DSS Express

User's Manual

V8.0.4

Foreword

General

This user's manual introduces the functions and operations of the DSS platform (hereinafter referred to as "the system" or "the platform").

Safety Instructions

The following signal words 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, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

1 Overview

1.1 Introduction

DSS Express can be used with a certain number of cameras for free. In addition, it is easy to be integrated with access control, video intercoms and AI features such as facial recognition, ANPR, and video metadata.
It is suitable for retail stores, vehicle entrance management, and office buildings.

1.2 Highlights

- Lower investment
  - Free for a certain number of cameras.
  - Purchase other licenses on demand.
  - Low hardware performance requirements.
- Pay-as-you-go
  With license, it is an easily scalable product with up to 256 cameras, 64 doors, and 256 video intercoms.
- Easy upgrade
  For more features and capacity, simply upgrade your license to DSS Pro.
- Unified platform
  Integrates applications, such as video monitoring, access control, video intercoms, face recognition, and ANPR, to achieve a unified and easy-to-use solution.

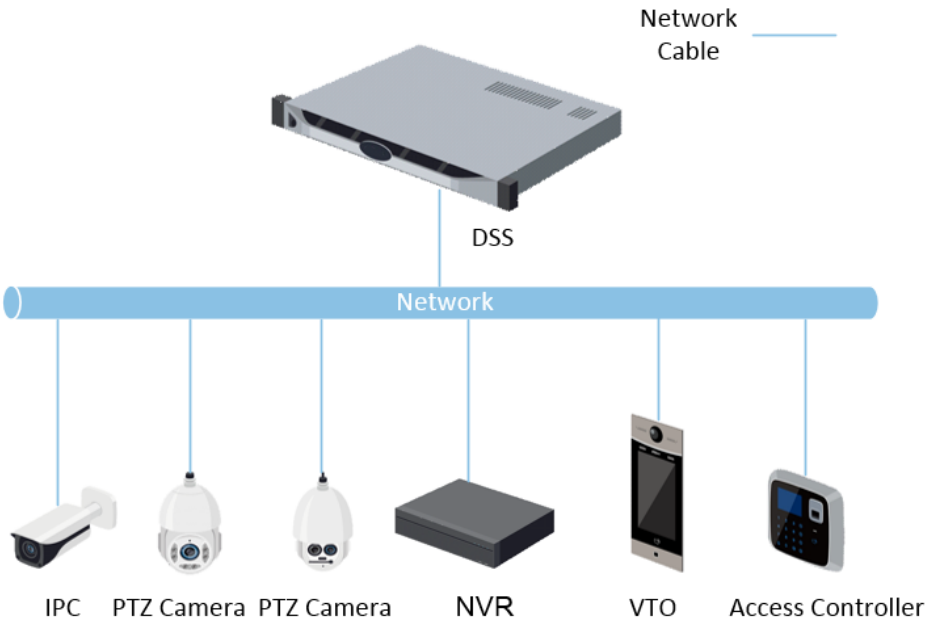
2 Installation and Deployment

DSS platform supports standalone deployment, and LAN to WAN mapping.

Standalone Deployment

For projects with a small number of devices, only one DSS server is required.

Figure 2-1 Standalone deployment



2.1 Standalone Deployment

2.1.1 Server Requirements

Table 2-1 DSS Express hardware requirement

Parameter	Hardware Requirement	Operating System
Recommended configuration	• CPU: Intel® Core(TM) I7-9700K CPU@3.60GHZ • RAM: 8 GB • Network card: 1 × Ethernet port @ 1000 Mbps • Hard drive type: 7200 RPM Enterprise Class HDD 1 TB • DSS installation directory space: 500 GB	Windows 7 and above

Parameter	Hardware Requirement	Operating System
Minimum configuration	• CPU: Intel® Core(TM) I5-9400 CPU@2.90GHZ • RAM: 8 GB • Network card: 1 × Ethernet port @ 1000 Mbps • Hard drive type: 7200 RPM Enterprise Class HDD 1 TB • DSS installation directory space: 200 GB	Windows 7 and above

- Face recognition images cannot be stored on the system disk and DSS installation disk. Make sure that your server has at least 3 HDD partitions to ensure that the face images have a storage location.
- For best performance, we recommend adding additional hard drives to store pictures.

2.1.2 Installing DSS

Prerequisites

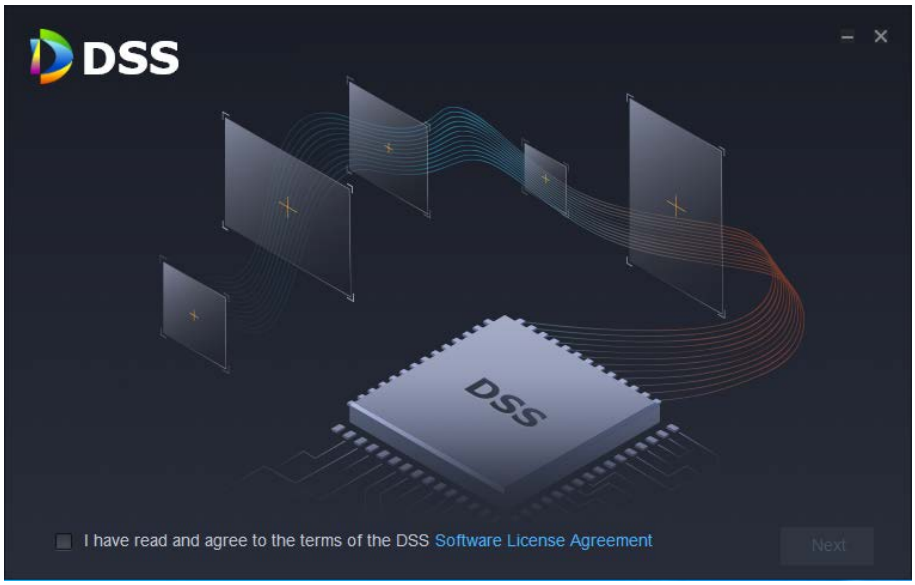
- You have downloaded the DSS installer from the official website or received it from our sales or technical support.
- You have prepared a server that meets the hardware requirements mentioned in "2.1.1 Server Requirements", and the server IP address is configured.

Procedure

Step 1 Double-click the DSS installer .

The name of the installer includes version number and date, confirm before installation.

Figure 2-2 Install DSS server



Step 2 Click **Software License Agreement**, and then read the agreement,

Step 3 Select the checkbox to accept the agreement, and then click **Next**.

Figure 2-3 Select the installation path

Step 4 Click **Browse**, and then select the installation path.

If the **Install** button is gray, check whether your installation path and space required meet the requirements. The total space required is displayed on the interface.

We do not recommend you install the DSS server on Disk C, because features such as face recognition require higher disk performance.

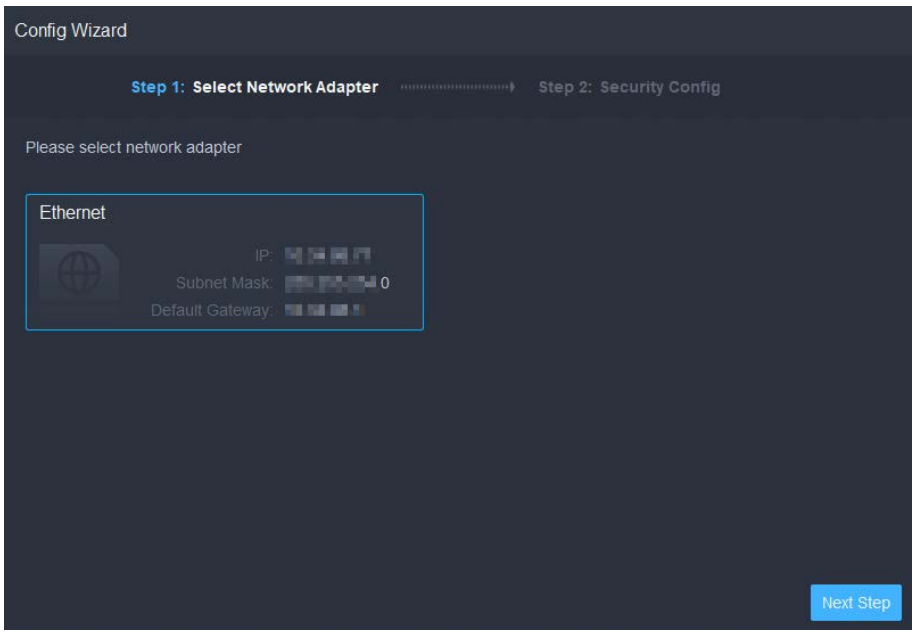
Step 5 Click **Install**.

The installation process takes about 4 to 8 minutes.

Figure 2-4 Run the DSS server

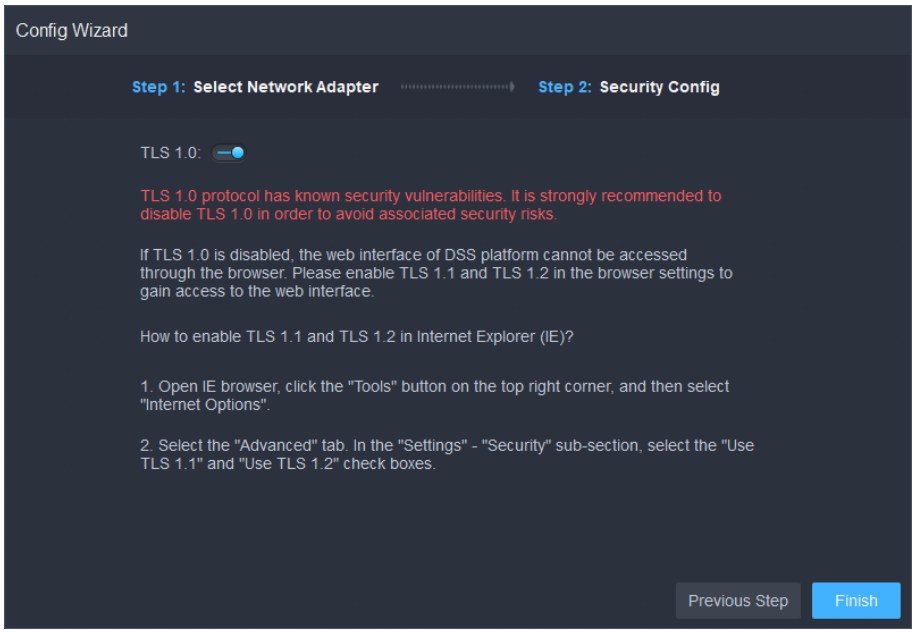
Step 6 Click **Run** when the installation finishes.

Figure 2-5 Select a network card



Step 7 Select the network card you need and click **OK**.

Figure 2-6 Enable or disable TLS1.0



Step 8 Enable or disable TLS1.0 as needed.

TLS 1.0 has known security vulnerabilities. We strongly recommend you disable it to avoid security risks. If it is disabled, the web interface of DSS platform cannot be accessed through the browser. You need to enable TLS 1.1 and TLS 1.2 in the browser settings to gain access to the web interface.

Step 9 Click **Finish**.

If the available RAM of the server is less than 2 GB, you can only use basic functions related to video. If it is less than 1.5 GB, you cannot use any function.

Related Operations

- To uninstall the platform, log in to the server, go to "..\DSS\DSS Server\Uninstall", double-click uninst.exe, and then follow the on-screen instructions to uninstall the program.
- To update the system, directly install the new program. The system supports in-place update. Follow the steps above to install the program.

2.1.3 Configuring Server IP Address

Change the server IP address as you planned. Make sure that the server IP can access the devices in your system. For details, see the manual of the server.

After changing the IP address of the server, you need to update it in the system services. See the following section.

2.1.4 Managing System Services

View service status, start or stop services, and change service ports.

On the server, double-click .

Figure 2-7 Service management interface

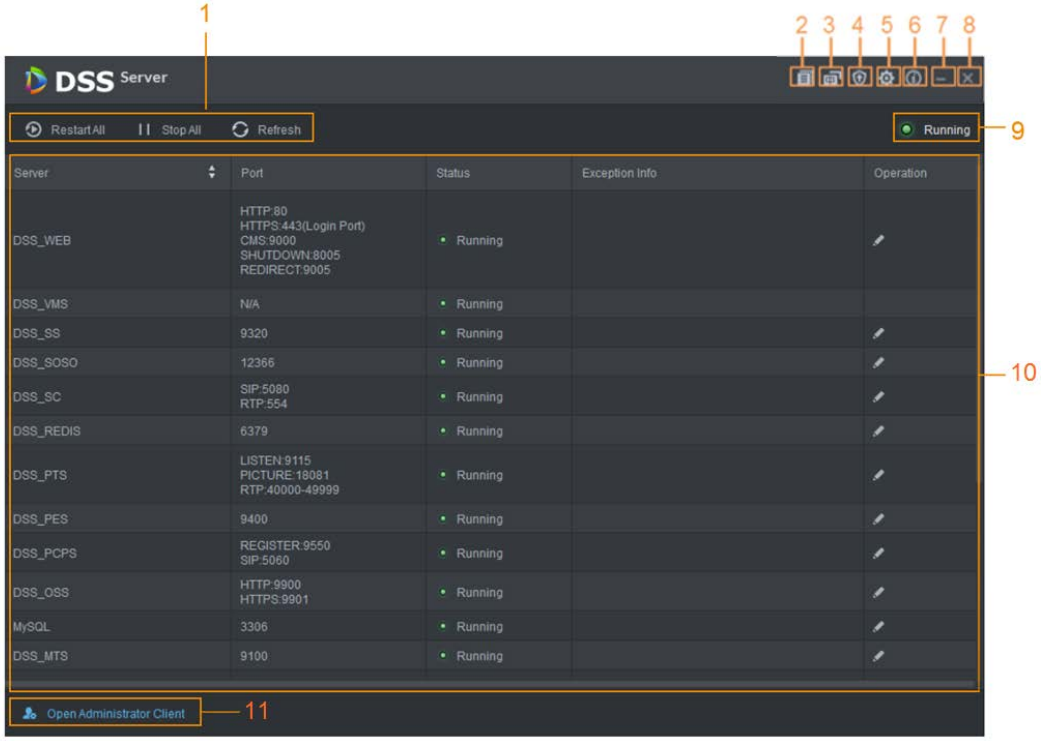


Table 2-2 Interface description

No.	Function	Description
1	Service Management	Supports 3 types of operations: ● Click Restart All to restart all services. When starting the platform, if the available memory of the server does not reach 2 GB, only the basic video services can be enabled. If the server has less than 1.5 GB of available memory, no services are available. ● Click Stop All to stop all services. ● Click Refresh to refresh services.
2	User's manual	User manual.
3	Language	Switch language.

No.	Function	Description
4	Security Setting	TLS 1.0 has known security vulnerabilities. We strongly recommend you disable it to avoid security risks. If it is disabled, the web interface of DSS platform cannot be accessed through the browser. You need to enable TLS 1.1 and TLS 1.2 in the browser settings to gain access to the web interface. 1. Open Internet Explorer. 2. Click the Tools button at the upper-right corner, and then select Internet Options. 3. Select the Advanced tab. 4. Go to the Settings > Security section, and then select Use TLS 1.1 and Use TLS 1.2. 5. Click OK.
5	Setting	Set the server IP as the platform CMS IP. If the network has to go across LAN and WAN, you need to enter WAN IP in the **Mapping IP** box.
6	About	Software version information.
7	Minimize	Minimize the interface.
8	Close	—
9	Service Status	• Starting • Unavailable: Service is running abnormally • Stopping • Running: Service is running normally • Stopped
10	Services	Display each service and service status. Click to modify service port number, and then the services will restart automatically after modification.
11	Download Client	Go to client download interface.

2.1.5 Installing and Logging into DSS Client

Install the DSS client before licensing it.

2.1.5.1 Installing DSS Client

You can visit the system through the DSS Client for remote monitoring.

2.1.5.1.1 DSS Client Installation Requirements

To install DSS Client, prepare a computer in accordance with the following requirements.

Table 2-3 Hardware requirements

Parameters	Description
Recommended system requirements	• CPU: I5-6500@3.20GHz • Memory: 8 GB and above • Graphics: NVIDIA® GeForce®GT 530 • Network Card: 1000 Mbps • HDD: Make sure that at least 100GB is reserved for DSS client.
Minimum system requirements	• CPU: I3-2120@3.20GHz • Memory: 4 GB • Graphics: Intel® HD Sandbridge Desktop Graphcs • Network Card: 1000 Mbps • DSS client installation space: Make sure that at least 50 GB is reserved for DSS client.

2.1.5.1.2 Downloading and Installing DSS Client

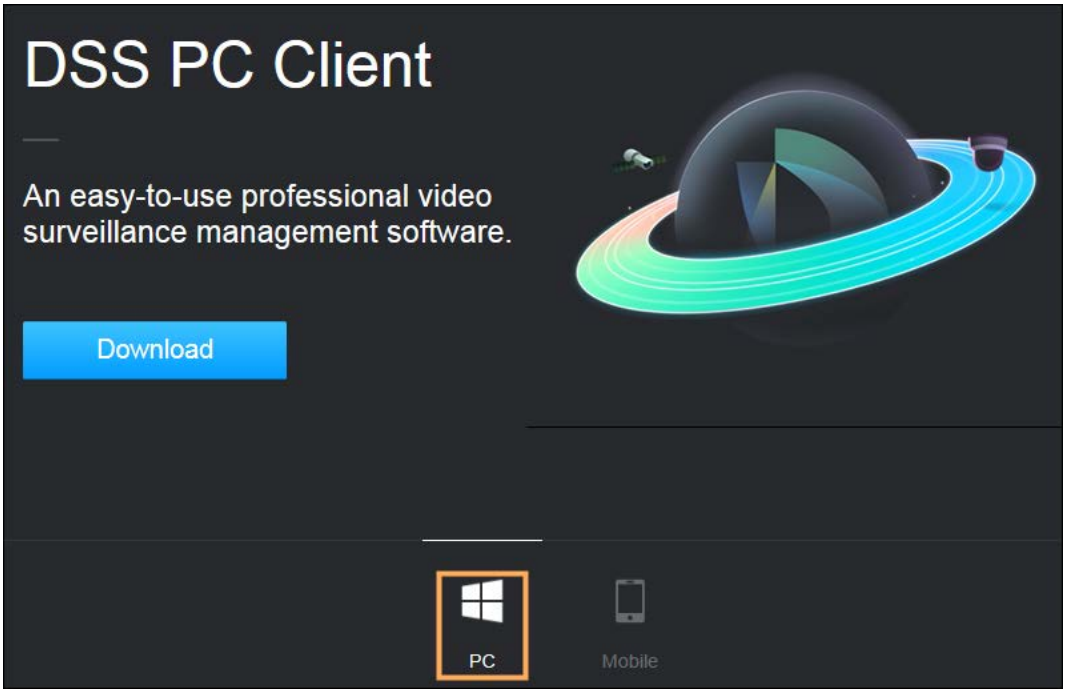
Step 1 Enter the IP address of DSS into the browser and then press Enter.

Step 2 Click **PC**, and then **Download**.

If you save the program, go to Step3.

If you run the program, go to Step4.

Figure 2-8 Download DSS Client



Step 3 Double-click the DSS Client program.

Step 4 Select the check box of **I have read and agree to the DSS agreement** and then click **Next**.

Step 5 Select installation path.

Step 6 Click **Install**.

System displays the installation progress. It takes about 5 minutes to complete.

2.1.5.2 Logging in to DSS Client

Step 1 Double-click on the desktop.

- The first time you log in to the platform, go to Step2.
- If this is not your first time logging in to the platform, go to Step3.

Step 2 Initialize the platform.

The first time you log in, you have to initialize the platform. Set the system username and password, and password protection questions. The questions are used when you need to change your password in the future.

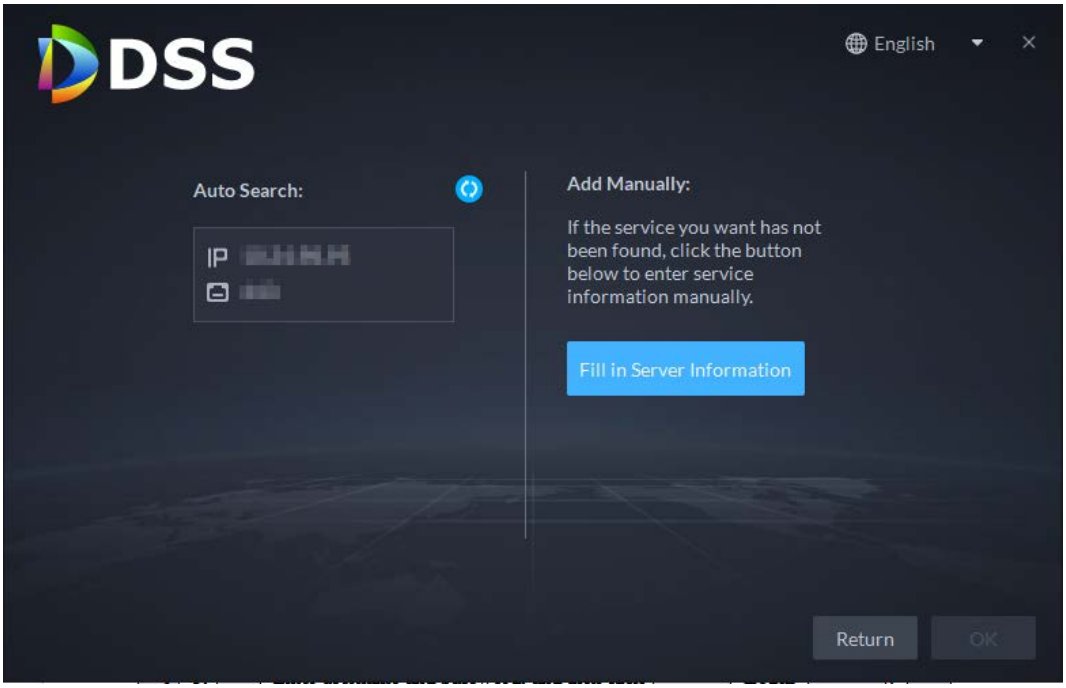
1) Configure system username and password, and then click **Next**.
   The password must consist of 8 to 32 non-blank characters and contain at least two types of characters: Uppercase, lowercase, number, and special character (excluding ' " ; : &).
2) Select your questions and their answers, and then click **OK**.

Step 3 Select the detected server on the left of the interface, or click **Fill in site information**, and then enter the IP address or domain name, and the port number.

Server IP is the IP address of DSS server or PC. The port is 443 by default.

If you want to log in to the platform using domain name, you must bind the IP address of the platform to a domain name first. See "2.3 Mapping Domain".

