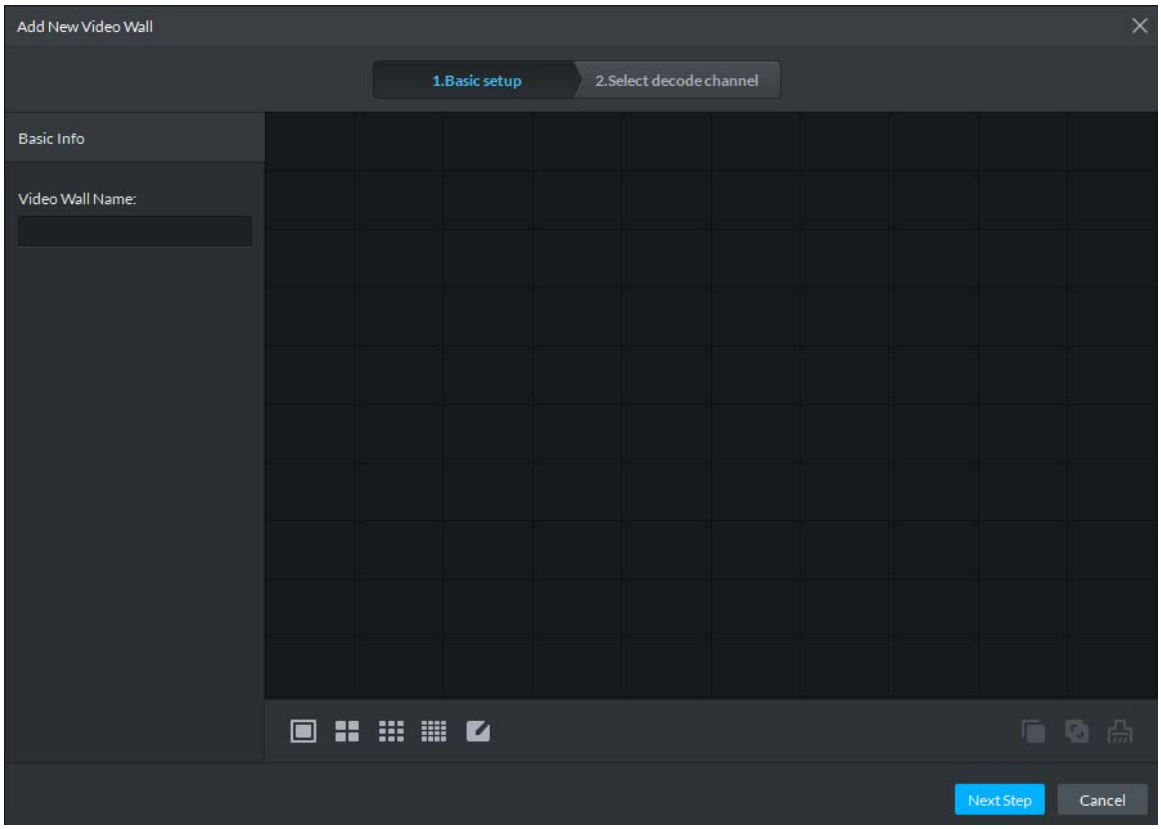
4.6.3 Adding Video Wall

Create video wall, and bind decoding channel to screen.

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

The **Add New Video Wall** interface is displayed. See Figure 4-153.

Figure 4-153 Add new video wall



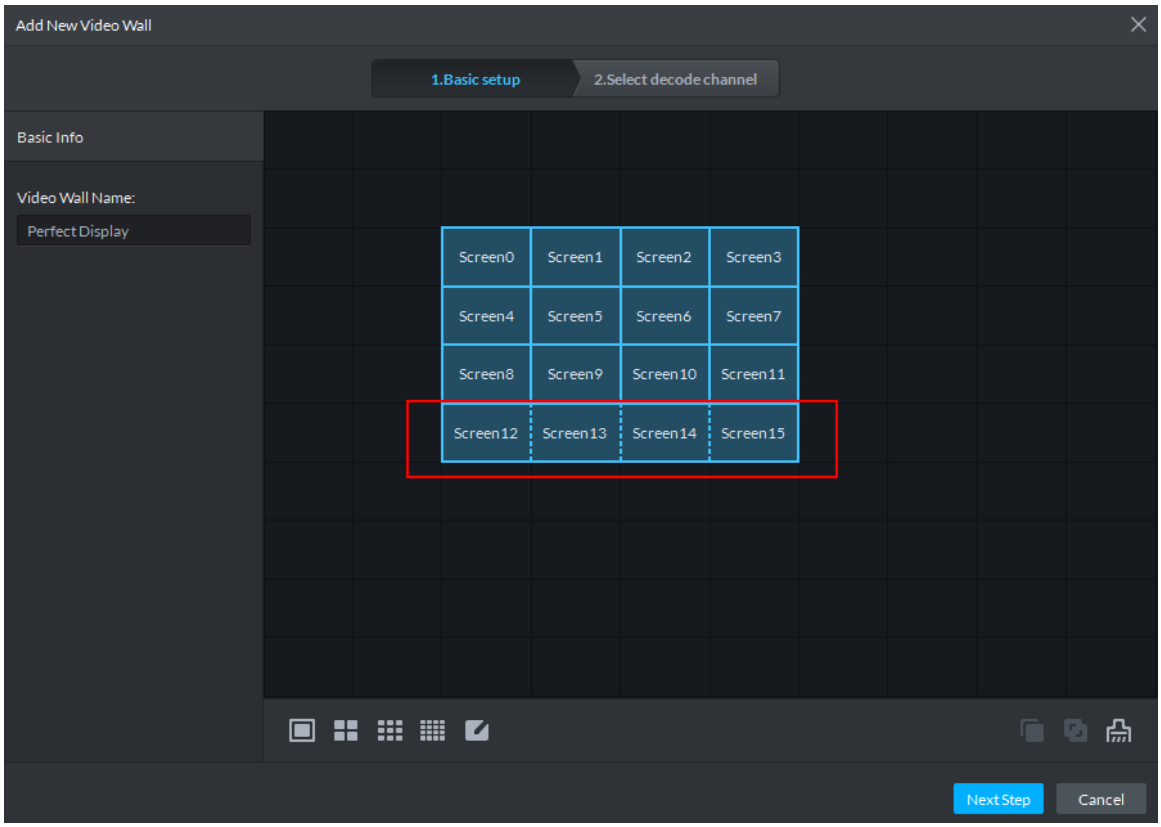
Step 2 Enter **Video Wall Name**, select screen quantity icon on the bottom, and click add anywhere on the screen.

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

Step 3 (Optional) Press **Shift** button, select several screens, click and combine the screens. See Figure 4-154.

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

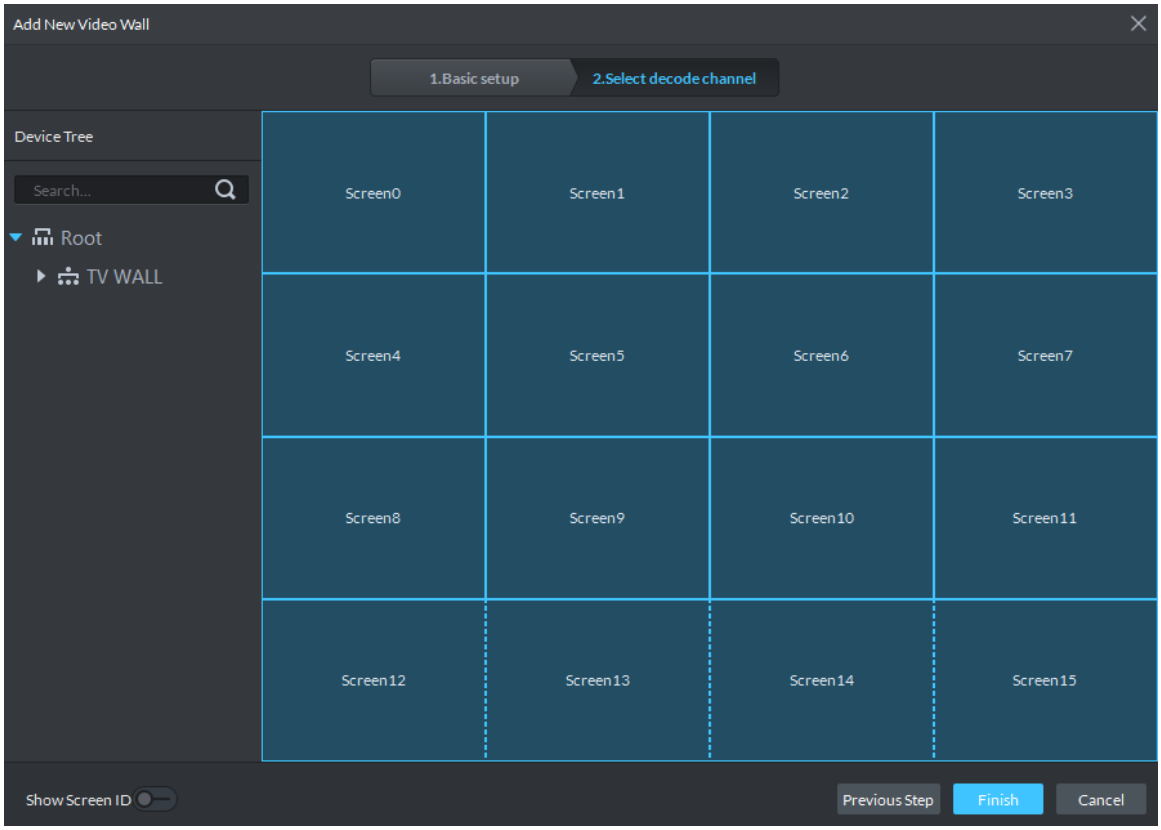
Figure 4-154 Combination Screen



Step 4 Click Next Step.

The **Select Decode Channel** is displayed. See Figure 4-155.

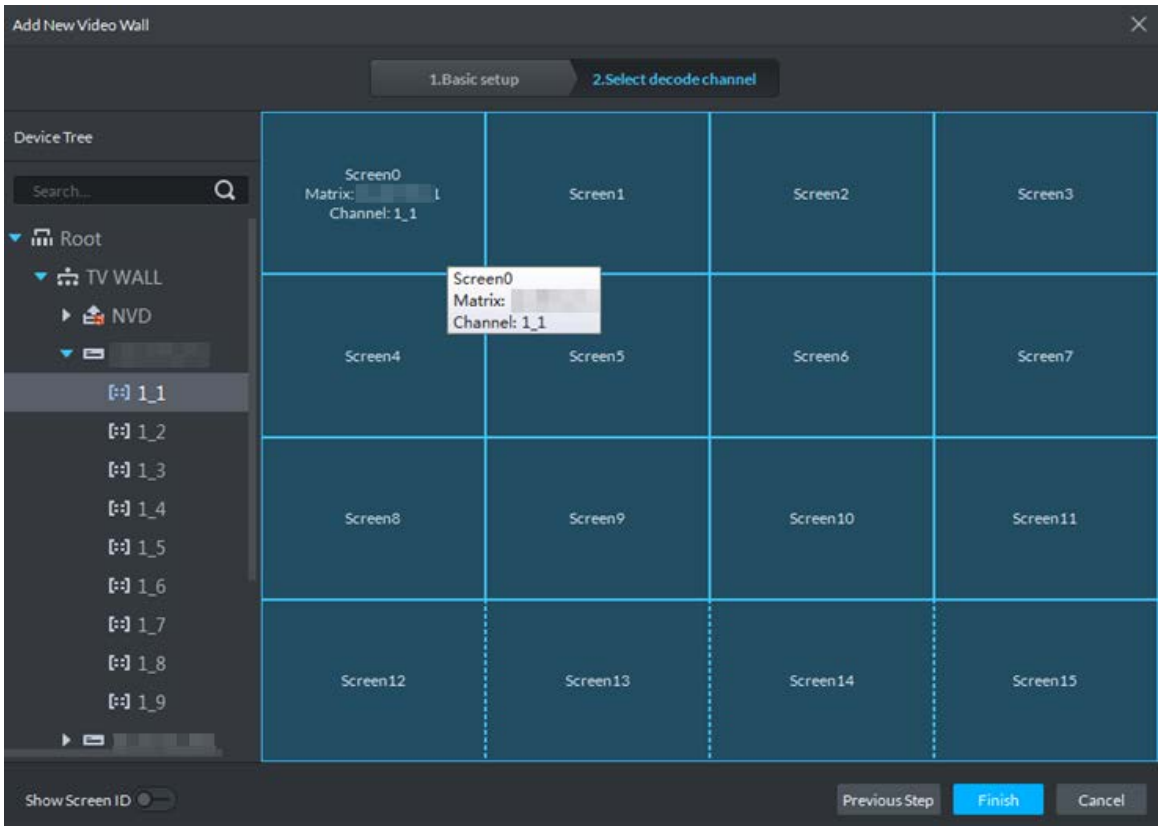
Figure 4-155 Bind decode channel



Step 5 Drag the decode channel on the left to each screen on the right for binding. See Figure 4-156.

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

Figure 4-156 Binding result



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

4.6.4 Adding Task

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

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

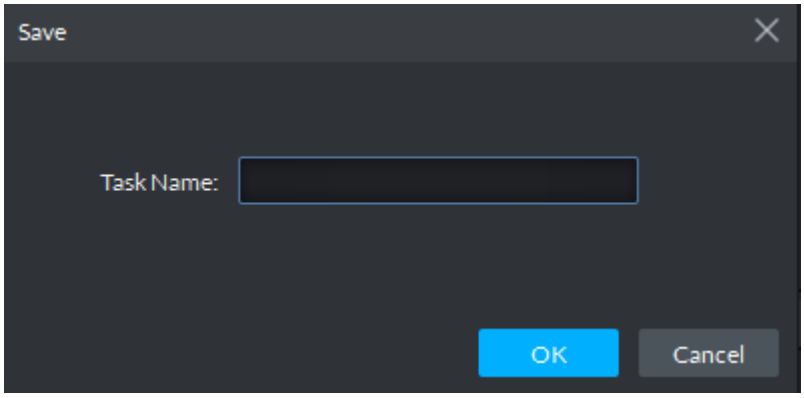
Step 2 Drag the video channel on the left to the screen on the right.

Step 3 Click .

The **Save** interface is displayed. See Figure 4-157.

If you select created task from task box, then drag video channel for binding, click and save as other task. The saved task displays on wall automatically.

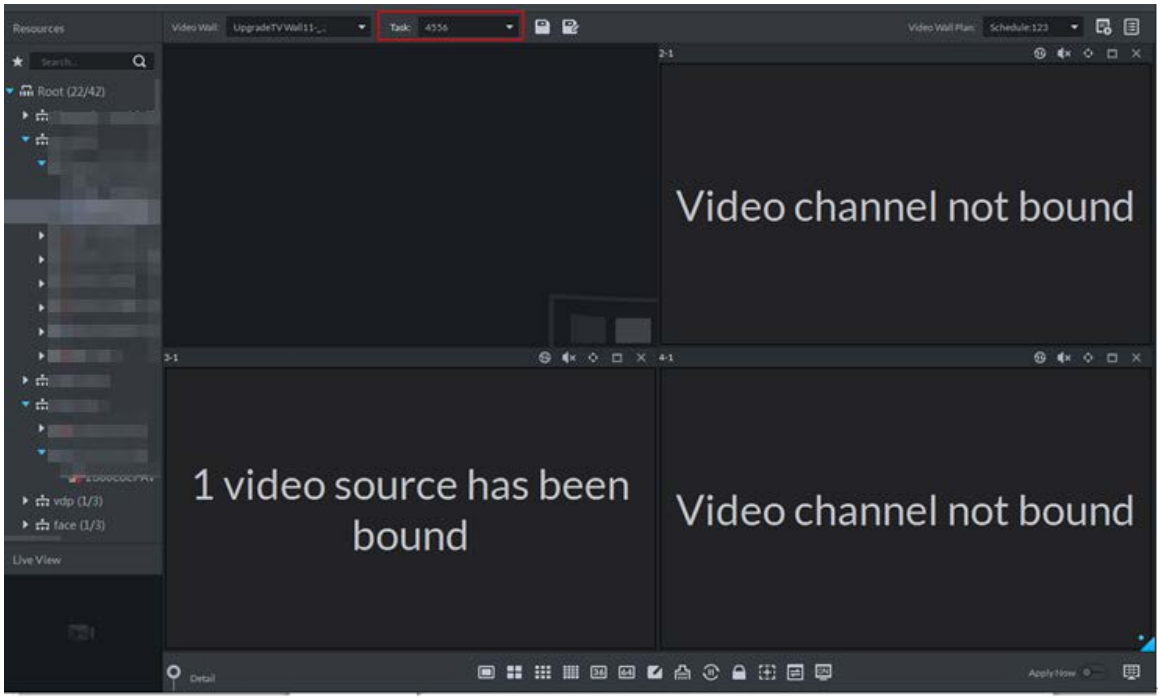
Figure 4-157 Save task



Step 4 Enter task name, click OK and save.

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

Figure 4-158 Task display on wall



4.6.5 Setting Video Wall Plan

4.6.5.1 Adding Scheduel Plan

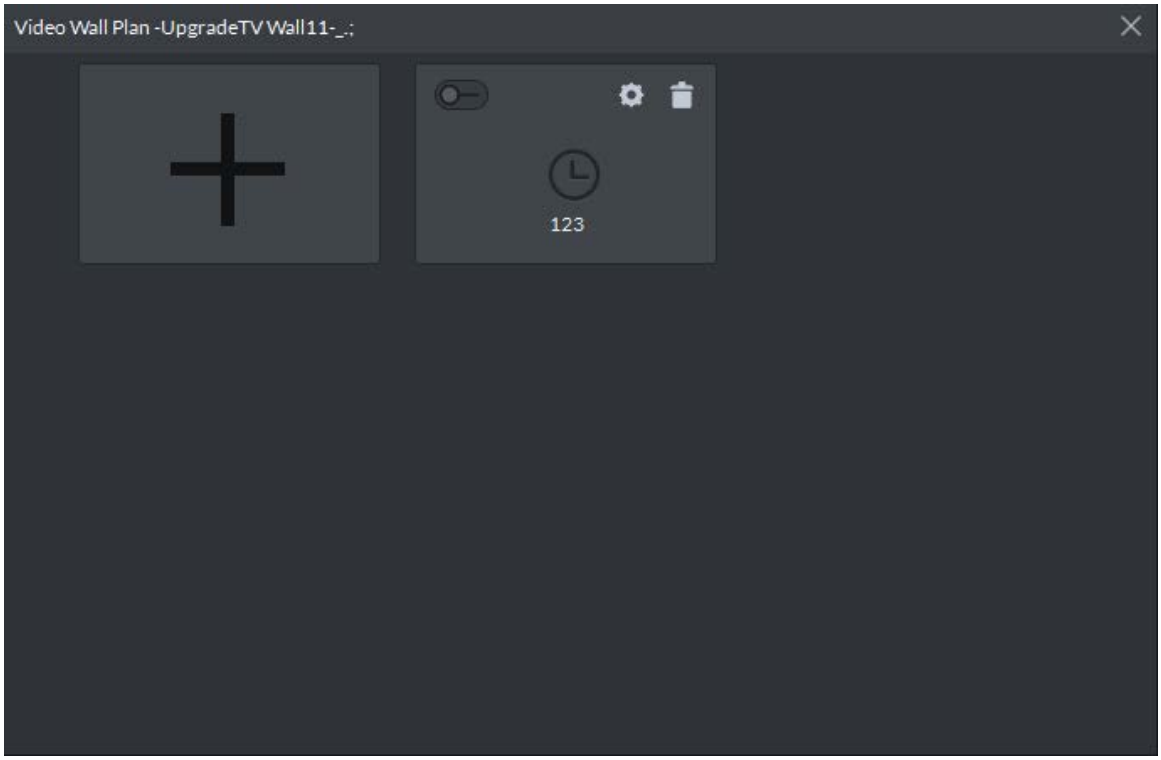
If task is configured, you can set task start time, end time and duration of each task, form plan and realize by schedule. If the set task occupies less than 1 day, then you can set remaining time to implement other tasks.

The task is required to be configured. For detailed operations, see"4.6.4 Adding Task."

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

The interface of video wall plan is displayed. See Figure 4-159.Video wall plan

Figure 4-159 Video wall plan



Step 2 Move the mouse to"+", and select **Schedule**. See Figure 4-160.

The **Schedule Plan** interface is displayed. See Figure 4-161.

Figure 4-160 Plan type

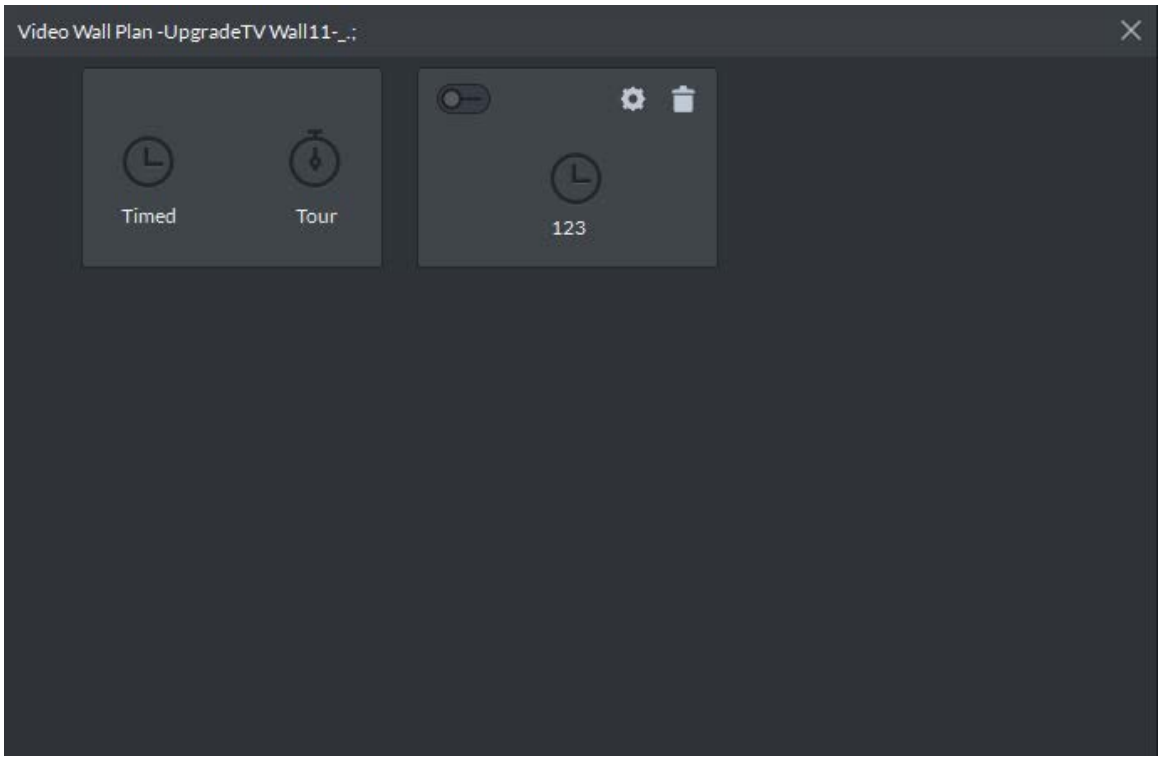
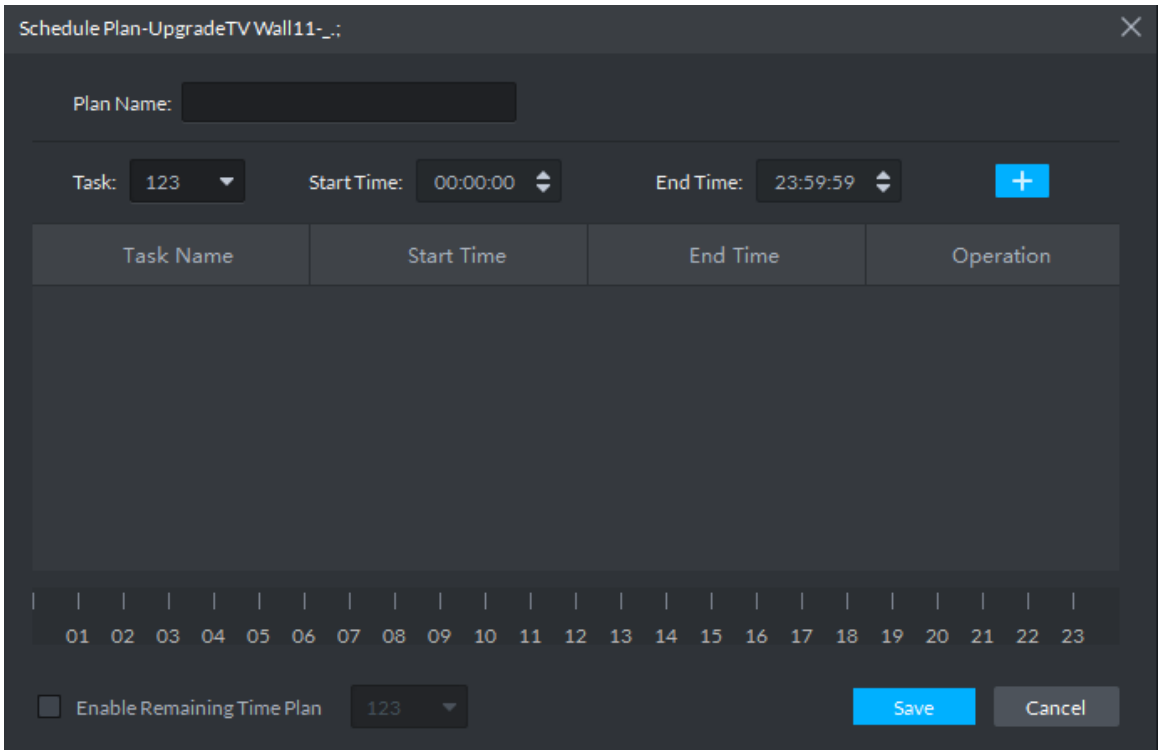


Figure 4-161 Add schedule plan



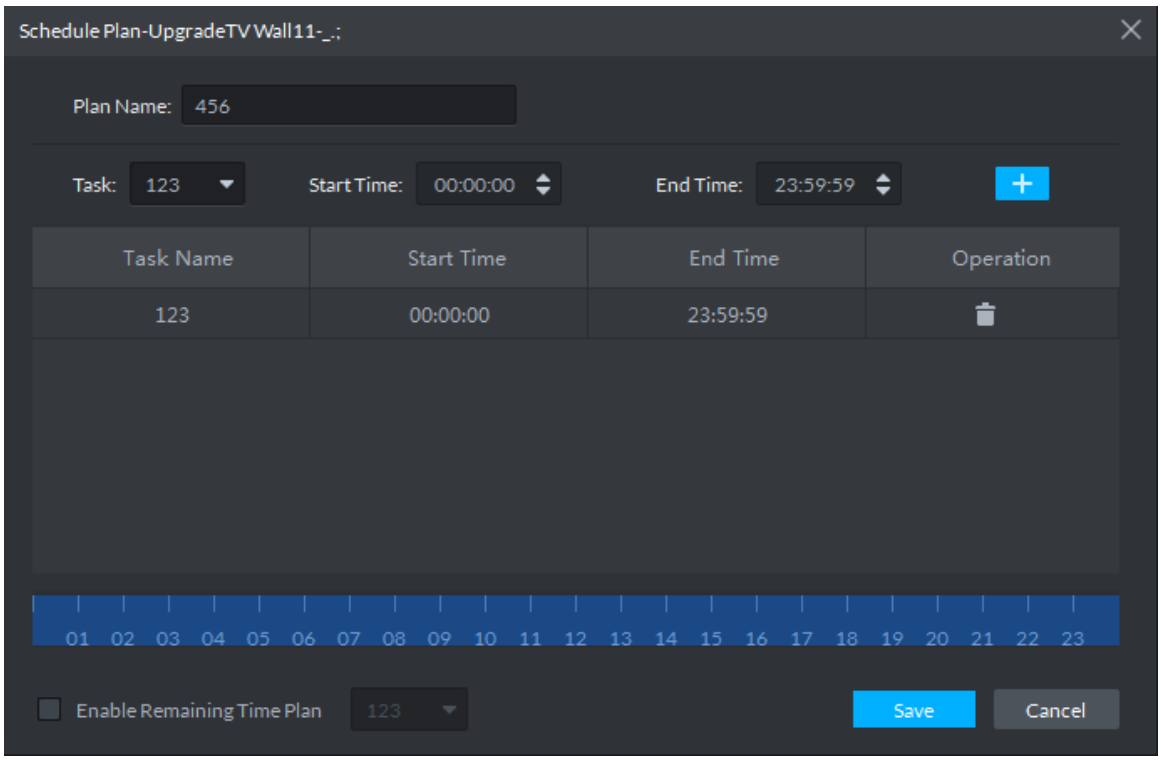
Step 3 Enter plan name.

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

Repeat the operation and you can add several tasks. But the start time and end time cannot be repeated. See Figure 4-162.

If task is added and it occupies less than 1 day, then you can select **Enable Remaining Time Plan**, and select tour plan of remaining time.

Figure 4-162 Added task

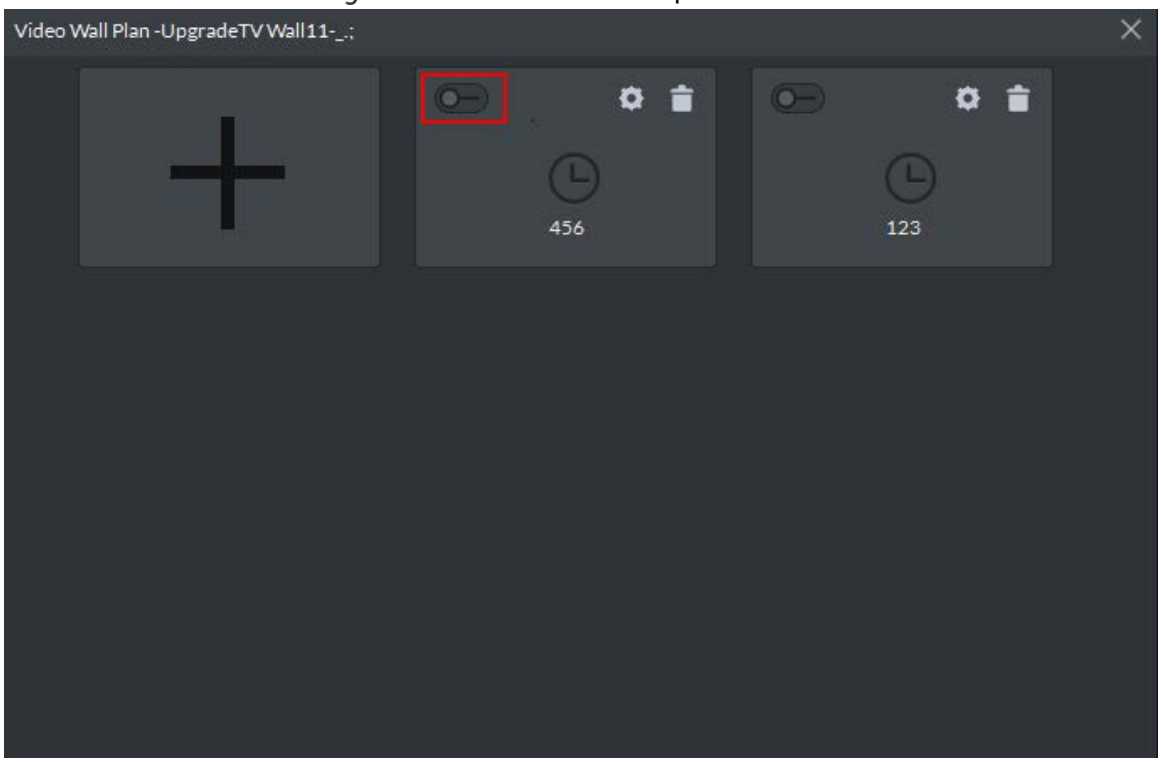


Step 5 Click **Save** to add.

Step 6 In the plan list, click  and realize schedule plan. See Figure 4-163.

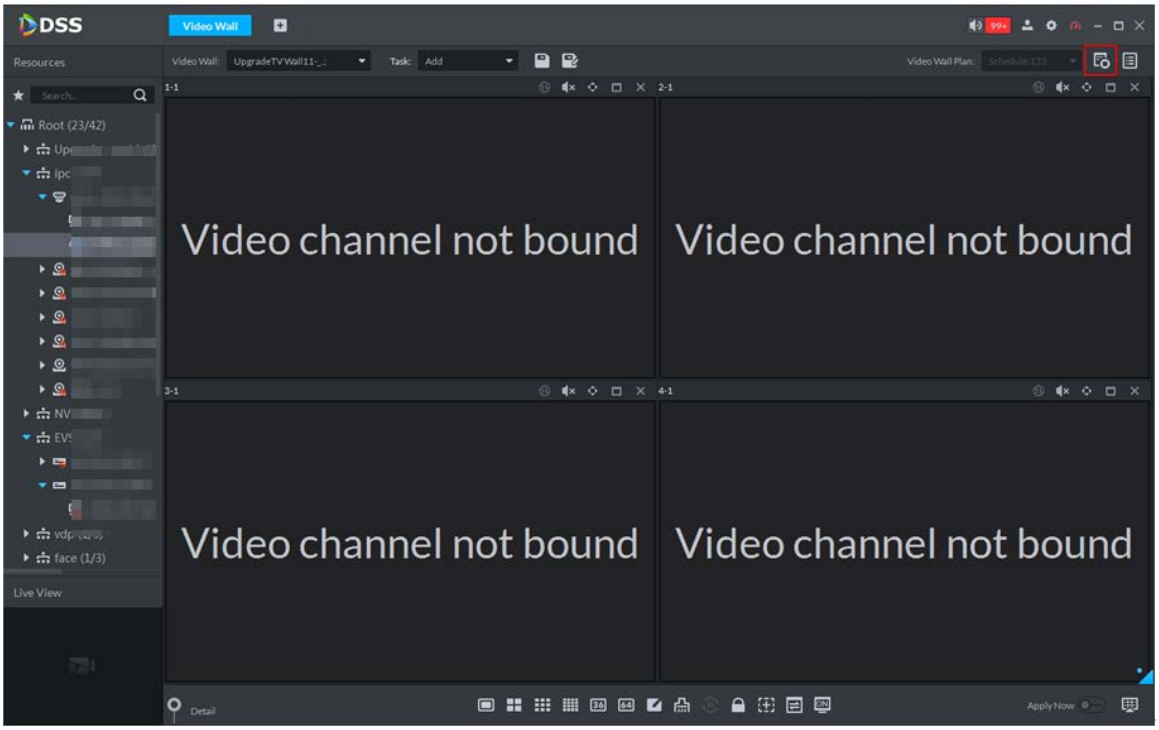
- Several plans cannot be displayed on wall at the same time; the previous plan is closed when you open another plan.
- Click  and modify plan.
- Click  and delete plan.

Figure 4-163 Enable schedule plan



If you want to stop plan, click  . See Figure 4-164. The icon is switched to  , click again to display on wall; If you want to switch other plans, you can enable other plan in the list.

Figure 4-164 Stop/Start plan



4.6.5.2 Adding Tour Plan

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

The task is required to be configured. For details, refer to"4.6.4 Adding Task."

Step 1 On Video Wall interface, click  on upper right corner. The plan management interface is displayed. See Figure 4-165.

Step 2 Move the mouse to "+", select **Tour**. See Figure 4-165.
The **Tour Plan** interface is displayed. See Figure 4-166.

Figure 4-165 Plan type

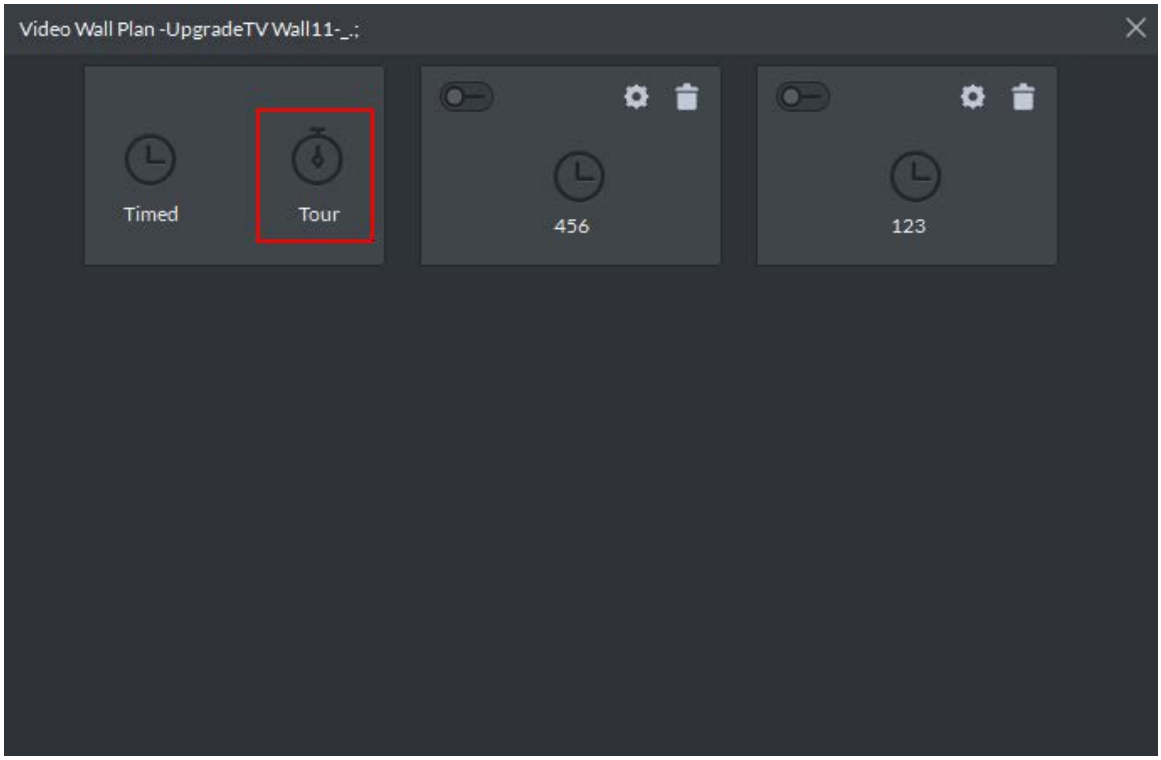
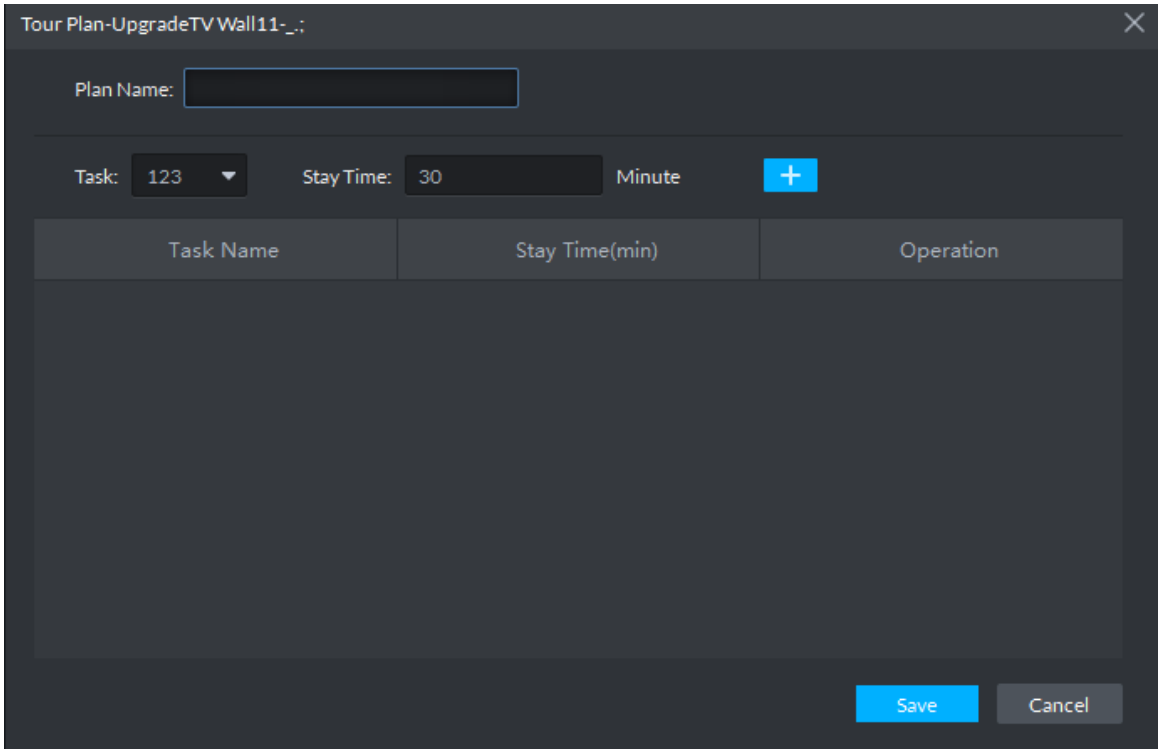


Figure 4-166 Add tour plan



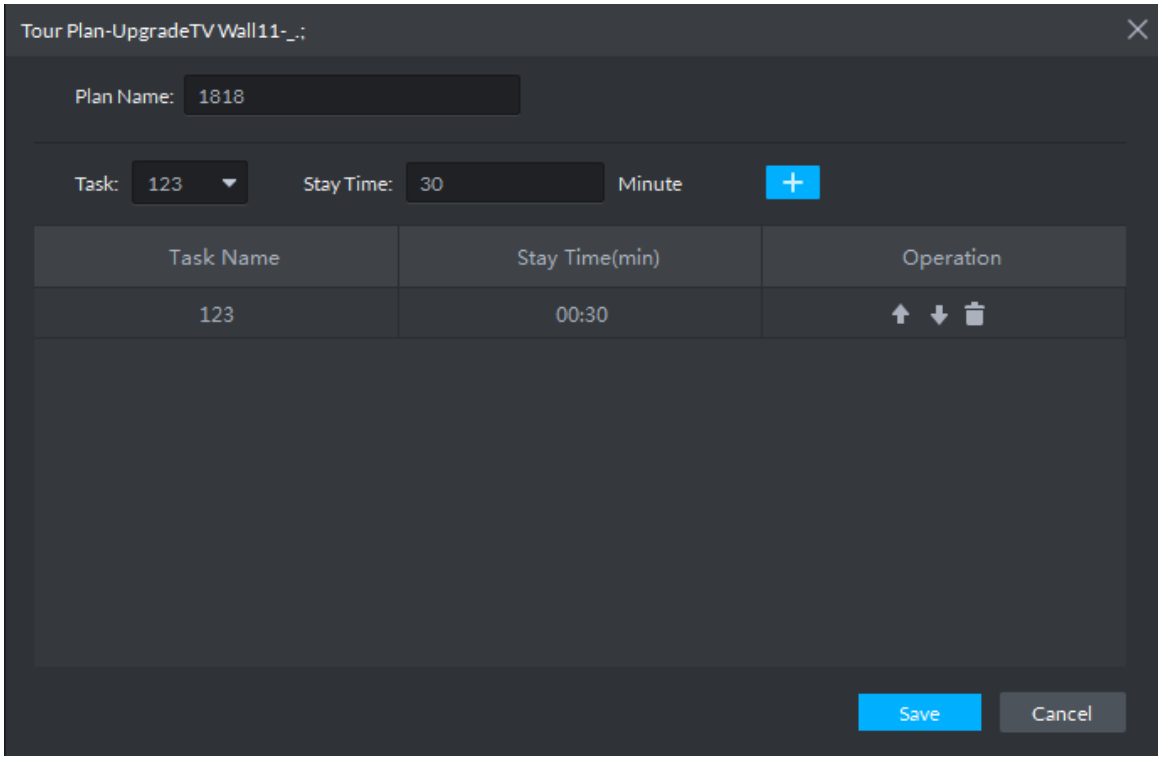
Step 3 Enter plan name.

Step 4 Select task, enter stay time, click "+", add to list.

Repeat the operation and you can add several tasks. See Figure 4-167.

Click / and adjust the display sequence of taks.

Figure 4-167 Added task

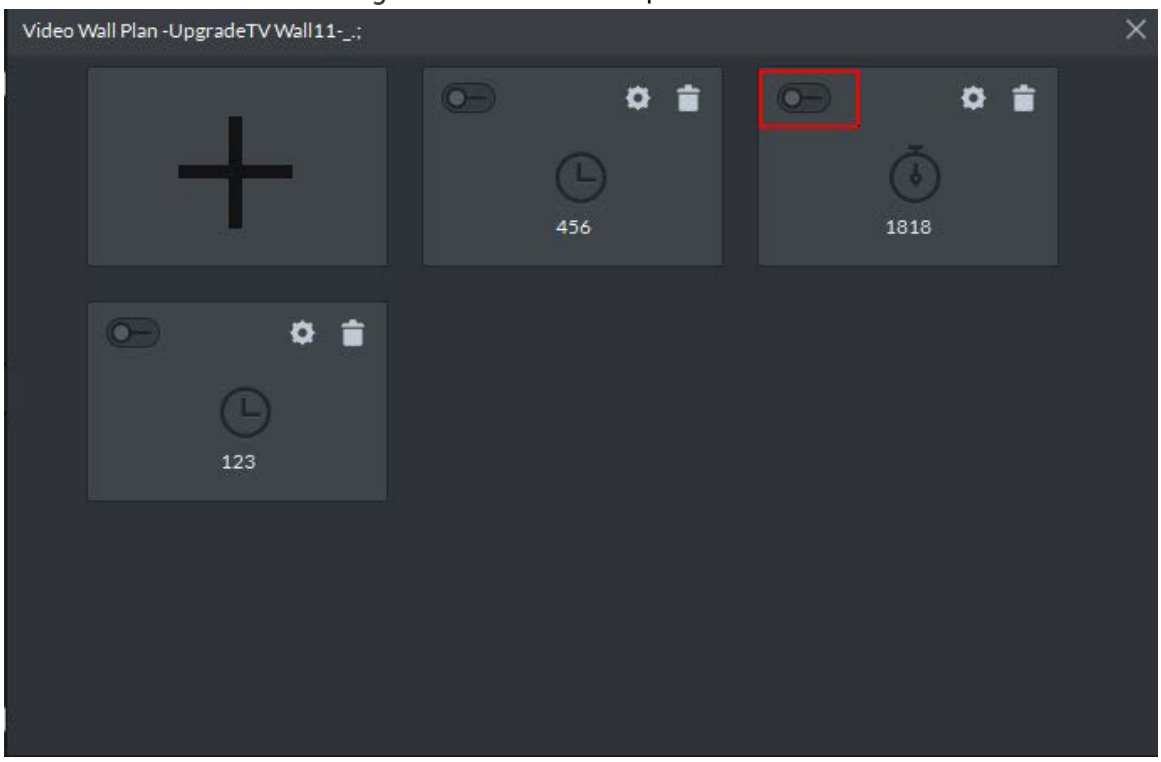


Step 5 Click **Save**, and plan is added.

Step 6 In plan list, click  and enable tour plan. See Figure 4-168.

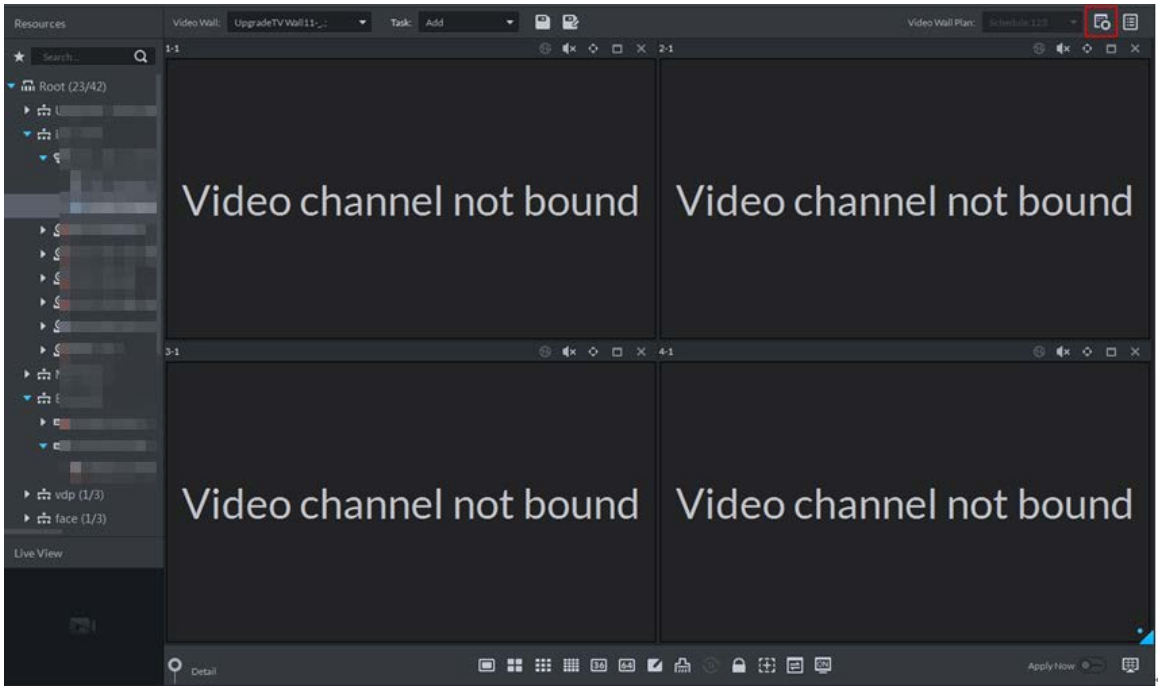
- Several plans cannot be displayed on wall at the same time; the previous plan is closed when you open another plan.
- Click  and modify plan.
- Click  and delete plan.

Figure 4-168 Enable tour plan



If you want to stop plan, click , see Figure 4-169. The icon is switched to , click again to display on wall; If you want to switch other plans, you can enable other plan in the list.

Figure 4-169 Stop/Start plan



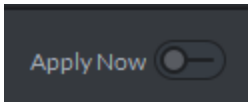
4.6.6 Applying Video Wall

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

4.6.6.1 Apply Now

Drag video channel to screen and display on wall directly.

Step 1 Select video wall from the box.

Step 2 Click 

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

Step 3 Drag left video channel to right screen for binding. See Figure 4-170.

If you select fisheye channel display on wall, right click to select fisheye mounting mode and realize fisheye dewarping. See Figure 4-171.

Figure 4-170 Bind video channel

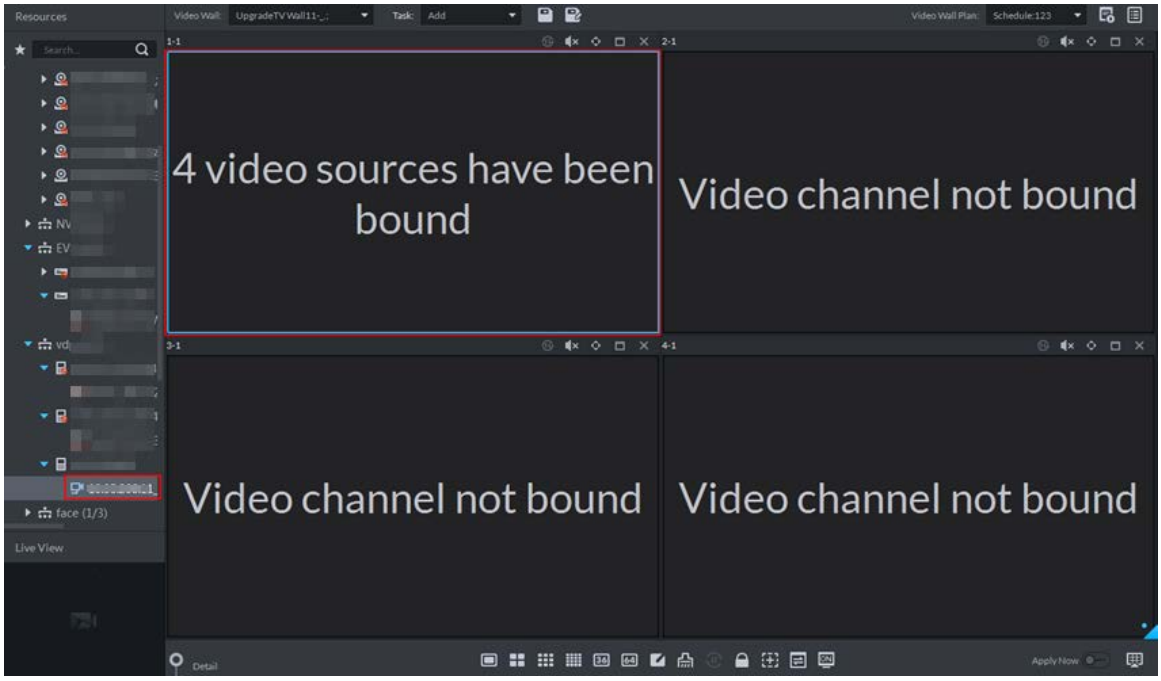
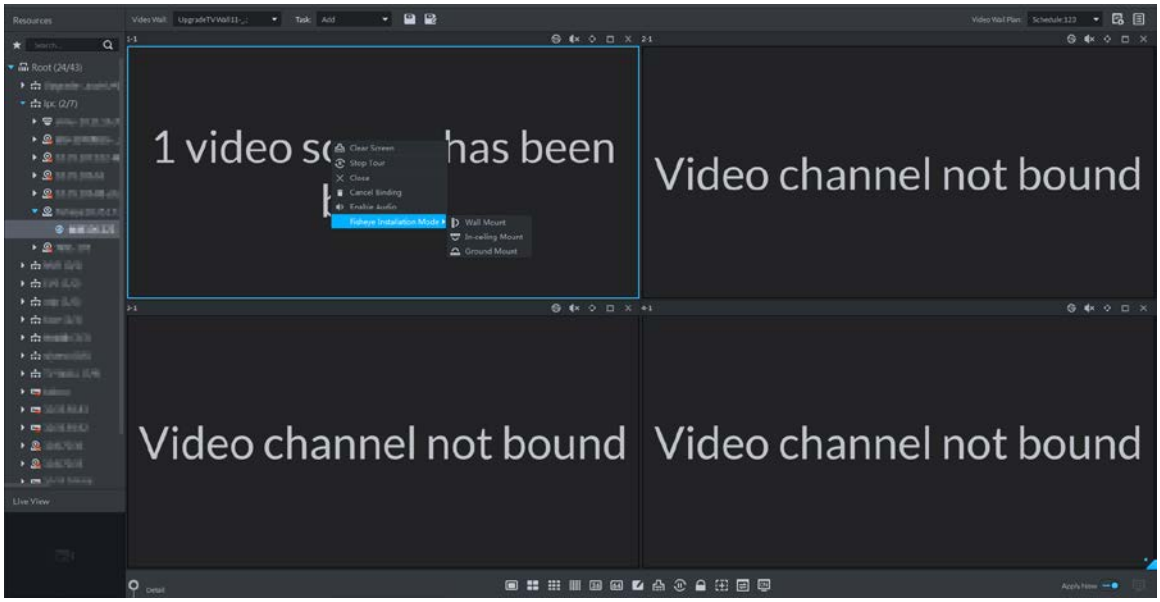


Figure 4-171 Fisheye dewarp

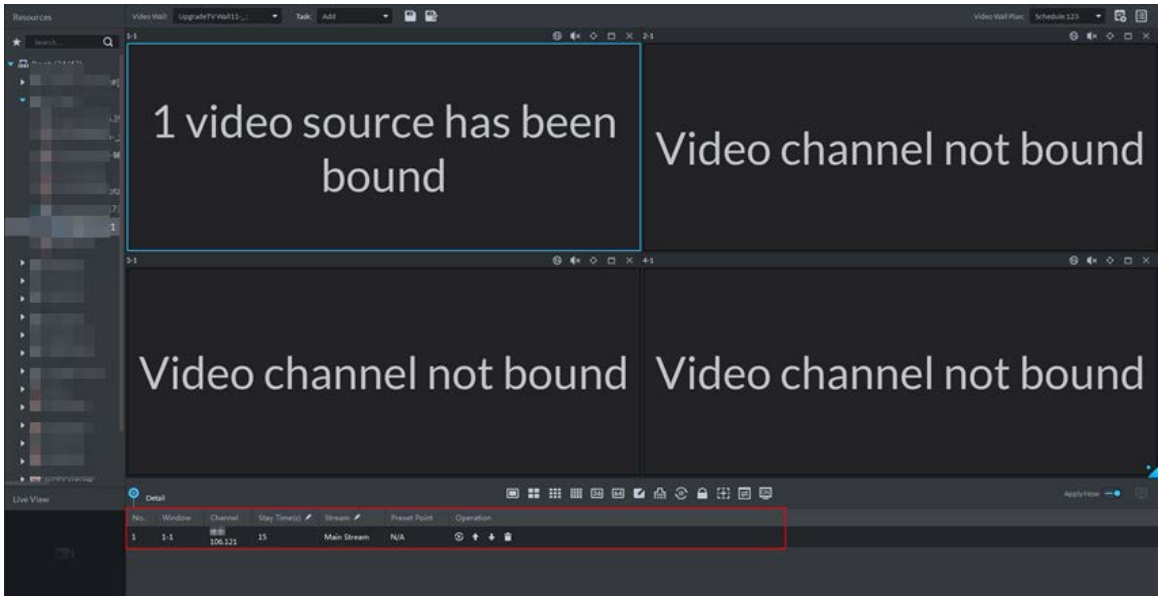


Step 4 Select screen, click **Detail** on the bottom.

System displays setting interface of channel. See Figure 4-172. View the bound video channel info, meanwhile you can set stay time, stream type, preset and operation of each video channel.

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

Figure 4-172 Set video channel parameter



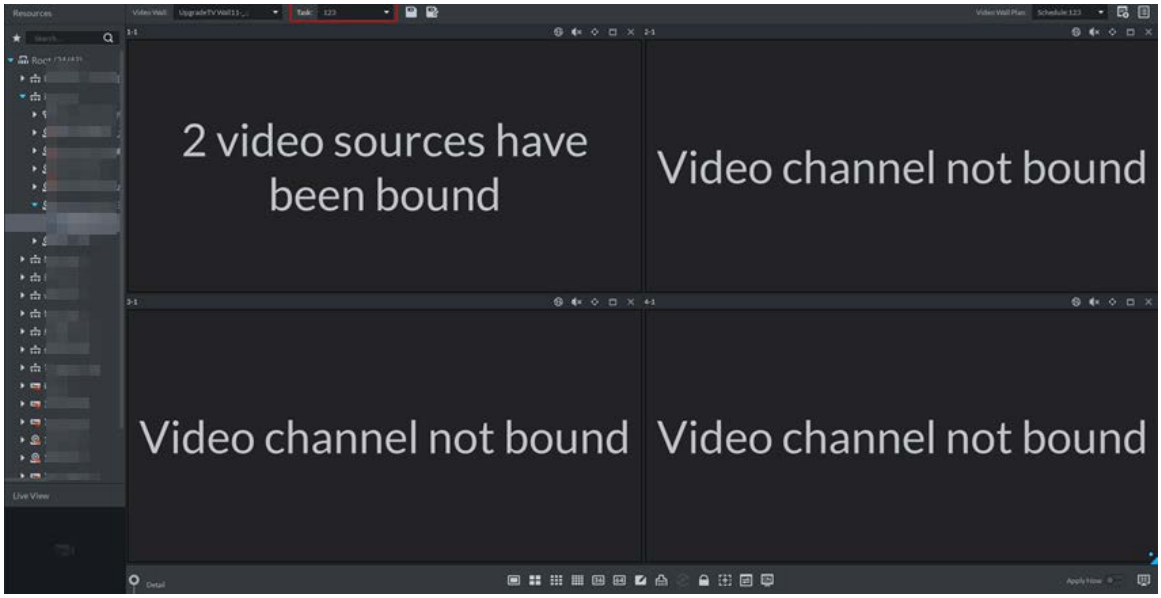
4.6.6.2 Task Displayed on Wall

Call configured task plan and realize quick display on wall.

The task is required to be configured, for detailed config operation, see"4.6.4 Adding Task."

Select task from the box, task is automatically displayed on wall. See Figure 4-173.

Figure 4-173 Task displayed on wall



Support following operations after displayed on wall.

- After task is displayed on wall, if bound video channel is modified, then you need to click on lower right corner and display on wall manually.
- Task displayed on wall, click / on the bottom, then you can stop or start tour.
- Select screen, click **Detail** on the bottom. You can view info of bound video channel; meanwhile you can set stay time, stream type, preset and operation for each video channel.
  - ◇ Click , open real-time video of the channel on lower left corner.
  - ◇ When binding several video sources, click /, and adjust display sequence of video source.
  - ◇ Click and delete video source.

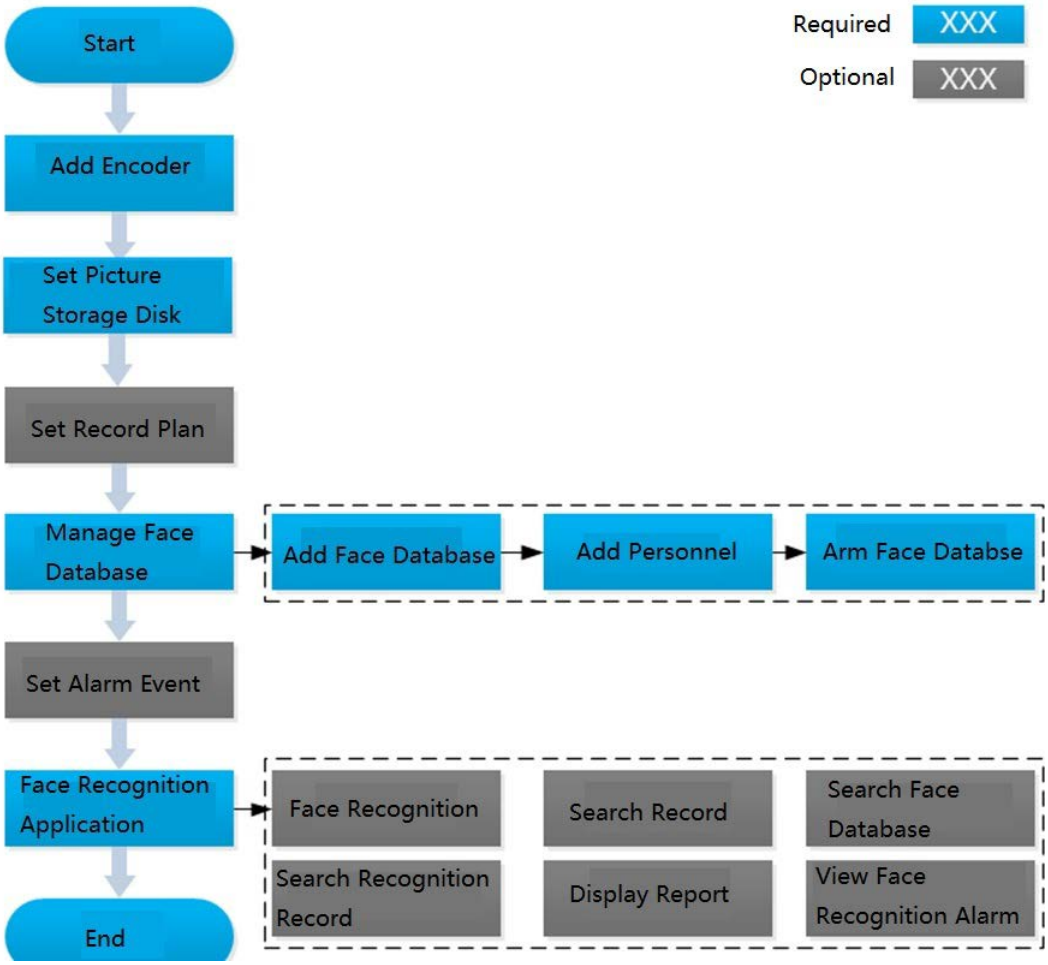
4.6.6.3 Plan Displayed on Wall

According to the timed plan and tour plan that have been set, display on wall automatically with specific period. For details of config plan, refer to"4.6.5 Setting Video Wall Plan."

4.7 Face Recognition

After face recognition device is added to platform, platform displays face recognition results. The operation of face recognition is shown in Figure 4-174.

Figure 4-174 Face recognition flow



4.7.1 Adding Encoder

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

⚠

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

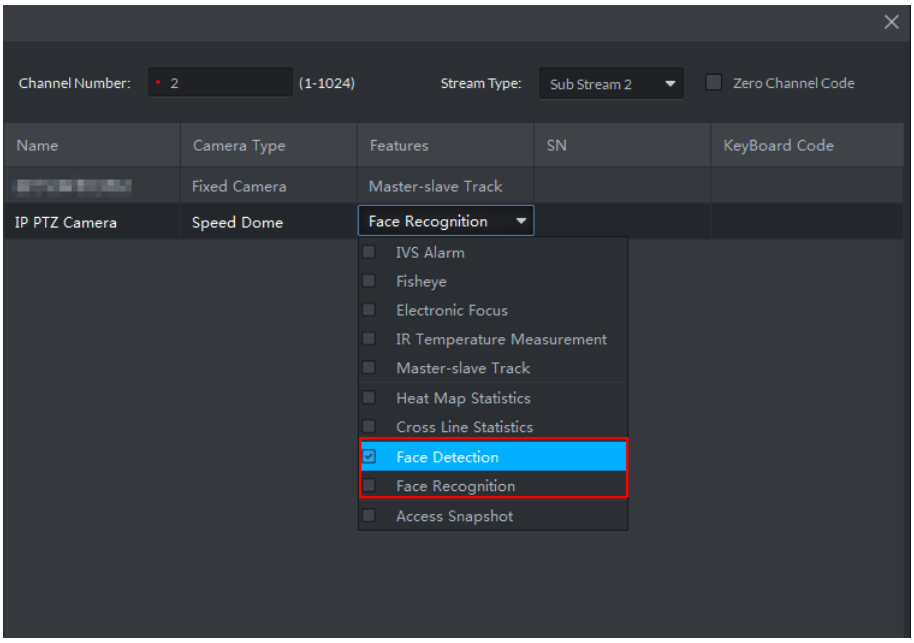
Step 1 Add face recognition camera, NVR or IVSS. For detailed operations, refer to"4.1.2.4 Adding Device."

Step 2 Modify device channel features. On Device interface, click next to device, modify device channel **Features**. See Figure 4-175.

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

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

Figure 4-175 Modify feature



4.7.2 Setting Picture Storage Disk

Configure local storage disk, you have to reserve a general picture disk to store snapshots, otherwise snapshots cannot be stored and displayed. For detailed operations, refer to"4.1.1.4 Setting Storage Space."

4.7.3 Setting Record Plan

After record storage plan is configured, the video before and after face detection snapshot is stored, the platform can playback video 10 s before and after snapshot. If you want to set record storage plan, refer to"4.1.5 Setting Record Plan."

4.7.4 Managing Face Database

Face database management includes following functions.

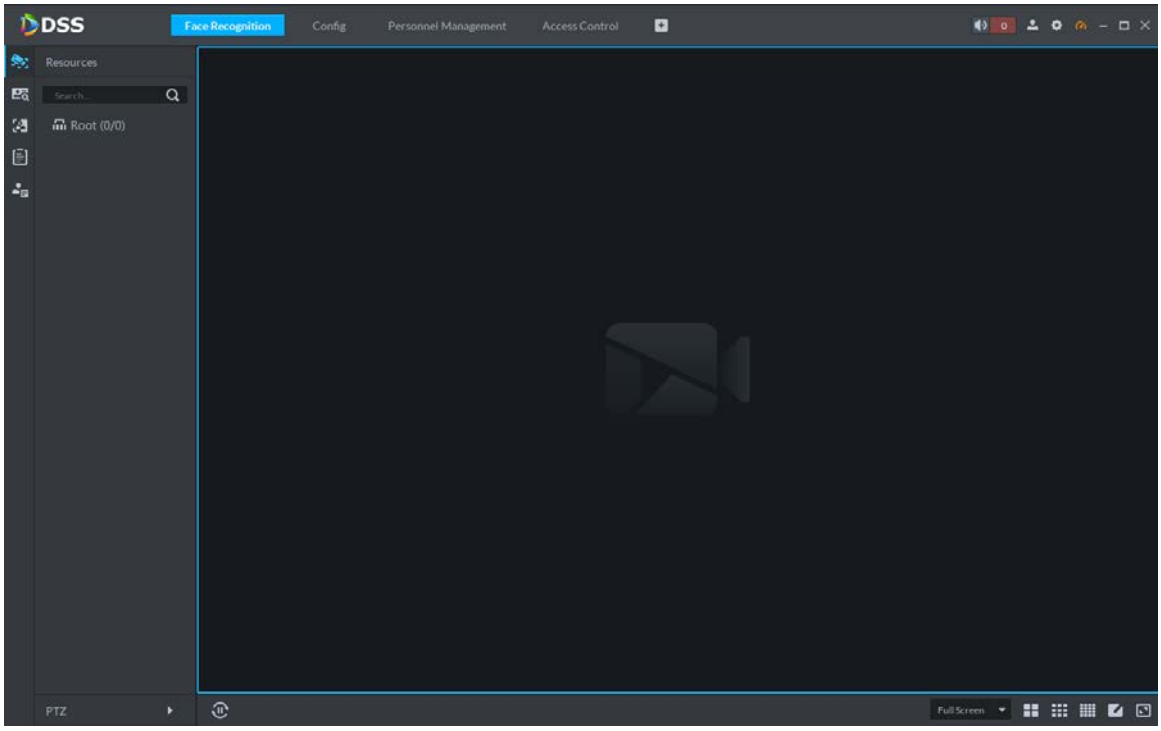
- Add face database to store personnel info, which is convenient for unified deployment over personnel in database. Meanwhile, you can edit and delete face database.
- Add personnel into face database. Meanwhile, you can edit and delete personnel.
- Arm face database. After database is armed, face recognition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

4.7.4.1 Adding Face Database

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

The **Face Recognition** interface is displayed. See Figure 4-176.

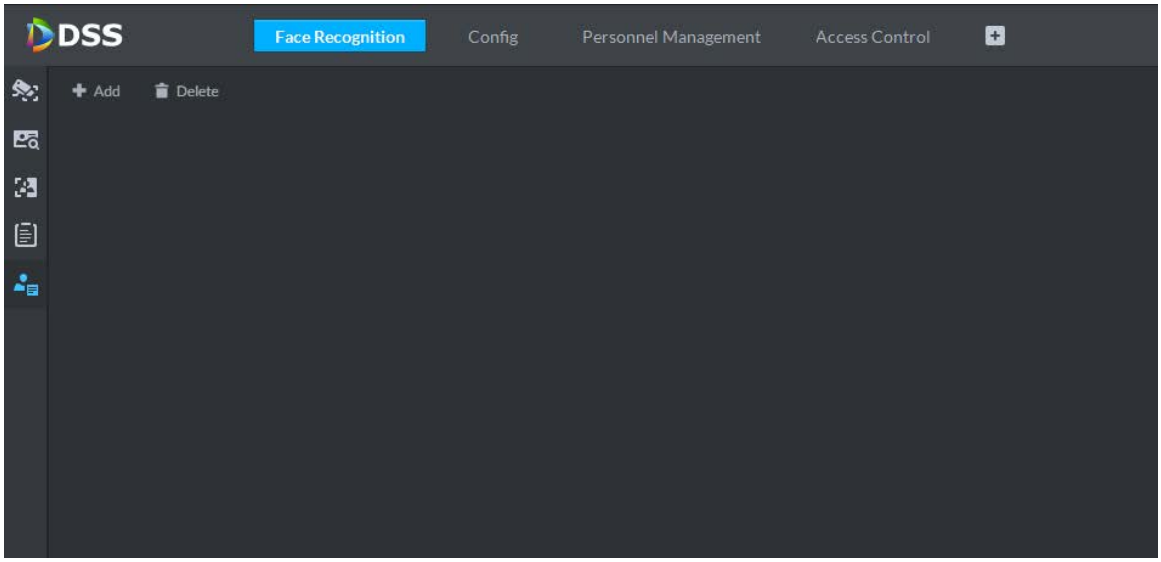
Figure 4-176 Face recognition



Step 2 Click  .

The **Face Database** interface is displayed. See Figure 4-177.

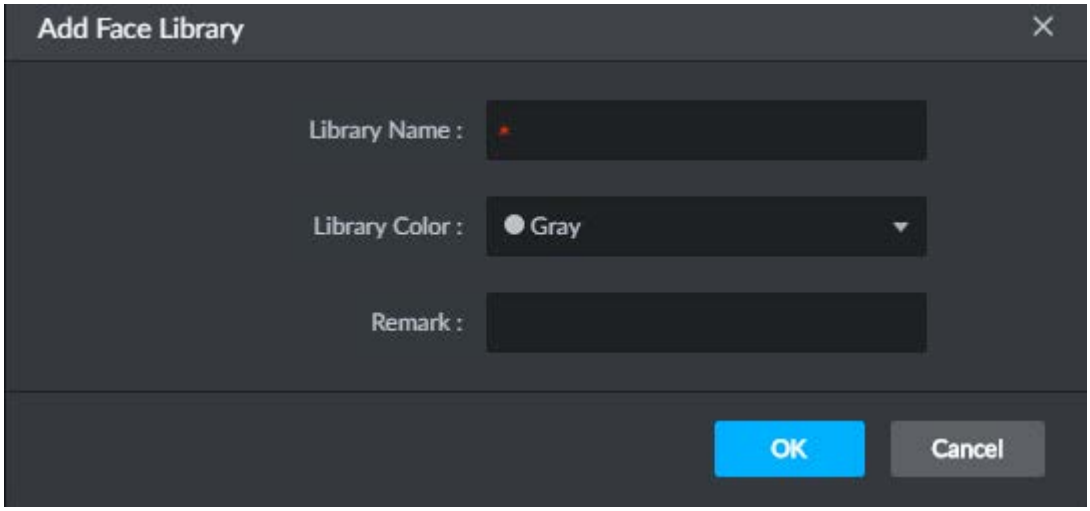
Figure 4-177 Face database management



Step 3 Click Add.

The **Add face library** interface is displayed. See Figure 4-178.

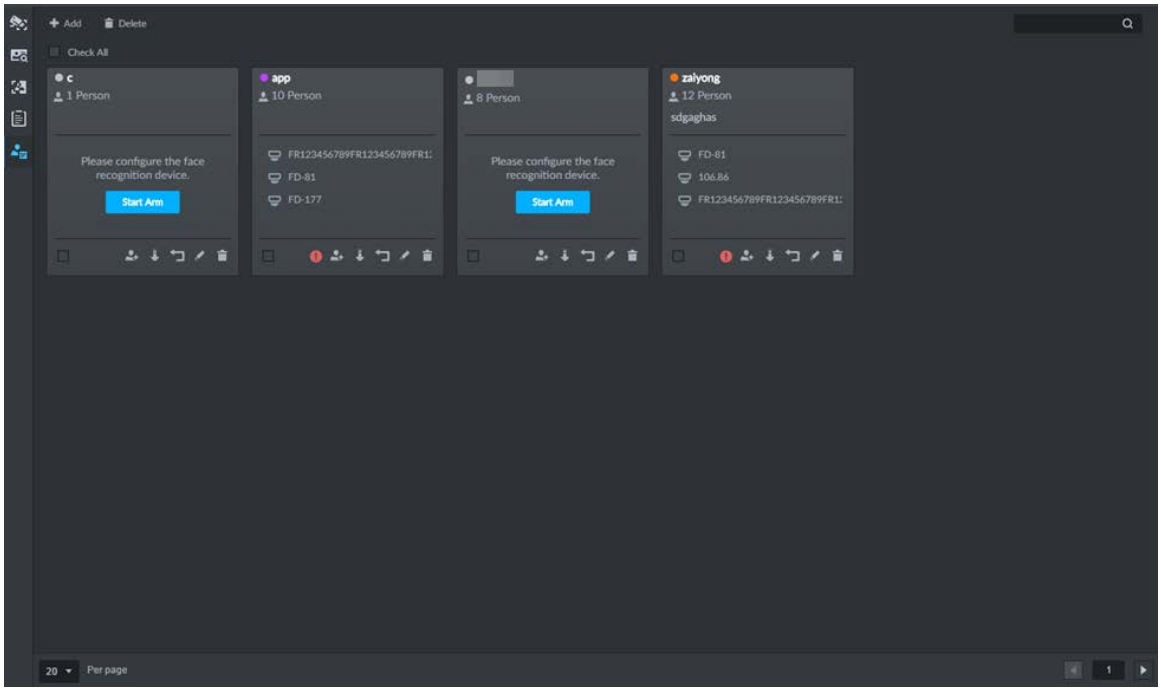
Figure 4-178 Add face library



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

Library color is identified. The new face database info is displayed. See Figure 4-179.

Figure 4-179 Added face database



4.7.4.2 Adding Personnel

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

4.7.4.2.1 Adding Personnel Singly

Step 1 On **Face Database** interface, click  on face database or click face database. See Figure 4-180.

The interface of adding personnel is displayed. See Figure 4-181.

Figure 4-180 Enter add interface

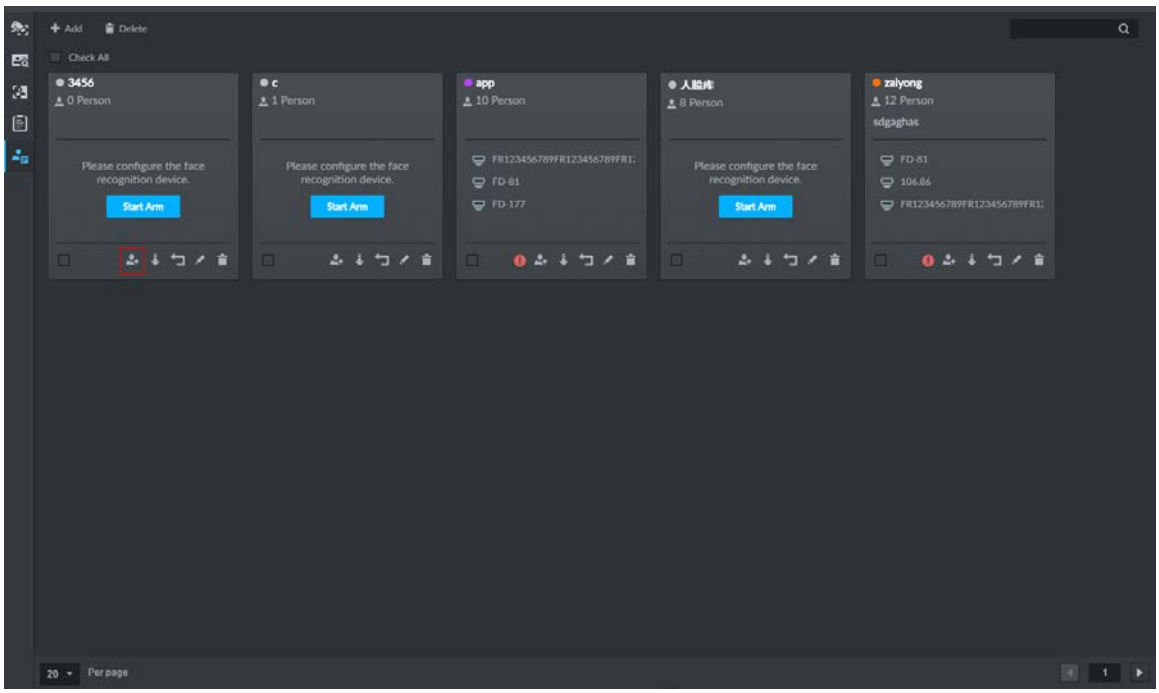
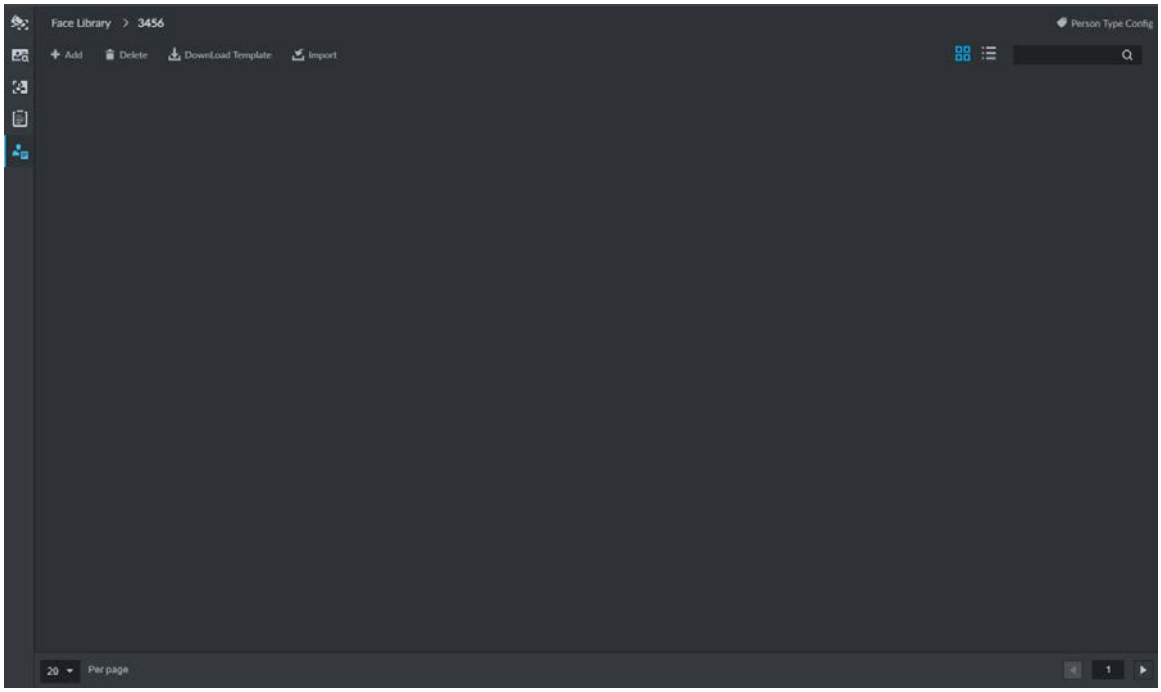


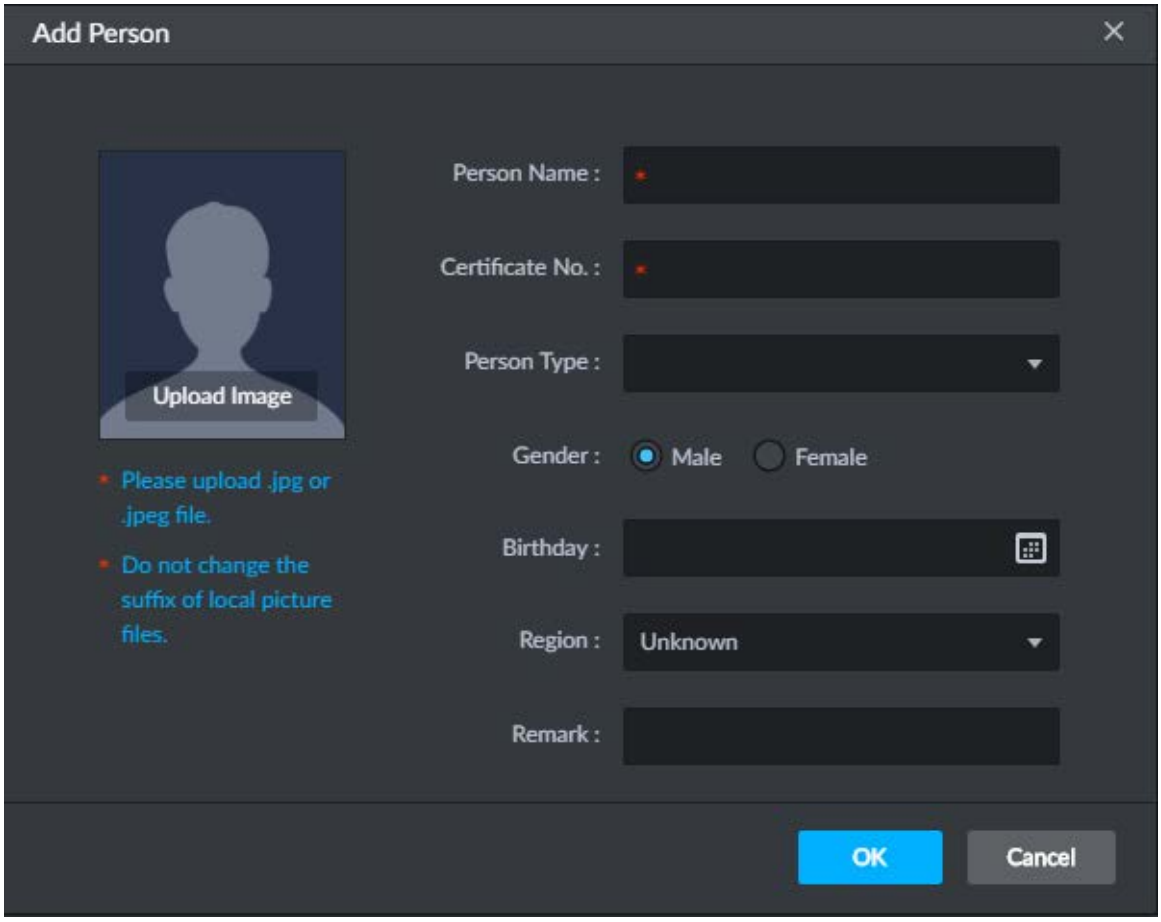
Figure 4-181 Add personnel (1)



Step 2 Click **Add**.

The **Add Person** interface is displayed. See Figure 4-182.

Figure 4-182 Add personnel (2)



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

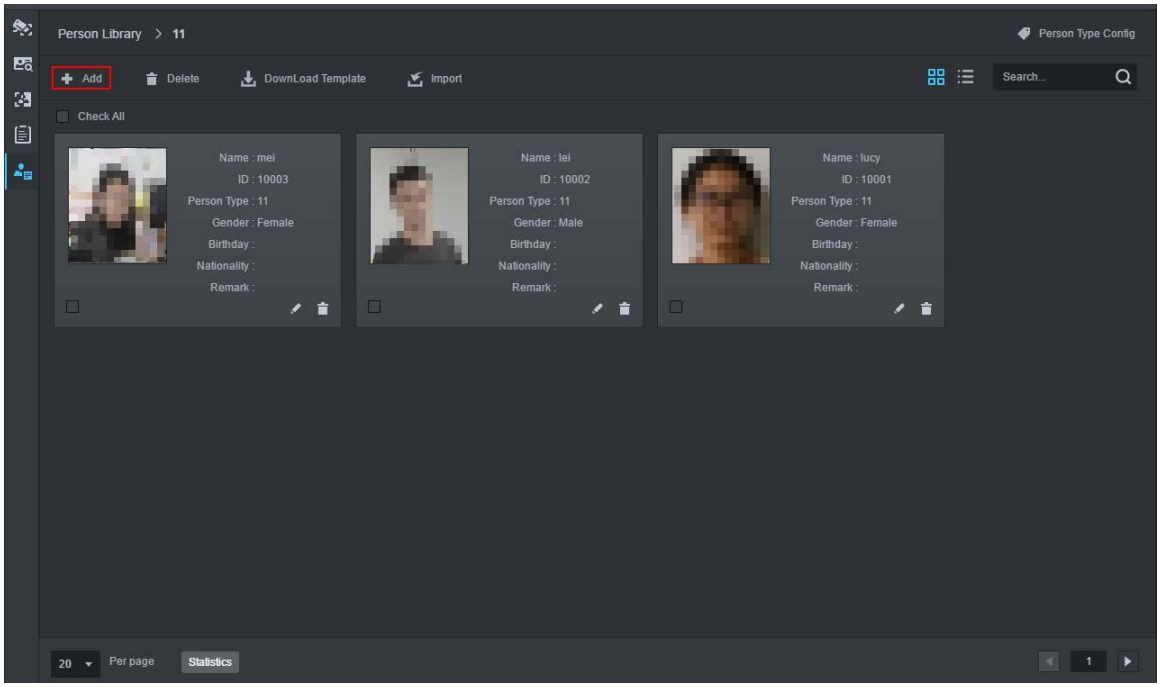
Person type is considered as person property to distinguish person.