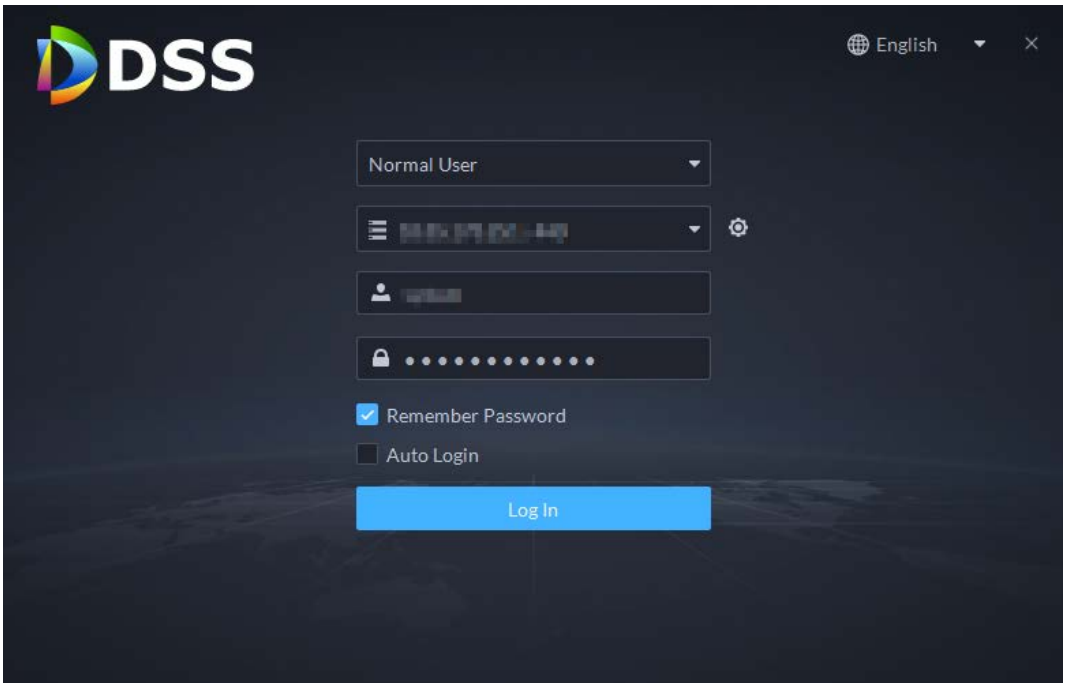
Figure 2-9 Select a site



Step 4 Select a user type, language and platform.

Step 5 Enter username and password, and then click **Login**.

Figure 2-10 Login interface (not first-time login)



2.1.5.3 Homepage of DSS Client

Figure 2-11 Homepage

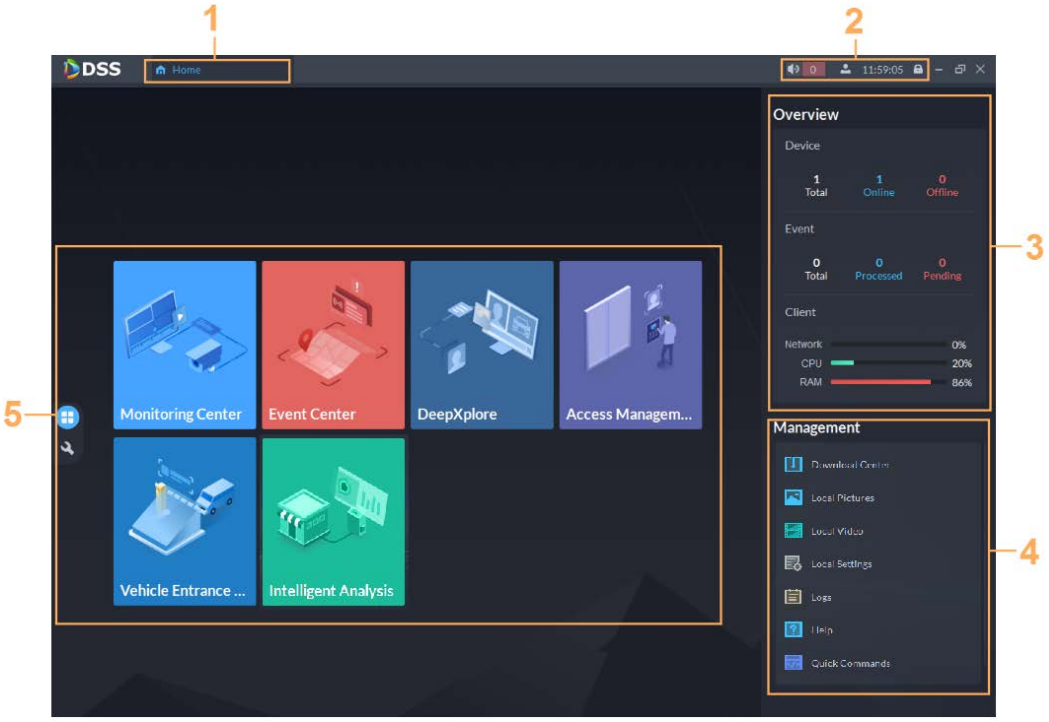


Table 2-4 Description

No.	Name	Function
1	Tab	Tabs.

No.	Name	Function
2	System settings	● : Enable or disable alarm audio. ● 0 : Displays number of alarms. Click the icon to go to **Event Center**. ● : User information: Click the icon, and then you can log in to the web interface by clicking system IP address, change password, lock client and log out. ◇ Click platform IP address to go to the Web interface. ◇ Click **Change Password** to modify user password. ◇ Click **About** to view version information. ◇ Click **Sign Out** to exit client. ● Click to lock client.
3	Overview	● The number of devices in total, offline and online. ● The number of total, processed and pending events. ● The client network, CPU and RAM usage.
4	Management	● Download videos. ● Check local pictures and videos. ● Settings for video, snapshot, alarm, security and shortcut keys. ● View and manage logs. ● View user manual.
5	Applications	● : Application options including monitoring center, access management, intelligent analysis and vehicle entrance control. ● : Configuration options.

2.1.6 Licensing

You can upgrade your license for more features and increased capacity.
This section introduces license capacity, how to apply for a license, how to use the license to activate the platform, and how to renew your license.

2.1.6.1 Applying for a License

A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS

Express, scroll to the bottom, click **Apply**, and then follow the instructions.

2.1.6.2 Activating License

The following images of the interface might slightly differ from the actual interfaces.

2.1.6.2.1 Online Activation

Prerequisites

- You have received your license. If not, see "2.1.6.1 Applying for a License".
  A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS Express, and then follow the application instructions.
- The platform server can access the Internet.

Procedure

Step 1 On the **Home** interface, click , and then in **System Configuration**, select **License**.

Step 2 Click **Online Activate License**.

Step 3 Enter your new **Activation Code**.

Step 4 Click **Activate Now**.

Step 5 On the **License** interface, view your license details.

2.1.6.2.2 Offline Activation

Prerequisites

You have received your license. If not, see "2.1.6.1 Applying for a License".
A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS Express, and then follow the application instructions.

Procedure

Step 1 On the **Home** interface, click , and then in **System Configuration**, select **License**.

Step 2 Click **Offline Activate License**.

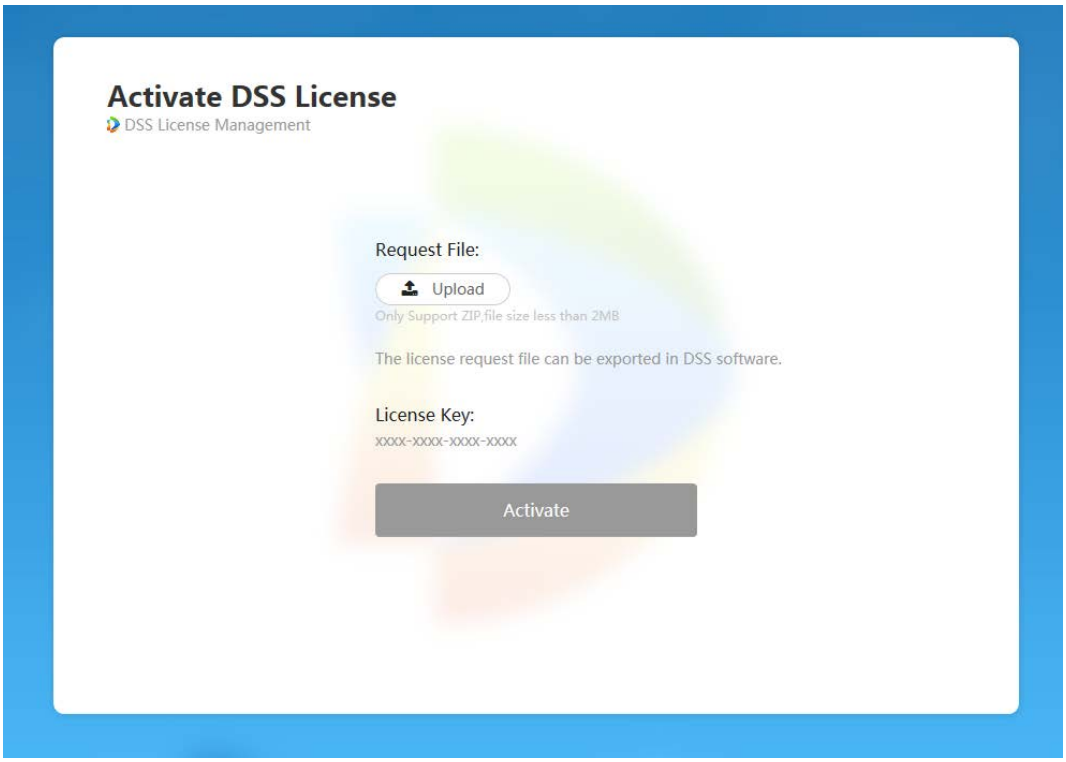
Step 3 Enter your new **Activation Code**.

Step 4 Click **Export** to export the license request file.

Step 5 Generate license file.

1) Move the request file to a computer with Internet access.
2) On that computer, open the system email that contains your license, and then click the attached web page address or **Click to go to DSS License Management** to go to the license management page.
3) Click **Activate License**.
4) Click **Upload**, select the license request file, and then when you are prompted **uploaded successfully**, click **Activate**.
   The success interface is displayed, where a download prompt is displayed asking you to save the license activation file.

Figure 2-12 Upload license request file



5) On the success interface, click **Save** to save the file, and then move the file back to the computer where you exported the license request file.
6) On the **Offline Activate License** interface, click **Import**, and then follow the on-screen instructions to import the license activation file.

Step 6 On the **License** interface, view your license details.

2.2 Configuring LAN or WAN

2.2.1 Configuring Router

If the platform is in a local network, you can visit it from the public network by performing DMZ mapping. For the list of the ports to be mapped, see the port matrix of the platform.

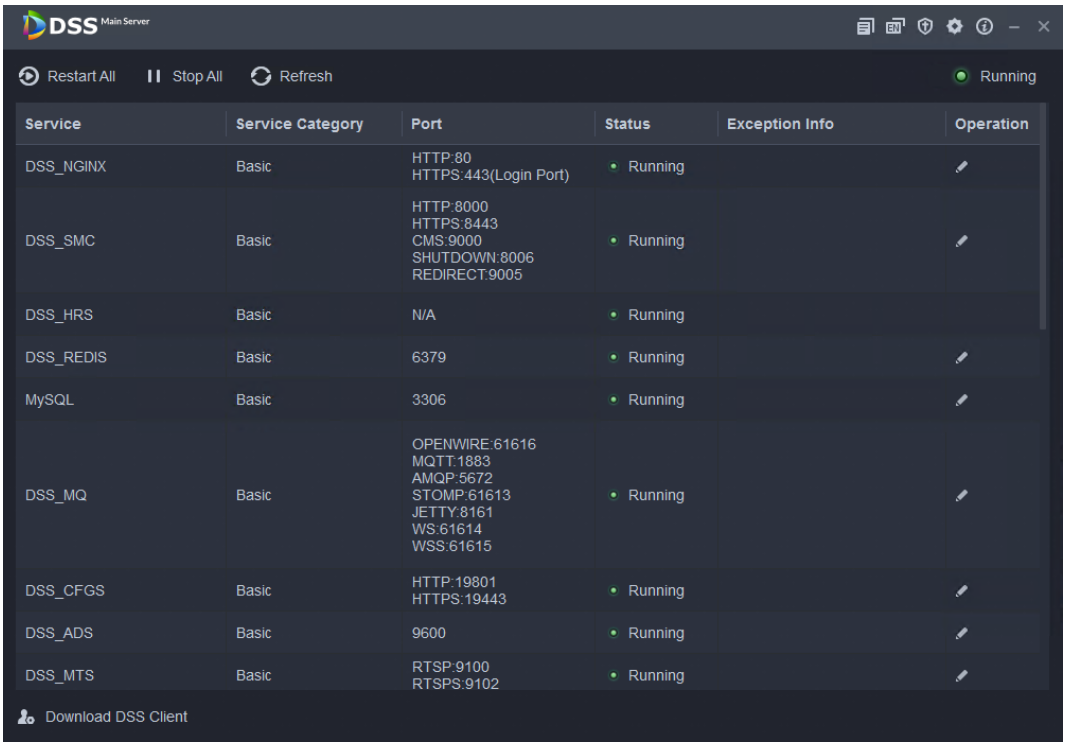
Make sure that the number of the WAN ports is consistent with that of the LAN ports.

2.2.2 Mapping IP

The interface might vary between the main server and the sub server. This section uses the main server interface as an example.

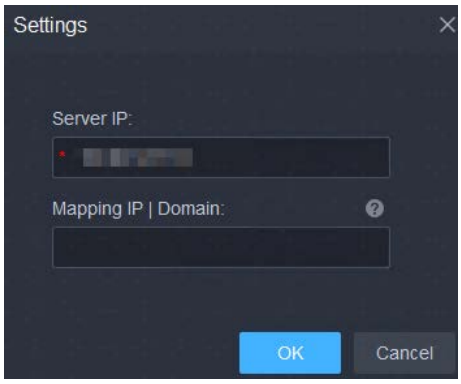
Step 1 Log in to DSS server, and then double-click .

Figure 2-13 Status of all services



Step 2 Click the ⚙ on the upper-right corner.

Figure 2-14 Setting



Step 3 Enter WAN address in the **Mapping IP** box, and then click **OK**.

Step 4 Click **OK**, and then the services will restart.

2.3 Mapping Domain

If the server is deployed in a local network, you can map the IP address of the server to a domain name, and then log in to the server using the domain name.

Prerequisite

Prepare a domain name.

Procedures

See "2.2.2 Mapping IP". In the **mapping IP | Domain** input box, enter the domain name that you prepared, and then click **OK**.

3 Basic Configurations

Configure basic settings of the system functions before using them, including system activation, organization and device management, user creation, storage and recording planning, and event rules configuration.

3.1 Preparations

3.1.1 Installing DSS Client

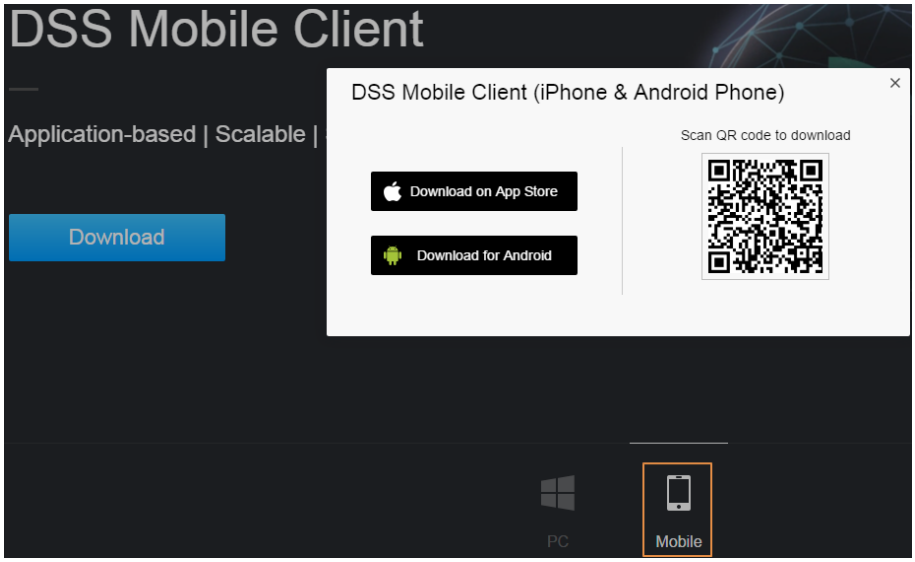
See "2.1.5 Installing and Logging into DSS Client".

3.1.2 Installing Mobile Client

Step 1 Enter IP address of the DSS in the browser and then press Enter.

Step 2 Click **Mobile** > **Download**, and then scan the QR code to download the App.

Figure 3-1 Download App by scanning QR code



3.2 Managing Resources

Manage system resources such as devices, users, and storage space. You can add organizations and devices, configure recording plans and backup plans, bind resources, and more.

3.2.1 Adding Organization

Classify devices by logical organization for the ease of management. The default organization is

Root. If the parent organization is not specified, newly added devices are attached to **Root**.

Procedure

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

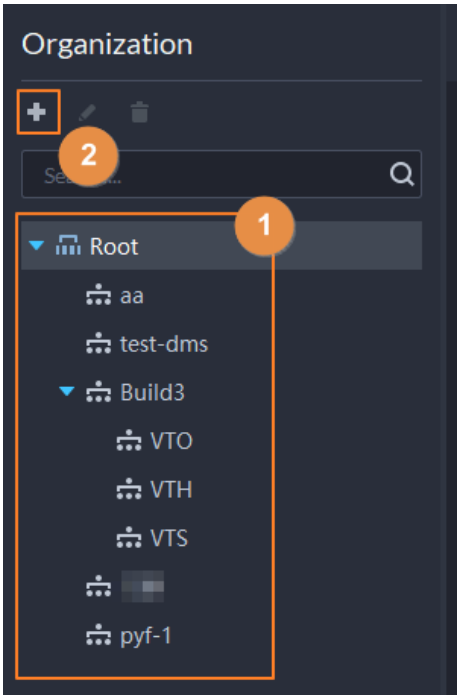
Step 2 Click

Step 3 Add an organization.

1) Select a parent organization.

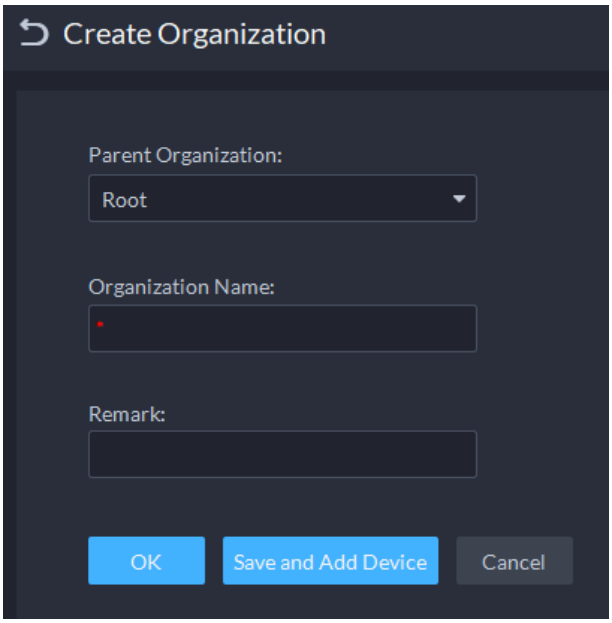
1) Click .

Figure 3-2 Add an organization



1) Enter the name of the organization, and then click **OK**.

Figure 3-3 Add an organization



You can also right-click the root, and then click **Create Organization** to add an organization.

Related Operations

- Changing organization name
  Right-click the organization, and then click **Rename**.
- Delete an organization
  Organization with devices cannot be deleted.
  Select the organization, click , or right-click an organization and select **Delete**.
- Adjust device organization
  Click the device, and then **Move To**, select the new organization, and then click **OK**.

3.2.2 Managing Device

Add devices before you can use them for video monitoring. This section introduces how to add, initialize, and edit devices and how to change device IP address.

3.2.2.1 Searching for Online Devices

Search for devices on the same network with the platform before you can add them to the platform.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

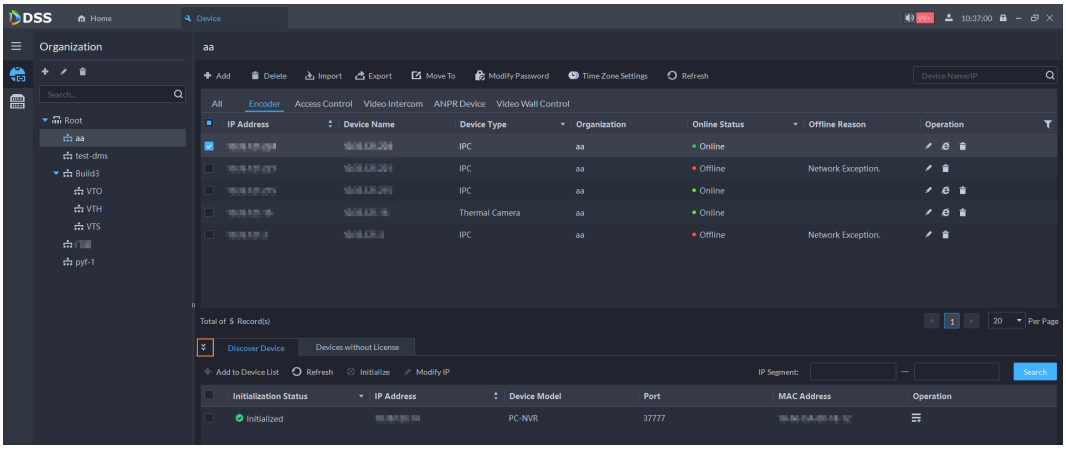
Step 2 Click .

Step 3 Click .

The icon changes to when devices are searched.

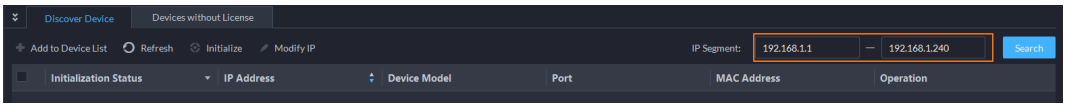
- When using the platform for the first time, the platform automatically searches for devices in the same network segment.
- If not the first time, the platform automatically searches for the devices in the network segment you configured last time.

Figure 3-4 Search for devices



Step 4 Specify **IP Segment**, and then click **Search**.

Figure 3-5 IP segment search



3.2.2.2 Initializing Devices

You need to initialize the uninitialized devices before you can add them to the platform.

Step 1 Search for devices. For details, see "3.2.2.1 Searching for Online Devices".

Step 2 Select an uninitialized device, and then click **Initialize**.

- You can select multiple devices to initialize them in batches. Make sure that the selected devices have the same username, password and email information.
- Click [redacted] next to **Initialization Status** to quickly sort out the status column, and then you can see all the uninitialized devices.

Step 3 Enter the password, and then click **Password Security**.

Step 4 Enter the email address, and then click **Change IP**.

The email is used to receive security code for resetting password.

Step 5 Enter the IP address, and then click **OK**.

When setting IP addresses in batches, the IP addresses increase in an ascending order.

3.2.2.3 Changing Device IP Address

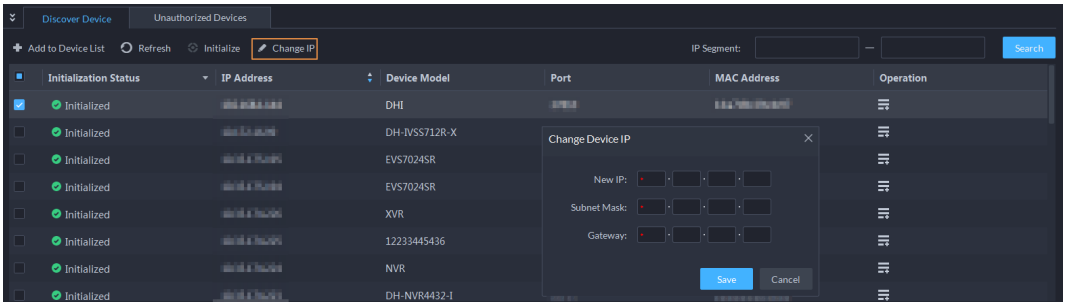
You can change IP addresses of the devices that have not been added to the platform.

Step 1 Search for devices. For details, see "3.2.2.1 Searching for Online Devices".

Step 2 Select a device, and then click **Change IP**.

For devices that have the same username and password, you can select and modify their IP addresses in batches.

Figure 3-6 Change IP address



Step 3 Enter **New IP**, **Subnet Mask** and **Gateway**, and then click **Save**.

When setting IP addresses in batches, the IP addresses increase in sequence.

3.2.2.4 Adding Devices

You can add different types of devices, such as encoder, decoder, ANPR device, access control, LED, and video intercom. In this chapter, take adding encoder as an example. For other devices, the actual configuration interface shall prevail.

3.2.2.4.1 Adding Devices One by One

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click

Step 3 Click **Add**.

Step 4 Enter device login information, and then click **Add**.

In the **Add Mode** drop-down list,

- **IP Address**: Add a device. We recommend selecting this option when you know the IP address of the device.

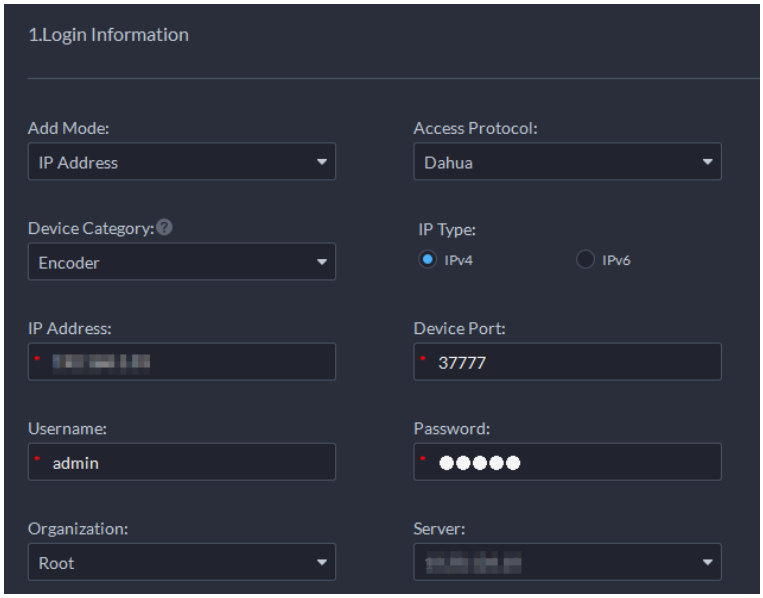
  Only **Encoder** devices support IPv6.

- **IP segment**: Add multiple devices in the same segment. We recommend selecting this option when the login username and password of the multiple devices in the same segment are the same.
- **Auto Registration**: We recommend this method when the IP address of a device might change. The ID of auto register has to be in accordance with the registered ID configured on the device you want to add. The port number must be the same on the platform and on the device. The auto register port is 9500 on the platform by default. To modify, open the system configuration tool to modify the DSS_ARS port number.
- **P2P**: Add devices under the specified P2P account to the platform by entering device SN. The platform and P2P server are required to have smooth connection with each other. There is no need to apply for the dynamic domain name of the device, perform port mapping or deploy a transit server when using it.

- **Domain Name** : We recommend selecting this option when the IP address of the device changes frequently and a domain name is configured for the device.

The parameters vary with the selected protocols.

Figure 3-7 Add an encoder



Step 5 Enter the information.

Step 6 Click **OK**.

- To add more devices, click **Continue to add**.
- To go to the web interface of devices, click .

3.2.2.4.2 Adding Devices through Searching

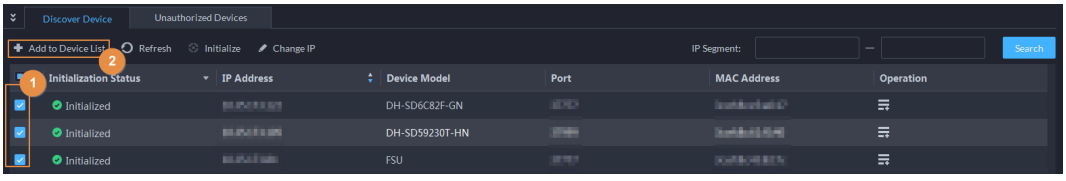
Devices on the same network with the platform server can be added using the automatic search function.

Step 1 Search for devices. For details, see "3.2.2.1 Searching for Online Devices".

Step 2 Select a device, and then click **Add to Device List** or .

If devices have the same username and password, you can select and add them in batches .

Figure 3-8 Add in batches



Step 3 Select the server and organization, enter username and password, and then click **OK**.

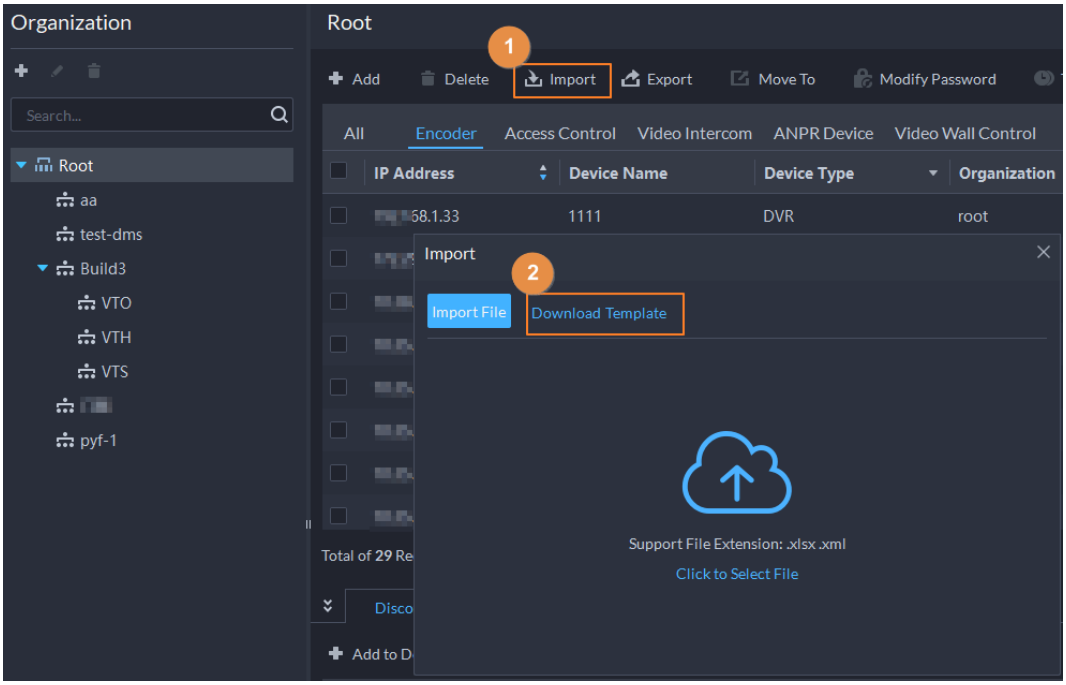
3.2.2.4.3 Importing Devices

Enter the device information in the template, and then you can add devices in batches.

Prerequisites

You have downloaded the template, and then enter device information in the template.

Figure 3-9 Download template



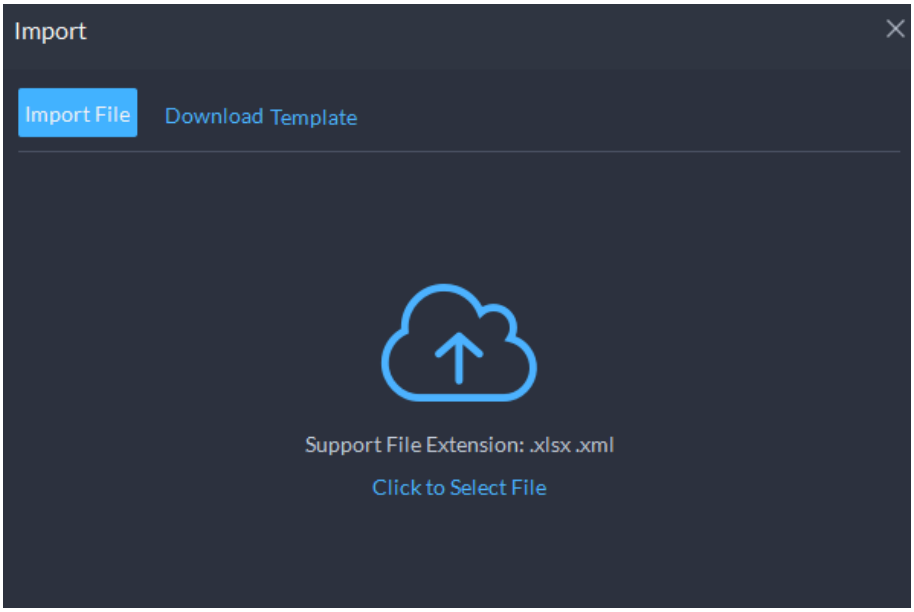
Procedure

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Configuration** section, select **Device**.

Step 2 Click .

Step 3 Click **Import**.

Figure 3-10 Import devices



Step 4 Click **Import File**, and then select the completed template.

Step 5 Click **OK**.

3.2.2.5 Editing Devices

Modify device information and organization.

3.2.2.5.1 Modifying Device Information

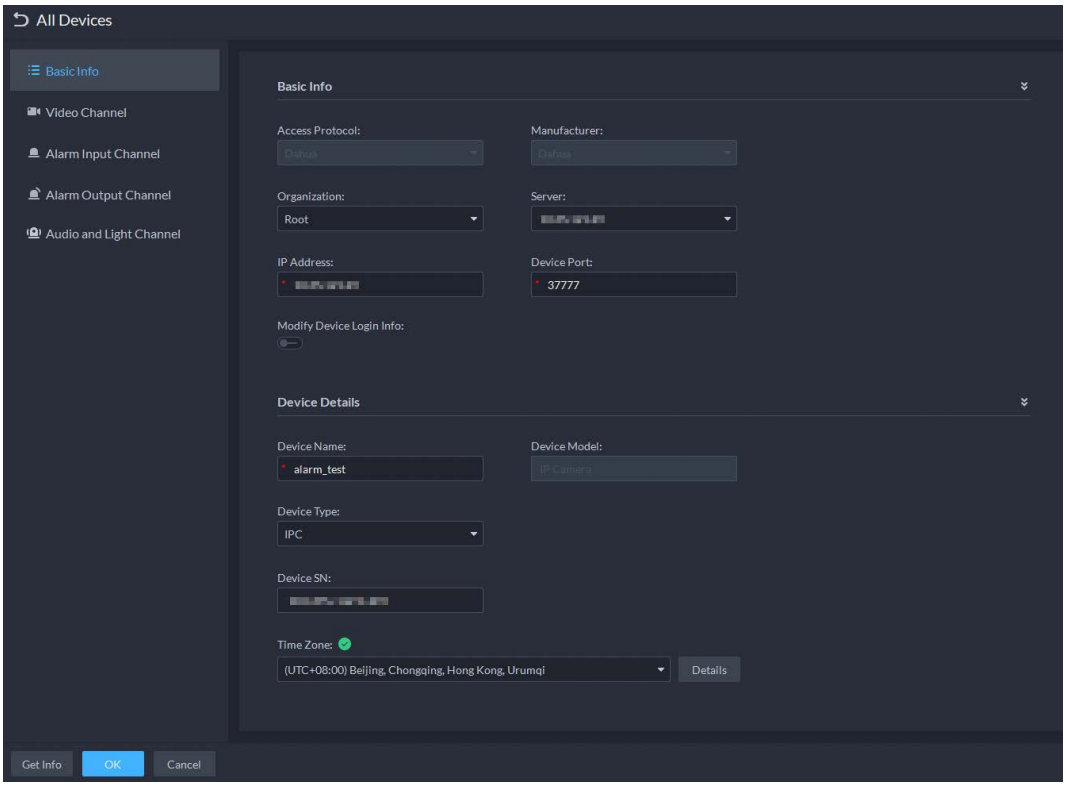
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Click of a device, and then edit device information.

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

Figure 3-11 Basic information



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

The types of features vary with different devices. Select features according to the capability of the camera.

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

Skip the step when the added devices do support alarm input.

- Alarm type includes external alarm, Infrared detect, zone disarm, PIR, gas sensor, smoke sensor, glass sensor, emergency button, stolen alarm, perimeter and preventer move.
- Alarm type supports custom. Select **Customize Alarm Type** in the **Alarm Type** drop-down list. Click **Add** to add new alarm type. It supports up to 30 custom alarm types.

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

Step 7 Click the **Audio and Light Channel** tab, and then edit the channel name.

This tab will only appear if the device has audio and light channels.

Step 8 Click **OK**.

3.2.2.5.2 Modifying Device Organization

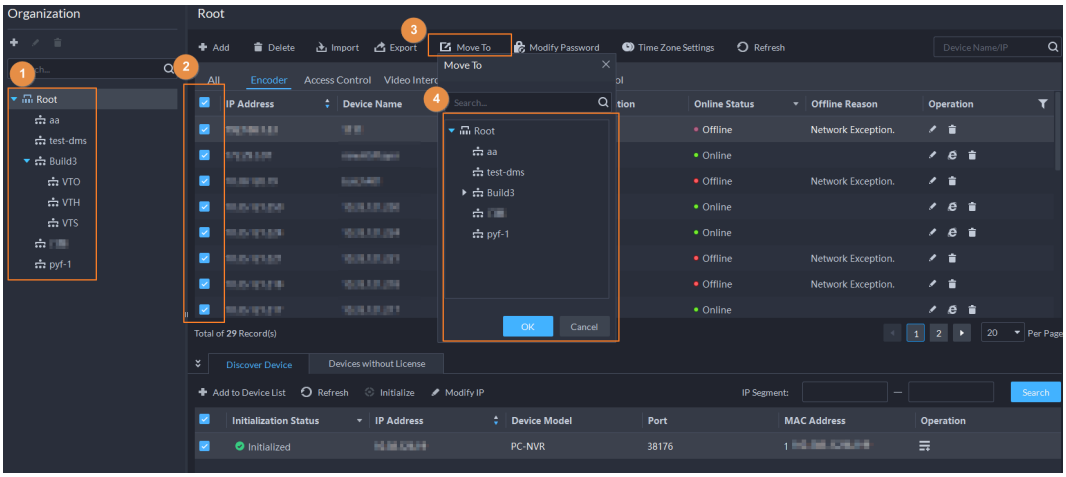
You can move a device from an organization node to another one.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a device to be moved, click **Move To**, select the target organization, and then click **OK**.

Figure 3-12 Move a device



3.2.2.5.3 Changing Device Password

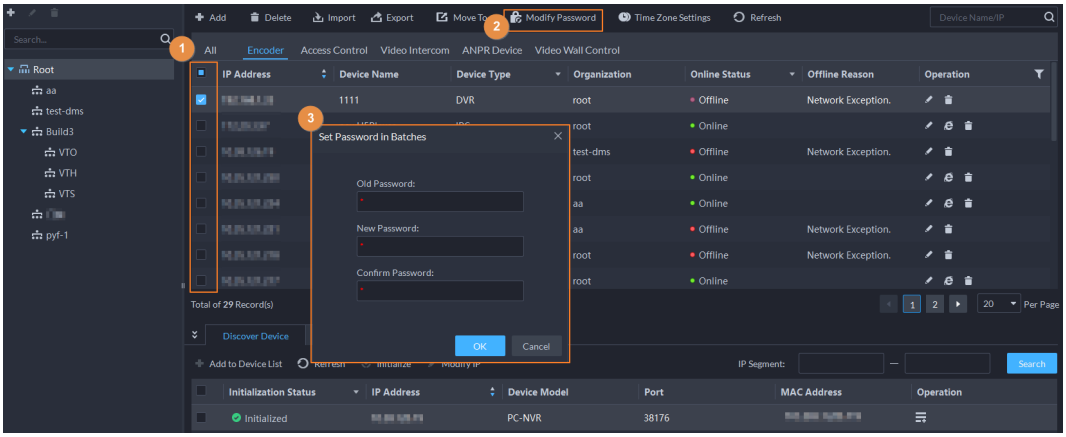
You can change device usernames and passwords in batches.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a device, and then click **Modify Password**.

Figure 3-13 Change device password



Step 4 Enter the old and new passwords, and then click **OK**.

3.2.2.6 Modifying Device Time Zone

Configure device time zone correctly. Otherwise you might fail to search for recorded video.

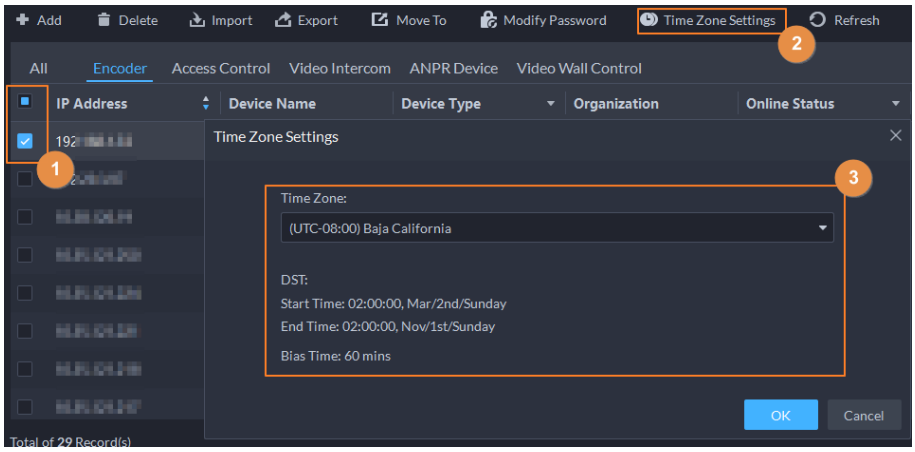
If a device is accessed through ONVIF and the ONVIF version is earlier than 18.12, the device DST cannot be edited on the platform. You can only edit manually.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a device, and then click **Time Zone Settings**.

Figure 3-14 Modify device time zone



Step 4 Select a time zone.

Step 5 Click **OK**.

3.2.2.7 Exporting Devices

You can export the information of all the devices on the DSS client. When you need to switch or configure a new platform, you can quickly add them all.

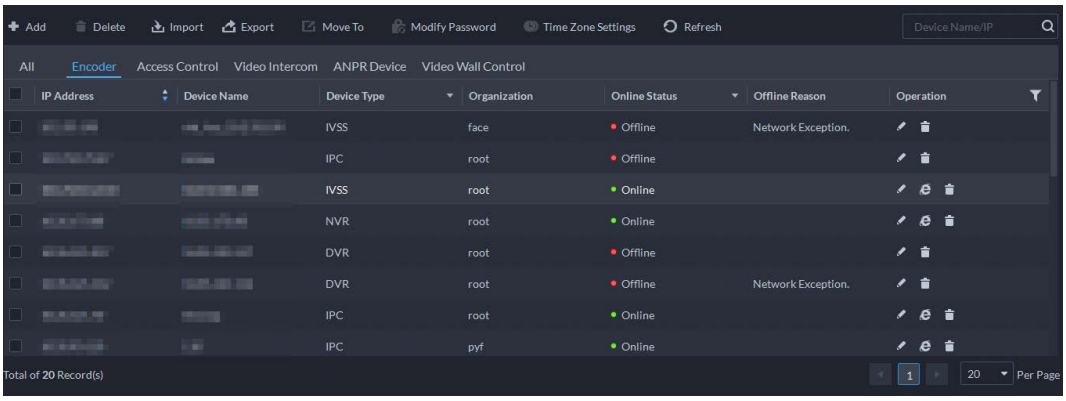
You can export up to 100,000 devices at a time.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 (Optional) Select only the devices that you need.

Figure 3-15 Select a device type



Step 4 Click **Export**.

Step 5 Enter the password used to log in to the DSS client, encryption password, and range, and then click **OK**.

- Encryption password: You need to enter this password when you open the exported file.
- You can select **All** to export all the devices, or **Selected** to export the devices you selected.

Step 6 Select a path on your PC, and then click **Save**.

3.2.3 Binding Resources

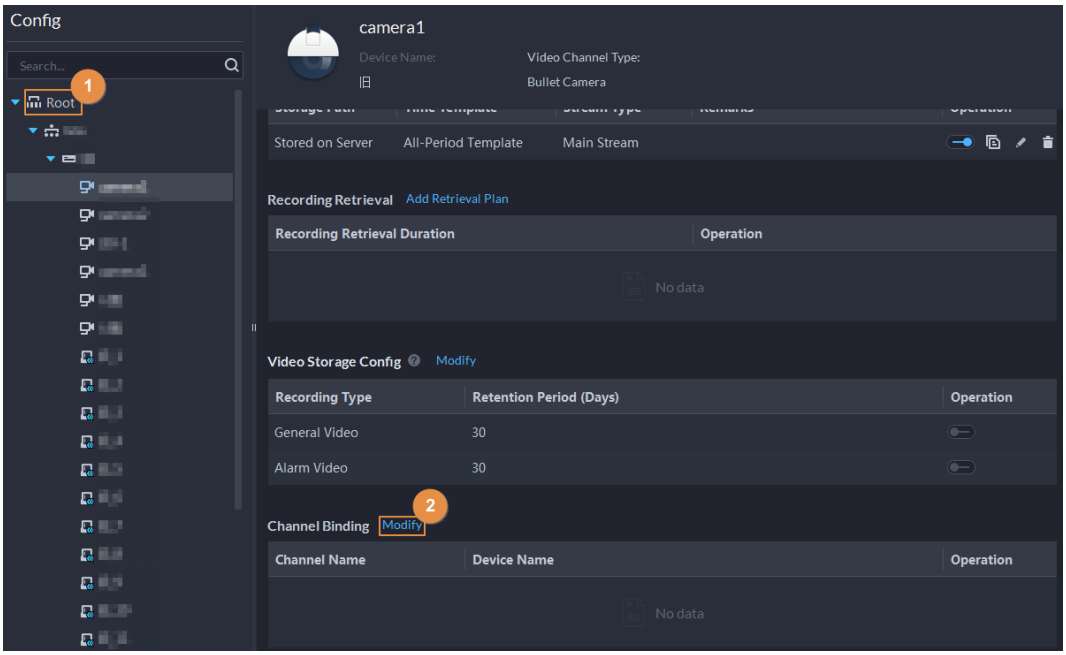
The platform supports binding resources for linked actions. You can bind a video channel with an alarm input channel, ANPR channel, access control channel or another video channel, so that you can view the associated video for alarm, face and other businesses.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a channel, and then click **Modify**.