Click Person Type Config on upper right corner of Figure 4-181, and you can configure person type as well.

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

The info of added person is displayed. See Figure 4-183.

Figure 4-183 Add



4.7.4.2.2 Importing Personnel

Step 1 On **Face Database** interface, click  or the face database. See Figure 4-180.

The interface of adding person is displayed. See Figure 4-181.

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

Step 3 Make upload file.

1) Edit personnel info excel table. Picture info is required to be in accordance with picture file name.

Figure 4-184 Enter information in the template

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

*Name	*ID	*Type	*Gender	Birthday	Nationality	Remark	*Face Image
Jerry	35125	Staff	Male	1988/5/6	China	Joined on October 2th	face.jpg

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

Step 4 Click **Import**, and upload compression package according to interface prompt.

The import progress and result is displayed.

4.7.4.2.3 Captured Person Register Library

Step 1 Enter person register interface.

Support following methods to enter register interface.

- On **Face Recognition** interface, double click person snapshot. See Figure 4-185. Enter person detail interface. See Figure 4-186. Click  and enter register interface.

Figure 4-185 Double click snapshot

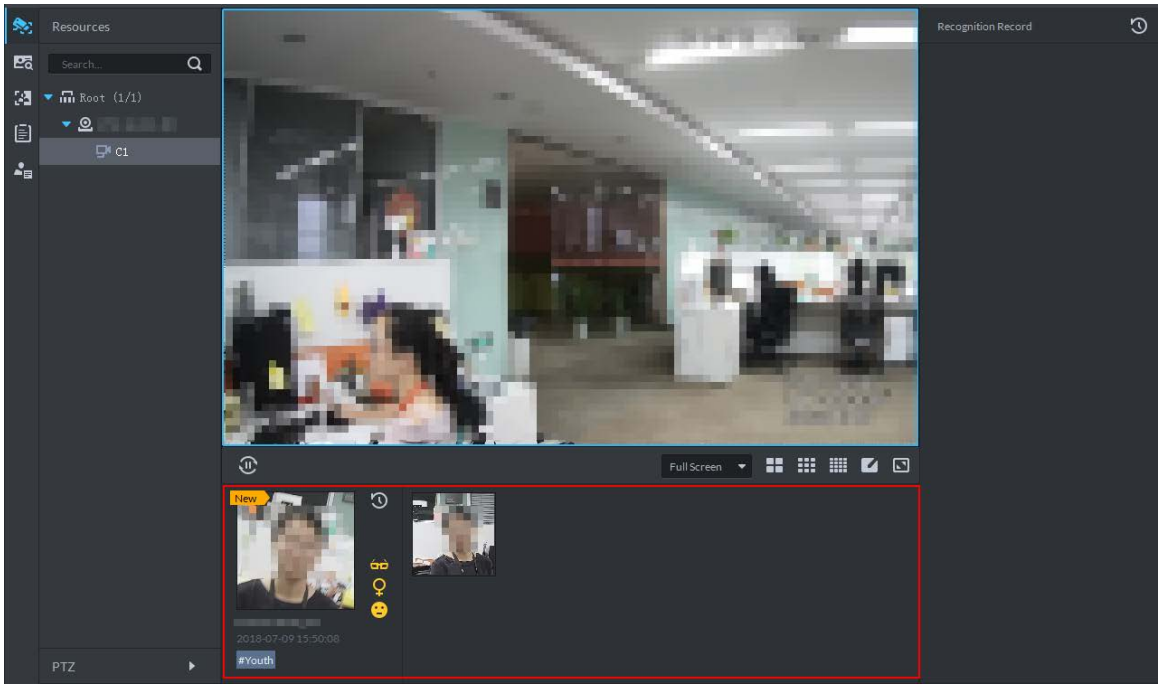
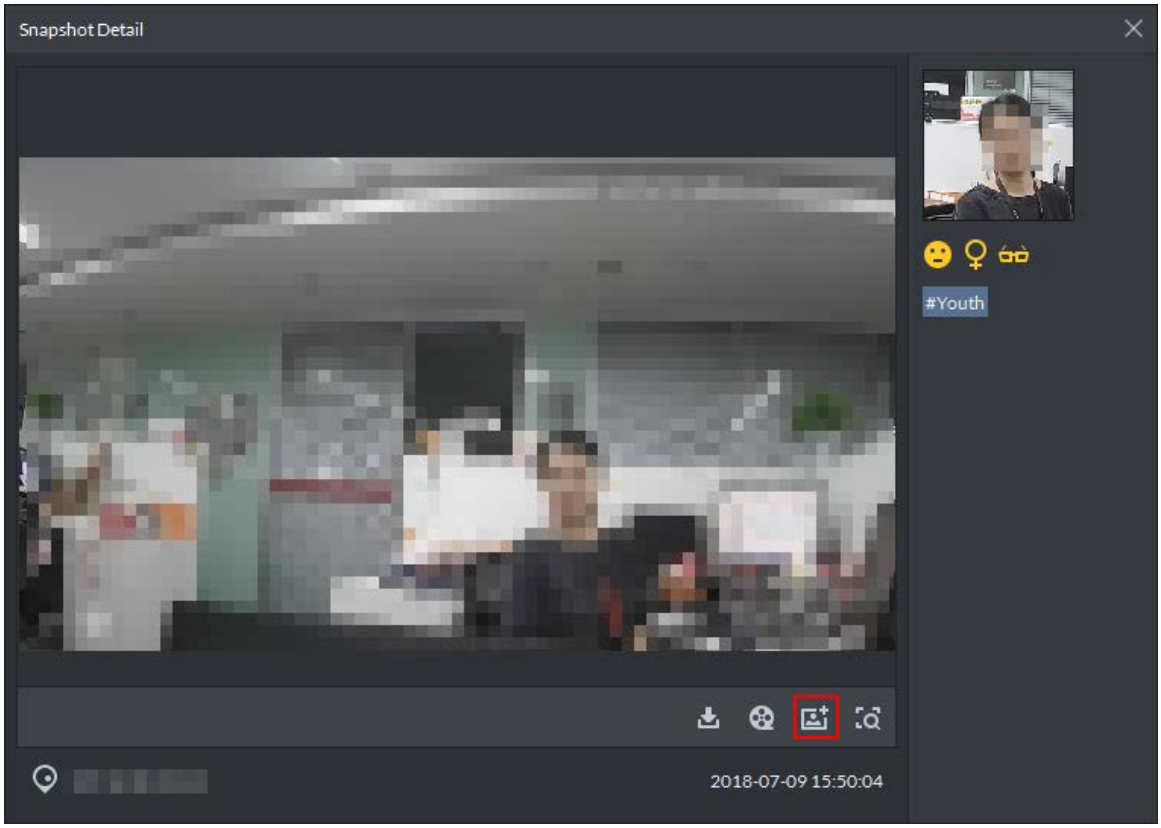
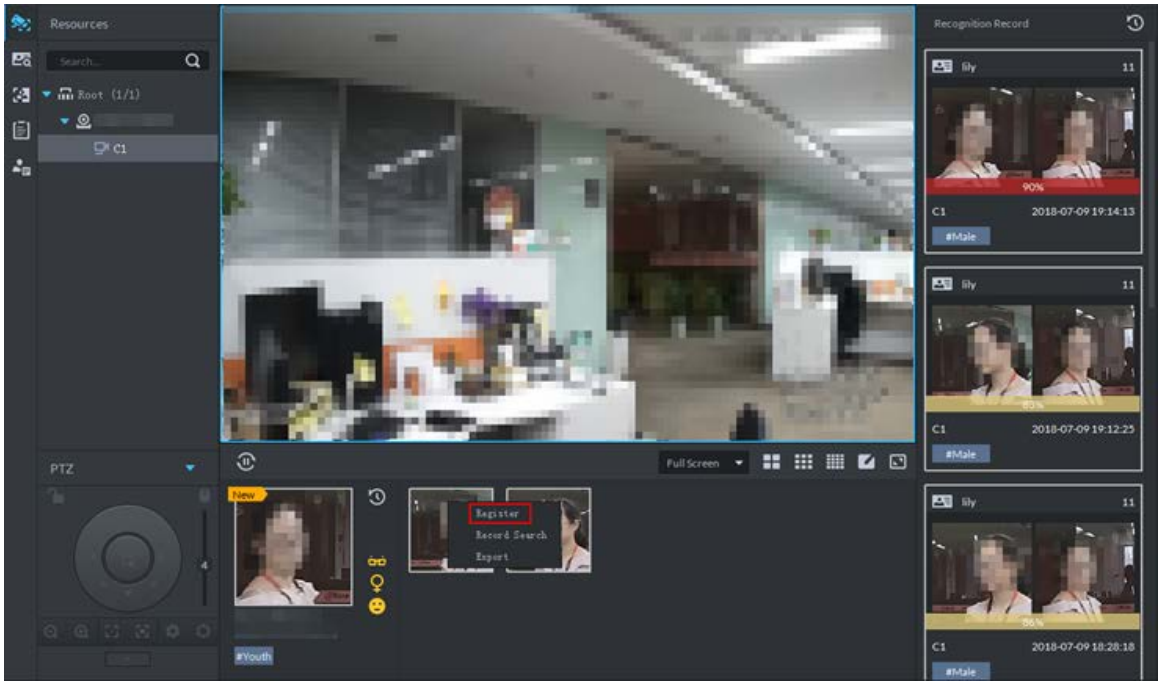


Figure 4-186 Person detail



- On **Face Recognition** interface, move mouse to person snapshot, right click and select **Rgister**, and enter register interface. See Figure 4-187.

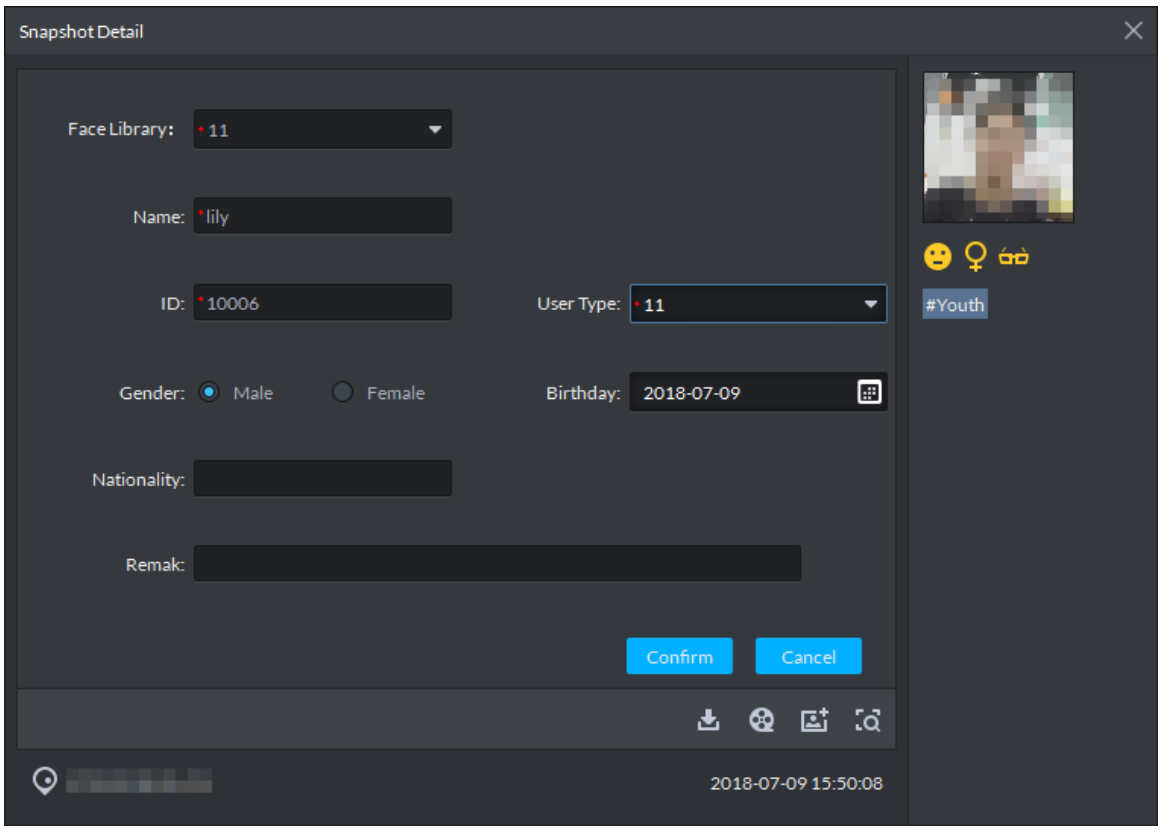
Figure 4-187 Register captured person



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

Step 2 Select face database you want to add, enter person info. Click **OK**. See Figure 4-188.

Figure 4-188 Register person



4.7.4.3 Arming Face Database

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

The **Face Database** interface is displayed.

Step 2 Click **Start Arm** or  on the face database. See Figure 4-189.

The **Face Config** interface is displayed. See Figure 4-190.

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

Figure 4-189 Arm button

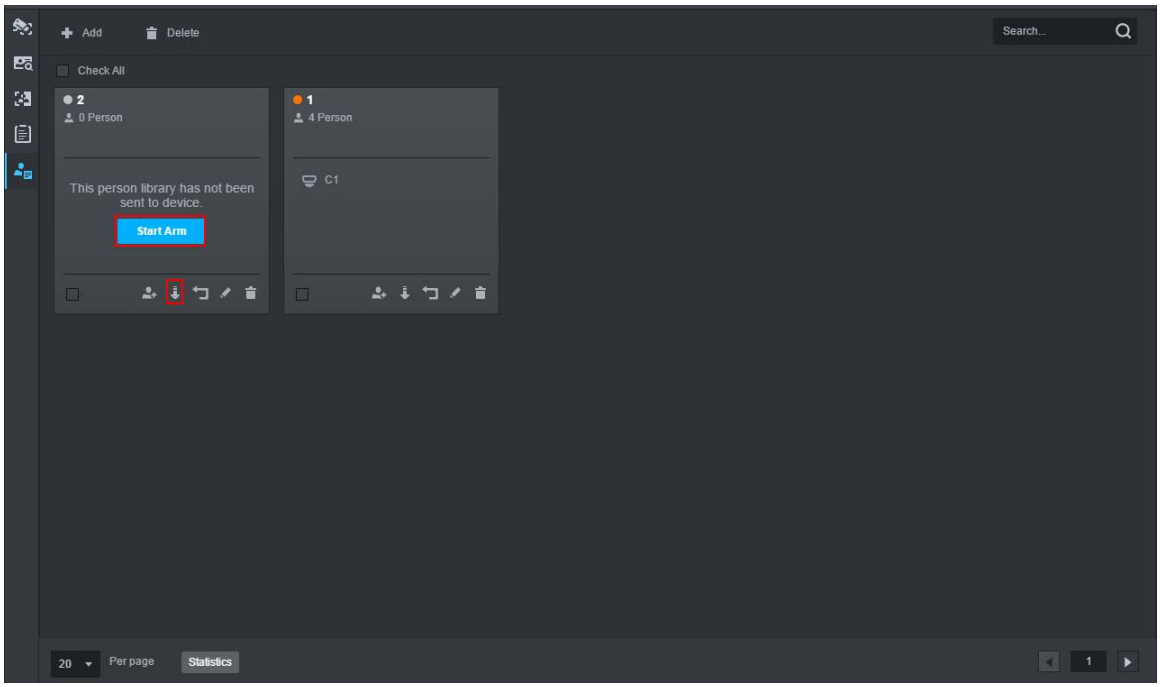
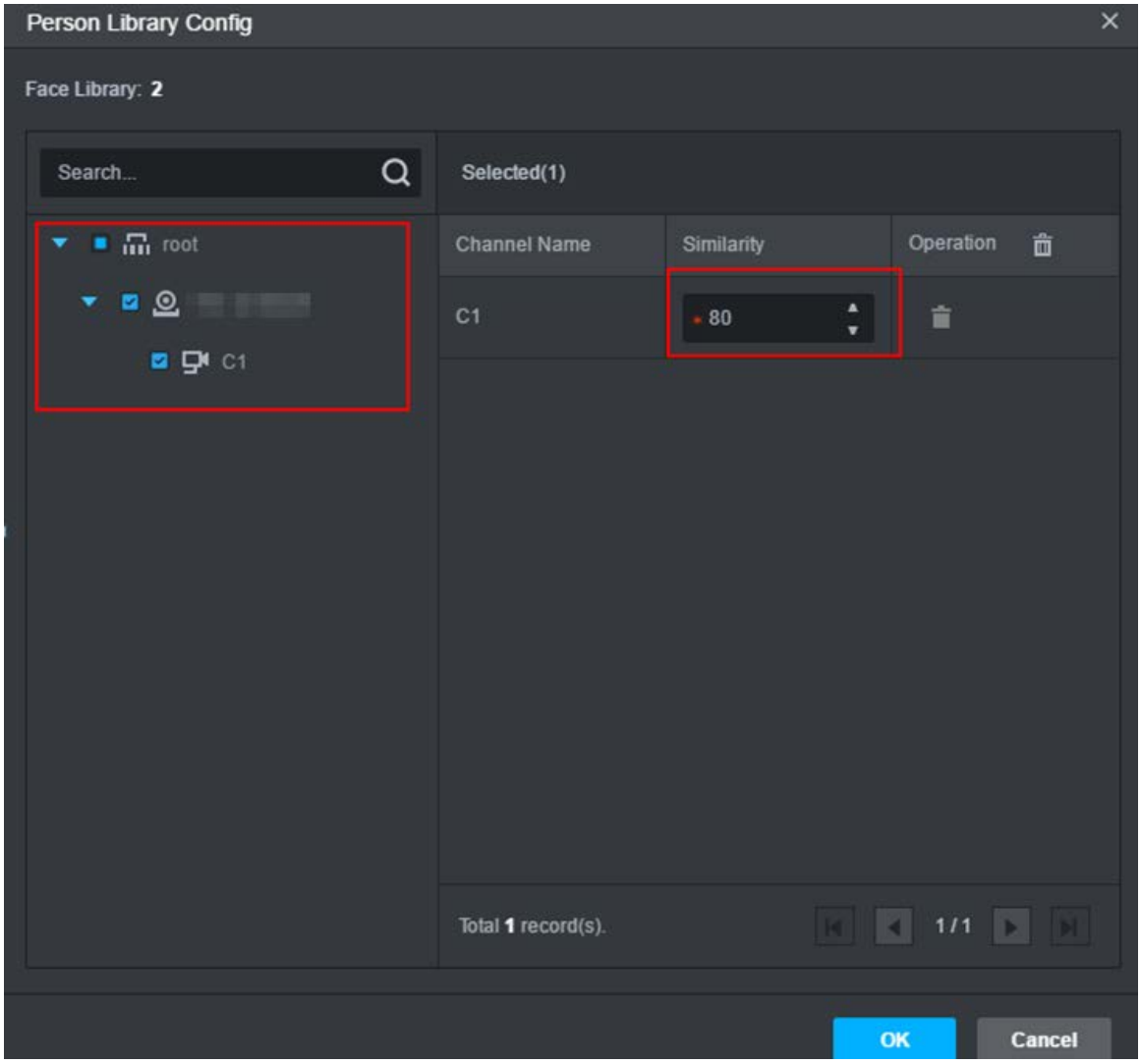


Figure 4-190 Arm config



Step 3 Select the channel you want to arm (multiple choice supported), set similarity, and click **OK**. Recognition record is reported when similarity is≥ threshold.

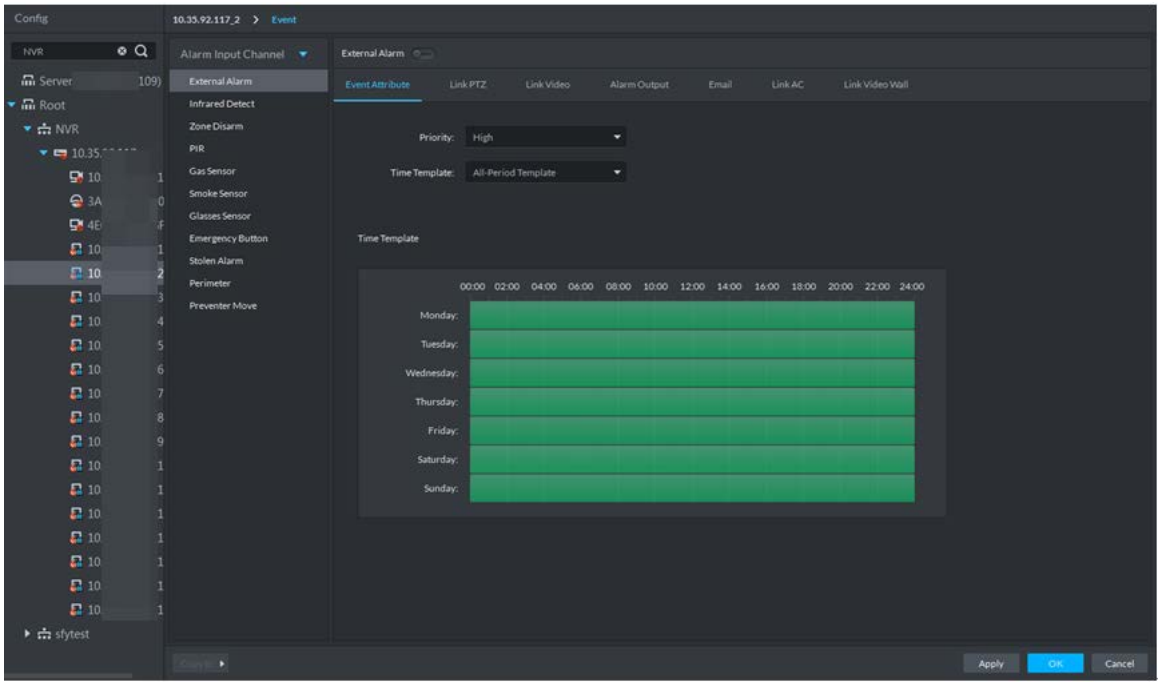
4.7.5 Setting Alarm Event

This chapter only introduces related alarm about face recognition. For more alarm event setting, see"4.1.4 Setting Alarm Event." Face recognition alarms include following types.

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

Set alarm event. See Figure 4-191.

Figure 4-191 Face recognition alarm event



4.7.6 Face Recognition Application

Application of face recognition business client includes:

- Live Preview
  Live preview supports view of live view, person snapshot and recognition record. Meantime it supports view of corresponding panorama and link video of person snapshot, download link video, sign up snapshot person and etc.
- Snapshot Search
  Search matched person by feature info in face library or snapshot record.
- Recognition Search
  By setting feature info, search matched recognition record in recognition record.
- Report
  For a certain channel, according to snapshot time, snapshot person age, create a report of snapshot person.

Face snapshot storage info:

- Snapshot is stored in server installation path: "/opt/tomcat/tmp/autoBackup".
- Take 2 snapshots a time, one face snapshot and the other panoramic picture. In general the picture size is 100KB.
- Snapshots are stored for 30 days by default. If you want to modify details, refer to"4.1.1.1 Setting Message Storage."

4.7.6.1 Face Recognition

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

4.7.6.1.1 Live View

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

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

The **Face Recognition** interface is displayed.

Step 2 Enable realtime monitoring, enable realtime monitoring interface, and see Figure 4-192.

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

Figure 4-192 Live view

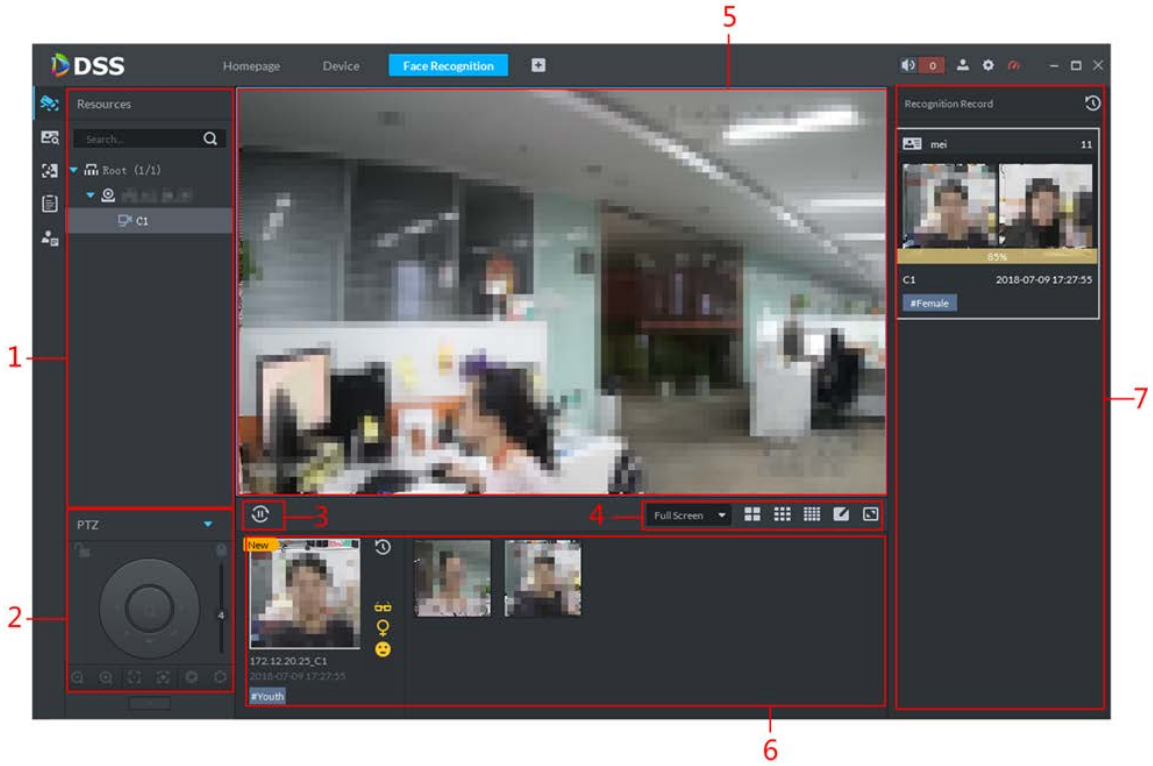


Table 4-33 Live video interface description

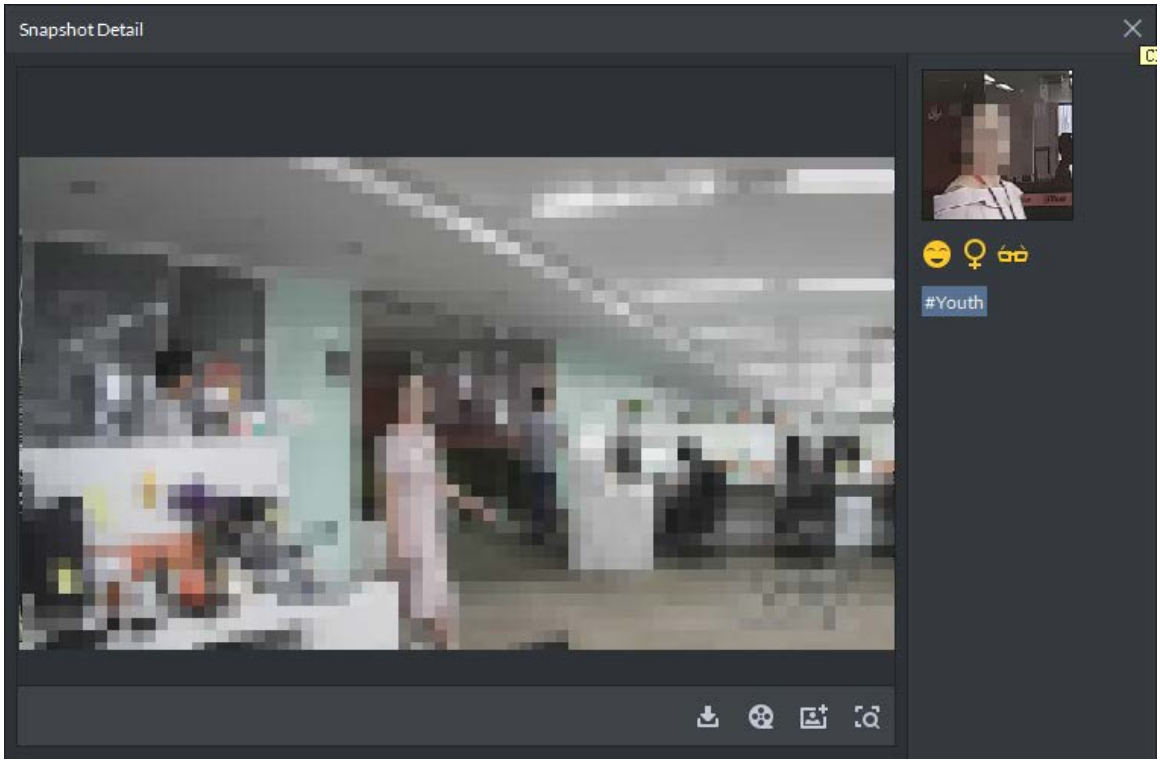
No.	Name		Description
1	Device Tree		Display device and device channel info. ● Right click root node, support display type. You can set display by name and IP. Support ranking, by ascending and descending and default sequence. Support to hide and show offline node. ● Right click device, select tour，support to set all channel tour preview of this device. After you enter touring, if you want to stop touring, then you can right click in preview video, select **Stop Touring** to end tour. ● Right click channel to enter Record Configuration and Event Configuration.
2	PTZ		Speed dome adjust. If you want to expand PTZ operation zone, click behind PTZ to hide PTZ area. When PTZ area is hidden, click behind PTZ to expand PTZ zrea.
3	Pause Refresh/Start Refresh		● , page shows this icon，snapshot area does not refresh face snapshot. Click this icon, live refresh face snapshot. ● , page shows this icon. Snapshot display area shows refresh of face snapshot. Click this icon, refresh face snapshot.
4	Full Screen	Picture Display Scale	Support full screen and original scale.
		Window Switch Number	Support switch display of window quantity, and customized setup.
		Full Screen	Show full screen.
5	Monitor Window		Show channel preview channel. ● Multiple window/single window switch Multiple window display mode, double click window, switch to single display mode and double click again to return to multiple window display mode. ● Full screen mode Right click window to select to enter full screen mode. If it is already in full screen mode, right click to exit full screen. ● Exit tour. ● If it is in touring mode, to stop touring, you can right click in the preview window and select **Stop Tour**.

No.	Name	Description
6	Person Snapshot Record Display Area	Show snapshot face snapshot. Move mouse to person snapshot and right click the snapshot, you can: ● If this person is only snapshot but not recognized ◇ Select **sign up**, add person to library following prompt. ◇ Select **record search**, go to snapshot search page. In snapshot history record, search all snapshots of this person. ◇ Select **Export**, save person snapshot to client locally. Path is default path: ..\DSS \Client\Picture\Face\Export\Capture. ● If this person is recognized ◇ Select **Recognition Record Search**, go to search page, and in snapshot history record search all recognition records of this person. ◇ Select **Export**, save person snapshot and pictures of this person in library to client locally. Path is default path: ..\DSS\Client\Picture\Face\Export\Recognize. Double-click person snapshot, to view person details, including snapshot person cutout and panorama.
7	Recognition Record Display Area	Show recognition record. ● Move mouse to person snapshot, and right click. You can: ◇ Select **Recognition Record Search,** go to recognition search page, and in snapshot history record, search all recognition records of this person. ◇ Select **Export**, and save person snapshot and snapshot of this person already uploaded to library all to client locally, default path is ..\DSS\Client\Picture\Face\Export\Recognize。 ● Double-click recognition record，you can view person cutout, panorama, used to person picture and info in face library. ● Click  at the upper right corner, go to recognition search page.

4.7.6.1.2 Viewing and Processing Snapshot Detail

- View snapshot detail
  In the area of person snapshot record, double click person snapshot to view face cutout and panoramic picture. See Figure 4-193.

Figure 4-193 Snapshot detail

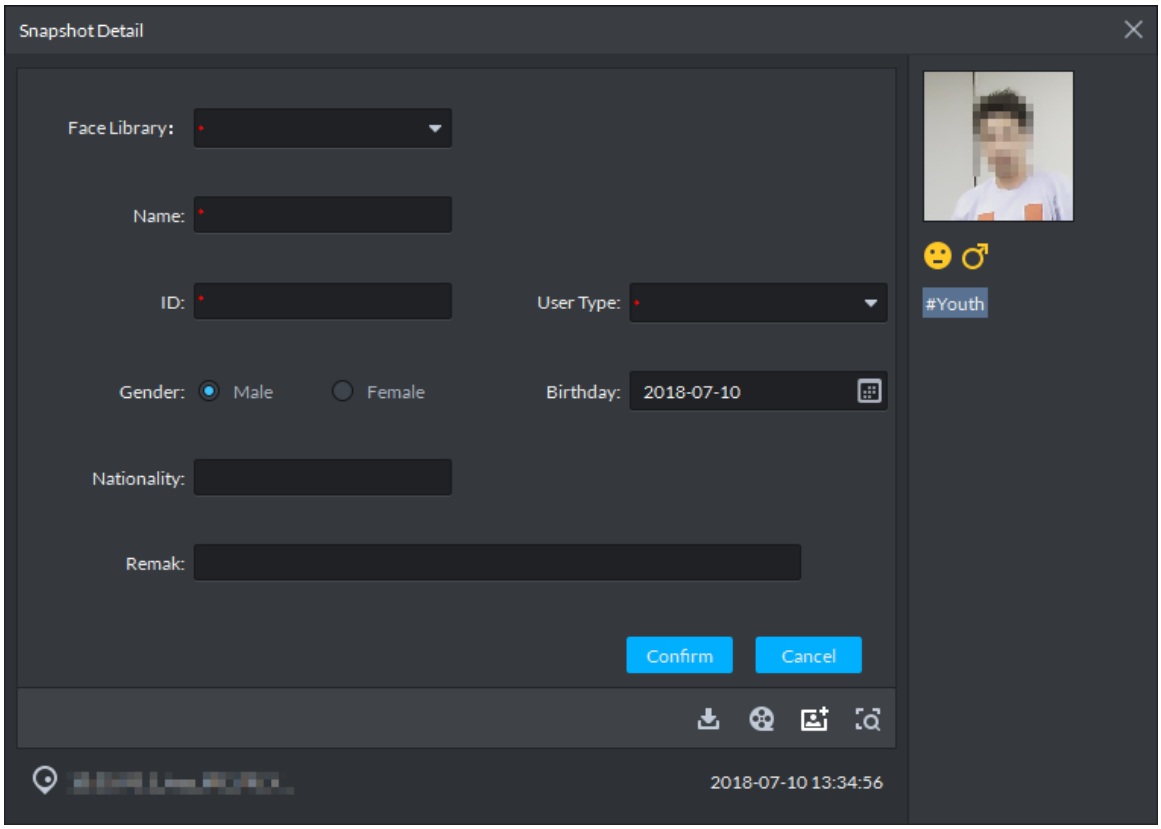


- Register captured person

Step 1 On snapshot detail window, click .

The **Snapshot Detail** interface is displayed. See Figure 4-194.

Figure 4-194 Snapshot detail



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

- View video

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

  On snapshot detail window, click  and enter download center, download video according to requirement. For details, refer to"4.4.8 Downloading Record."
- Search record

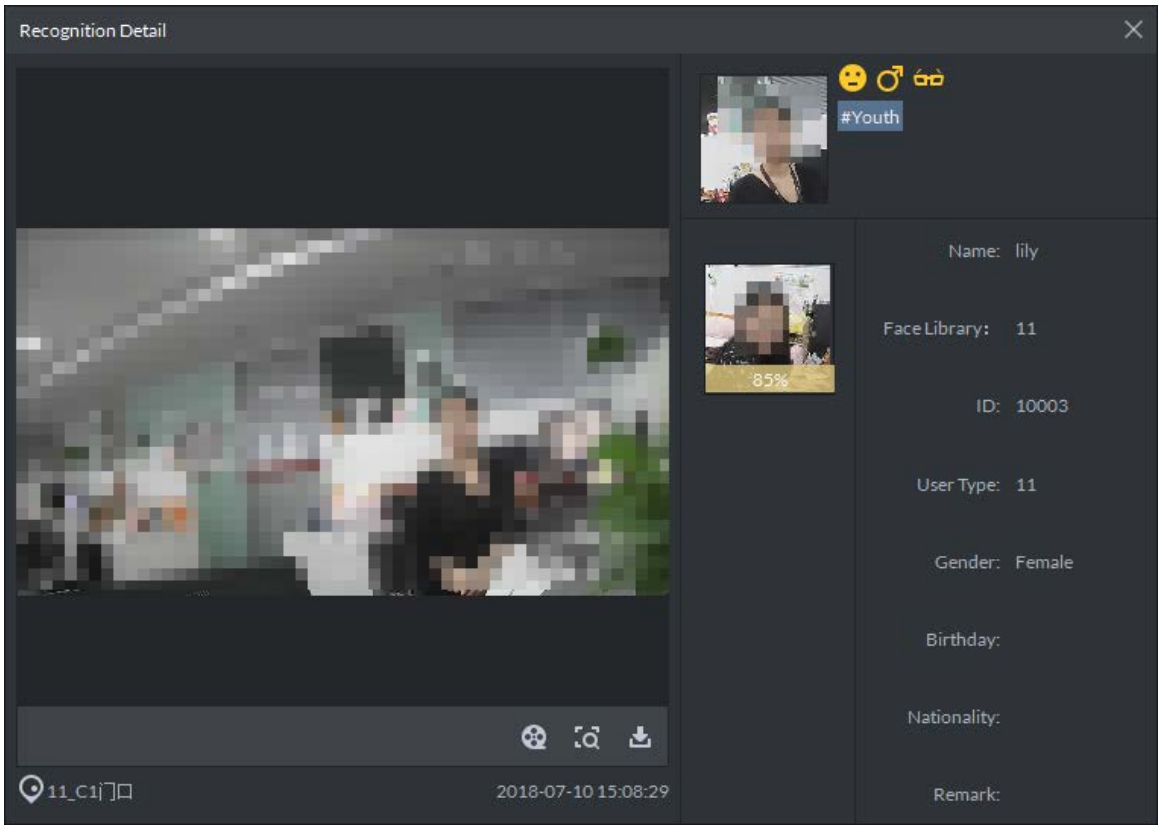
  On snapshot detail window, click  to enter record search page. Set search time and channel, click **Search** to search result.

4.7.6.1.3 Viewing and Processing Recognition Record Detail

- View recognition detail

  In recognition record display area, double recognition record to view snapshot person cutout, panorama, person picture and person info used to compare. See Figure 4-195

Figure 4-195 Recognitiond detail



- View video

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

On snapshot detail window, click and enter download center, download video according to requirement. For details, refer to"4.4.8 Downloading Record."

- Search record

On snapshot detail window, click to enter record search page. See Figure 4-196. Set search time and channel, click **Search** to search result. See Figure 4-197.

Figure 4-196 Search recognition

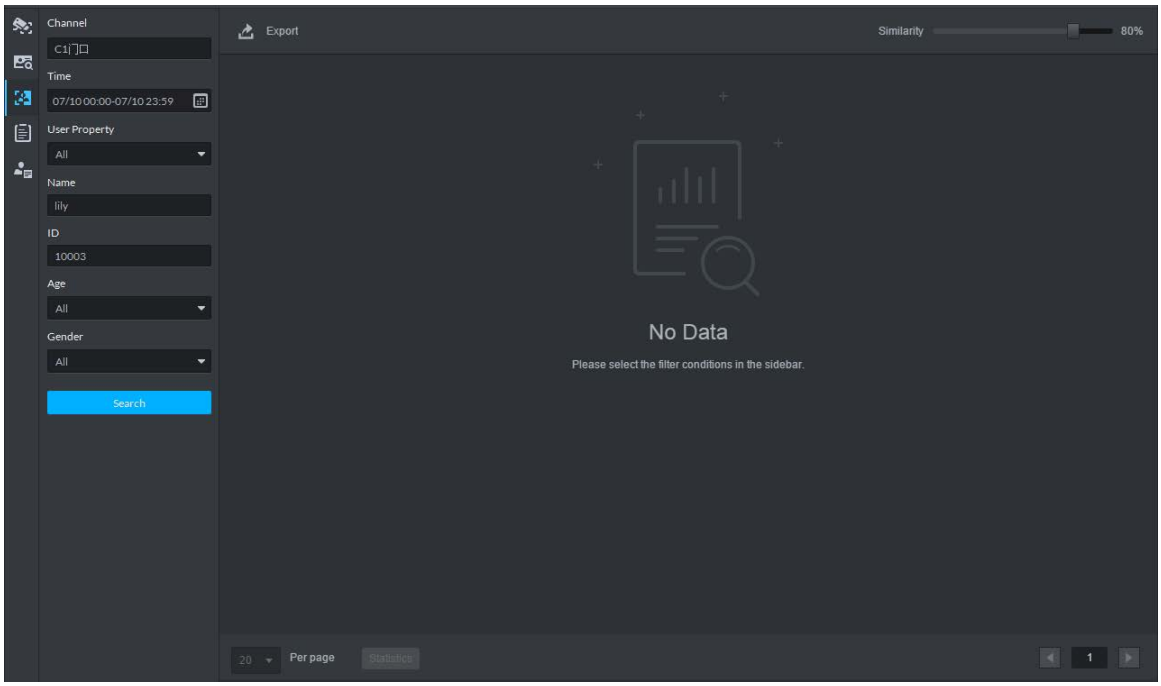
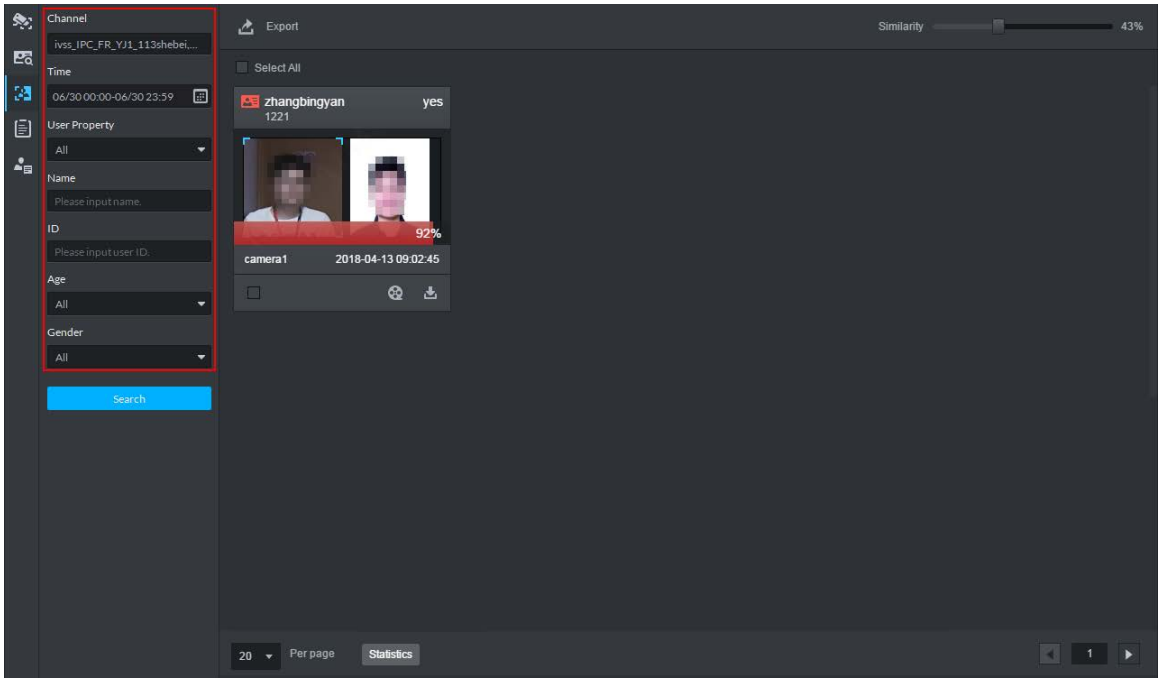


Figure 4-197 Search result

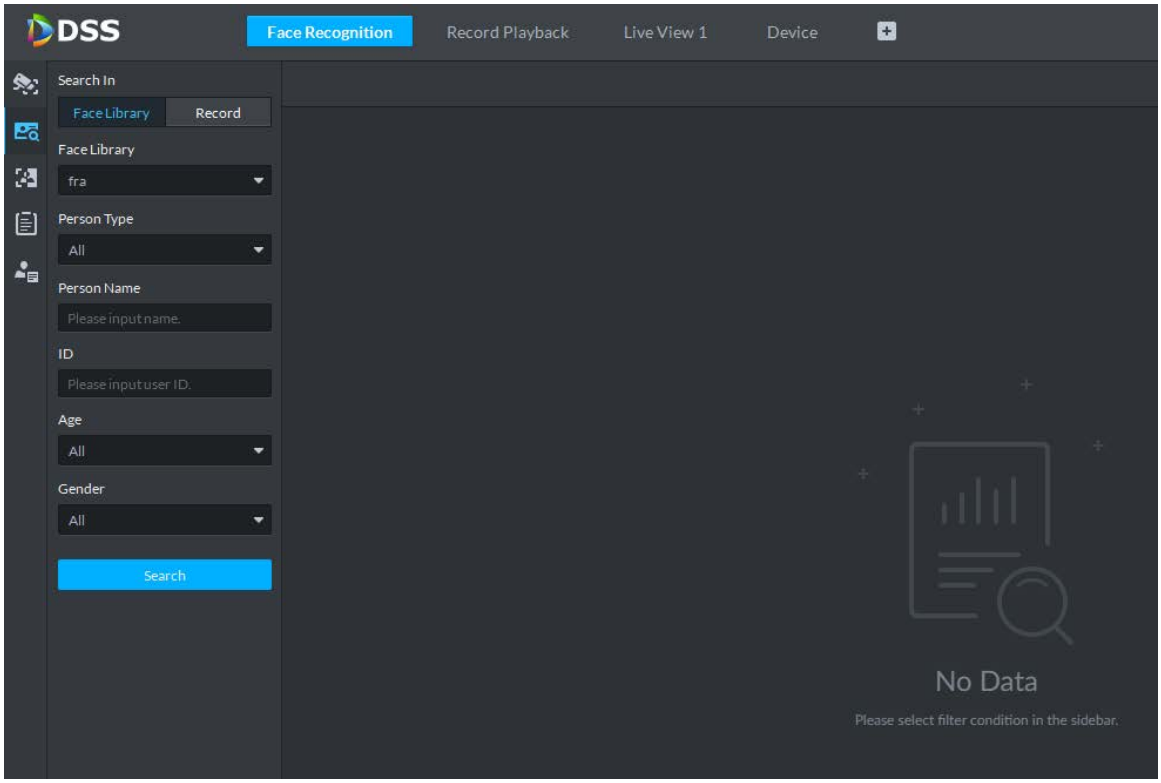


4.7.6.2 Searching Person

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

The **Face Search** interface is displayed. See Figure 4-198.

Figure 4-198 Face search



Step 2 Set search conditions in **Face Library** or **Record**. Click **Search**. The interface of search result is displayed.

The search result supports the following operations:

- If it is the face database search result, then support click , skip to recognition search interface, and search the recognition record of the person.
- Search detail
  Double click to view detail.
- Download video

  On snapshot detail window, click and enter download center, download video according to requirement. For details, refer to"4.4.8 Downloading Record."
- View video

  On the snapshot detail window, click and enter record playback interface. If corresponding video exists in central server or device, then playback video, otherwise, system promps no record file. Video source priority is central server > device.
- Register captured person to face database

  Click and display window of registered person.

4.7.6.3 Searching Recognition Record

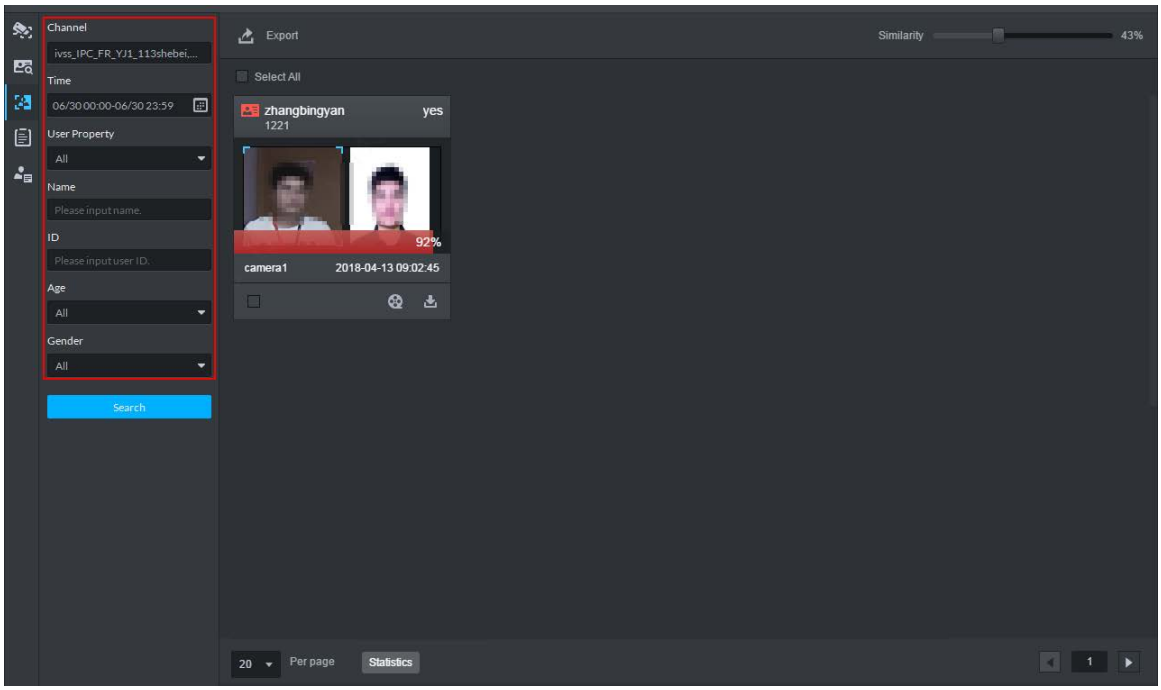
You can search qualified record from recognition record.

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

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

The search result is displayed.

Figure 4-199 Search for recognition records



4.7.6.4 Showing Report

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

The **Report** interface is displayed.

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

- Line chart is shown in Figure 4-200.

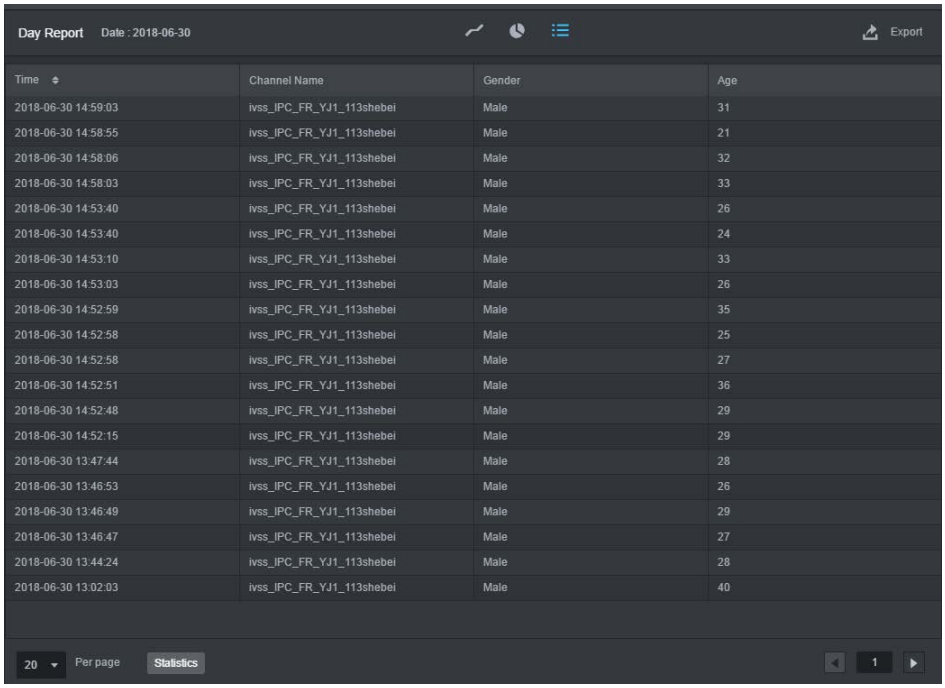
Figure 4-200 Face report line chart

- Pie chart is shown in Figure 4-201.

Figure 4-201 Face report pie chart

- List is shown in Figure 4-202.

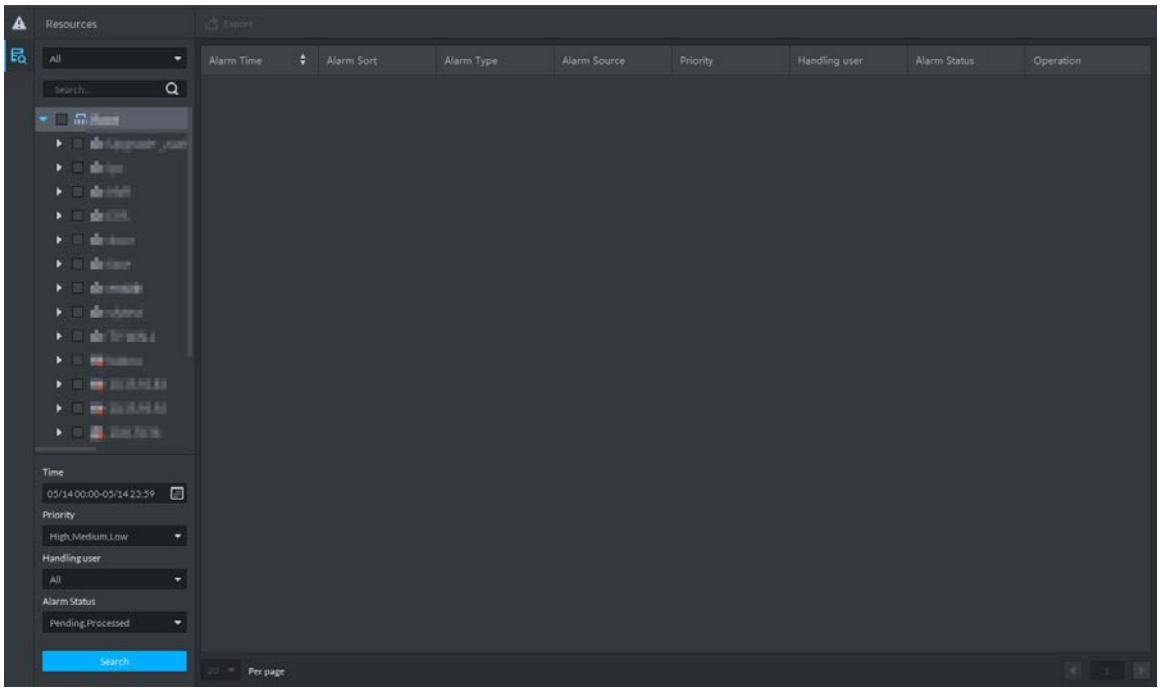
Figure 4-202 List display



4.7.6.5 Viewing Face Recognition Alarm

View and process face recognition alarm event in event center. See Figure 4-203. For more details, see"4.5 Event Center."

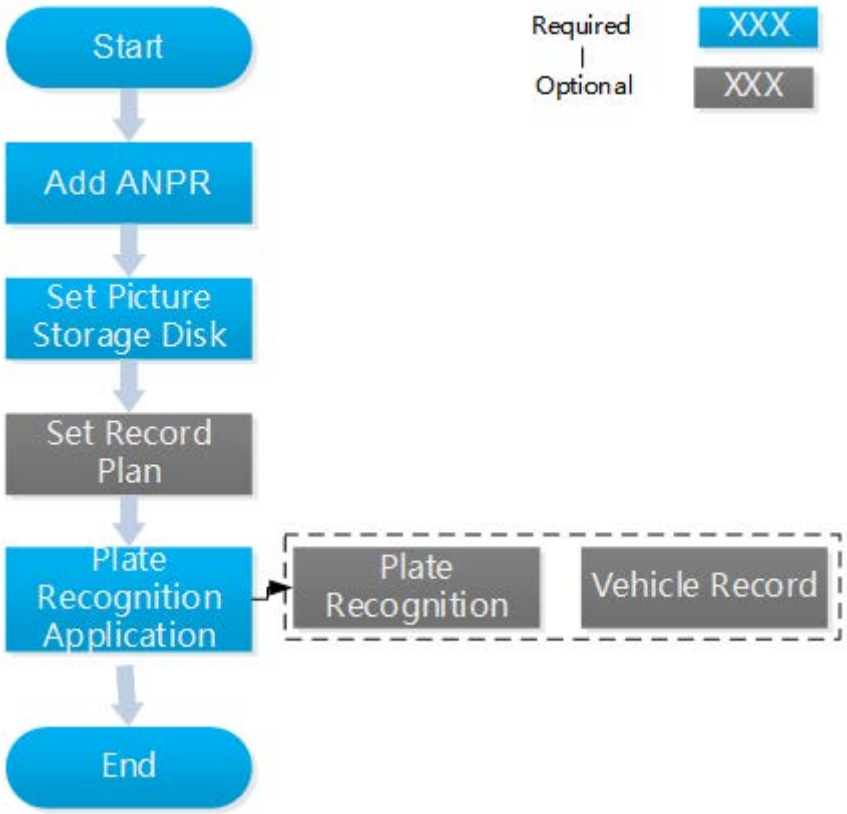
Figure 4-203 List display



4.8 ANPR

After ANPR is added to platform, the platform can receive plate recognition result reported by ANPR. The plate recognition operation flow is shown in Figure 4-204.

Figure 4-204 Plate recognition flow



4.8.1 Adding ANPR

Add ANPR; see"4.1.2.4 Adding Device" for more details.

4.8.2 Setting Picture Storage Disk

Configure local storage disk, you have to reserve a ANPR picture disk to store ANPR snapshot, otherwise, snapshot cannot be stored, and snapshots are not displayed. For more details, see"4.1.1.4 Setting Storage Space."

4.8.3 Setting Record Plan

Only when record storage plan is configured, then video before and after snapshot can be stored, the platform can playback video 10 seconds before and after ANPR snapshot. If you need to set record storage plan, see"4.1.5 Setting Record Plan."

4.8.4 Plate Recognition Application

4.8.4.1 Plate Recognition

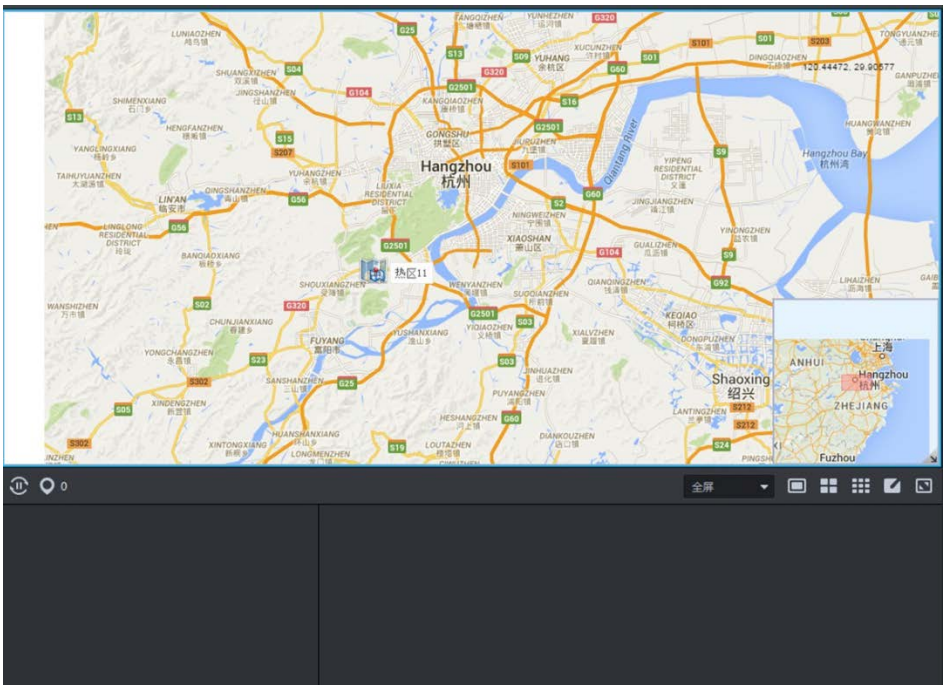
Step 1 On client homepage, click **ANPR**.

The **ANPR** interface is displayed.

Step 2 Click  .

The **ANPR** interface is displayed. The emap is displayed with single window by default; you can switch number of windows. See Figure 4-205.

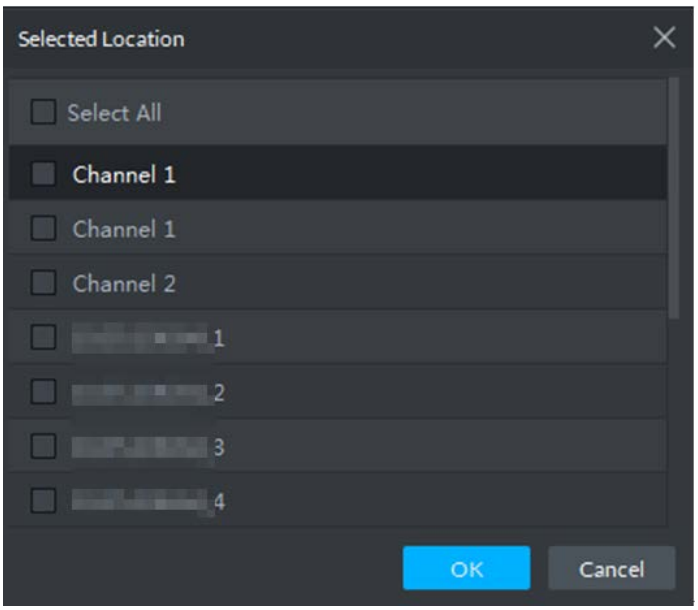
Figure 4-205 Plate recognition



Step 3 Click  .

The **Selected Location** interface is displayed. See Figure 4-206.

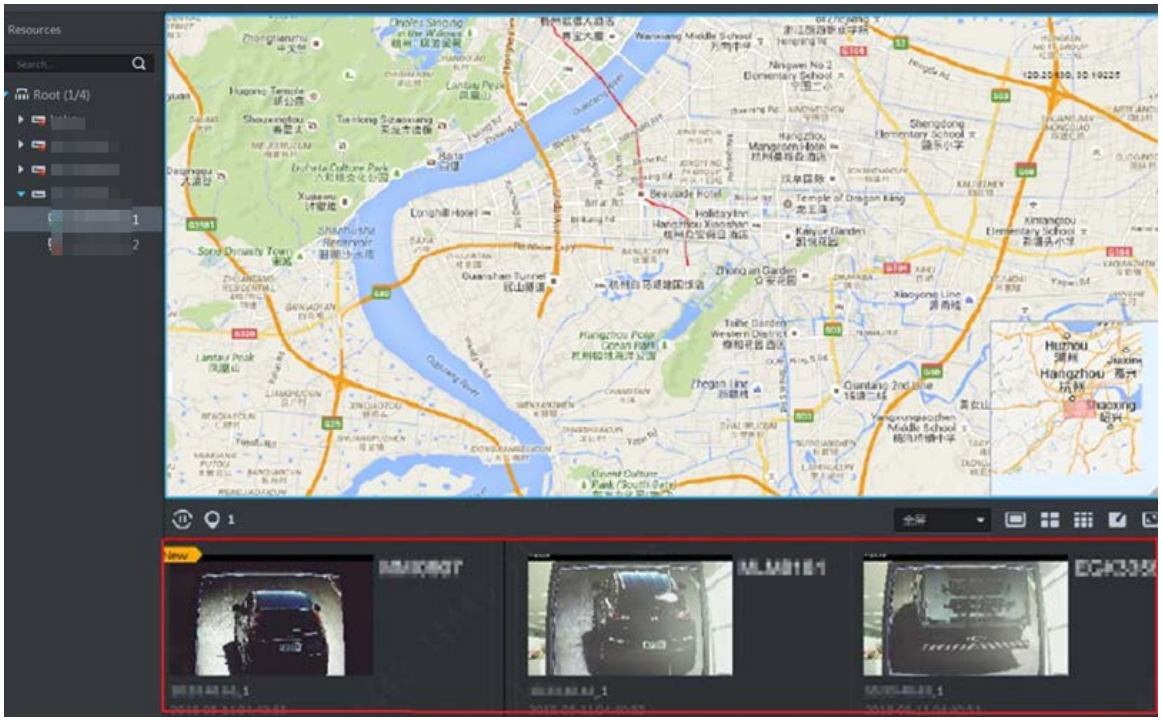
Figure 4-206 Select ANPR channel



Step 4 Select ANPR device and then click **OK**.

System displays the selected channel amount and the latest passing vehicle image on the rolling pane. See Figure 4-207.

Figure 4-207 Plate recognition result



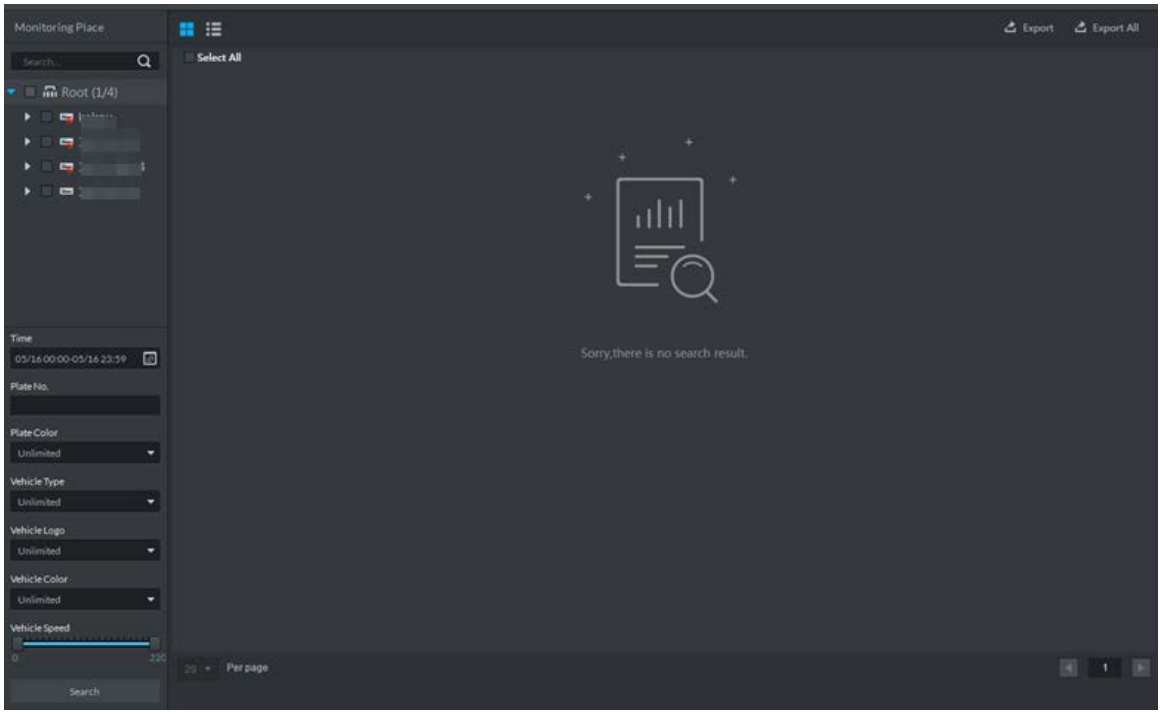
Step 5 Double-click the image to view image details. It includes plate number, snapshot time, ANPR channel name, vehicle logo, vehicle color.

4.8.5 Vehicle Record

Step 1 On ANPR interface, click  .

The **Vehicle Record** interface is displayed. See Figure 4-208.

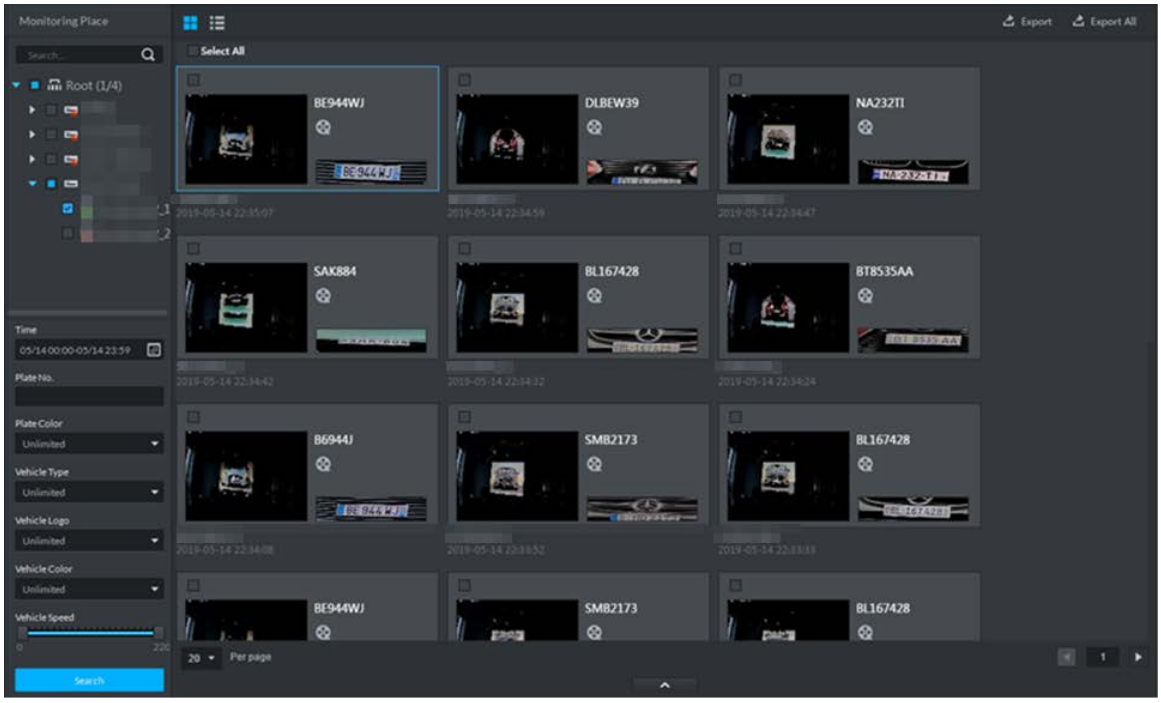
Figure 4-208 Vehicle record



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

System displays search result. See Figure 4-209.

Figure 4-209 Passed vehicle search result



For the passed vehicle, you can view its detailed information, record and running track. Refer to the operations listed below.

- Click View mode ( ) or list mode ( ), it is to select different display mode.
- Select a snapshot image and then click or double click the image. The detailed information is displayed. See Figure 4-210. Move the cursor to the middle to select the specified zone, you can zoom in it. See Figure 4-211.

Figure 4-210 Vehicle details

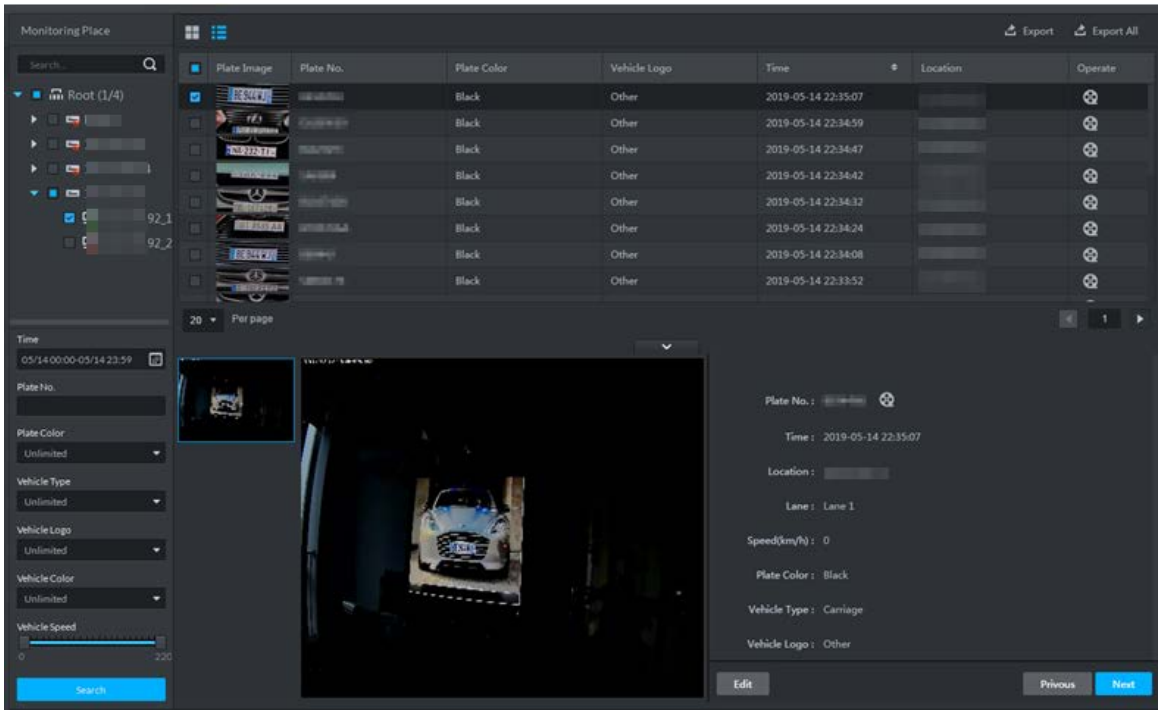
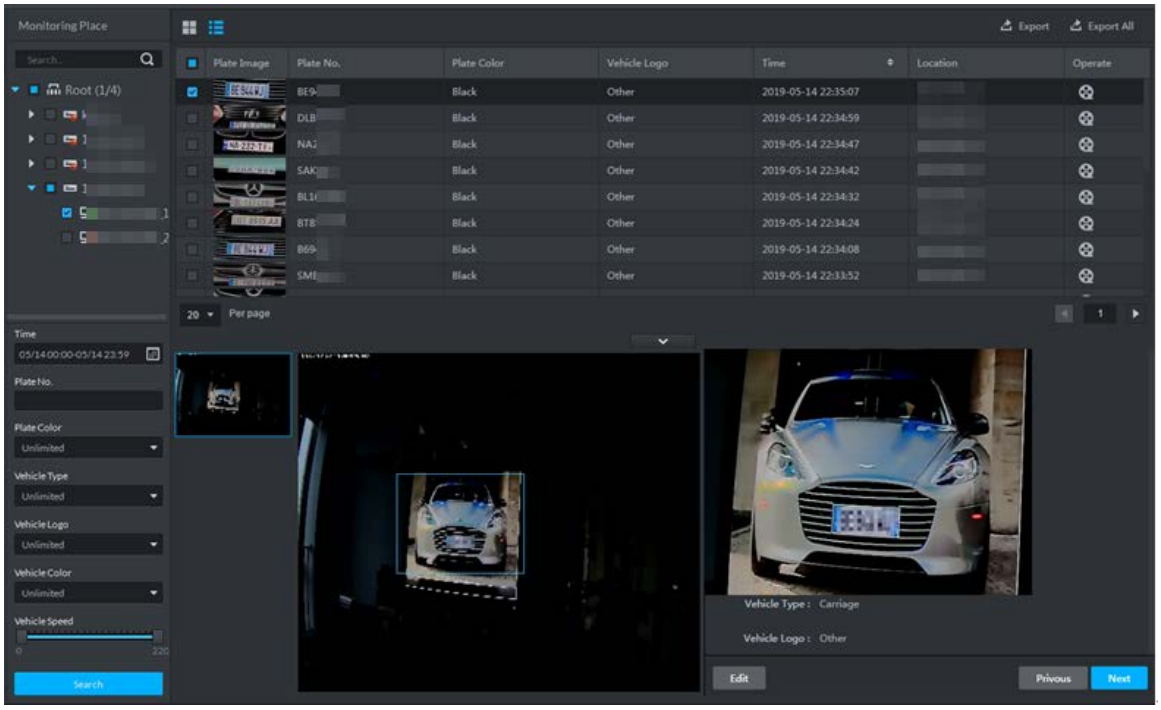
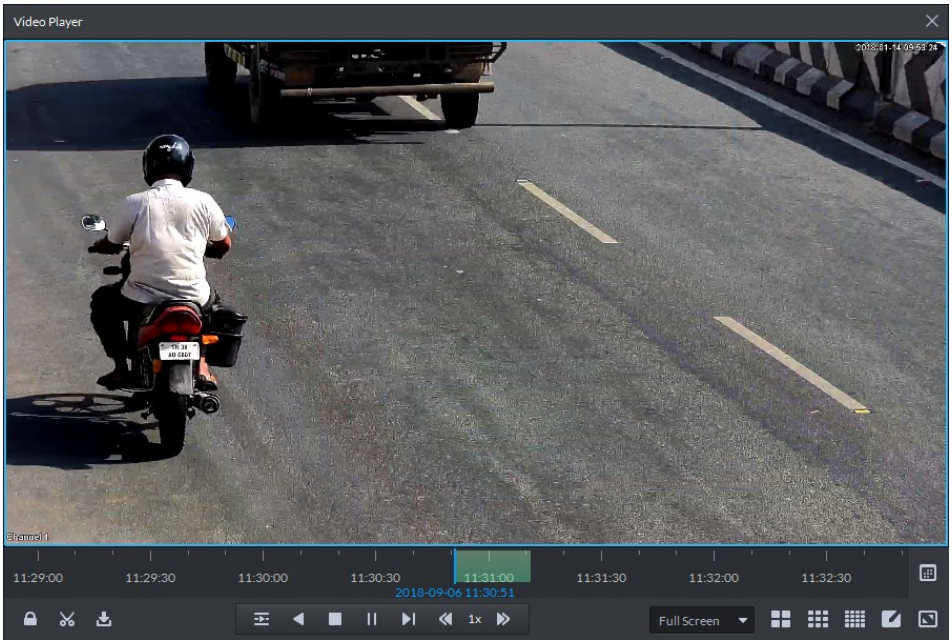


Figure 4-211 Regional zoom



- Click  to playback the 15-second video before and after the vehicle passed time. See Figure 4-212. The video file is total 30 seconds. Display the 15-second video before and after the vehicle passed.

Figure 4-212 Playback video



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

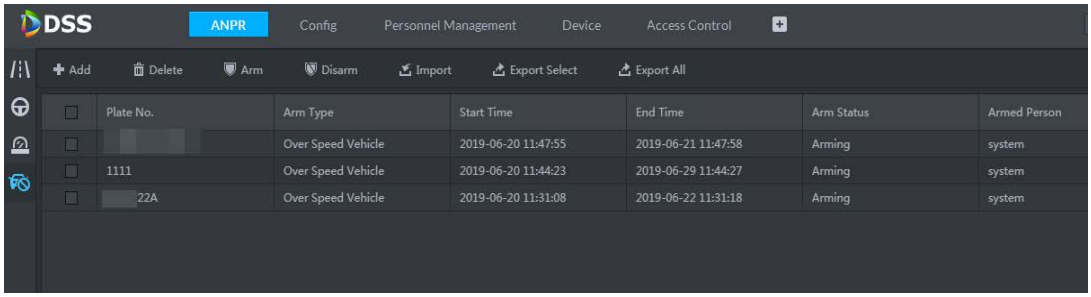
4.8.6 Blocklist Vehicle

4.8.6.1 Adding Blocklist Vehicle

Arm means monitoring vehicles, it will trigger alarm when capturing and recognizing the vehicle with designated license plate.

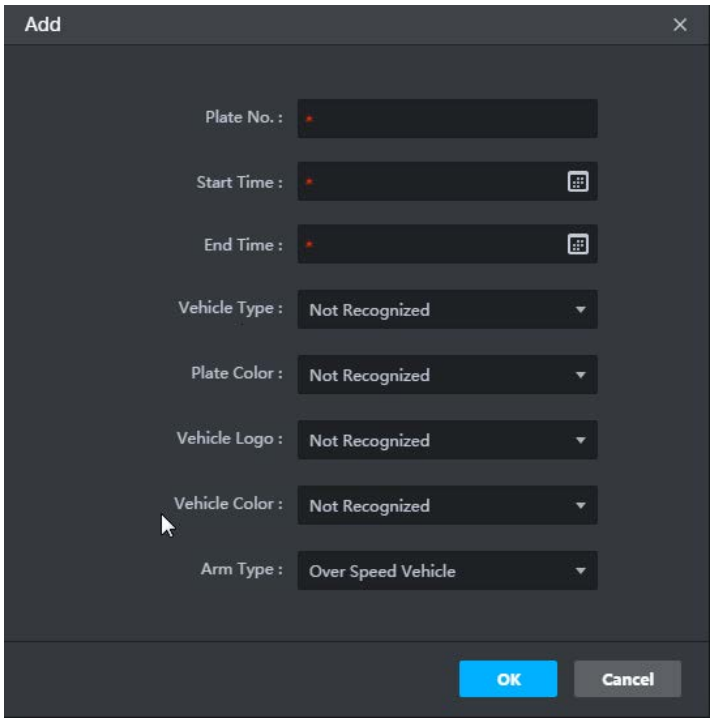
Step 1 Click  .

Figure 4-213 Vehicle blocklist



Step 2 Click **Add**.

Figure 4-214 Add a vehicle to the blocklist



Step 3 Set parameters of armed vehicle, including plate No., plate type, arm time, arm reason and arm type etc.

Step 4 Click **OK**.

The information of adding blocklist vehicle is displayed, and then it is considered as armed status by default.

Related Operations

- Export blocklist vehicle information

  Click **Export All** on the top of the interface, and then it exports all the information of blocklist vehicle according to the interface prompt, and it is saved locally; or select blocklist vehicle, it supports selecting several vehicles, click **Export Select**, and it exports the information of blocklist vehicles according to interface prompt, and then it is saved locally.

- Import Blocklist Vehicle Information

  If blocklist vehicle information is backed up or filled in according to template, then you can add blocklist vehicle quickly by importing.

  Click **Import** on the top of the interface, select the local blocklist vehicle file, click Import and blocklist vehicle information is imported. If there is no blocklist vehicle file, then you can click **Click to download template** on the import interface, download template and fill in blocklist vehicle information.

- Modify blocklist vehicle information

  Click  and modify blocklist vehicle information.

- Search blocklist vehicle Information

  Select search conditions, including time, plate No., plate type, arm status and arm type, click Search.

  It supports fuzzy search upon license plate. For example, if you enter 5, it will display all the vehicles whose license plate includes 5.

- Delete blocklist vehicle

Click  in the line of blocklist vehicle, and delete corresponding blocklist vehicle according to prompt; select blocklist vehicle, it can select several vehicles, click **Delete** on the top of the interface, and then you can delete selected blocklist vehicle according to prompt.

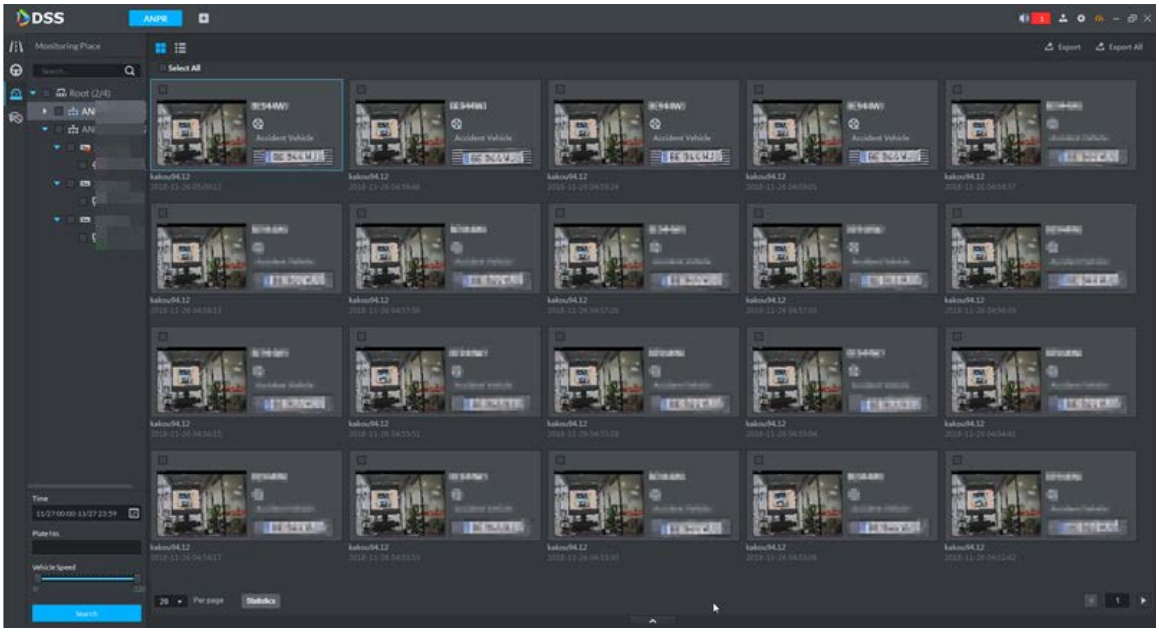
4.8.6.2 Arming Blocklist Vehicle

- On the interface of **Vehicle Blocklist**, click  in the line of blocklist vehicle, the icon becomes  and arming is enabled; select one or several blocklist vehicles, click **Arm** on the top of the interface, then the icon becomes  , arming is enabled.
- On the interface of **Vehicle Blocklist**, click  in the line of blocklist vehicle, the icon becomes  and arming is cancelled; select one or several blocklist vehicles, click **Disarm** on the top of the interface, then the icon becomes  , arming is cancelled.

4.8.6.3 Searching Arm Record

Step 1 On the interface of **Vehicle Blocklist**, click  .