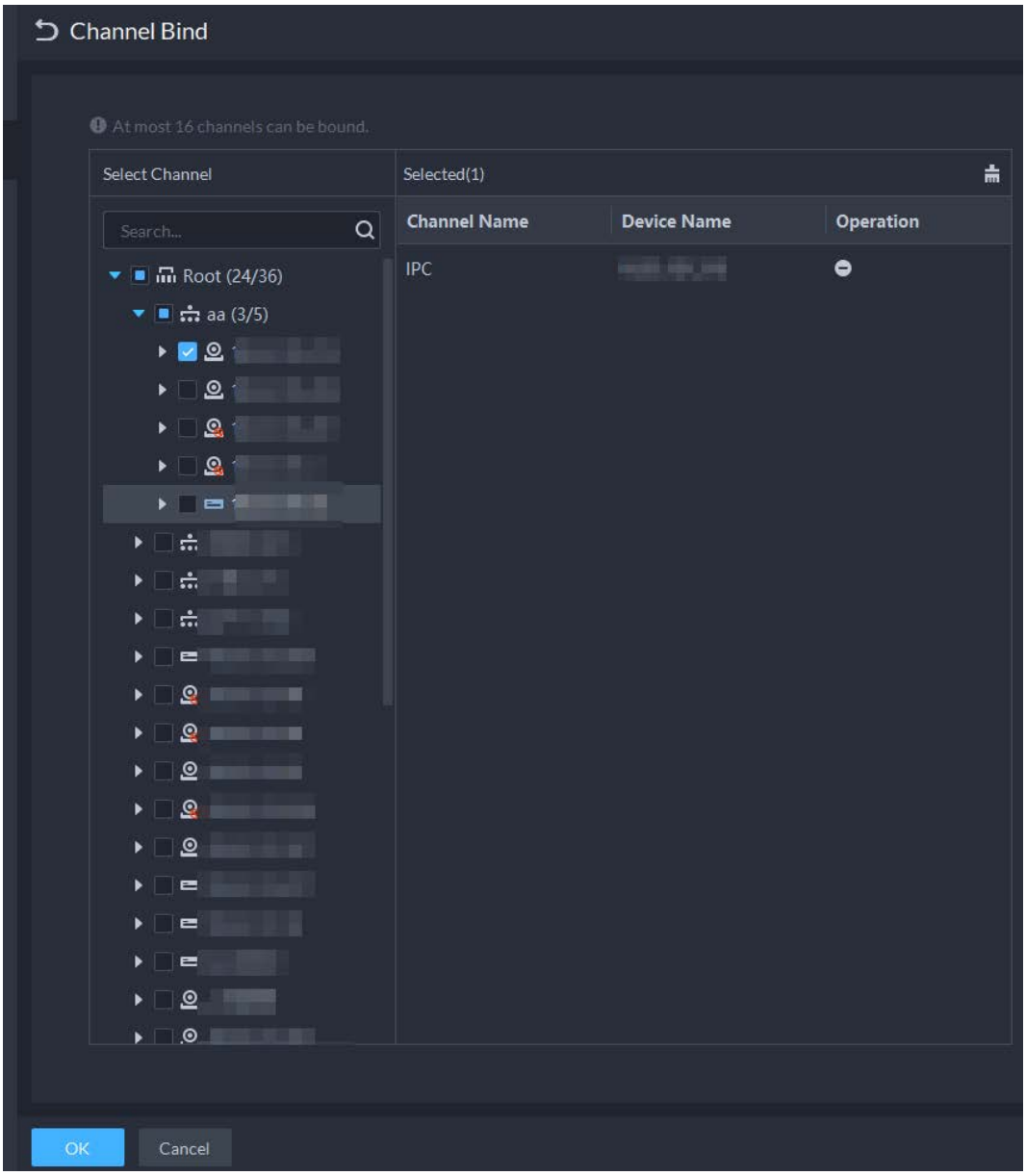
Figure 3-16 Go to channel bind interface



Step 4 Select a channel, and then click **OK**.

Multiple channels can be selected

Figure 3-17 Go to channel bind interface



Step 5 Click **OK**.

3.2.4 Adding Recording Plan

Configure recording plans for video channels so that they can record videos accordingly.
You can configure two recording plans for a channel. One is center recording plan for storing videos on the server, and the other is device recording plan for storing videos on the device.

3.2.4.1 Adding Recording Plan One by One

Add a center recording plan or device recording plan for a channel, so that it can make recordings

within the defined period.

Procedure

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a channel, and then configure a recording plan.

- Configure a center recording plan.

1) Click **Add Recording Plan** next to **Center Recording Plan**.

Figure 3-18 Add a center recording plan (1)

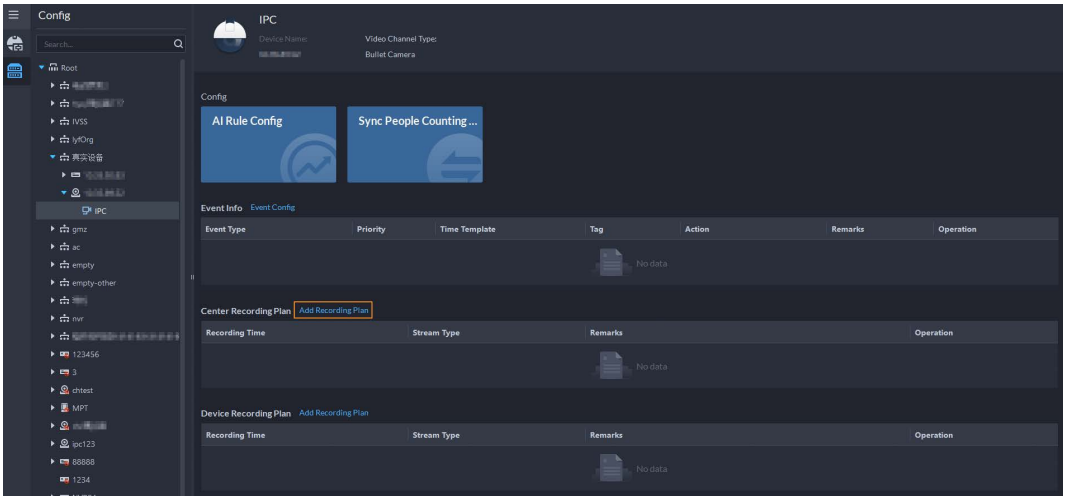
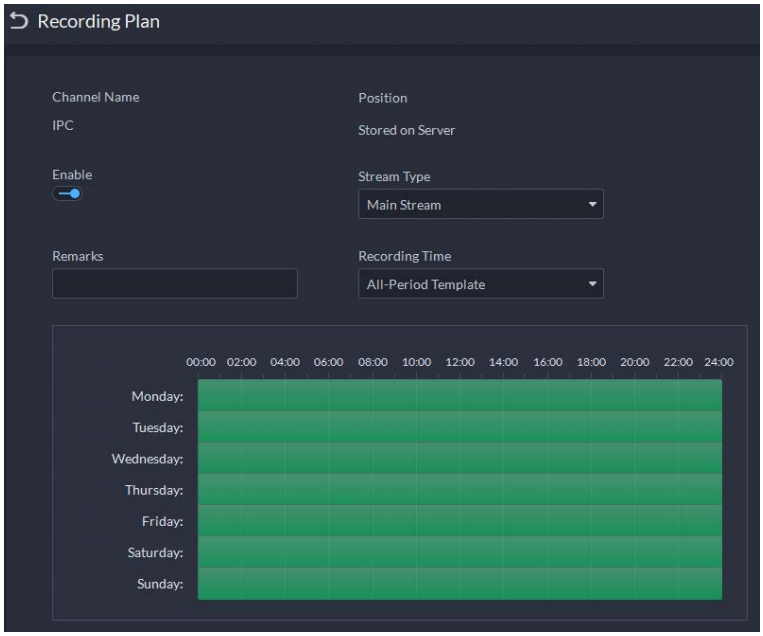


Figure 3-19 Add a center recording plan (2)



2) Configure the parameters.

Table 3-1 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the server by default. It cannot be changed.
Stream Type	Select **Main Stream**, **Sub Stream 1** or **Sub Stream 2**.

Parameter	Description
Remarks	Customizable description for the recording plan.
Recording Time	Select a default time template or click **Create Time Template** to add a new time template. See "3.2.5 Adding Time Template".

3) Click **OK**.

- Configure a device recording plan.

1) Click **Add Recording Plan** next to **Device Recording Plan**.

Figure 3-20 Add a device recording plan (1)

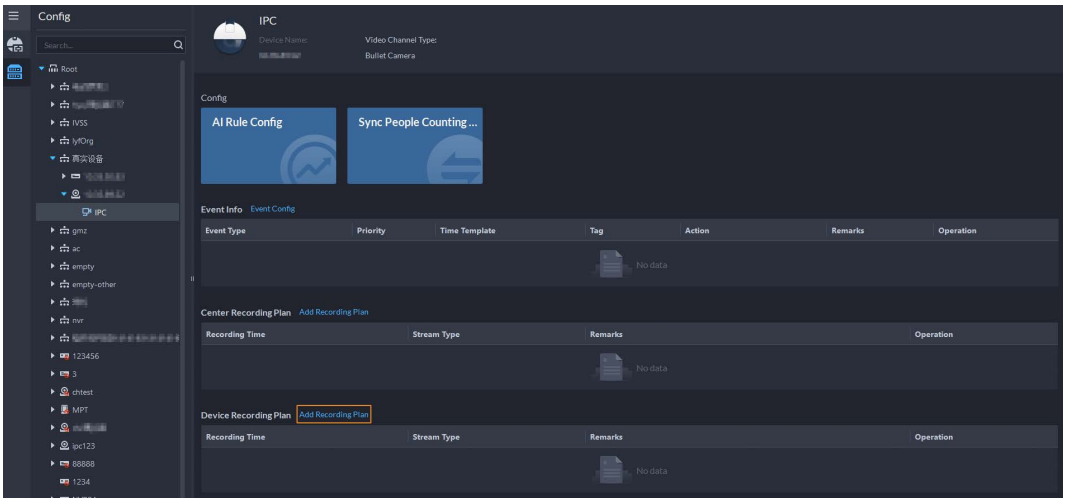
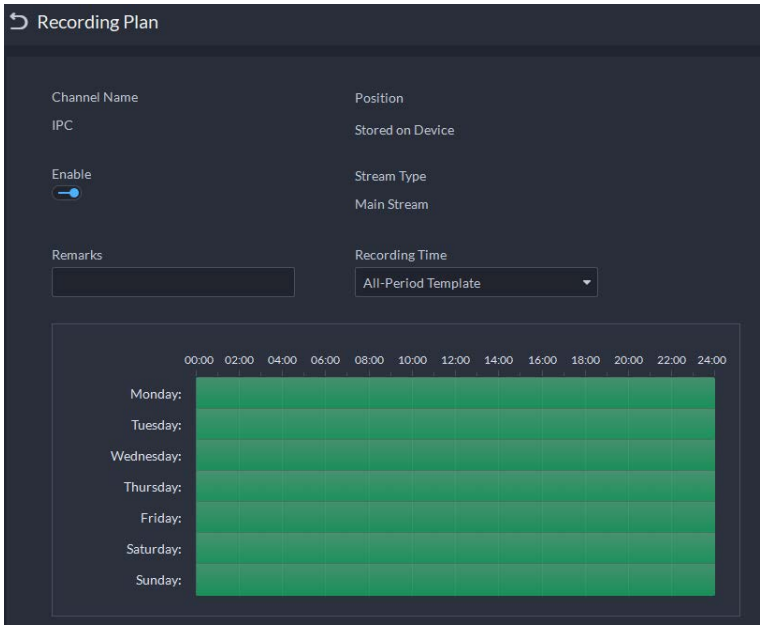


Figure 3-21 Add a device recording plan (2)



2) Configure the parameters.

Table 3-2 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the device by default. It cannot be changed.
Stream Type	The device will make recordings using the main stream by default. It cannot be changed.
Remarks	Customizable description for the recording plan.

Parameter	Description
Recording Time	Select a default time template or click **Create Time Template** to add a new time template. See "3.2.5 Adding Time Template".

3) Click **OK**.

Related Operations

- Enable/disable a recording plan

  means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.
- Click : Copy the recording plan to other channels. You can select up to 100 channels at the same time.
- Edit a recording plan

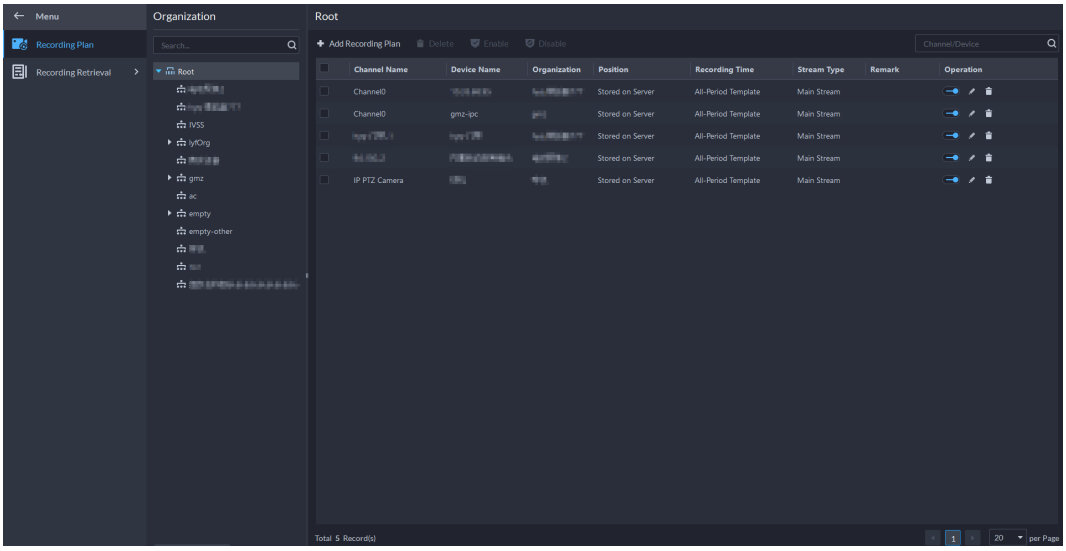
  Click of corresponding plan to edit the plan.
- Click to delete recording plans one by one.

3.2.4.2 Adding Center Recording Plans in Batches

Add a center recording plan for multiple channels at the same time.

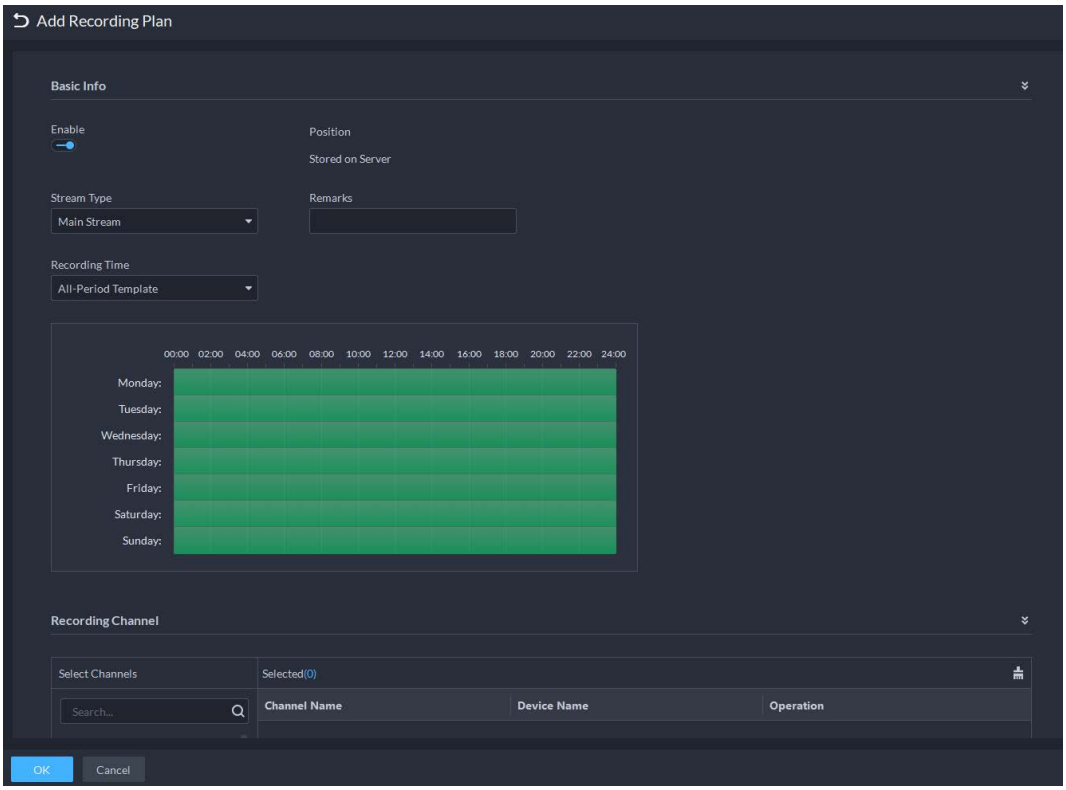
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **App Config** section, select **Storage Plan** > **Recording Plan**.

Figure 3-22 Center recording plan



Step 2 Click **Add Recording Plan**.

Figure 3-23 Configure a center recording plan



Step 3 Configure the parameters, and then select channels in the **Recording Channel** section.

Table 3-3 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the server by default. It cannot be changed.
Stream Type	Select **Main Stream**, **Sub Stream 1** or **Sub Stream 2**.
Remarks	Customizable description for the recording plan.
Recording Time	Select a default time template or click **Create Time Template** to add a new time template. See "3.2.5 Adding Time Template".

Step 4 Click **OK**.

- Enable/disable a recording plan

  means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.
- Edit a recording plan

  Click of corresponding plan to edit the plan.
- Edit a recording plan

  Click of corresponding plan to edit the plan.
- Delete: Select multiple channels, and then delete them at the same time.
- Enable and Disable: Select multiple channels, and then enable or disable them at the same time.

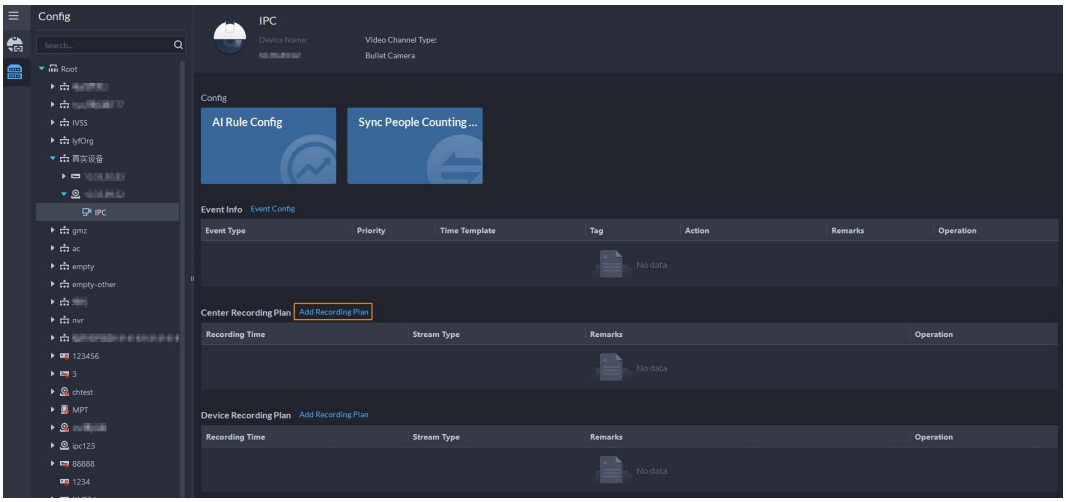
3.2.5 Adding Time Template

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a channel, and then click **Add Recording Plan**.

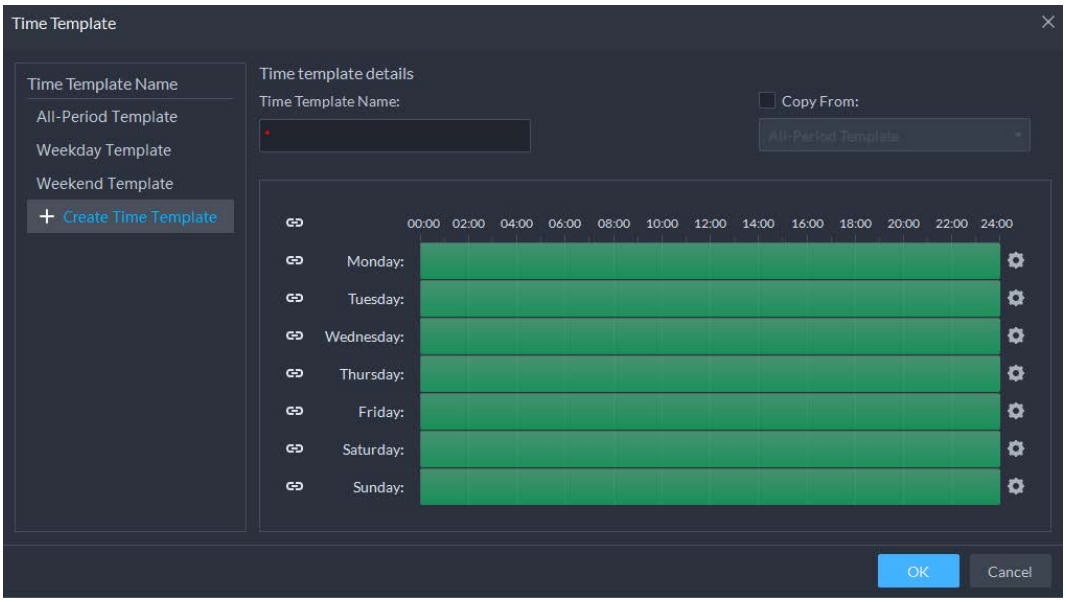
Figure 3-24 Go to add record plan interface



Step 4 In the **Time Template** drop-down list, select **Create Time Template**.

Creating time template in other interfaces is the same. This chapter takes creating time template in **Record Plan** interface as an example.

Figure 3-25 Create time template



Step 5 Configure name and periods. You can set up to 6 periods in one day.

Select the **Copy From** check box, and then you can select a template to copy from.

- On the time bar, click and drag to draw the periods.
- You can also click to configure periods.

Step 6 Click **OK**.

3.2.6 Configuring Video Retention Period

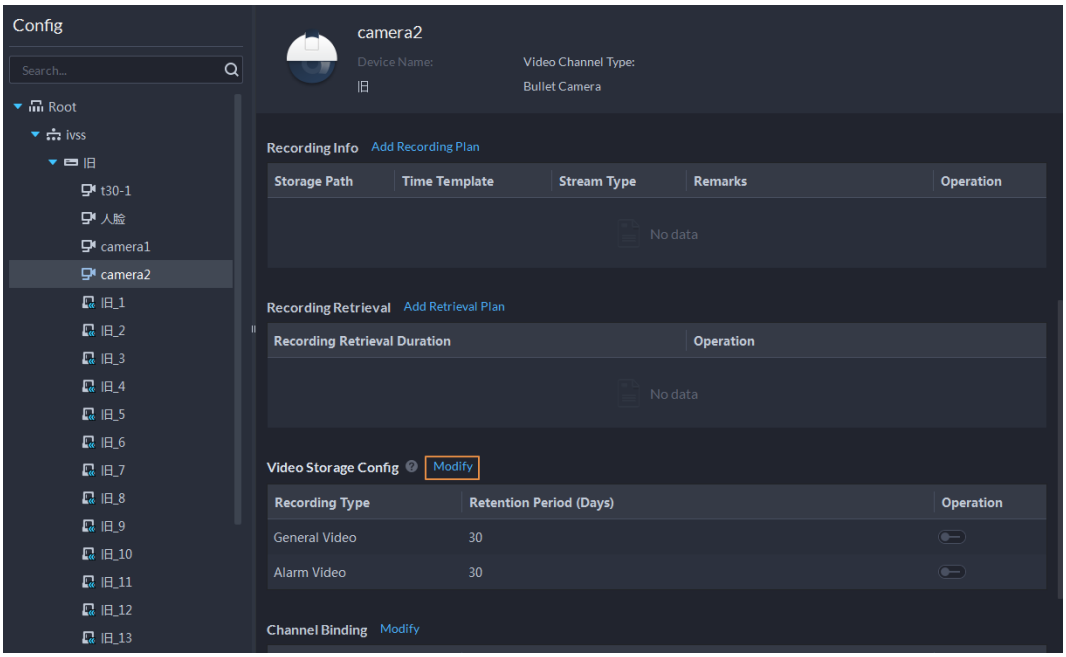
For videos stored on the DSS server, you can configure video retention period. When the storage space runs out, new recorded videos will cover the oldest videos automatically.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a camera, and then click **Modify**.