Figure 4-215 Arming records



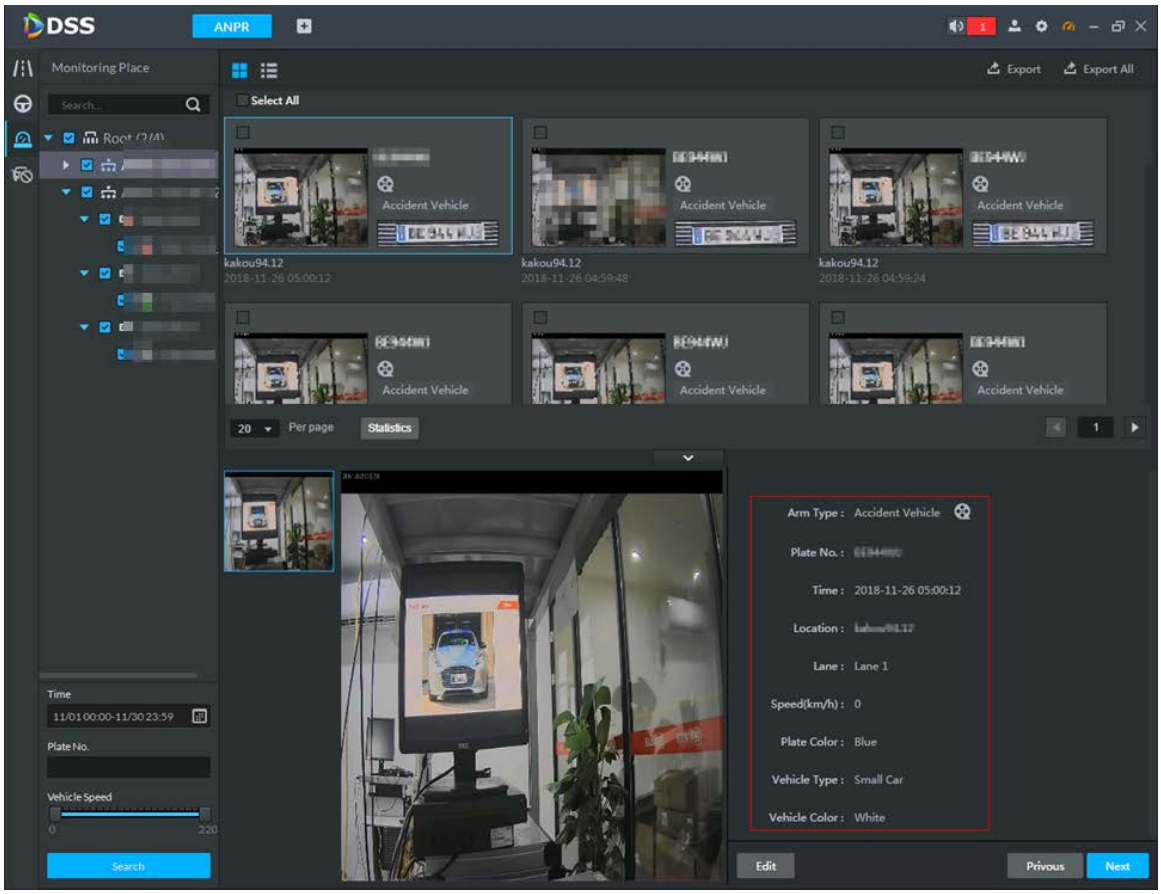
Step 2 Set search conditons, including time, plate No., and speed.

Step 3 Click **Search**.

The search result is displayed. Click and view by thumbnail; click and view by list.

Step 4 Double click the picture and you can view details, including viewing vehicle picture by regional zoom, plate No., snapshot time, snapshot location, lane, speed, plate color, vehicle type, logo, vehicle color.

Figure 4-216 ANPR



If there is any error for the vehicle information, you can click **Edit** and modify manually. You can modify plate No., plate color, vehicle type, logo and vehicle color. Click **Save** after modfification is finished and click **Cancel** to cancel modification.

Figure 4-217 Edit the information of a vehicle (1)

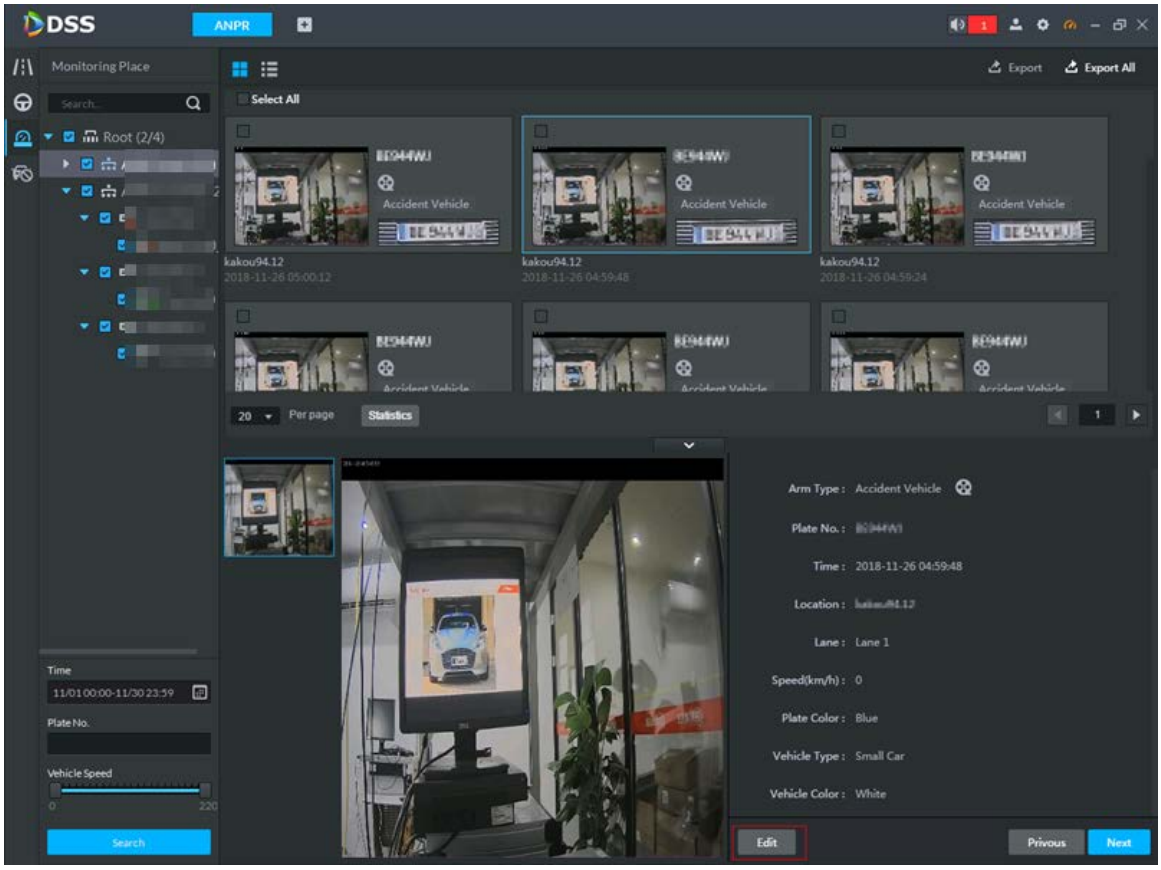
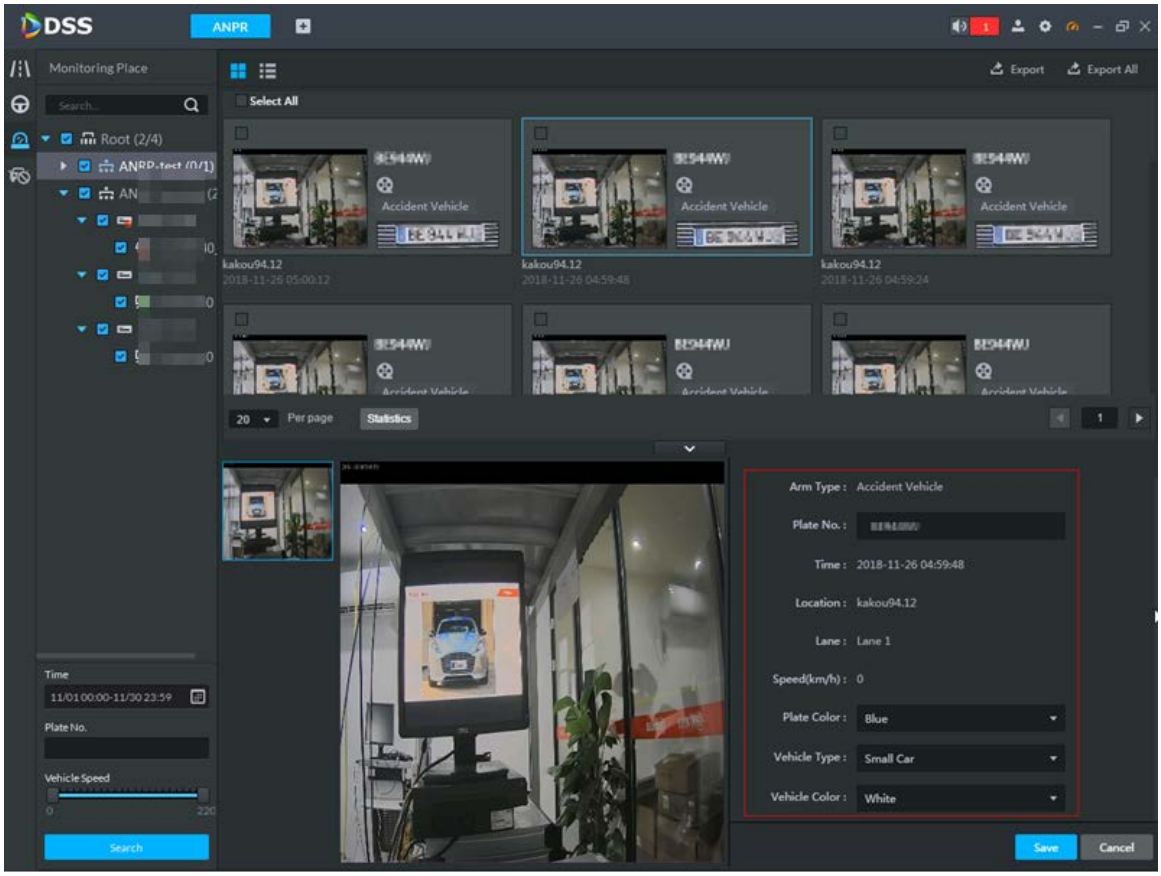


Figure 4-218 Edit the information of a vehicle (2)

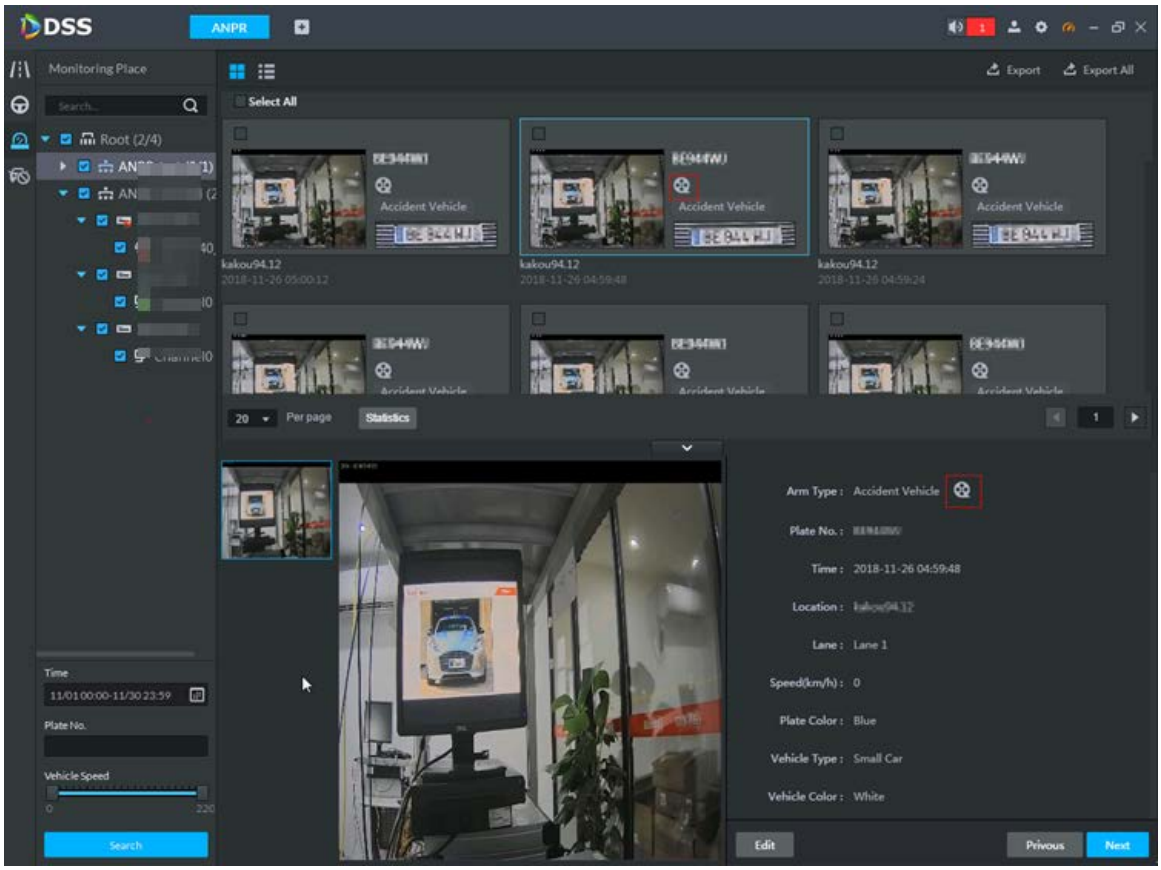


4.8.6.4 Viewing Related Video of Arm Record

You need to configure ANPR channel with general record plan before searching vehicle video, the config method of record plan is the same as that of video channel.

Select corresponding arming record from the result, click or click from the details, and view the captured video of both front and back scenarios.

Figure 4-219 View linked video

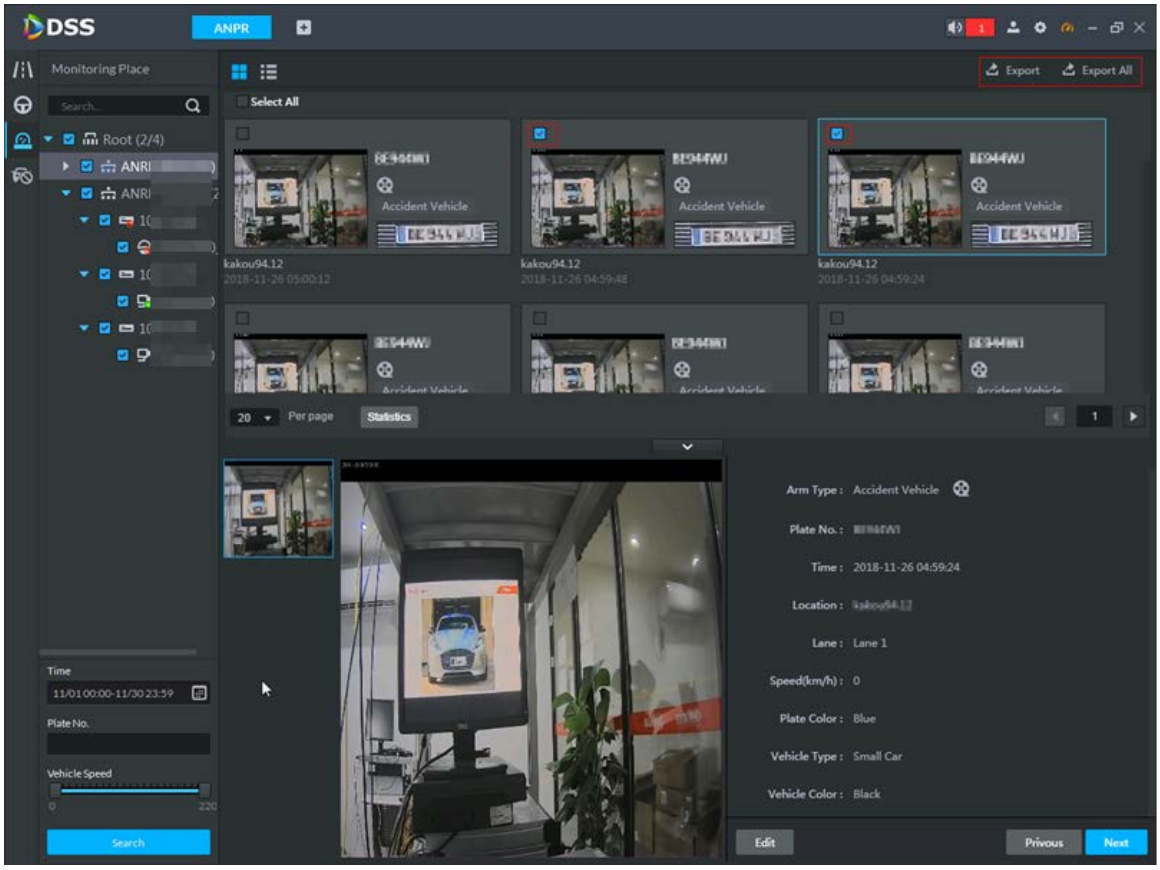


4.8.6.5 Exporting Arm Record

Users can export all or some selected vehicle records according to actual requirement.

Step 1 Select the records which need to be exported from the searched results, click **Export** or **Export All**.

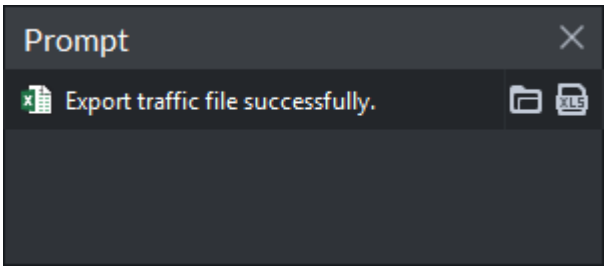
Figure 4-220 Export records



Step 2 Select save path according to the system prompt.

The system will pop up prompt box after it is exported successfully.

Figure 4-221 Prompt message

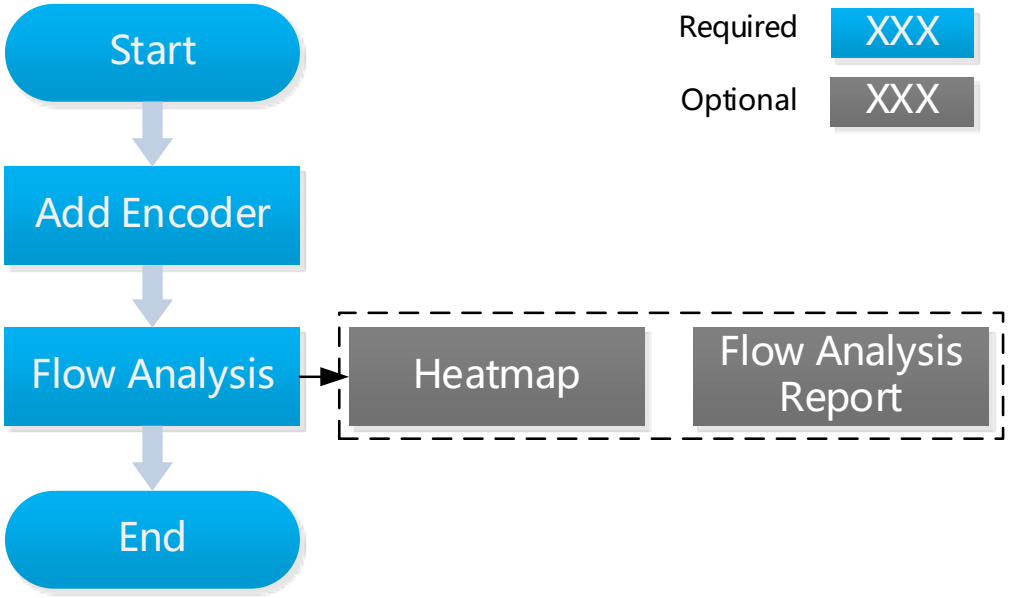


Step 3 Click the open button in the prompt message to view the report.

4.9 Flow Analysis

After adding steoreo vision flow analysis camera to platform, the platform supports searching flow analysis report and heat map. The operation of flow analysis is shown in Figure 4-222.

Figure 4-222 Flow analysis



4.9.1 Adding Encoder

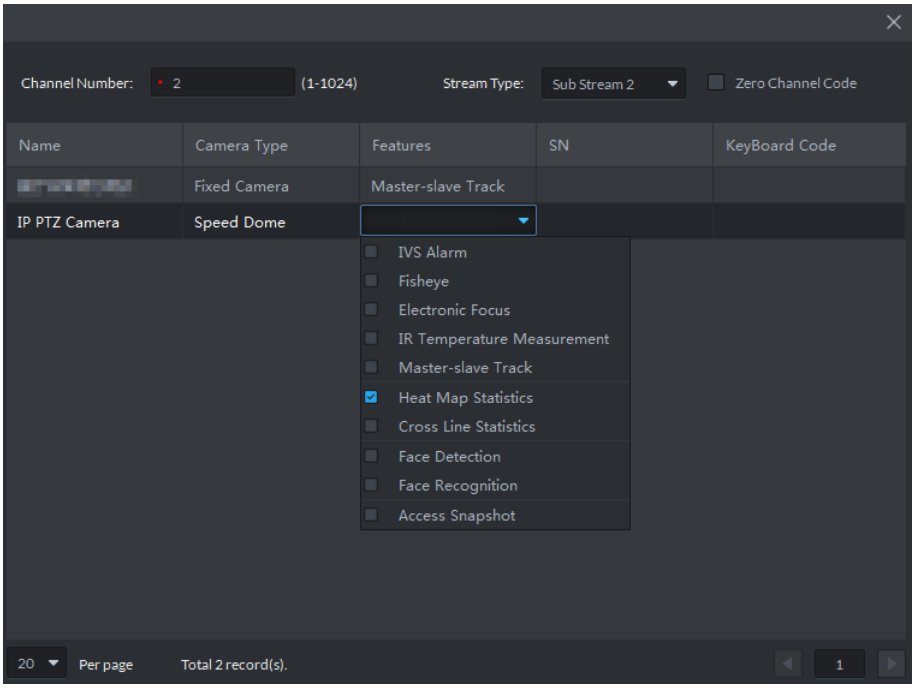
The platform only displays results reported by camera. Please make sure the added steoreo vision camera already enables people counting function. For detailed operation, please refer to device user manual.

Step 1 Add steoreo vision camera. For detailed operation, see"4.1.2.4 Adding Device."

Step 2 Modify device feature.

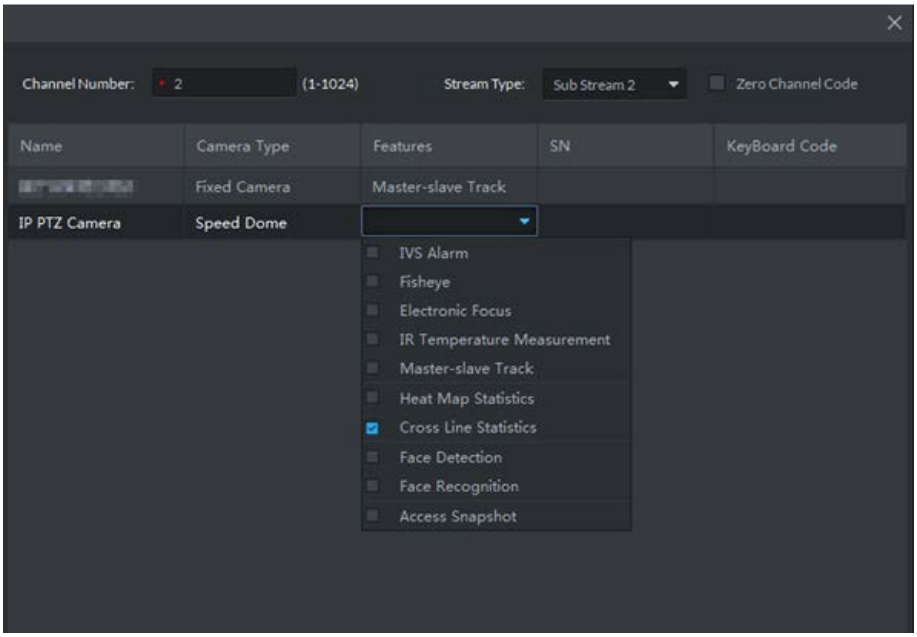
- To enable heatmap function, click on **Device** interface and modify device **Features** as **Heatmap Statistics**. See Figure 4-223.

Figure 4-223 Modify feature (heatmap)



- To enable people counting function, click on **Device** interface and modify device **Features** as **Cross Line Statistics**. See Figure 4-224.

Figure 4-224 Modify features (Cross line statistics)



4.9.2 Flow Analysis Application

4.9.2.1 Heatmap

Present distribution of moving objects according to color.

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

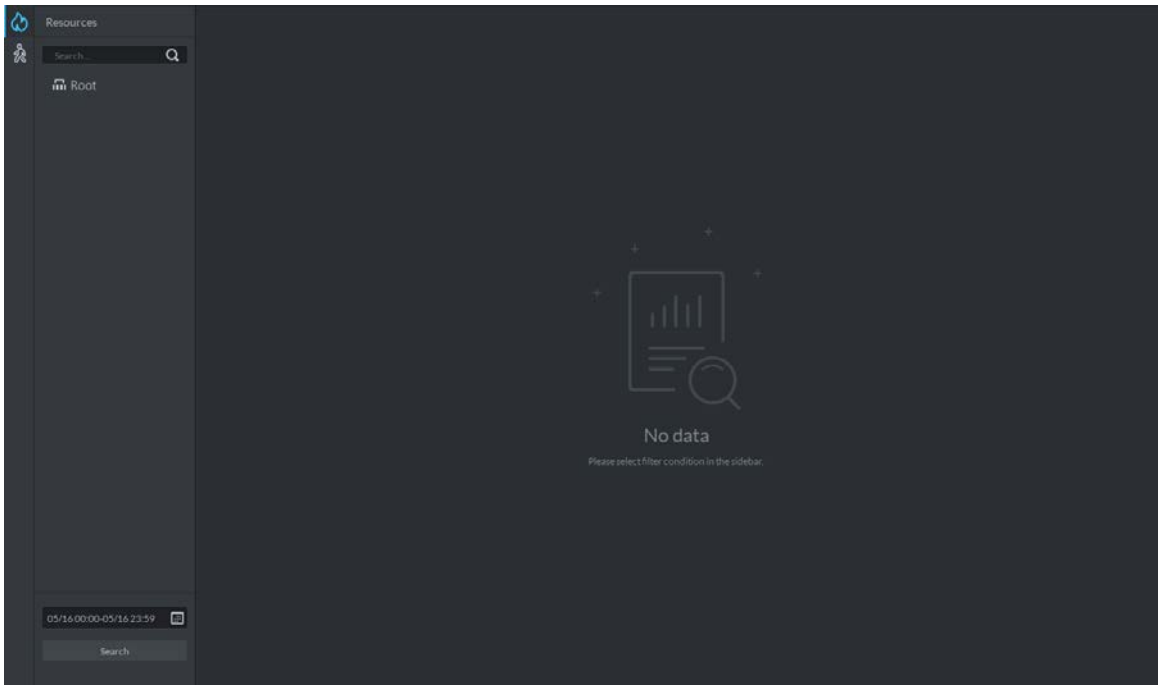
Step 1 On client homepage, click **Flow Analysis**.

The **Flow Analysis** interface is displayed.

Step 2 Click .

The **Heatmap** interface is displayed. See Figure 4-225.

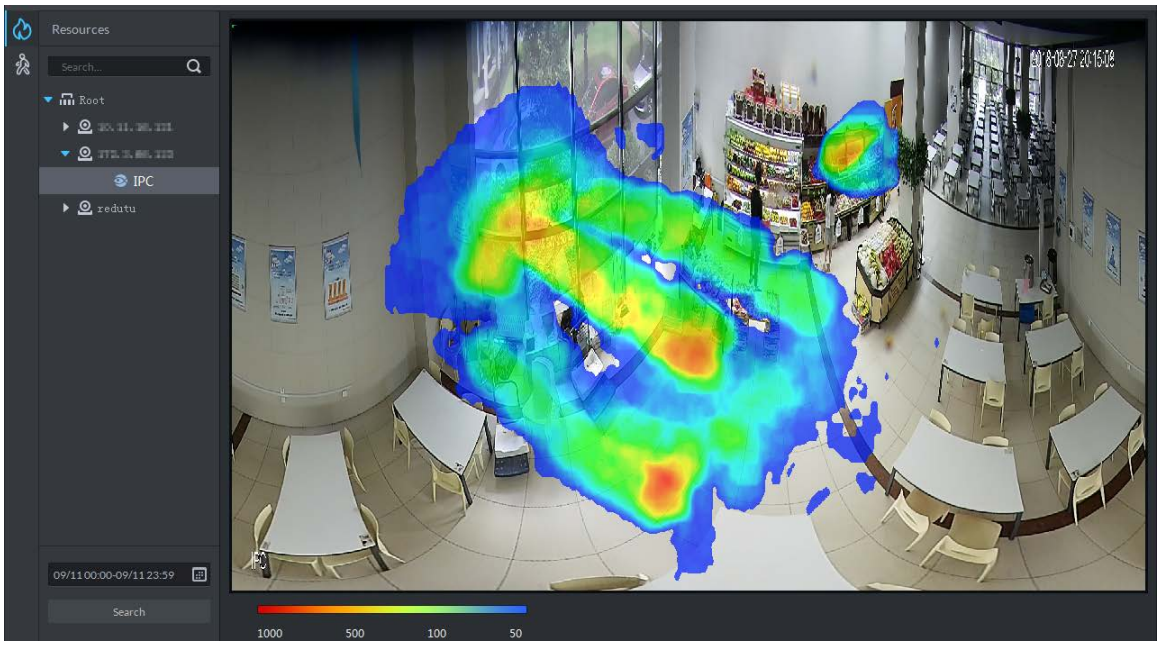
Figure 4-225 Heatmap



Step 3 Select the channel that displays heatmap, select time and click **Search**.

The heatmap is displayed. See Figure 4-226.

Figure 4-226 Heatmap search result



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

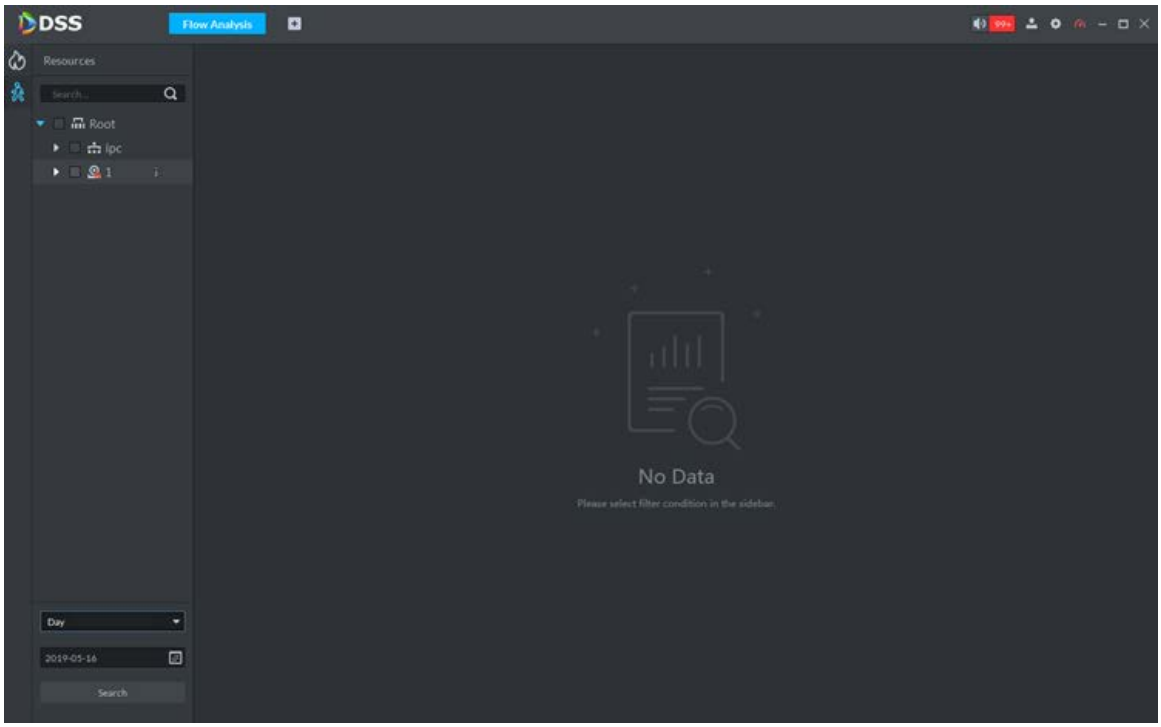
4.9.2.2 Flow Analysis Report

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

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

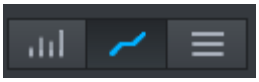
The **Flow Analysis** interface is displayed. See Figure 4-227.

Figure 4-227 Flow analysis



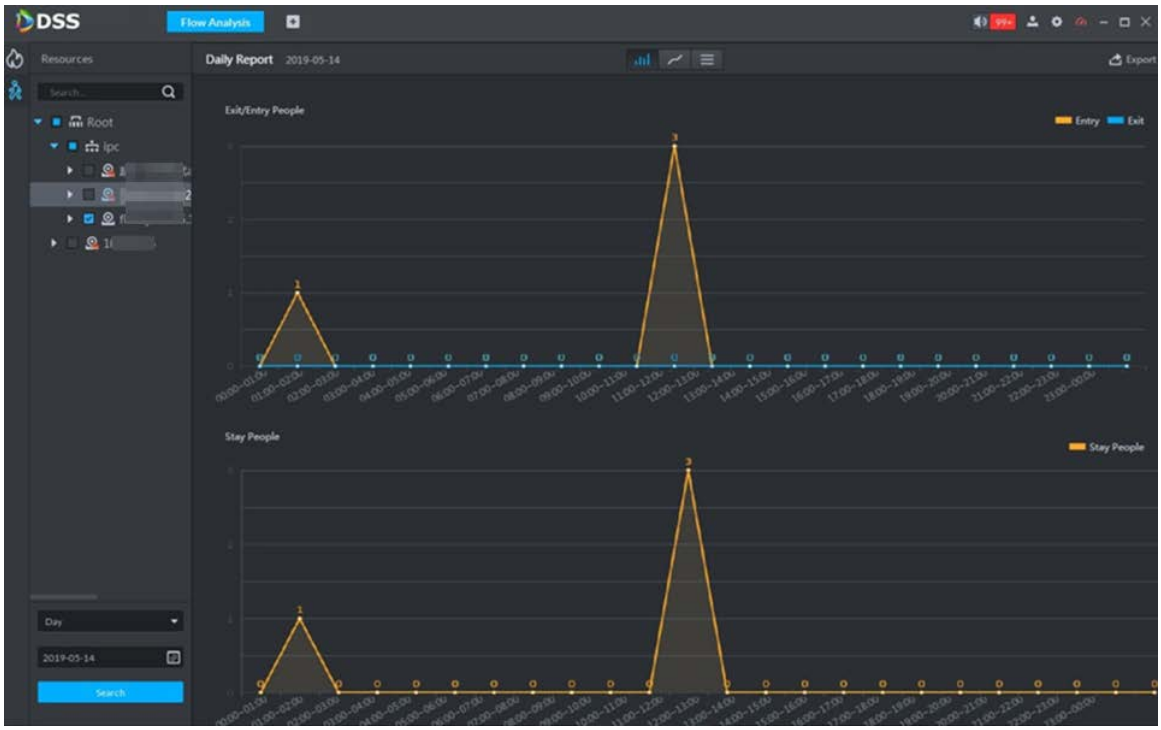
Step 2 Select device channel, search period and statistics time, and click **Search**.

The system generates report. See Figure 4-228.

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

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

Figure 4-228 Search result

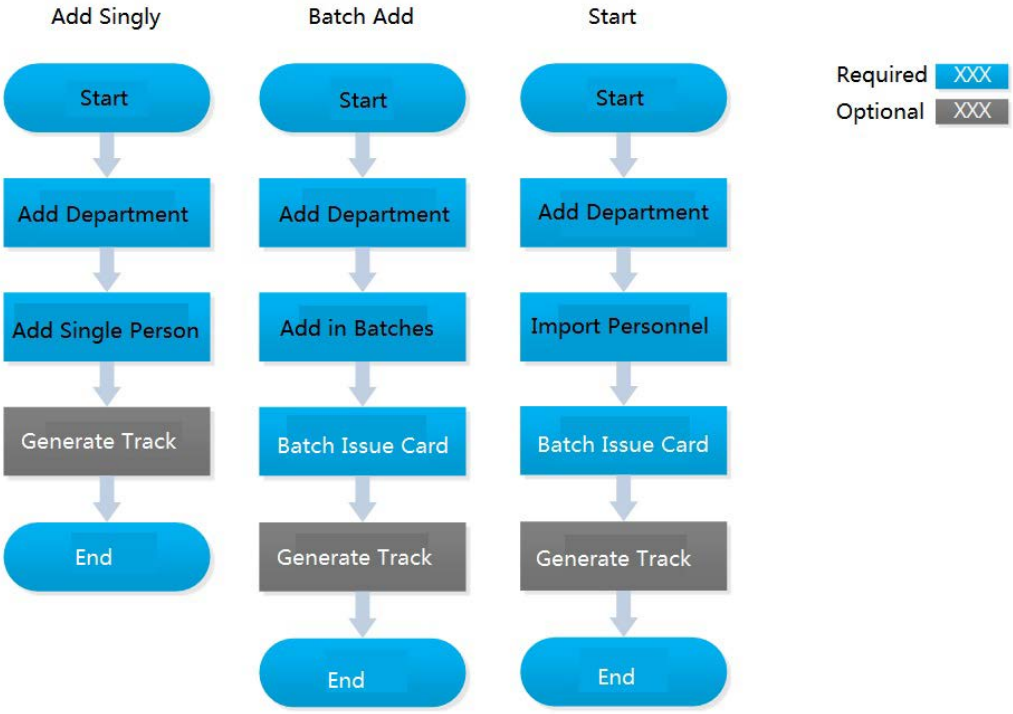


Step 3 Click **Export** on upper right corner of interface, save report to local in pdf according to prompt on interface.

4.10 Personnel Management

Personnel include those of access control amanament, attendance and video intercom. They have the authorization to unlock doors with password, fingerprint, card, or face recognition. Operation flow is shown in Figure 4-229.

Figure 4-229 Personnel management flow



4.10.1 Adding Department

Adding department is to manage personnel in the added departments.

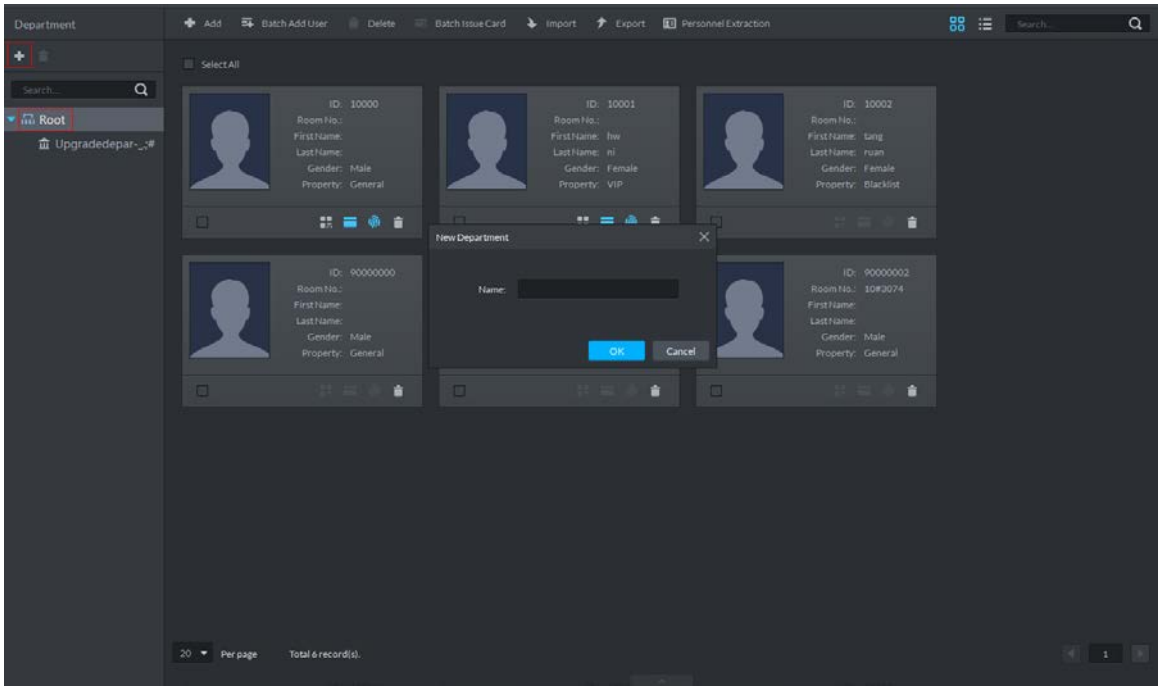
Step 1 Click . On the **Homepage** interface, select **Personnel Management**.

The **Personnel Management** interface is displayed.

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

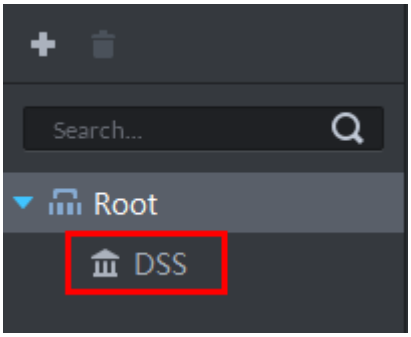
The **New Department** interface is displayed. See Figure 4-230. The new department is directly under the selected node.

Figure 4-230 New department



Step 3 Input the department name and click **OK**.
The newly added department is displayed.

Figure 4-231 New department



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.

4.10.2 Adding Personnel

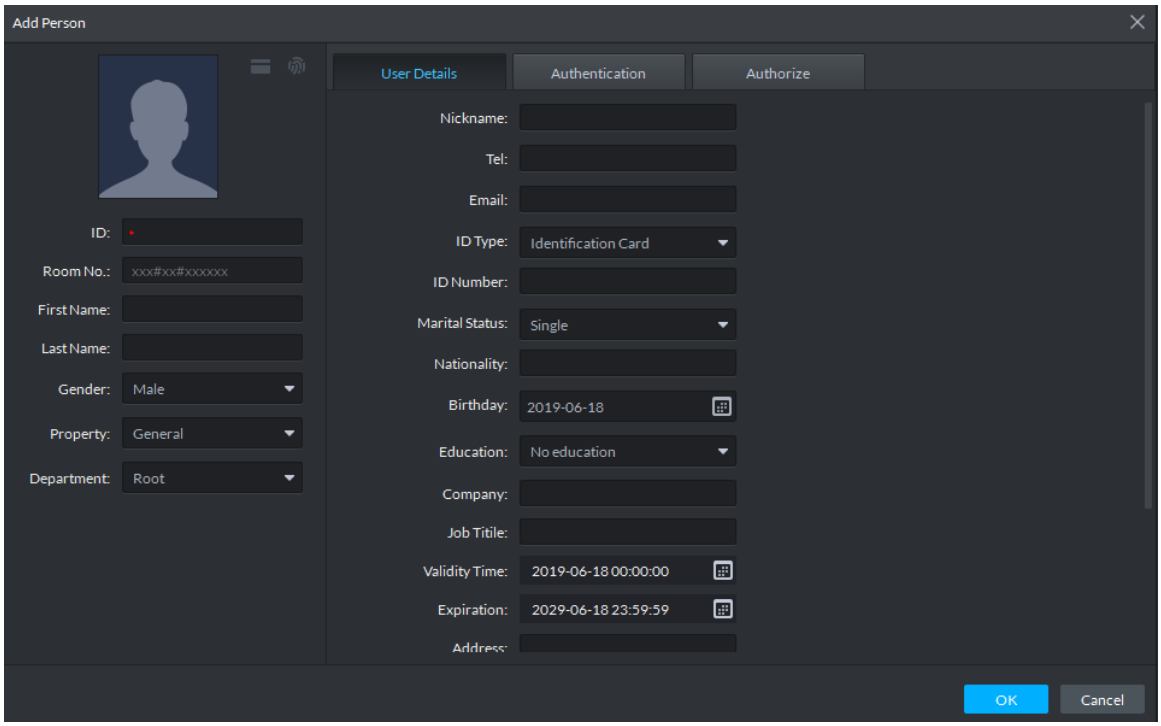
Add personnel and authorize them to unlock doors. When adding personnel, system uploads the collected personnel information to the server for proper protection.

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

4.10.2.1 Adding Person One by One

Step 1 On the **Personnel Management** interface, click **Add**.
The **Add Person** interface is displayed. See Figure 4-232.

Figure 4-232 Add personnel



Step 2 Configure personnel details.

1) Move the mouse to the picture section, click **Upload**. Follow the instructions on the interface to upload a picture. If the PC comes with a camera, click **Snapshot** to take a face snapshot and upload it.
2) Fill in personnel information as necessary.

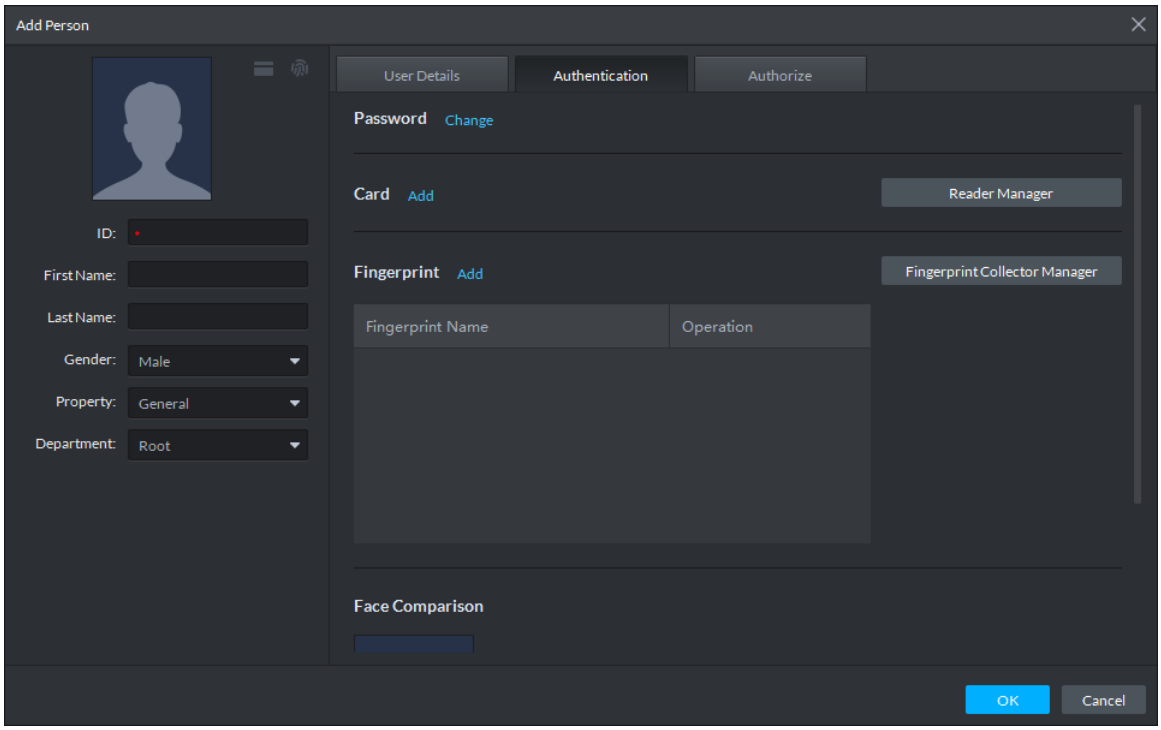
Table 4-34 Personnel detail description

Parameter	Description
ID	Required, used to recognize personnel, each ID number is unique.
Room No.	The same as the VTH SIP number. If VTH SIP number is 1#2#1001#0, the room number is 1#2#1001.
Property	Set person as different types. If the person is the first card unlock, then person property is set as **General**.
Householder	If the added personnel belong to the same household, then you can set one person as householder, you can issue contacts and householder info under video intercom.
Admin	Personnel divided into general and admin. Admin has the permission to operate device interface. The parameter takes effect only when personnel info issued to 2nd generation access control.

Step 3 Click the **Authentication** tab.

The **Authentication** interface is displayed. See Figure 4-233.

Figure 4-233 Authentication

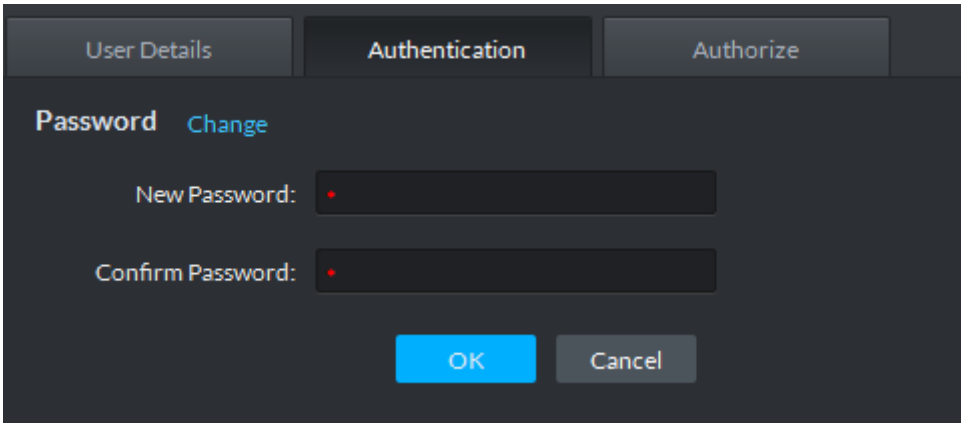


Step 4 Set a password.

1) Click **Change**.

The password setting interface is displayed. See Figure 4-234.

Figure 4-234 Set password



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

Step 5 Issue cards to personnel.

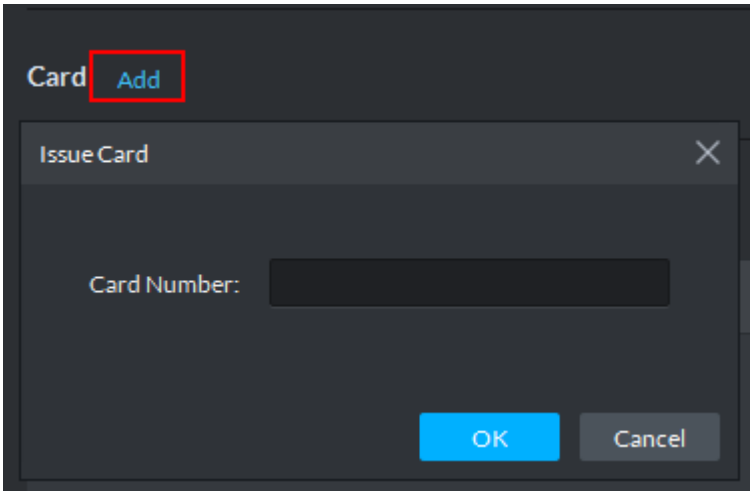
The system supports issuing card by entering card No. manully and card reader.

- Issue card by entering card No. manully

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

The **Issue Card** interface is displayed. See Figure 4-235.

Figure 4-235 Add card



2) Enter personnel card number and click **OK** to save the card added. See Figure 4-236. For more details, refer to Table 4-35.

Figure 4-236 Card added

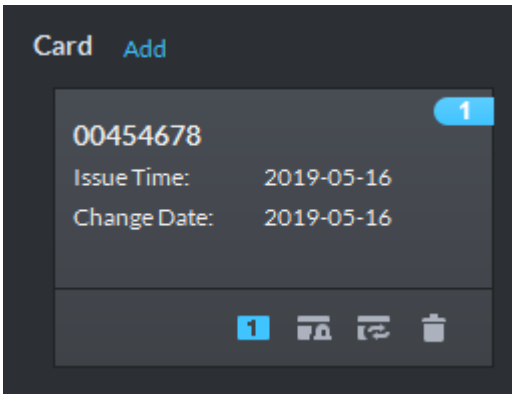


Table 4-35 Card operation

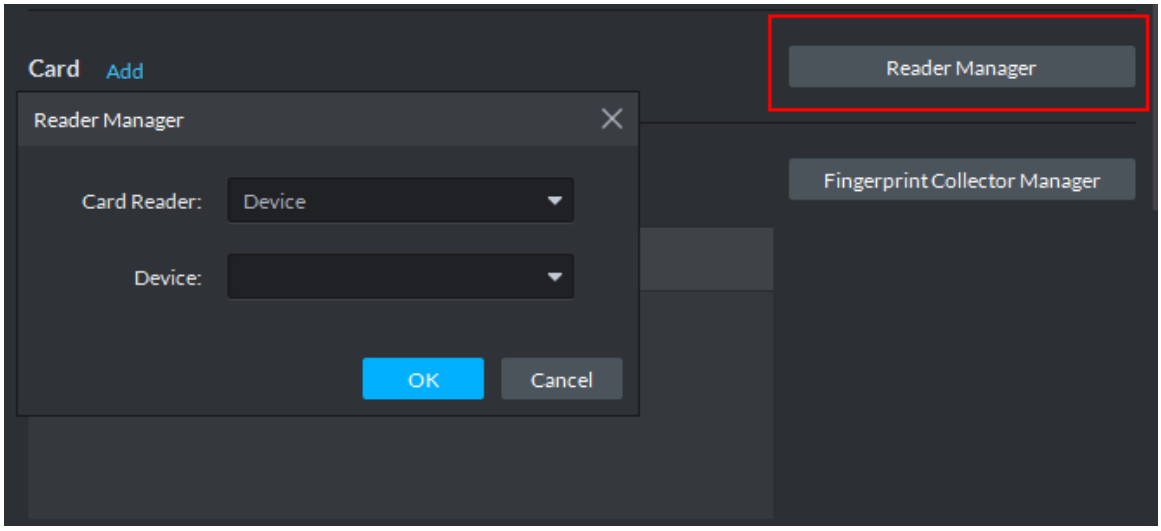
Icon	Description
1	If a person has several cards, only the main card can be issued to 1st generation access control device. The first added card is considered as main card by default. Click the icon and it becomes 1, and then 1 is displayed on upper right corner of the interface, which means that the card is set as main card. Click 1 to cancel main card setting.
	Set the card as duress card, after that use the card to unlock, then duress alarm is generated. After clicking the icon, it becomes , is displayed on upper right corner of the interface, which means that the card is set as duress card. Click to cancel duress card setting.
	Card cannot be used if it is damaged, so you can change a new card.
	Delete card info, after that the card has no unlock permission.

- Issue card by card reader.

1) Click **Reader Manager**.

The **Reader Manager** interface is displayed.

Figure 4-237 Reader manager



2) Select from **Card Reader** or **Device**, and click **OK**.

3) Swipe the card on the card reader or device.

Complete issuing cards.

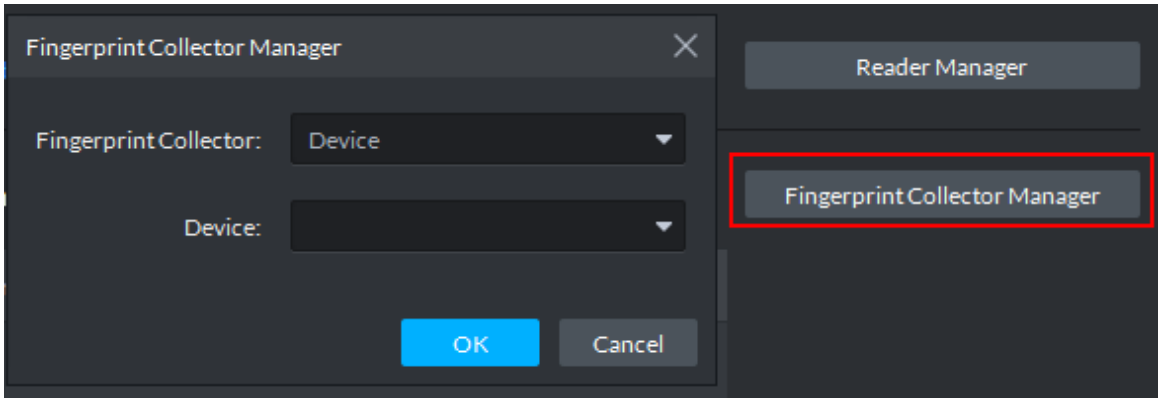
Step 6 Collect fingerprint.

When the system is connected to access control, unlocks by fingerprint, you need to collect personnel fingerprint. Each person can collect max 10 fingerprints.

1) Click **Fingerprint Collector Manager**.

The **Fingerprint Collector Manager** interface is displayed. See Figure 4-238.

Figure 4-238 Fingerprint collector manager

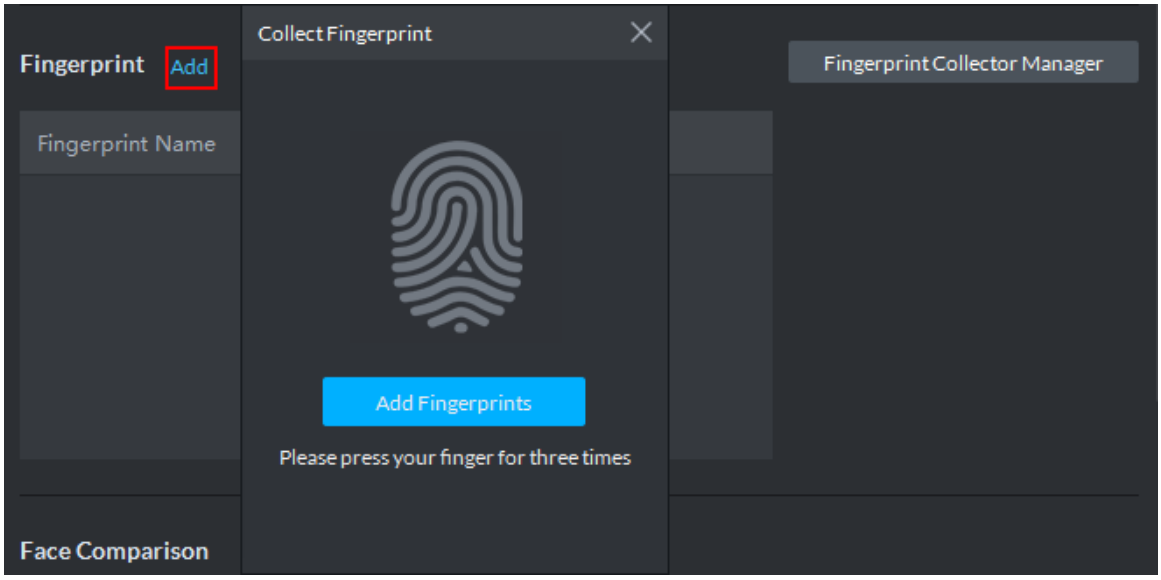


2) Select from **Fingerprint Collector** and click **OK**.

3) Click **Add**.

The **Collect Fingerprint** interface is displayed. See Figure 4-239.

Figure 4-239 Collect fingerprint



4) Click **Add Fingerprints**.
The **Collect Fingerprint** interface is displayed. See Figure 4-240.

Figure 4-240 Collect fingerprint

5) Records fingerprint on the reader by raising and then laying down the finger upon hearing the beep sound. Repeat this for three times. See Figure 4-241. Fingerprint collection is completed. See Figure 4-242. For more details, see Table 4-36.

Figure 4-241 Collecting fingerprint

Figure 4-242 Fingerprint collection completed

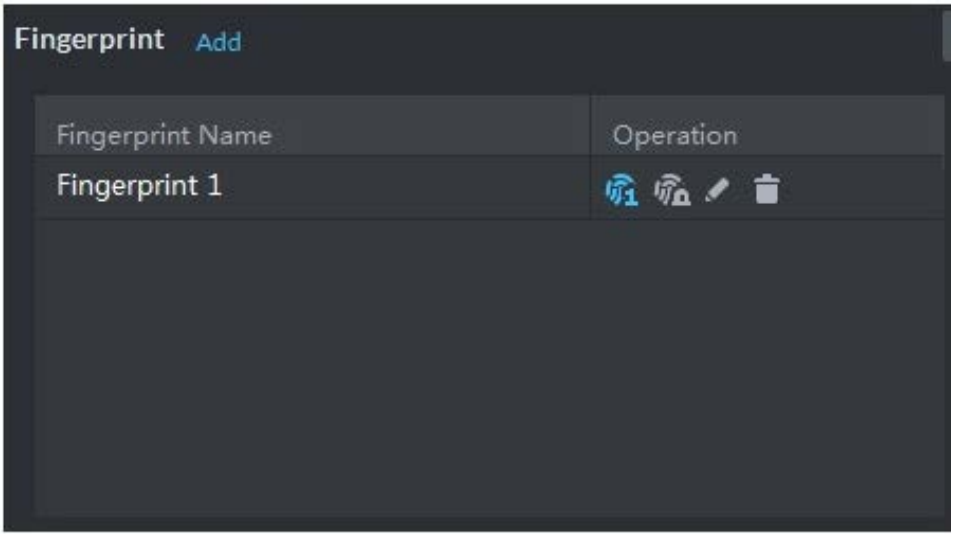


Table 4-36 Fingerprint operation

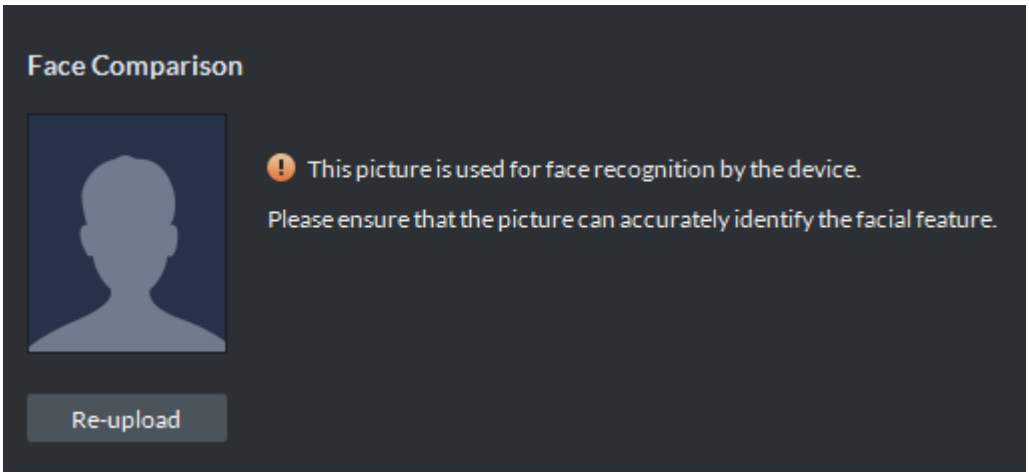
Icon	Description
	If more than 3 fingerprints are imported, then only then main fingerprint can be issued to access control device. The latest three fingerprints are considered as main fingerprint by default. One person cam set max three main fingerprints. After clicking the icon, it becomes , which means that the fingerprint is set as main fingerprint. Click and cancel main fingerprint setting.
	Set fingerprint as duress fingerprint, after that you can unlock the door by the fingerprint and generate duress alarm. Click the icon, it becomes , which means the fingerprint is set as duress fingerprint. Click and cancel duress fingerprint setting.
	Modify fingerprint name.
	Delete fingerprint, after that the fingerprint has no permission to unlock door.

Step 7 Upload pictures for face recognition.

Click **Add**, and select picture to upload according to system prompt. See Figure 4-243.

- If the picture is wrong, or need to be replaced. Click Re-upload and upload new picture.
- Move the mouse to uploaded picture, shows up on the picture, click the icon and delete the uploaded picture.

Figure 4-243 Face picture upload



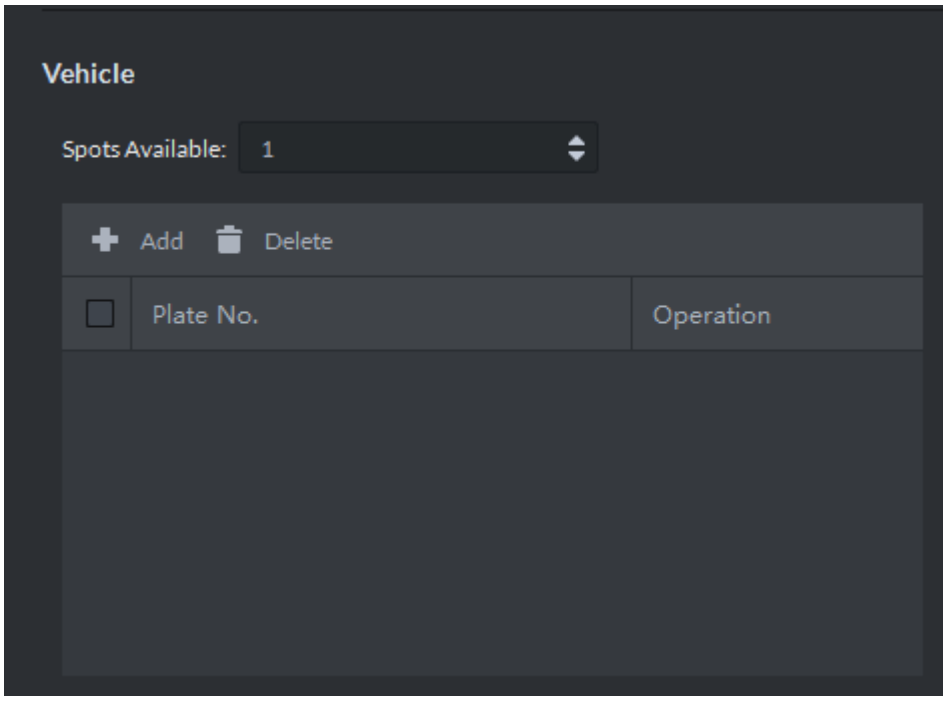
Step 8 Add vehicle info.

Added vehicle info is synced to entrance module, used as recognition info for vehicle entrance and exit.

Set the available spots for personnel, click **Add**, set plate No. and see Figure 4-244. If the person has several cars, then you need to add vehicle plate No. one by one.

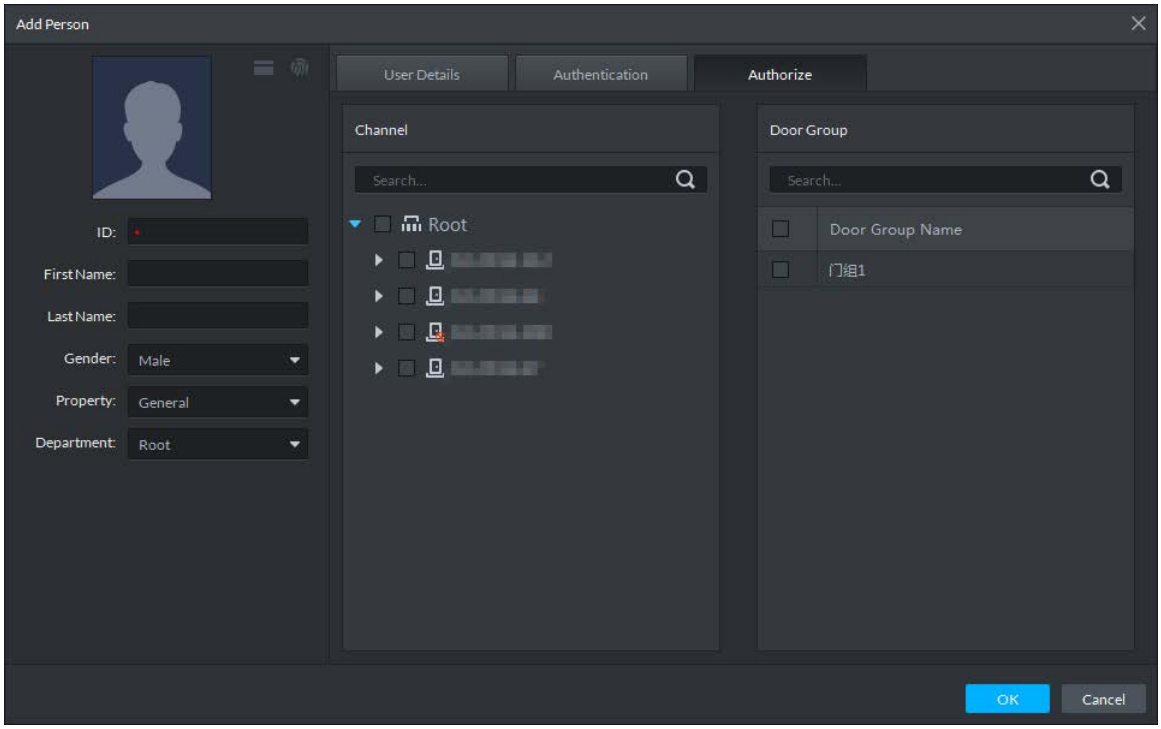
If the number of added vehicles is more than available spots, then the number of entered vehicles cannot exceed the number of available spots which has been set.

Figure 4-244 Add vehicle info



Step 9 Click **Authorize** and select the channels to which the authorized users can have access. See Figure 4-245.

Figure 4-245 Authorize

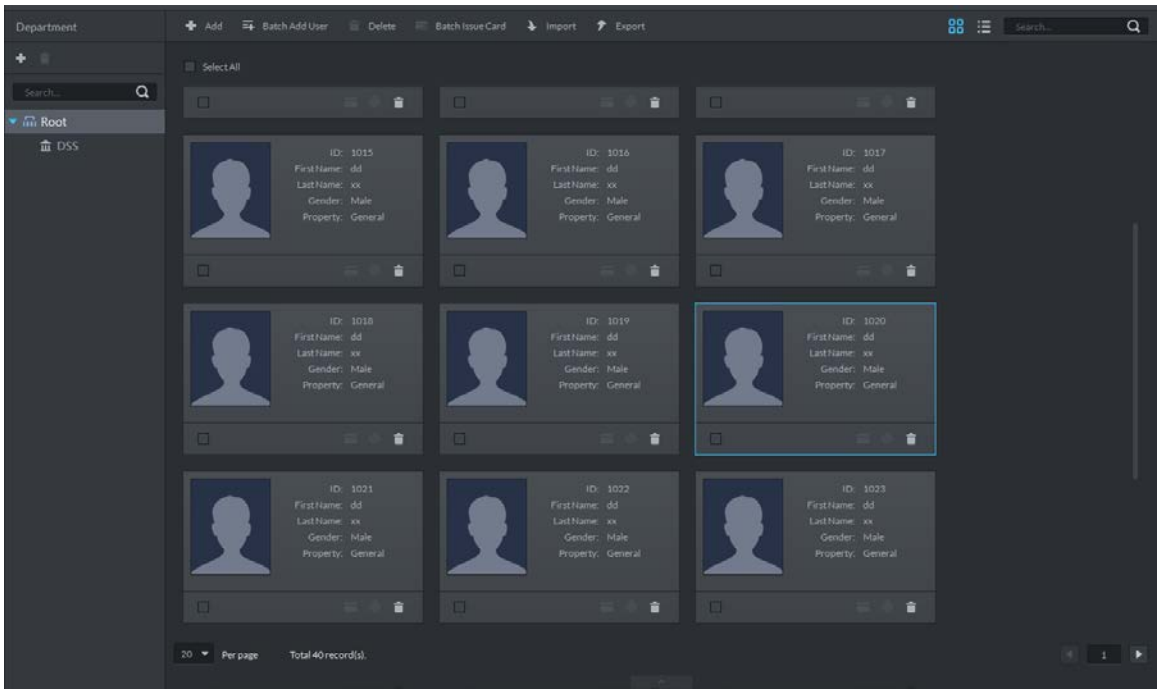


Step 10 Click **OK**.

For the information of the added personnel, see Figure 4-246. 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 4-246 Personnel list



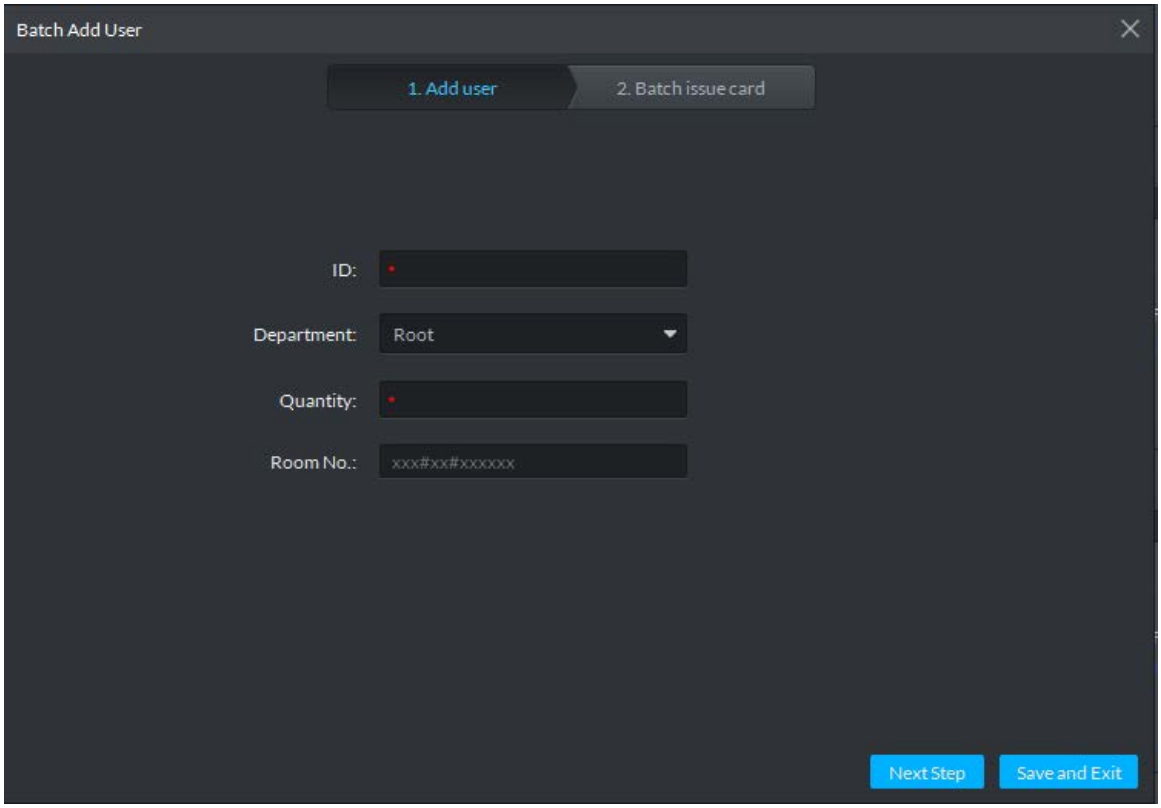
4.10.2.2 Adding Personnel in Batch

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 4-247.

Figure 4-247 Batch add user



Step 2 Configure personnel info. See Table 4-37.

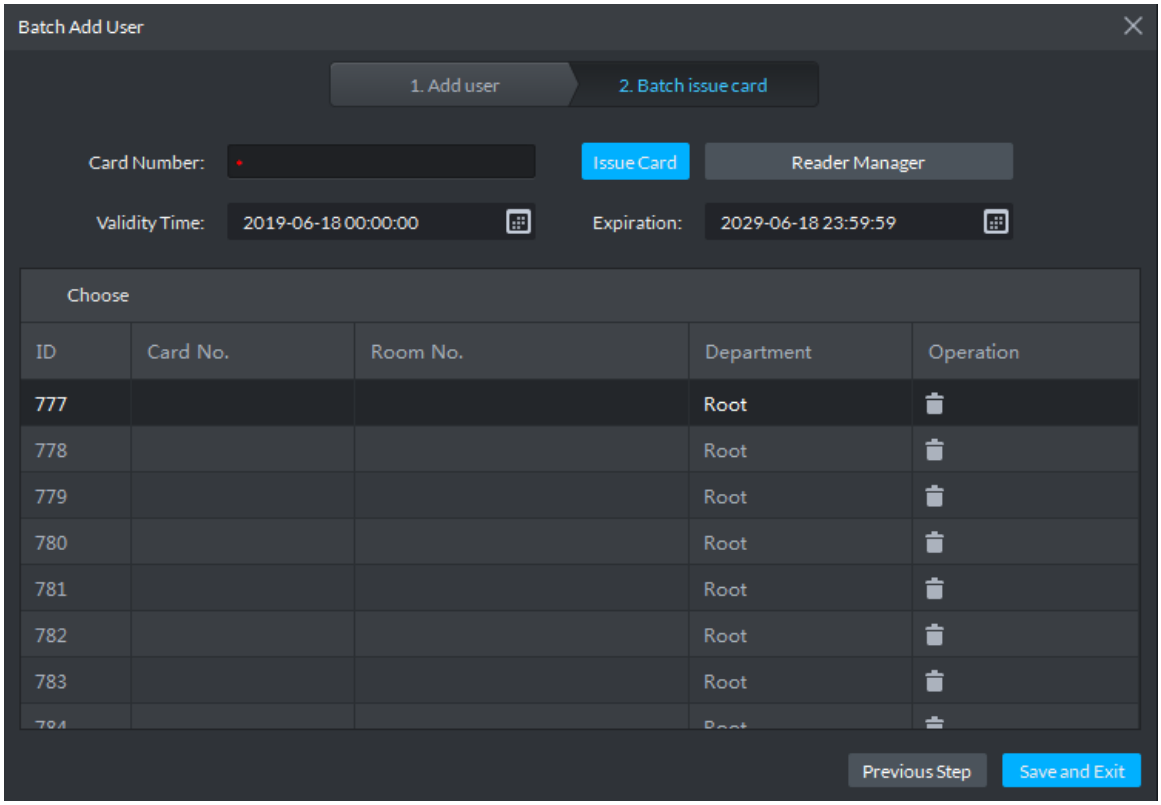
Table 4-37 Personnel info

Parameter	Description
ID	ID is unique for each person.
Quantity	The number of added persons
Room No.	The same as the VTH SIP number. If VTH SIP number is 1#2#1001#0, the room number is 1#2#1001.
Property	Set person as different types. If the person is the first card unlock, then person property is set as **General**.

Step 3 Click Next Step.

The interface of **Batch Add User** displays. See Figure 4-248.

Figure 4-248 Batch Add User



Step 4 Issue cards to personnel.

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

- Issue card by entering card No. manually

1) Select person, input card number and set affective time and expiration time.
2) Click **Issue Card**.
3) Repeat the operation until all cards are issued.
4) Click **Save and Exit**.

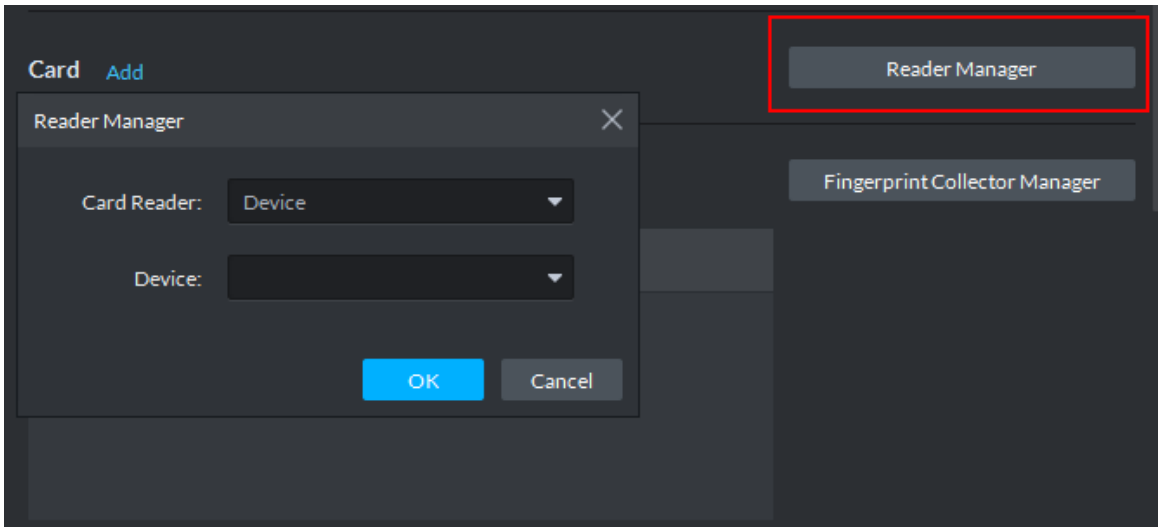
   The interface of personnel info displays.

- Issue card by card reader

1) Click **Reader Manager**.

   The **Reader Manager** interface is displayed. See Figure 4-249.

Figure 4-249 Reader manager

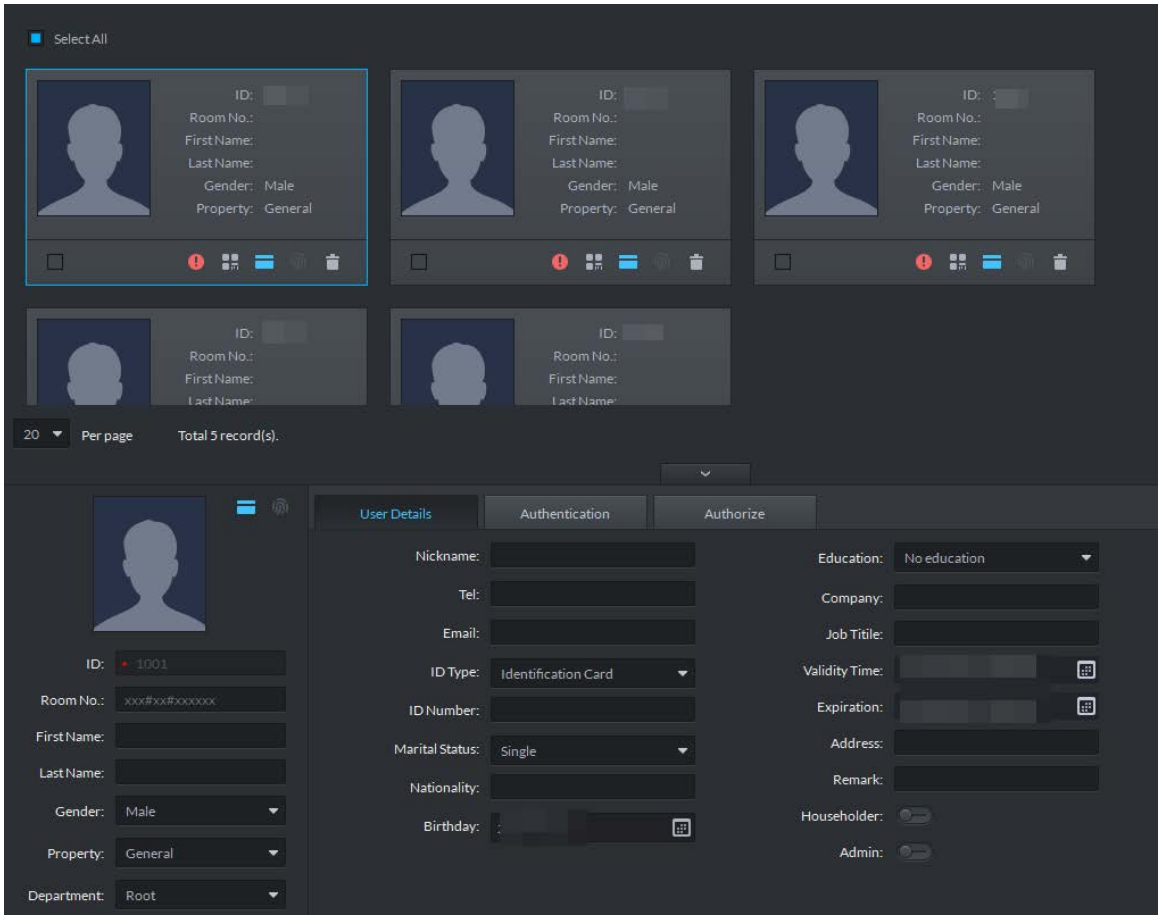


2) Select from **Card Reader** or **Device**, and click **OK**.
3) Swipe the card on the card reader or device.
4) Select person and set effective time and expiration time. Click **Issue Card**.
5) Repeat the operation to complete issuing cards to all personnel.
6) Click **Save and Exit**.

Step 5 Double-click personnel or click  to edit personnel info.

Support editing personnel info, setting password, collecting fingerprint and face pictures and access control permission authentication. The info will take effect on finishing editing. See Figure 4-250.

Figure 4-250 Editing personnel info



4.10.3 Editing Personnel

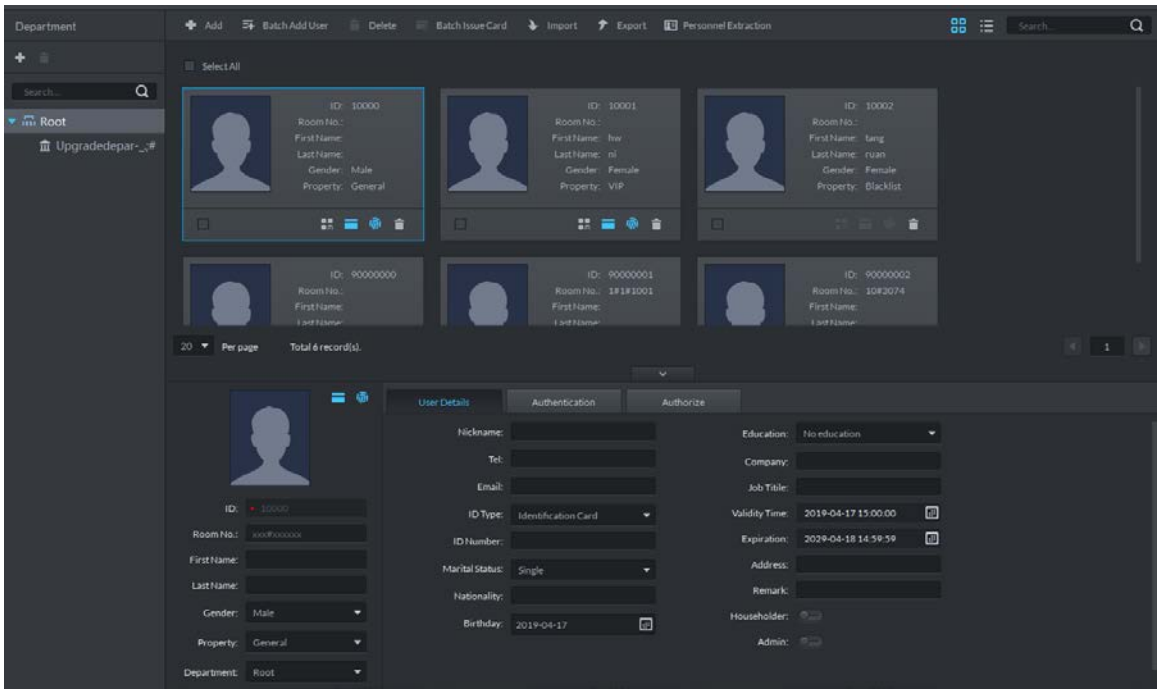
You can modify information of added person like user details, authentication and authorize except ID.

- If system adopts IR face attendance, you have to edit personnel and extract face feature code of person with same ID from IR face attendance device.
- If you want to read or import fingerprint, card or face feature from fingerprint collector, reader or IR face access control, please make sure the device is connected.

Step 1 On **Personnel Management** interface, double-click person, or select the person and click  .

The interface of **Editing Personnel Info** is displayed. See Figure 4-251.