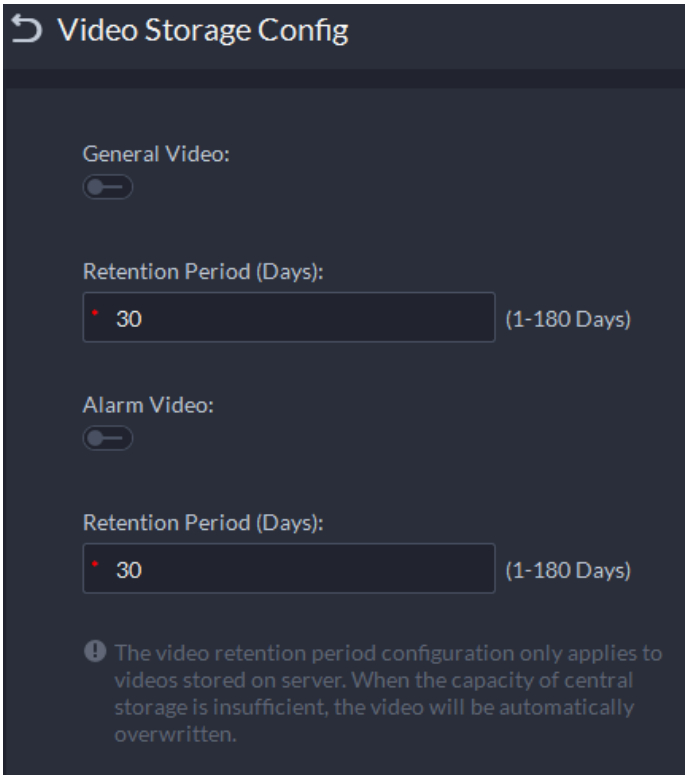
Figure 3-26 Go to recording storage configuration interface



Step 4 Configure video retention period, and then click to enable the setting.

For the free version of Express, the retention period cannot be more than 7 days. If you need more than 7 days, you need to purchase an official version.

Figure 3-27 Configure video retention period



Step 5 Click **OK**.

Related Operations

Enable/disable record plan

In the operation column,  means that the recoding storage configuration has been enabled. Click the icon and it becomes  , meaning that the configuration has been disabled.

3.2.7 Configuring Events

You need to set up the event configuration on a device its channels to display events on the platform.

Log in to the DSS client. On the Home interface, click  , and then in the **Applications Configuration** section, select **Event**. For details, see "4.1 Configuring Events".

Step 1 Log in to the DSS Client. On the **Home** interface, click  , and then in the **Basic Config** section, select **Device**.

Step 2 Click 

Step 3 Select a channel or a device, and then click **Event Config**.

Figure 3-28 Go to the event configuration (device)

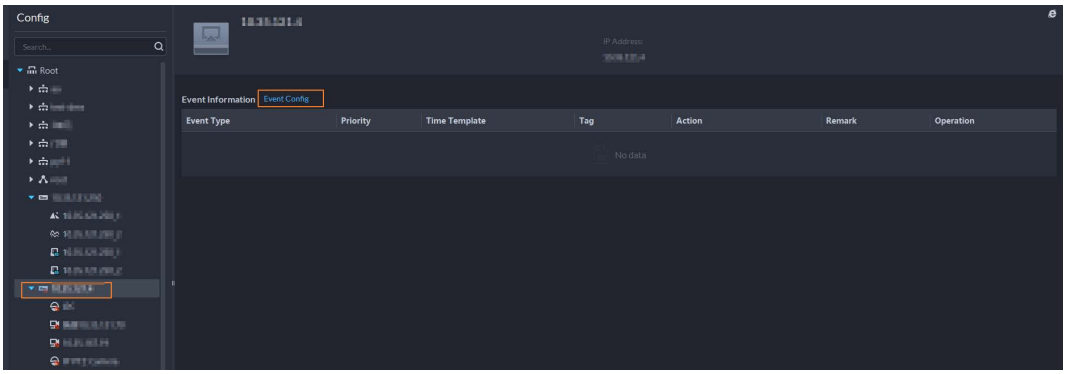
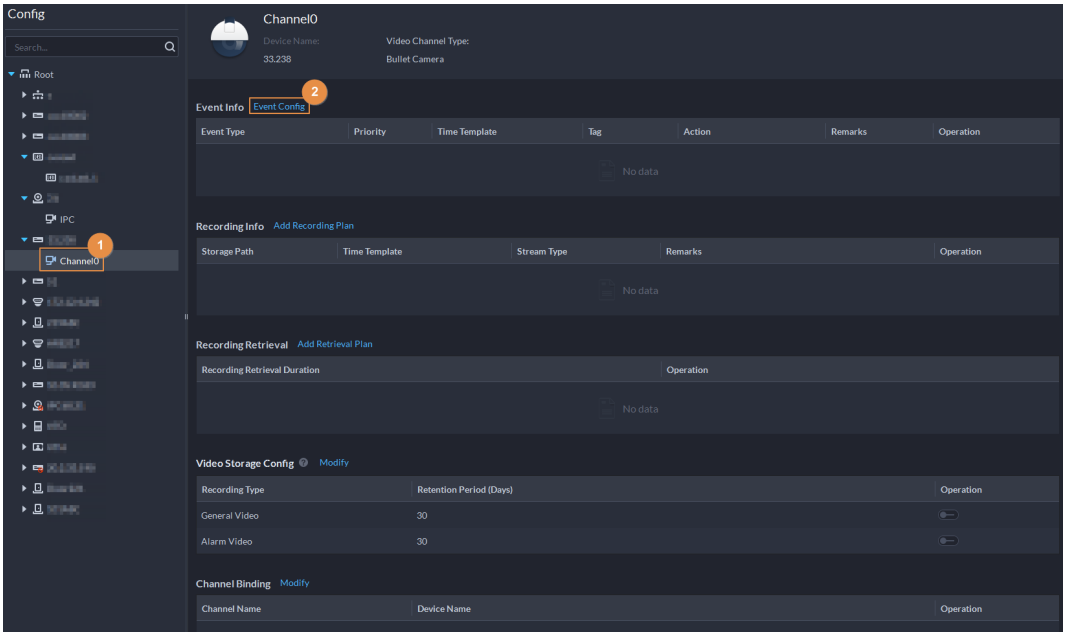


Figure 3-29 Go to the event configuration (channel)



Step 4 Configure events. See "4.1 Configuring Events".

3.2.8 Configuring Device Parameters

Configure the camera properties, video stream, snapshot, video overlay, and audio configuration for the device channel on the platform. The platform only supports configuring the channels added via IP in Dahua protocols.

Device configuration might vary depending on the capacities of the devices. The interfaces in the section are for reference only, and might differ from the actual ones.

3.2.8.1 Configuring Camera Properties

Configure camera image parameters for the **Daytime**, **Night**, and **Regular** modes to ensure high image quality.

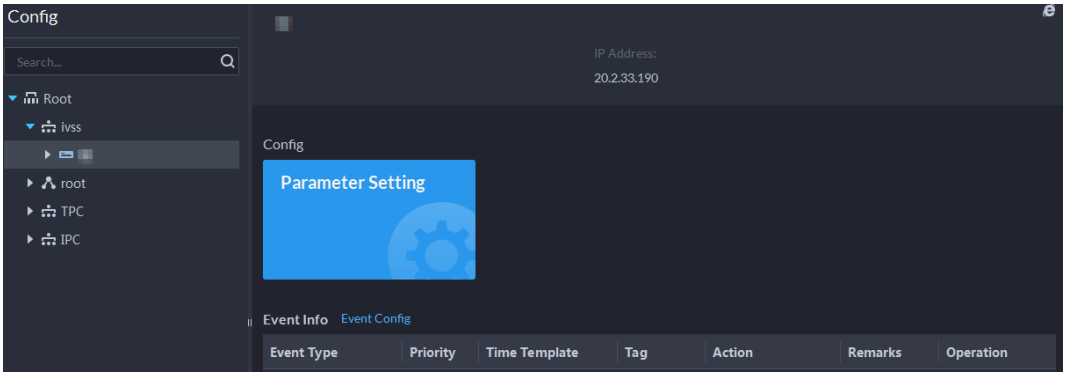
3.2.8.1.1 Configuring Property Files

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

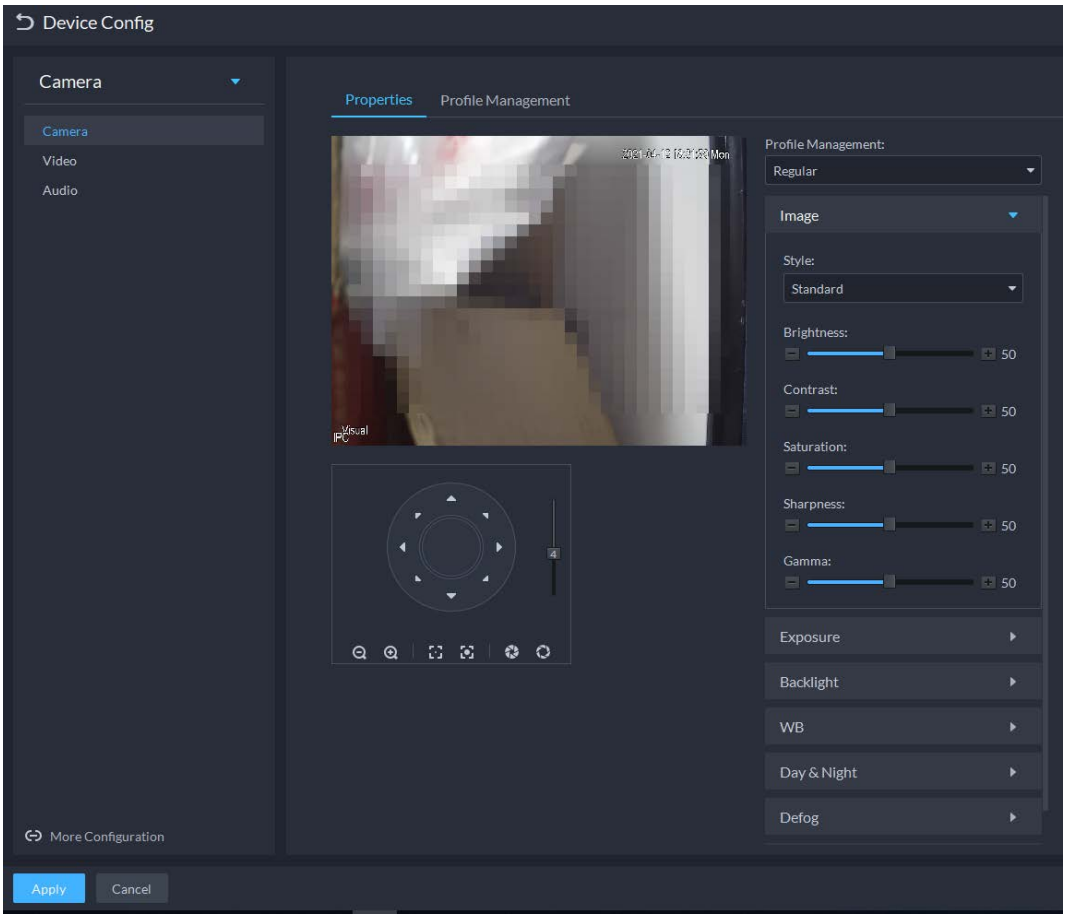
Step 3 Select a device, and then click **Device Config**.

Figure 3-30 Device configuration



Step 4 Select **Camera** > **Camera** > **Properties** > **Image**.

Figure 3-31 Image



- To go to the device web interface, you can click **More configuration**.
- PTZ will be displayed if the device has PTZ function.

Step 5 Select **Profile Management**.

Step 6 Click **Image** to configure image parameters.

Table 3-4 Image parameters

Parameter	Description
Style	You can set the image style to be **Standard**, **Gentle**, or **Flamboyant**.
Brightness	You can adjust the overall image brightness through linear tuning. The higher the value, the brighter the image and vice versa. If this value is set too high, images tend to look blurred.
Contrast	Adjusts the contrast of the images. The higher the value, the bigger the contrast between the bright and dark portions of an image and vice versa. If the contrast value is set too high, the dark portions of an image might become too dark, and the bright portions might be over-exposed. If the contrast value is set too low, images tend to look blurry.
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.

Parameter	Description
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 7 Click **Exposure** to set relevant parameters.

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

Figure 3-32 Exposure

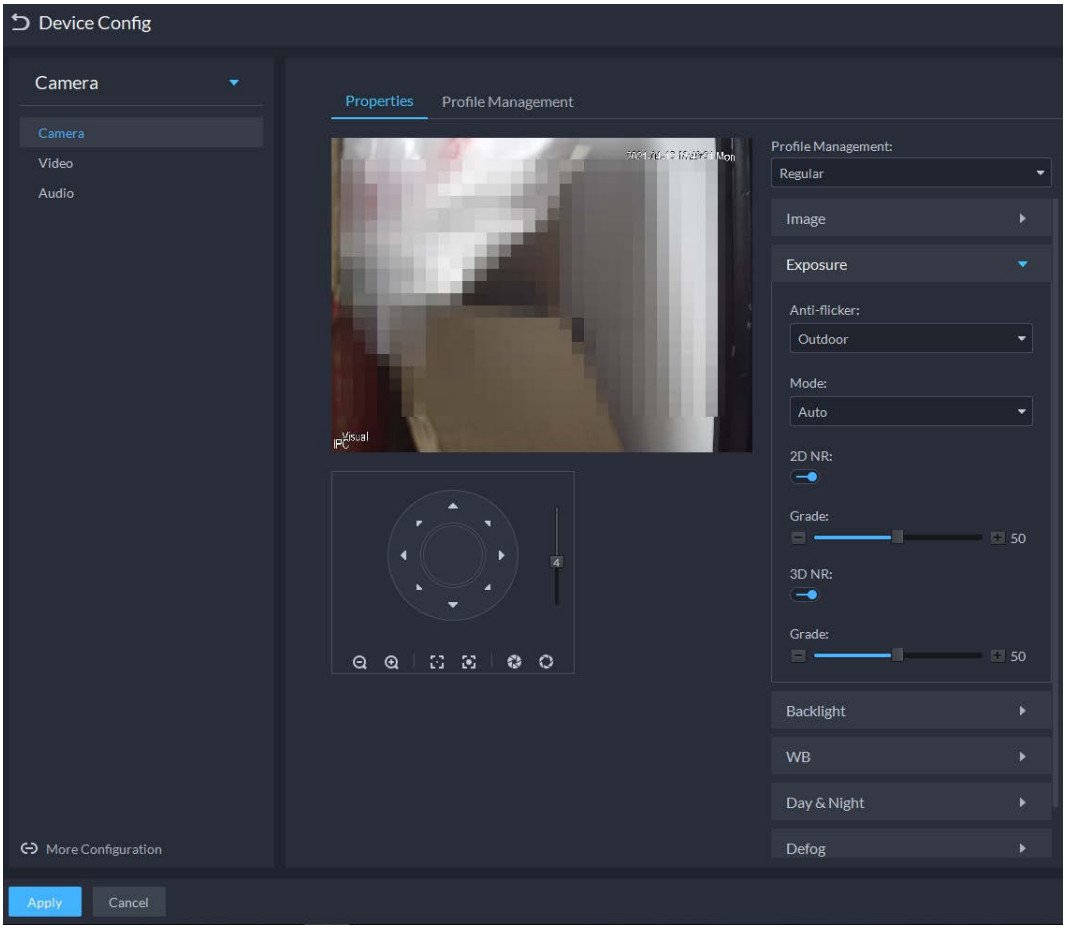


Table 3-5 Exposure parameters

Parameter	Description
Anti-flicker	• **50Hz** and **60Hz**: With the 50/60 Hz household power supply, exposure can be automatically adjusted based on the brightness of the scene to ensure that horizontal stripes do not appear on the image. • **Outdoor**: In an outdoor scenario, you can switch the exposure modes to achieve your target effect.

Parameter	Description
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 might be different.
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 8 Click **Backlight** to set up relevant parameters.

The backlight mode offers backlight correction, Wide Dynamic, and Glare Inhibition features.

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

Figure 3-33 Backlight

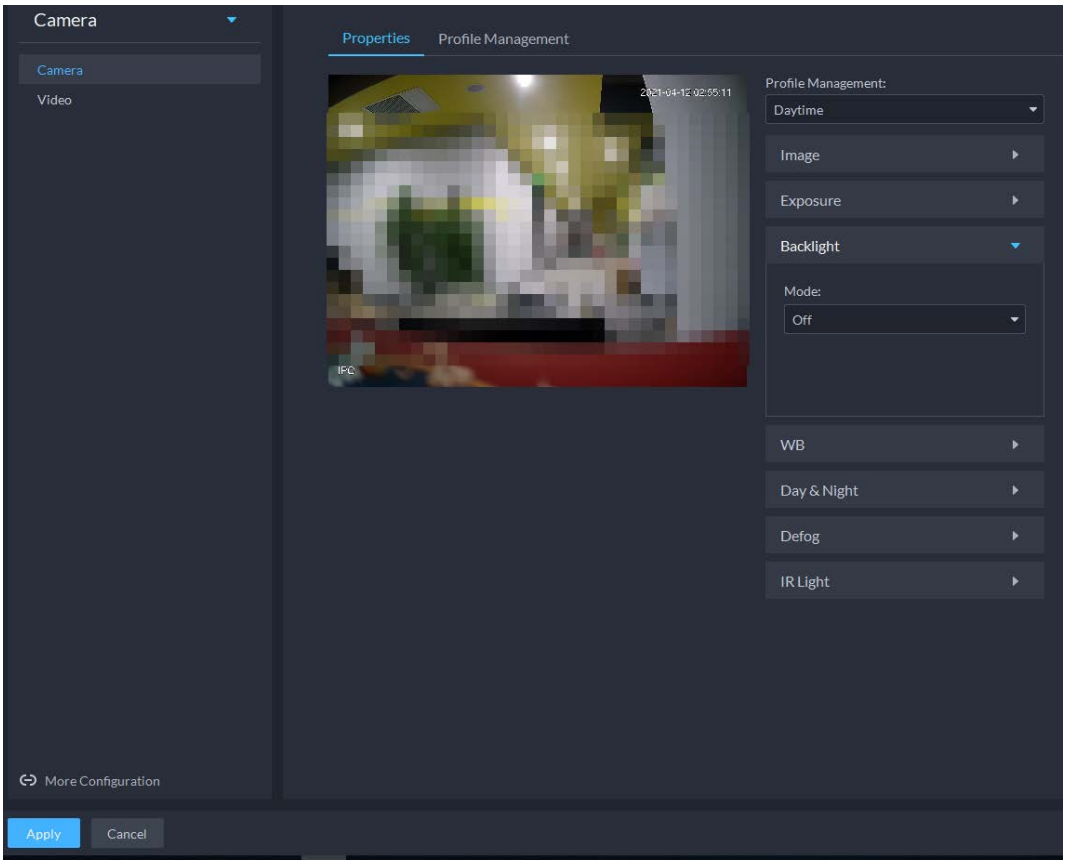


Table 3-6 Backlight parameters

Backlight Mode	Description
Backlight Correction	• 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.
HLC	Glare inhibition. The system inhibits the brightness in bright regions and reduces the size of the halo, to make the entire image less bright.
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.
SSA	The system adjusts image brightness automatically based on the environmental lighting conditions to show image details clearly.

Step 9 Click **WB** to set relevant parameters.

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

Figure 3-34 WB

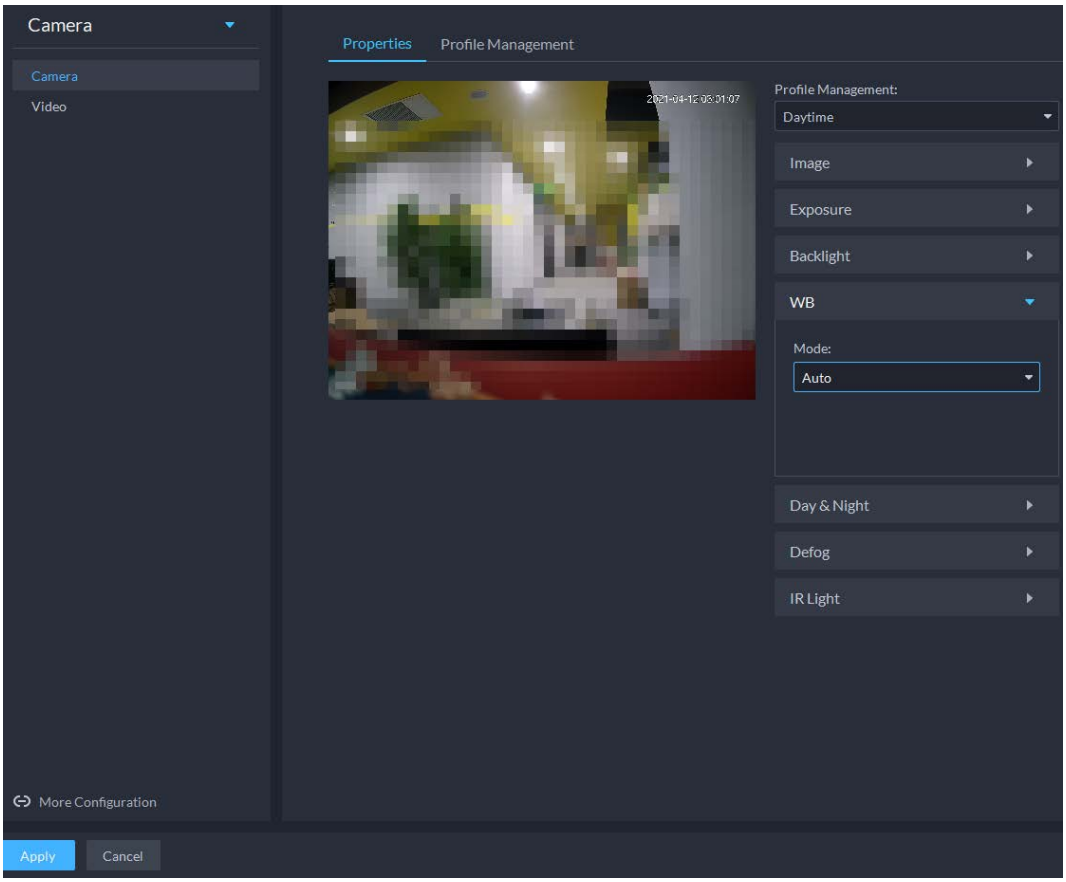


Table 3-7 WB parameters

WB Mode	Description
Auto	The system automatically corrects different color temperatures to ensure normal display of image colors.
Natural Light	The system automatically corrects the scenes without manmade lighting to ensure normal display of image colors.
Street Lamp	The system automatically corrects the outdoor scenes at night to ensure normal display of image colors.
Outdoor	The system automatically 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 corrects different color temperatures to ensure normal display of image colors.

Step 10 Click **Day & Night** to set up relevant parameters.

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

Figure 3-35 Day & night

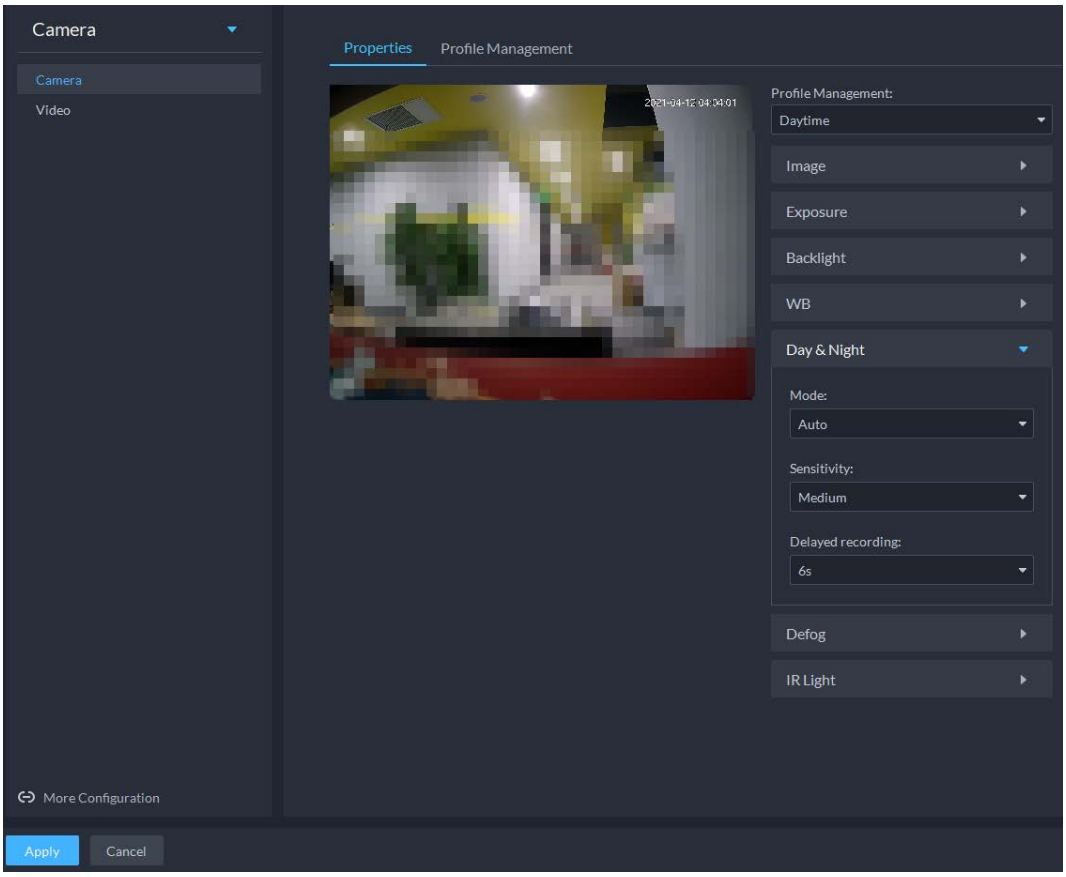


Table 3-8 Day & night parameters

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

Step 11 Click **Defog** to set up relevant parameters. See "Defog". For details of the parameters, see "Defog parameters".

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

Figure 3-36 Defog

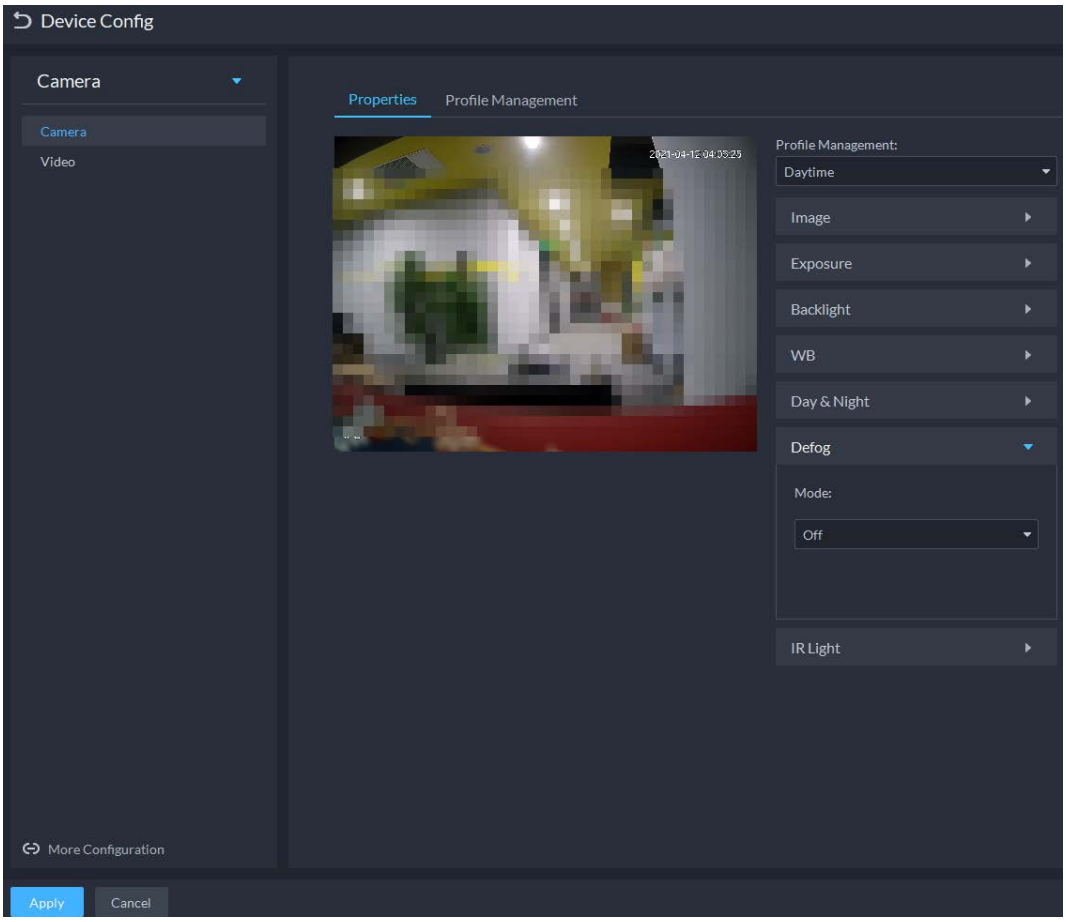


Table 3-9 Defog parameters

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

Step 12 Click **IR Light** to set relevant parameters.

Figure 3-37 IR light

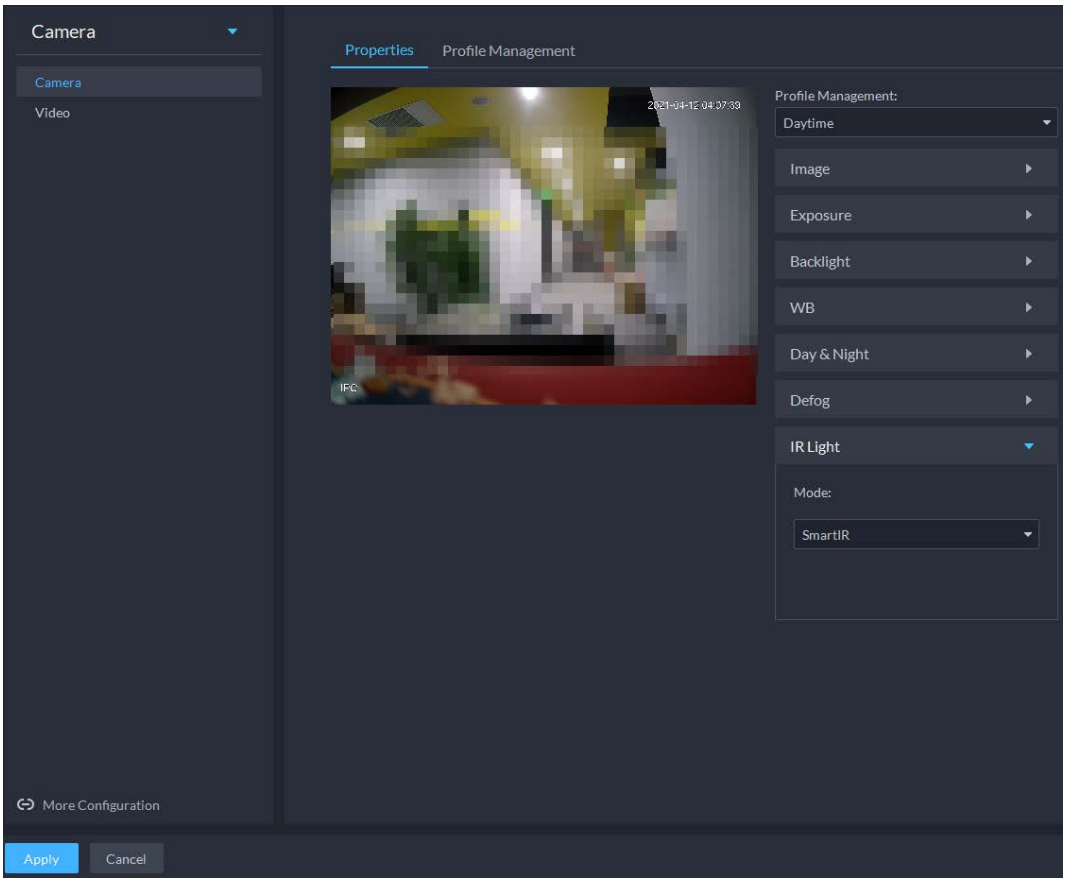


Table 3-10 IR light parameters

IR Light Mode	Description
Manual	You can set up the IR light brightness manually. The system provides 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.
Off	IR light disabled.

Step 13 Click **OK**.

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

3.2.8.1.2 Applying Configuration Files

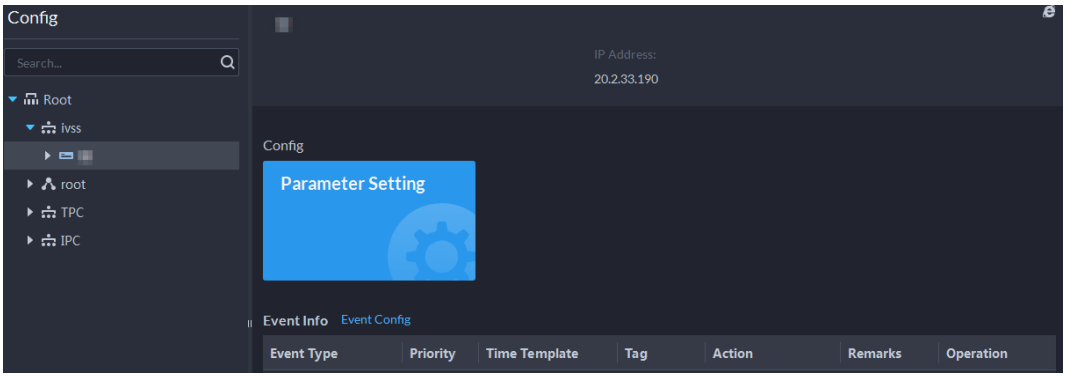
Apply the image parameters as configured in the pre-defined periods.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a device, and then click **Device Config**.

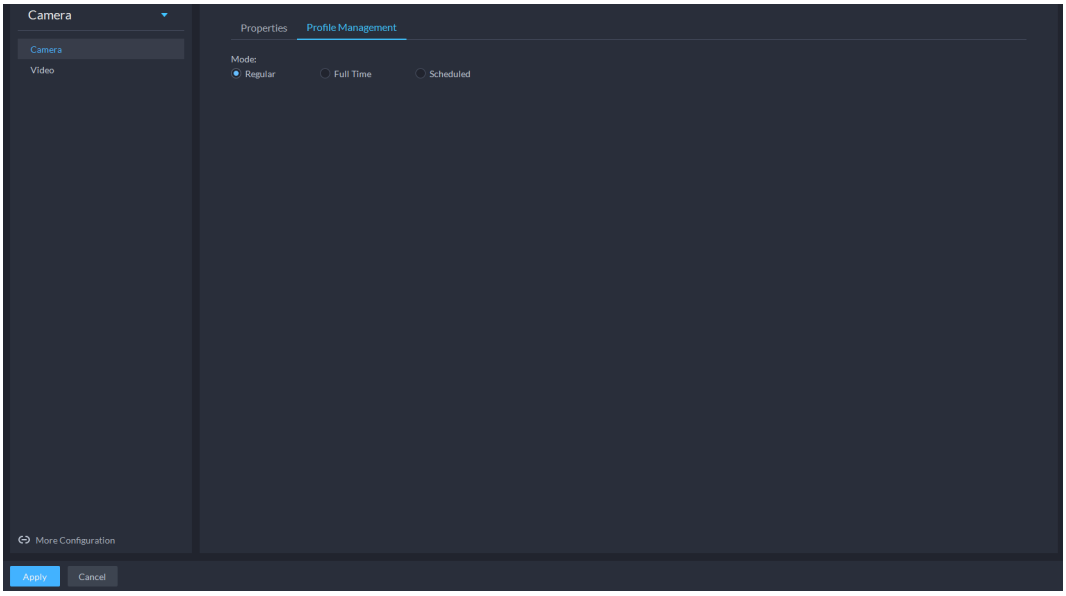
Figure 3-38 Device configuration



Step 4 Click **Profile Management**, and set configuration files.

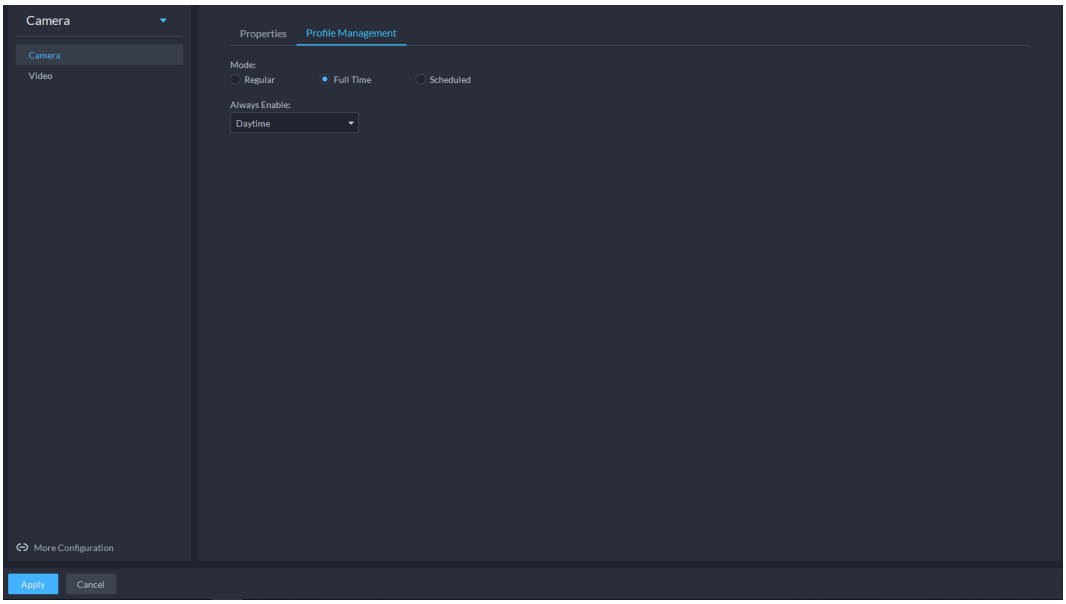
- When **Config Files** is set to **Regular**, the system monitors the objects as per regular configurations.

Figure 3-39 Set configuration files as regular



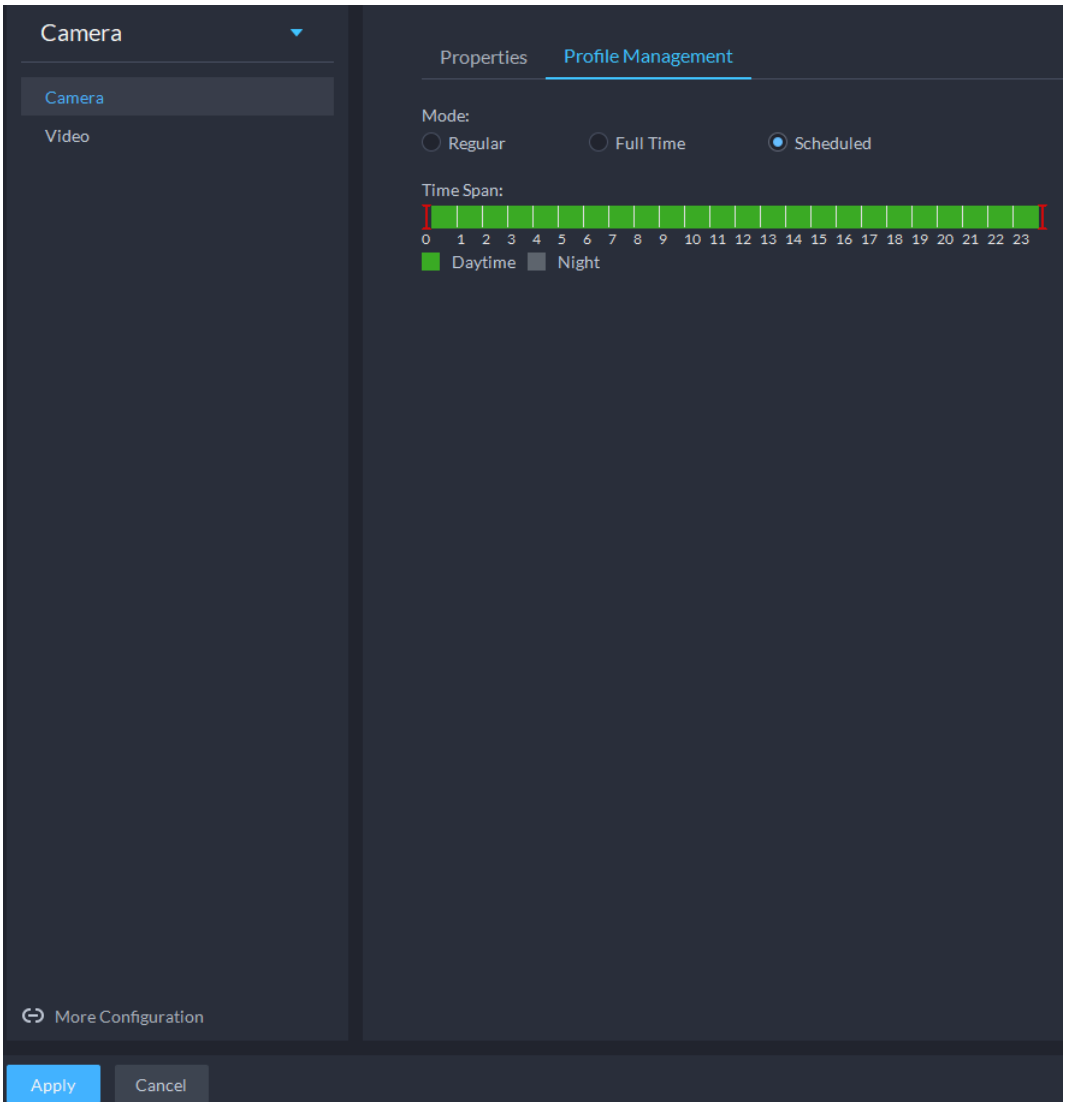
- When **Config Files** is set to **Full Time**, you can set **Always Enable** to **Daytime** or **Night**. The system monitors the objects as per the **Always Enable** configurations.

Figure 3-40 Set configuration files as full time



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

Figure 3-41 Set configuration files as shift by time



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

3.2.8.2 Video

Set video parameters such as video stream, snapshot stream, overlay, ROI, saving path, and video encryption.

3.2.8.2.1 Video Stream

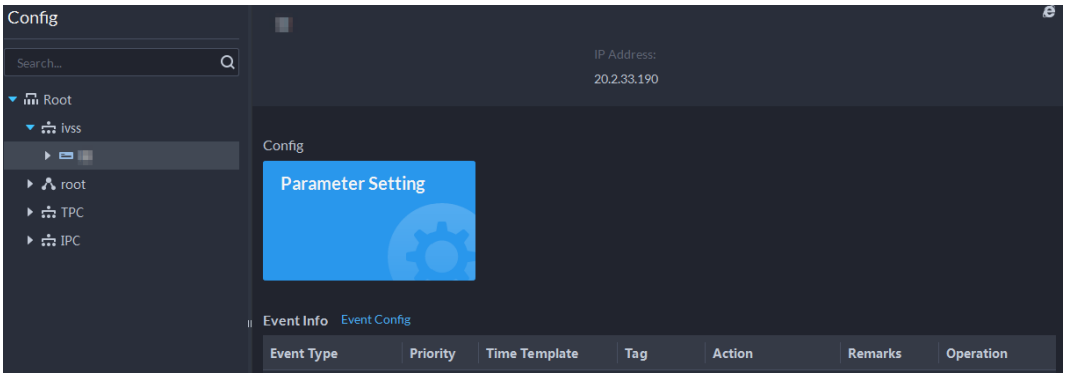
Set the video stream parameters such as stream type, encoding mode, resolution, frame rate, stream control, stream, I frame interval, SVC, and watermark.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a device, and then click **Device Config**.

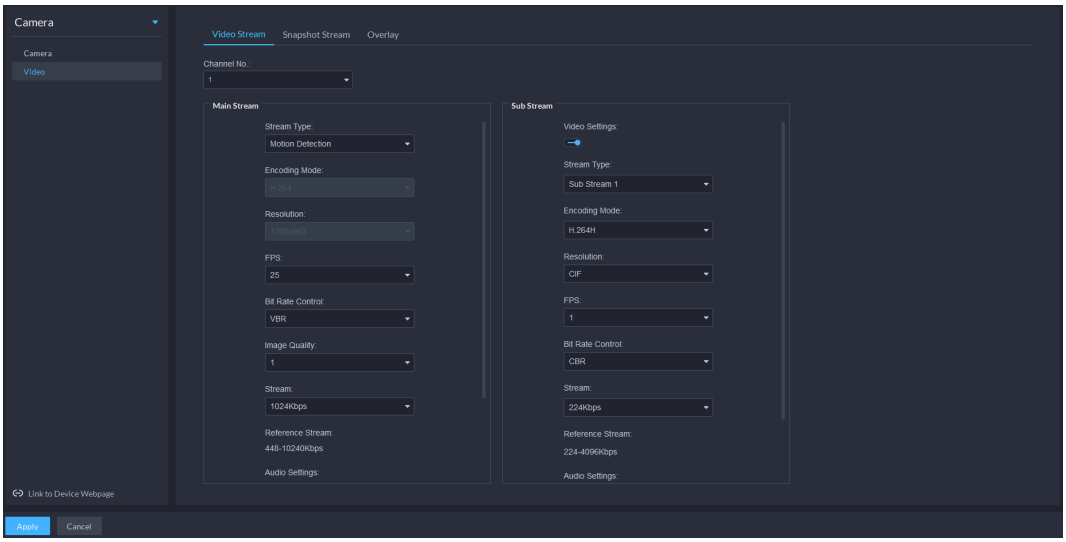
Figure 3-42 Device configuration



Step 4 Select **Camera** > **Video** > **Video Stream**.

Step 5 Set **Video Stream**.

Figure 3-43 Configure video stream settings



The default values of streams are for reference only, and the actual interfaces might be different.

Table 3-11 Video stream parameters

Parameter	Description
Video Settings	Indicates whether to set up the **Sub Stream** parameters.
Encoding Mode	• H.264: H.264B (Baseline Profile), H.264 (Main Profile), H.264H (High Profile). Bandwidth consumption level at the same image quality: H.264B > H.264 > H.264H. • H.265: Main Profile encoding, consuming less bandwidth than H.264 at the same image quality. • MJPEG: Frame-by-frame compression, requiring large bandwidth and high video stream to ensure clear image. To achieve better video image, it is recommended that you select the largest stream value from the given options.