Figure 4-251 Edit personnel



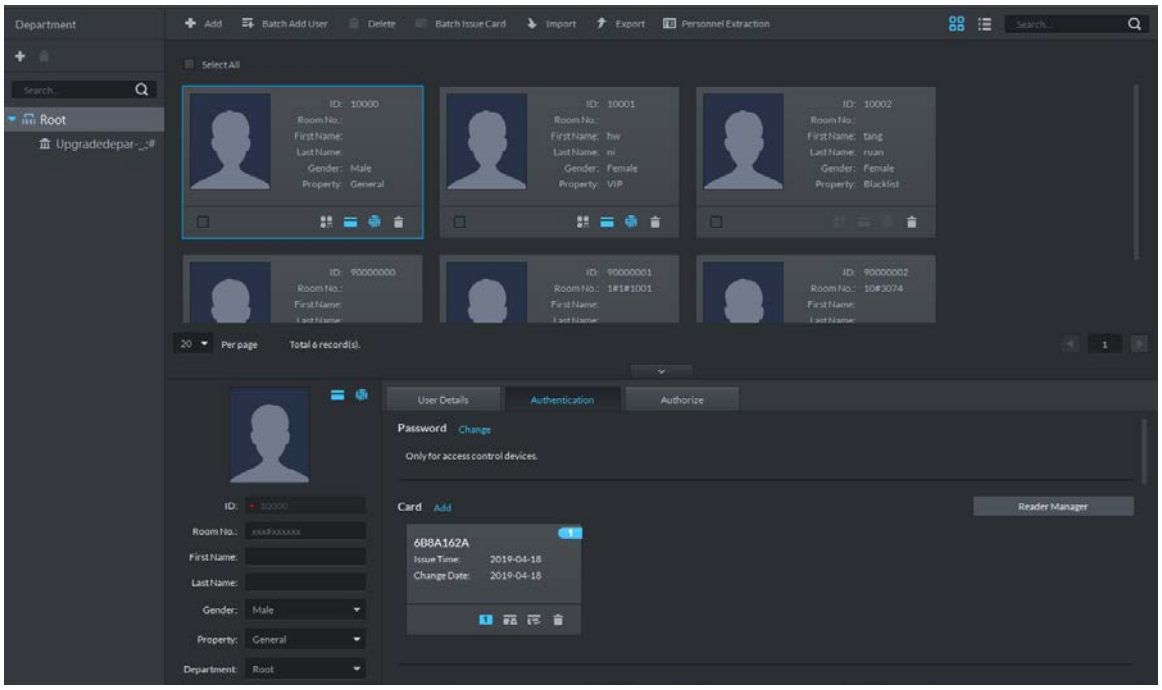
Step 2 Modify personnel info and details except ID.

If the person is the first card unlock, then you need to set person property as **General**.

Step 3 Click Authentication tab.

The **Authentication** interface is displayed. See Figure 4-252.

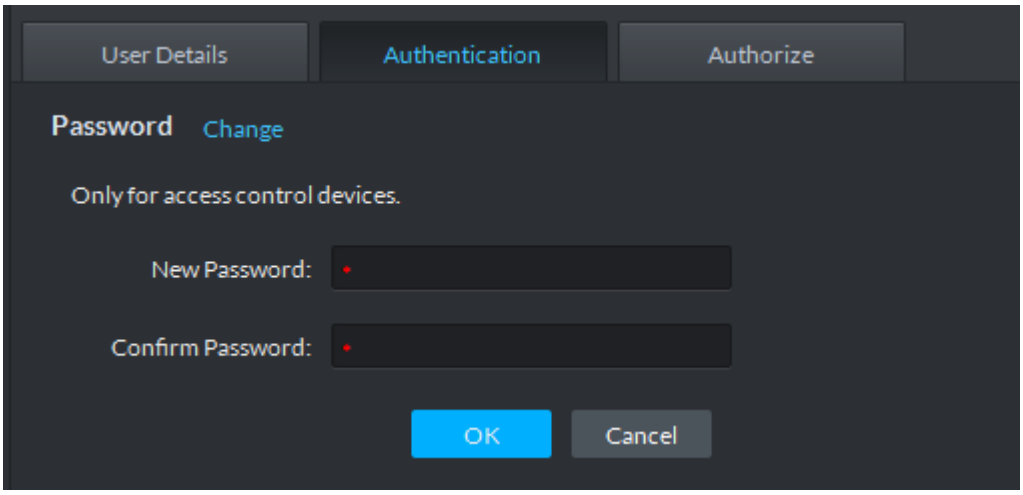
Figure 4-252 Authentication



Step 4 Click **Change**, you can set new password according to prompt, click **OK**. See Figure 4-253.

When the system is connected to access control, use password to unlock door, you need to set password.

Figure 4-253 Set password



Step 5 Manage card info.

After door card is added, and you can modify card. For more details, see Figure 4-254 and Table 4-38.

Figure 4-254 Add card

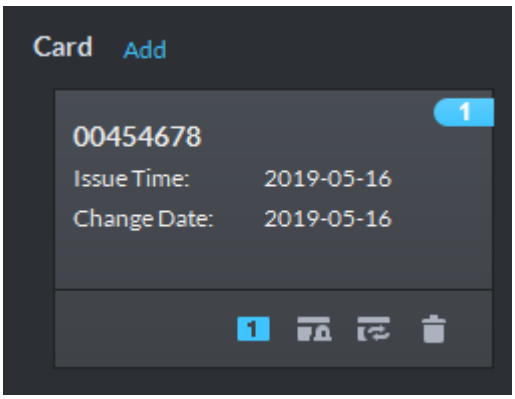


Table 4-38 Card operation

Icon	Description
	If a person has several cards, only the main card can be issued to 1st generation access control device. The first added card is considered as main card by default. Click the icon and it becomes  , and then  is displayed on upper right corner of the interface, which means that the card is set as main card. Click  to cancel main card setting.
	Set the card as duress card, after that use the card to unlock, then duress alarm is generated. After clicking the icon, it becomes  ,  is displayed on upper right corner of the interface, which means that the card is set as duress card. Click  to cancel duress card setting.
	Card cannot be used if it is damaged, so you can change a new card.
	Delete card info, after that the card has no unlock permission.

Step 6 Manage fingerprint.

Personnel fingerprint is collected, and you can modify status and name. For more details, see Figure 4-255.

Figure 4-255 Fingerprint collected

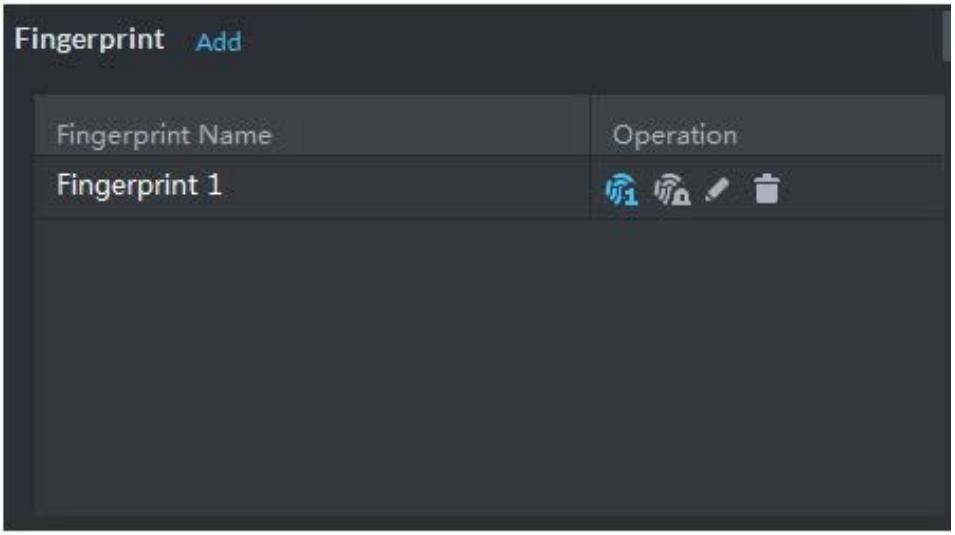


Table 4-39 Fingerprint operation

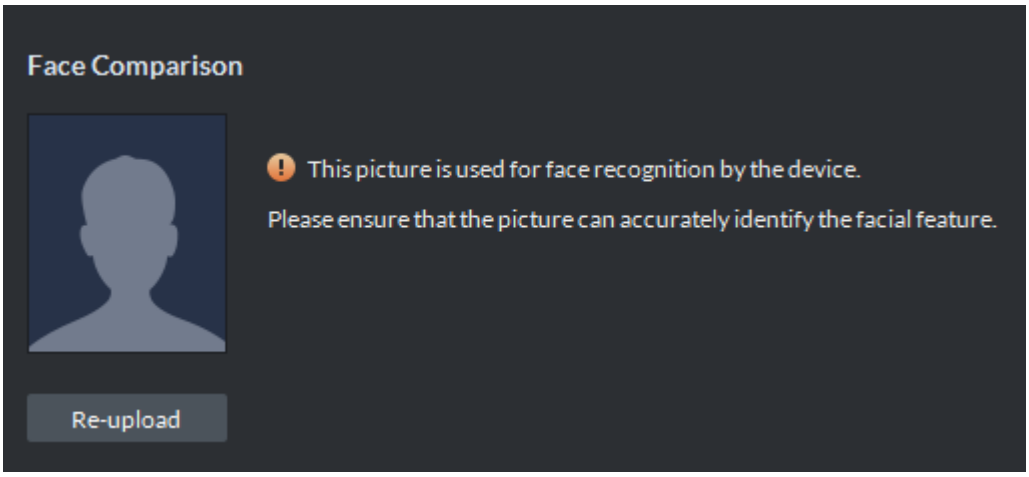
Icon	Description
	If more than 3 fingerprints are imported, then only then main fingerprint can be issued to access control device. The latest three fingerprints are considered as main fingerprint by default. One person can set max three main fingerprints. After clicking the icon, it becomes , which means that the fingerprint is set as main fingerprint. Click and cancel main fingerprint setting.
	Set fingerprint as duress fingerprint, after that you can unlock the door by the fingerprint and generate duress alarm. Click the icon, it becomes , which means the fingerprint is set as duress fingerprint. Click and cancel duress fingerprint setting.
	Modify fingerprint name.
	Delete fingerprint, after that the fingerprint has no permission to unlock door.

Step 7 Update face recognition picture.

Click **Re-upload** and upload new face picture according to system prompt.

Move the mouse to uploaded picture, shows up on the picture, click the icon and delete the uploaded picture.

Figure 4-256 Upload face picture

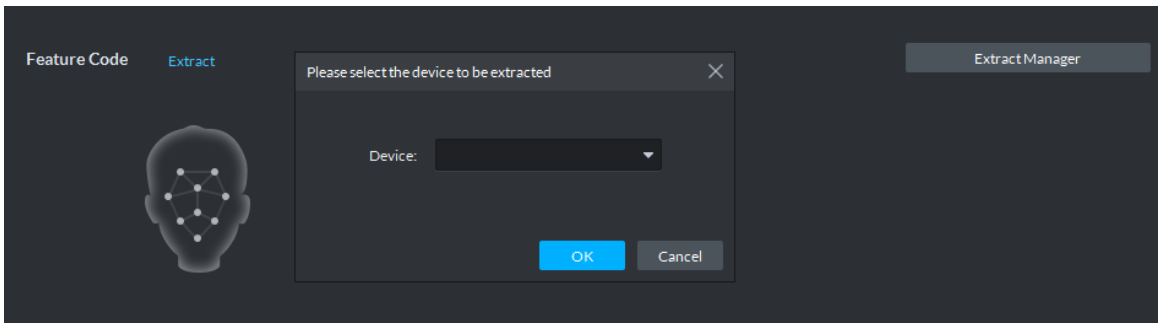


Step 8 Extract IR face feature code.

1) Click **Extract Manager**.

The interface of **Please select the device to be extracted** is displayed**.** See Figure 4-257.

Figure 4-257 Extract IR face feature code



2) Select IR face device, click **OK**.

3) Click **Extract**.

The system extracts IR face feature code from device, and prompts that extracted successfully.

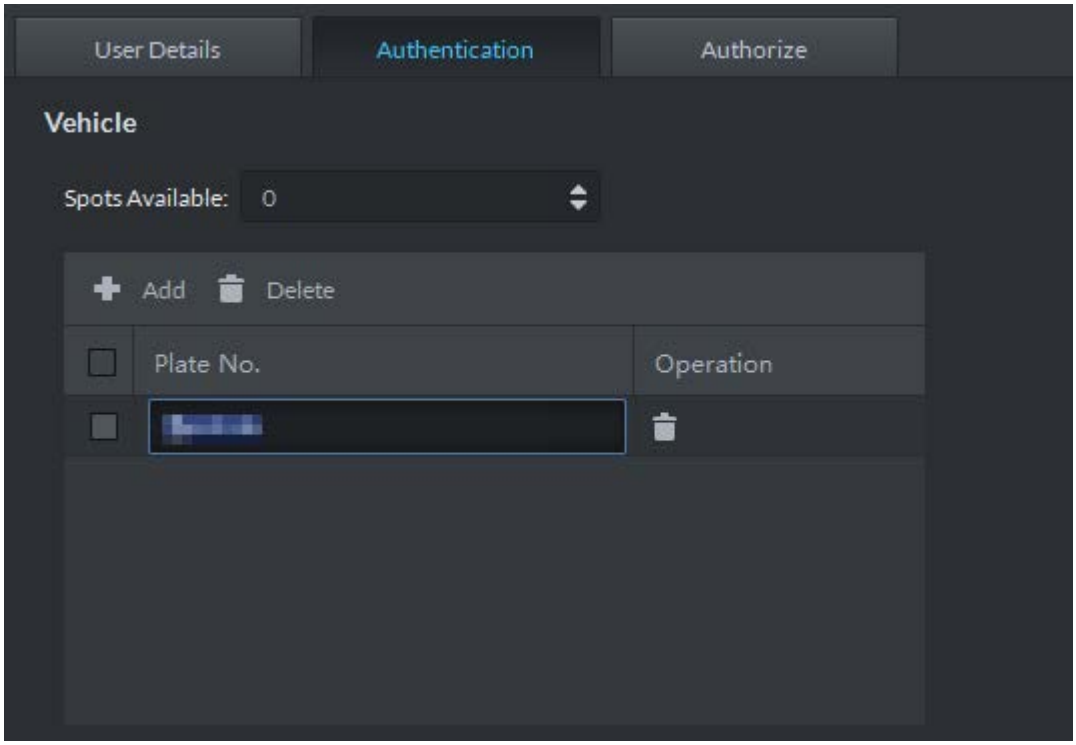
The IR face feature code is extracted; click **Re-extract** to update IR face feature code.

Step 9 Modify available spots and plate number.

Click **Spots Available**, modify spots, click **Plate No.** and modify plate No.

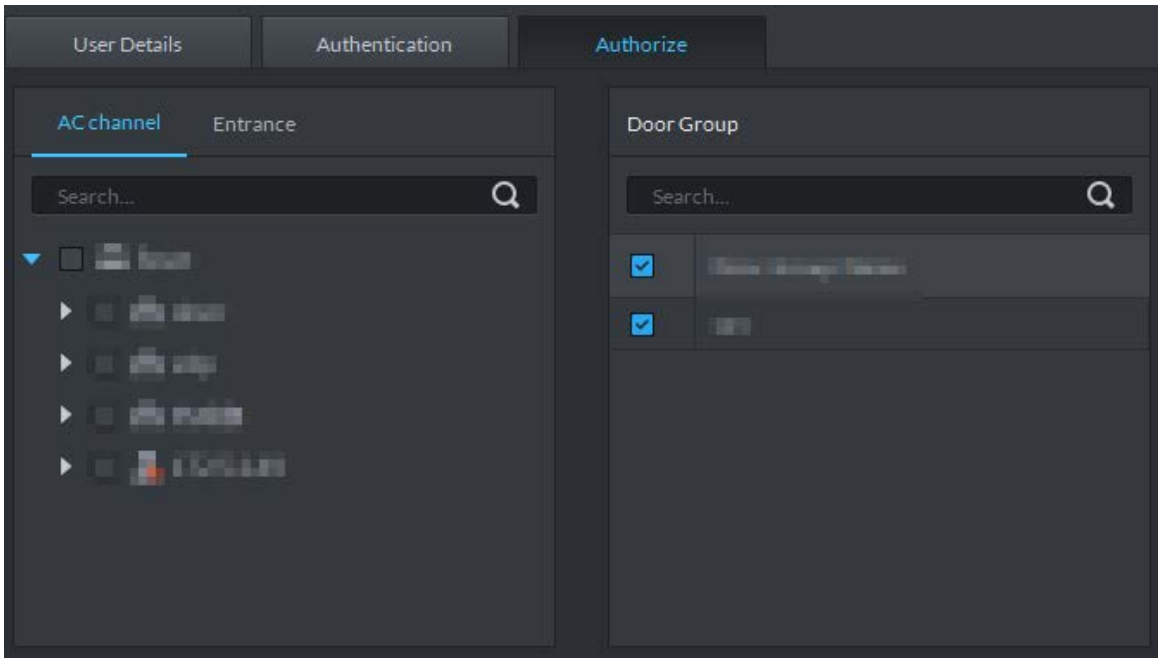
Click next to plate, or select plate and click to delete plate.

Figure 4-258 Add vehicle



Step 10 Click **Authorize**, modify access control and entrance is open to personnel. See Figure 4-259.

Figure 4-259 Authorize



Step 11 Click **OK** and confirm modification.

4.10.4 Importing/Exporting Personnel

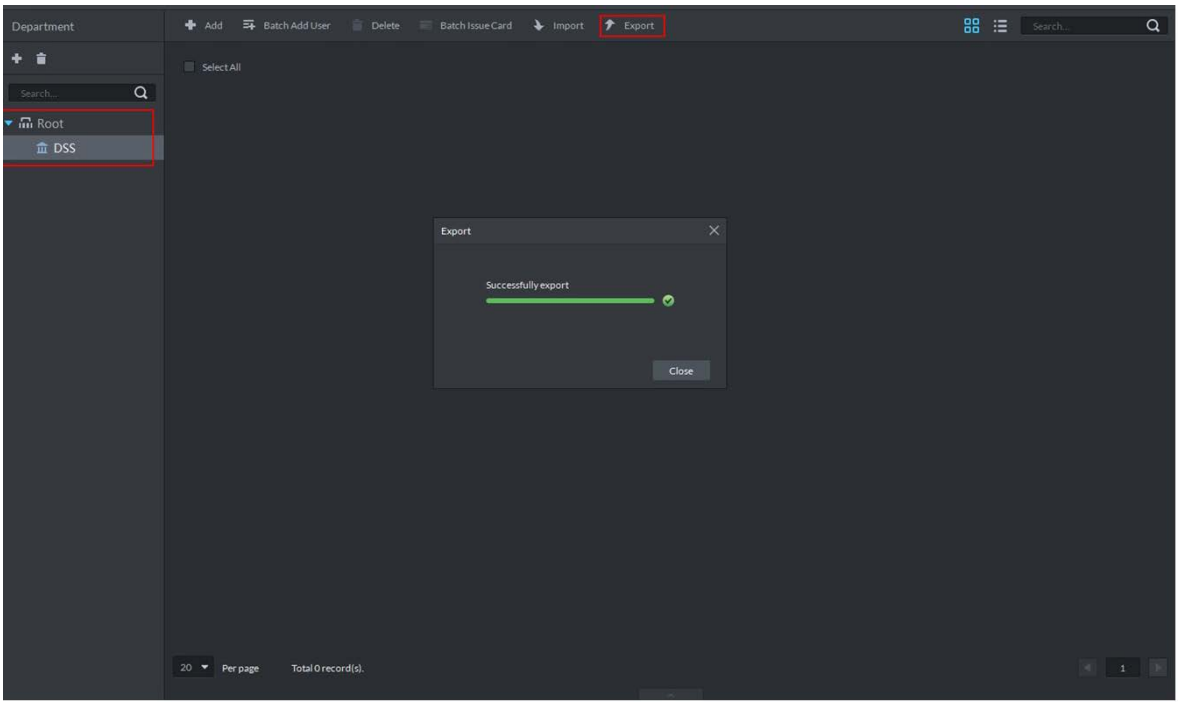
4.10.4.1 Exporting Personnel

Back up personnel data to restore damaged data or complete personnel configuration on the platform when there is a need for quick import of the personnel information.

Step 1 On the left side of the **Personnel Management** interface, select an organization, click **Export**, and follow the instructions on the interface to save the exported information to a local disk.

The progress of the export is displayed. See Figure 4-260.

Figure 4-260 Export personnel



Step 2 Select save path, click **Save**.

The system pops up **Export** dialog box, displays export progress.

Step 3 Click **Close** to close dialog box.

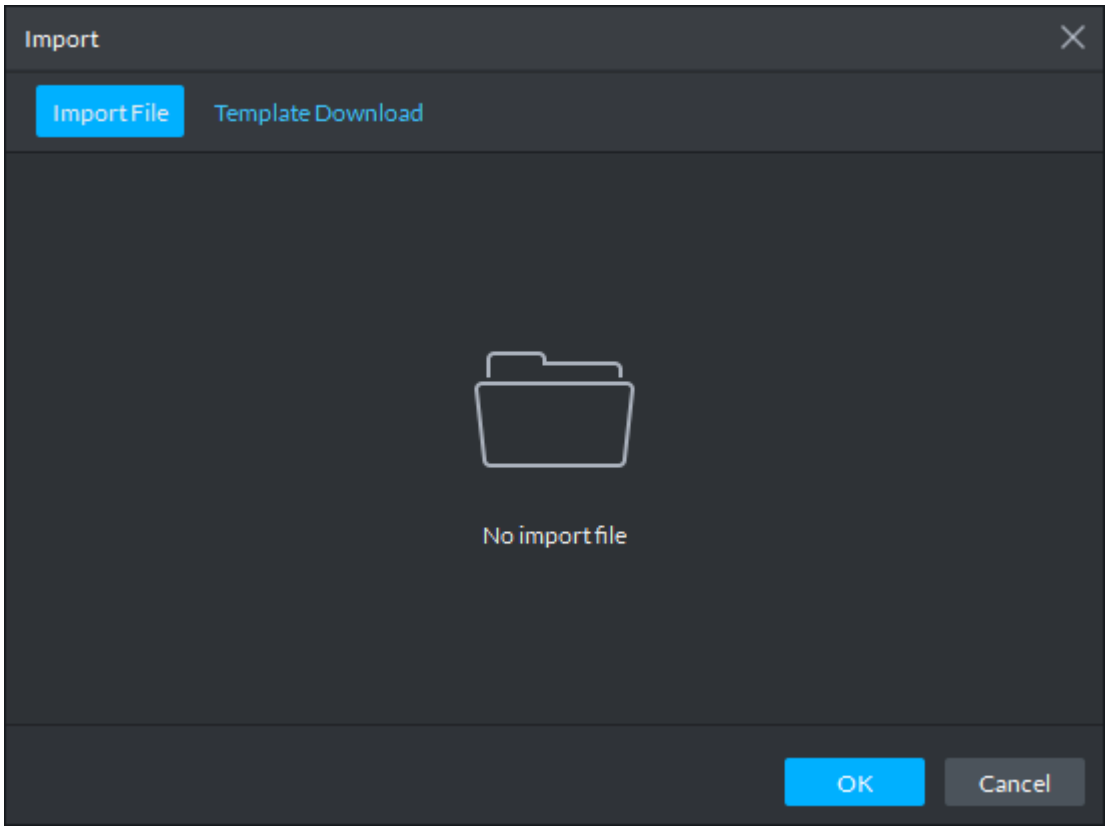
4.10.4.2 Importing Personnel

Edit the template or import information of existing personnel to quickly add them. You can import a file in .xls no larger than 1 M.

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

The **Import** interface is displayed. See Figure 4-261.

Figure 4-261 Import



Step 2 Import personnel information files.

1) Click **Import**, and follow the instructions on the interface to select the files.

If there is no personnel information file, click **Template Download** and follow the instructions on the interface to create personnel information.

2) Click **OK**.

Complete the import of personnel information.

The following might occur during an import:

- The system prompts that the imported personnel already exist on the platform.
- Personnel ID duplicate in the imported file. If the same ID does not exist, the system accepts it as a new ID; if it already exists, the system gives a prompt.
- The system prompts that the imported personnel information is improperly filled, such as field length exceeding the limit on the client, and timeout resulting in a failure to upload to the database.
- Abnormal default values. The rules are: Gender (male), property (common staff), department (root node), ID type (Identification Card), marital status (null) and education (No education). The valid period starts from now and ends in 2028 by default.
- A person does not exist. If the department does not exist, a new department is created under the root node; if the department exists, the person is created under the department; department information matches by name.
- Cannot read the contents with a parsing error reported directly.

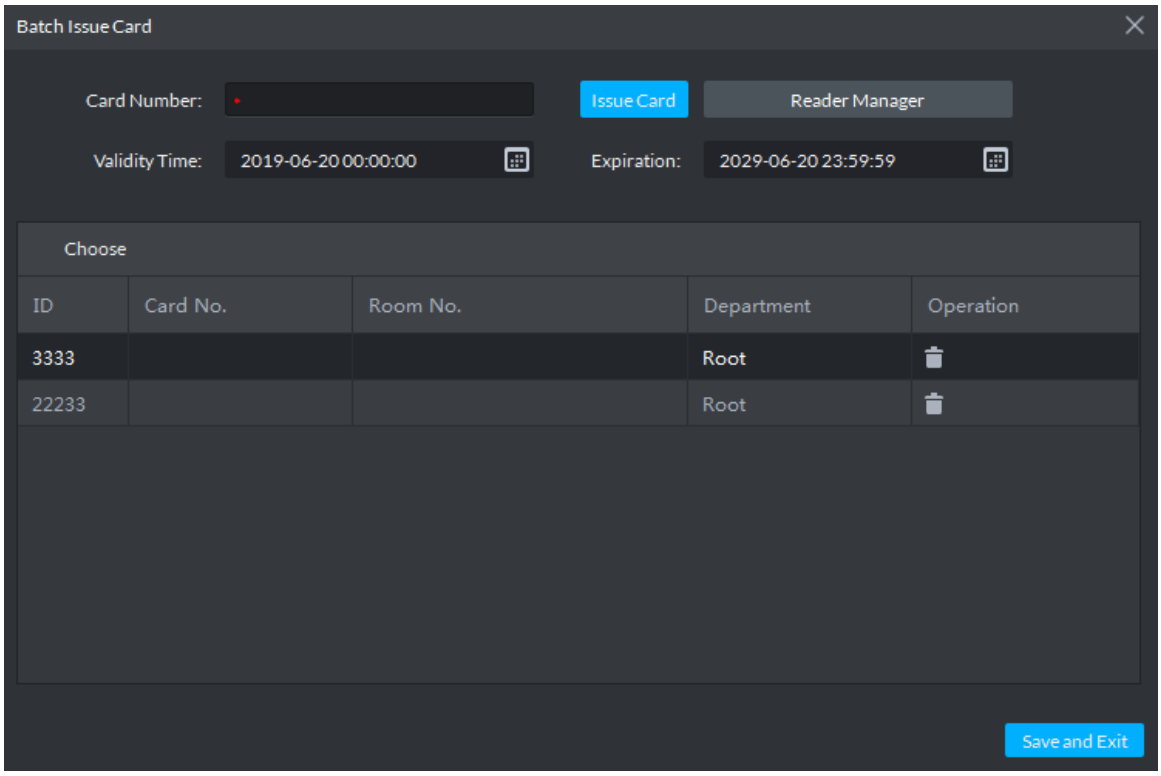
4.10.5 Batch Issue Card

Supports batch issuing cards to personnel.

Step 1 On the **Personnel Management** interface, select the personnel to issue card to, and click **Batch Issue Card**.

The **Batch issue card** interface is displayed. See Figure 4-262.

Figure 4-262 Batch issue card



Step 2 Issue cards to personnel.

You can issue card by entering card No. manually or card reader.

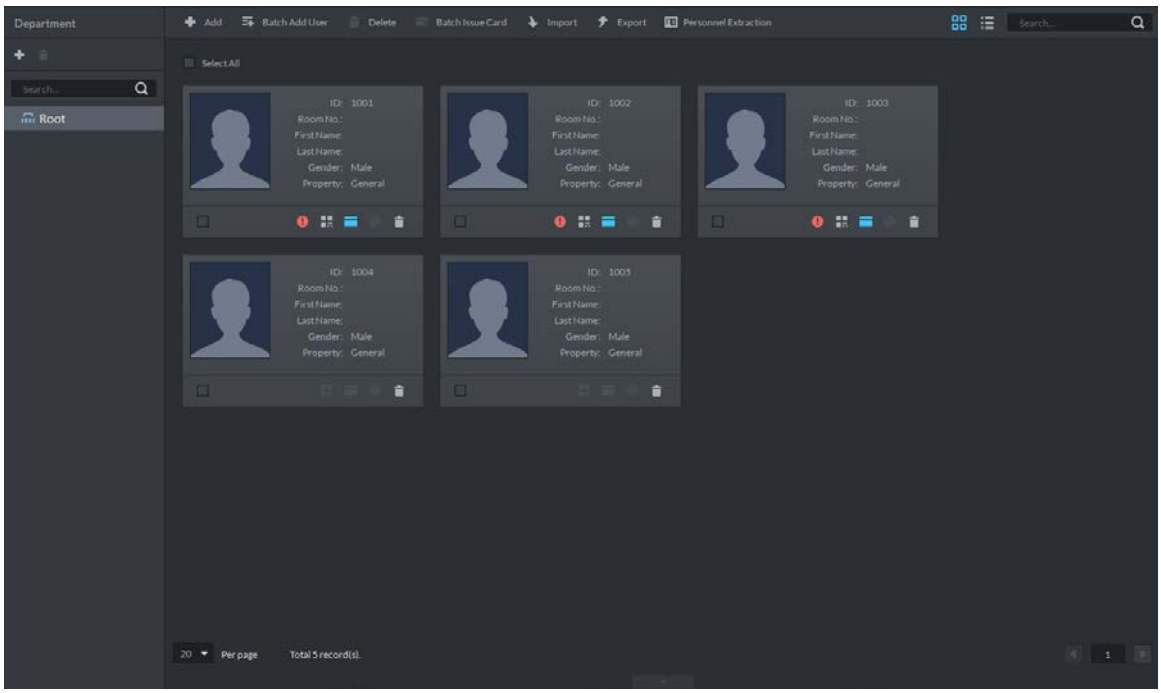
- Issue card by entering card No. manually

1) Select a person, enter the card number, and set up the validity time and expiry time.
2) Click Issue Card.

   Complete issuing card to the selected personnel and the interface shows the personnel card number.
3) Repeat the steps until all personnel get their cards.
4) Click Save and Exit.

   The personnel info interface is displayed. See Figure 4-263.

Figure 4-263 Personnel info

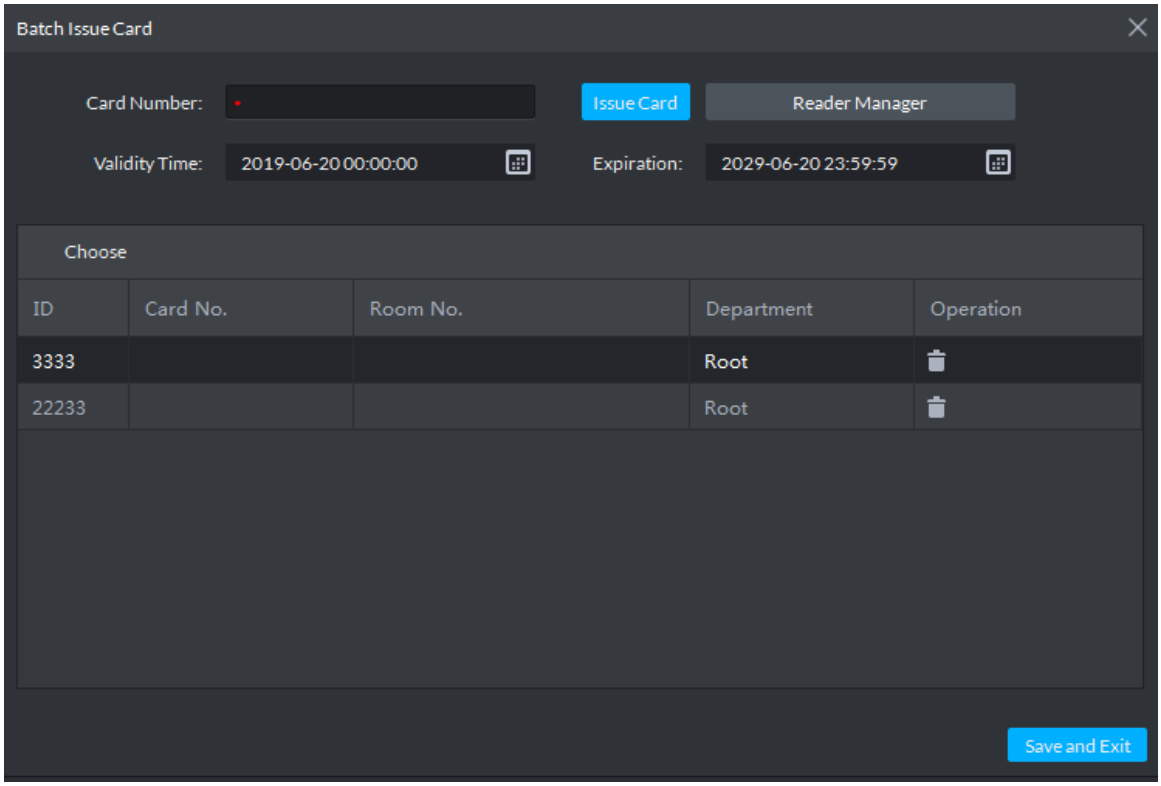


- Issue card by card reader

1) Click **Reader Manager**.

   The **Reader Manager** interface is displayed. See Figure 4-264.

Figure 4-264 Reader manager



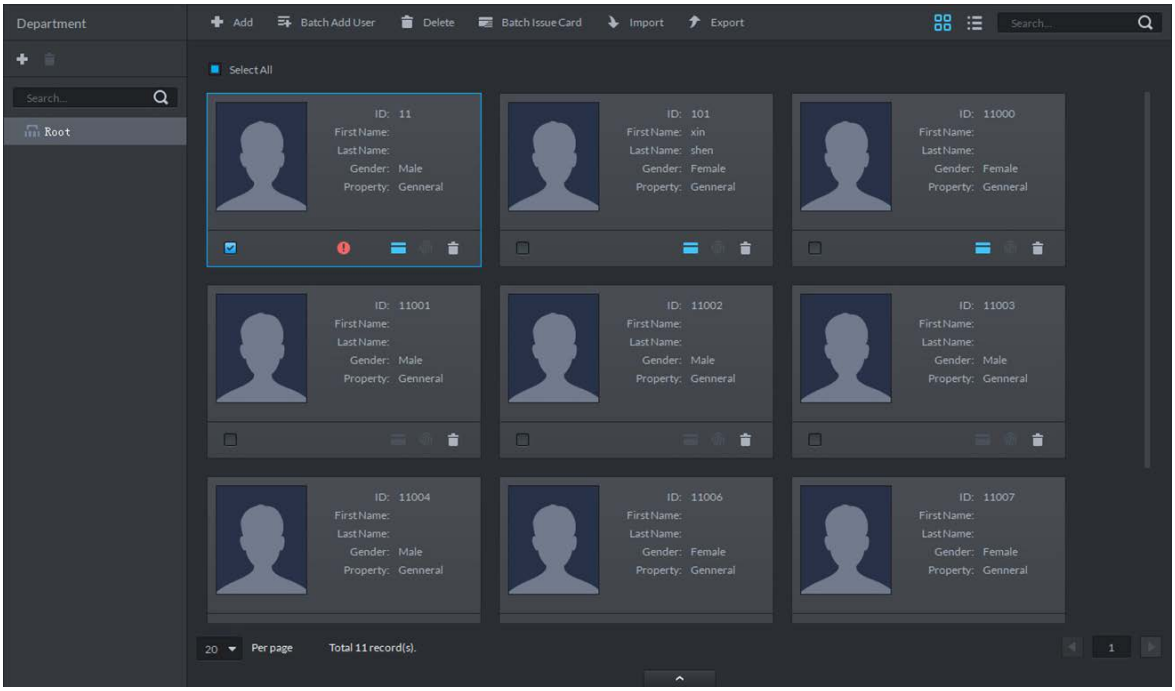
2) Select from **Card Reader** or **Device**, and click **OK**.
3) Swipe the card on the card reader or device.
4) Select a person, set up the validity time and expiry time, and click **Issue Card**.
5) Repeat the steps until all personnel get their cards.
6) Click **Next Step**.

The personnel info interface is displayed.

Step 3 Select the access control channels or door groups to which the personnel have access, and click **Finish**.

The interface displays the card issuing results. See Figure 4-265. The card icon changes into blue, as  and it means that you have issued a card to the person.

Figure 4-265 Issue card result



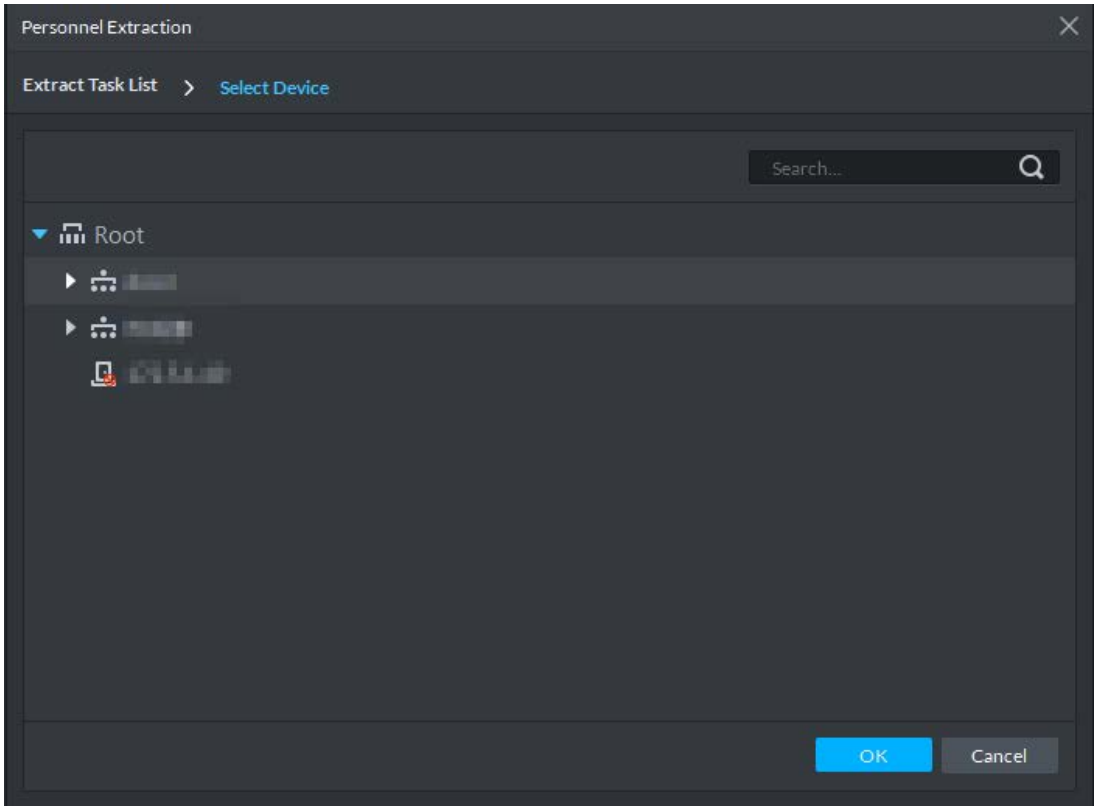
4.10.6 Personnel Extraction

Extract personnel info from access control, and sync it to platform.

Step 1 On Personnel Management interface, click Personnel Extraction.

The **Personnel Extraction** interface is displayed. See Figure 4-266.

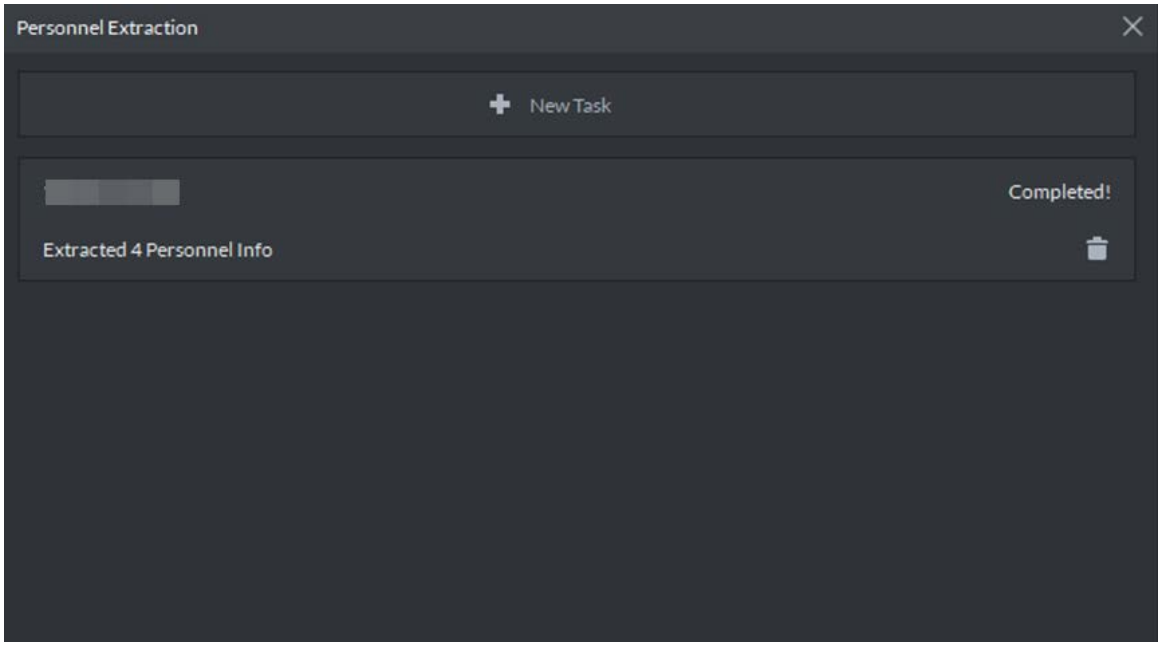
Figure 4-266 Personnel extraction



Step 2 Select access control device, click **OK**.

The extraction result is displayed. See Figure 4-267.

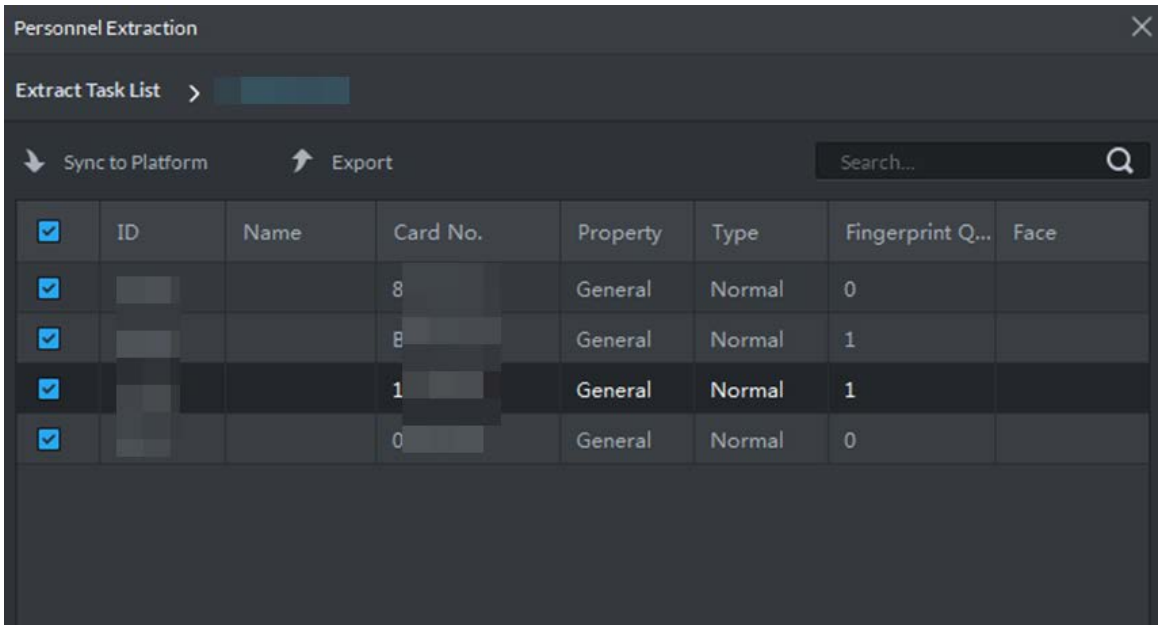
Figure 4-267 Extraction result



Step 3 Double click record.

The info of extracted personnel is displayed. See Figure 4-267.

Figure 4-268 Extracted personnel detail



Step 4 Select personnel, click **Sync to platform**.

Select personnel and add to list.

Select personnel, click **Export** and save personnel info to local PC.

4.10.7 Generating Path

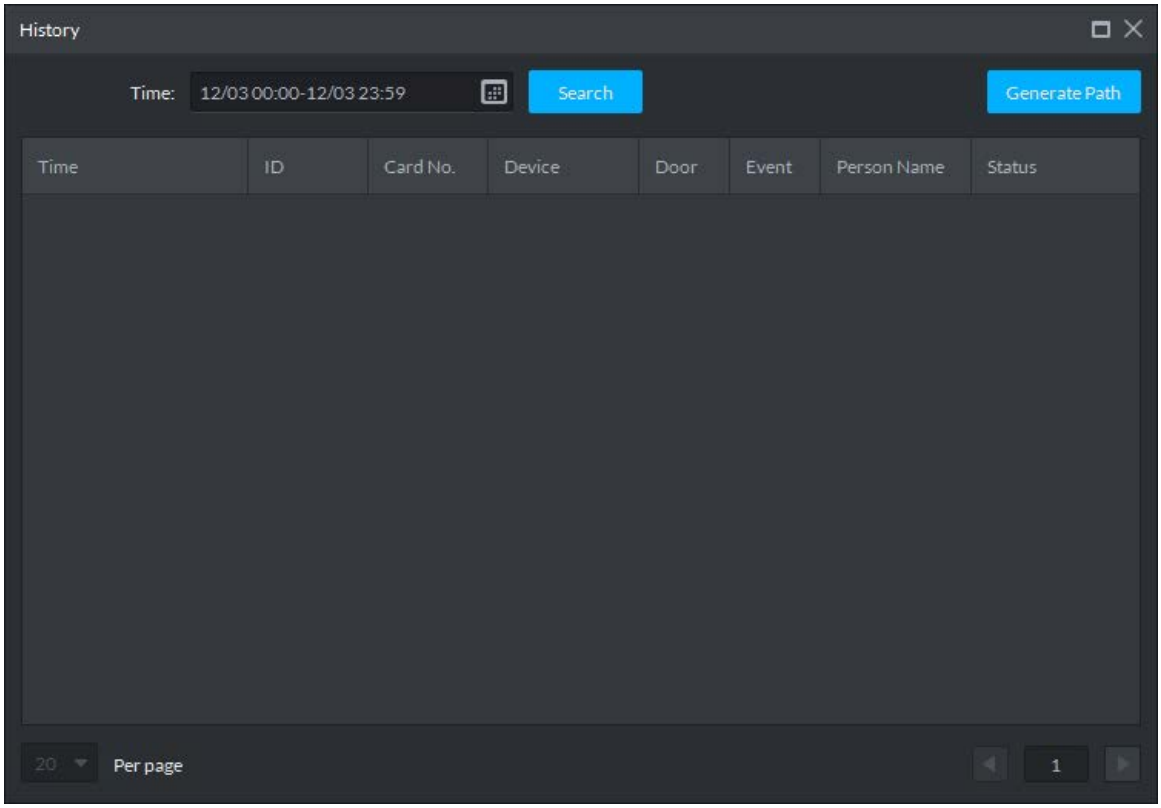
You can check all door unlocking records by personnel and generate a path.

To view the generated path, you have to drag the access control device to the map for display first. See 4.1.6 Configuring Emap for detailed steps.

Step 1 On **Personnel Management** interface, click or of the person.

Step 2 The **History** interface is displayed. See Figure 4-269.

Figure 4-269 Personnel history record



Step 3 Set up time for the search and click **Search**.

The search results is displayed.

Step 4 Click Generate Path.

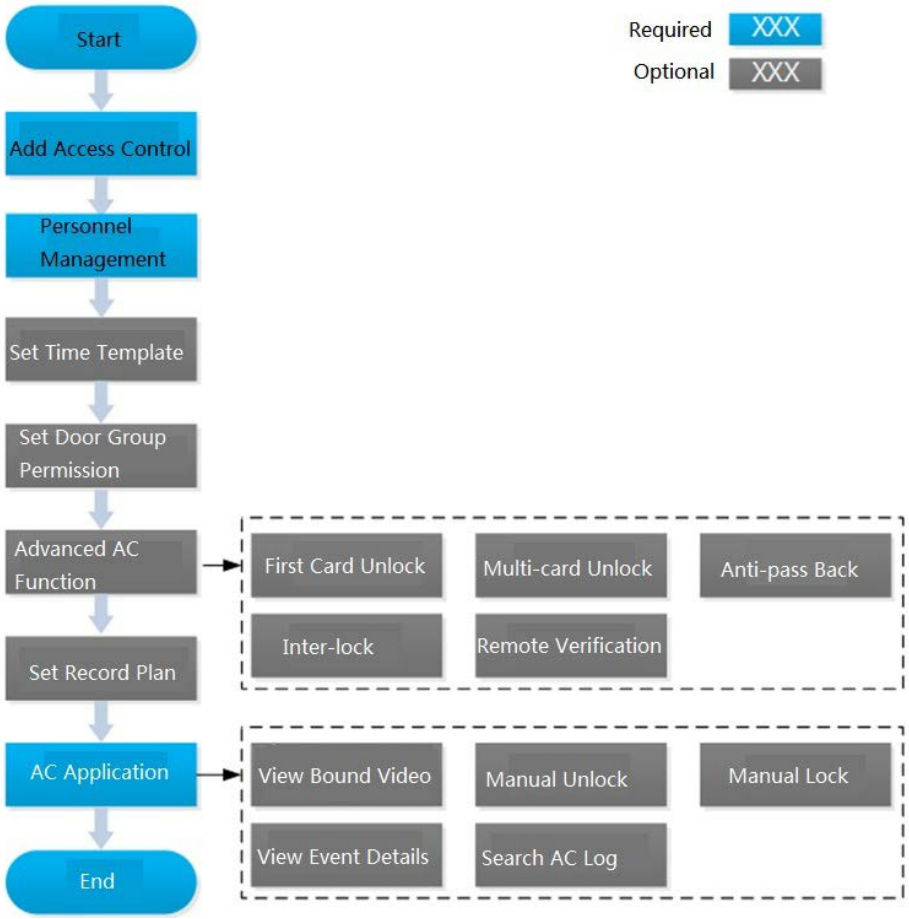
The map interface to show the activity path of the person is displayed.

Step 5 Click **Export**, and drag the mouse on the interface to select a region. Follow the instructions on the interface to save the path as a picture to a local disk.

4.11 Access Control

After adding access control devices on Pro, you can control the door locking/unlocking on platform, view videos and events related to the access control channel, and configure advanced access control functions, such as First Card Unlock and Multi-card Unlock. For operation flow, see Figure 4-270.

Figure 4-270 AC management flow



4.11.1 Adding Access Control

Step 1 Add access control device. For more details, see "4.1.2.4 Adding Device."

Support access control devices including general AC device, AC integrated controller, 2nd generation AC, face AC and IR face AC. Set **Device Category** as **Access Control** when adding.

Step 2 Bind resources.

If panoramic camera is installed in the scene, it supports binding AC channel and panoramic camera. You can view real-time video image of panoramic camera on console. When alarm is triggered, you can view video of bound panoramic camera.

The panoramic camera is required to be added to platform before binding resources.

1) On client homepage, click **Config.**
   The **Config** interface is displayed.
2) In the left device tree, select AC channel, click **Resource Bind**, and see Figure 4-271. The **Resource Bind** interface is displayed. See Figure 4-272.

Figure 4-271 Enter resource bind interface

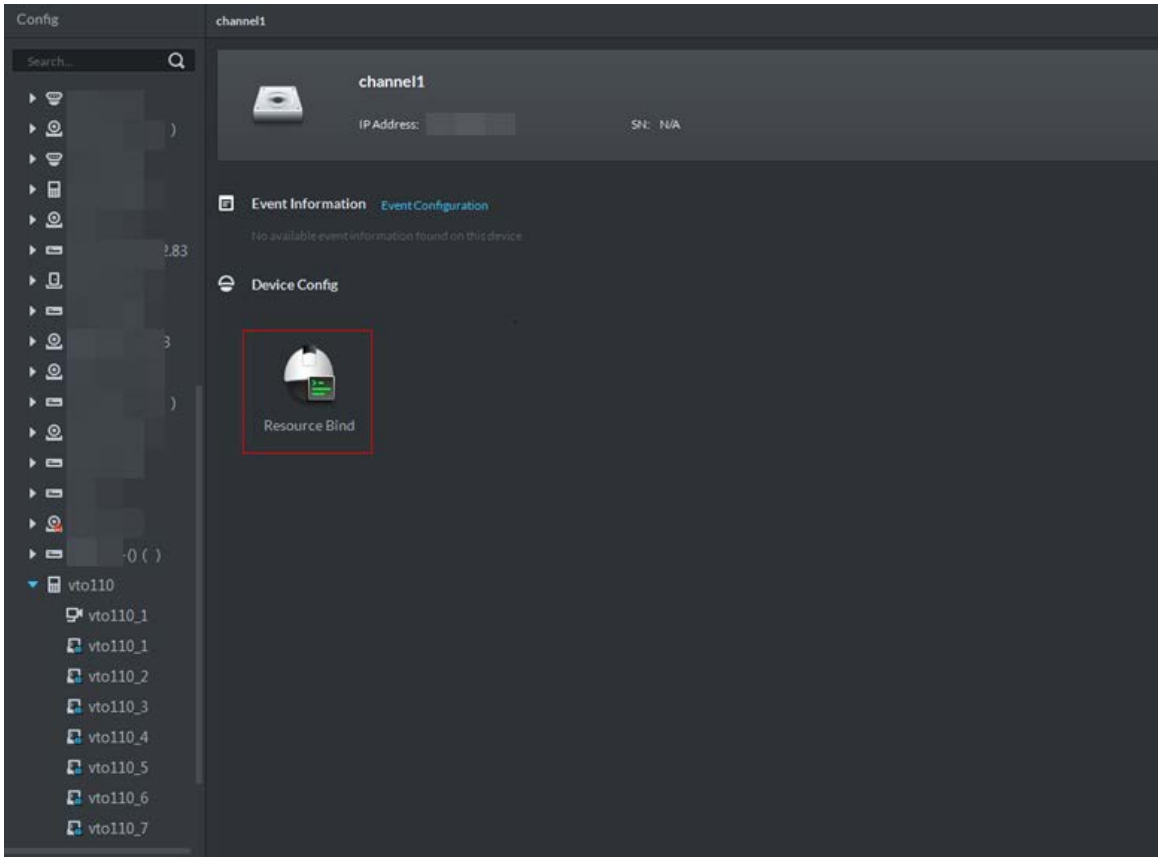
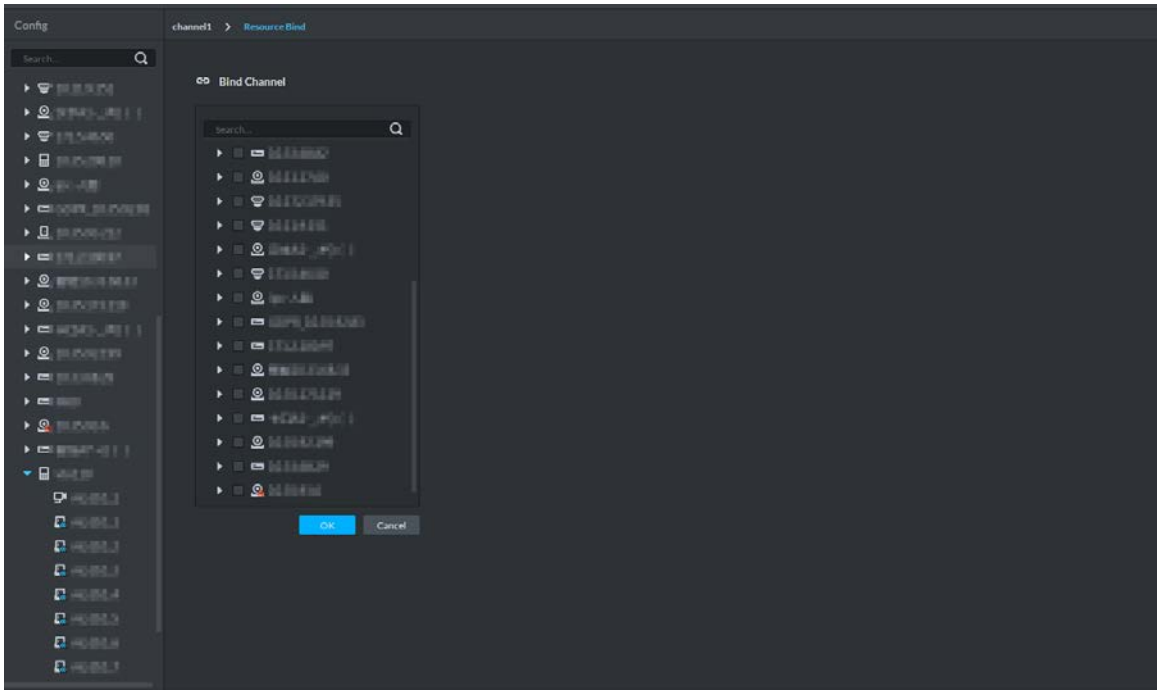


Figure 4-272 Resource bind



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

Step 3 Configure door info.

You can configure door status, NC and NO period, alarm enable and unlock length.

1) On client homepage, click **Config**.
   The **Config** interface is displayed.
2) In left device tree, select AC channel, click **Door Configuration**, and see Figure 4-273.

The **Door Config** interface is displayed. See Figure 4-274.

For the console on access control interface, right-click **AC Channel**, select **AC Channel Config** and enter **Door Config** interface.

Figure 4-273 Enter config interface

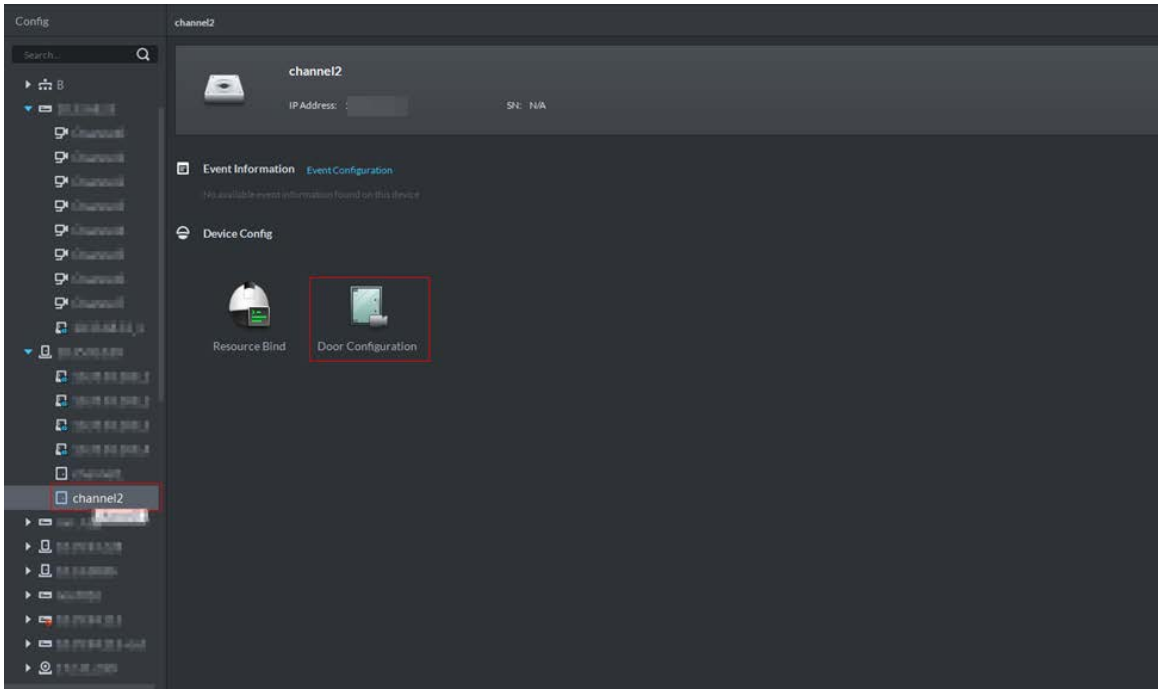
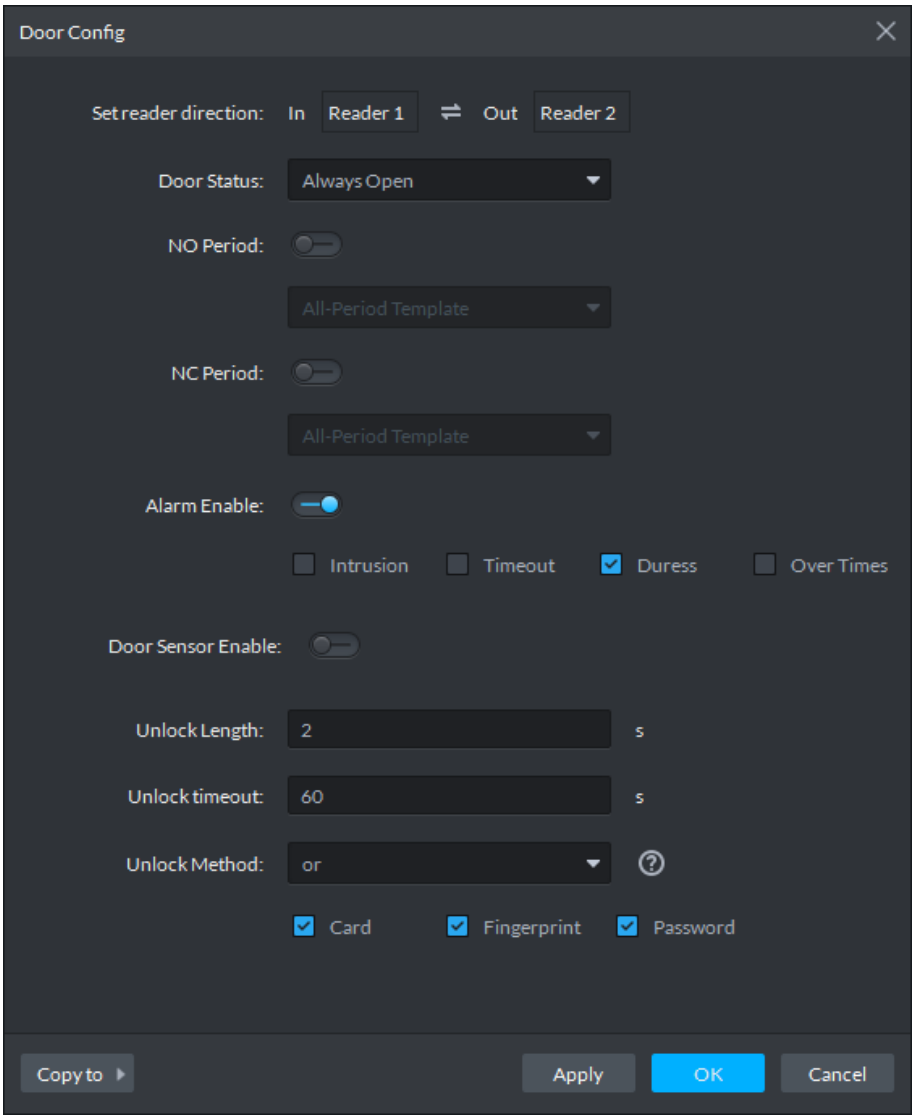


Figure 4-274 Door config



3) Configure door information and click **OK**. For details of the parameters, see Table 4-40.

The interface might be different for different access control devices connected. The actual interfaces shall prevail.

Table 4-40 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.

4.11.2 Personnel Management

If you want to add personnel, see"4.10 Personnel Management." When adding personnel, you need to add information such as card, fingerprint and face comparison according to requirement, and enable access control permission.

4.11.3 Managing Time Template

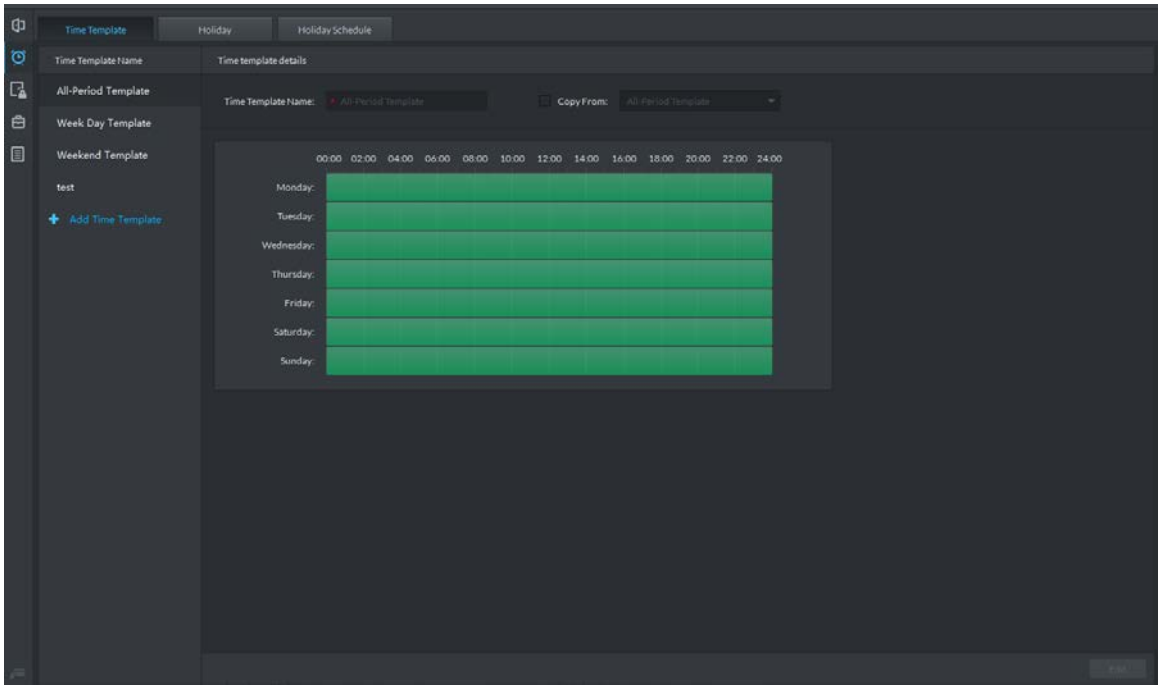
4.11.3.1 Setting Time Template

Default time template includes all-period template, week day template and weekend template. If default template fails to meet requirement, then set time template and you can adopt different unlock modes at different time.

Step 1 On client homepage, click **Access Control**.
The **Access Control** interface is displayed.

Step 2 Click and the **Time Template** interface is displayed. See Figure 4-275.

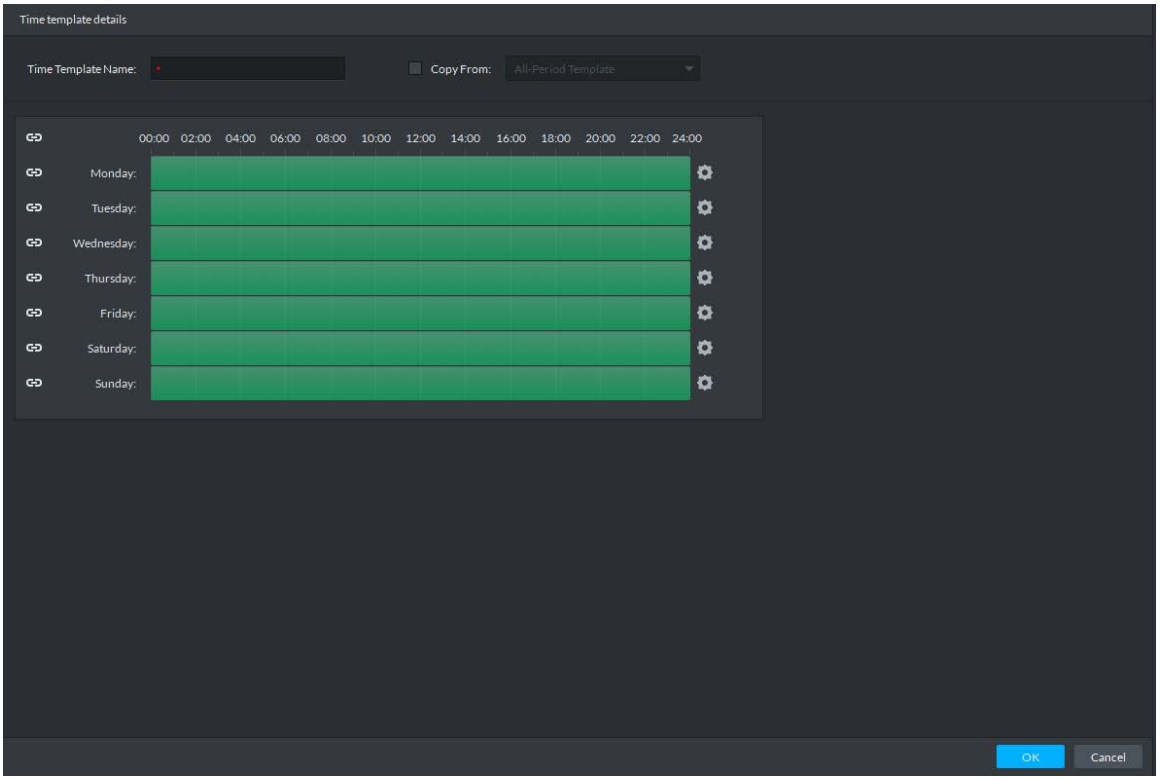
Figure 4-275 Time template



Step 3 Click Add Time Template.

The **Time template details** interface is displayed. See Figure 4-276.

Figure 4-276 Add time template



Step 4 Set up **Time Template Name** and the required time period, and click **OK**.

Select **Copy From** and the copied template, and you can use the time periods of the copied template. In this way, you can quickly configure the time periods by modifying the ones of the copied template.

Methods to set up the time period:

- Method I: Press and hold the left button of the mouse. Over the time periods not selected, the mouse displays as a pen, and you can drag the mouse on the setting interface to select a time period. Over the selected time periods, the mouse displays as an eraser, and you can erase selected time periods with it.

  Click the icons in front of multiple week numbers one by one and the icons change to . In this way, you can configure the time periods corresponding to the week numbers. You can quickly select all the week numbers by clicking on the top.

- Method II: Click and set up the time periods in the popup interface. You can set up six time periods at most.

Step 5 The new time template is displayed in the left list.

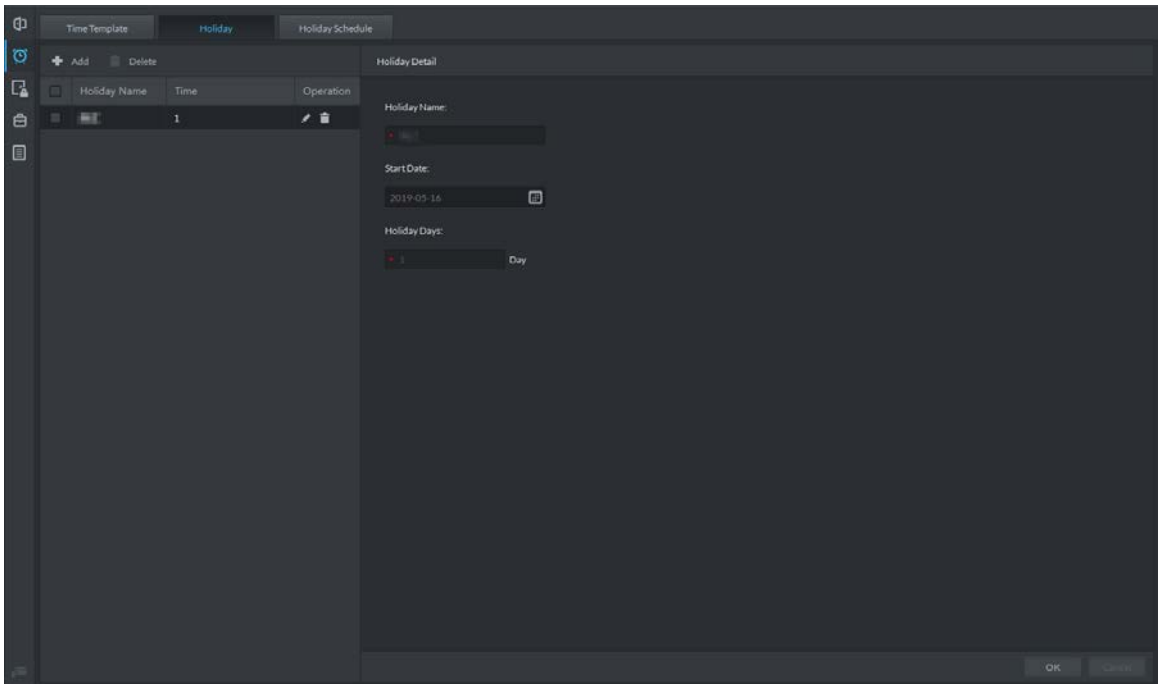
4.11.3.2 Setting Holiday

Set holiday according to actual situation, used to configure holiday plan, and you can unlock according to holiday plan.

Step 1 On **Access Control** interface, click and select **Holiday**.

The **Holiday** interface is displayed. See Figure 4-277.

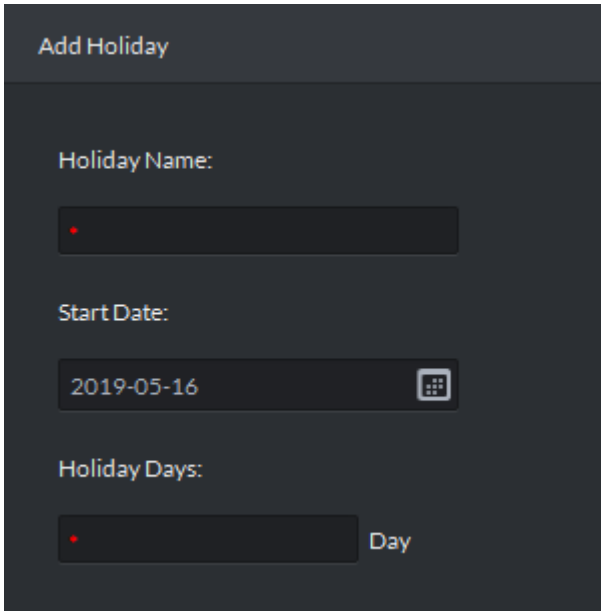
Figure 4-277 Holiday



Step 2 Click **Add**.

The holiday config interface is displayed. See Figure 4-278.

Figure 4-278 Add holiday



Step 3 Set holiday info, click **OK**.

4.11.3.3 Setting Holiday Schedule

Door group can unlock according to the holiday schedule that is set.

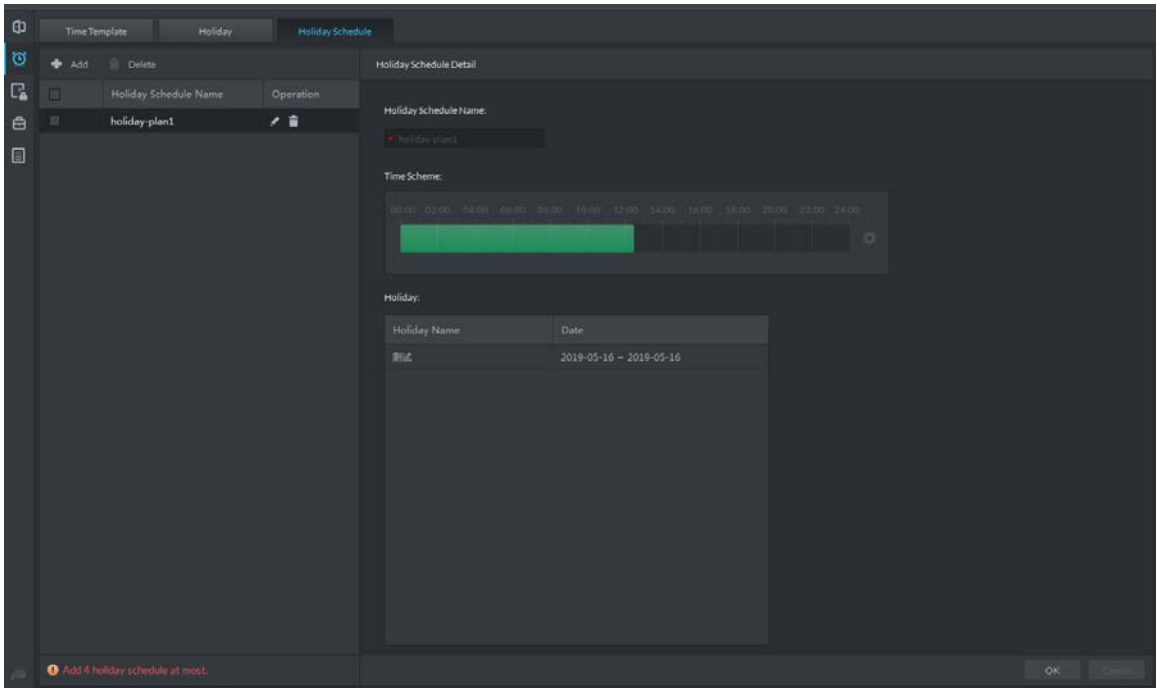
Step 1 On **Access Control** interface, click and select **Holiday Schedule**.

The **Holiday Schedule** interface is displayed.

Step 2 Click **Add**.

The interface of add holiday schedule is displayed. See Figure 4-279.

Figure 4-279 Add holiday schedule



Step 3 Set holiday schedule parameters, click **OK** and complete config.

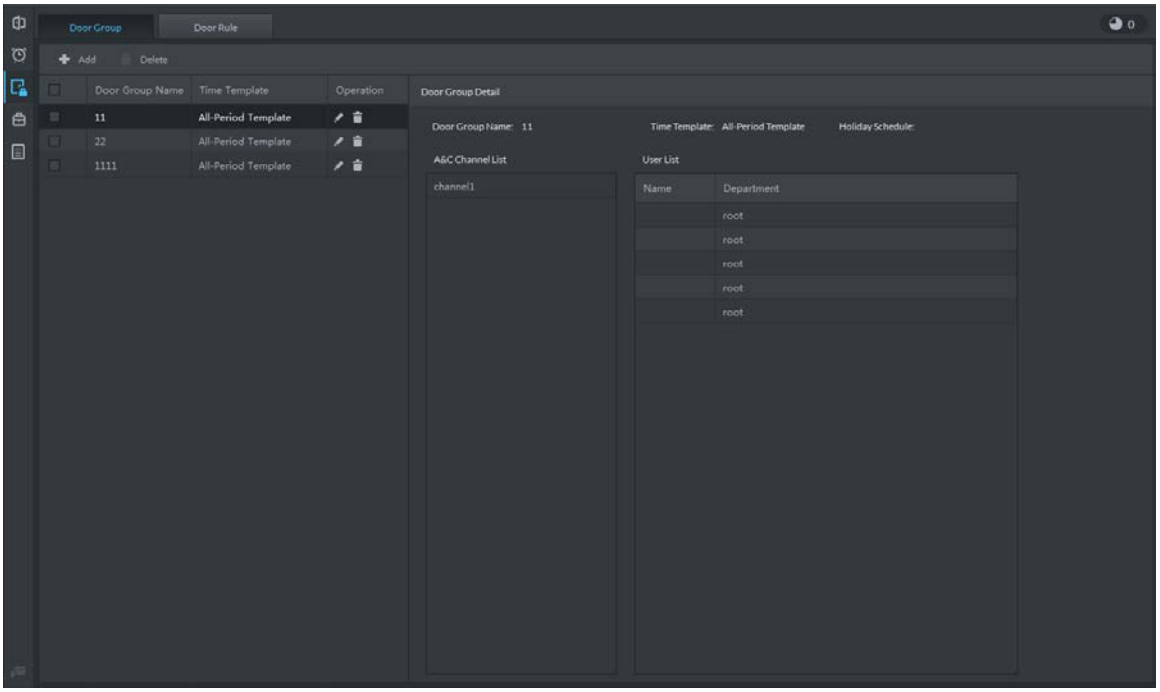
4.11.4 Setting Access Level

If you manage the doors by groups, you can quickly grant users with the authorizations to unlock the doors in a specific group.

Step 1 On the **Access Control** interface, click .

The **Access Level** interface is displayed. See Figure 4-280.

Figure 4-280 Access level



Step 2 Create door groups.

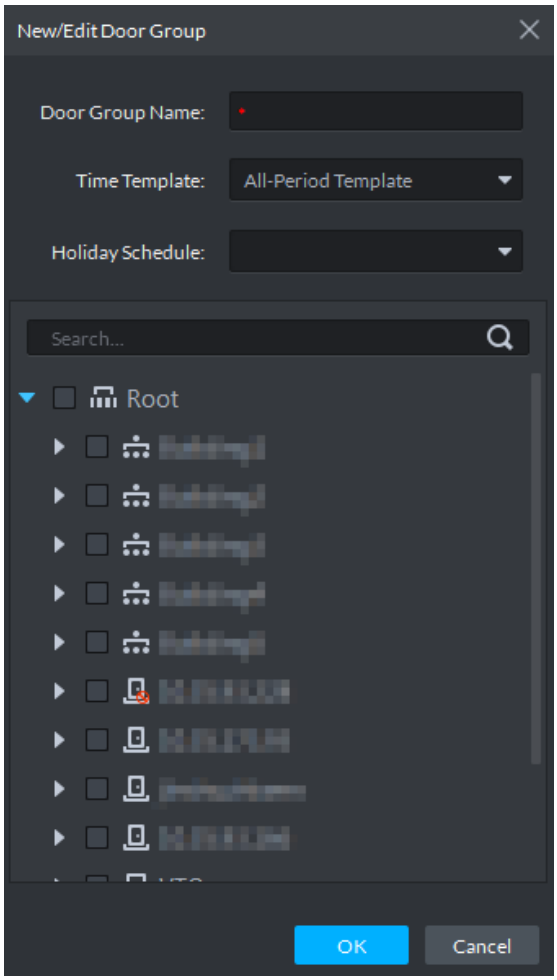
1) Click the **Door Group** tab.

   The **Door Group** interface is displayed.

2) Click **Add**.

   The **New/Edit Door Group** interface is displayed. See Figure 4-281.

Figure 4-281 New/Edit door group



3) Enter **Door Group Name**, select **Time Template** and an access control channel, and click **OK**.

After selecting the time template and access control channel, you can only use the time periods of the selected time template and the selected access control channel when granting authorizations to users. The interface displays the information of the newly created door groups.

Step 3 Authorize users.

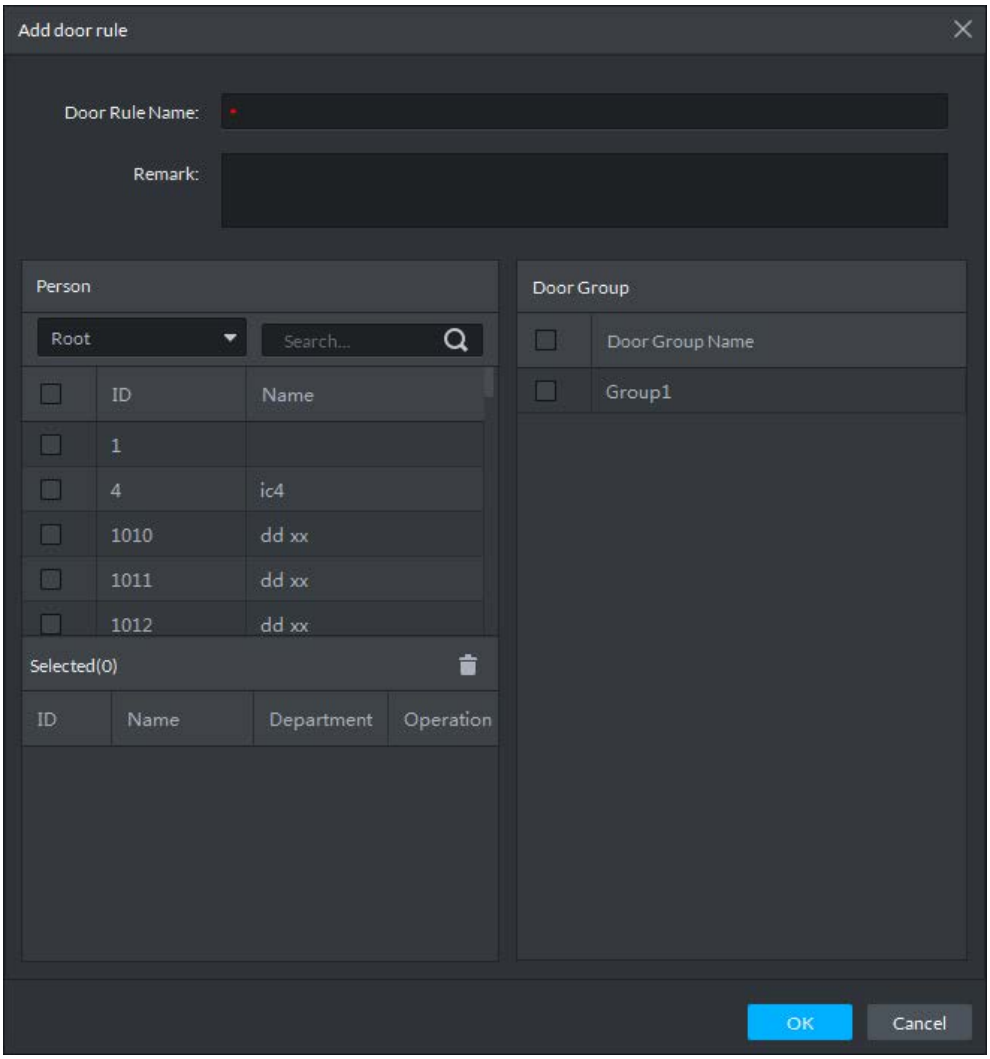
1) Click the **Door Rule** tab.

The **Door Rule** interface is displayed.

2) Click **Add**.

The **Add door rule** interface is displayed. See Figure 4-282.

Figure 4-282 Add door rule



3) Enter **Door Rule Name**, select **Person** and **Door Group**, and click O**K**.
The interface displays the authorization information.

Click  at top right to check authorizing process. Double click the failture record to check detailed info.