Parameter	Description
Smart Codec	Turning on **Smart Codec** will compress the images to save storage space. When smart code is on, the device does not support sub stream 2, ROI, IVS event detection.
Resolution	The resolution of the videos. Different devices might have different max resolutions.
FPS	The number of frames per second in a video. The higher the FPS, the more distinct and smooth the images.
Bit Rate Control	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.
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.
Stream	This parameter can be set only when **Stream Ctrl** is set to **BRC_CBR**. You can select the proper stream value from the drop-down box based on actual scenarios.
Reference Stream	The system will recommend an optimal range of stream values to users based on the resolution and FPS set up by them.
I Frame 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.
Watermark	Turn on **Watermark** to enable this feature. You can verify the watermark characters to check whether the video has been tempered or not.
Watermark	Characters for watermark verification. The default value is DigitalCCTV.

Step 6 Click **Apply**.

3.2.8.2.2 Snapshot Stream

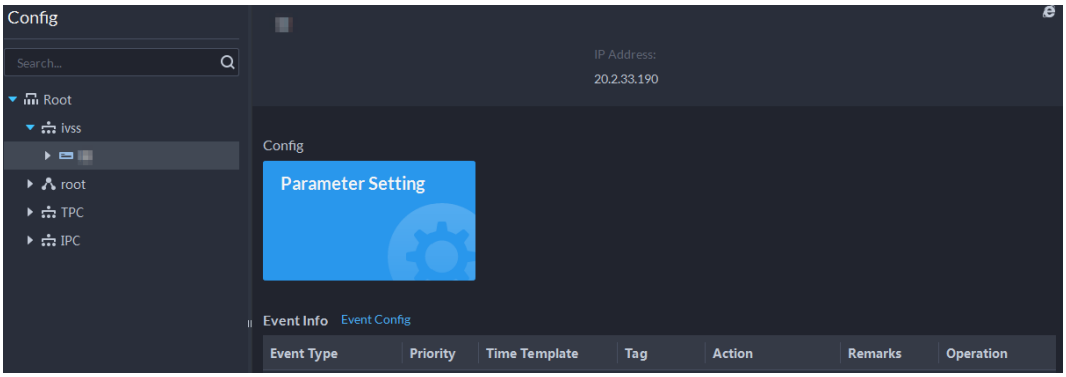
Set snapshot parameters, including snapshot type, picture size, picture quality, and snapshot speed.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

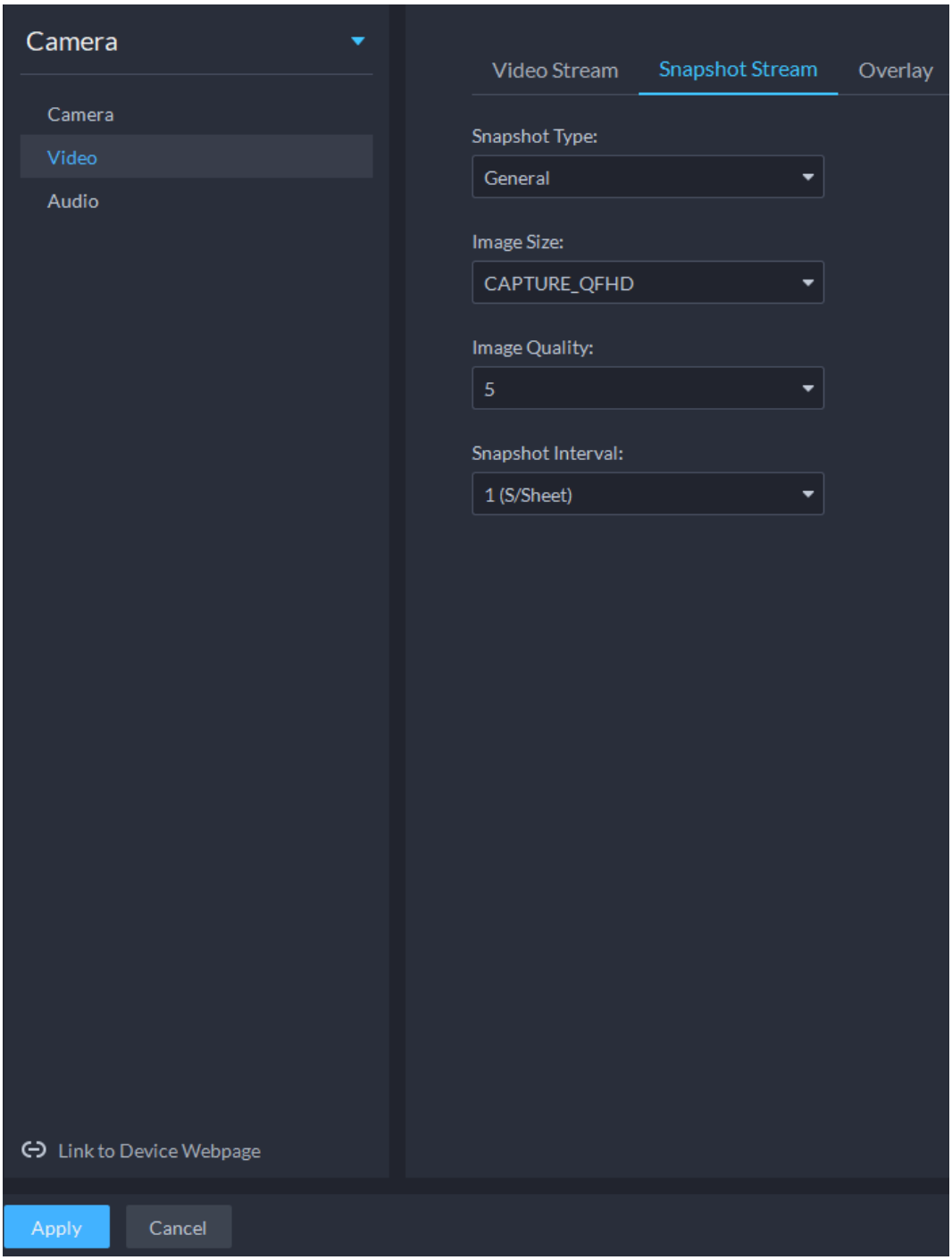
Step 3 Select a device, and then click **Device Config**.

Figure 3-44 Device configuration



Step 4 On the **Device Config** interface, select **Camera** > **Video** > **Snapshot Stream**.

Figure 3-45 Configure snapshot stream settings



Step 5 Set **Snapshot Stream**.

Table 3-12 Snapshot stream parameters

Parameter	Description
Snapshot Type	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 enabled.
Image Size	Same as the resolution in Main Stream.

Parameter	Description
Image Quality	Sets up image quality. It is divided into six grades: Best, Better, Good, Bad, Worse and Worst.
Snapshot Interval	Sets up the frequency of snapshots. Select Custom to manually set up the frequency of snapshots.
Link to Device Webpage	Go to the web interface of the device.

Step 6 Click **OK**.

3.2.8.2.3 Overlay

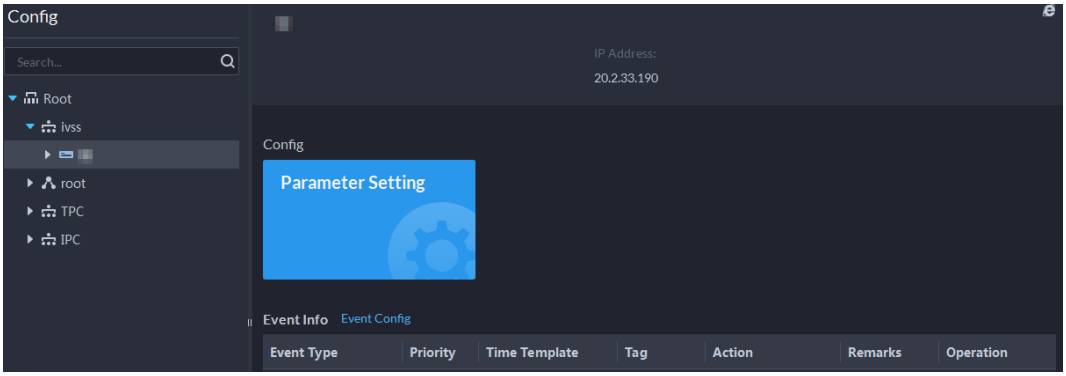
Set video overlay parameters, including tampering, privacy mask, channel title, period title, geographic position, OSD, font, and picture overlay.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a device, and then click **Device Config**.

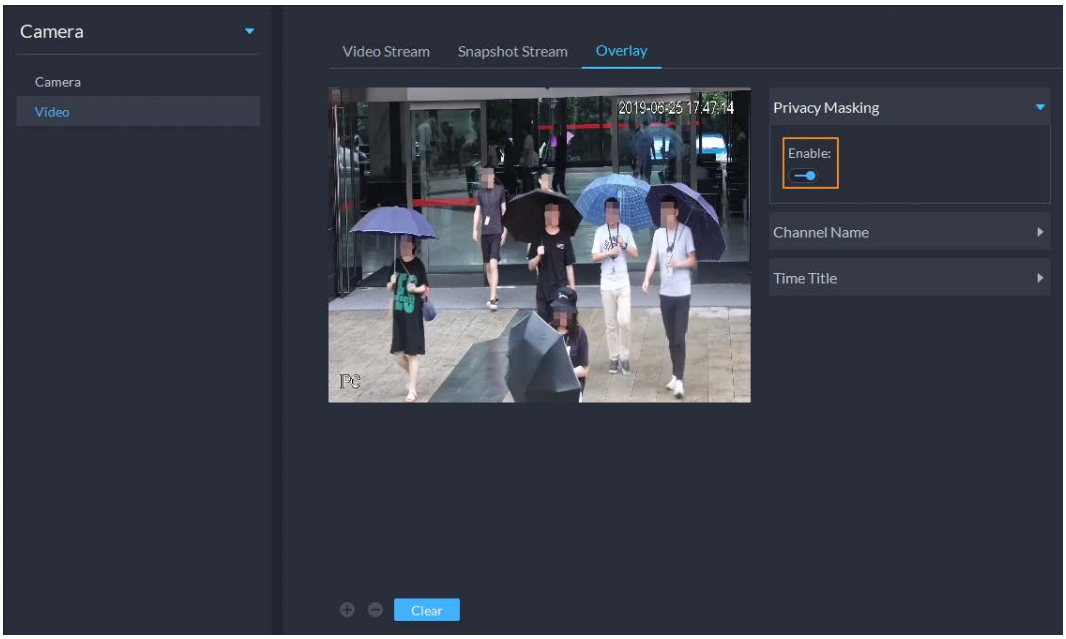
Figure 3-46 Device configuration



Step 4 On the **Device Config** interface, select **Camera** > **Video** > **Overlay**.

Step 5 Set privacy mask.

Figure 3-47 Overlay

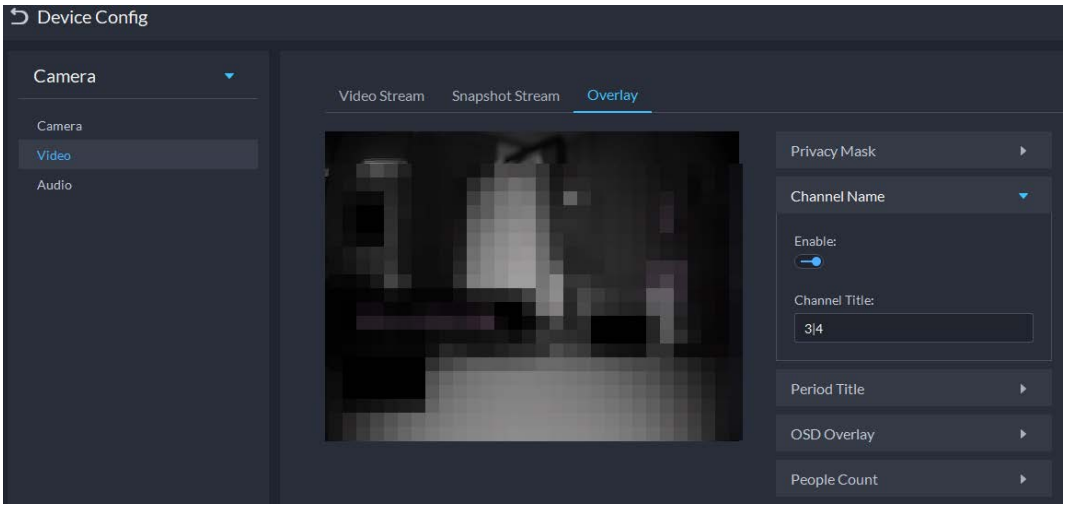


1) Click the **Privacy Mask** tab.
2) Click  to enable the function.
3) Click  to adjust the size and position of the area frame. You can add 4 area frames at most.

Step 6 (Optional) Set the channel name to display on the video.

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

Figure 3-48 Set channel name

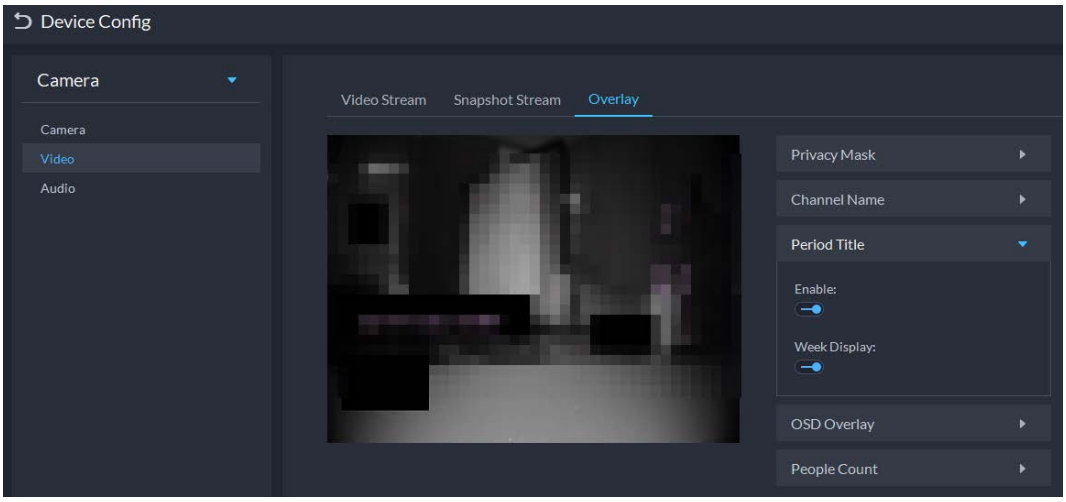


2) Click  to enable the function.
3) Adjust the size and position of the name frame.

Step 7 (Optional) Set the period title to display on the video.

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

Figure 3-49 Set period title



2) Click  to enable the function.

3) (Optional) Select **Week Display** so that the week information displays in video images.

4) Adjust the size and position of the frame.

Step 8 Click **OK**.

3.2.8.3 Audio

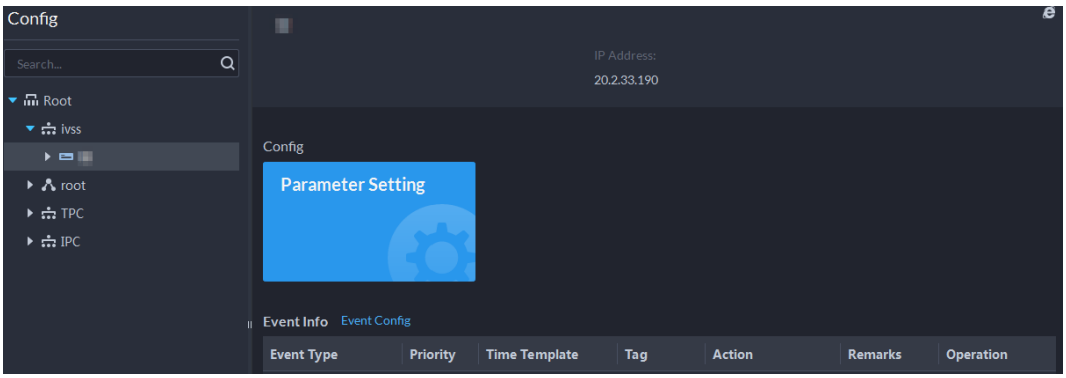
Set audio parameters such as encoding mode, sampling frequency, audio input type, and noise filtering.

Step 1 Log in to the DSS Client. On the **Home** interface, click  , and then in the **Basic Config** section, select **Device**.

Step 2 Click  .

Step 3 Select a device, and then click **Device Config**.

Figure 3-50 Device configuration



Step 4 On the **Device Config** interface, select **Camera** > **Audio**.

Step 5 Set parameters.

Figure 3-51 Configure audio settings

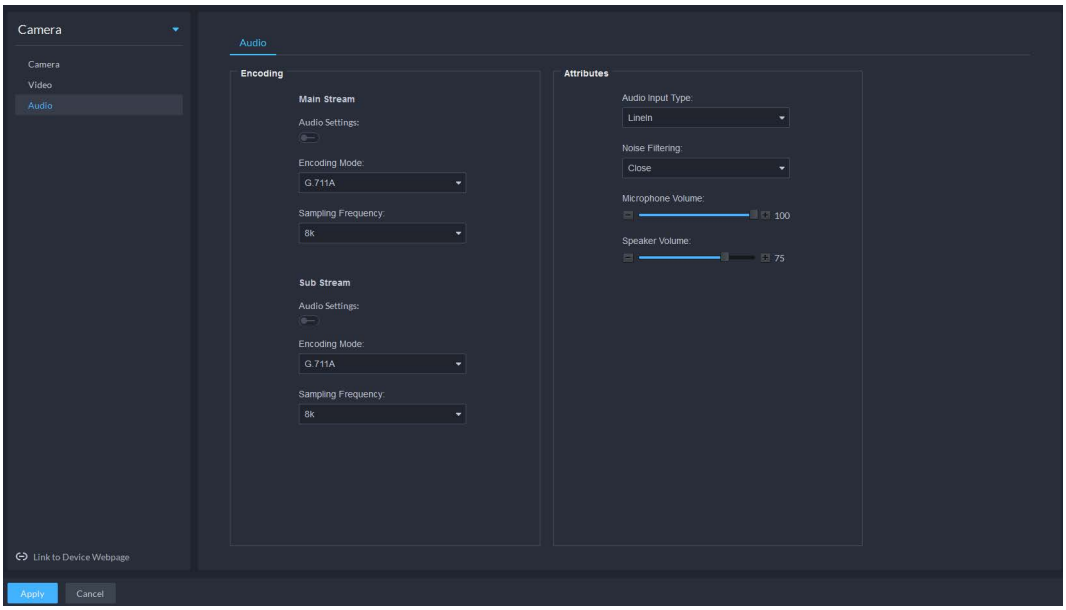


Table 3-13 Audio parameters

Parameter	Description
Audio Settings	Audio settings can be enabled when video has been enabled. After disabling **Audio Settings** 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.
Encoding Mode	The encoding modes of audios include G.711A, G.711Mu, AAC, PCM, and G.726. The preset audio encode mode applies to audio 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 6 Click **Apply**.

3.2.9 Configuring Intelligent Analysis

See requirements as follows when deploying devices:

- The total target ratio does not exceed 10% of the screen.
- The size of the target in the picture is not less than 10 pixels× 10 pixels, the target size of the

abandoned object is not less than 15 pixels× 15 pixels (CIF image); the target height and width is not more than 1/3 of the picture height and the recommended target height is 10% of the picture height.

- The difference between the brightness value of the target and the background is not less than 10 gray levels.
- At least ensure that the target appears continuously for more than 2 seconds in the field of view, the moving distance exceeds the target's own width, and is not less than 15 pixels (CIF image).
- Minimize the complexity of the monitoring and analysis scenario when conditions permit. It is not recommended to use the smart analysis function in scenarios with dense targets and frequent light changes.
- Avoid glass, ground and water surface reflection; avoid branches, shadows and mosquito interference; avoid backlight scenes and direct light.

3.2.9.1 Enabling IVS Smart Plan

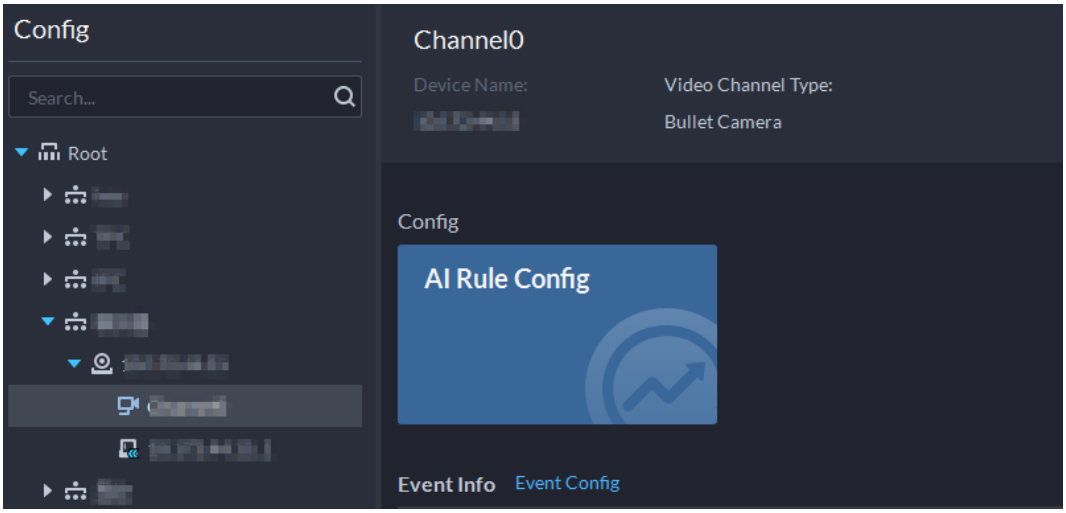
Enable IVS functions.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a channel, and then click **AI Rule Config**.

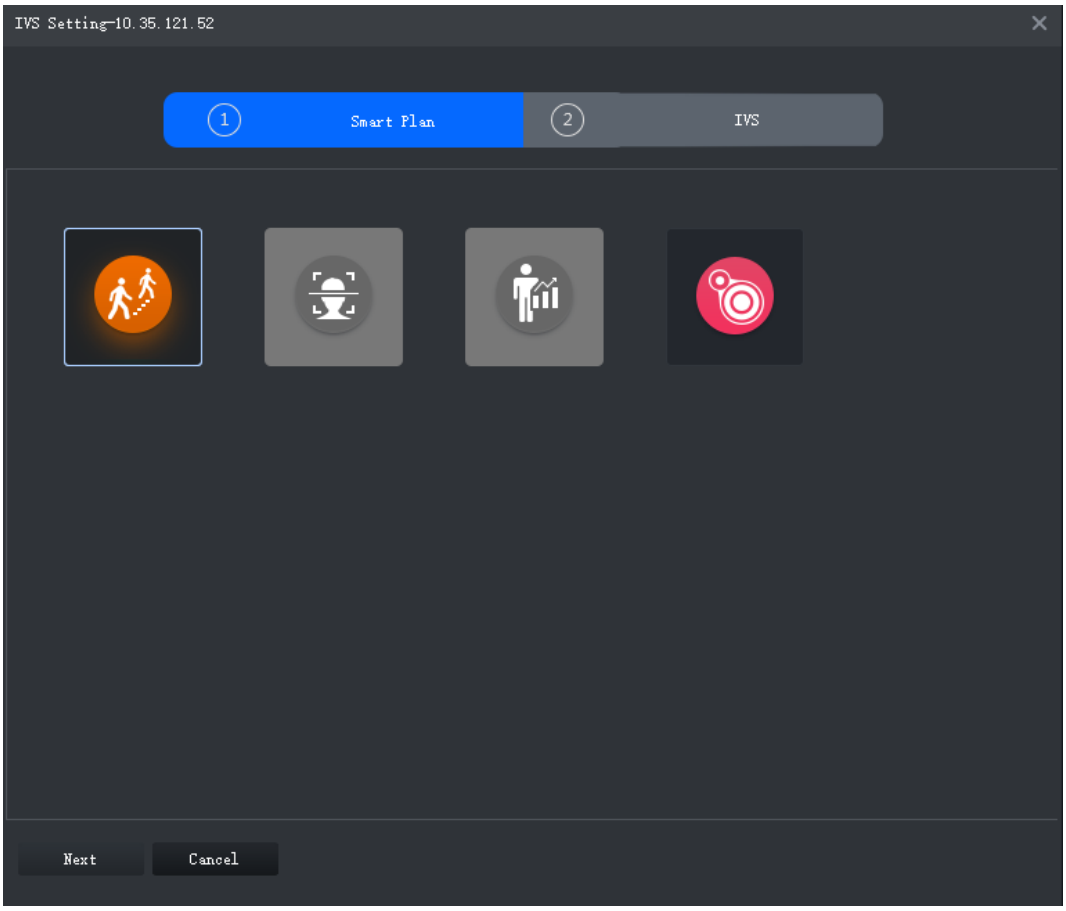
Figure 3-52 Go to AI rule config interface



Step 4 Click on the smart plan interface to enable IVS smart plan.