4.11.5 Advanced Function

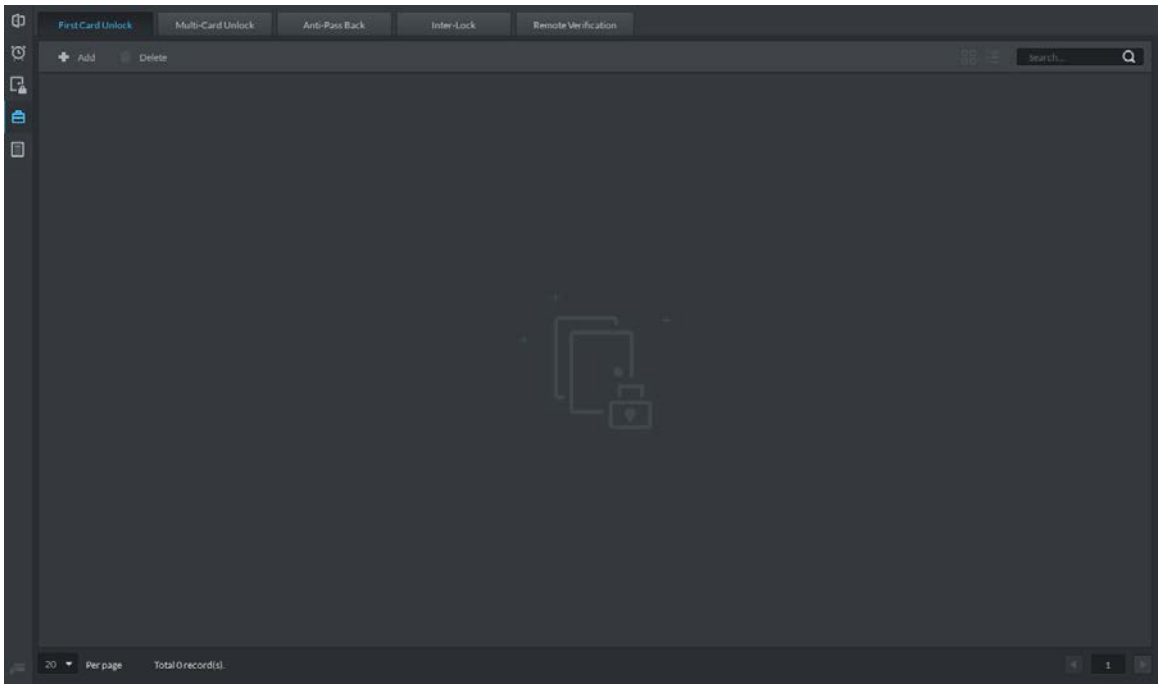
4.11.5.1 First Card Unlock

Only after the specified first-card user swipes the card every day can other users unlock the door with their cards. You can set up multiple first cards. Only after any one of the users swipes the first card can other users without first cards unlock the door with their cards.

Step 1 On the **Access Control** interface, click  and select **First Card Unlock**

The **First Card Unlock** interface is displayed. See Figure 4-283.

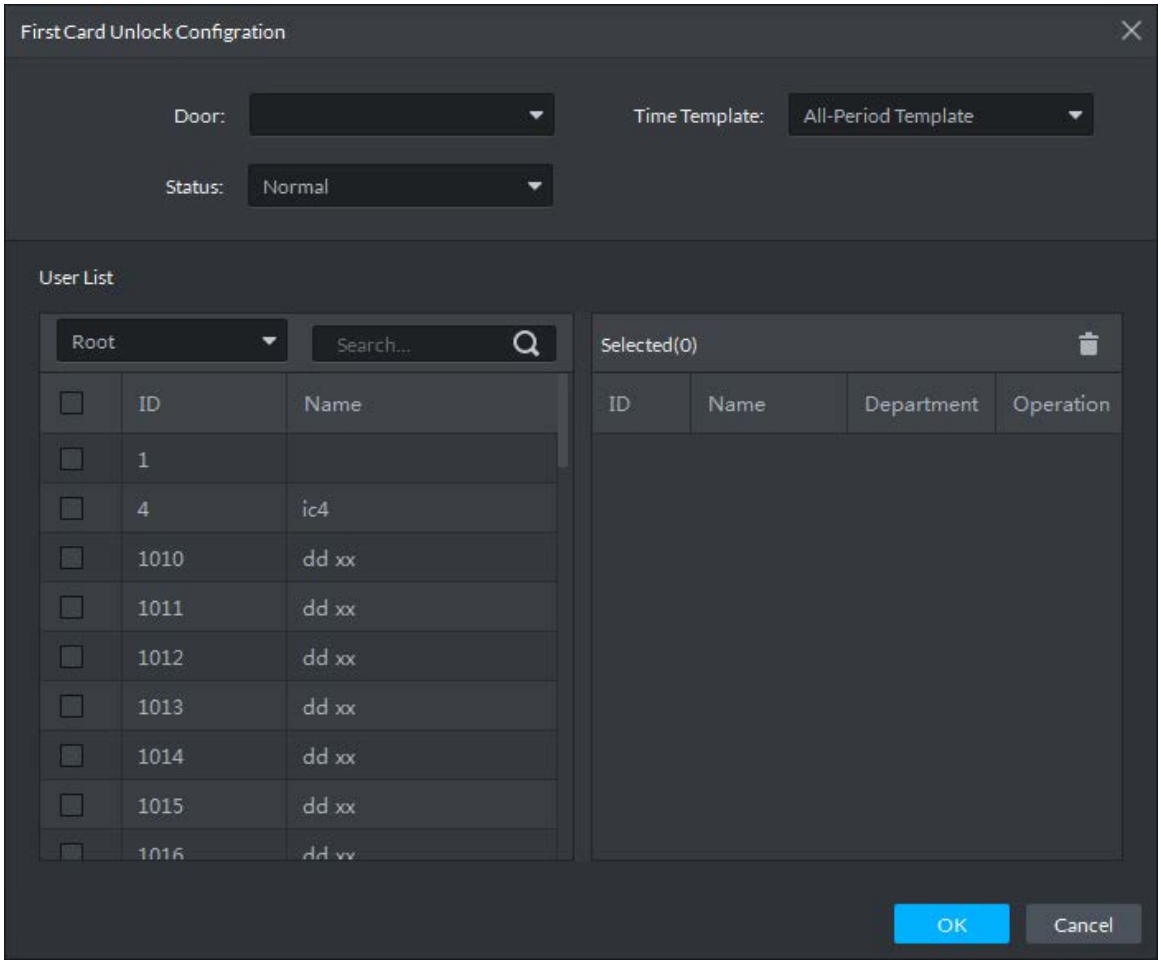
Figure 4-283 First card unlock



Step 2 Click **Add**.

The **First Card Unlock Configuration** interface is displayed. See Figure 4-284.

Figure 4-284 First card unlock config



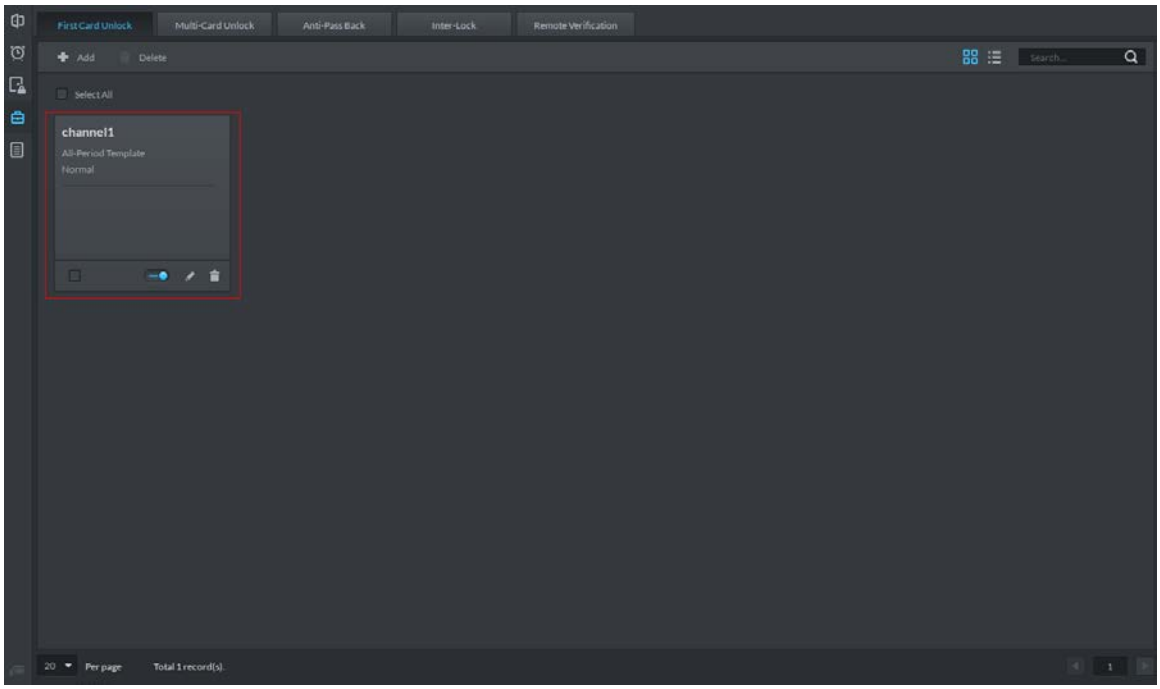
Step 3 Configure the **First Card Unlock** parameters and click **OK**. For details of the parameters, see Table 4-41.

The **First Card Unlock** information is displayed. See Figure 4-285. First Card Unlock is enabled by default.

Table 4-41 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 4-285 First card info list



Step 4 Click .

The icon changing into indicates **First Card Unlock** is enabled.

4.11.5.2 Multi-Card Unlock

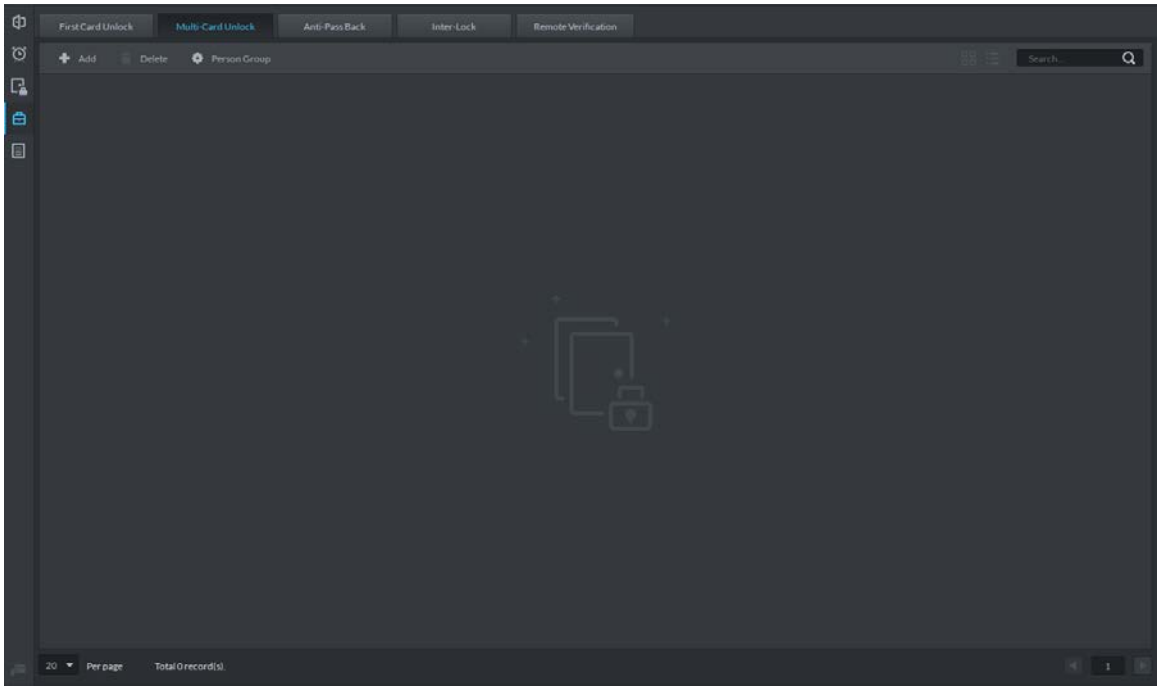
In this mode, multiple groups of users have to swipe cards for an access control channel in an established sequence to unlock the door.

- One group can have up to 64 users.
- With Multi-Card Unlock enabled for an access control channel, it supports up to four groups of users being on site at the same time for verification. The total number of users can be 64 at most, with up to five valid users.

Step 1 On the Access Control interface, click and select **Multi-card Unlock**.

The **Multi-Card Unlock** interface is displayed. See Figure 4-286.

Figure 4-286 Multi-card unlock

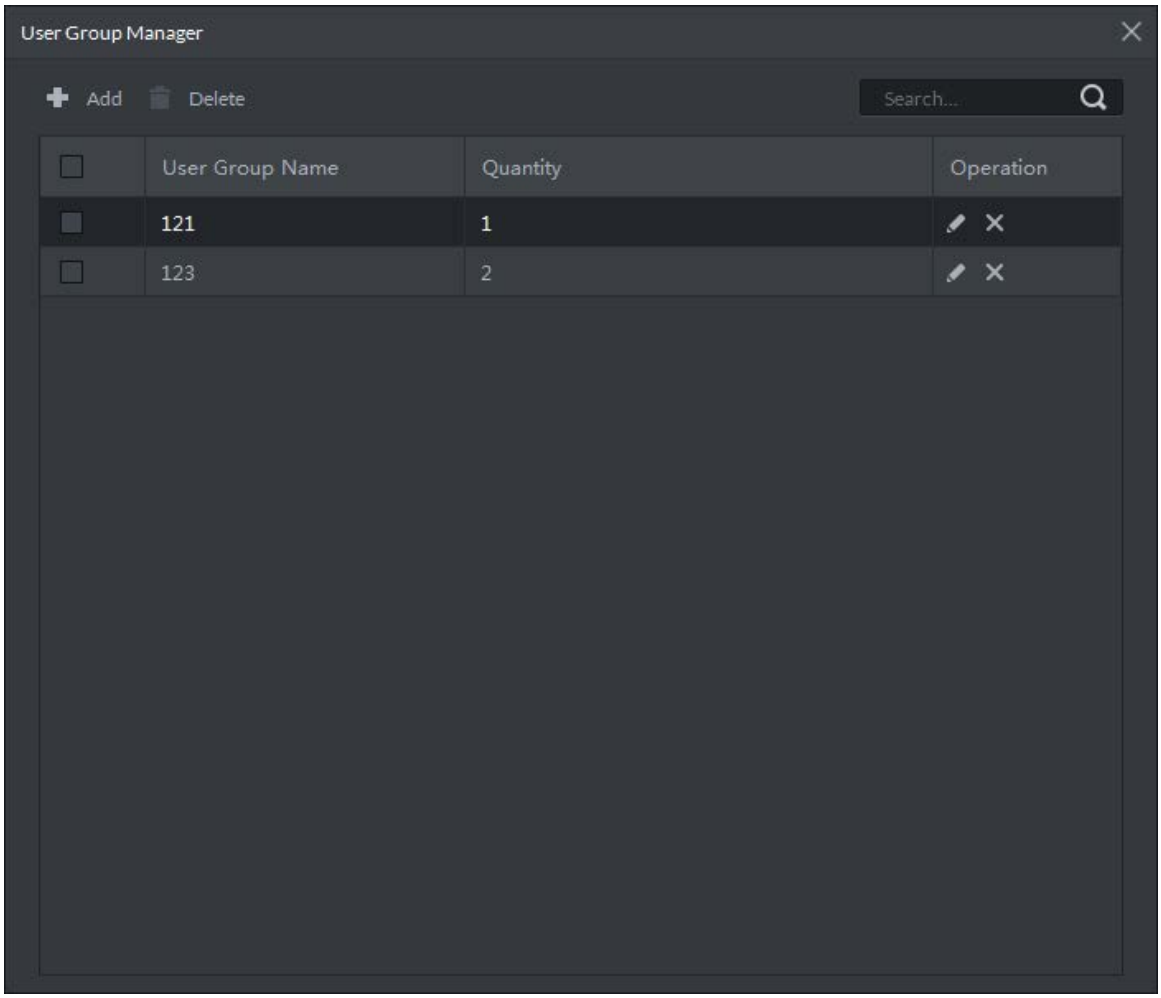


Step 2 Add user group.

1) Click Person Group.

The **User Group Manager** interface is displayed. See Figure 4-287.

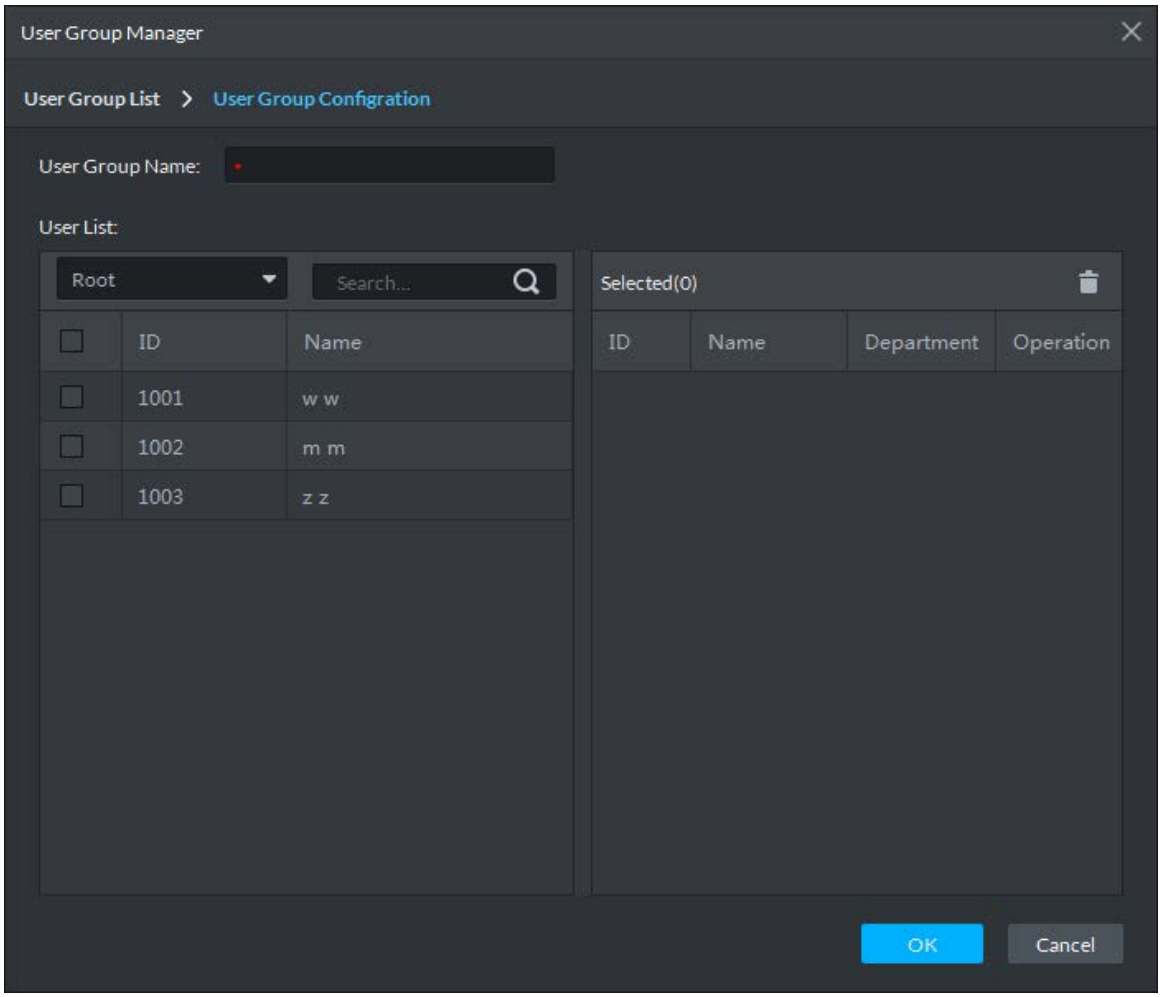
Figure 4-287 User group manager



2) Click **Add**.

The **User Group Manager** interface is displayed. See Figure 4-288.

Figure 4-288 User group config



3) Set up **User Group Name**. Select users from **User List** and click **OK**. You can select up to 64 users.

The user group information is displayed.

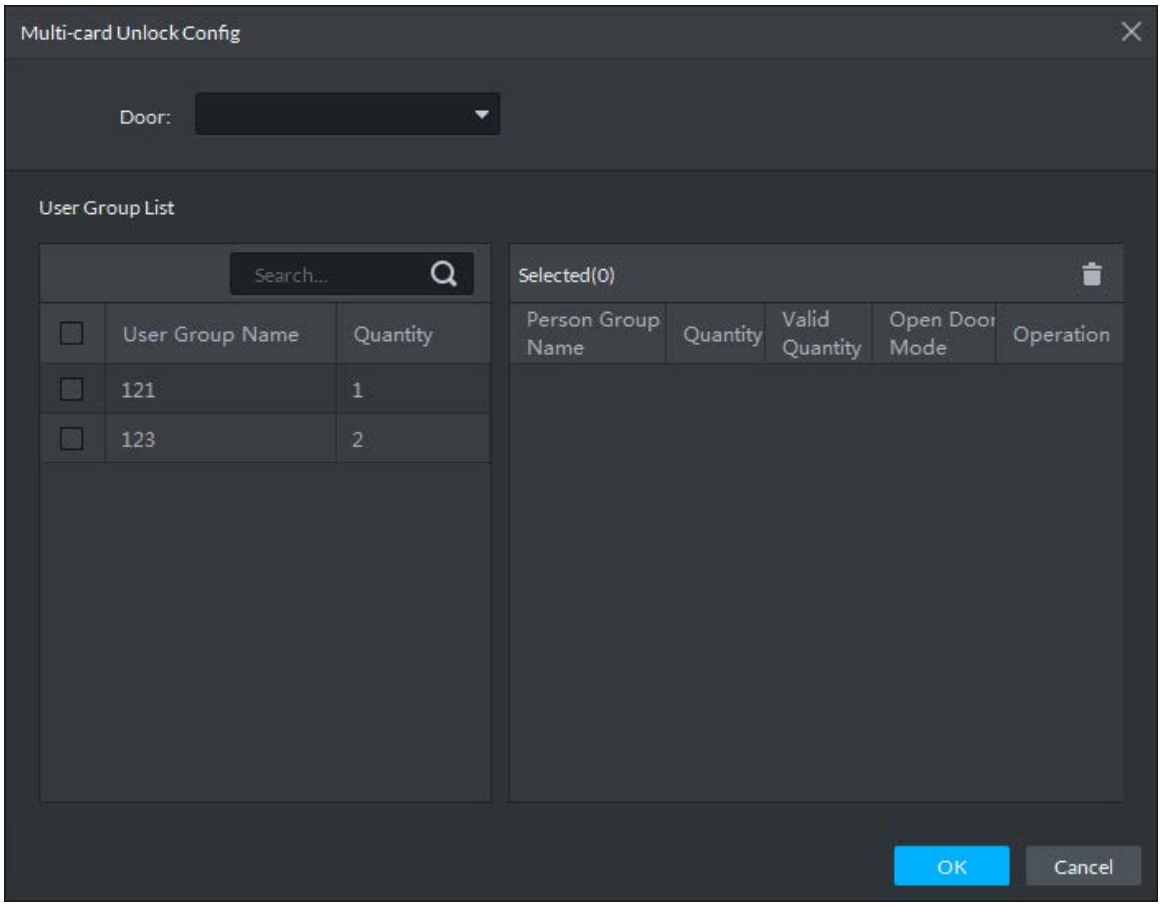
4) Click ☒ in the upper right corner of the **User Group Manager** interface.

Step 3 Config Multi-Card Unlock.

1) Click **Add**.

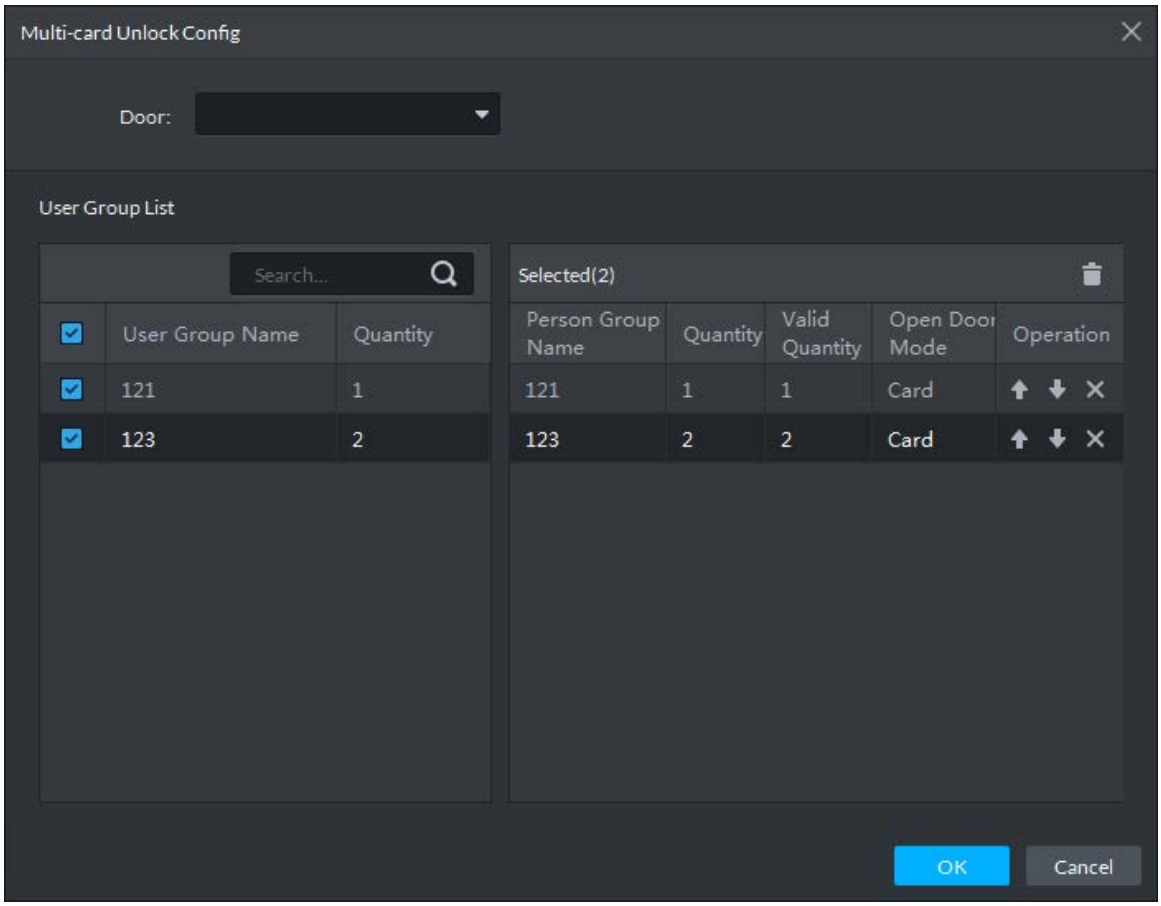
The **Multi-card Unlock Config** interface is displayed. See Figure 4-289.

Figure 4-289 Configure user group



2) Select the door to set up Multi-Card Unlock.
3) Select the user group. You can select up to four groups.
   The user group information is displayed. See Figure 4-290.

Figure 4-290 Select user group



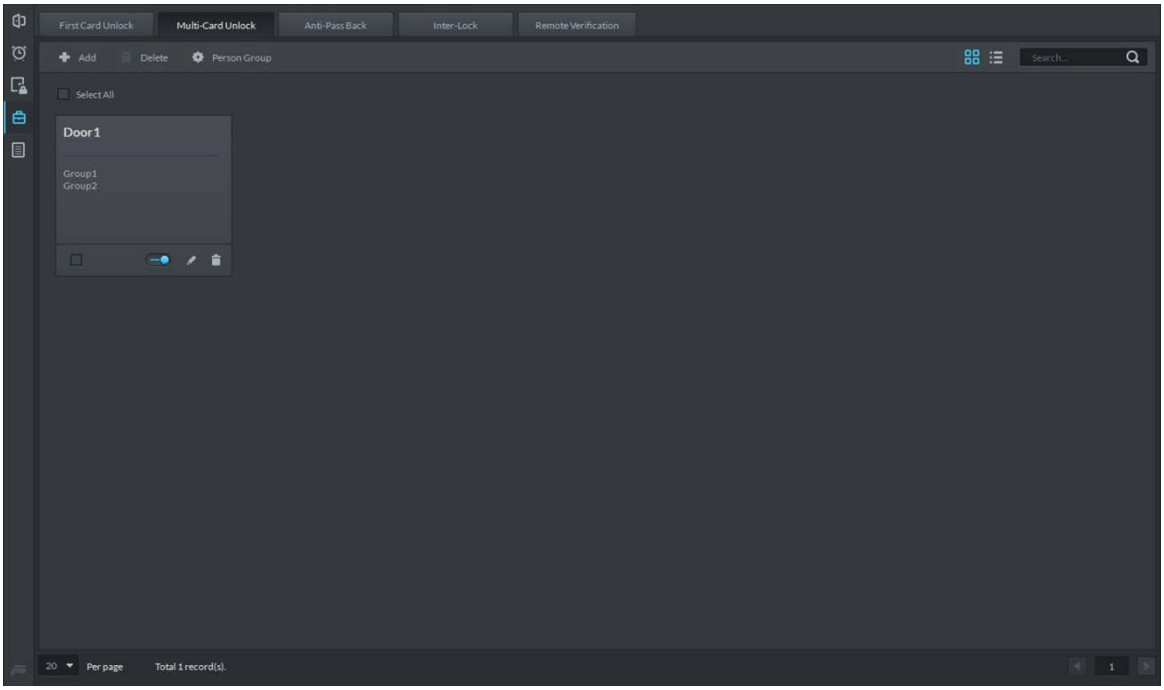
4) Fill in the **Valid Quantity** for each group to be on site and the **Open Door Mode**. Click or to adjust the user sequence for each group to unlock the door.

   The valid quantity refers to the number of users in each group that must be on site to swipe their cards.

5) Click **OK**.

   The **Multi-Card Unlock** information is displayed. See Figure 4-291.

Figure 4-291 Multi-card unlock



Step 4 Click .

The icon changing into indicates **Multi-Card Unlock** is enabled.

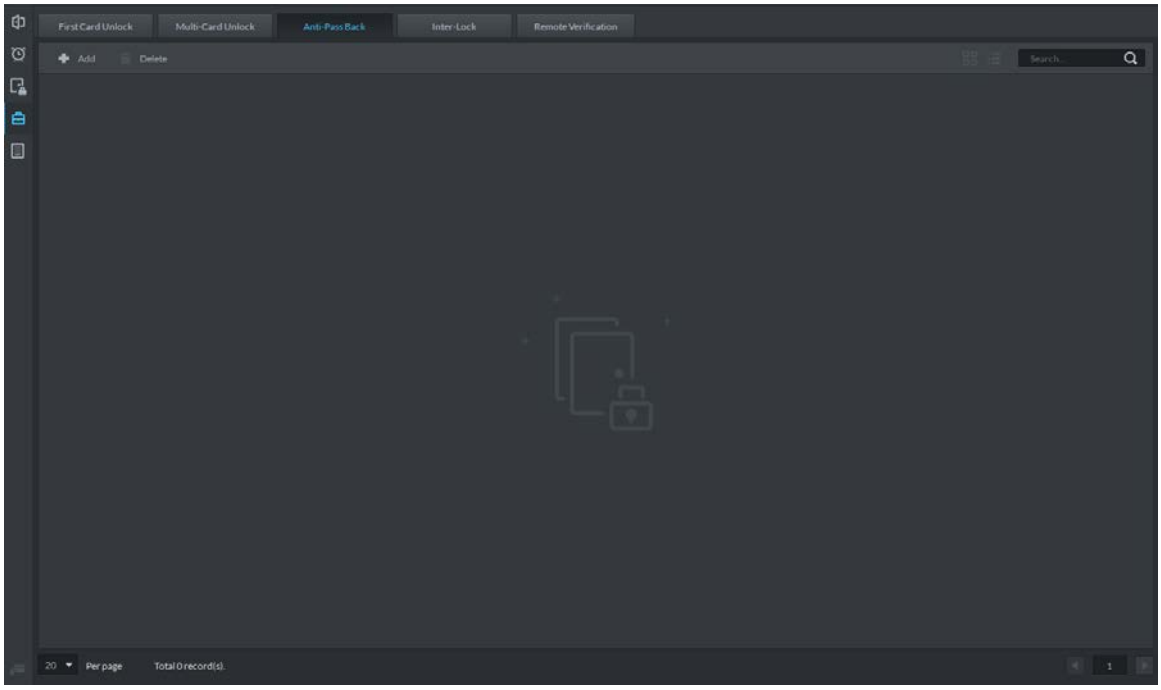
4.11.5.3 Anti-Pass Back

The Anti-Pass Back feature refers to that a user entering through a door group by verification must exit from the same door group by verification. One entry swipe must have a matching exit swipe. A non-verified user following a verified one to enter cannot pass the verification when taking exit; a non-verified user following a verified one to exit cannot pass verification when taking entry again. The door cannot be unlocked by swiping cards until the reset period on the A&C Central Controller expires.

Step 1 On the **Access Control** interface, click and select **Anti-pass Back**

The **Anti-Pass Back** interface is displayed. See Figure 4-292.

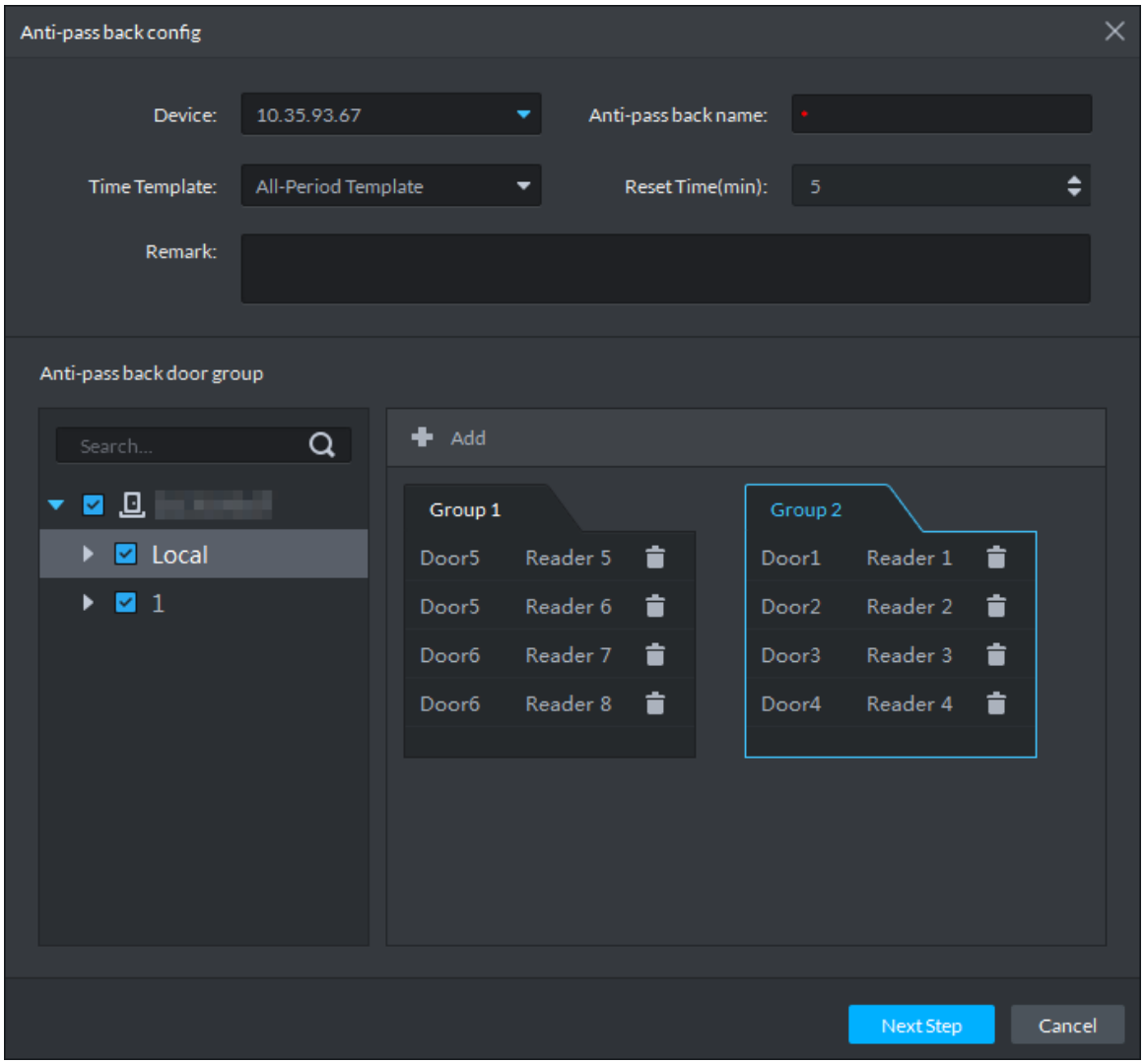
Figure 4-292 Anti-pass back



Step 2 Click **Add**.

The **Anti-pass back config** interface is displayed. See Figure 4-293.

Figure 4-293 Anti-pass back config



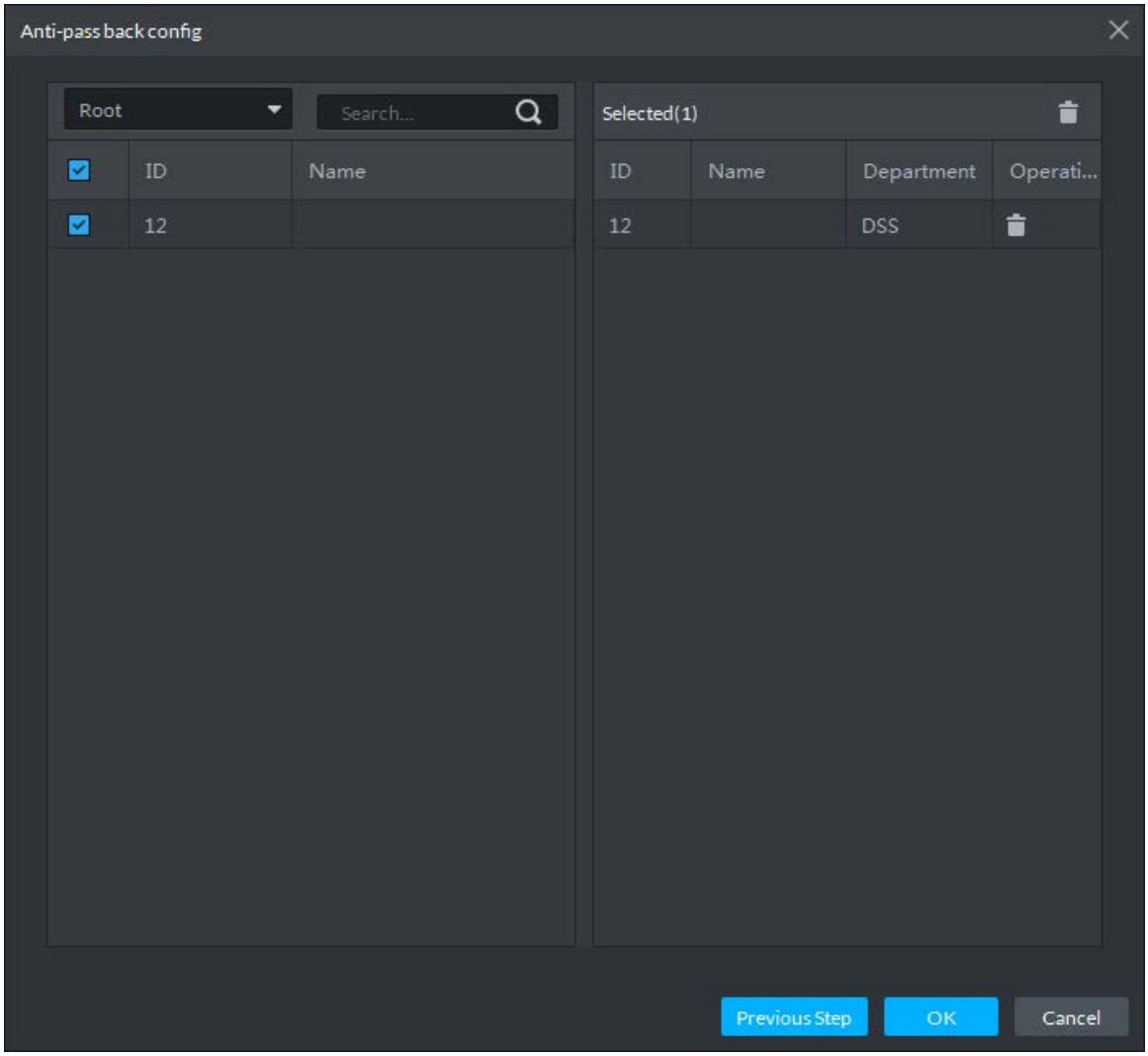
Step 3 Configure the anti-pass back parameters and click **Next Step**. For details of the parameters, see Table 4-42.

The user selection information is displayed. See Figure 4-294.

Table 4-42

Parameter	Description	
Device	You can select the device to configure the anti-pass back rules.	
Anti-pass back name	You can customize the name of an anti-pass back rule.	
Reset Time(min)	The access card becomes invalid if an anti-pass back rule is violated. The reset time is the invalidity duration.	When the selected device is a multi-door controller, you must set up these parameters.
Time Template	You can select the time periods to implement the anti-pass back rules.	
Remark	Note info.	
Group X X is a number.	The group sequence here is the sequence for swiping cards. You can add up to 16 readers for each group. Each group can swipe cards on any of the readers.	

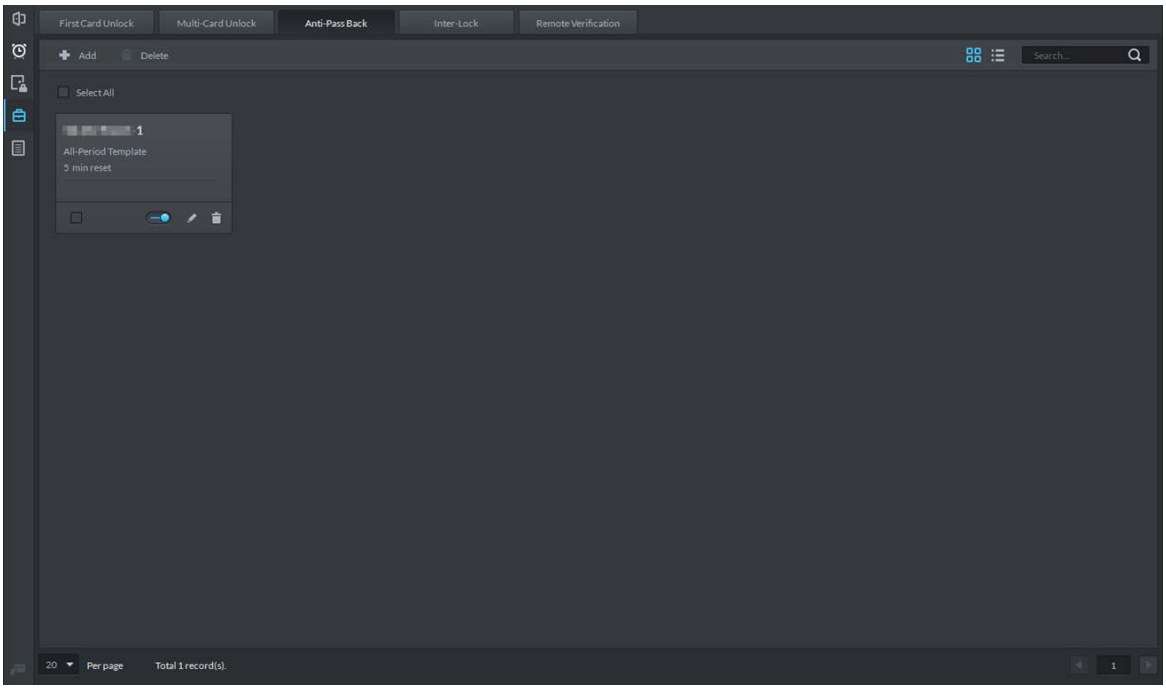
Figure 4-294 Select user



Step 4 Select users and click **OK**.

The anti-pass back information is displayed. See Figure 4-295.

Figure 4-295 Anti-pass back



Step 5 Click .

The icon changing into indicates Anti-Pass Back is enabled.

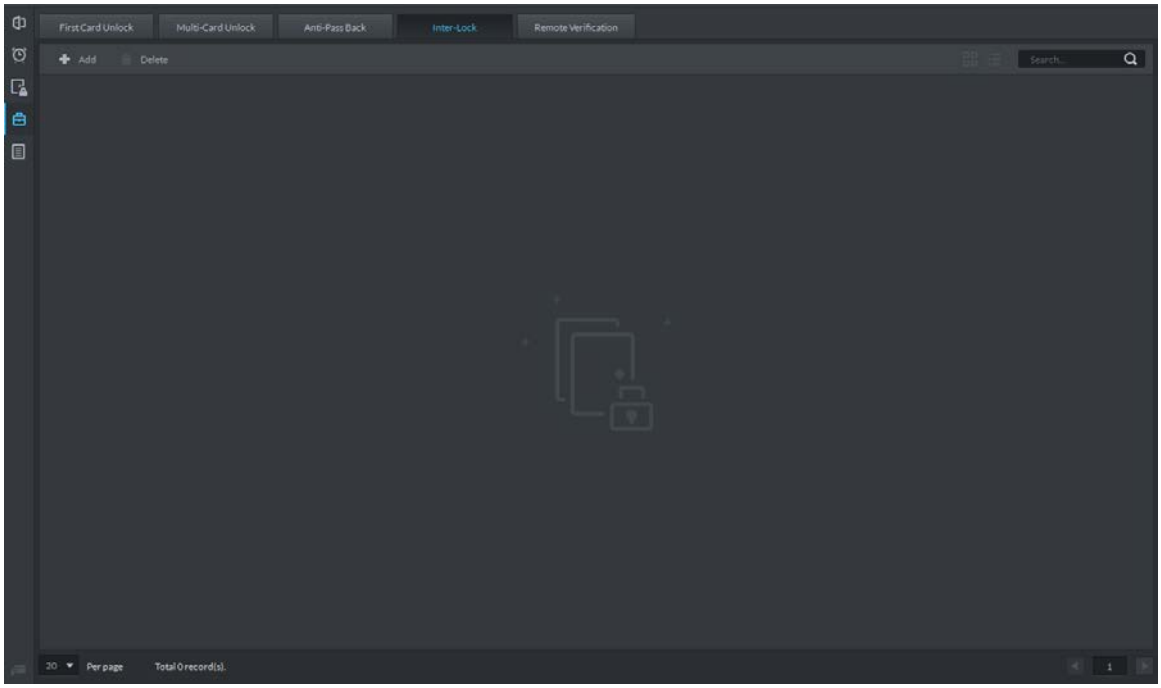
4.11.5.4 Inter-door Lock

A regular access controller employs inter-lock within the group. When one of the access control channels is opened, other corresponding channels are closed. To open one of the access control channels (under normal access control), other corresponding access control channels must be closed; otherwise the door cannot be unlocked. The A&C Central Controller employs inter-group inter-lock, where the access control channels are independent of the inter-lock and can all be opened. However, whenever an access control channel in a group is opened, no channels of other groups can be opened. The configuration steps in this chapter are for an A&C Central Controller.

Step 1 On the **Access Control** interface, click and select **Inter-lock**.

The **Inter-Lock** interface is displayed. See Figure 4-296.

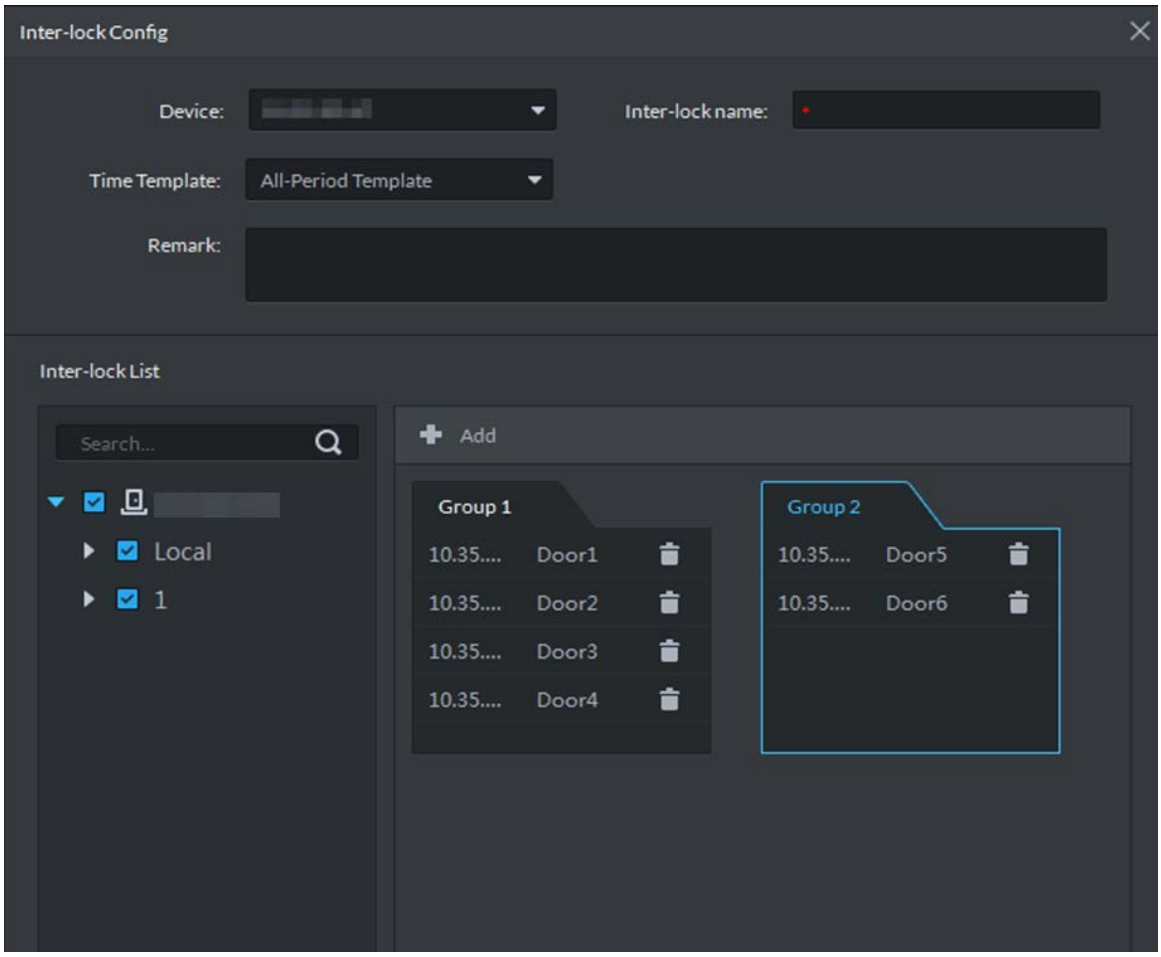
Figure 4-296 Inter-lock



Step 2 Click **Add**.

The **Inter-lock Config** interface is displayed. See Figure 4-297.

Figure 4-297 Inter-lock config

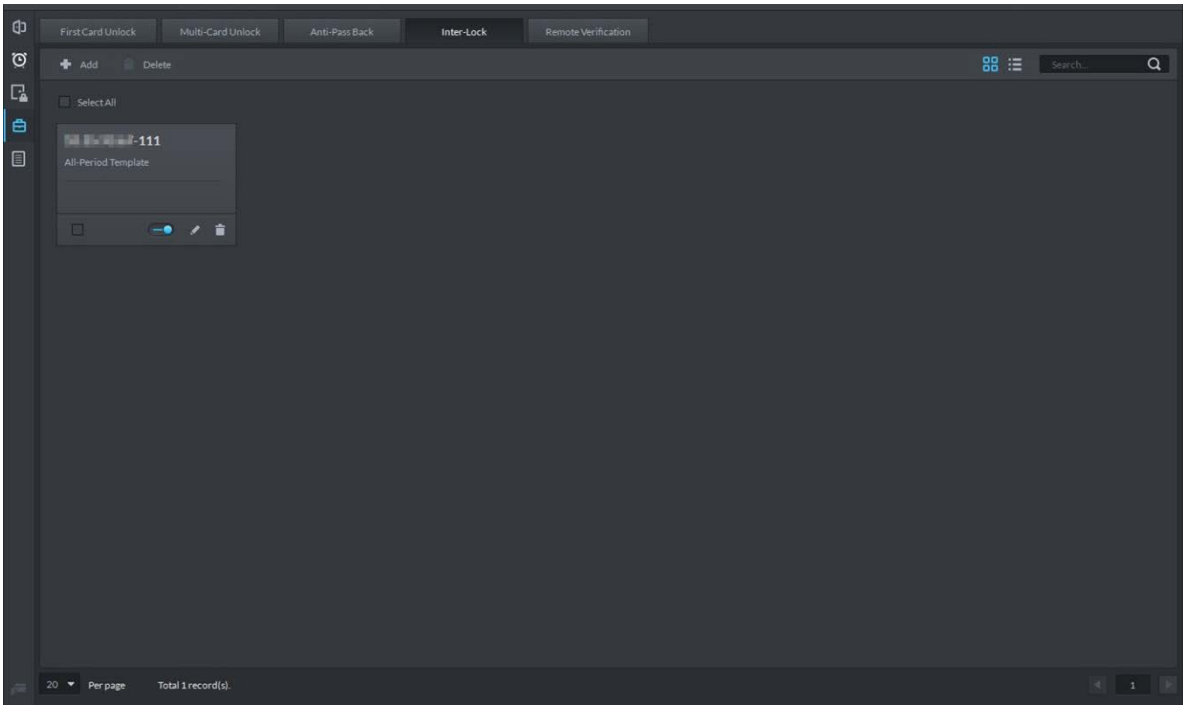


Step 3 Configure inter-lock parameters and click **OK**. For details of the parameters, see Table 4-43. The inter-lock information is displayed. See Figure 4-298.

Table 4-43 Inter-lock config

Parameter	Description	
Device	You can select the device to set up inter-lock.	
Inter-lock name	You can customize the name of the inter-lock rule.	
Time Template	You can select the time period to implement inter-lock.	When the selected device is a multi-door controller, you must set up these parameters.
Remark	Note info.	
Group X X is a number.	You can set up inter-lock across different door groups. If a door in Group 1 is opened, no doors can be opened in Group 2 until all doors in Group 1 are closed. Supports up to 16 door groups, with up to 16 doors in each group.	

Figure 4-298 Inter-lock list



Step 4 Click .

The icon changing into indicates Inter-Lock is enabled.

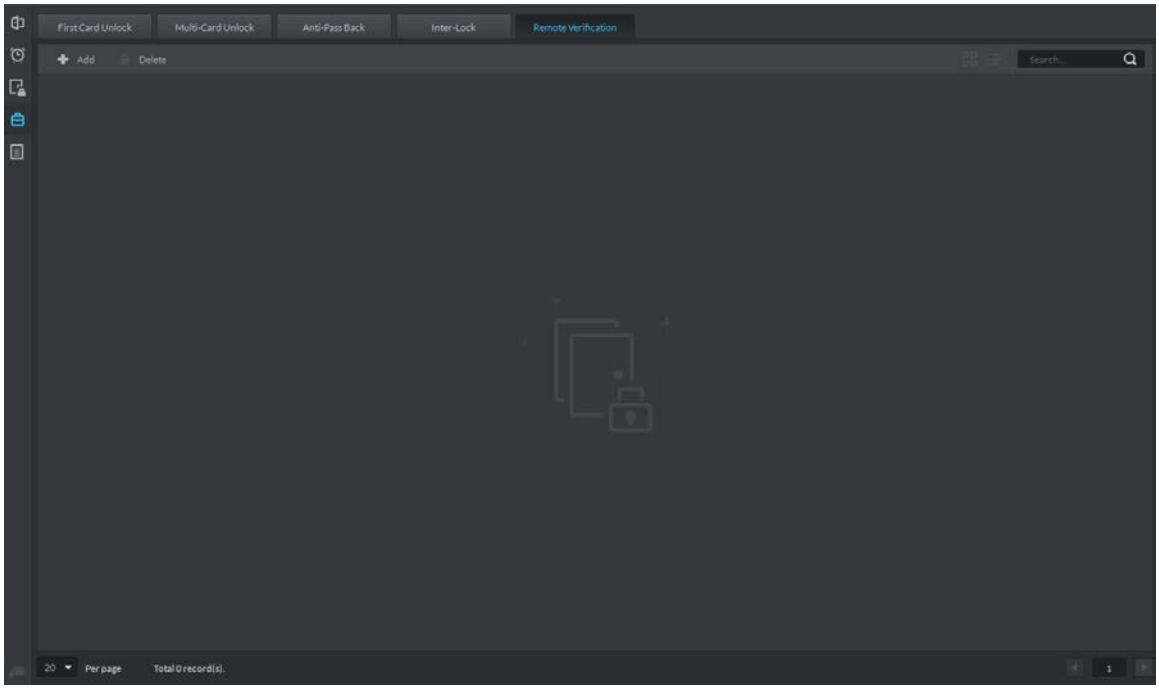
4.11.5.5 Remote Verification

For devices with remote verification, when users unlock the doors with card, fingerprint, or password in the specified time period, it must be confirmed on the platform client before the access controller can be opened.

Step 1 On the **Access Control** interface, click and select **Remote Verification**.

The **Remote Verification** interface is displayed. See Figure 4-299.

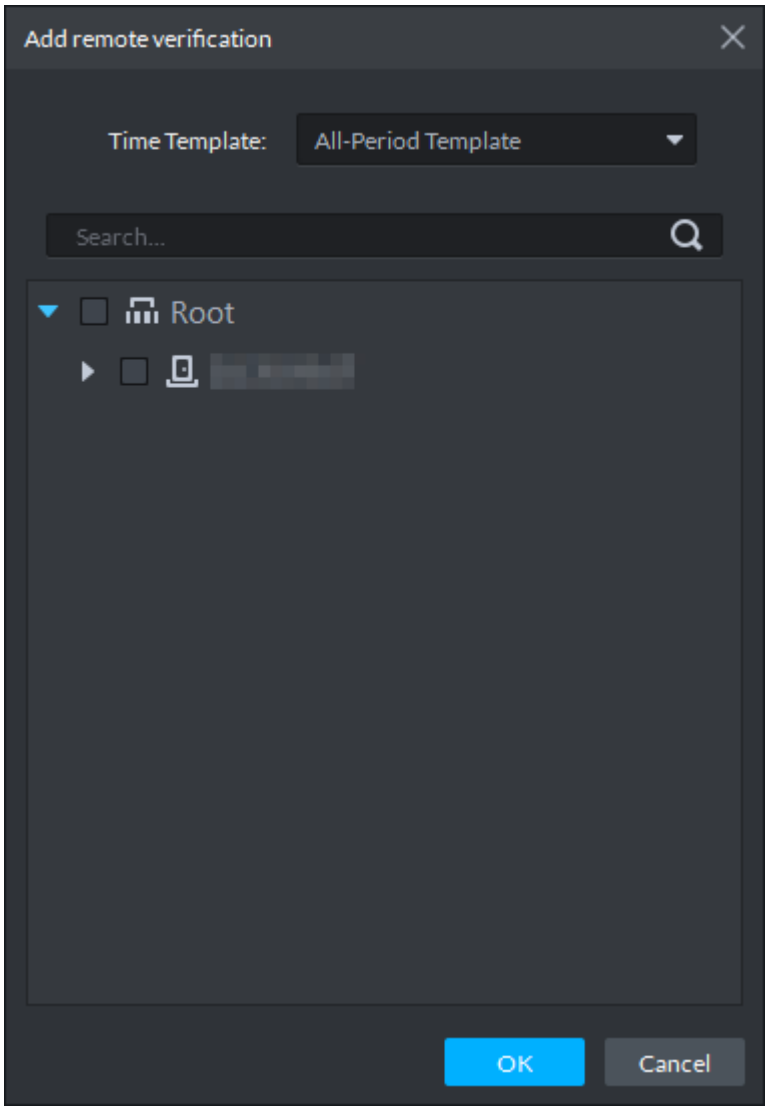
Figure 4-299 Remote verification



Step 2 Click **Add**.

The **Add remote verification** interface is displayed. See Figure 4-300.

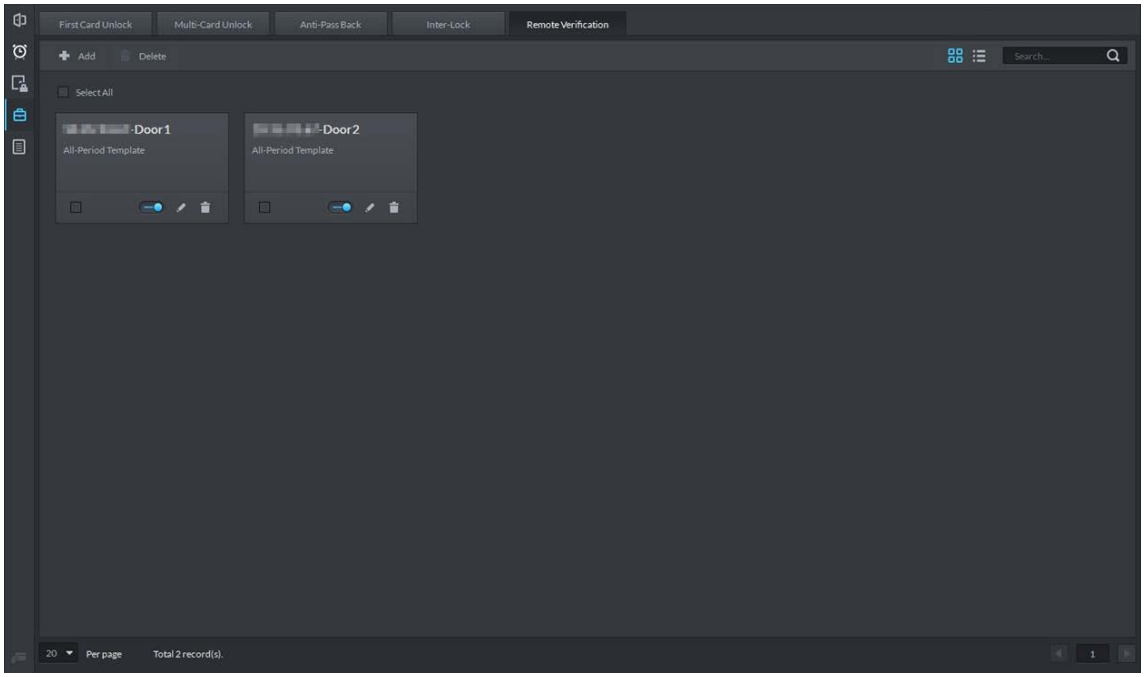
Figure 4-300 Add remote verification



Step 3 Select **Time Template** and access control channel, and click **OK**.

The remote verification information is displayed. See Figure 4-301.

Figure 4-301 Remote verification list



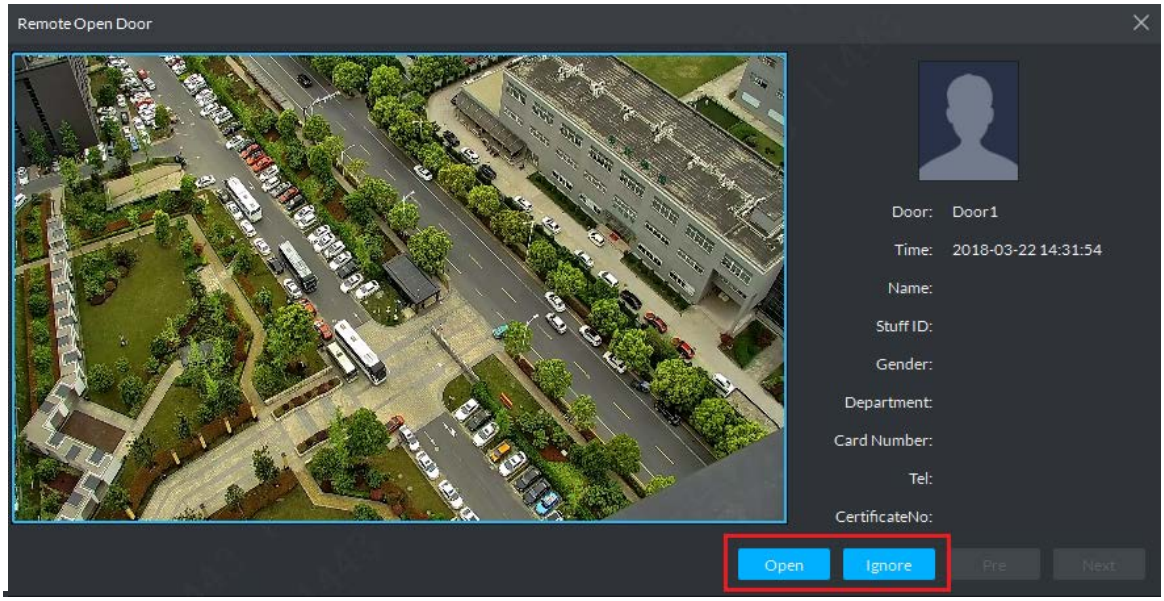
Step 4 Click  .

The icon changing into  indicates First Card Unlock is enabled.

Step 5 After the setup, door unlocking by card, fingerprint, or password that takes place in the corresponding access control channel triggers a popup on the client. See Figure 4-302.

Step 6 You can choose to unlock the door or ignore it by clicking the corresponding button, and the popup automatically disappears.

Figure 4-302 Remote open door



4.11.6 Setting Record Plan

Video before and after alarm can be stored only when record storage plan is configured, and the platform can play video 10 seconds before and after event alarm. If you want to set record storage plan, see"4.1.5 Setting Record Plan."

4.11.7 Configuring Super Password

2nd generation access control supports using super password to open door. You only need to enter super password to open door.

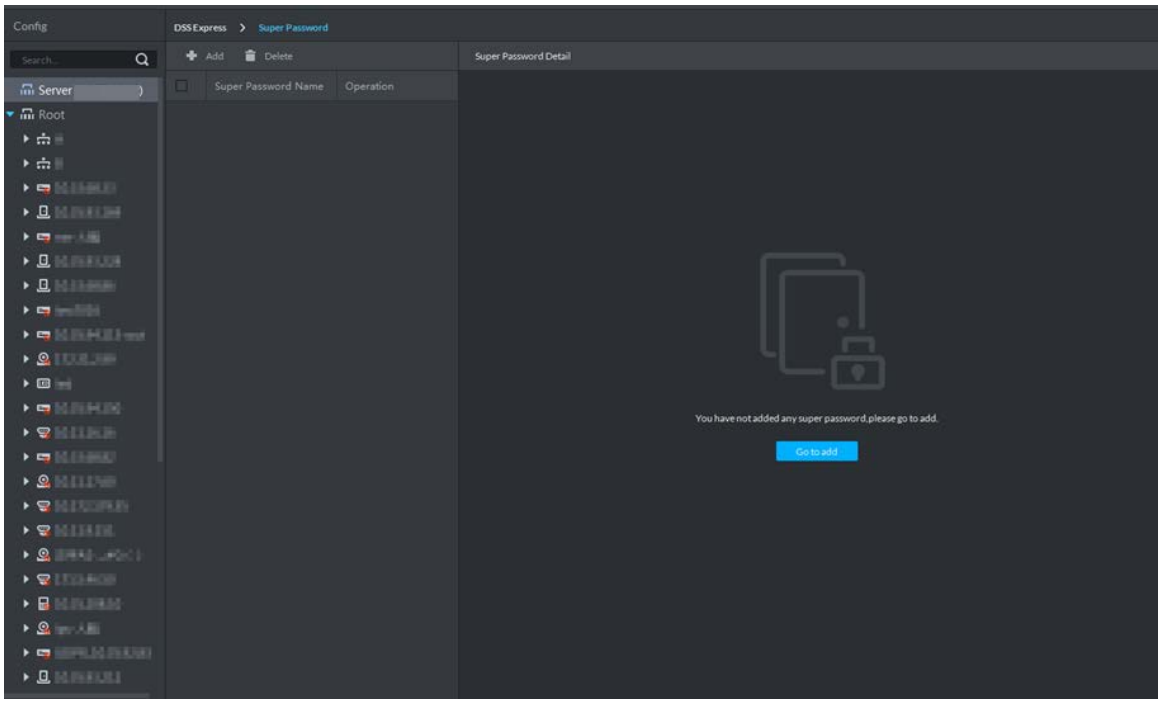
Step 1 On client homepage, click **Config**.

The **Config** interface is displayed.

Step 2 Click **Super Password**.

The **Super Password** interface is displayed. See Figure 4-303.

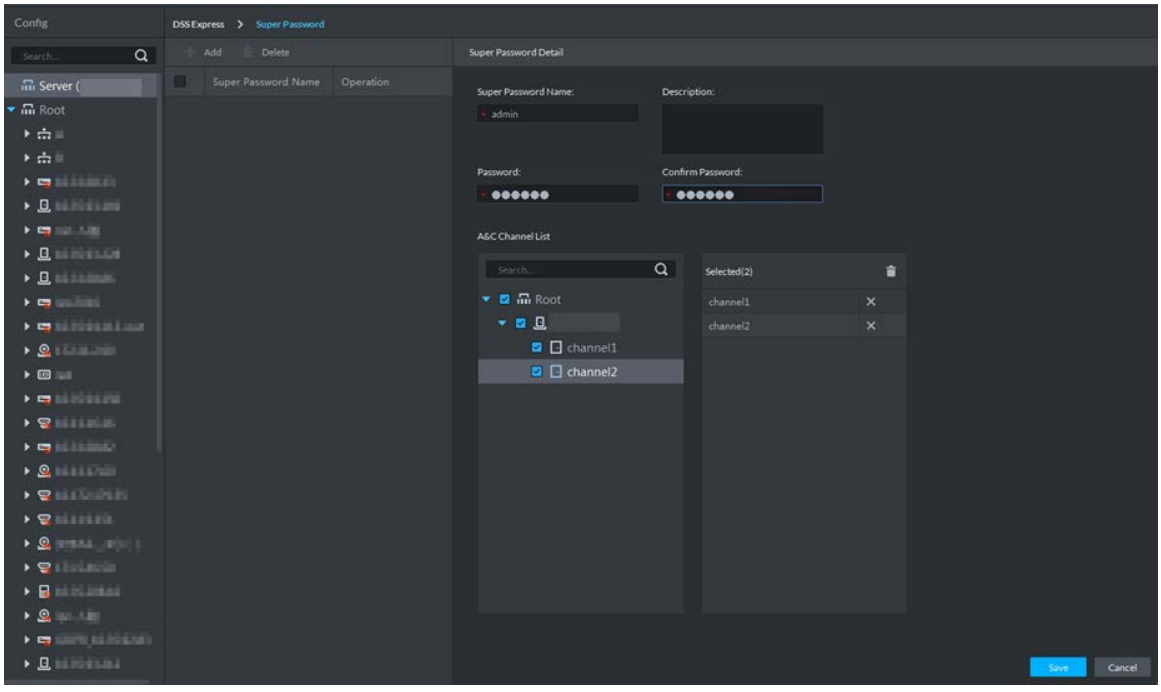
Figure 4-303 Super password



Step 3 Click **Add**.

The interface of adding super password is displayed. See Figure 4-304

Figure 4-304 Add super password



Step 4 After setting super password, you can select AC channel (only supported by 2nd generation device), click **Save** and complete config.

4.11.8 Access Control Application

You can control lock, unlock and view related video and event info on console, and enter door config interface.

4.11.8.1 Viewing Video of Bound Channel

When adding access control devices, if you have already bound a video channel to the channel, you can preview the real-time videos of the bound video channels on the console. To bind video channels, see"4.11.1 Adding Access Control."

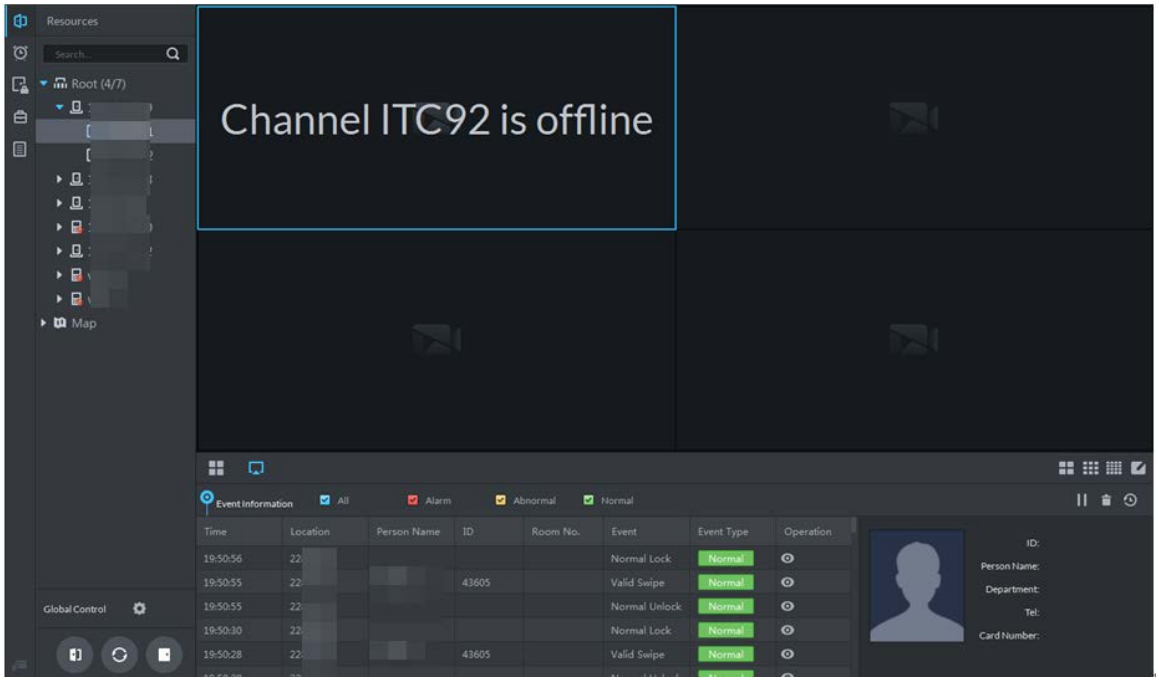
Step 1 On client homepage, click **Access Control**.

The **Access Control** interface is displayed.

Step 2 Click  .

The **Console** interface is displayed. See Figure 4-305.

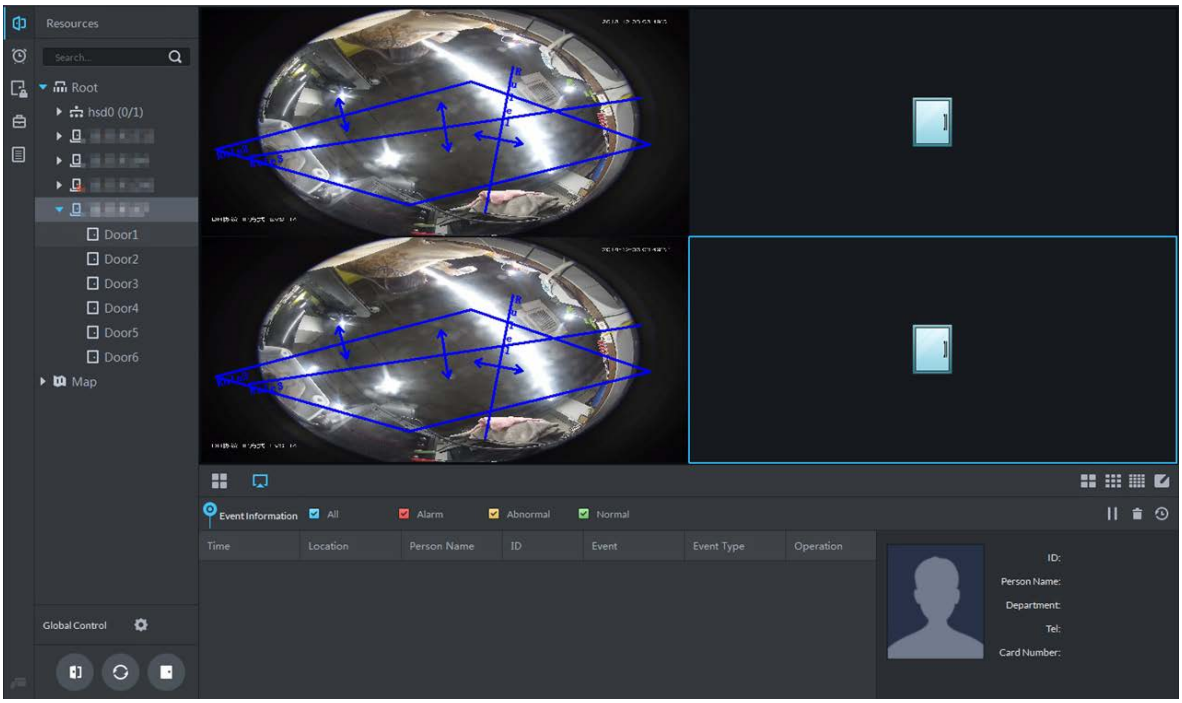
Figure 4-305 Console



Step 3 View related video of AC channel.

- On the right side of the console interface, click  in the access control channel list. The videos in real time is displayed. See Figure 4-306
- Click  on the console interface. The video interface is displayed. 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 4-306

Figure 4-306 Linked channel video



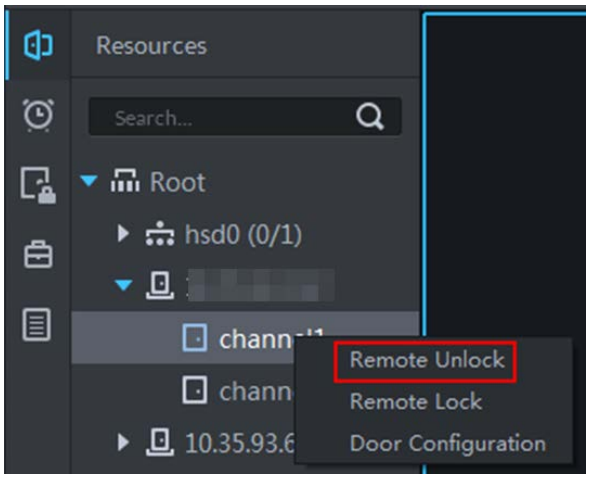
4.11.8.2 Manual Unlock

In addition to **Always Open** or linked unlock in specified periods, the console also supports unlocking by manually controlling the access control channel. After unlock, the door automatically locks up after a specified time period (5s by default, and 10s in this example) set up in Door Config.

You can unlock the door in the following ways:

- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Unlock** in the popup menu. See Figure 4-307. After unlocking, the door status in the access control channel list on the right side of the interface changes to open, as  .

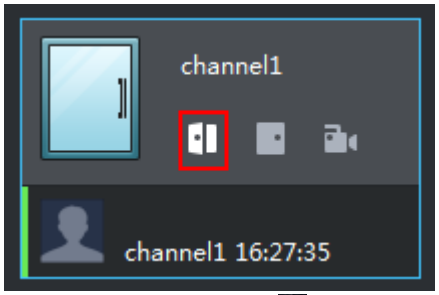
Figure 4-307 Remote unlock (1)



- Click  on the door channel interface to unlock the door. See Figure 4-308. After unlocking, the door status in the access control channel list on the right side of the interface changes to

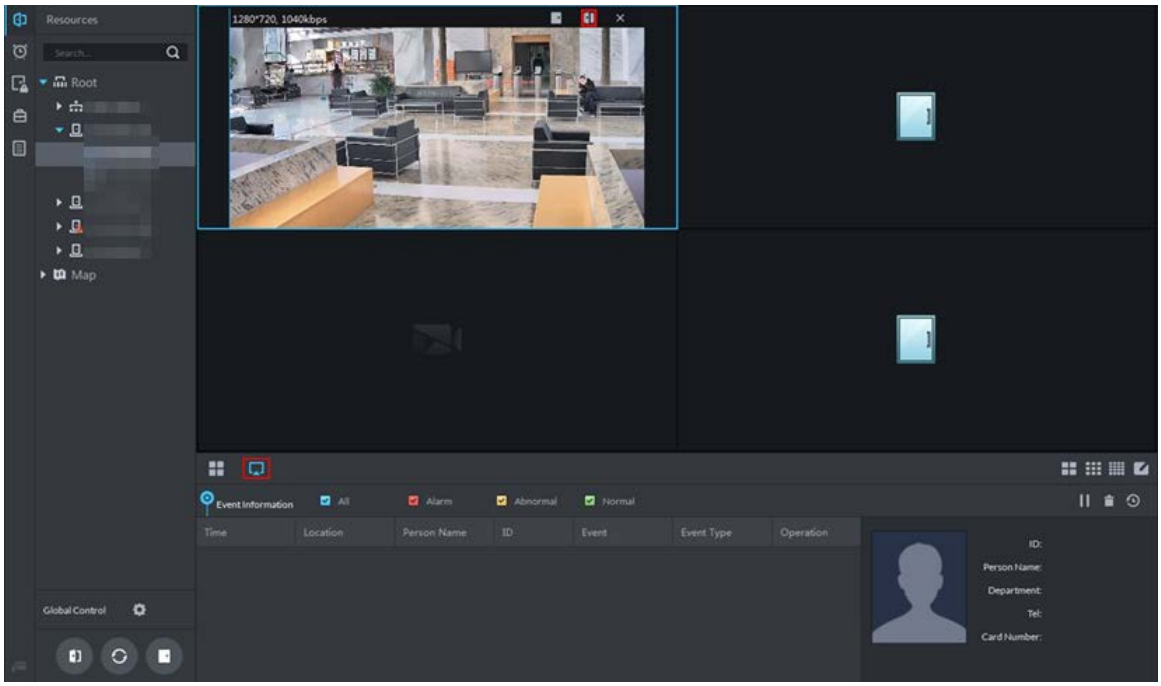
open, and the icon changes to .

Figure 4-308 Unlock (2)



- When viewing videos bound to the channel, click on the video interface to unlock the door. See Figure 4-309.

Figure 4-309 Unlock (3)



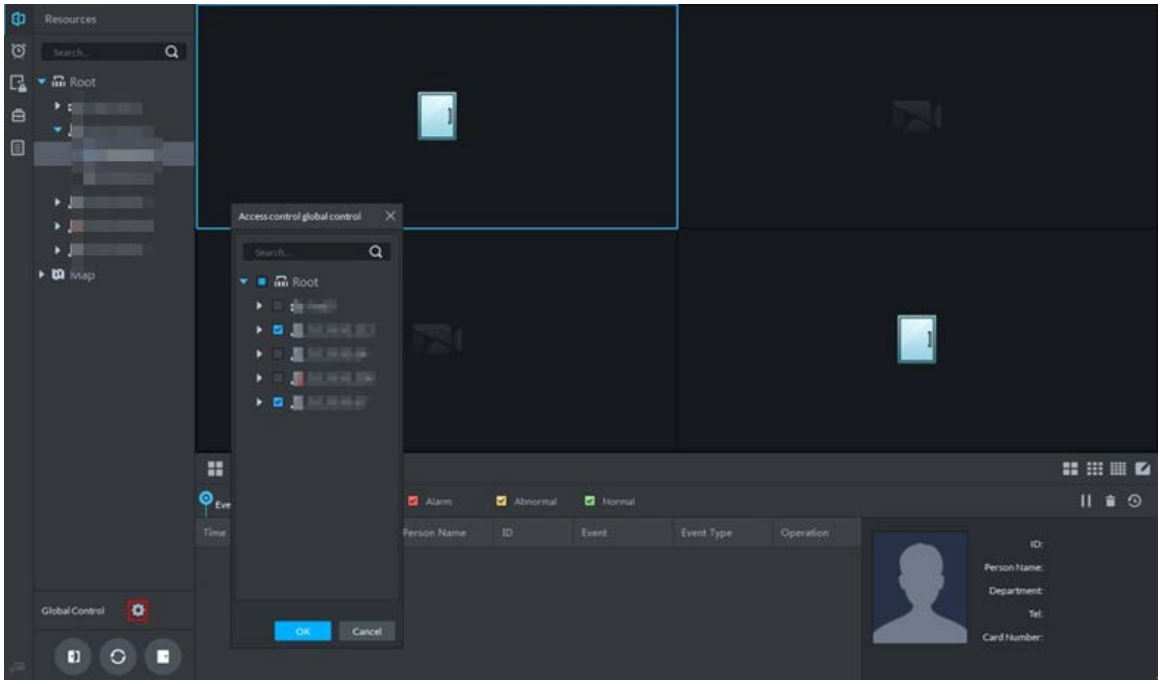
- Temporary Always Open of multiple doors

  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 4-310.

Figure 4-310 Global control



Step 3 Select an access control channel to be set to Always Open through 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**.

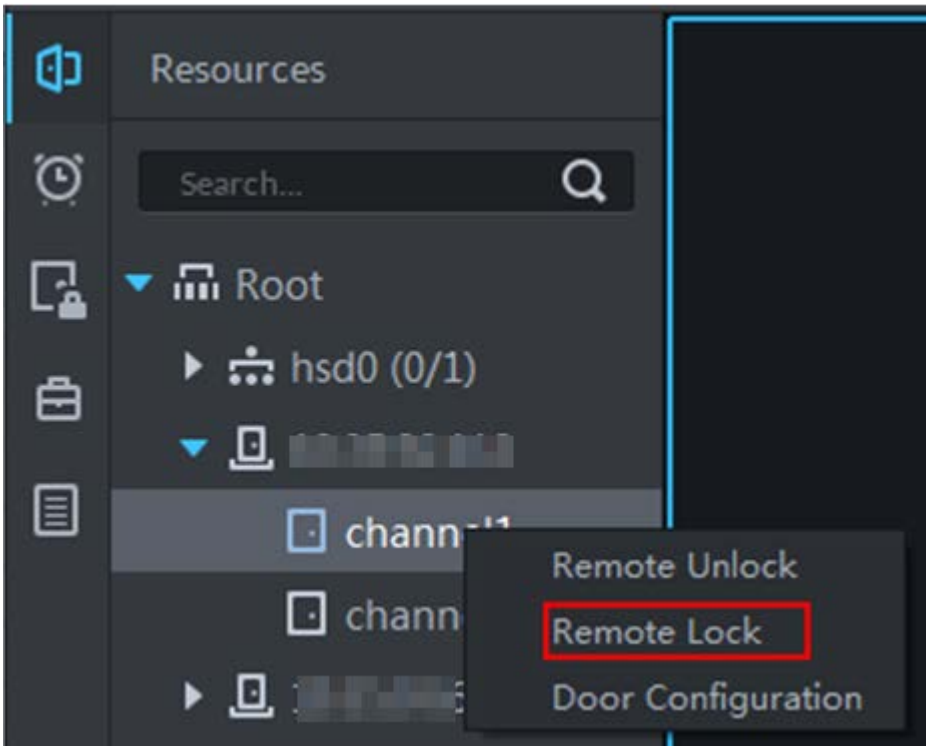
Click **Recover** and the doors return to normal status.

4.11.8.3 Manual Lock

In addition to Always Close or linked lock in specified periods, the console also supports locking by manually controlling the access control channel. You can lock the door in the following ways:

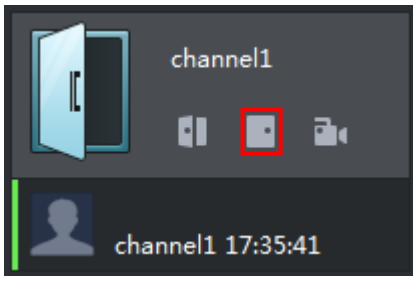
- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Lock** in the popup menu. See Figure 4-311. After locking, the door status in the access control channel list on the right side of the interface changes to closed, as  .

Figure 4-311 Lock (1)



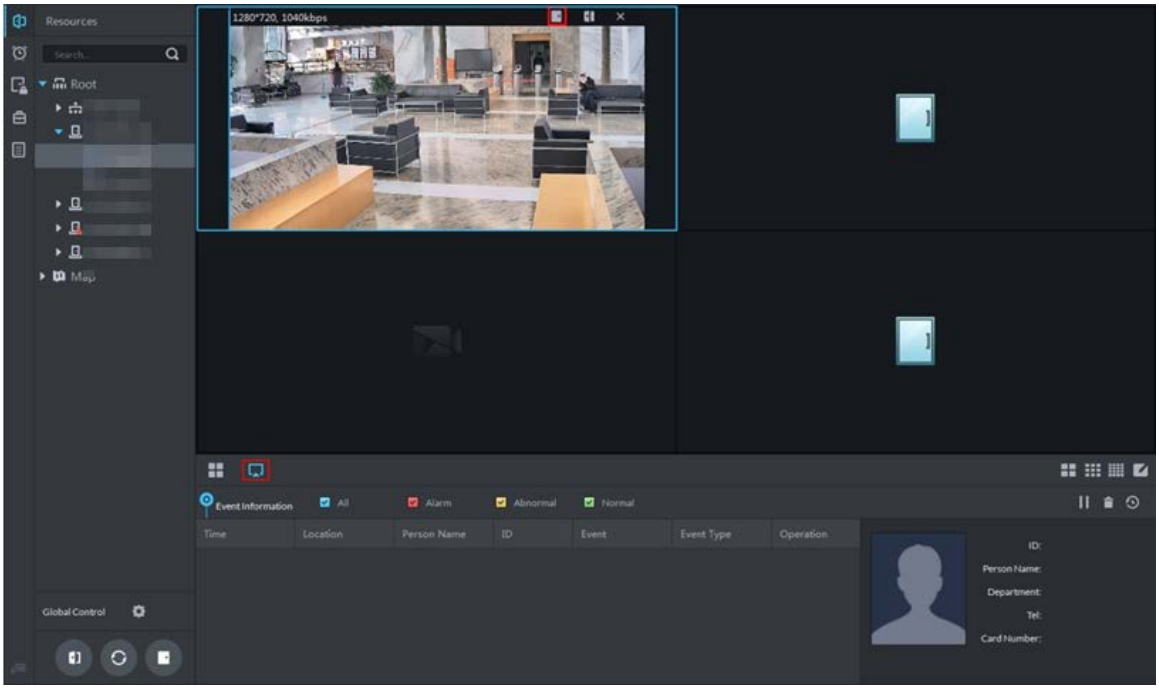
- Click on the door channel interface to lock the door. See Figure 4-312. After locking, the door status in the access control channel list on the right side of the interface changes to closed, as .

Figure 4-312 Lock (2)



- When viewing videos bound to the channel, click on the video screen to lock the door. See Figure 4-313.

Figure 4-313 Lock (3)

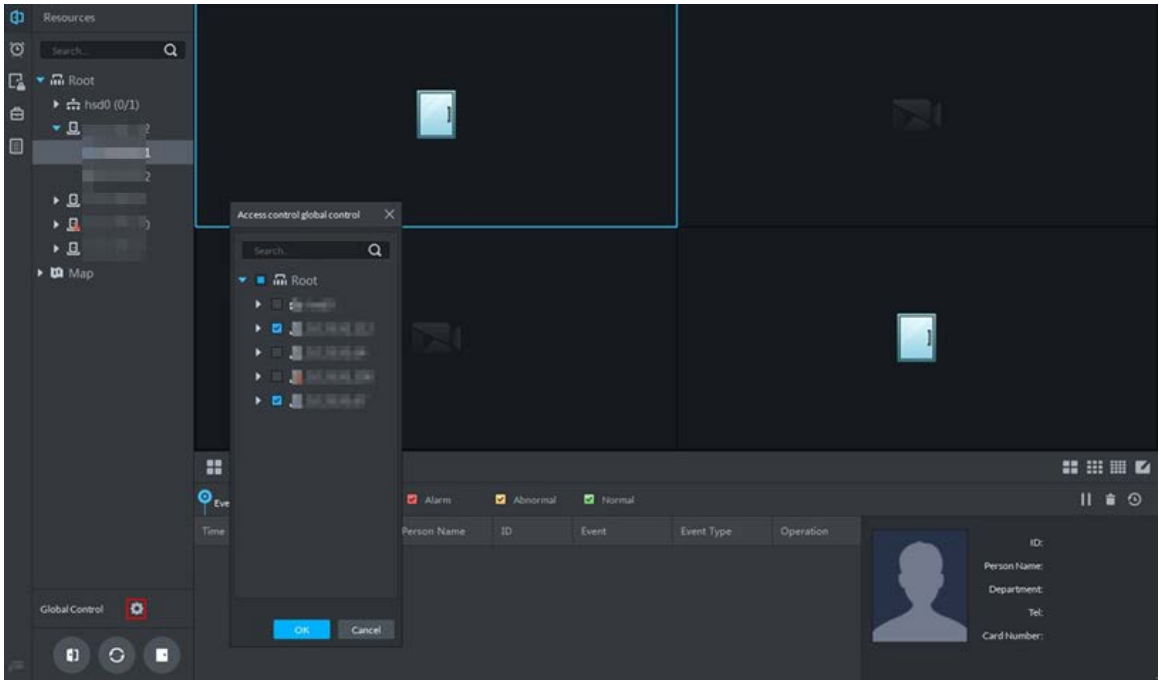


- Temporary Always Open of multiple doors
  Select a door channel through global control and you can set the door to be Always Close. Recovery to normal status after locking requires manual operations.

Step 1 Click  on the bottom left of the console interface of the Access Control module.

The **Access control global control** interface is displayed. See Figure 4-314.

Figure 4-314 Global control



Step 2 Select an access control channel to be set to Always Close through global control, and click **OK**.

Step 3 Click **Always Close** on the bottom left of the interface.

The **Password Verification** interface is displayed.

Step 4 Input current user's password, and click **OK**.

Step 5 All the doors of the selected access control channels are set to Always Close. The status of all the doors in the access control channel list on the right side of the interface changes to closed, as  . The interface control changes from **Always Close** to **Recover**.

Click **Recover** and the doors return to normal status.

4.11.8.4 Viewing Event Details

Supports viewing details of the events reported on door locking and unlocking, including: Event Info, Live View, Snapshot, and Recording.

- Live View is only available when a video channel is bound to the access control channel. To bind video channels, see"Step 2 Bind Resources" in"4.11.1 Adding Access Control."
- When snapshot and video recording require configuring event management, access control-related alarm devices are linked with the camera.
- The console displays all event information except for locking related info, including unlock, duress unlock, invalid swipe.

Step 1 In the event list below the console interface, click  next to the event records.

Step 2 The **AC Event Info** interface is displayed. See Figure 4-315. See Table 4-44 for more descriptions on the controls.

Figure 4-315 Event detail

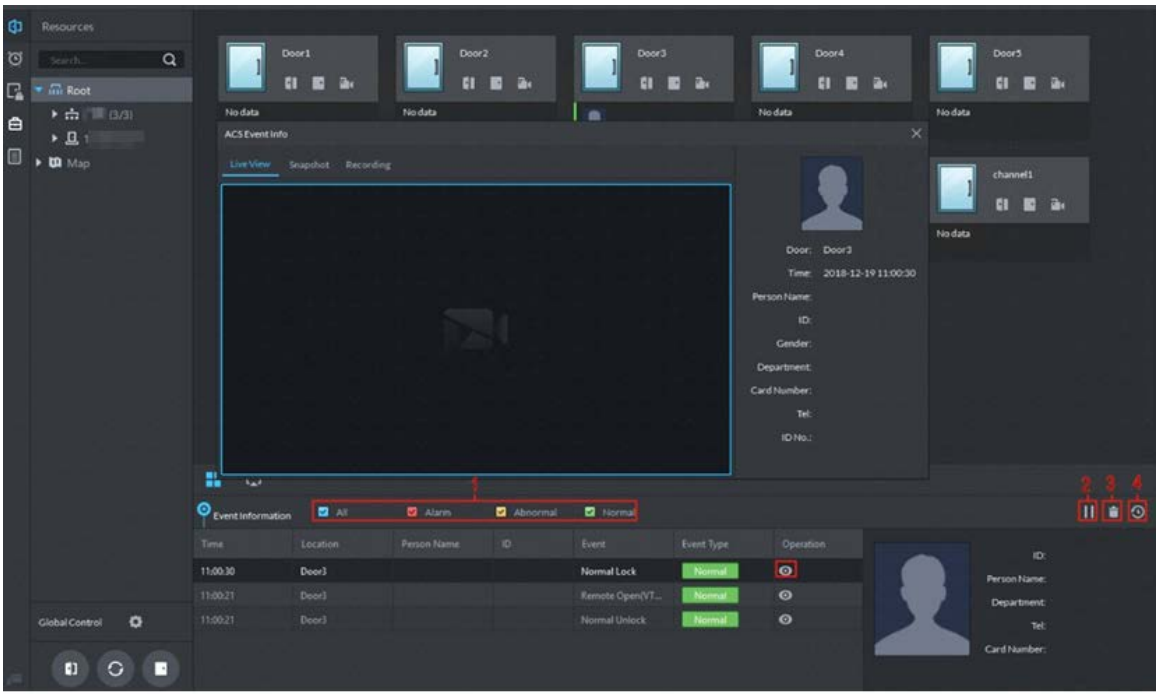


Table 4-44 Operation description

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.

4.11.9 Searching Access Control Log

You can view the reported AC log and device local log.

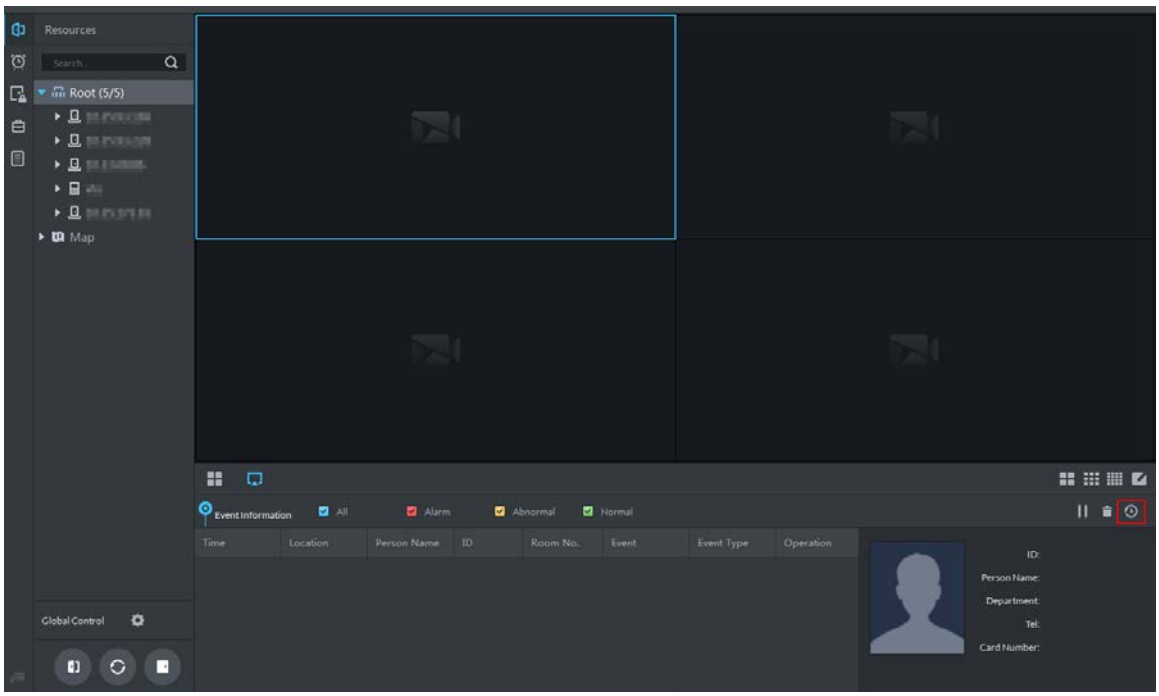
4.11.9.1 Searching Logs on Platform

Step 1 Enter AC log interface.

Supports following two methods.

- On **Access Control** interface, click .
- On **Access Control** interface, click and enter console, click and see Figure 4-316.

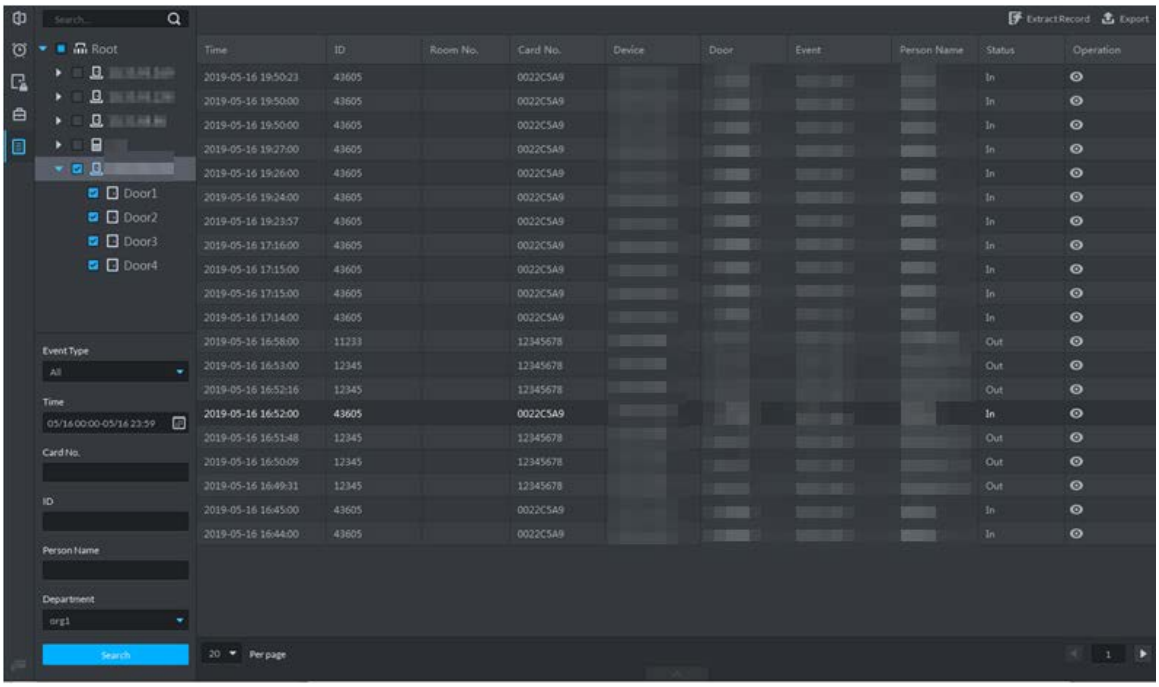
Figure 4-316 Enter AC log interface



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

The log info is displayed. See Figure 4-317.

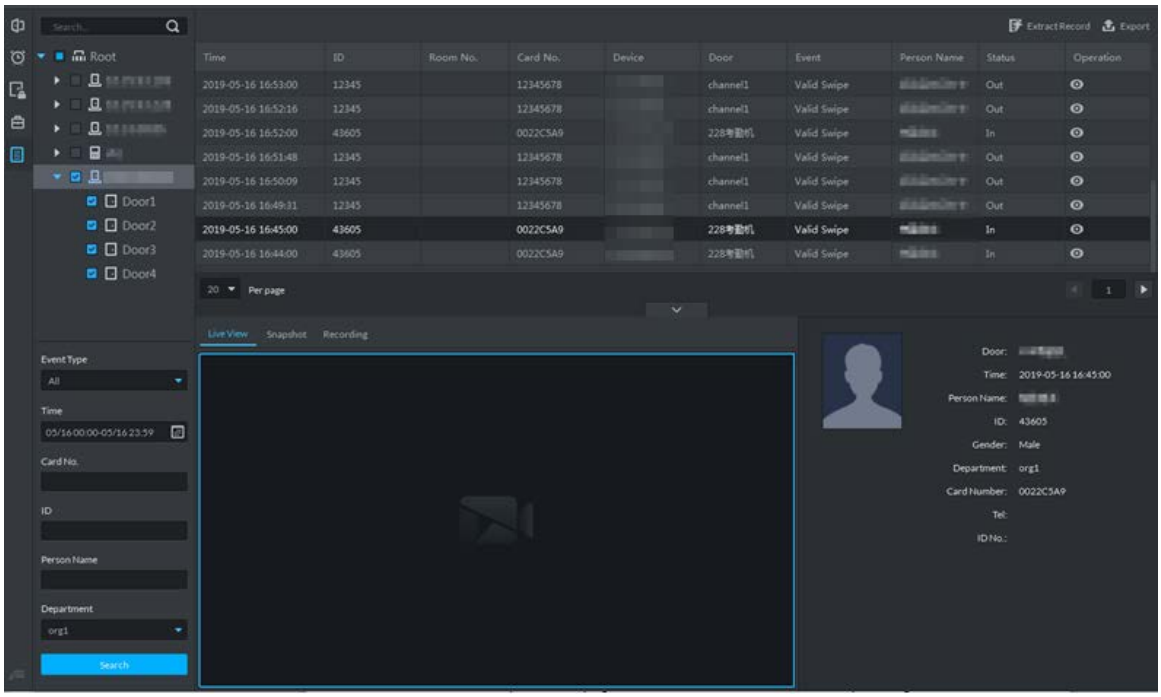
Figure 4-317 Search AC log



Step 3 Click .

The system displays AC info and live view, snapshot and record of linked video channel. See Figure 4-318.

Figure 4-318 AC log details



Step 4 Click **Export** and save log to local according to system prompt.

4.11.9.2 Extracting Log during Device Offline

If device is offline during application, you can extract offline AC logs to platform.

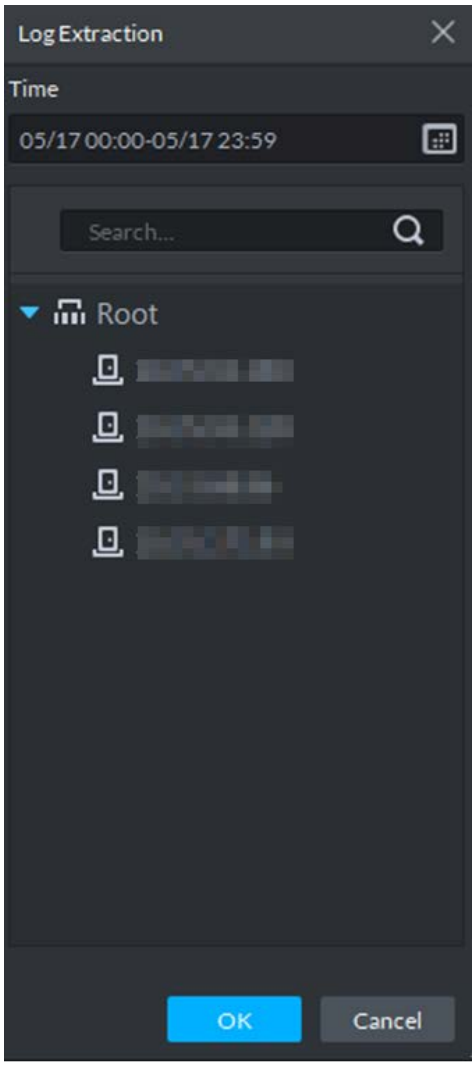
Step 1 Enter AC log interface.

Supports following two methods.

- On **Access Control** interface, click .
- On **Access Control** interface, click and enter console, click and see Figure 4-316.

Step 2 Click Extract Record on upper right corner.

Figure 4-319 Extract logs during device offline



Step 3 Click and set period.

Step 4 Click and display AC devices, select channel.

Step 5 Click **OK**.

The extracted logs is displayed.

4.11.9.3 Searching Device Logs

You can search log info of AC device.

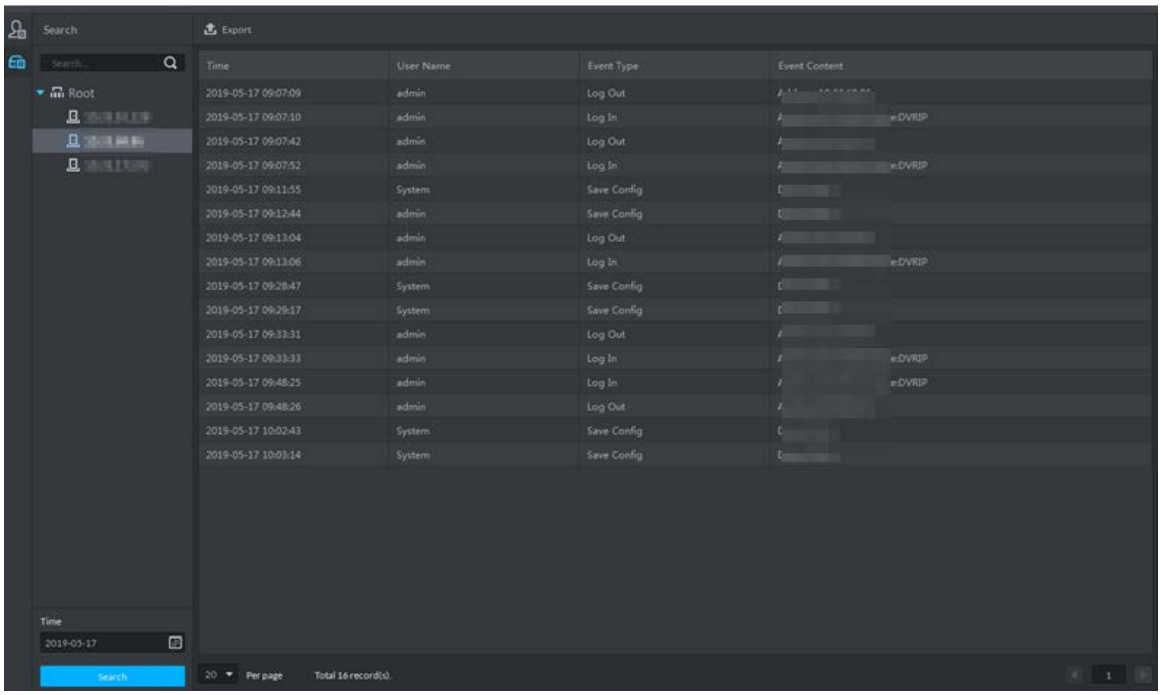
Step 1 On client homepage, click **Log**.

The **Log** interface is displayed.

Step 2 Click  .

The **Device Log** interface is displayed. See Figure 4-320.

Figure 4-320 Device log



Step 3 Select AC device and time, click **Search**.

The search results are displayed.

4.11.10 AC Device Maintenance

Support update or AC device reboot by platform. Please skip the chapter if you do not need to update or restart AC device.

4.11.10.1 Updating AC Device

You can update AC device remotely by platform. Before update, please make sure you have acquired AC device program, otherwise, please contact technical support for the program.

Step 1 On client homepage, click **Config**.

The **Config** interface is displayed.

Step 2 In left device tree, select AC device, click **Device Update** and see Figure 4-321.

The **Device Update** interface is displayed. And version info of AC device. See Figure 4-322.

Figure 4-321 Enter device update interface

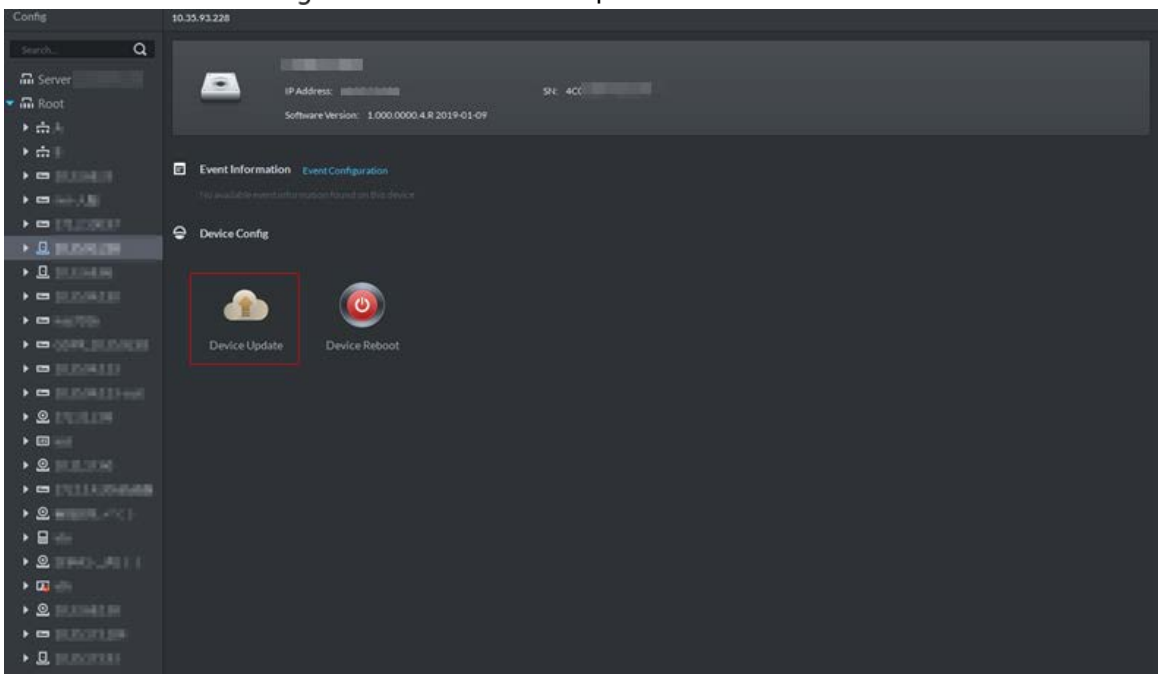
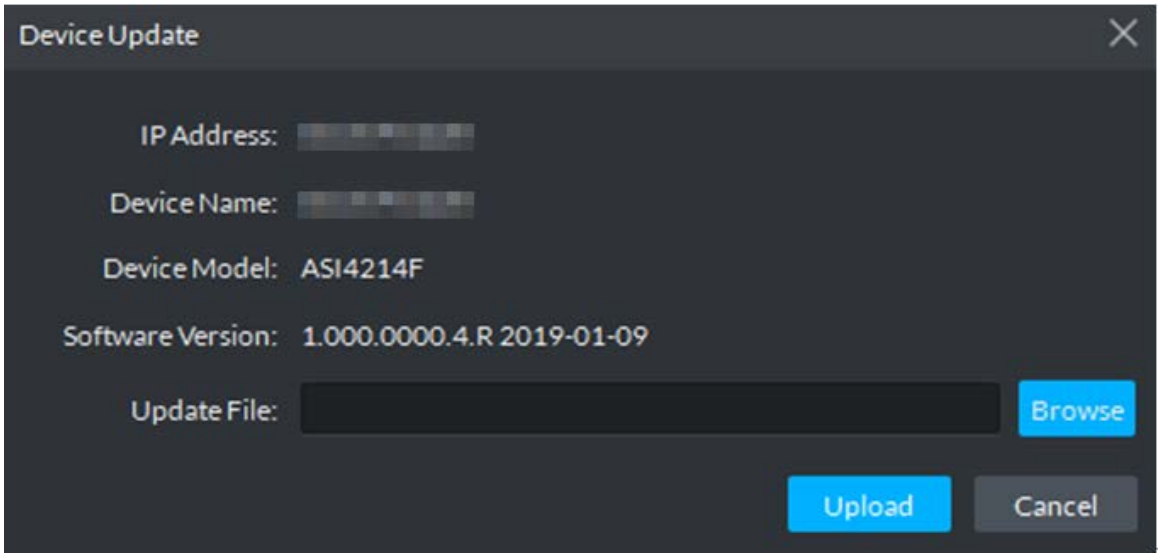


Figure 4-322 Device update



Step 3 Click **Browse** and select update file.

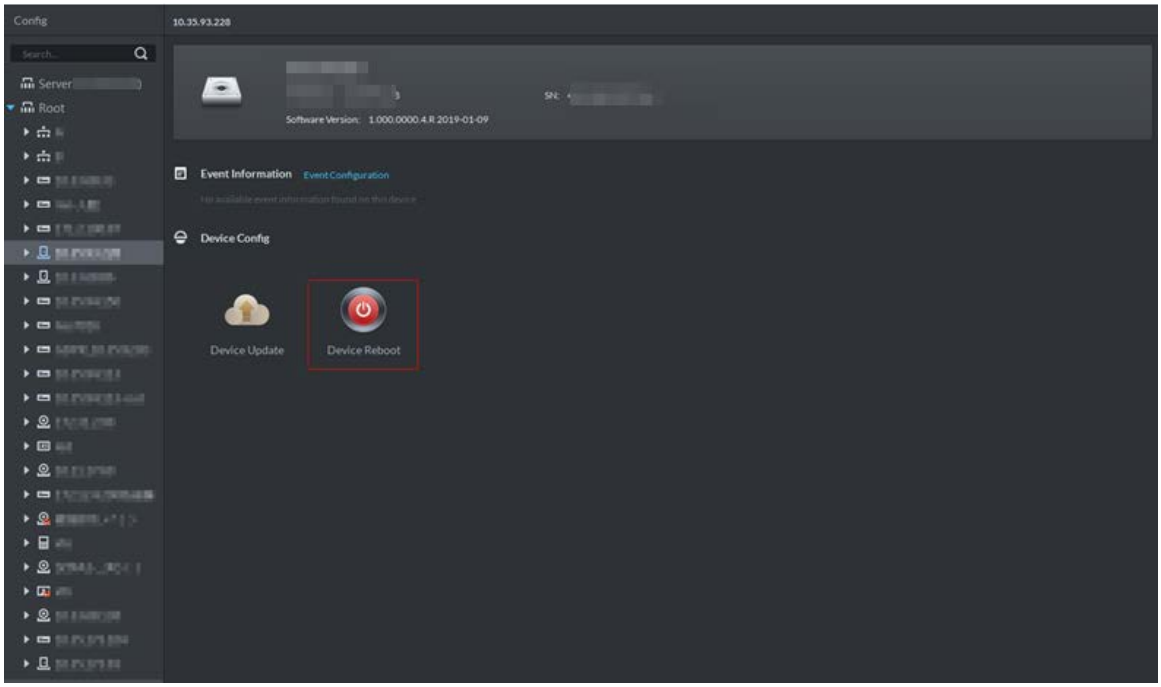
Step 4 Click **Upload** and update AC device.

4.11.10.2 Rebooting AC Device

Step 1 On client homepage, click **Config**.
The **Config** interface is displayed.

Step 2 In left device tree, select AC device, click **Device Reboot**, and see Figure 4-323.
The prompt box of rebooting device is displayed.

Figure 4-323 Enter device reboot



Step 3 Click **Yes** and reboot device.

4.12 Visitor Management

A visitor should registers at the entrance to get access permission. Access permission is disabled when leaving the company.

Figure 4-324 Visitor flow

4.12.1 Adding AC Device

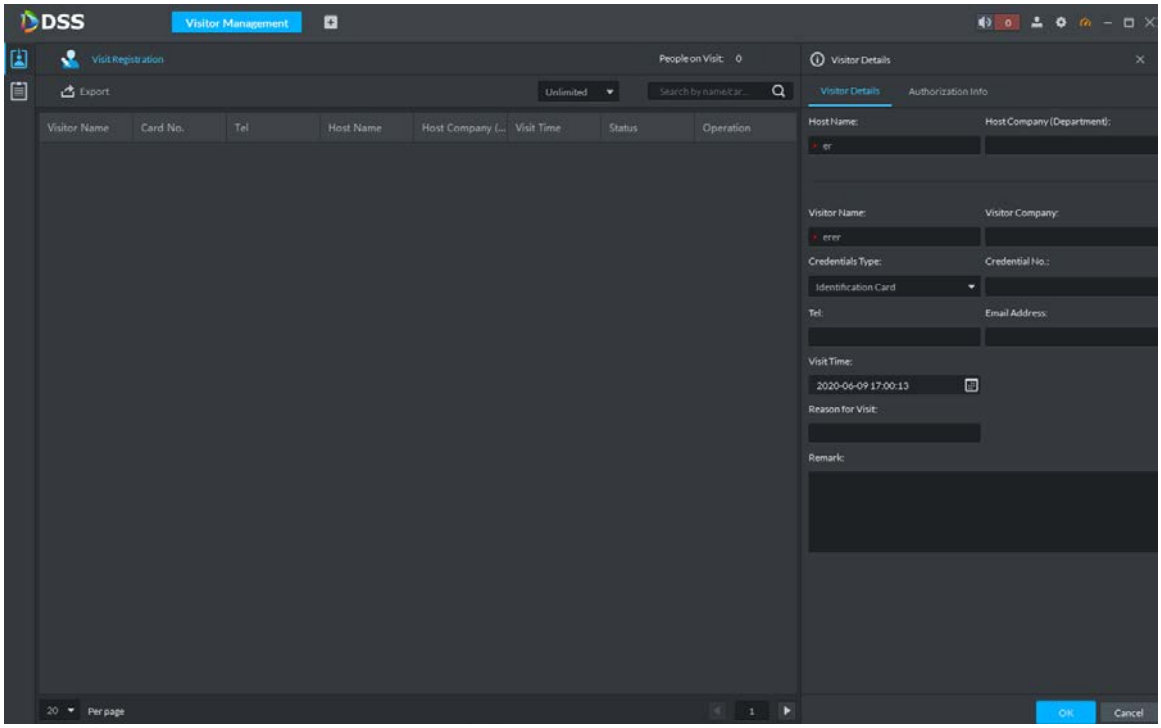
Add access control device. For more details, refer to "4.1.2.4 Adding Device."

4.12.2 Visit Registration

When a visitor comes to visit, you need to confirm person info and grant access permission. On-site registration is supported when there is temporary visitor, and grant access permission. Visitor can have access by swiping card or face recognition.

Step 1 On **Visitor Management** interface, click > **Visit Registration**.

Figure 4-325 Visit details

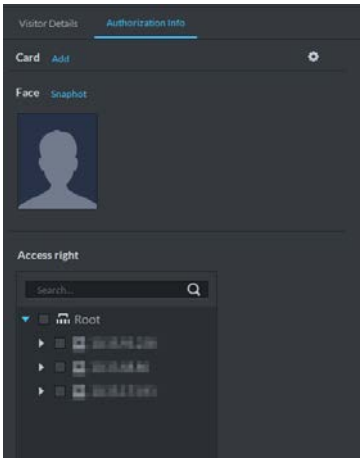


Step 2 On **Visit Details** interface, enter visitor info. See Figure 4-325.

Step 3 Click **Authorization Info** tab.

The system displays **Authorization Info** interface, see Figure 4-326.

Figure 4-326 Visitor authorization



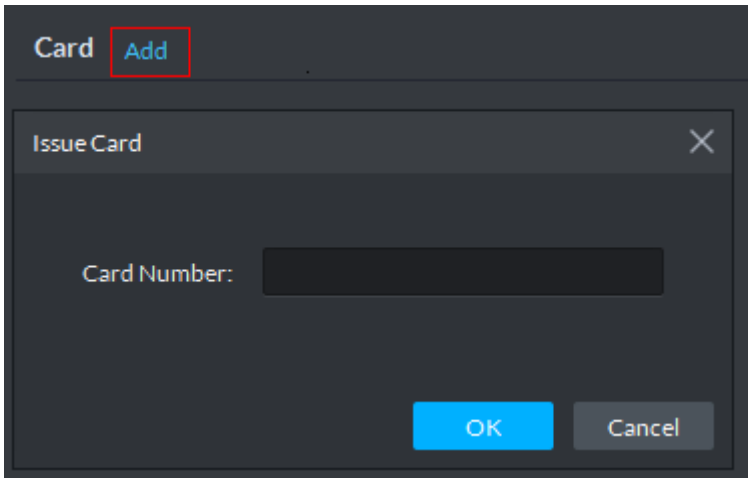
Step 4 Issue card to visitor.

You can issue card by entering card No. manually or card reader. Card No. supports 8 and 16 digits, if the card No. is less than 8 or 16 digits, the platform adds 0 by default to meet the card No. requirement. For example, if you enter card number 8004, then the platform will change it to 00008004. If you enter card number 1000056821, then the platform will change it to 0000001000056821.

- Issue card by entering card No. manually

1) Click **Add** next to **Card**.
   The system displays Issue Card interface, see Figure 4-327.

Figure 4-327 Add card



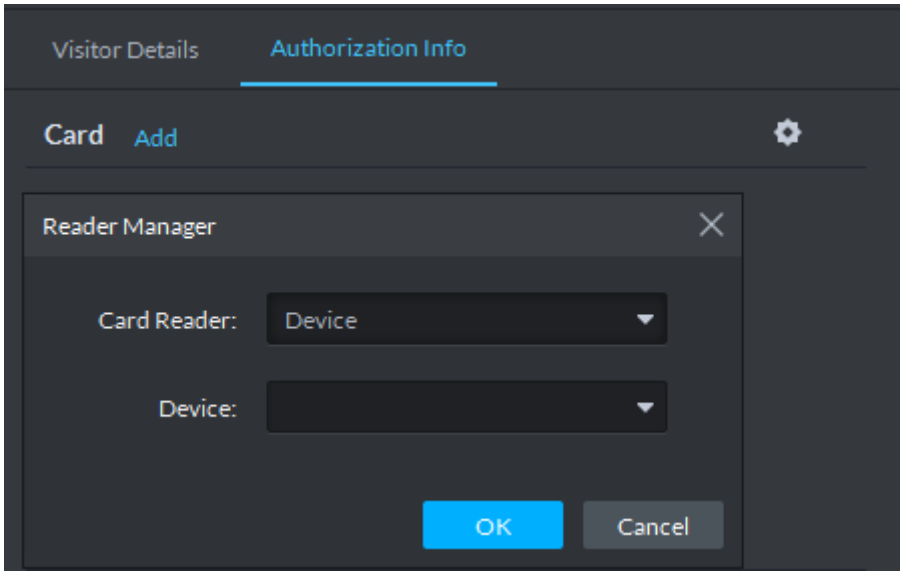
2) Enter card number, click **OK**, and card is issued.

- Issue card by reader

1) Click 

.
   The system displays **Reader Manager** interface, see Figure 4-328.

Figure 4-328 Reader manager

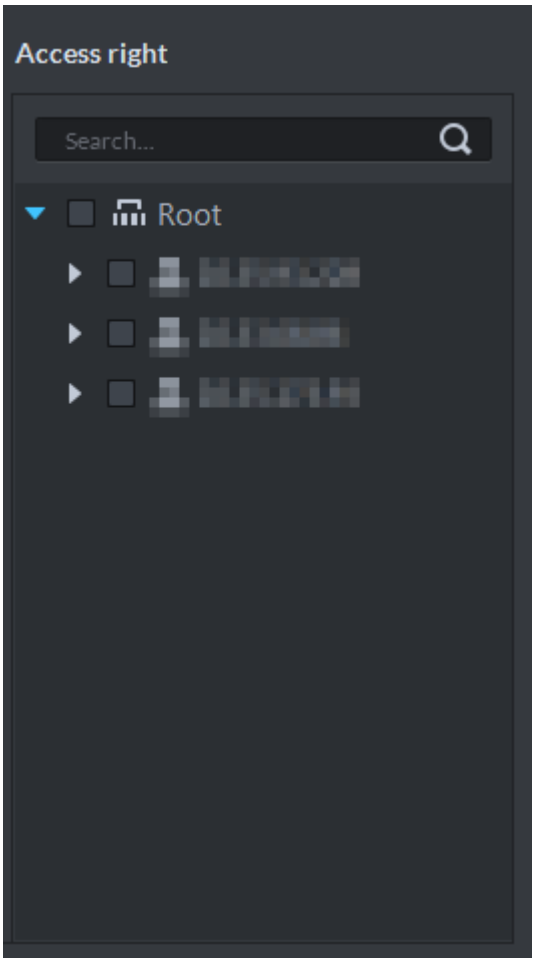


2) Select card reader or device, click **OK**.
3) Swipe card on reader or device, and card is issued.

Step 5 Click **Snapshot**, and you can take face snapshot according to system prompt.
The face snapshot is used for face recognition and unlock door.

Step 6 In **Access Right** area, select AC channel that visitor can pass, see Figure 4-329.

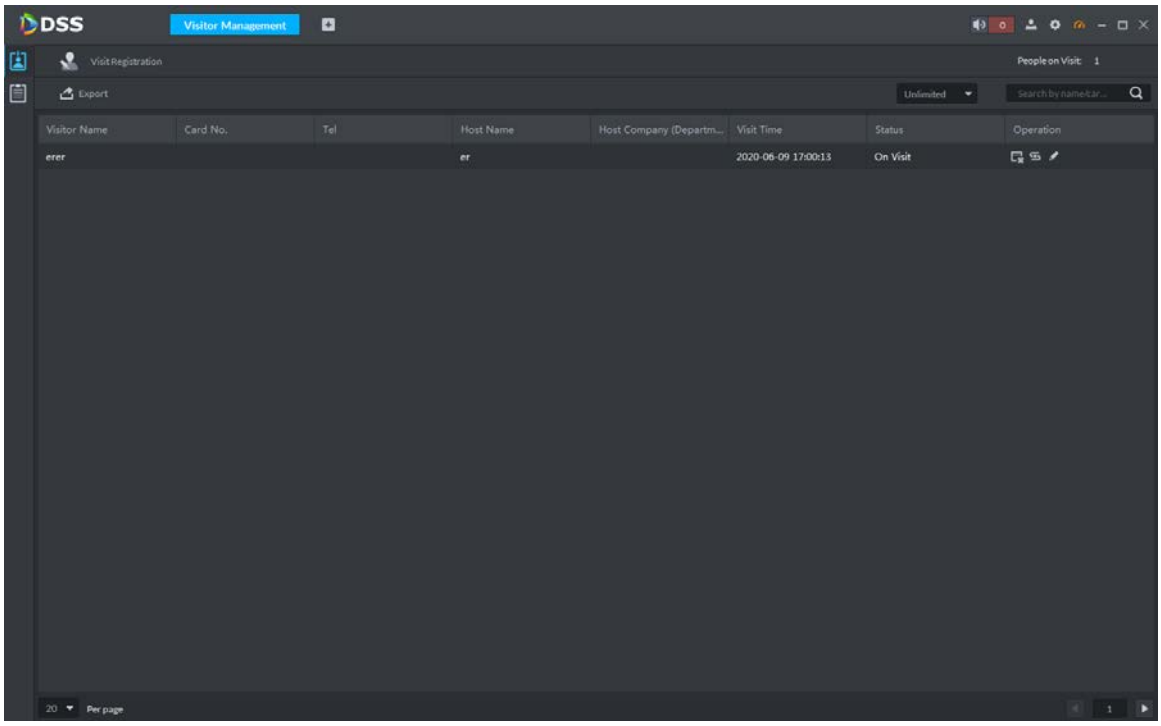
Figure 4-329 Select channel



Step 7 Click **OK** and complete visitor registration, see Figure 4-330.

- Click and skip to end visit interface.
- Click and view visitor swiping card records.

Figure 4-330 Visit registration



4.12.3 End Visit Registration

When visitor leaves, close access permission.

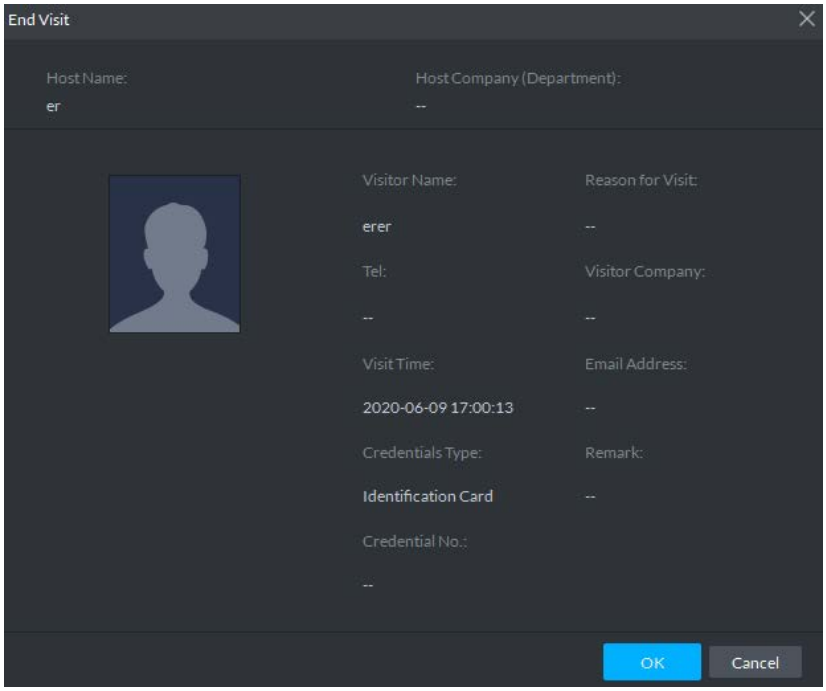
Step 1 On **Visitor Management** interface, click .

The system displays **Visitor Management** interface.

Step 2 Search end visit person info, click .

The system displays **End Visit** interface, see Figure 4-331.

Figure 4-331 End visit



Step 3 Click **OK** and close access permission.

If you issue card to visitor, make sure the card is returned when visitor leaves.

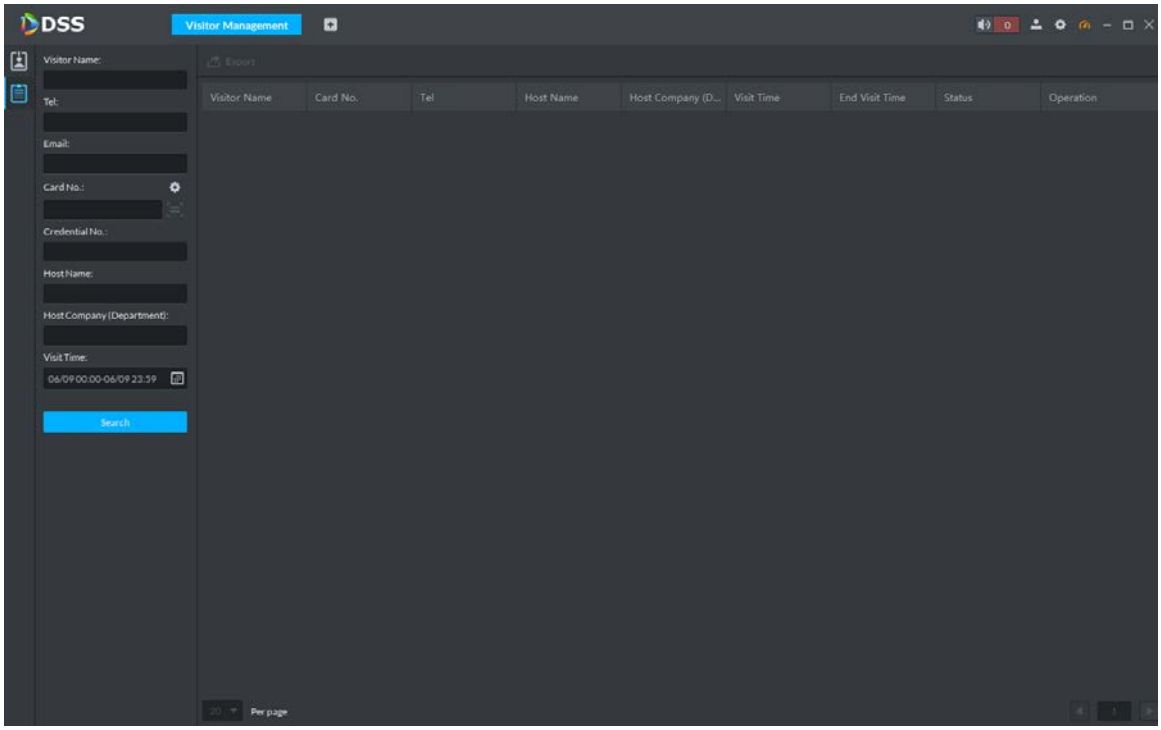
4.12.4 Searching Visit Record

You can set condition and search visit record, and view visitor details and card swiping records.

Step 1 On **Visitor Management** interface, click .

The system displays **Visit Record** interface, see Figure 4-332.

Figure 4-332 Visit record

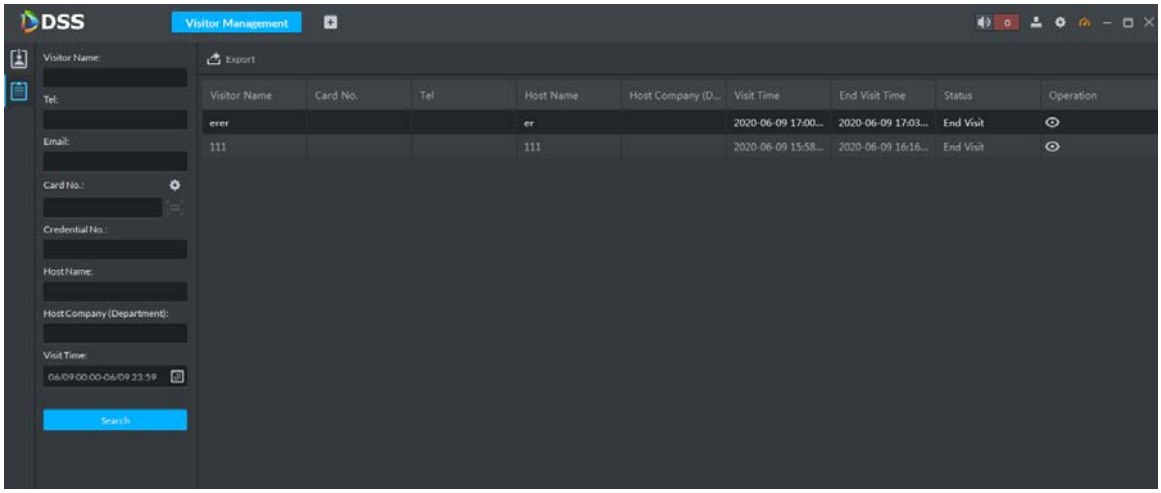


Step 2 Set search condition, click **Search**.

The system displays results. See Figure 4-333.

Card number info supports clicking to set card reader, and you can read by reader.

Figure 4-333 Search visit result

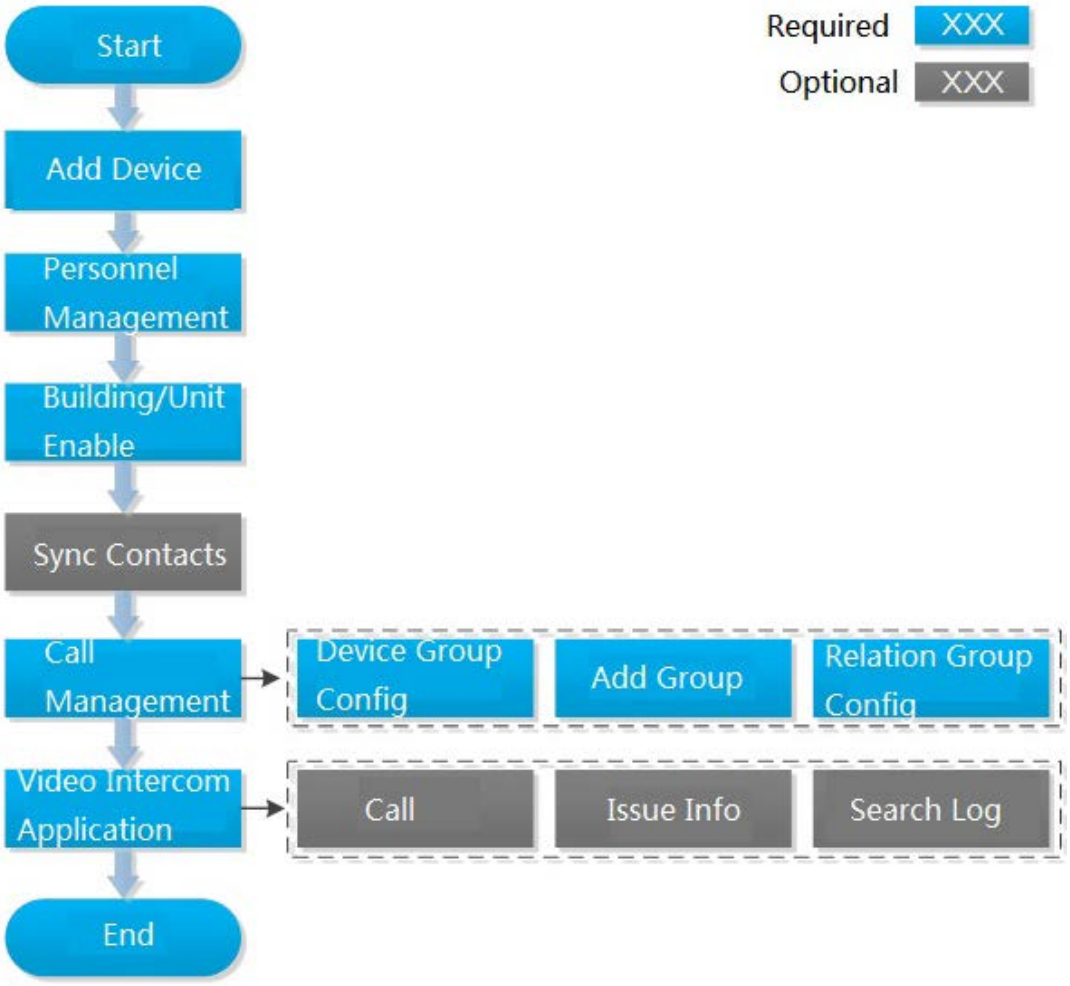


Step 3 Click and view visitor details and card swiping records.

4.13 Video Intercom

After integrating video talk module and adding video intercom device, you can realize device talk, realtime monitoring and issuing info. The video intercom operation flow is shown in Figure 4-334

Figure 4-334 Operation flow



Configure video intercom on platform, the device is required to be configured. For more details, refer to user manual.

4.13.1 Adding Video Intercom Device

Add video intercom devices such as unit VTO, VTH and fence VTO. For more details, see"4.1.2.4 Adding Device."

If you modify config when using device, the device will not actively push message to platform. You need to acquire device info manually from platform. For more details, see"4.1.2.5 Editing Device."

4.13.2 Personnel Management

For video intercom, you can add personnel by the module of personnel management. See"4.10 Personnel Management" for more details. Room number is required to be configured when adding personnel.

4.13.3 Configuring Building/Unit

It needs to make sure the enable of building and unit is in accordance with the device if you want to use the video talk module of the platform, otherwise, the device is offline after adding device.

The setting of building and unit affects the dialing rule. Take room 1001 unit 2 building 1 as an example, the dialing rule is shown as follows after it is enabled.

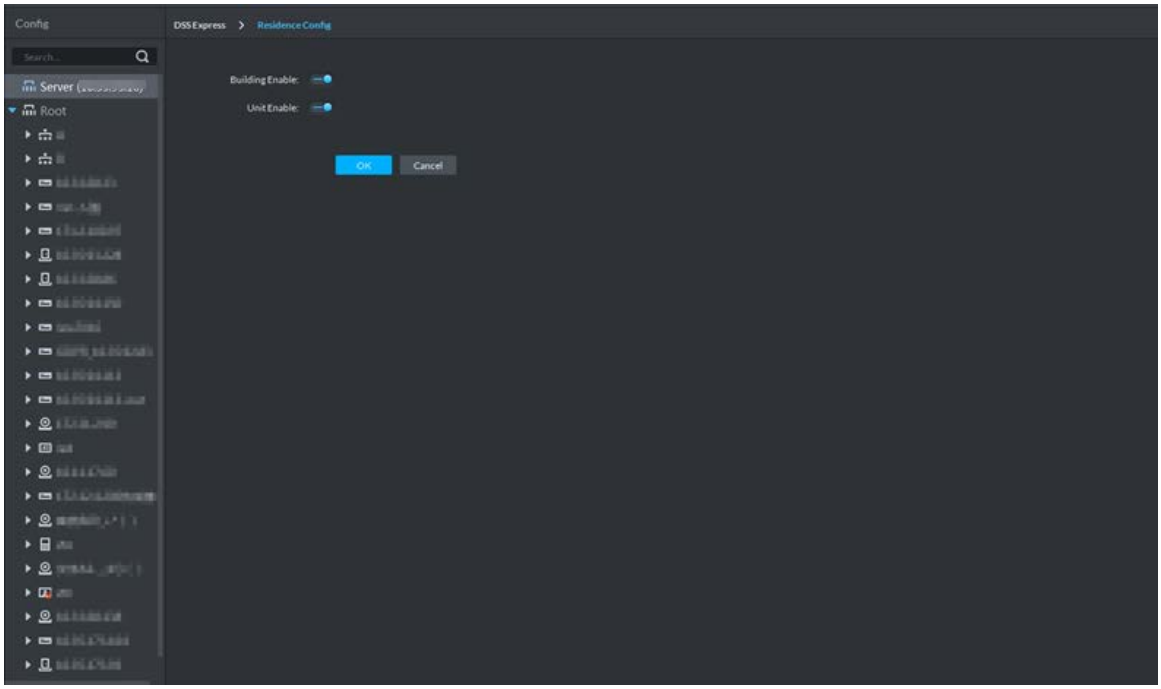
- If building is enabled and unit not enabled, the main VTH number is"1#1001#0" and the sub VTH number is"1#1001#1".
- If building is enabled and unit is enabled as well, the main VTH number is"1#2#1001#0" and the sub VTH number is"1#2#1001#1".
- If building is not enabled and unit is not enabled either, the main VTH number is"1001#0" and the sub VTH number is"1001#1".

Step 1 On client homepage, click **Config**.

The **Config** interface is displayed.

Step 2 Click **Residence Config**.

Figure 4-335 Residence configuration



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

4.13.4 Synchronizing Contacts

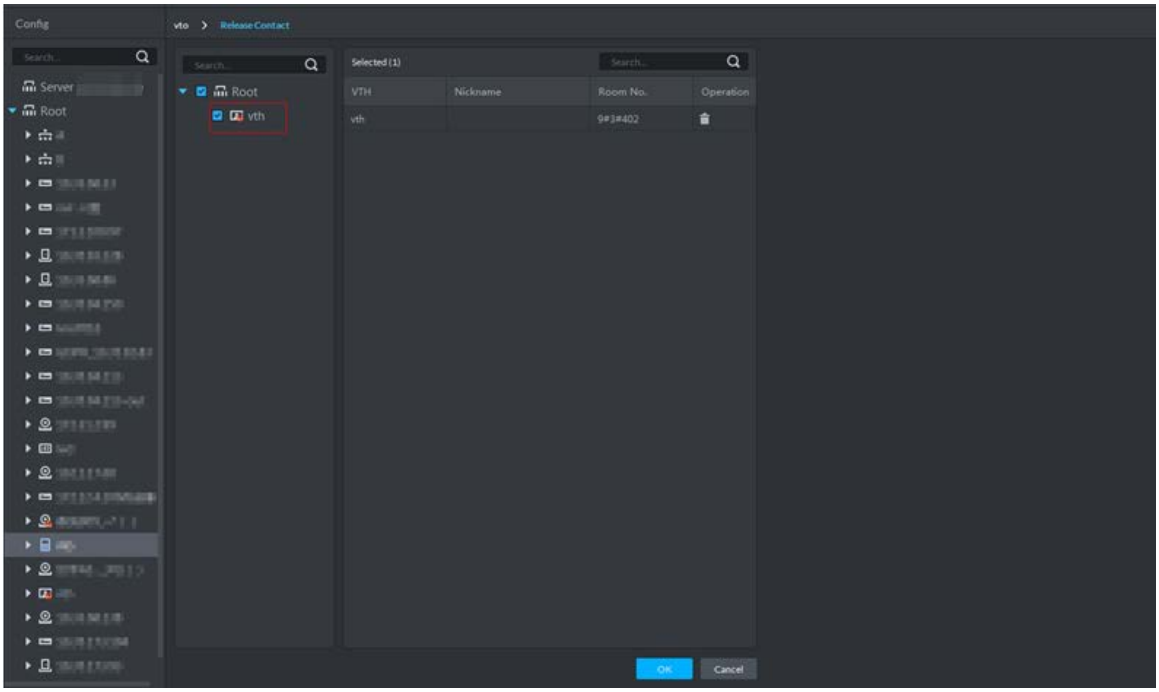
Synchronize contacts information to VTO and then you can view contacts on the VTO display screen or WEB interface.

Step 1 On client homepage, click **Config**.

The **Config** interface is displayed.

Step 2 Select VTO from the device list, and then click **Contacts**.

Figure 4-336 Release contact



Step 3 Select VTH, click **OK**.

You can view contacts on VTO screen or WEB interface after it is released.

4.13.5 Call Management

Create device group, management group and relation group respectively; realize mutual call in the specific group. Only default system account supports the function.

Click  on the interface of device group, management group or relation group, the system will restore management group and relation group to original status.

4.13.5.1 Device Group Config

It can realize mutual call only when VTO and VTH are added into the same device group. Pro will automatically generate corresponding device group when VTO, verifying VTO and fence station are added to Pro.

- Add VTO and automatically generate a device group, add VTH of the unit into the group, and realize mutual call between VTH and VTO within the group.
- Add verifying VTO and automatically generate a device group, add it to the group together with the VTH of the same room, and realize mutual call between VTH and verifying VTO within the group.

- Add fence station and automatically generate a device group, add all the VTH into the group. Realize mutual call between fence station and all the VTH.
- Add VTH, if the VTH is automatically connected to unit VTO, verifying VTO, fence station, and then it will be automatically added to the device group, and realize mutual call among unit VTO, verifying VTO or fence station.

Call between VTH is not restricted by device group; mutual call can be realized among VTH in different device groups.

4.13.5.2 Adding Management Group

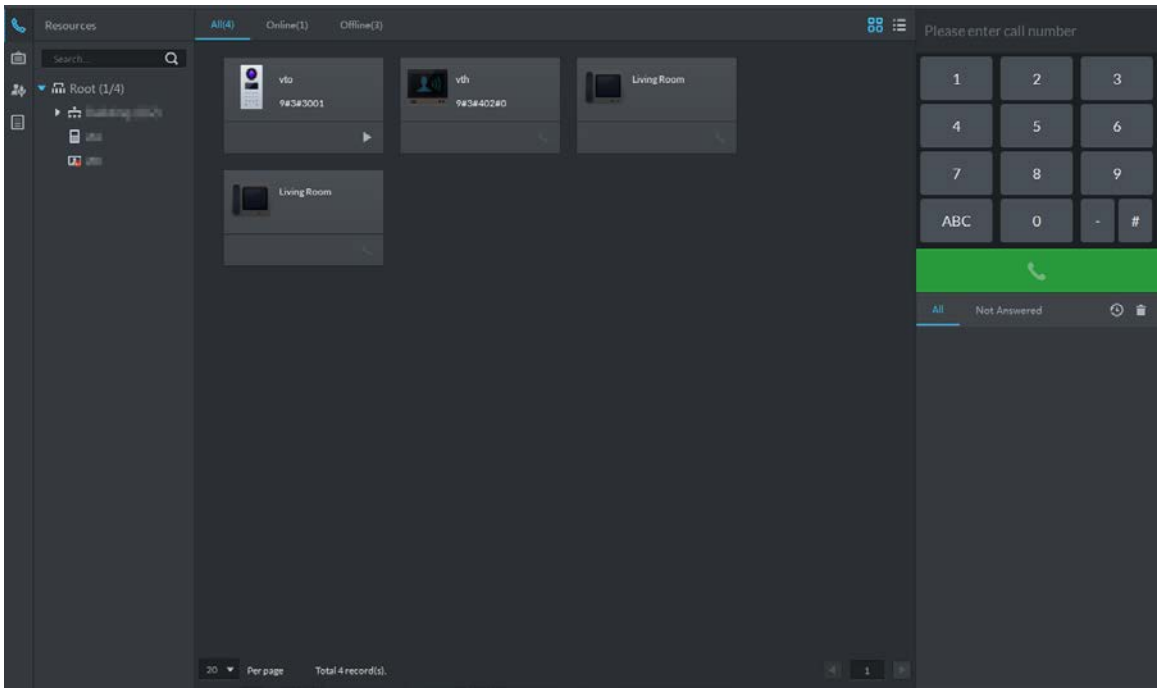
Management group is to make groups for administrators, and realize relation binding of one to one, one to many or many to many. Administrators include Pro administrator and VTS. If there is default management group, VTS will be automatically added to management group when it is added.

- Before configuring management group, it needs to create user, select video intercom menu permission and device permission, and add new users into management group.
- Use system user to configure group relation, need to switch to new user for login. If system logs onto many devices, then it cannot be used as administrator.

Step 1 On client homepage, click **Video Intercom**.

The **Video Intercom** interface is displayed. See Figure 4-337.

Figure 4-337 Video intercom



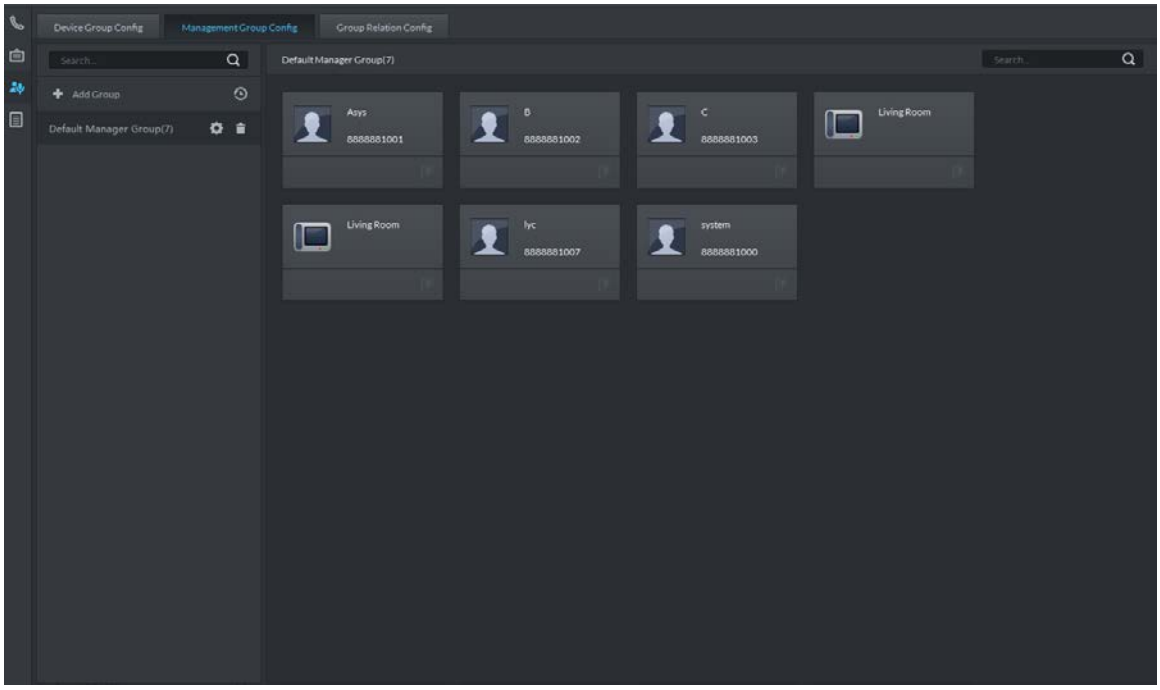
Step 2 Click .

The interface of **Call Management** is displayed.

Step 3 Click Management Group Config.

The interface of **Management Group Config** is displayed. See Figure 4-338.

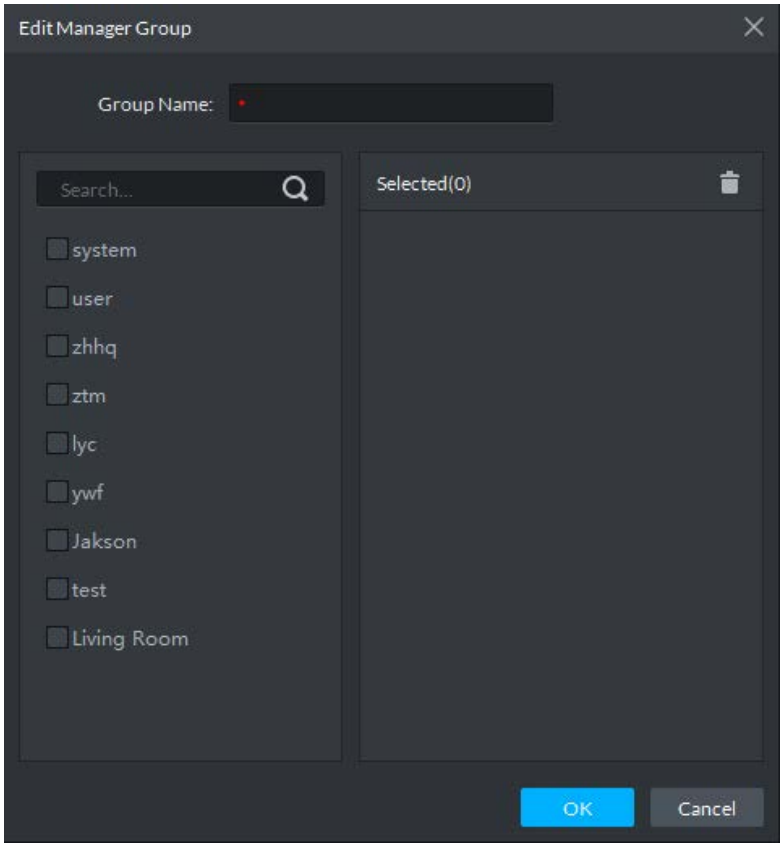
Figure 4-338 Call management



Step 4 Click Add Group.

The interface of **Edit Manager Group** is displayed. See Figure 4-339.

Figure 4-339 Manager group



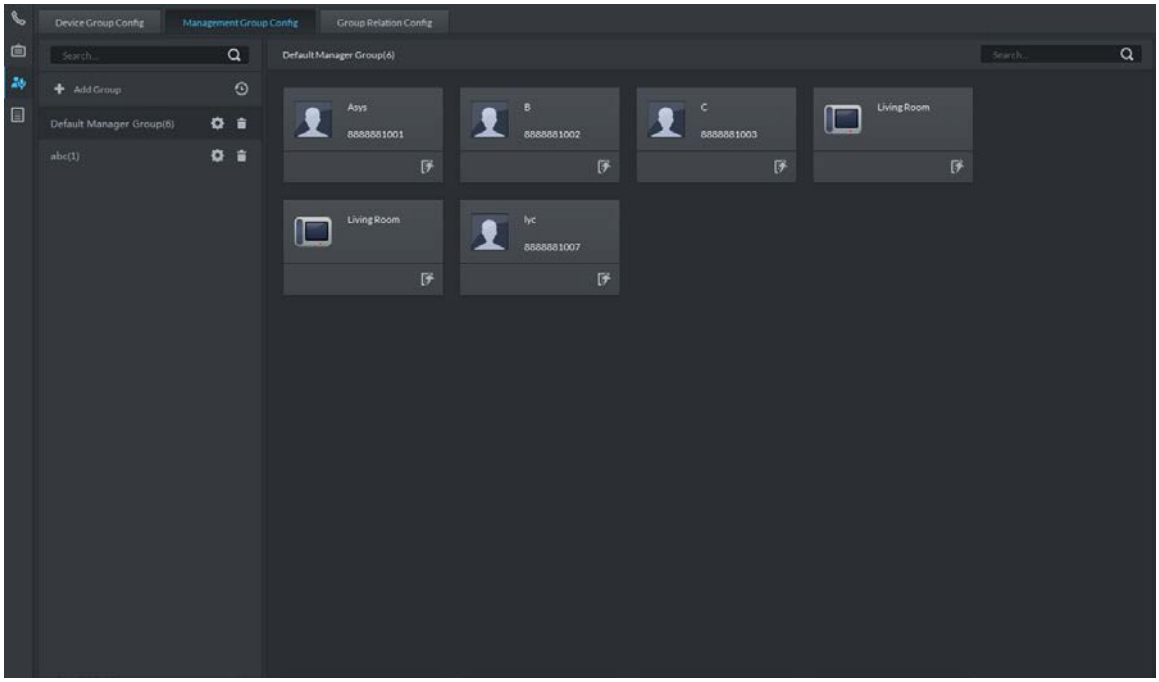
Step 5 Enter group name, select administrator account or VTS, and click **OK**.

The added management group is displayed in the list. See Figure 4-340.

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 4-340 Manager group



4.13.5.3 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.

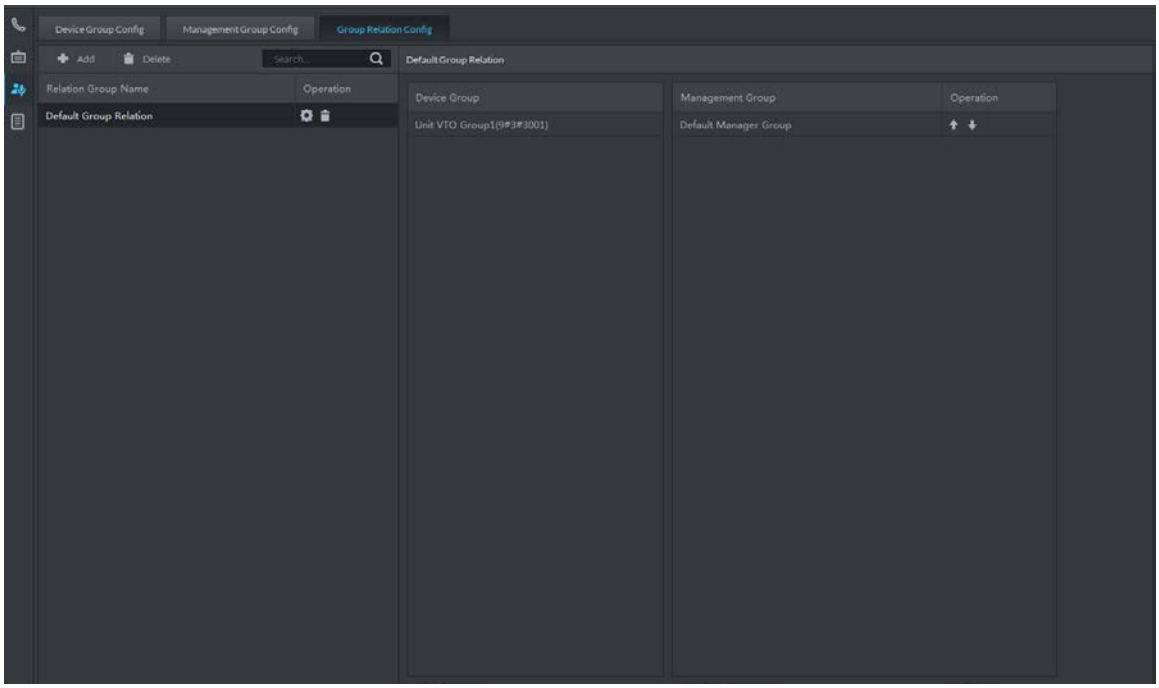
Step 1 Click on the interface of **Video Intercom**.

The interface of **Relation Group Config** is displayed.

Step 2 Click the tab of Relation Group Config.

The interface of **Relation Group Config** is displayed. See Figure 4-341.

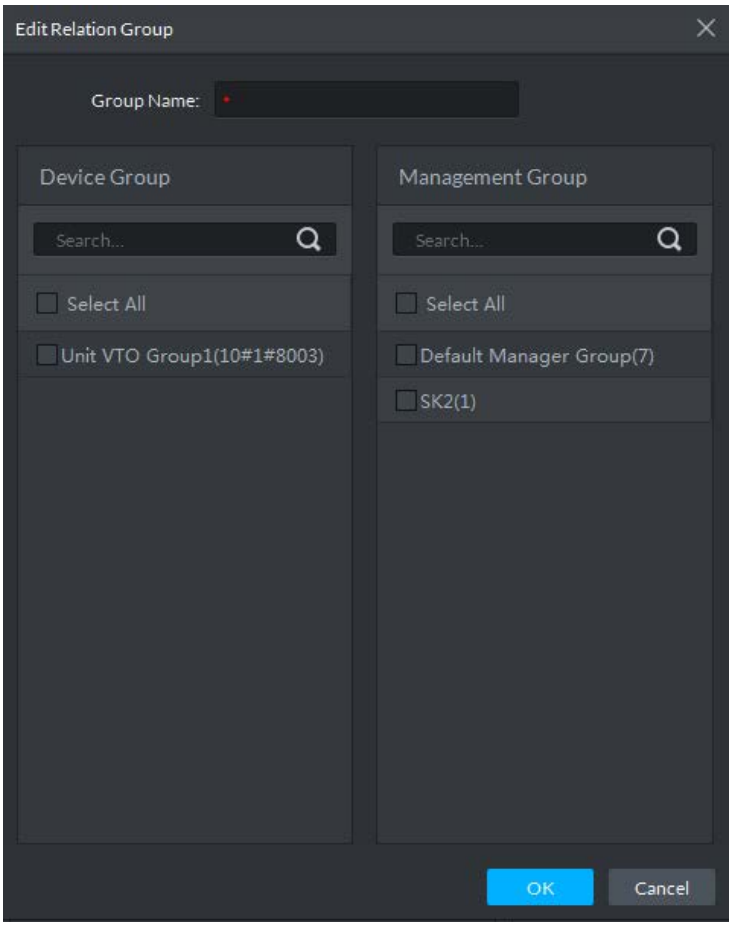
Figure 4-341 Group relation config



Step 3 Click **Add**.

The interface of **Edit Relation Group** is displayed. See Figure 4-342.

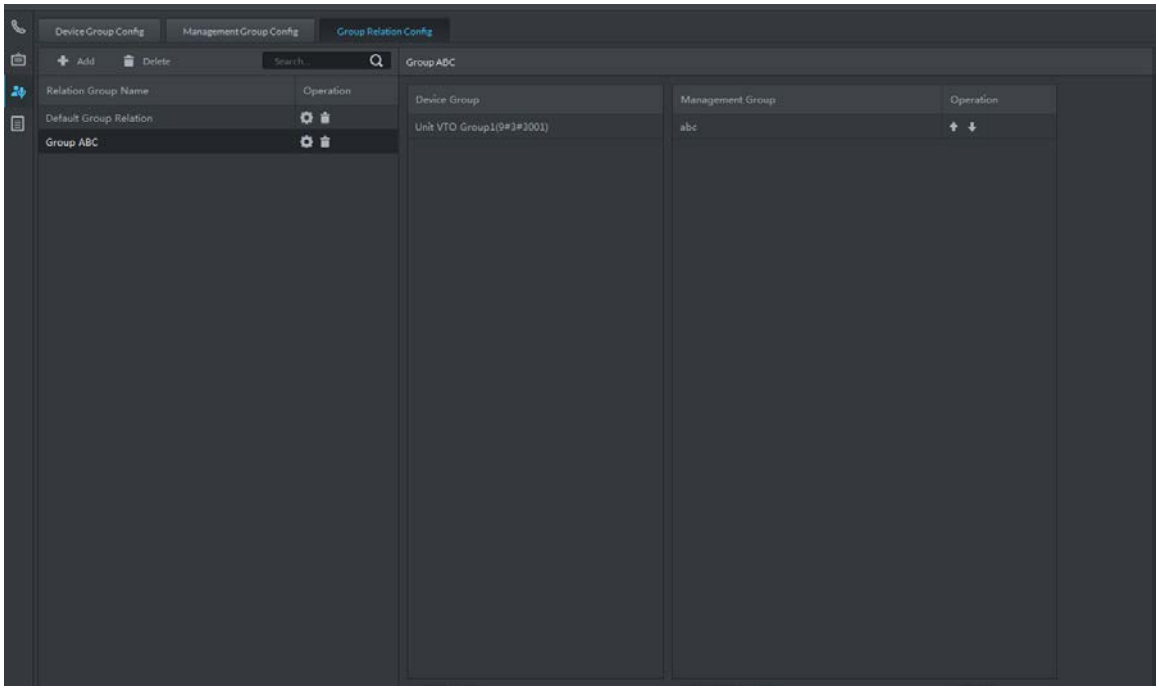
Figure 4-342 Edit relation group



Step 4 Enter name, select device group and management group, Click **OK**.

Added relation group is displayed in the list. See Figure 4-343. If there are several relation groups, you can click or to adjust priority level. When there is call, the online administrators with high priority will generate ring bell first.

Figure 4-343 Edit relation group



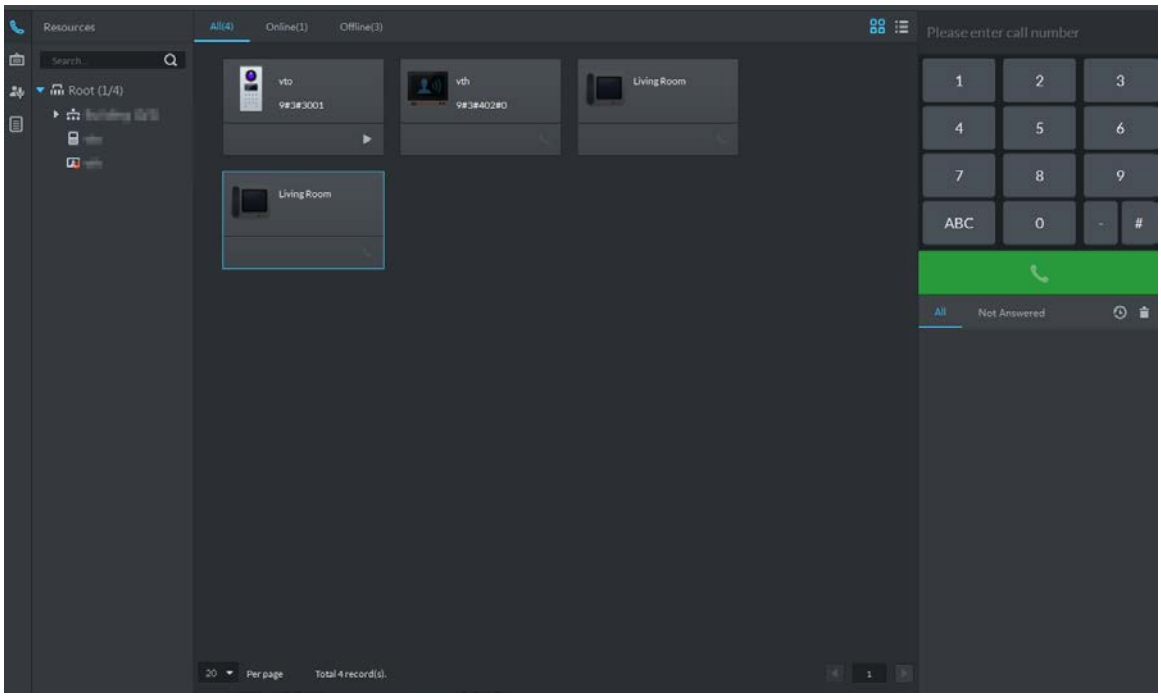
4.13.6 Video Intercom Application

4.13.6.1 Call Center

Step 1 Click on the interface of **Video Intercom**.

The interface of **Call Center** is displayed. See Figure 4-344.

Figure 4-344 Call center



Step 2 You can call VTO and VTH on the interface of **Call Center**.

- Platform calls VTO

  Select VTO in the device list; click corresponding  of VTO and call VTO. The system pops out call interface and realizes video talk. See Figure 4-345. Following operations are supported during call.

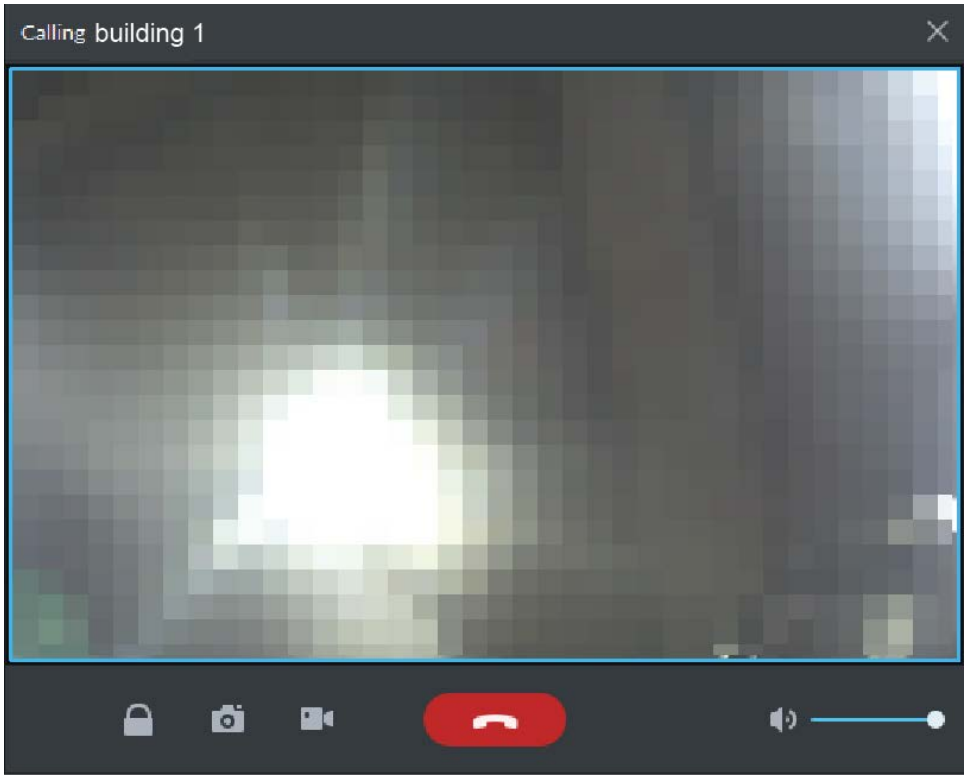
  ◇  , if VTO is connected to lock, click the icon to unlock.

  ◇  , click the icon to capture picture, the snapshot is saved into the default directory installed by client. If you need to modify the save path of snapshot, refer to"4.2.4 Setting Snapshot" for more details.

  ◇  , click the icon to start record, and click again to stop record. The video is saved in default path installed by client. If you need to modify the save path, refer to"4.2.5 Setting Recording Parameter" for more details.

  ◇  , click the icon to hang up.

Figure 4-345 Call VTO



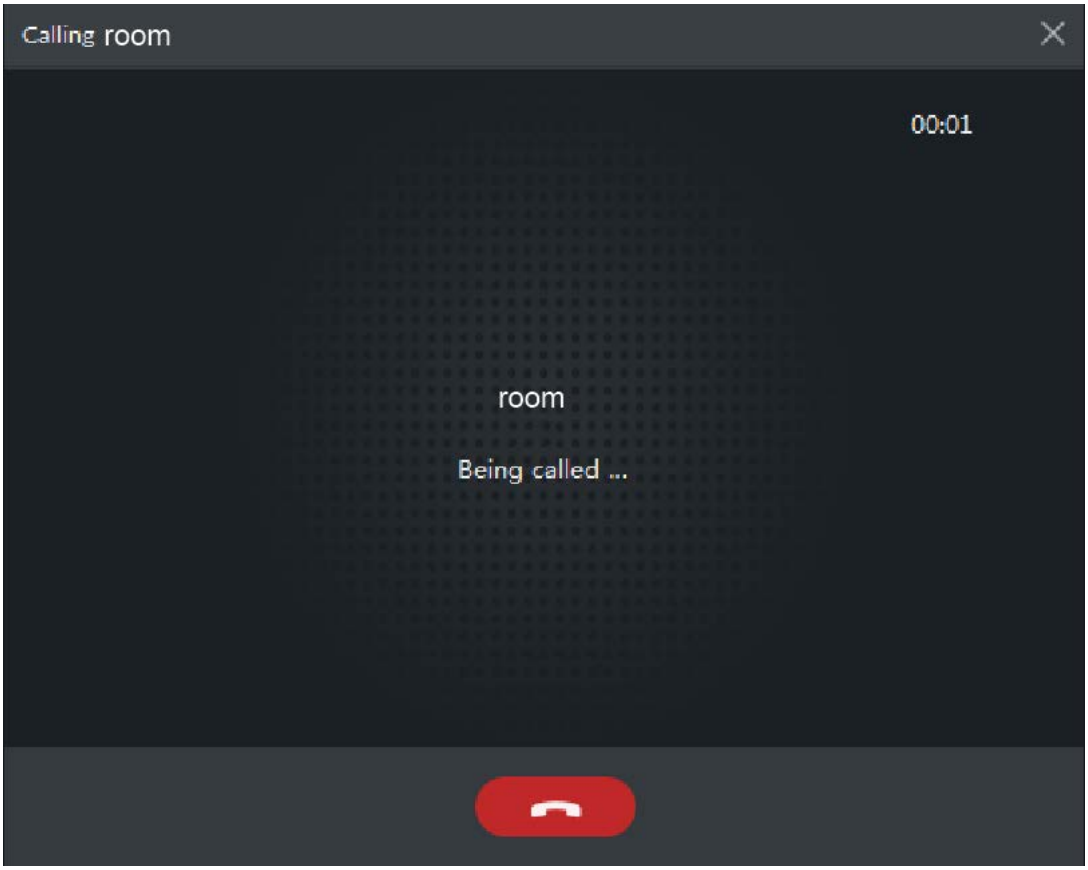
- Platform call VTH

  Select VTH from the device list, click  on the VTH or dial corresponding VTH on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait…**. See Figure 4-346. 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 direcly, then it means the callee is busy.

Figure 4-346 Call VTH

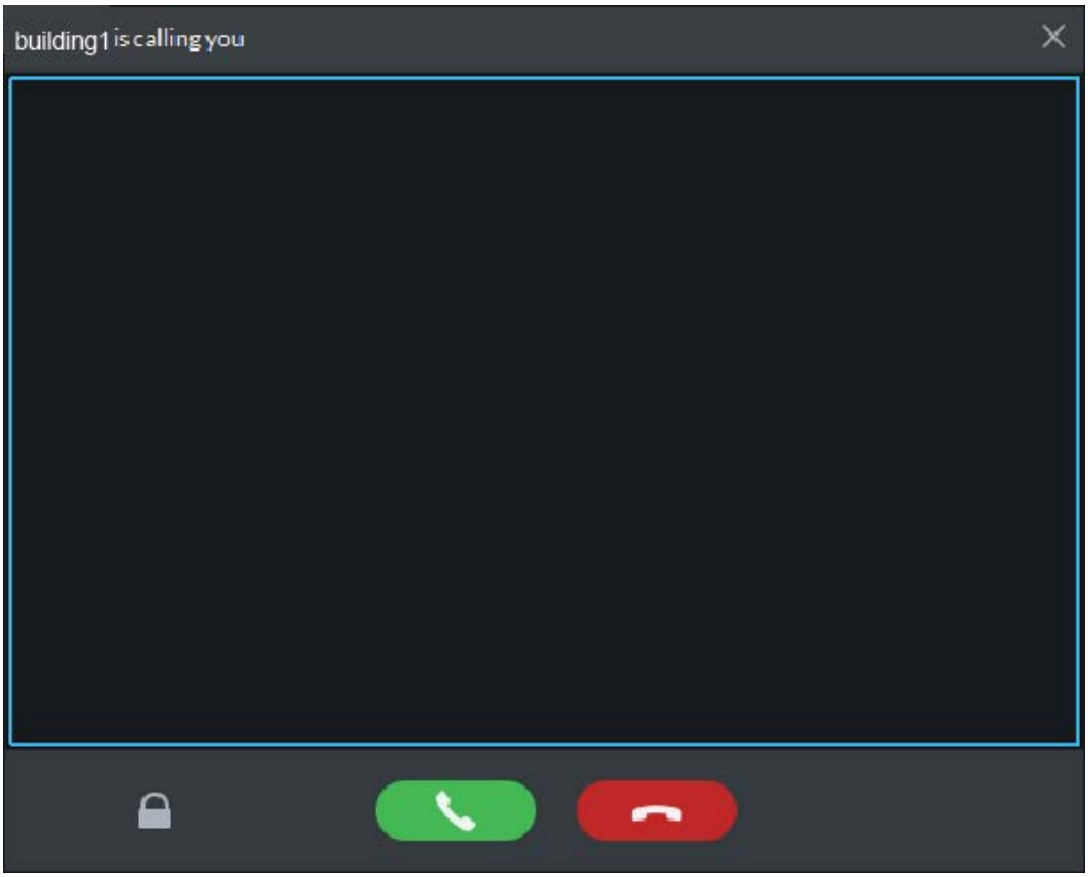


- VTO calls platform

  VTO calls platform, client pops up the dialog box of VTO calling. See Figure 4-347.

  -  , 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 4-347 VTO calling platform



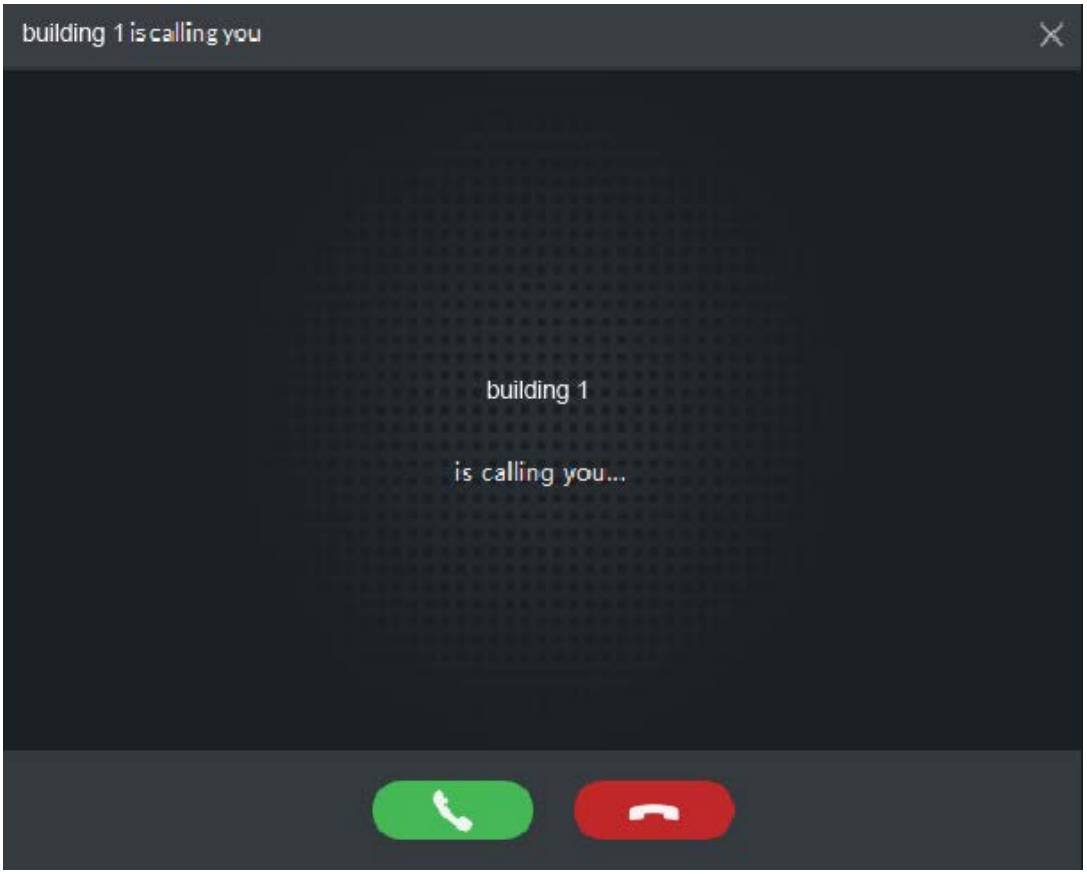
- VTH calls client

  The client pops out the dialog box of VTH calling. See Figure 4-348. Click  and realize talk with VTH.

  ◇  , click the icon and answer VTO, realize mutual talk after connected.

  ◇  , click the icon and hang up.

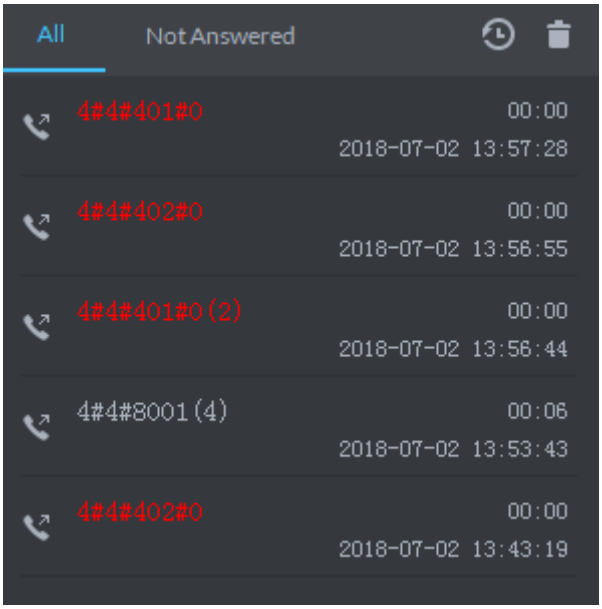
Figure 4-348 VTH calling client



- Call from 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 4-349. Move the mouse to the record, click  and call back.

Figure 4-349 Call records



4.13.6.2 Releasing Info

The platform sends message to designated VTO.

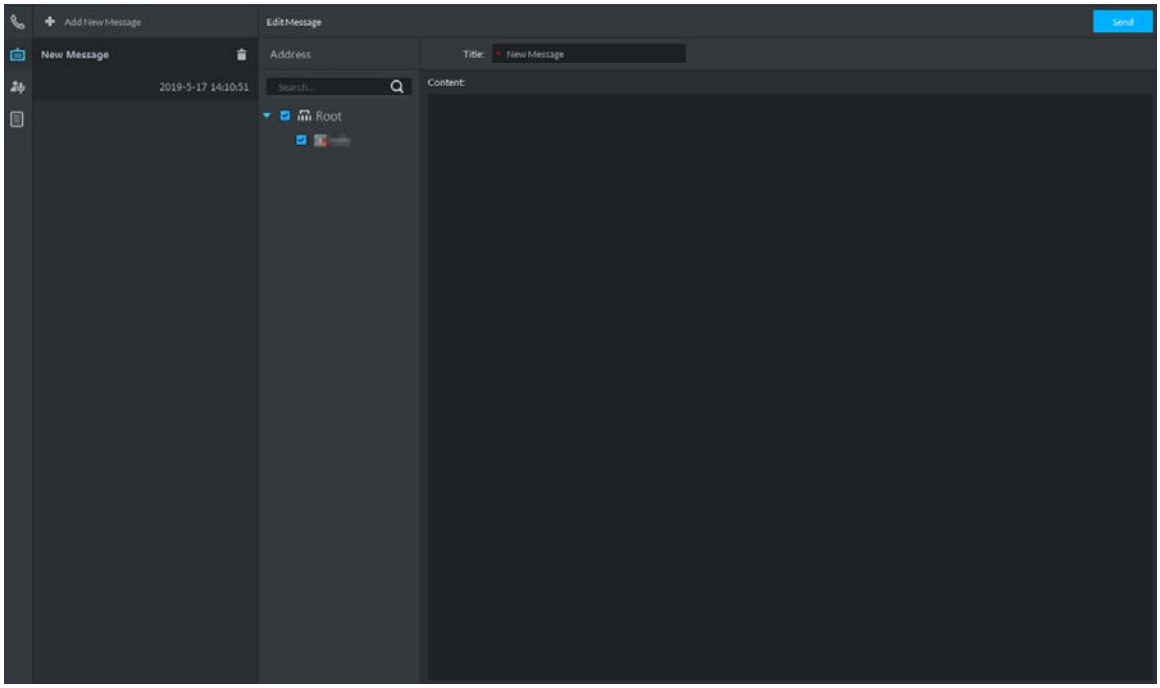
Step 1 Click  on the interface of **Video Intercom**.

The interface of **Release Info** is displayed. See Figure 4-350.

Figure 4-350 Release info (1)

Step 2 Click **Add New Message**, select VTH and add release info. See Figure 4-351.

Figure 4-351 Release info (2)



Step 3 Click **Send**.

The VTH will receive the message after it is sent successfully.

4.13.6.3 Searching Video Intercom Log

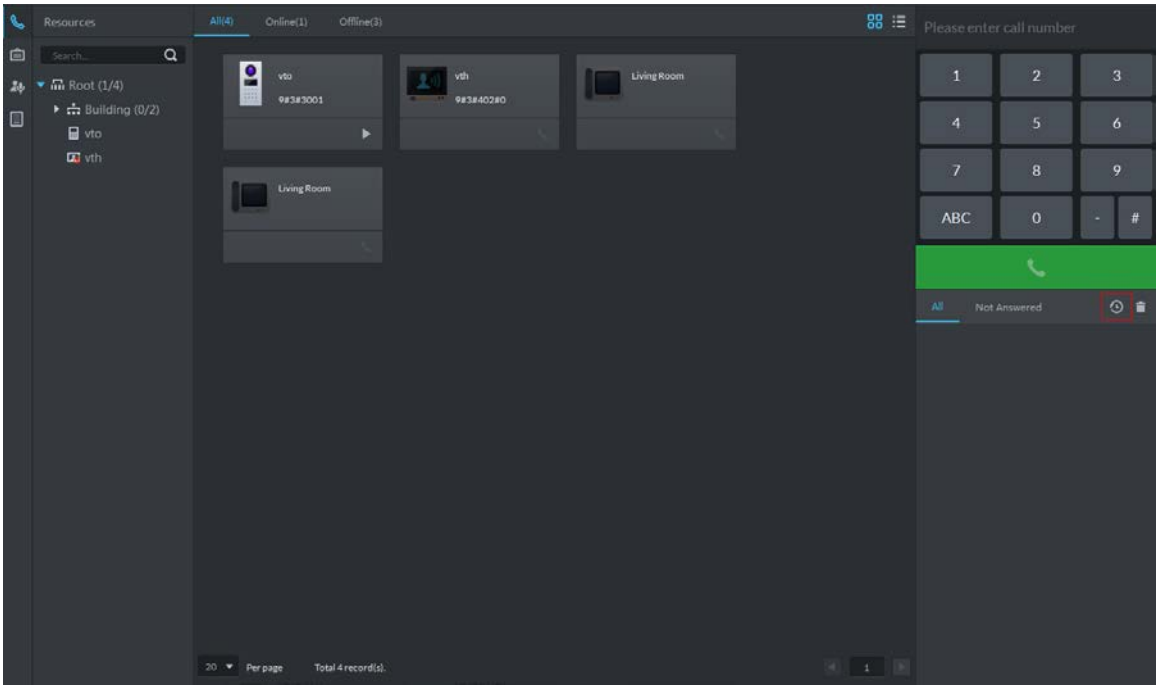
View log records and you can trace recorded calls.

Step 1 Enter the interface of video intercom log.

The system supports following two ways to enter.

- Click  on the interface of **Video Intercom**.
- Click  and enter console on the interface of **Video Intercom**. See Figure 4-352.

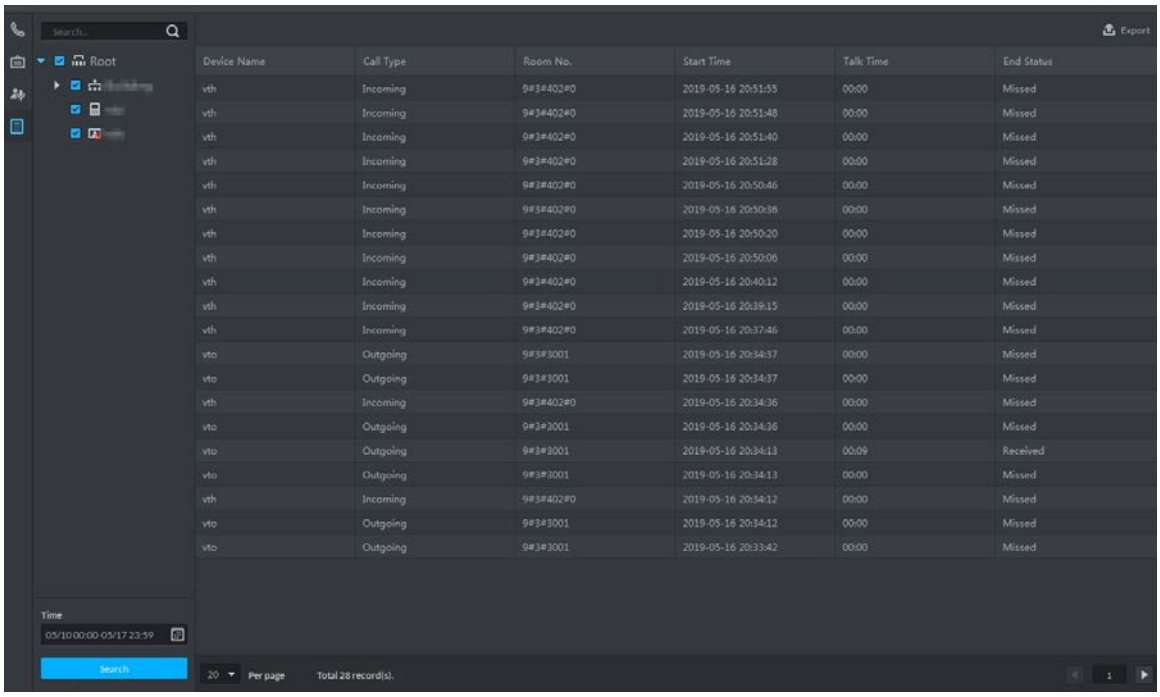
Figure 4-352 Enter log interface



Step 2 Set conditons, click **Search**.

The log info is displayed. See Figure 4-353

Figure 4-353 Search log

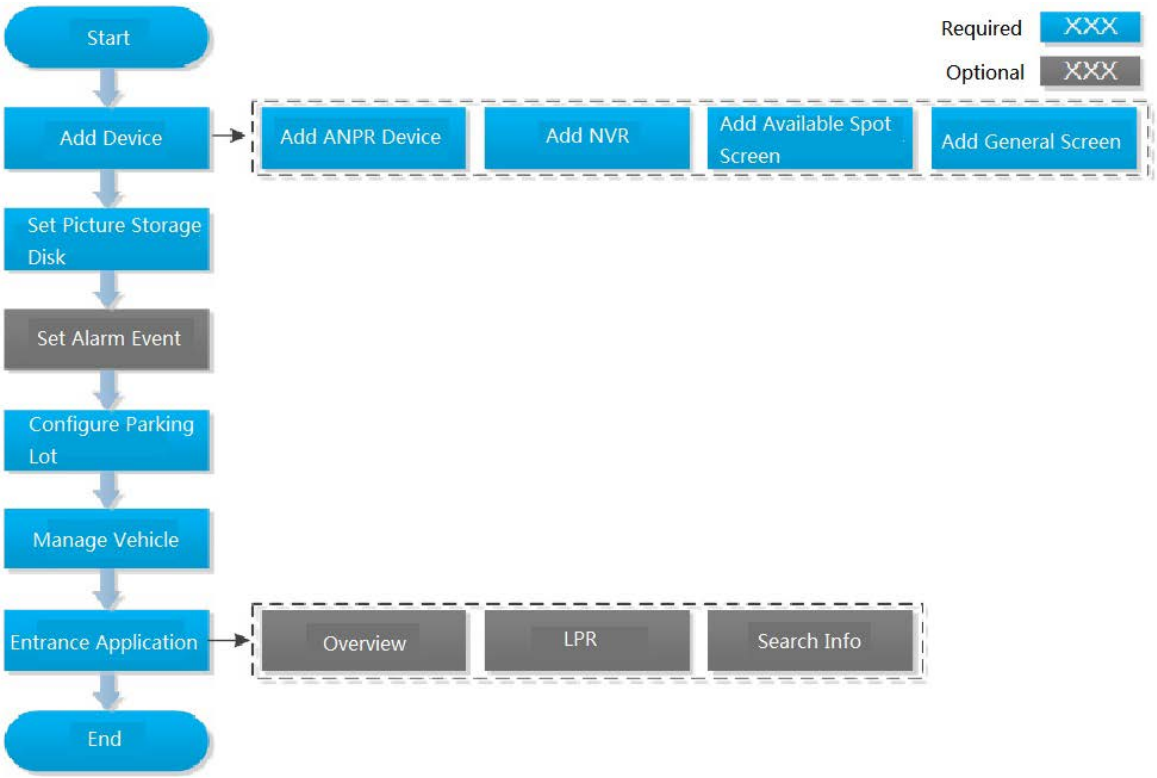


Step 3 Click **Export** and the logs will be saved locally according to system prompt.

4.14 Entrance

Integrare entrance module, realize entrance and exit recognition barrier unlock, remaining parking space info display, blocklist vehicle alarm, message search and other functions. When it fails to recognize vehicle by entrance, then it can unlock by VTO password, swipe card to unlock, fingerprint unlock and unlock by face recognition to open barrier. The supported VTO unlock mode is based on the performance of accessed VTO. The entrance operation flow is shown in Figure 4-354.

Figure 4-354 Entrance operation flow



4.14.1 Adding Device

If users want to use the new device, it needs to select **User Management** > **User** on WEB, enter **User** interface, and edit user to make him or her have access to device, otherwise the device cannot be used.

4.14.1.1 Adding ANPR Camera

ANPR device is used to recognize license plate and vehicle info.

- Please make sure ANPR device is fully configured before adding, for example, complete initialization config, and modify IP etc.
- The device category is **ANPR Device**.

Step 1 Add encoder ANPR, for more details, refer to"4.1.2.4 Adding Device."
Modify device type.

1) On the **Device** interface of Web, click of added ANPR device. See Figure 4-355. The device displays the interface of Edit Device. See Figure 4-356.

Figure 4-355 Enter ANPR device

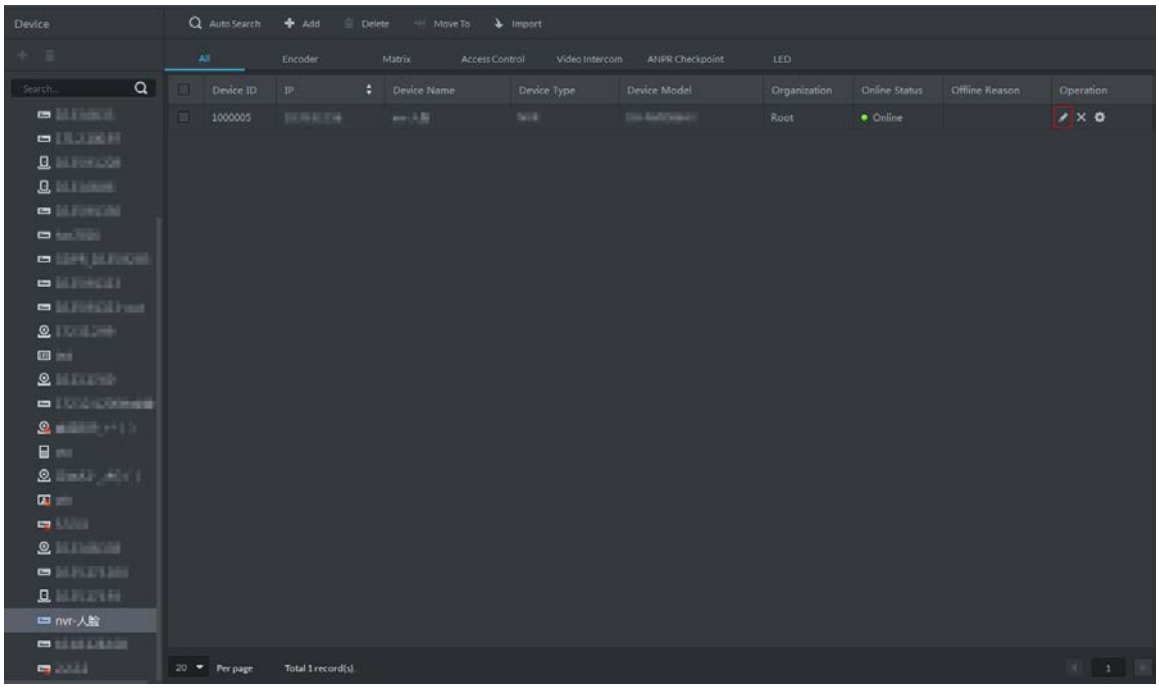
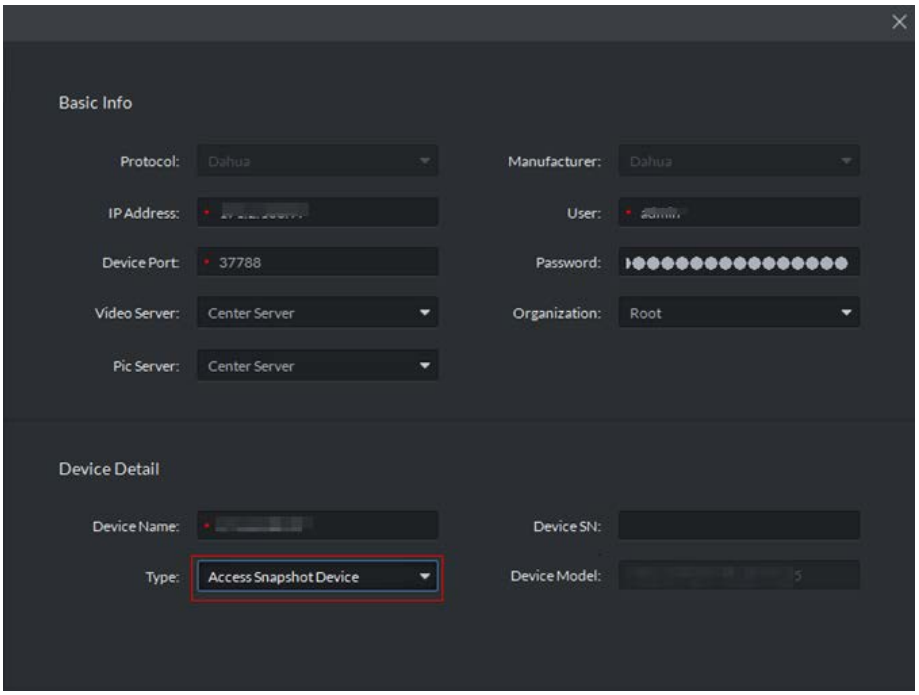


Figure 4-356 Edit device



2) Set Type as Access Snapshot Device.
3) Click OK and complete config.

Step 2 Bind Resource

If there is camera installed at the entrance to view entrance panoramic picture, support binding ANPR and video camera. License plate recognition can view realtime video image. You can view video of bound camera.

1) On client homepage, click **Config**.
   The **Config** interface is displayed.
2) In left device tree, select access control channel, click **Bind Resource**, and see Figure 4-357.

Figure 4-357 Enter resource bind interface

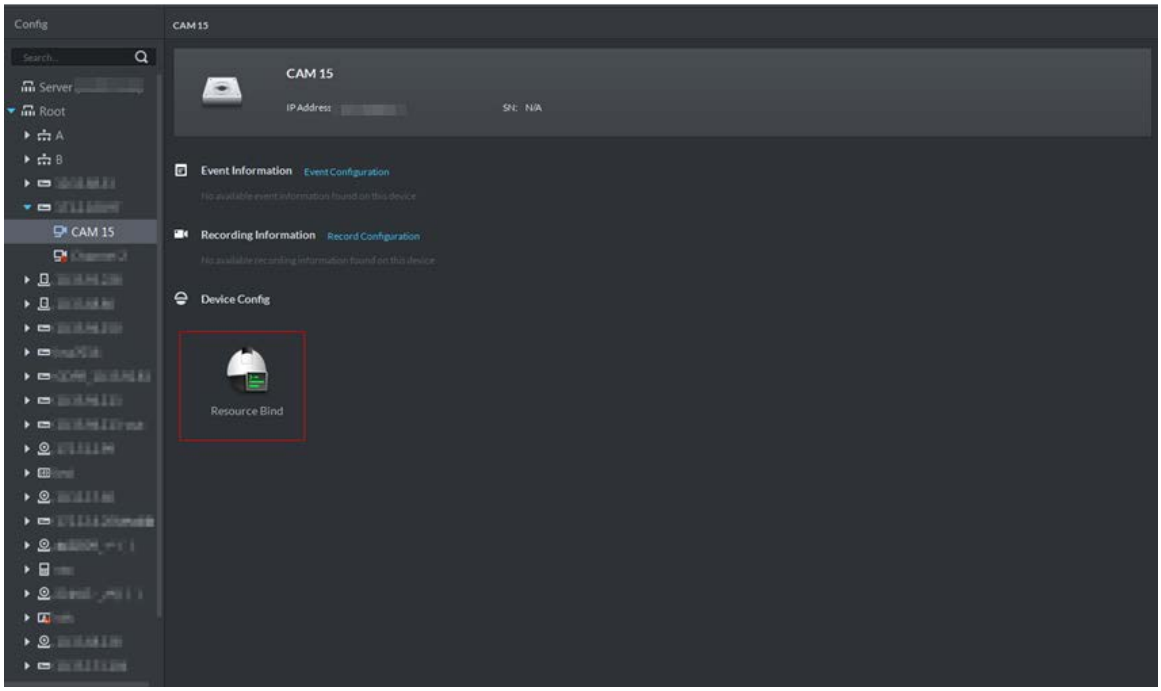
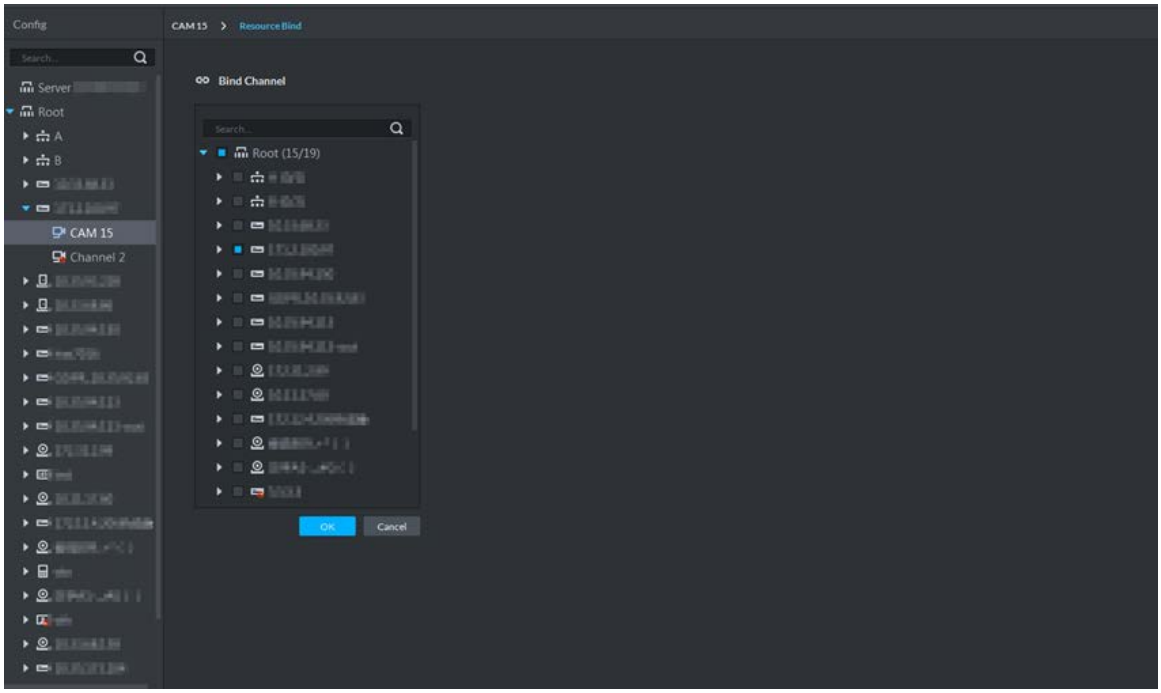


Figure 4-358 Resource bind



3) Select bound panoramic camera.
4) Click **OK** and complete config.

4.14.1.2 Adding NVR

NVR is used to connect ANPR 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"4.1.2.4 Adding Device."

Step 2 Modify device capacity set.

1) Click of added NVR on the **Device** interface on Web. See Figure 4-359.

The interface of **Edit Device** is displayed. See Figure 4-360.

Figure 4-359 Enter encoder edit interface

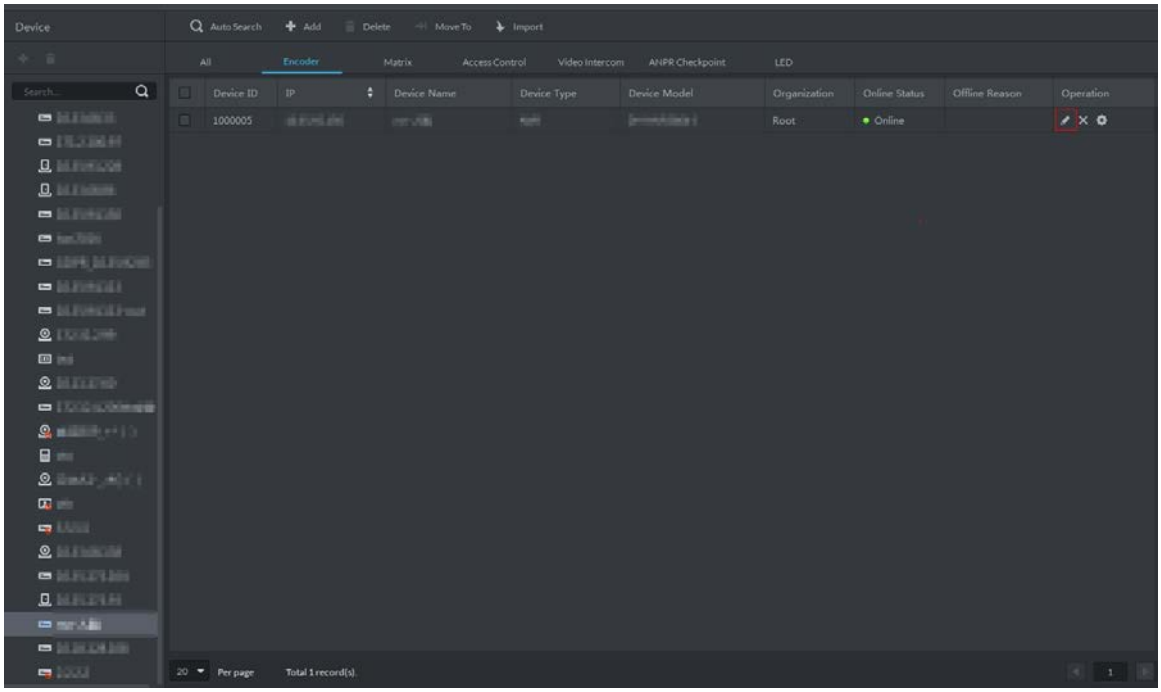
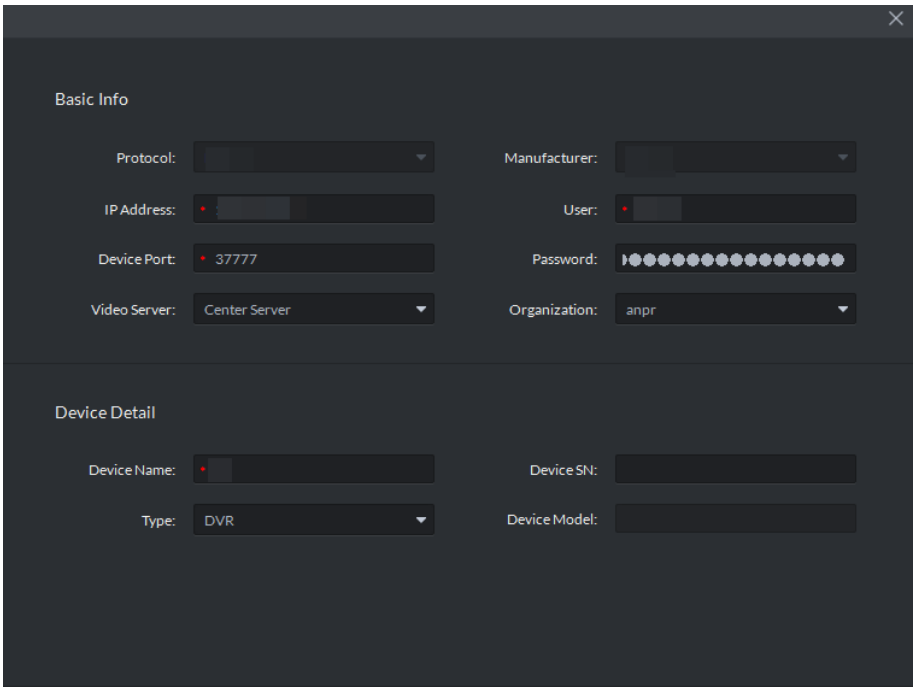


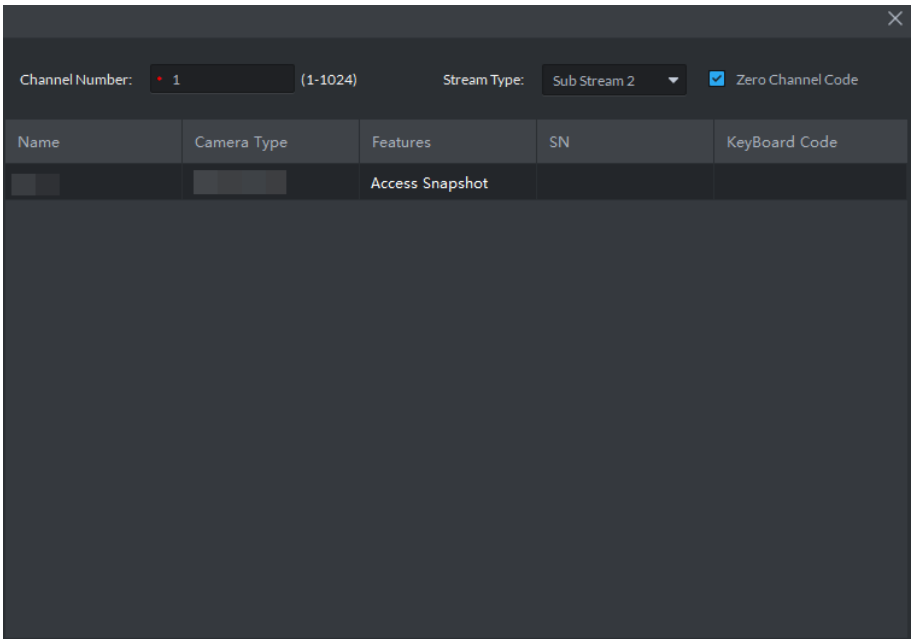
Figure 4-360 Edit device



2) Click the tab of Video Channel, set Features as Access Snapshot.

The feature of all the bound ANPR device channel is set as **Access Snapshot**.

Figure 4-361 Modify features



3) Click **OK** and complete config.

4.14.1.3 Adding Remaining Parking Screen

Collect the data of vehicle entrance and exit from ANPR camera; make statistics of parking space quantity, then parking space quantity will be displayed on the screen.

- 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"4.1.2.4 Adding Device."

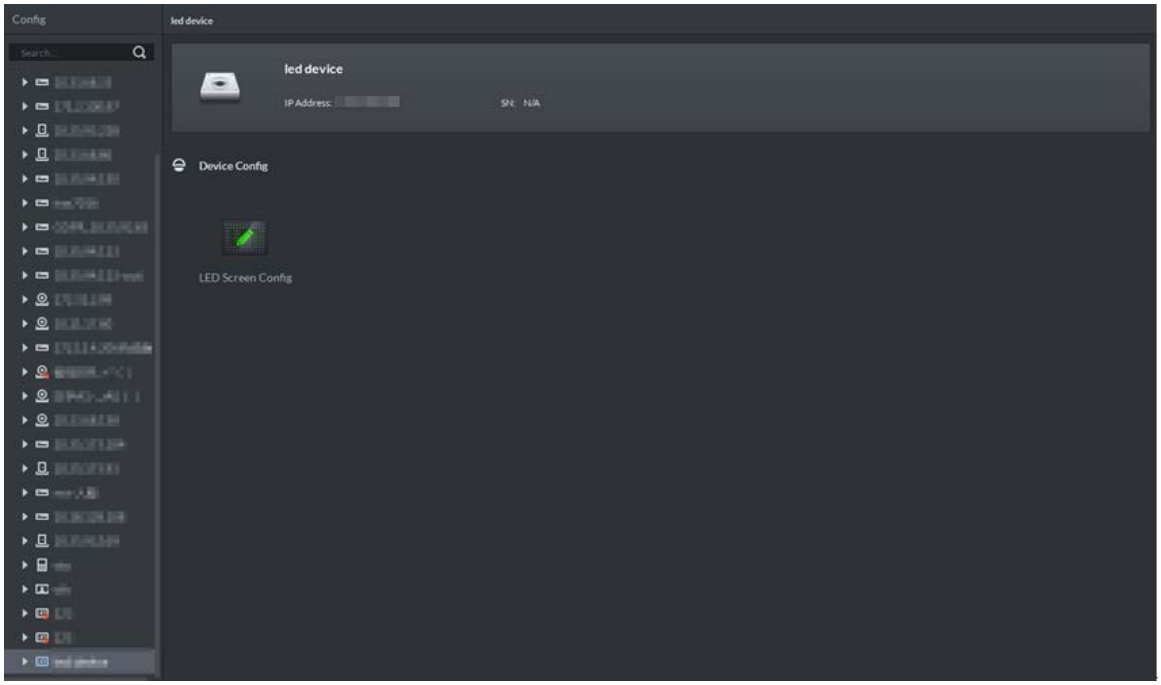
Step 2 On client homepage, click **Config**.

The **Config** interface is displayed.

Step 3 Select remaining parking screen from left device list.

The **LED Screen Config** button is displayed. See Figure 4-362.

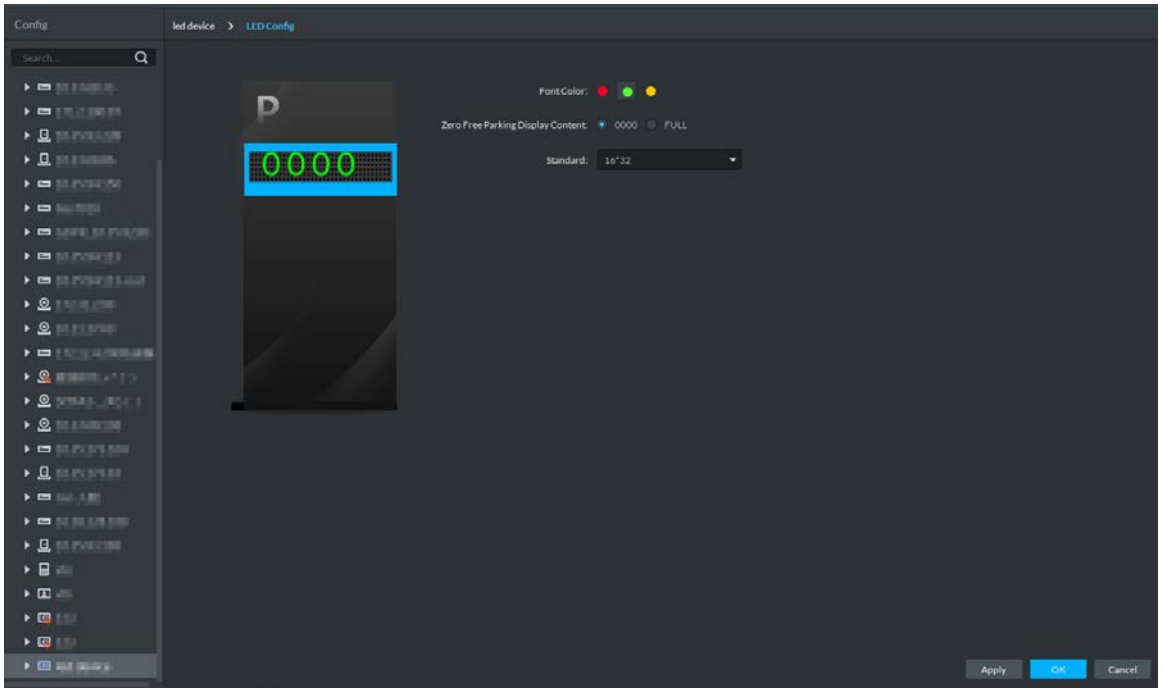
Figure 4-362 LED screen config



Step 4 Click LED Screen Config.

The **LED Config** interface is displayed. See Figure 4-363.

Figure 4-363 LED config



Step 5 You can set **Font Color** and **Zero Free Parking Display Content**. See Figure 4-363.

Font color is the color of the words displayed on the screen; Zero free parking display content is the information displayed on the screen when there is no parking space available.

Step 6 Click **OK** to complete config.

4.14.1.4 Adding Common Screen

Add common screen and display vehicle info. Currently the platform supports Jezetek common screen.

- Please make sure common screen is configured before adding, such as modifying IP address.
- Common screen is categorized as **LED Device**.

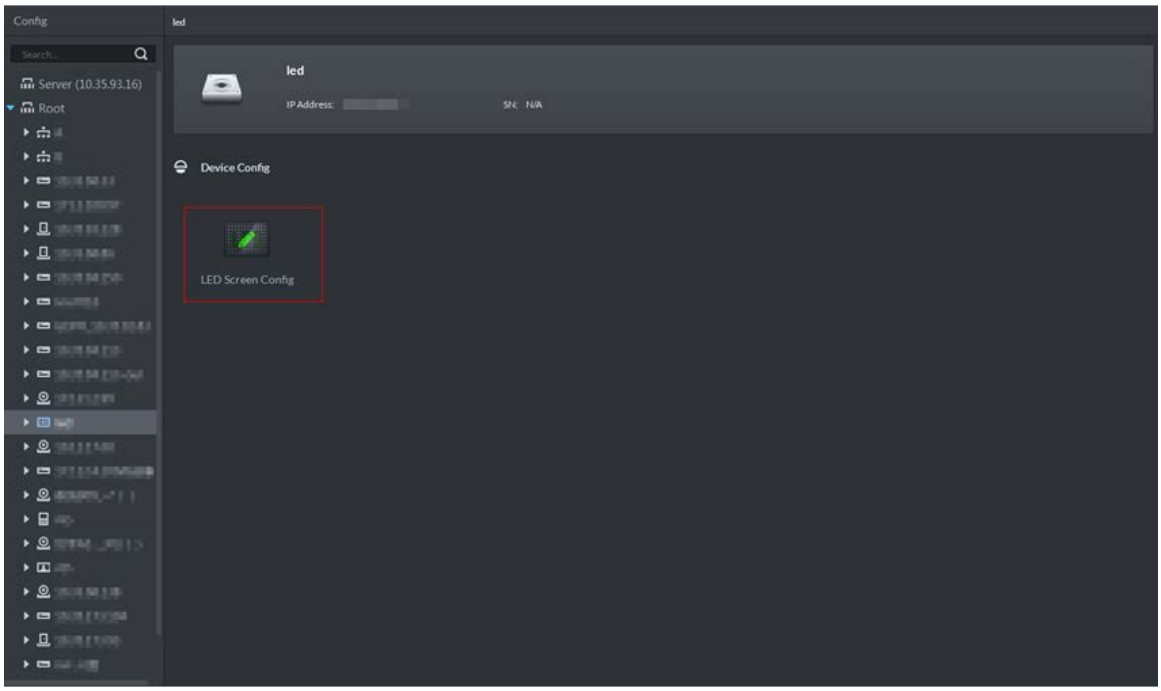
Step 1 Add common screen, for more details. See"4.1.2.4 Adding Device."

Step 2 On client homepage, click **Config**.

The **Config** interface is displayed.

Step 3 Select common screen from left device list.

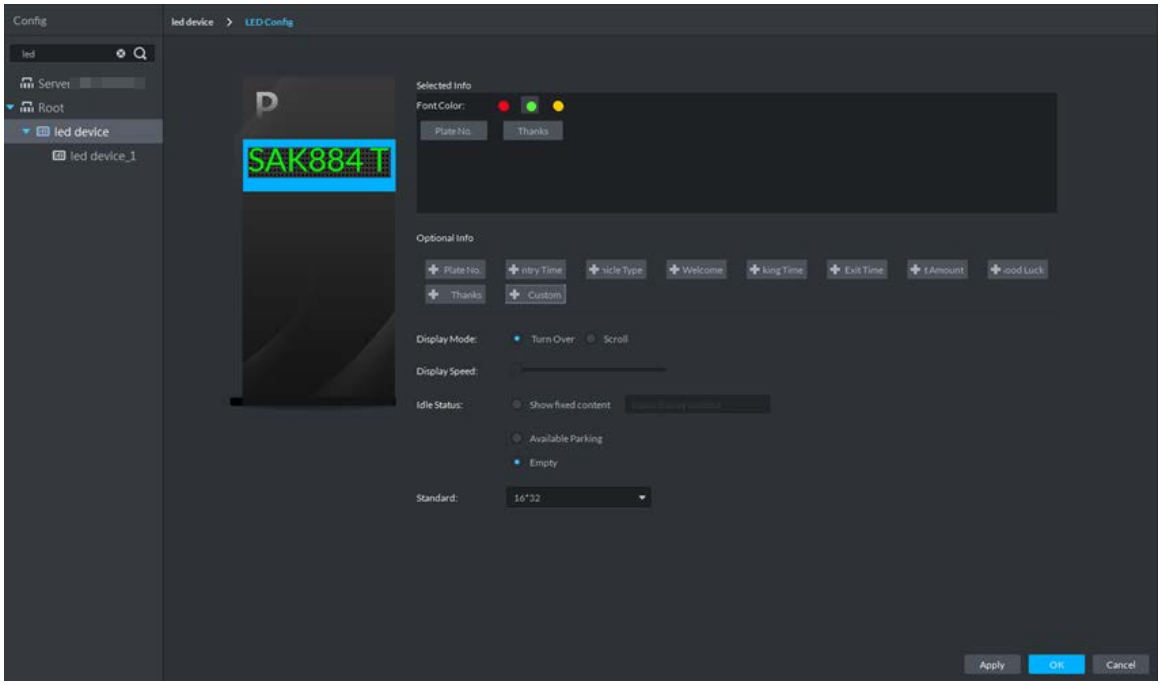
The button of **LED Screen Config** is displayed**.**



Step 4 Click LED Screen Config.

The **LED Screen Config** interface is displayed. See Figure 4-364.

Figure 4-364 LED config



Step 5 Set font color and info content, select display mode, display speed and show fixed content during idle status.

Step 6 Click **OK** and complete config.

4.14.2 Setting Picture Storage Disk

Configure local storage disk, you must reserve an ANPR picture disk to store ANPR snapshots, otherwise, snapshots cannot be stored or displayed. For more details, see"4.1.1.4 Setting Storage Space."

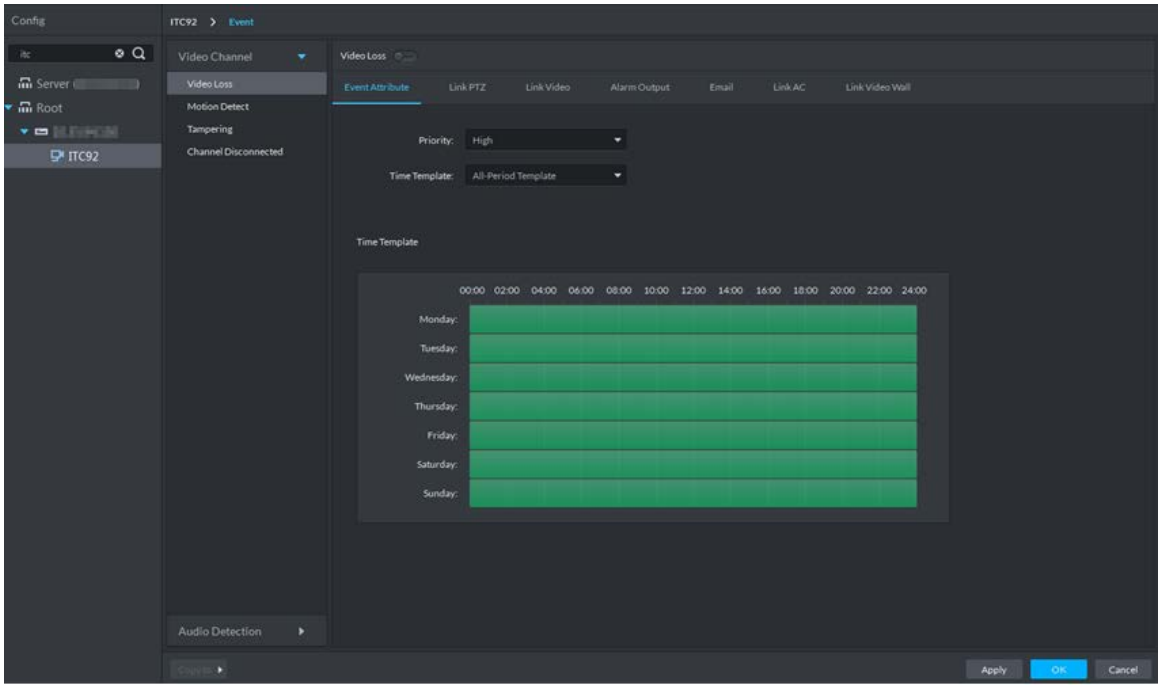
4.14.3 Setting Alarm Event

This chapter introduces entrance alarm, for more alarm events and details, refer to"4.1.4 Setting Alarm Event." Entrance alarms include following types.

- LPR (License plate recognition)
  After license plate is recognized by ANPR, reported to platform by NVR, the platform triggers alarm, and extract video before and after license plate recognition, saved into platform. The default video duration is 20s, 10s before and 10s after alarm is triggered.
- Blocked list alarm
  The platform supports marking some plate number as blocked list vehicle, meanwhile, compare the recognized plate number with blocked plated number, if it is the blocked plated number, then alarm is triggered.
  If you want to mark some plate number as blocked plate number, see"4.14.5 Vehicle Management."
- Parking timeout
  The parking duration exceeds the threshold, and then alarm is triggered.

Set alarm events. See Figure 4-365.

Figure 4-365 Alarm event



4.14.4 Configuring Parking Lot

Generally, one parking lot is considered as an area. Parking lot config includes setting parking space quantity, release situation and other information. Bind ANPR device channel and use it to recognize vehicles, bound VTO is used to recognize people.

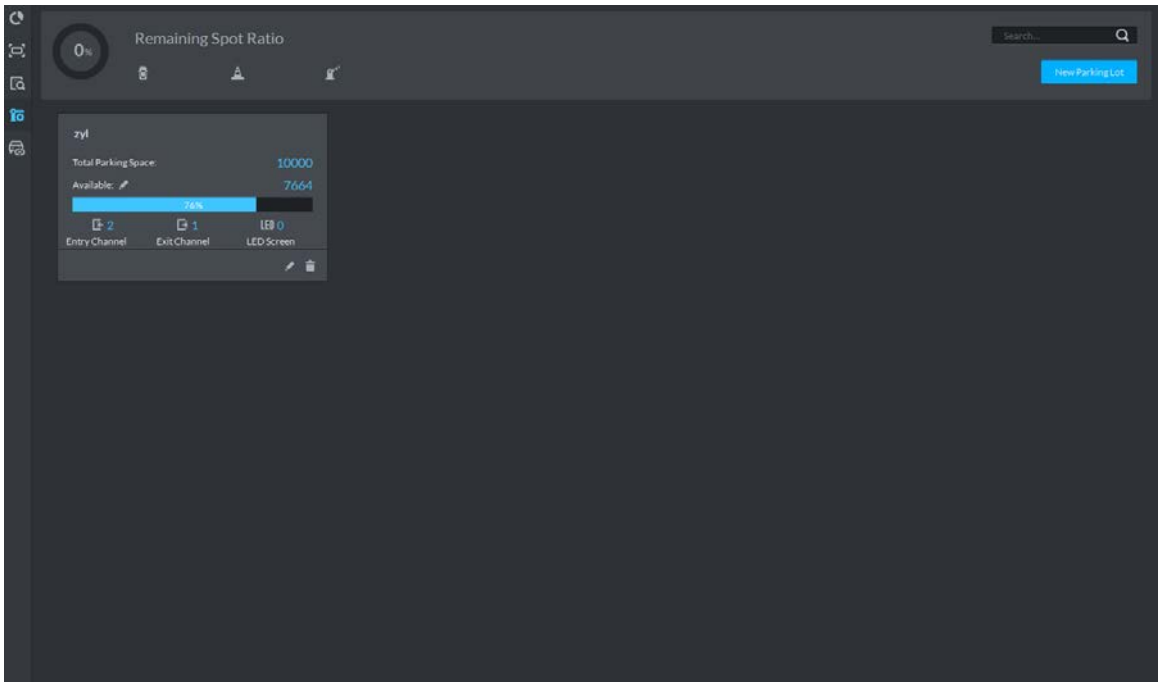
Step 1 On client homepage, click **Entrance**.

The interface of **Entrance** is displayed.

Step 2 Click  .

The interface of **Parking Lot Config** is displayed. See Figure 4-366.

Figure 4-366 Parking lot info



Step 3 Add parking lot.

1) Click New Parking Lot.
2) Configure parking lot info. For more parameter details, see Table 4-45.

Table 4-45 Parking lot info

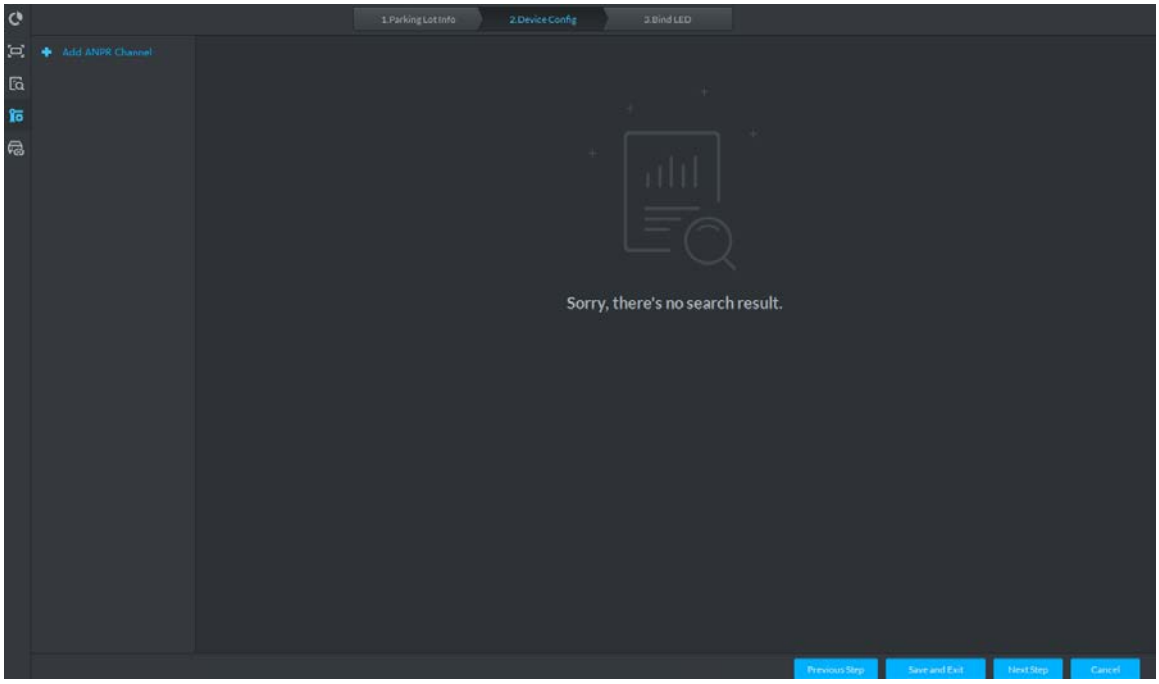
Parameter		Description
Parking Lot Info	Name	Parking lot name, used to recognize different areas.
	Total parking space	Total available parking space of the area.
	Available	Available parking lot quantity when configuring area.
Entry Release	Time template	Select the time template which conforms to entry release. If default template fails to meet the requirement, you can select **Manage Time Template** to set custom time template. Default templates include: ● 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. ● Allowlist Allowlist vehicles include several vehicle types, such as no group, general and VIP. Only three types of vehicle above are allowed to enter when remaining space is zero. ● VIP Only VIP vehicle is allowed to enter when remaining space is zero. Vehicle type should be set during vehicle management.
	Visitor auto release	Those which are not registered on DSS are considered as visitor vehicles. Confirm if it unlocks barrier automatically when visitor vehicle enters according scenario design. If it is required to release, and then click  , the icon displays as  . Otherwise, it remains as  , and it will not unlock barrier to release when visitor wants to enter parking lot.
	Alarm timeout	Vehicle enters parking lot and stays longer than threshold, alarm is triggered.

Parameter		Description
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.

3) Click **Next**.

The interface of **Device Config** is displayed. See Figure 4-367

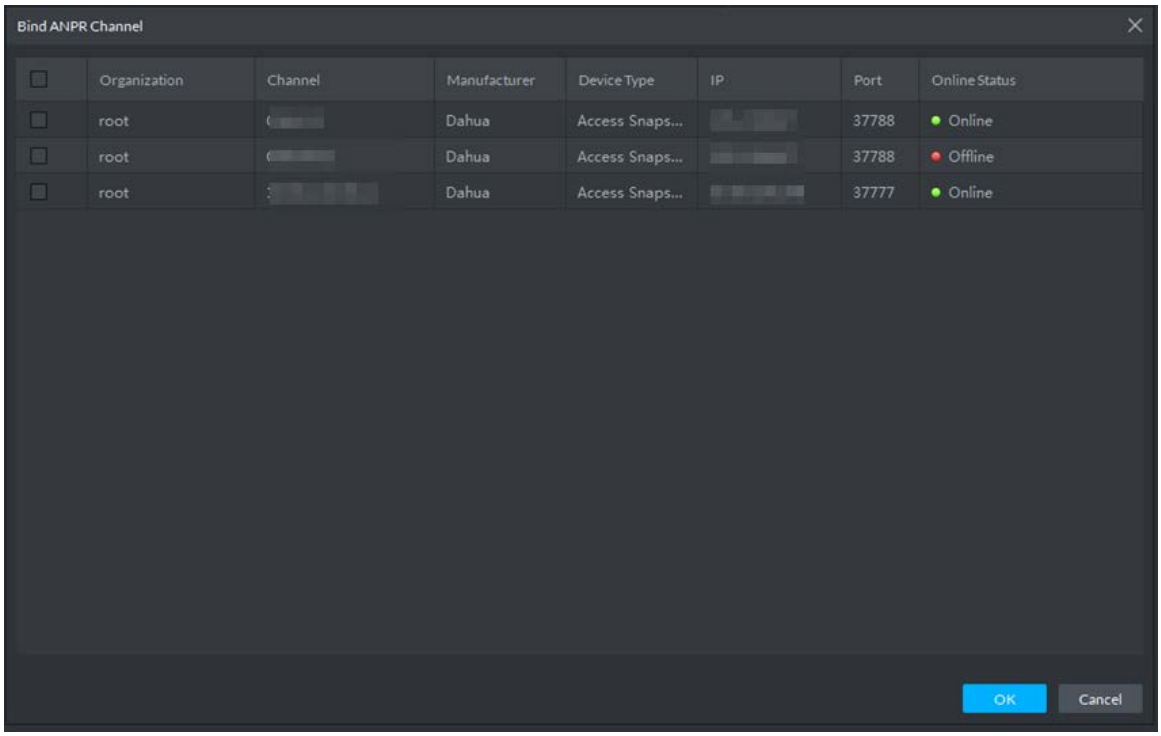
Figure 4-367 Device config



Step 4 Add ANPR device.

1) Click **Add ANPR Channel** and you can select all the ANPR devices deployed at entrance and exit of the parking lot on the interface. See Figure 4-368.

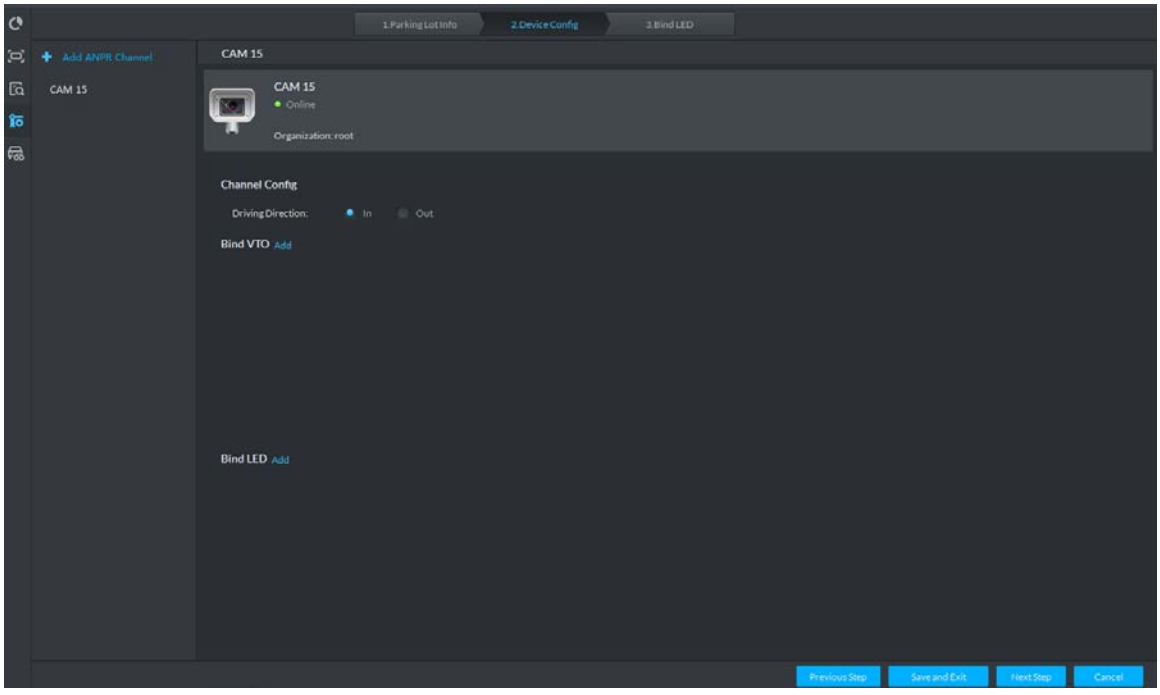
Figure 4-368 Add ANPR device



2) Click **OK**.

The information of added ANPR device is displayed. See Figure 4-369.

Figure 4-369 ANPR device info



3) Select ANPR device from device list in sequence, and set corresponding driving direction. Default driving direction is **In**.

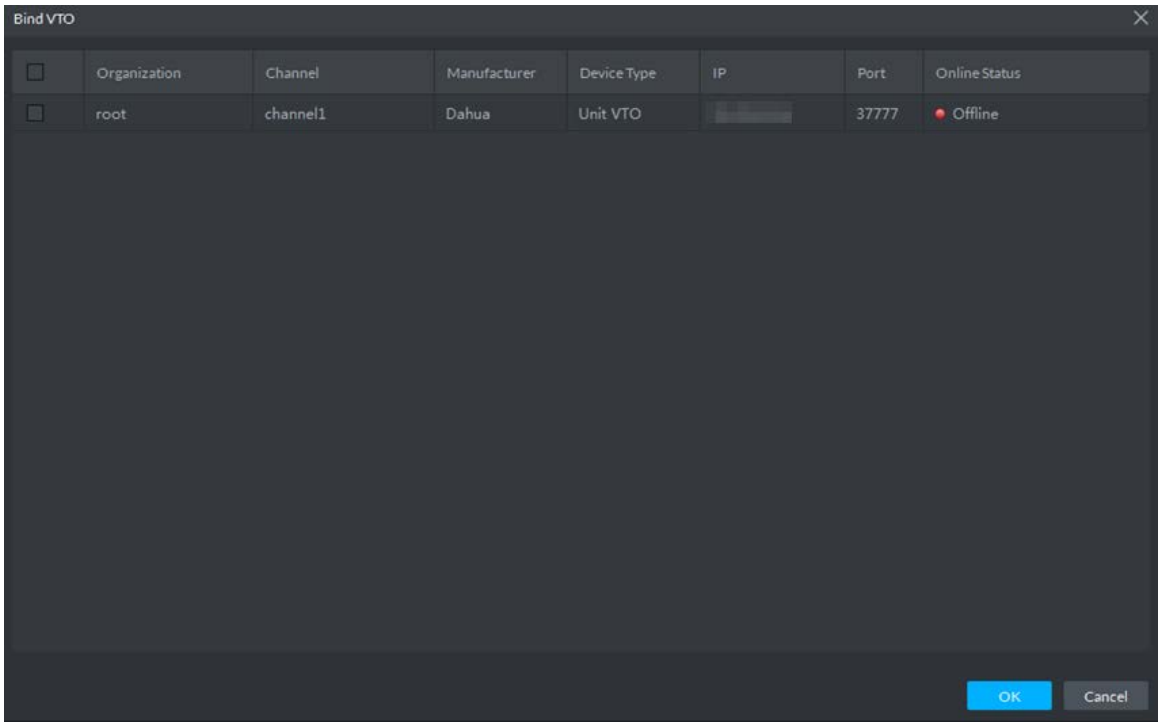
Step 5 Bind VTO device.

VTO device is used to recognize people, and unlock barrier. Please skip this step if there is no VTO in the networking.

1) Click **Add** next to **Bind VTO**.

The interface of **Bind VTO** is displayed. See Figure 4-370.

Figure 4-370 VTO device info



2) Select the VTO that is deployed next to barrier, and click OK.

The interface displays the VTO information.

Step 6 Click **Next**.

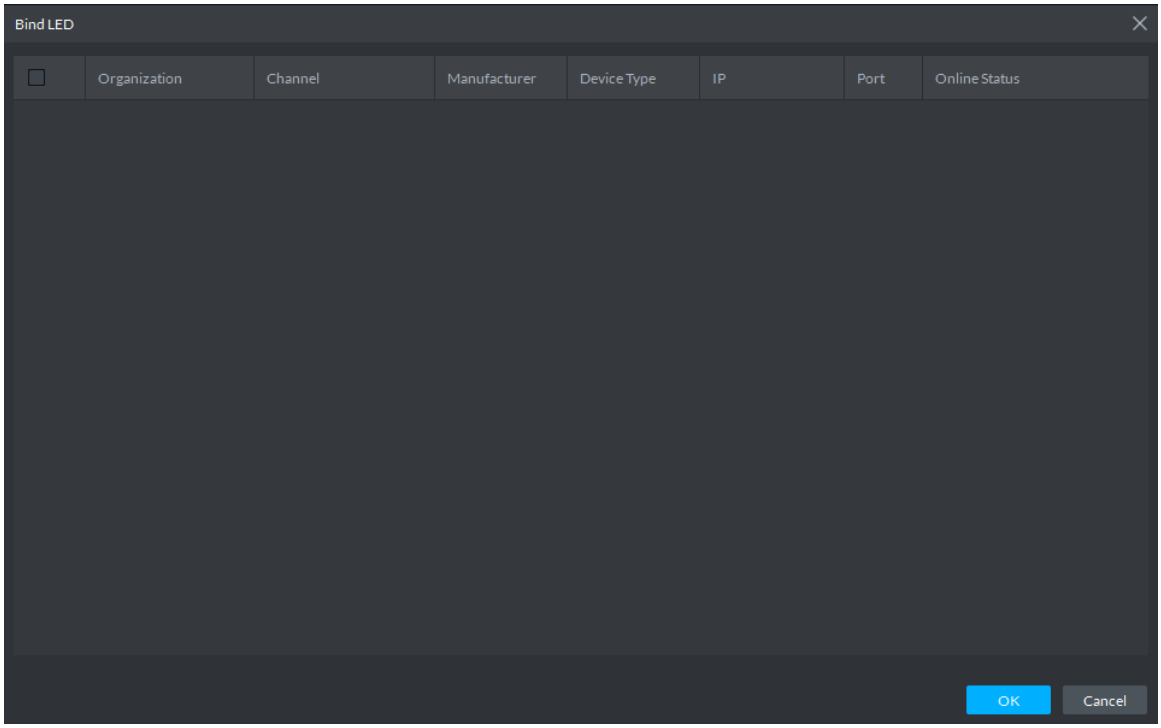
The **Bind LED** is displayed.

Step 7 Add LED.

1) Click **Add LED**.

The interface of **Bind LED** is displayed. See Figure 4-371.

Figure 4-371 LED device info



2) Select all the LED of the parking lot and click **OK**.

The information of LED is displayed.

4.14.5 Vehicle Management

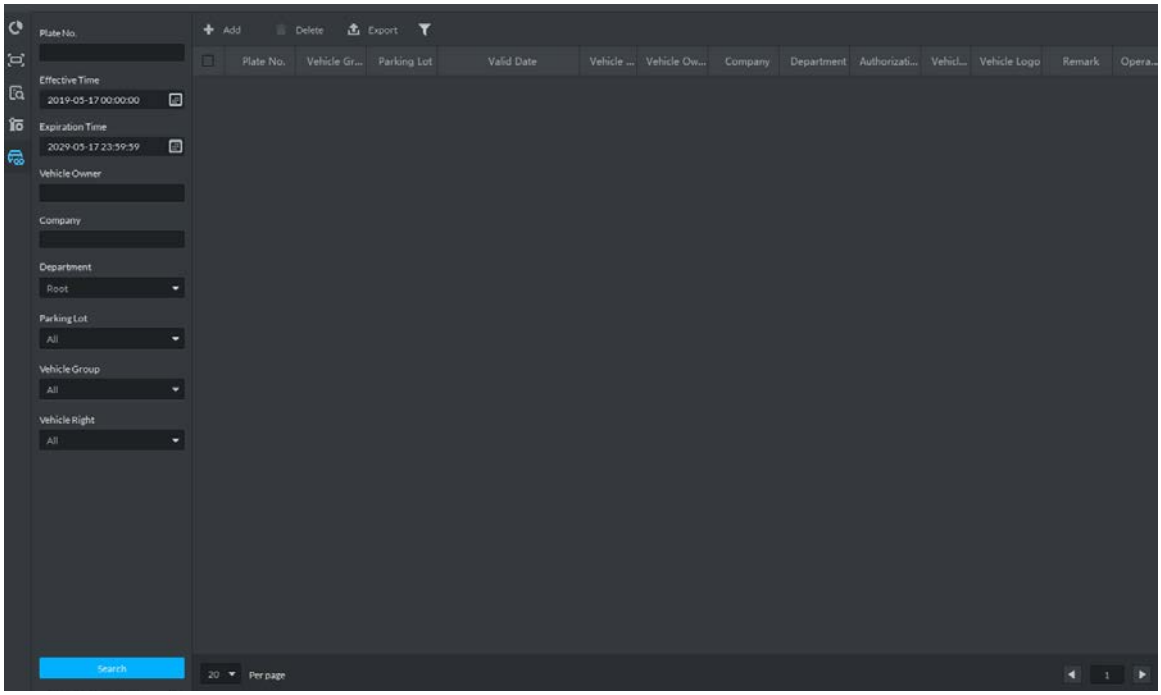
Vehicle info management includes vehicle type, department, related personnel and release ANPR, which are used as judgment basis to confirm if the vehicle can enter some area. Vehicle management can synchronize added vehicle info from personnel management module.

Step 1 Click on the interface of **Entrance**.

The interface of **Vehicle Management** is displayed. See Figure 4-372.

You can set serach condition, click **Search** and the system displays vehicle info including vehicle information added on personnel management module.

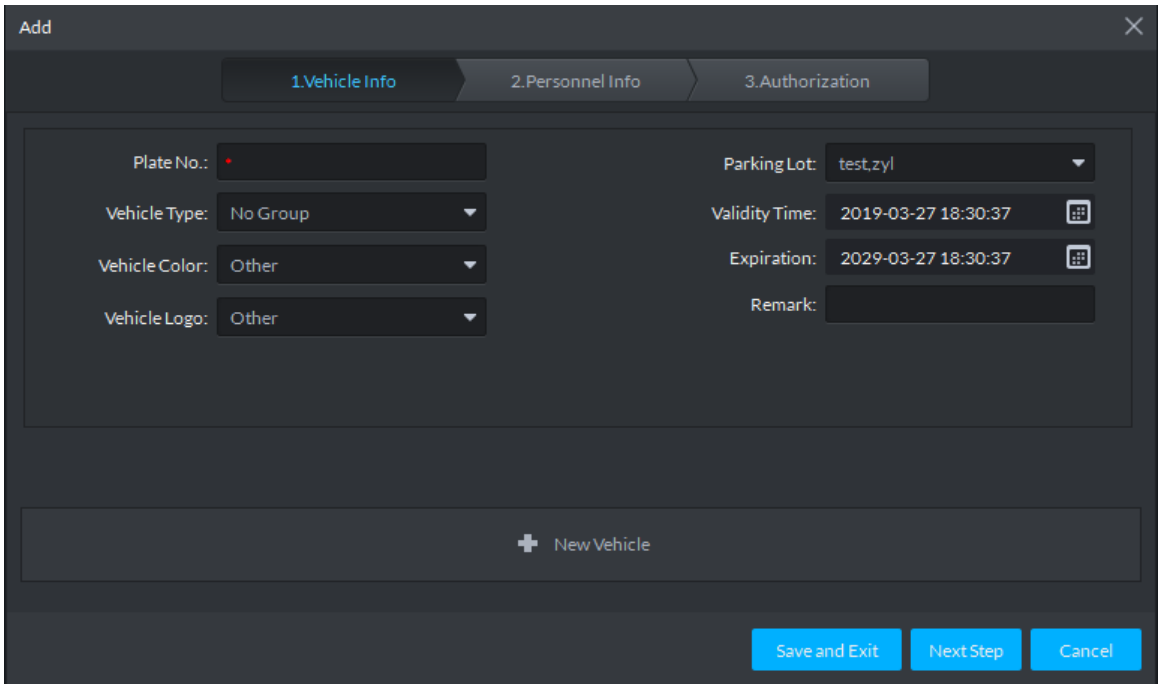
Figure 4-372 Vehicle management



Step 2 Click **Add**.

The interface of **Add** is displayed. See Figure 4-373.

Figure 4-373 Add vehicle



Step 3 Click the tab of **Vehicle Info** and add vehicle info, click **Next** and the interface of **Personnel Info** is displayed. Refer to Figure 4-374. Refer to Table 4-46 for parameter details.

Figure 4-374 Personnel info

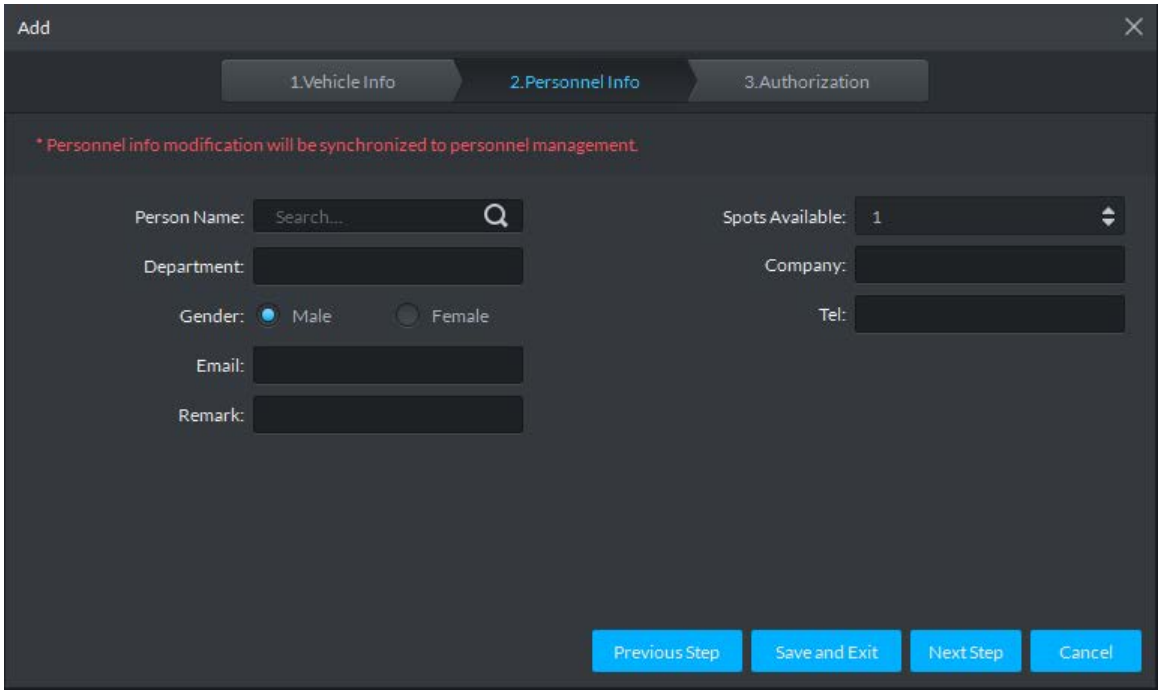


Table 4-46 Vehicle info

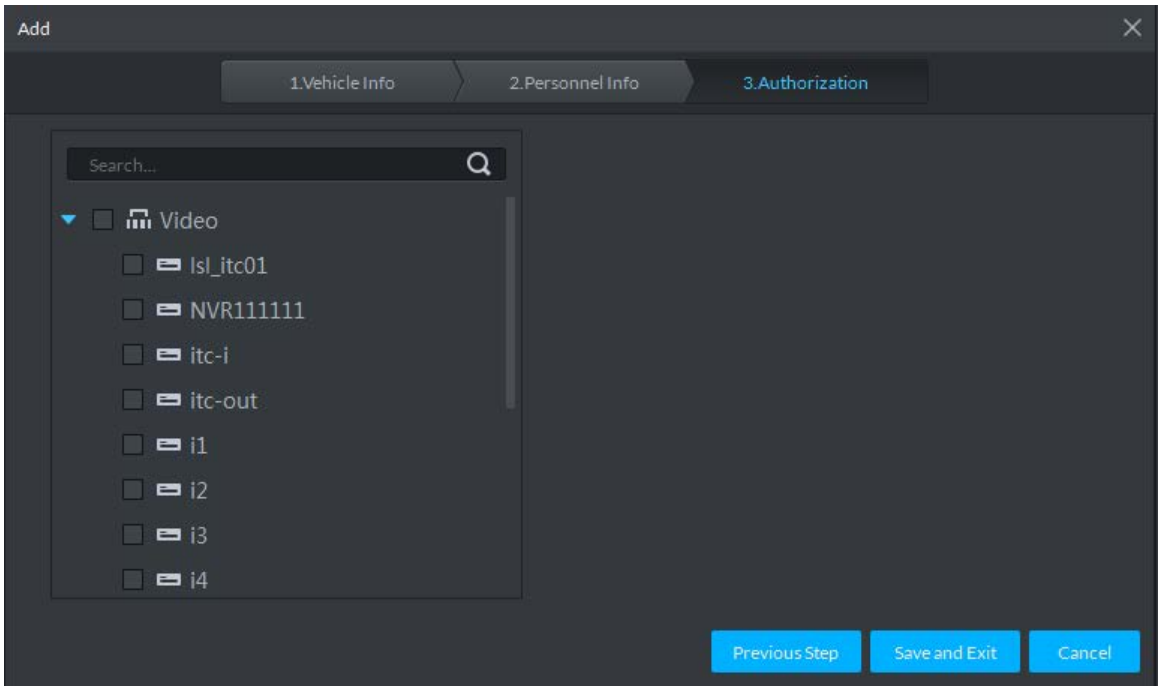
Parameter	Description
Plate No.	The plate number of added vehicle.
Vehicle Type	Include no group, general, VIP and blocklist. The first three types make up allowlist. If blocklist alarm scheme is set, then set vehicle type as blocklist, it will trigger alarm when vehicle is recognized.

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 **Authorization** interface is displayed. See Figure 4-375.

Figure 4-375 Authentication



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, and make sure the ANPR device can make judgment if it has to release the vehicle even if ANPR device is disconnected to platform.

4.14.6 Entrance Application

4.14.6.1 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 interface of **Overview** is displayed. See Figure 4-376. Refer to Table 4-47 for parameter details.

Figure 4-376 Overview

Table 4-47 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.
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.

4.14.6.2 License Plate Recognition

Click  on the **Entrance** interface. The interface of **License Plate Recognition** is displayed. See Figure 4-377. Refer to Table 4-48 for more parameter details.

Figure 4-377 LPR

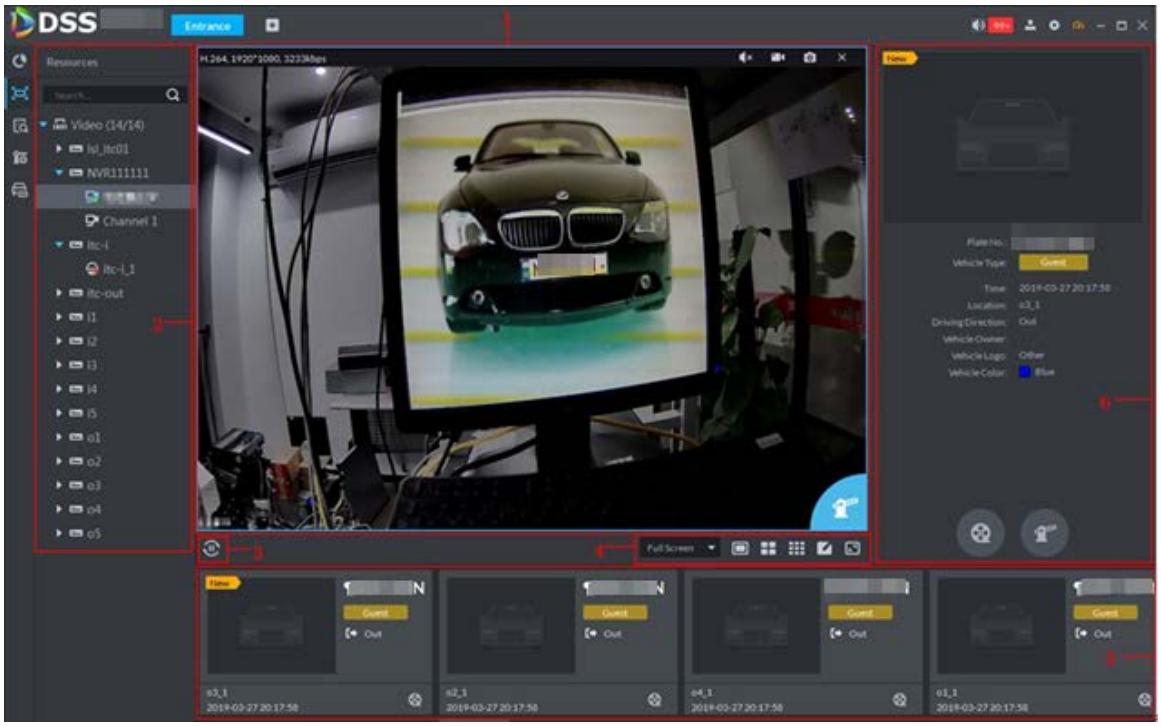
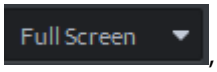


Table 4-48 LPR interface description

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	•  , set height and width ratio of video window, it plays video by two modes which are original scale and full screen. •  , used to set image split mode, which includes 1 split, 4 splits and 9 splits, or click  and customize split mode. •  , switch video window to **Full Screen** mode. If you want to exit **Full Screen**, you can also press ESC button or right click to select **Exit Full Screen**.

SN	Description
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.

4.14.6.3 Info Query

Search accessed vehicle, on-site vehicle and snapshot record.

Step 1 Click  on the **Entrance** interface.

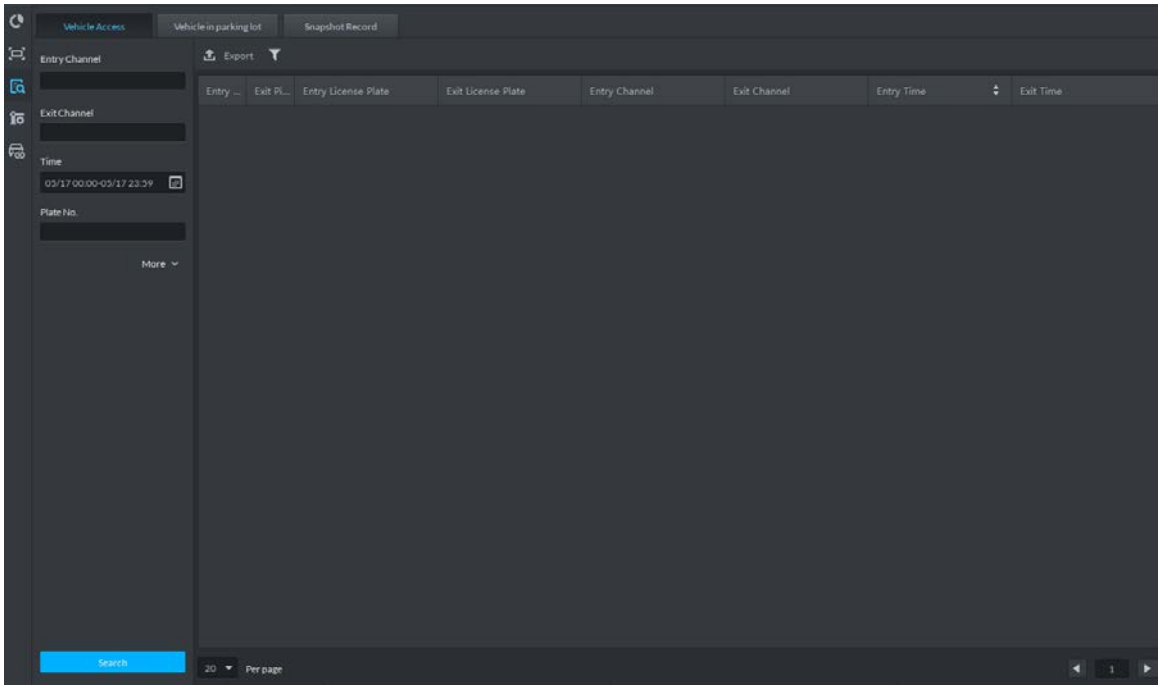
The interface of **Info Query** is displayed.

Step 2 Search vehicle in and out information.

1) Click the tab of **Vehicle Access**.

The interface of **Vehicle Access** is displayed. See Figure 4-378.

Figure 4-378 Vehicle access

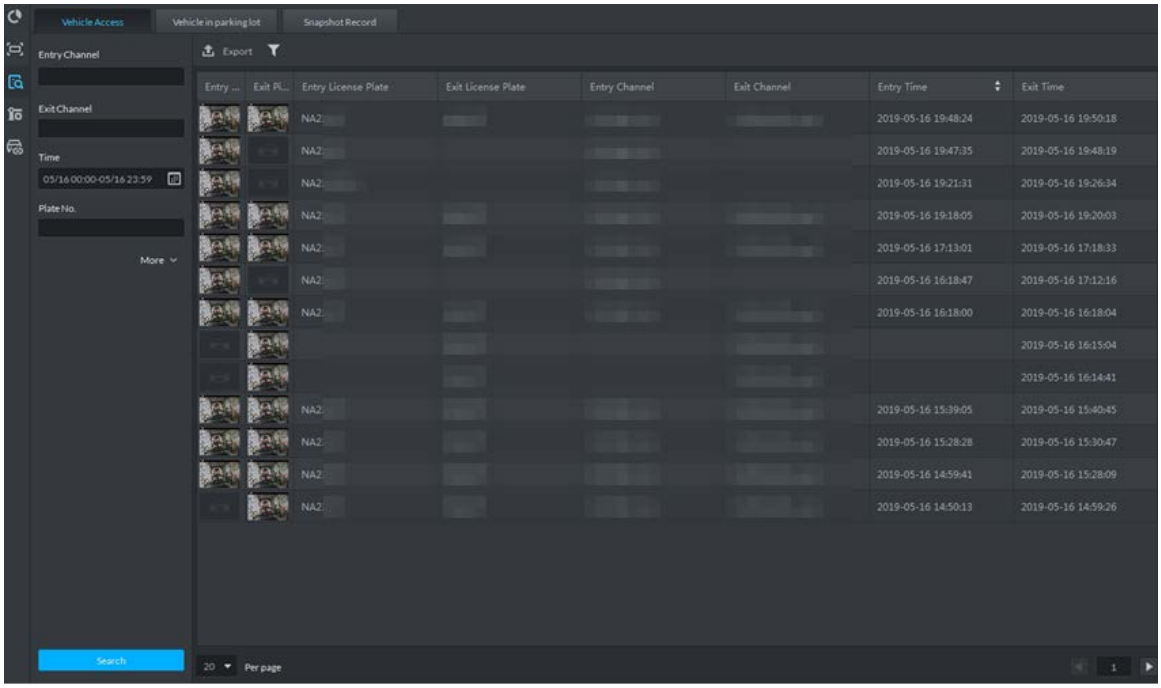


2) Set search condition, click **Search**.

The search results are displayed. See Figure 4-379.

Click **More** and you can search by vehicle owner, department and vehicle type etc.

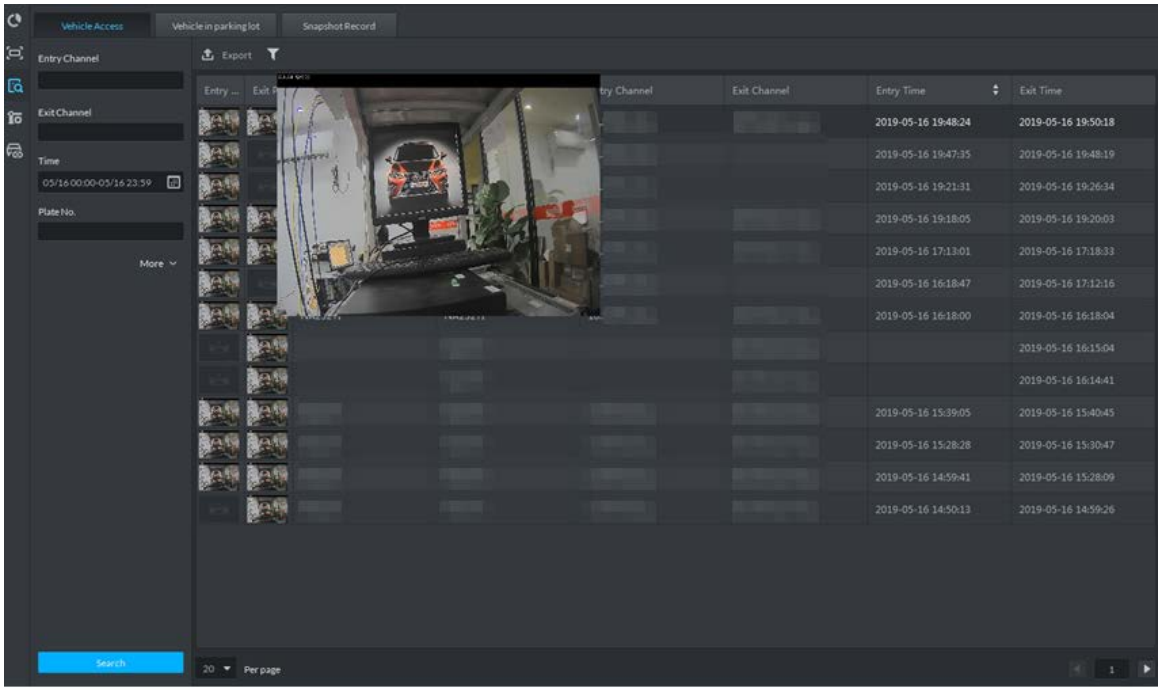
Figure 4-379 Vehicle access info



3) The related operations of vehicle access are as follows.

◇ Move the mouse to the recorded entry picture or exit picture, and the system will display a bigger picture. See Figure 4-380.

Figure 4-380 Big vehicle picture



◇ Double click the record, and detailed info is displayed on the right of interface. See Figure 4-381. 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 4-382. Click **Edit** to modify vehicle info, click **OK** to save config. Click **Video** to view linked video.

Figure 4-381 Vehicle details (1)

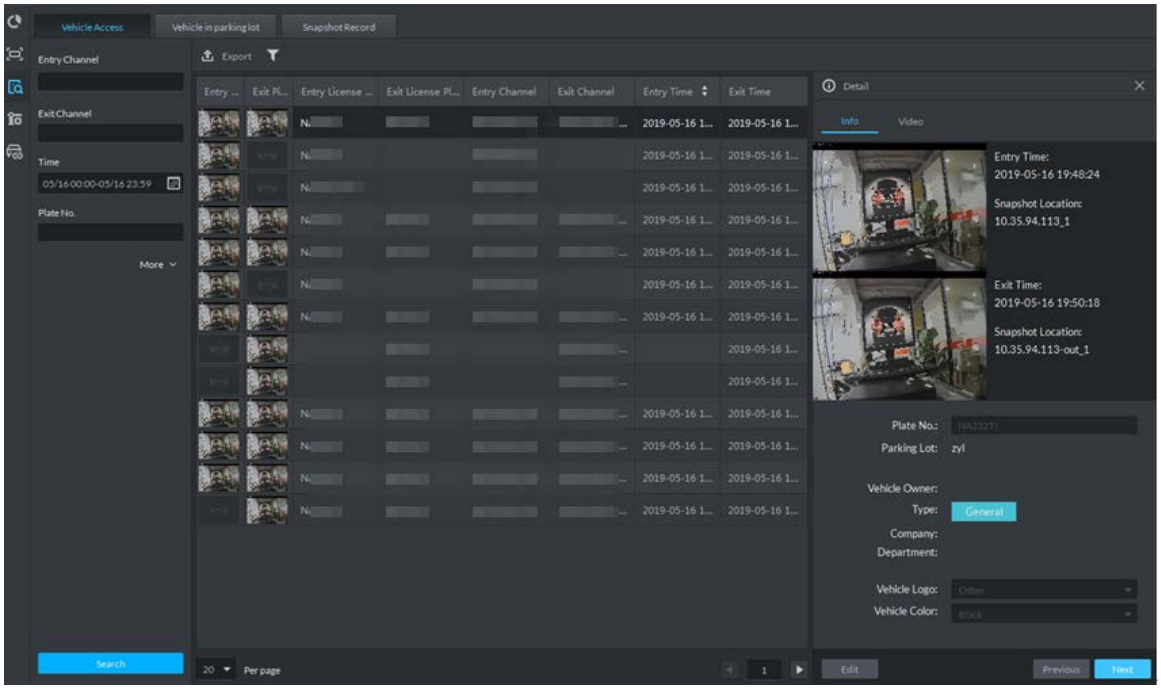
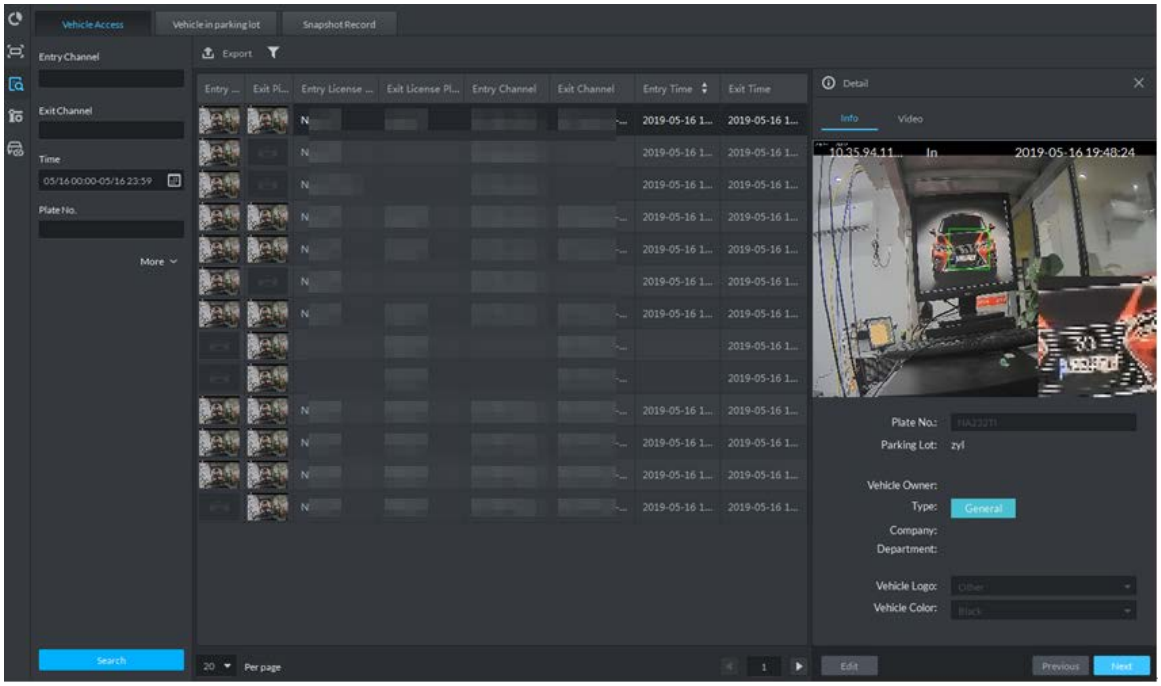


Figure 4-382 Vehicle details (2)



◇ Export info. Click **Export** to export all the searched vehicle access info.

◇ Set info display item. Click  and select display item.

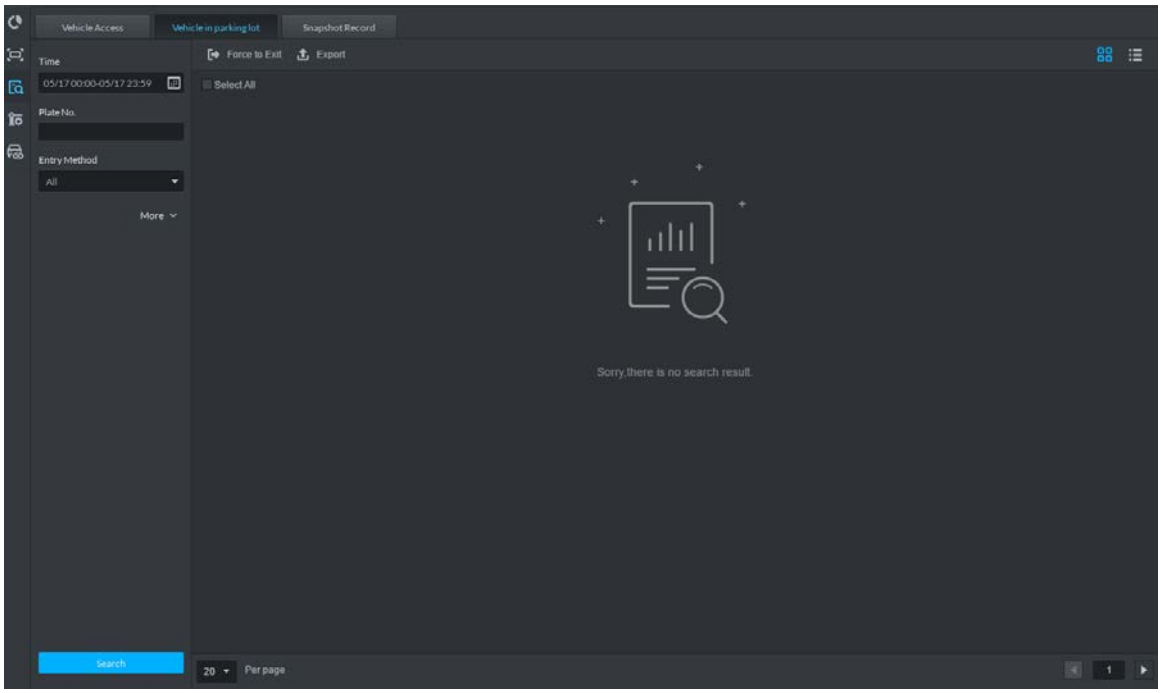
◇ Click **Next** and display next info detail. Click **Previous** and display previous info detail.

Step 3 Search on-site vehicle.

1) Click the tab of Vehicle in parking lot.

The interface of **Vehicle in Parking Lot** is displayed. See Figure 4-383.

Figure 4-383 Vehicle in parking lot

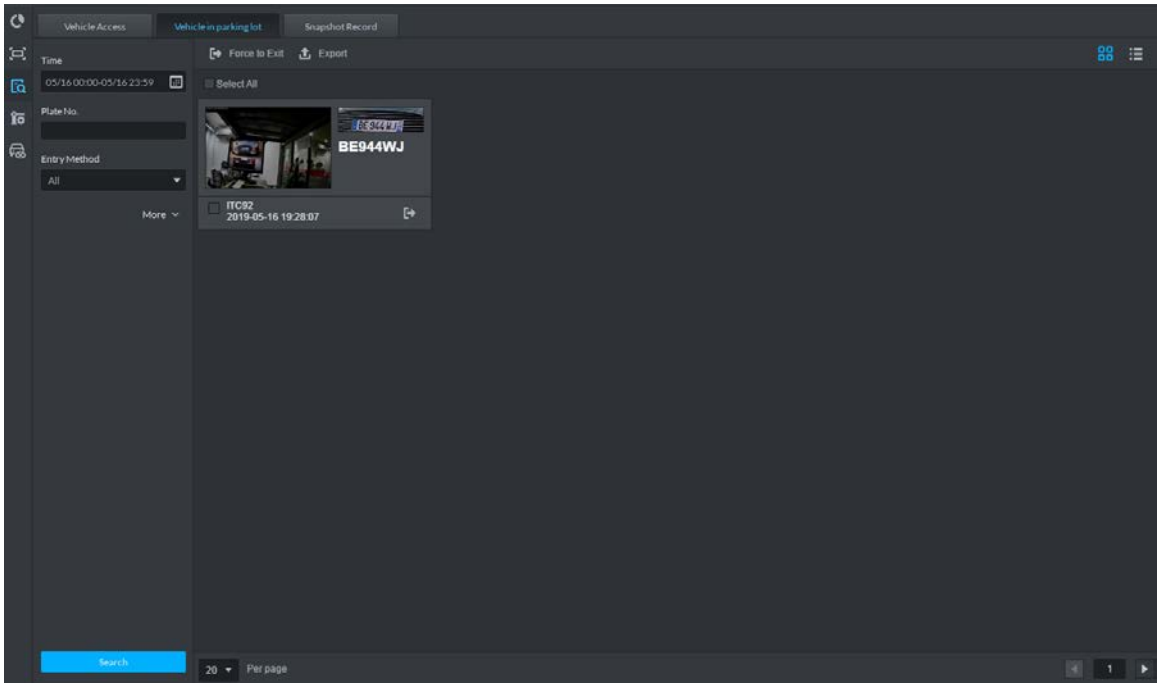


2) Set search condition, Click **Search**.

The search results are displayed. See Figure 4-384.

Click **More** and you can search info by vehicle owner, department and vehicle type etc.

Figure 4-384 Vehicle in parking lot info



3) Related operations of vehicle in and out are as follows.

◇ If the vehicle is confirmed not to be in the area, then click to select information (several items supported), and click **Force to Exit** or . Make sure the vehicle exits by Pro.

◇ Export information. Click **Export** and export all the information of on-site vehicles that can be searched.

◇ Set info display item. Click and select display item.

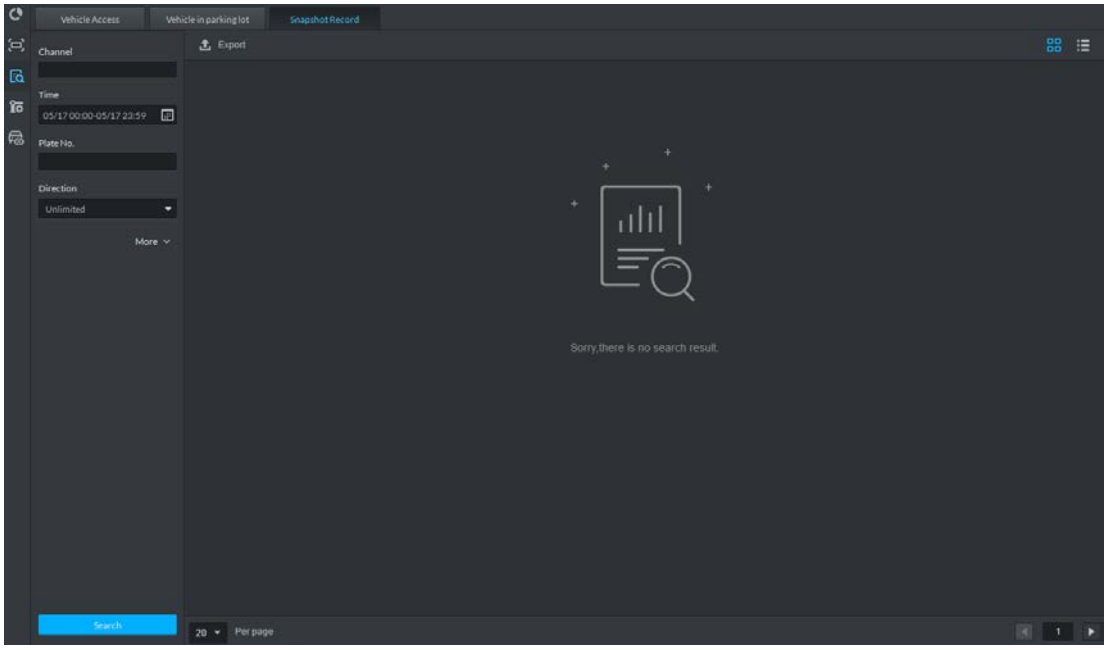
◇ Click view mode ( ) or list mode ( ) to select different display mode.

Step 4 Search Snapshot Record

1) Click the tab of **Snapshot Record**.

The interface of **Snapshot Record** is displayed. See Figure 4-385.

Figure 4-385 Snapshot record

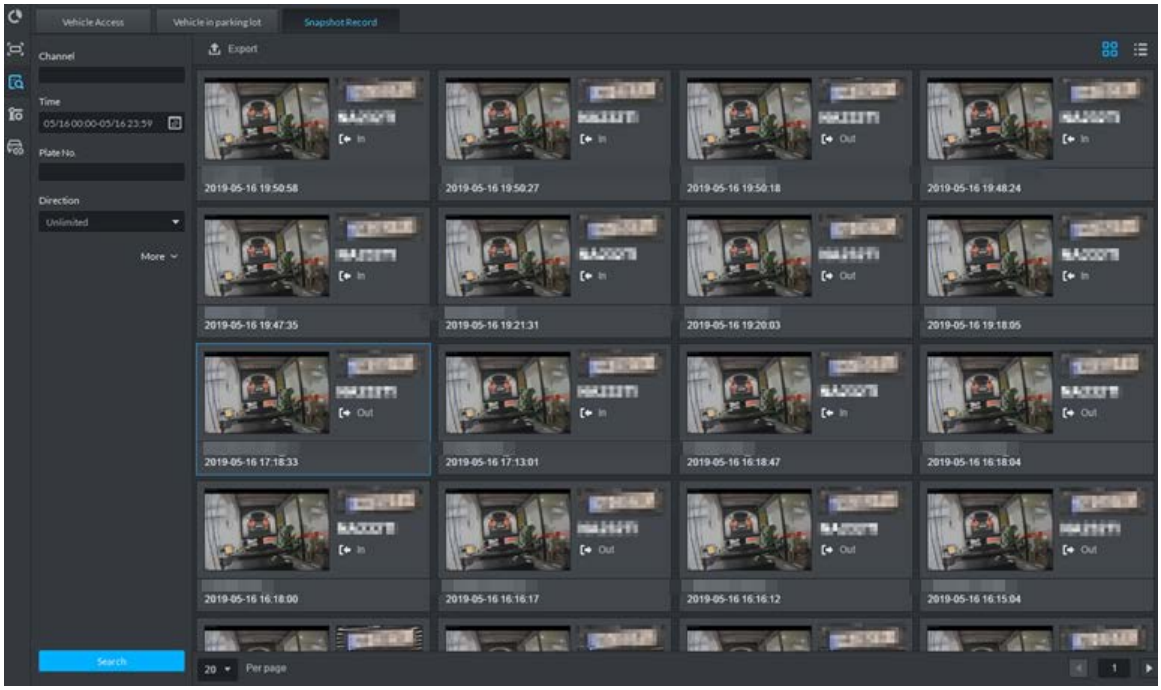


2) Set search condition, click **Search**.

The search results are displayed. See Figure 4-386.

Click **More** and you can search info by vehicle owner, department and vehicle type etc.

Figure 4-386 Snapshot record info



3) Related operations of vehicle snapshot are as follows.

◇ Export info. Click **Export** to export all the info of on-site vehicles that can be searched.

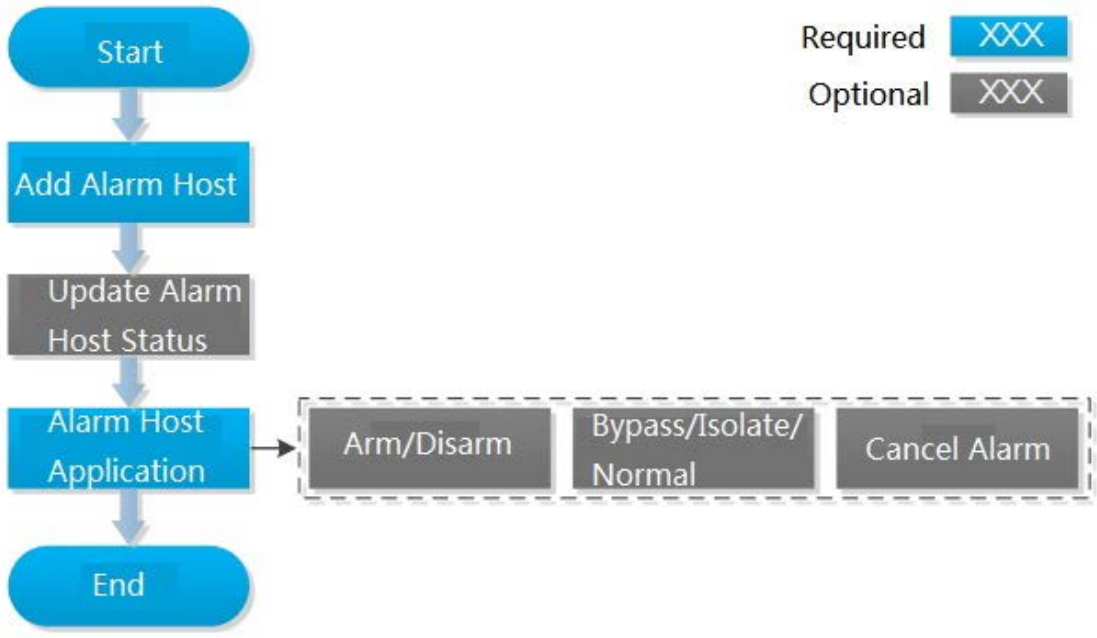
◇ Click view mode ( ) or list mode ( ) and select different display modes.

4.15 Alarm Host

After adding alarm host to platform, you can manage and configure alarm zone and sub system.

The alarm host operation flow is shown in Figure 4-387.

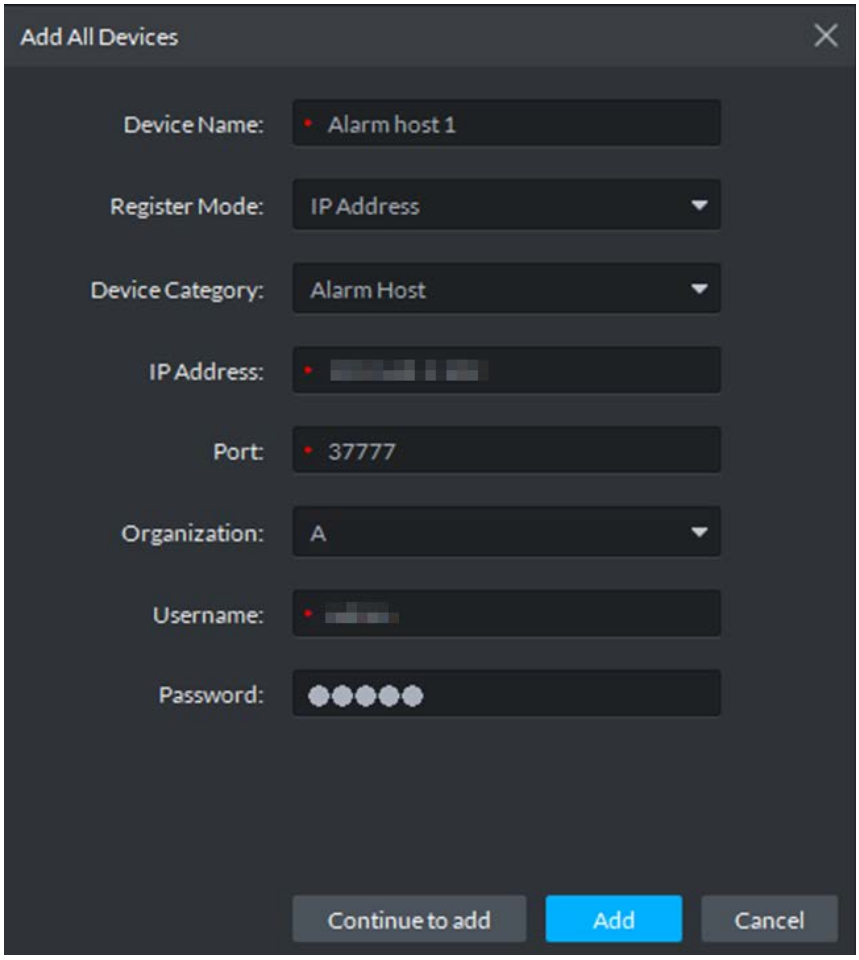
Figure 4-387 Alarm host management flow



4.15.1 Adding Alarm Host

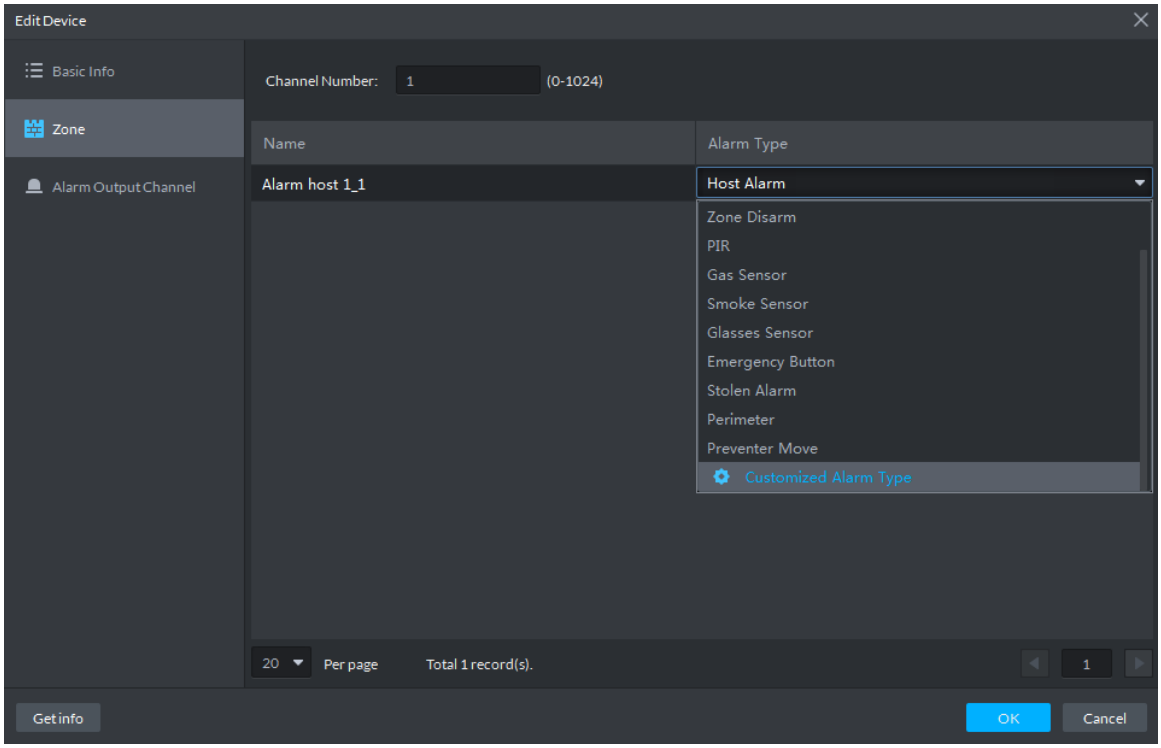
Step 1 Add alarm host, set **Device Category** as **Alarm Host**, and see Figure 4-388. For more details, see"4.1.2.4 Adding Device."

Figure 4-388 Add alarm host



Step 2 Modify device zone info. For example, zone is connected to smoke sensor, then select **Alarm Type** as **Smoke Sensor**. See Figure 4-389. Alarm type supports custom, you can select **Customized Alarm Type** from the **Alarm Type** box, and set the alarm type you need, used to quickly recognize alarm. After config, on event config interface, corresponding alarm input can configure corresponding alarm event.

Figure 4-389 Modify zone



4.15.2 Entering Alarm Controller Interface

Click  and select Alarm Controller on the client homepage. The **Alarm Controller** interface is displayed. See Figure 4-390.

Figure 4-390 Alarm controller interface

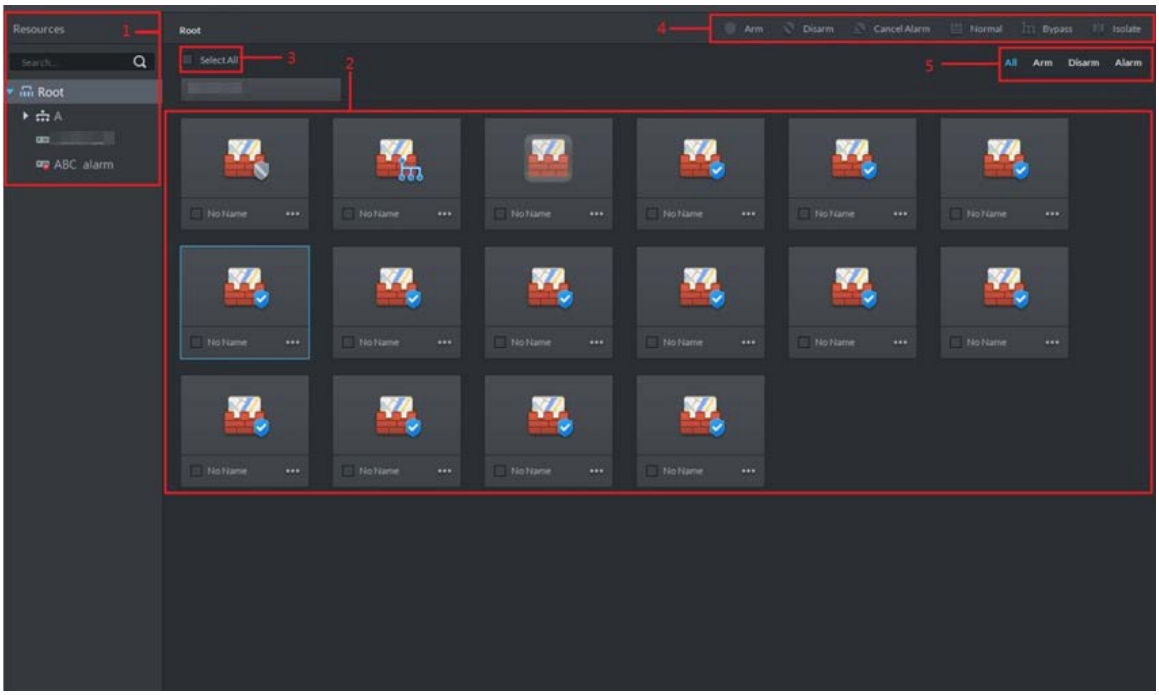


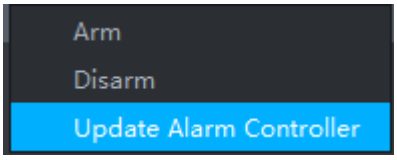
Table 4-49 Alarm controller interface description

No.	Name	Description
1	Device list	Display all alarm controller devices and subsystems under device. Icon status of subsystem ●  , no zone under subsystem. ●  , zone exists under subsystem  The subsystem and zone info displayed on platform can be acquired from device; the platform does not support config.
2	Subsystem and zone list	If you select alarm controller device from the left device list, display subsystem under alarm controller and zones not added to subsystem; if you select subsystem from left device list, then the platform displays zones under subsystem. The description of icon status is shown as follows. ● Zone status icon ◇  , arm. ◇  , disarm. ◇  , bypass. ◇  , isolate. ● Subsystem status icon ◇  , all zones armed under subsystem. ◇  , all zones disarmed under subsystem. ◇  , zones are not distributed by subsystem. ◇  , some zones under subsystem are armed.
3	Select all	Select all subsystems and zones displayed in list.
4	Operation button	Operation buttons supported by zone or subsystem.
5	Filter button	Click the button, the subsystem and zone of corresponding status are displayed in the list.

4.15.3 Updating Alarm Controller Status

In the device tree area, right click the alarm controller that needs to be updated, select **Update Alarm Controller**, and see Figure 4-391. The platform synchronizes status of alarm controller.

Figure 4-391 Update alarm controller



4.15.4 Alarm Controller Application

4.15.4.1 Arm/Disarm

After armed, the alarm controller makes response upon the alarm signal from zone; You can disarm the zone and controller will not upload alarm message.

4.15.4.1.1 Global Arm/Disarm

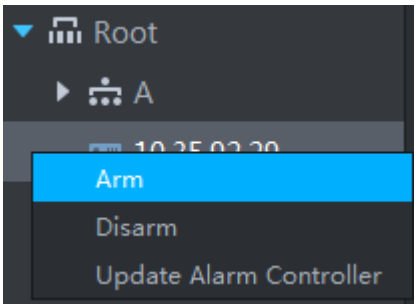
Globally arm or disarm all zones under alarm controller.

Arm

In device tree area, right click the alarm controller that needs to be armed globally, select **Arm**, and see Figure 4-392.

Arm fails when alarm input exists in zone. Please disarm if you continue to arm, clear alarms in each zone, zone with alarm input exists in bypass, and then arm again.

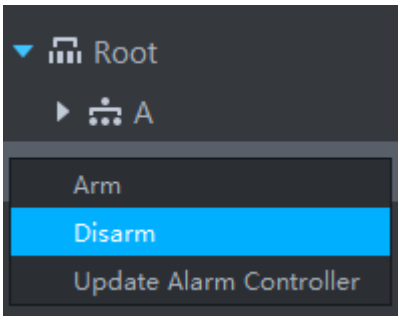
Figure 4-392 Global arm



Disarm

In device tree area, right click the alarm controller that needs to be disarmed globally, select **Disarm**, and see Figure 4-393.

Figure 4-393 Global disarm



4.15.4.1.2 Arm/Disarm Zone or Subsystem

Arm or disarm single zone.

Arm

- Arm fails when alarm input exists in zone. Please disarm if you continue to arm, clear alarms in each zone, zone with alarm input exists in bypass, and then arm again.
- If subsystem has no zone, then you cannot arm or disarm subsystem.

You can arm by following two methods

- Click the zone you want to arm or ••• of corresponding subsystem, select **Arm**. See Figure 4-394 and Figure 4-395.

Figure 4-394 Arm zone

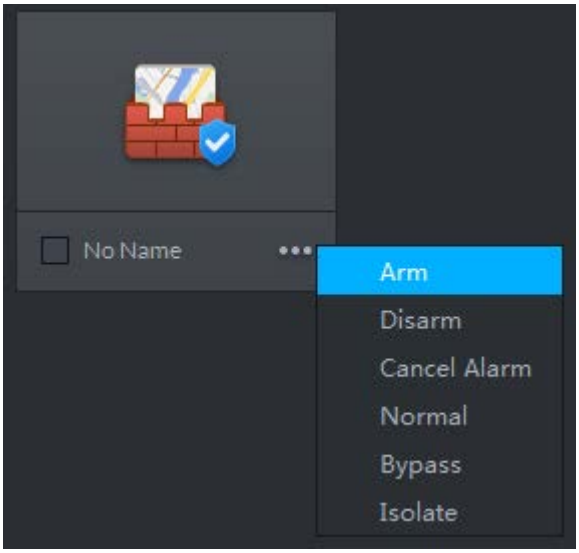
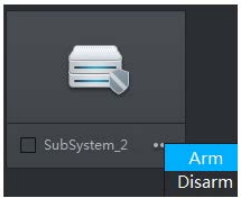
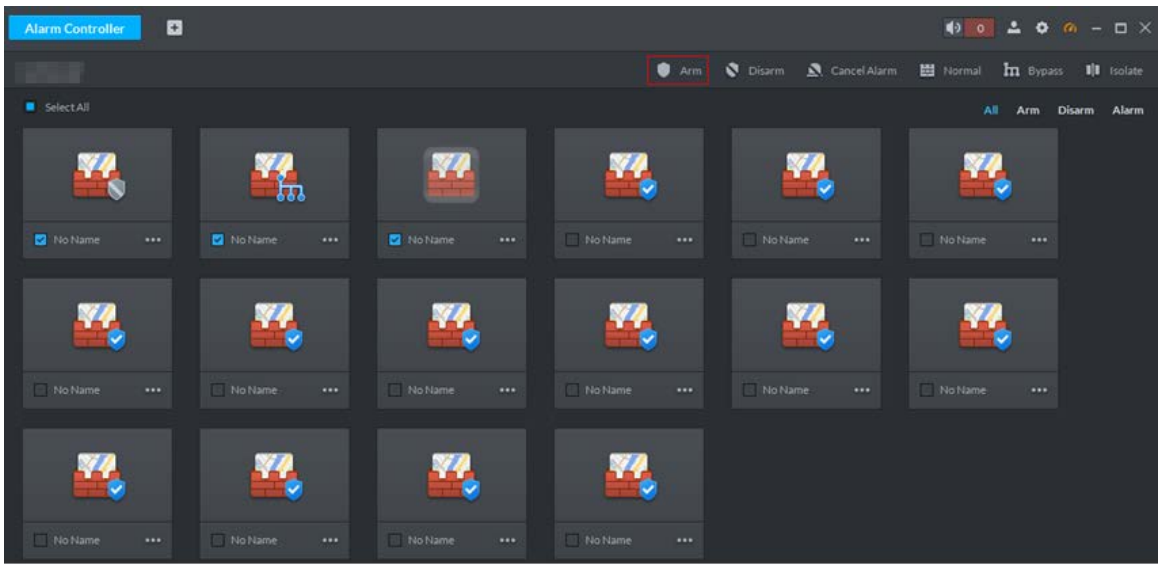


Figure 4-395 Arm subsystem



- Select the zone or subsystem you want to arm (multiple choice supported), click **Arm** on top of the interface, and see Figure 4-396.

Figure 4-396 Arm



Disarm

Supports disarm by following two methods.

- Click the zone you want to disarm or ••• of corresponding subsystem, select **Disarm**. See Figure 4-397 and Figure 4-398.

Figure 4-397 Disarm zone

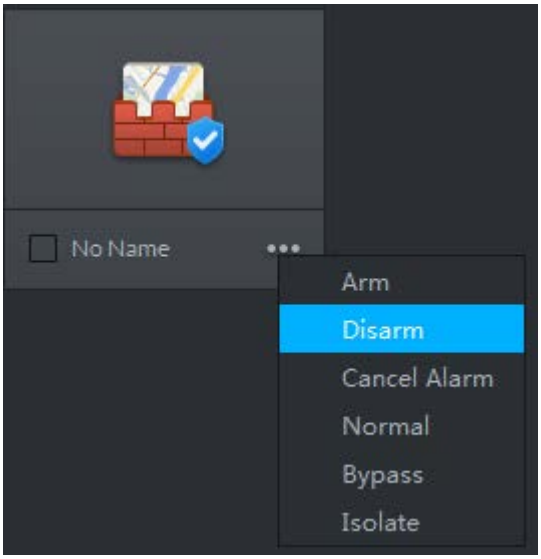
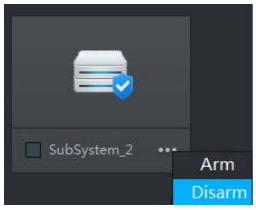
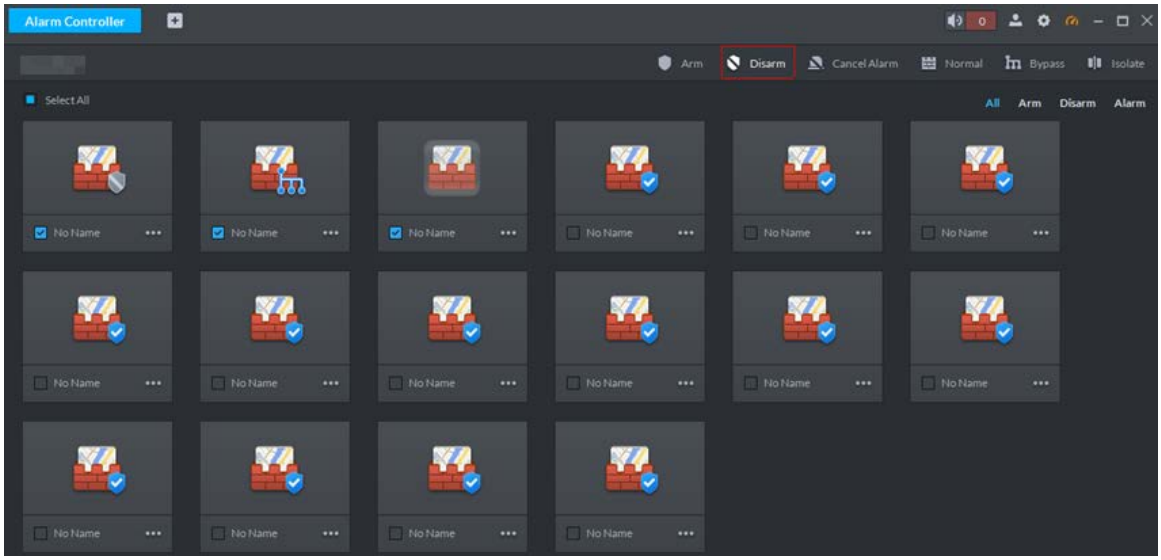


Figure 4-398 Disarm subsystem



- Select the zone or subsystem you want to disarm (multiple choice supported), click **Disarm** on top of the interface, and see Figure 4-399.

Figure 4-399 Disarm



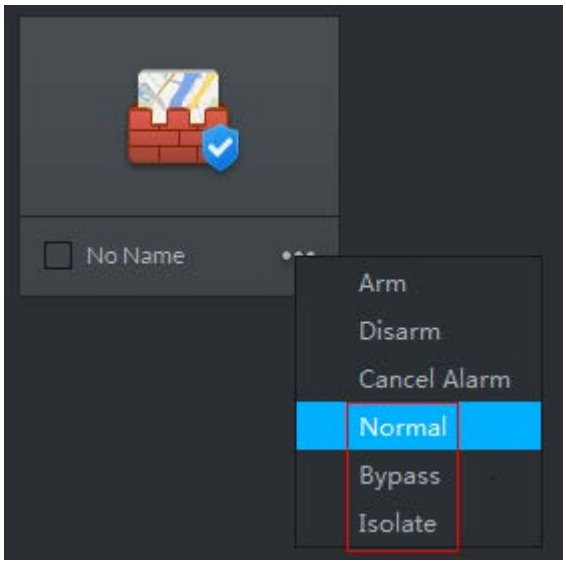
4.15.4.2 Bypass/Isolate/Normal

- Bypass zone, the alarm controller still monitors external detector and make records, but not forward to users. If you want to arm the bypassed zone, please disarm the zone into non-bypass and arm again.
- Isolate zone, the alarm controller still monitors external detector and make records, but not forward to users. When the zone is disabled or you want to disarm and arm again, the isolated zone is still disabled.
- Normal zone, the zone can trigger alarm normally when it is armed.

Two ways to operate over the zone.

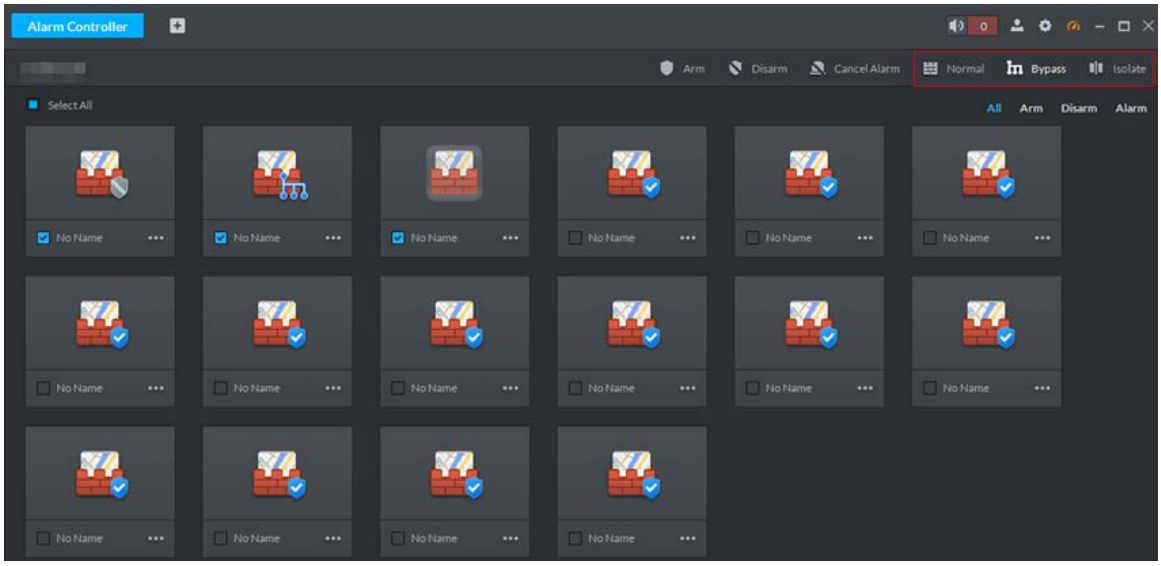
- Click ••• of the zone that needs to be bypassed, isolated or recovered to normal, select operation and see Figure 4-400.

Figure 4-400 Bypass/isolate zone (1)



- Select the zone that needs to be bypassed, isolated or recovered normal (multiple choice supported), click the operation buttons on top of the interface. See Figure 4-401.

Figure 4-401 Bypass/isolate zone (2)

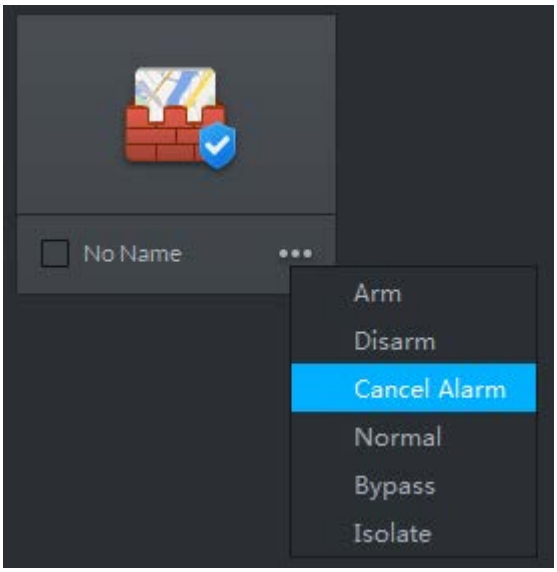


4.15.4.3 Cancel Alarm

You remove alarm by **Cancel Alarm** when alarm is triggered.

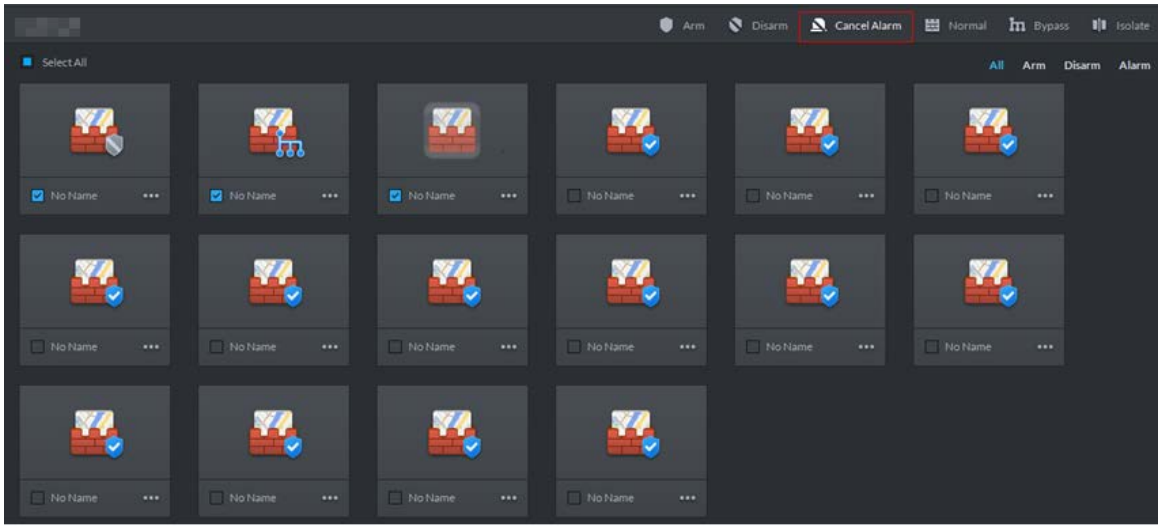
- Click the zone you want to cancel alarm, select **Cancel Alarm** and see Figure 4-402.

Figure 4-402 Cancel alarm



- Select the zone you want to cancel alarm (multiple choices supported), click **Cancel Alarm** on top of the interface and see Figure 4-403.

Figure 4-403 Cancel alarm (2)



5 Maintenance Guide

The chapter introduces daily maintenance, and make sure the platform runs safely and normally.

5.1 Backup and Restore

5.1.1 Backup

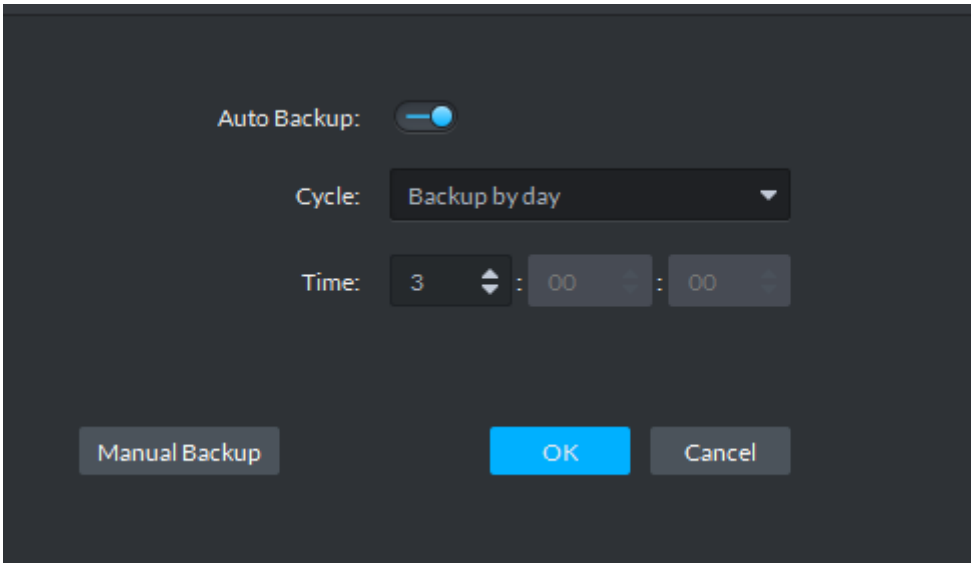
To guarantee data security, the platform provides data backup function; backup mode includes auto backup and manual backup. You are recommended to enable auto backup for regular data backup.

5.1.1.1 Auto Backup

Step 1 On client homepage, click **Config**.
The **Config** interface is displayed.

Step 2 Click **Backup**.
The **Backup** interface is displayed. See Figure 5-1.

Figure 5-1 Backup



Step 3 Click  next to Auto Backup.

The icon becomes  , and auto back is enabled.

Step 4 Set **Cycle** and **Time**, click **OK**.
The system pops out the interface of **Set Backup File Password**.

You can select any whole hour between 3:00 and 23:00 to implement backup.

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

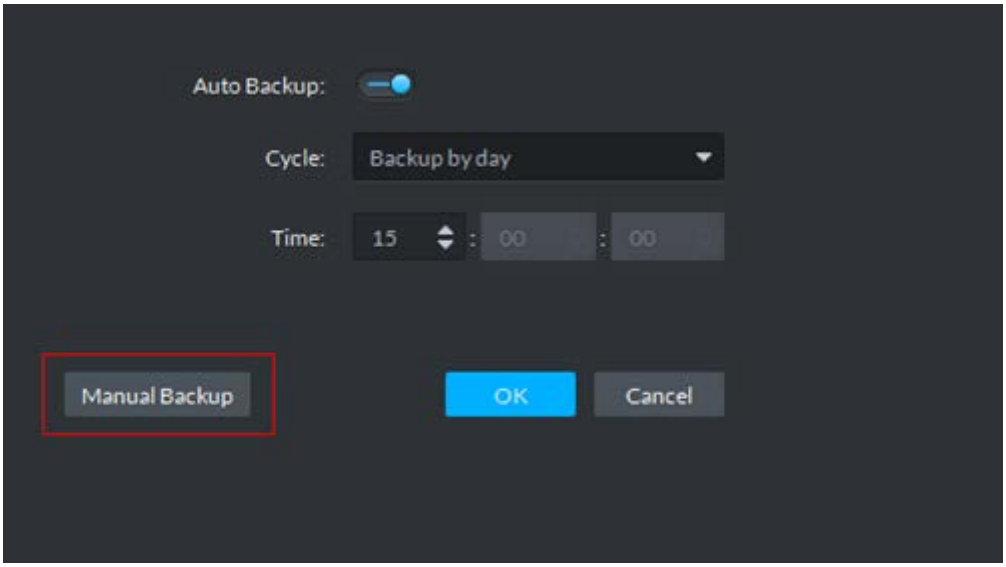
- File password, used to guarantee backup data file security, you need to enter password for verification if you want to open or restore backup file.
- Backup file is stored under server installation path, which is "..\Server\WEBCLIENT\webclient\apache-tomcat\tmp\systemBackup".

5.1.1.2 Manual Backup

Step 1 On client homepage, click **Config**.
The **Config** interface is displayed.

Step 2 Click **Backup**.
The **Backup** interface is displayed. See Figure 5-2.

Figure 5-2 Backup



Step 3 Click Manual Backup.
The system pops up the interface of **Set Backup File Password**

Step 4 Enter file password, click **OK**.

- File password, used to guarantee backup data file security, you need to enter password for verification if you want to open or restore backup file.
- Backup file is stored under server installation path, which is "..\Server\WEBCLIENT\webclient\apache-tomcat\tmp\systemBackup".

5.1.2 Restore

You can restore the system and data back to the latest backup time during database exception. The system can be quickly recovered and lower user loss.

⚠

Other users cannot operate the system when restoring the database. The data information will change after being restored, please operate with care.

5.1.2.1 Restoring Local File

Local file restoration is to restore manually backup file to server.

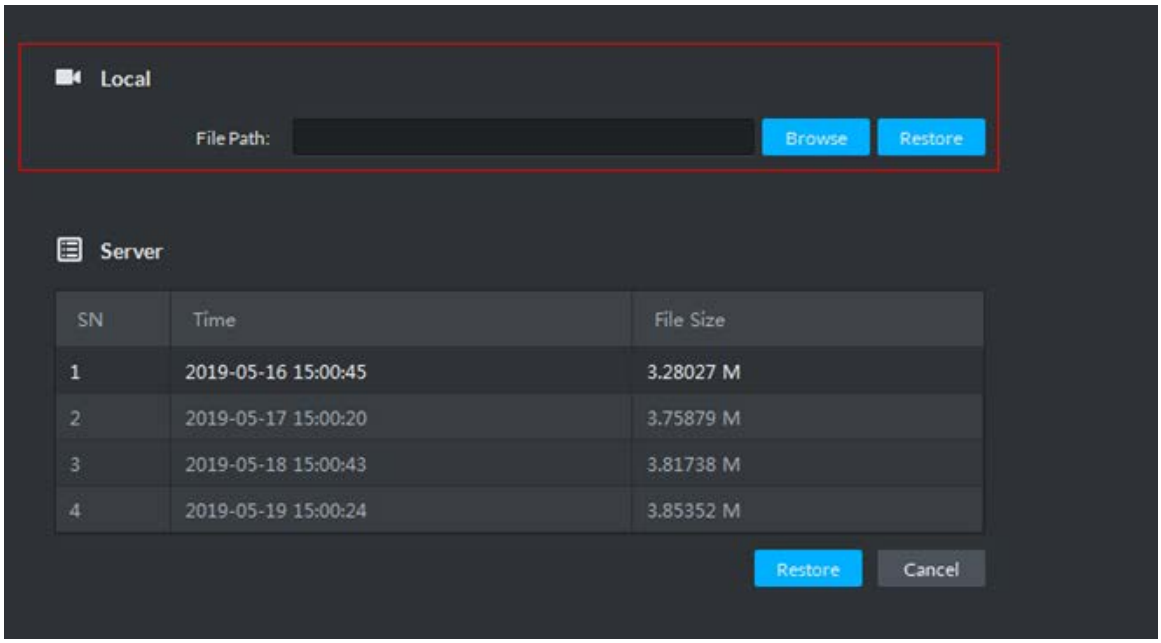
Step 1 On client homepage, click **Config**.

The **Config** interface is displayed.

Step 2 Click **Restore**.

The **Restore** interface is displayed. See Figure 5-3.

Figure 5-3 Local



Step 3 Click **Browse** and select backup data file.

Step 4 Click Restore.

The system pops out **Restore** box.

Step 5 Enter administrator login password and file password, click **OK**.

The restoration progress is displayed, and the system will prompt restored successfully on the lower right corner.

5.1.2.2 Restoring Server File

Restore data from backup file of server, the backup file on server is automatically backed up from system.

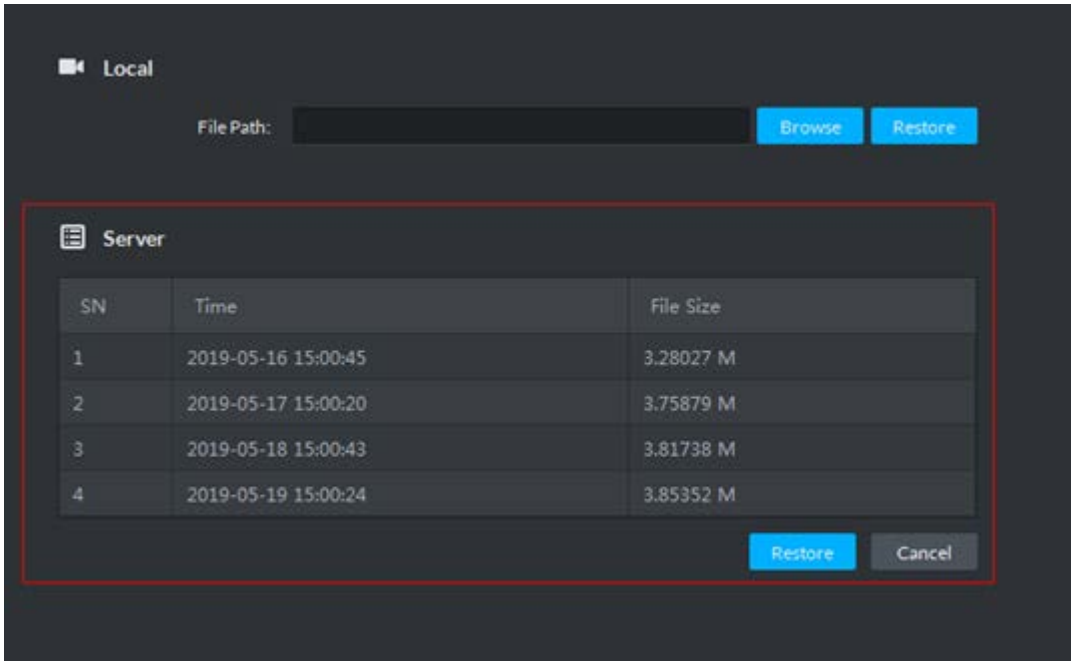
Step 1 On client homepage, click **Config**.

The **Config** interface is displayed.

Step 2 Click **Restore**.

The **Restore** interface is displayed. See Figure 5-4.

Figure 5-4 Restore server file



Step 3 Select backup file from server, click **Restor**e.

The system pops out prompt box.

Step 4 Enter administrator login password and file password, click **OK**.

The restoration progress is displayed; the system will prompt restored successfully on lower right corner.

5.2 Update

To ensure server safety and improve performance, the software is being upgraded constantly. You can upgrade your system when needed.

5.3 Log

In log module, you can view operator log and access control device log.

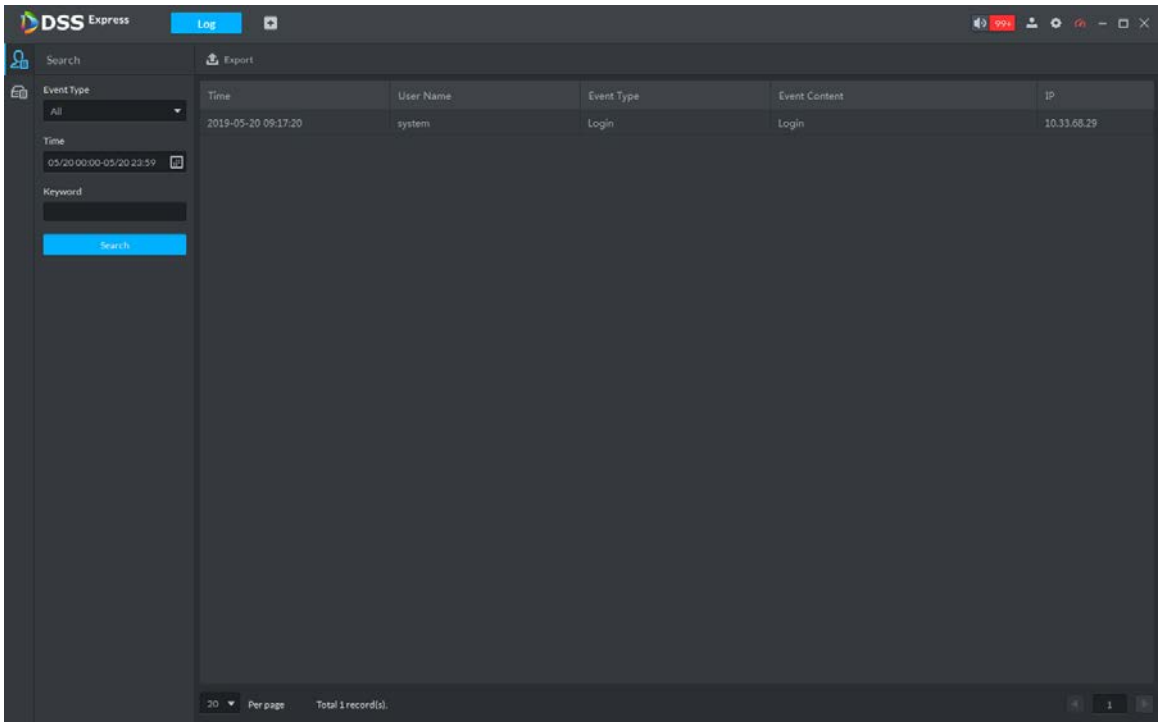
Step 1 On client homepage, click **Log**.

The **Log** interface is displayed.

Step 2 Click  .

The **Operator Log** interface is displayed. See Figure 5-5.

Figure 5-5 Operation log



Step 3 Select event typetime, enter keyword, and click **Search**.
The results are displayed.

5.4 Password Maintenance

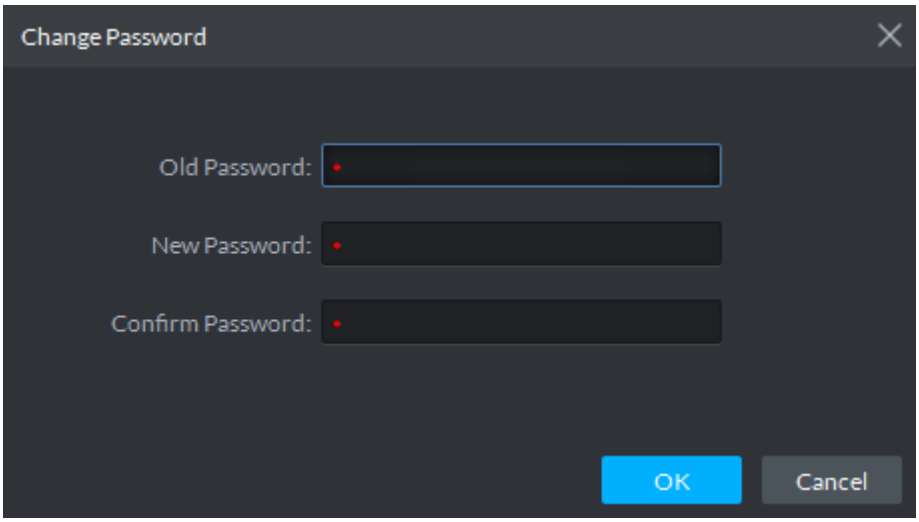
System supports modifying password and resetting password when you forget it. Non-system user cannot reset password.

5.4.1 Changing Password

To make sure the account is safe, you are recommended to change login password regularly.

Step 1 After logging in client, click  on top right corner of the interface, select **Change Password**.
The **Change Password** interface is displayed. See Figure 5-6.

Figure 5-6 Change password



Step 2 Enter Old Password, New Password and Confirm Password, click OK.

5.4.2 Resetting Password

When users forget password, you can reset a new password.

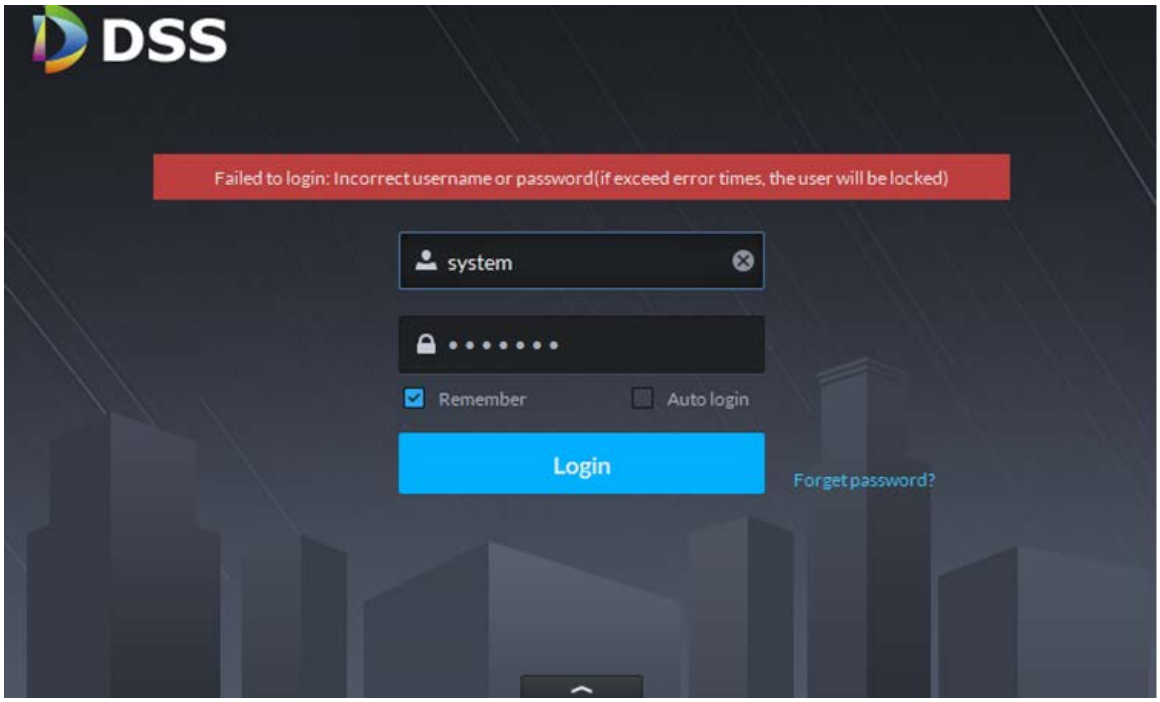
System User Password Reset

When system user forgets password, you can reset password by answering security question.

Step 1 Users forget password when logging in client, enter wrong password to log in client.

The login interface displays **Forget Password**. See Figure 5-7.

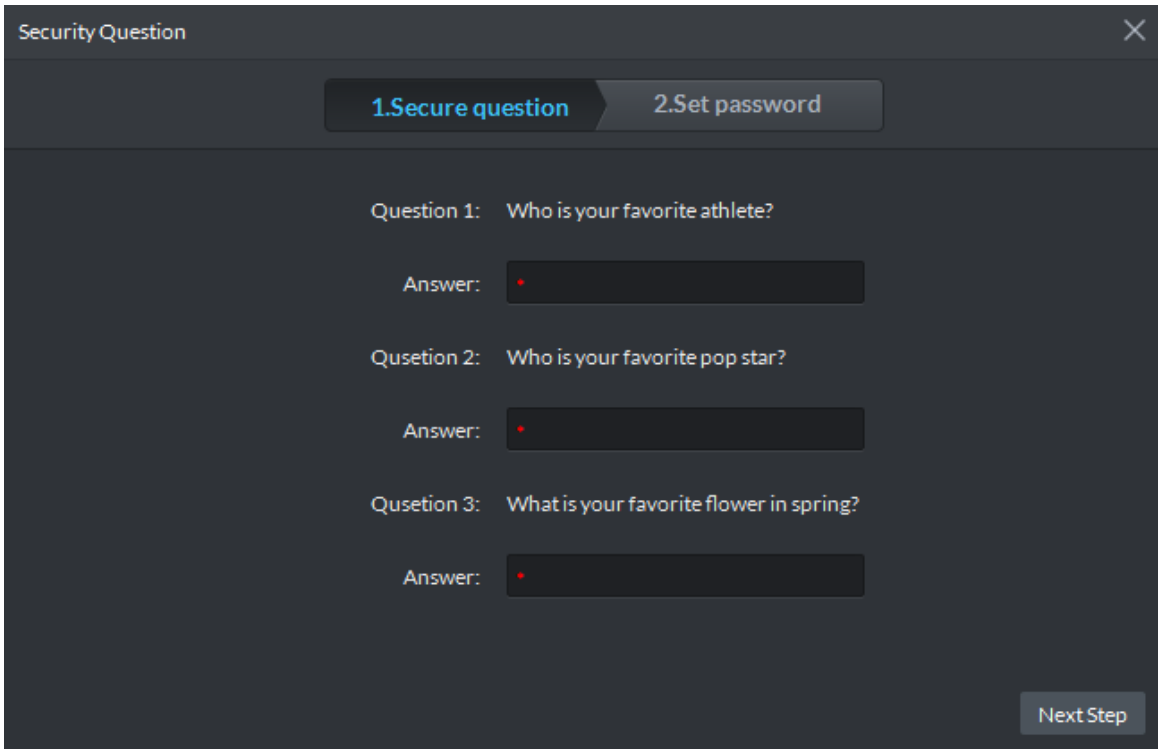
Figure 5-7 Forget password



Step 2 Click Forget Password.

The **Security Question** interface is displayed. See Figure 5-8.

Figure 5-8 Security question



Step 3 Enter answers to three questions, click **Next Step**.

The **Set Password** interface is displayed.

Step 4 Enter new password, click **OK** and password is reset.

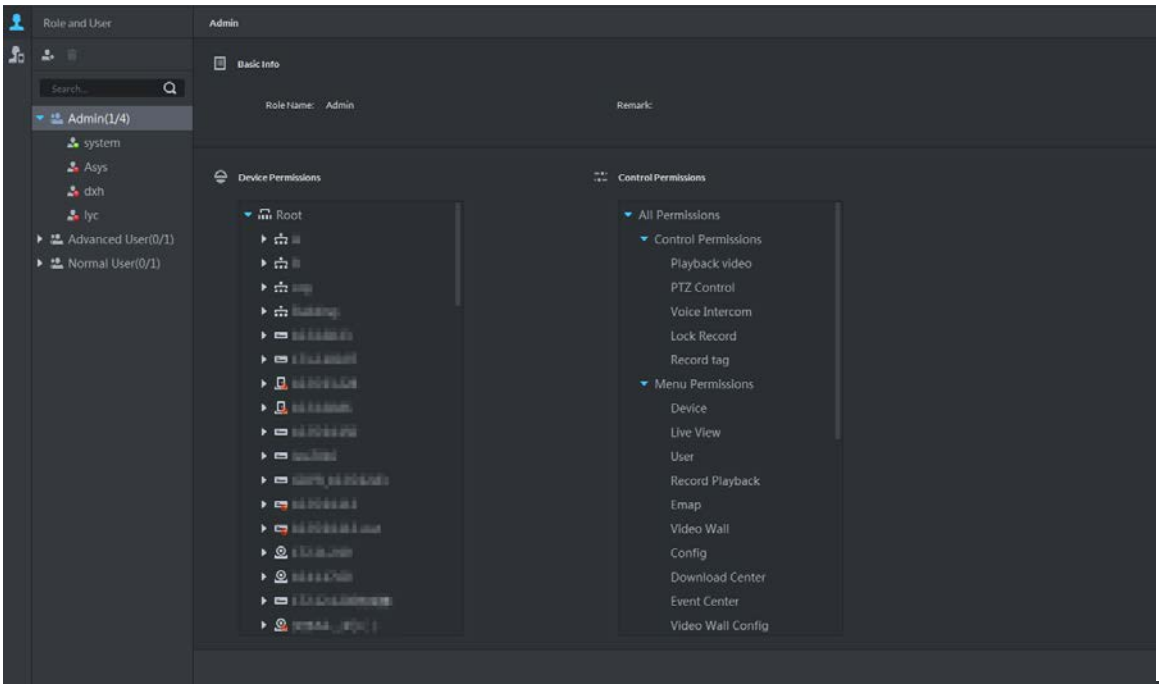
Non-system User Password Reset

When non-system user forgets password, you can only let system user set new password.

Step 1 On client homepage, click **User**.

The **User** interface is displayed. See Figure 5-9.

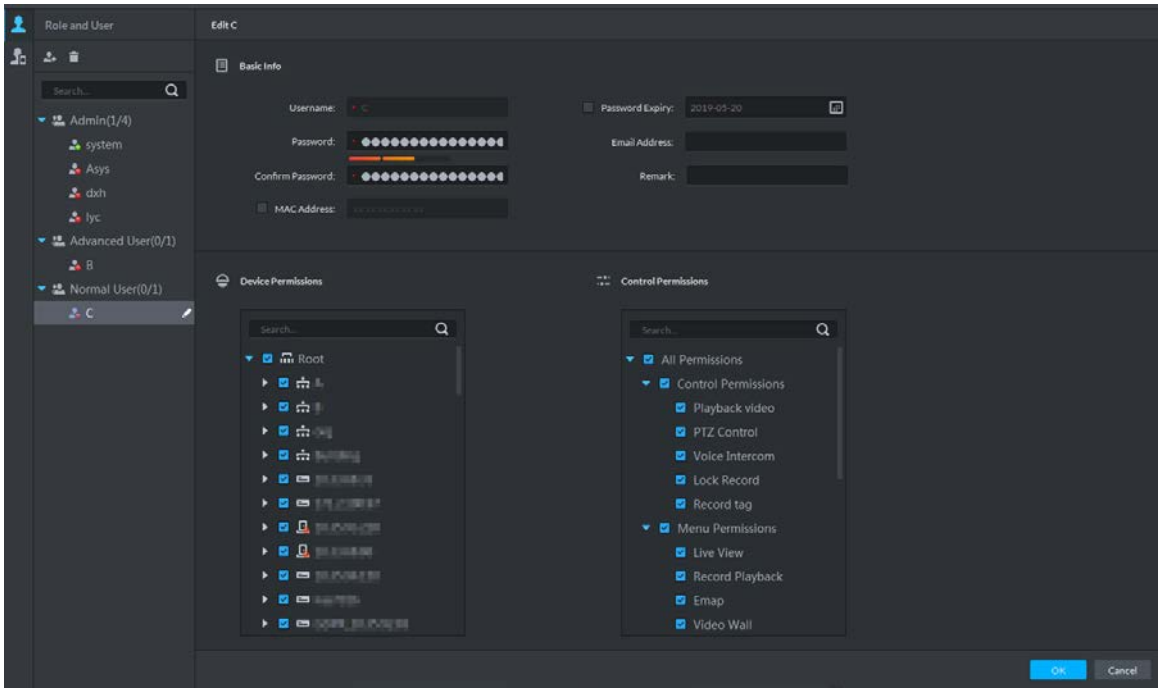
Figure 5-9 User



Step 2 Select the user you want to reset password, click  .

The interface of modifying user info is displayed. See Figure 5-10.

Figure 5-10 Modify user info



Step 3 Enter password and confirm password, click **OK** and password is changed.

Appendix 1 Service Module Introduction

Service Name	Function Description	Port	Protocol Type
DSS_WEB (Center Management Service)	Center management service is to manage each service and provide accessing port.	H HTTP: 80 HTTPS: 443 CMS: 9000	TCP
DSS_MQ (Message Queue Service)	Message queue service is to transfer messages between the platforms.	61616	TCP
DSS_DMS (Device Management Service)	Device management service is to register front-end encoder, receive alarm, transfer alarm and send out sync time command.	9200	TCP
DSS_MTS (Media Transmission Service)	Media transmission service is to get the audio/video bit stream from the front-end device and then transfer these data to the SS, client and decoder.	9100	TCP
DSS_SS (Storage Service)	Storage service is to storage/search/playback record.	9320	TCP
DSS_VMS (Video Matrix Service)	Video matrix service is to login the the decoder and send out task to the decoder to output to the TV wall.	Not fixed, do not need to be mapped to the outside.	TCP
DSS_MGW (Media Gateway Service)	Media gateway service is to send out MTS service to the decoder.	9090	TCP
DSS_PCPS (ProxyList control Proxy Service)	Login Onvif device and then get the stream and transfer the data to MTS.	SIP: 5060 REGISTER: 9550	UDP TCP
DSS_ADS (Alarm Dispatch Service)	Alarm dispatch service is to send out alarm information to different objects according to the plans.	9600	TCP
DSS_SOSO (Device Search Service)	Search devices by adding IP address	12366	TCP
DSS_SC (Video Intercom Service)	Video intercom SIP service	SIP：5080 RTP：554	TCP
DSS_MCDDOOR (Access Control Service)	Access control device accessed to service, interacted with access control device.	Not fixed, do not need to be mapped to the outside.	TCP

Appendix 2 Shortcut Key List

Function	Shortcut Key	Function	Shortcut Key
Wnd Move up	Up	Snap Single Wnd	P
Wnd Move down	Down	Snap pic	Ctrl+P
Wnd Move Left	Left	Local Record	Ctrl+R
Wnd Move Right	Right	Lock	Ctrl+L
Aperture-	Insert	PreSet1	1
Aperture+	Delete	PreSet2	2
Focus-	Home	PreSet3	3
Focus+	End	PreSet4	4
Wiper	PgUp	PreSet5	5
Light	PgDn	PreSet6	6
Open Single Wnd	L	PreSet7	7
Close Single Wnd	L	PreSet8	8
Open Full Screen	Ctrl+F	PreSet9	9
Close Full Screen	ESC	PreSet10	10

Appendix 3 Deleting Videos on Central Server

If you want to delete 1000001$0 record period [2018-07-08 10:00:00 2018-07-08 10:30:00], do the following steps.

Step 1 Log in central server.

Step 2 Enter...\DSS\Server\SS directory, drag **./CQFSTools.exe list** file to cmd input window, find disk uuid.

The disk info is displayed as follows:

[[Disk List]]
[Disk Path] [Target (Size) (Portal) (slot)]
D:\730c4deedd9f4f7786d49ab9e7802a7a.cqd D:\730c4deedd9f4f7786d49ab9e7802a7a.cqd (10.00GB) () (-1)
11:32:57.355 TID 584188 [INFO] cmd[cmd.exe /c "getmac /FO list >cqfs_tmp_584188.txt.tmp & type cqfs_tmp_584188.txt.tmp >cqf
[[CQFS List]]
[Disk Path] [CQFS UUID (Service Type) (Allocation Type)]
D:\730c4deedd9f4f7786d49ab9e7802a7a.cqd {1bdb9a6e-41a6-4058-87ef-d944f630edf1} (1) (0)

Step 3 Search streamed.

Use tool to connect to platform database, and implement the following SQL, the searched ID field is streamed.

SELECT ID FROM adm_record_stream where DEVICE_CODE= device No. and CHANNEL_SEQ = channel No.

Step 4 Implement the command of deleClip.

./CQFSTools.exe deleteClip <streamID> <beginTS> <endTS> <diskUUID>

Appendix 4 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device 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 device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device 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 device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device 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. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **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.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, 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.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device 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.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.