When the icon is displayed in the white frame, it means the smart plan is selected. If another smart plan has been selected, click that smart plan icon to deselect it and then click to select IVS.

Figure 3-53 IVS smart plan



Step 5 Click **Next** to go to the **IVS** interface.

3.2.9.2 Calibrating Depth of Field

After setting one horizontal gauge and three vertical gauges and the actual geographical distances of each gauge, the system can estimate the internal parameters (internal geometrical features and optical properties) and external parameters (the network camera position and direction on the actual environment) of network camera, so as to work out the relation between the two-dimensional image and three dimensional objects in the current surveillance environment.

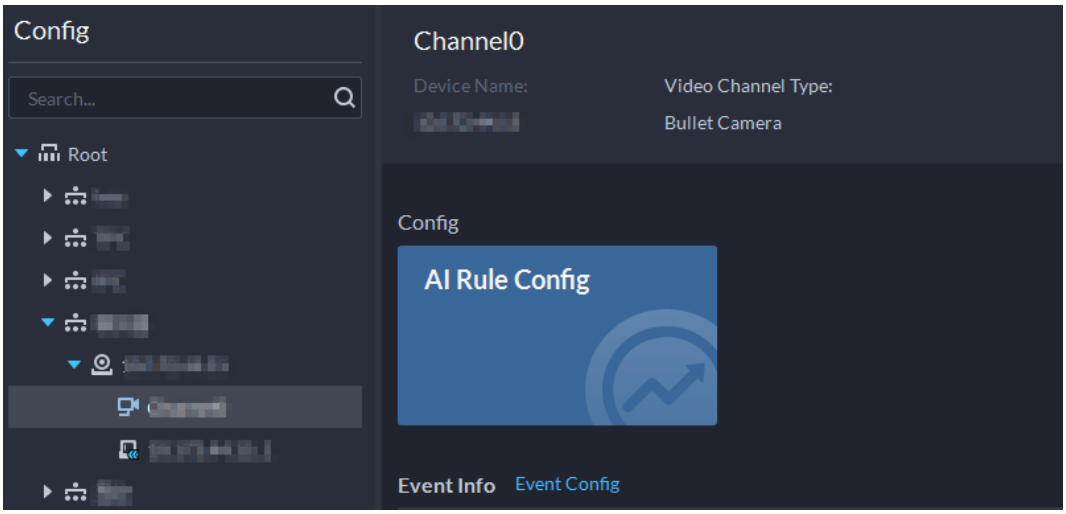
Calibrate depth of field when configuring fast moving detection. If you do not use face moving detection, skip this section.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a channel, and then click **AI Rule Config**.

Figure 3-54 Go to AI rule config interface



Step 4 After selecting the IVS smart plan on the **Smart Plan** interface, click **Next**.

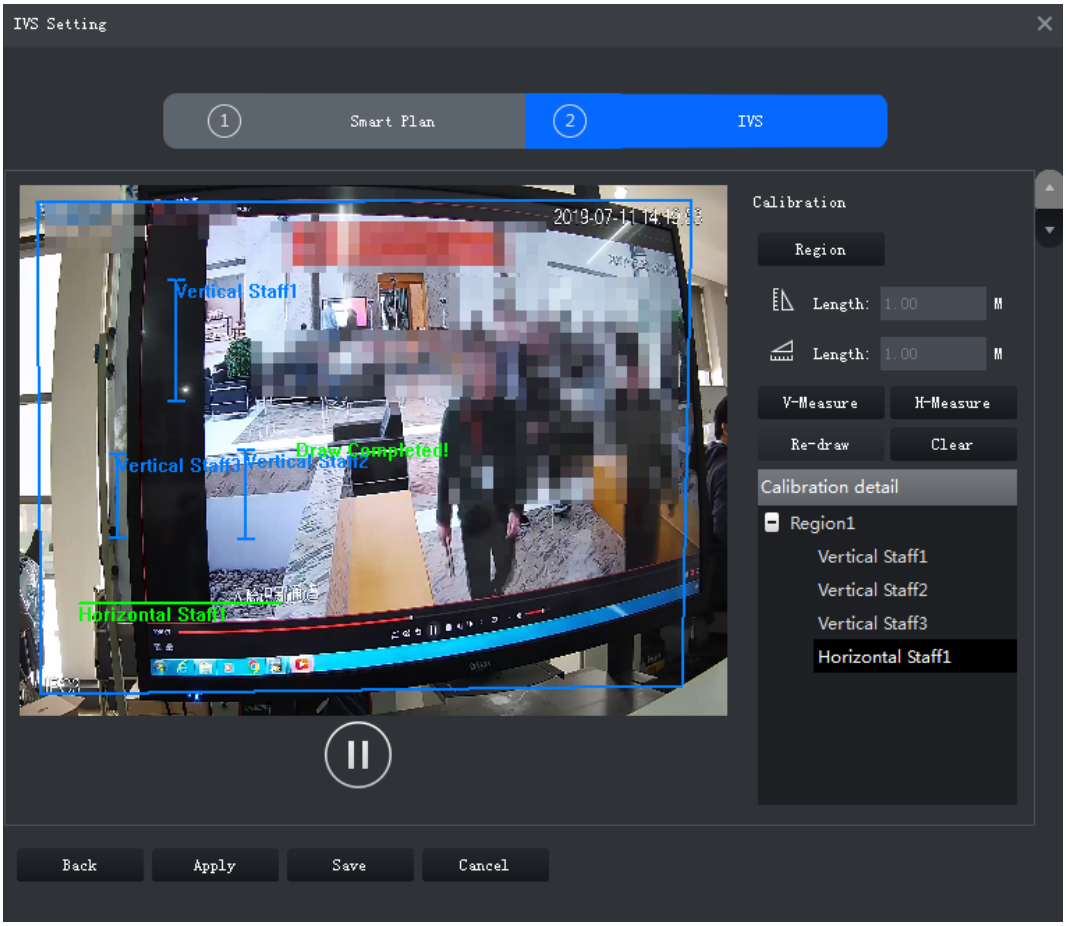
Step 5 Click ▾ to go to the calibration interface.

Step 6 Click **Region** and draw calibration zone on the video. Right-click to finish.

Step 7 Set length value of the vertical gauge. Click and then draw a vertical gauge in the calibration area. Click to finish.

Draw three other vertical gauges in the calibration area.

Figure 3-55 Calibrating depth of field



Step 8 Set length value of horizontal gauge. Click and then draw a horizontal gauge in the calibration area. Click to finish.

- To modify the gauge, you can select it and click **Re-draw**. You can also select the

calibration and click **Re-draw** to draw new calibration areas and gauges.

- To delete a gauge, select it and click **Delete**. To delete a calibration area and the gauges in it, select the area and click **Delete**.

Step 9 Click **Apply**.

Step 10 (Optional) Vertical/horizontal measuring

Do the following steps to measure distance.

- Click **V-Measure** and draw vertical lines in the calibration area. The measuring result will be displayed.
- Click **H-Measure** and draw horizontal lines in the calibration area. The measuring result will be displayed.

3.2.9.3 Configuring Detection Region

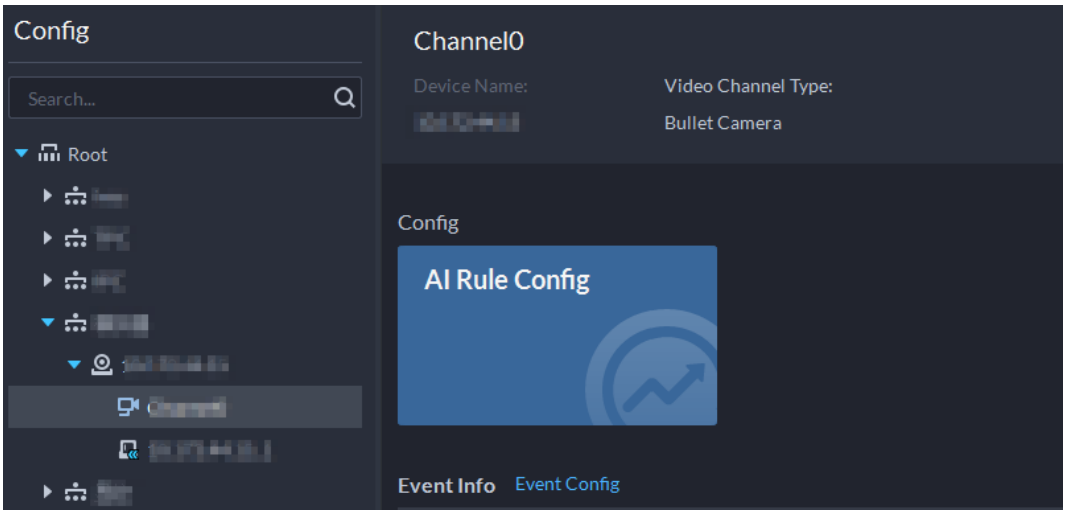
Configure the detection zone of IVS.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select a channel, and then click **AI Rule Config**.

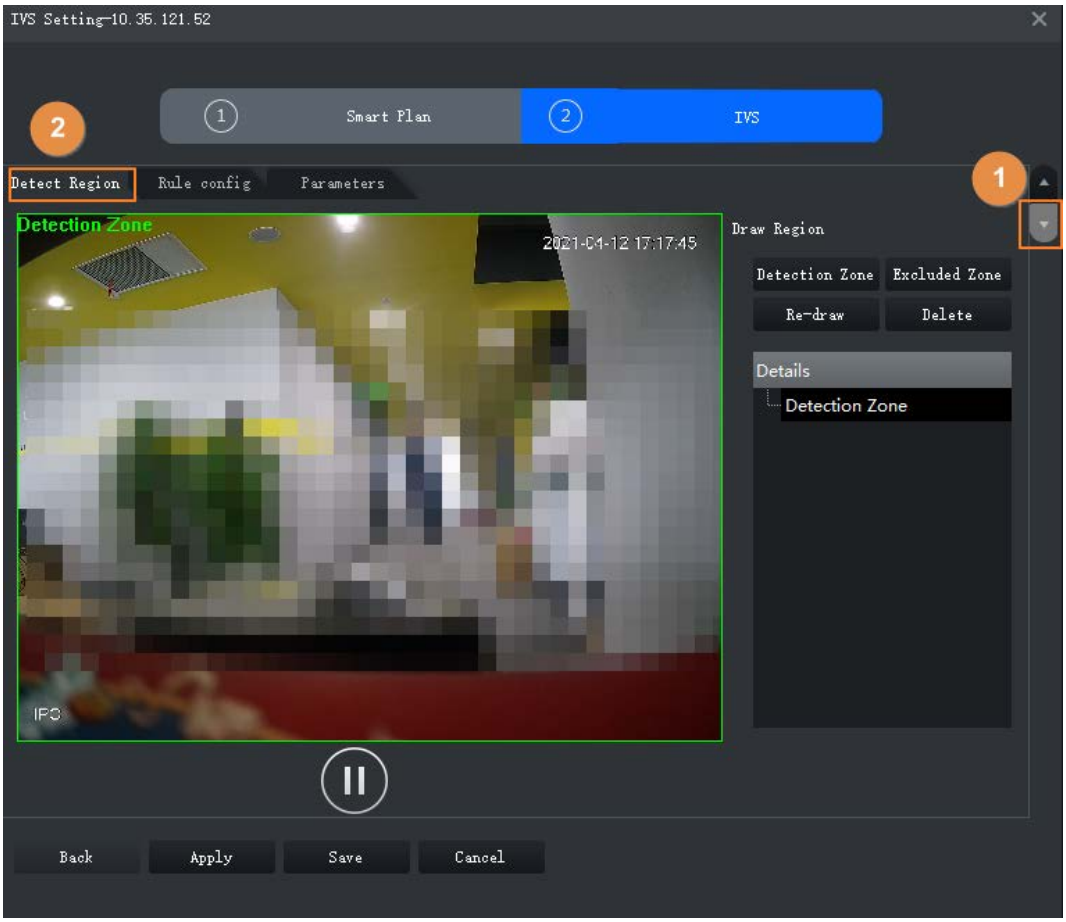
Figure 3-56 Go to AI rule config interface



Step 4 After selecting the IVS smart plan in the **Smart Plan** interface, click **Next**.

Step 5 Click .

Figure 3-57 Detection region



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

Step 7 Click **Excluded Zone**, and then draw the frame of the zone on the video and right-click to finish.

3.2.9.4 Configuring IVS Rule

Configure IVS detections such as fence-crossing, tripwire, intrusion, abandoned object, loitering detection, fast-moving, crowd gathering, missing object and parking detection.

Functions	Description	Applicable Scenarios
Fence-crossing	An alarm is triggered when a target is crossing the pre-defined fence.	Roads, airports and other areas with restricted zones.
Tripwire	An alarm is triggered when a target is crossing the pre-defined tripwire.	Restricted zone borders
Intrusion	An alarm is triggered when a target is entering, leaving, or appearing in the detection area.	
Abandoned Object	An alarm is triggered when an object is left in the detection area and the existence time is longer than the threshold.	Places where the target is sparse and has no obvious and frequent light changes. The detection area is required

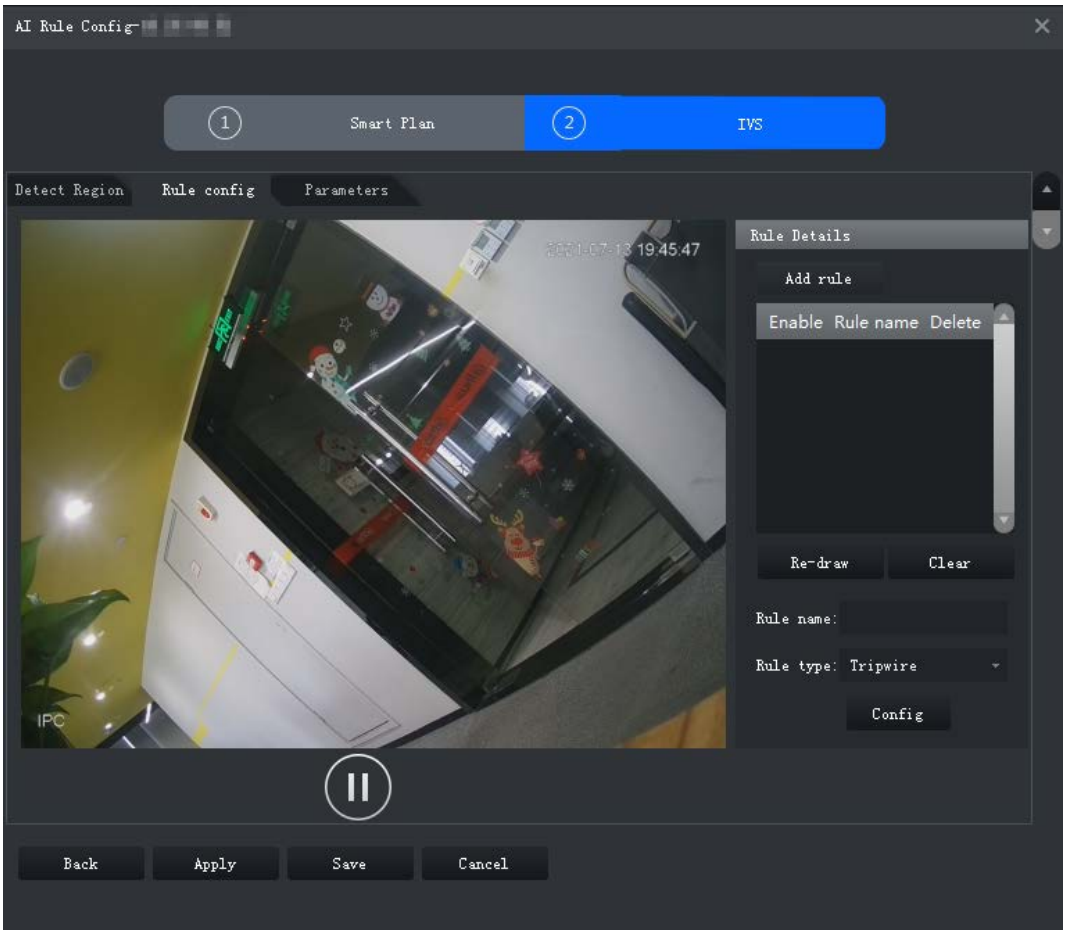
Functions	Description	Applicable Scenarios
Missing Object	An alarm is triggered when an object is removed from the detection area and not put back after the pre-defined time period.	to be as simple as possible.
Fast-moving	An alarm is triggered when the moving speed of a target exceeds the threshold.	Places with low target density and no obvious blocking. The camera should be installed right above the monitoring area, and the light direction is as vertical as possible with the direction of motion.
Parking Detection	An alarm is triggered when a target remains still within a time period longer than the pre-defined time duration.	Road monitoring and traffic management.
People Gathering	An alarm is triggered when people gathering is detected or people density is larger than the threshold.	Long or medium distance monitoring. For example, outdoor squares, government gates, and station entrances and exits.
Loitering	An alarm is triggered when a target keeps loitering in a time period longer than the threshold. Alarm will be triggered again if the target stays in the detection area after the first alarm.	Enterprise zones, halls and more.

3.2.9.4.1 Tripwire

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

Step 1 On the **AI Rule Config** interface, click **Rule config**.

Figure 3-58 Rule configuration interface



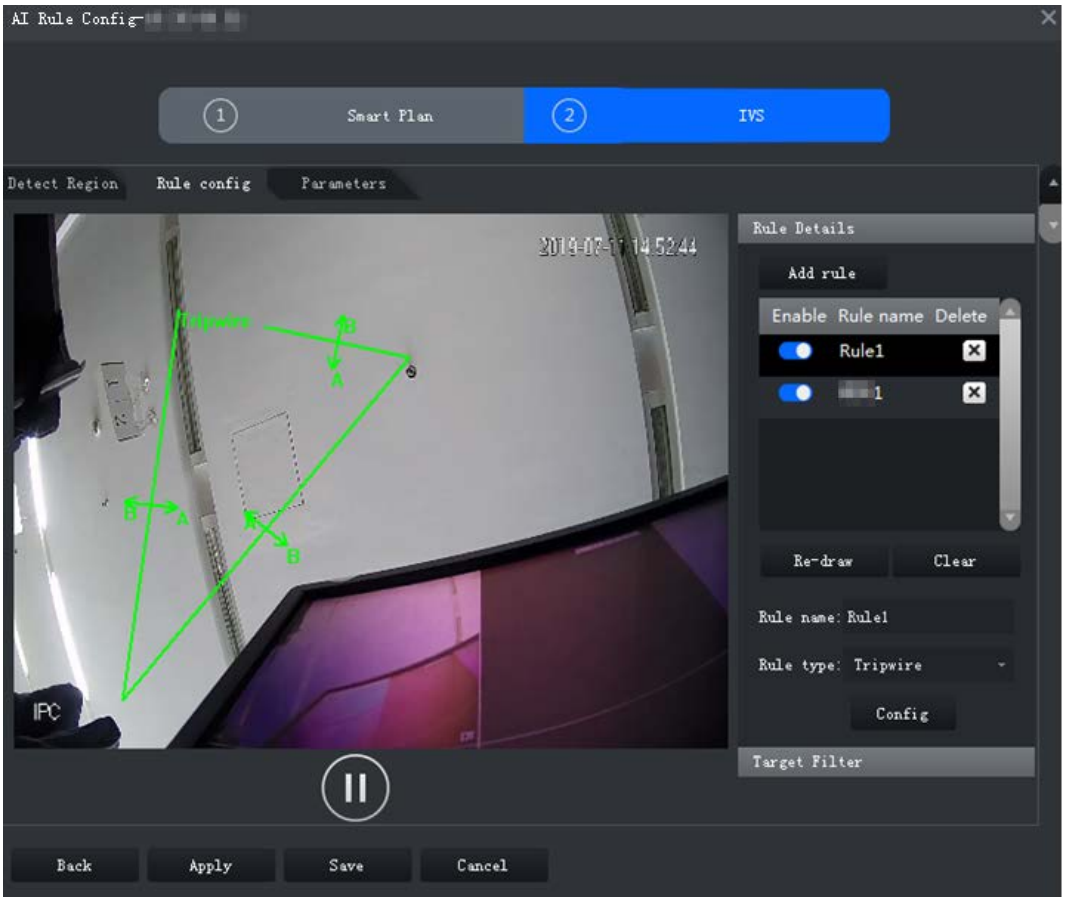
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

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

Step 4 Draw a line on the video and right-click to finish.

Figure 3-59 Tripwire



Step 5 Set parameters, arming schedule and alarm linkage.

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

Figure 3-60 Set parameters

Table 3-14 Parameters

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

2) Click **Arming schedule**, select day and hours and then set the start time and end time.

The default arming schedule is 24 hours each day.

Figure 3-61 Arming schedule

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

Figure 3-62 Alarm linkage

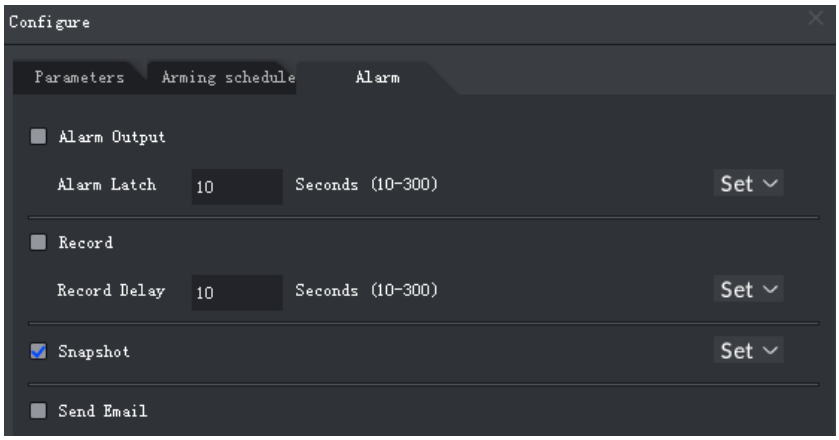


Table 3-15 Parameters

Parameter	Description	
Alarm Output	Connect alarm output devices to the alarm output ports. When an alarm is triggered, the system will send the alarm to the alarm output device.	Click **Set** next to **Alarm Latch** and select an alarm output channel.
Alarm Latch	The alarm output action will delay stopping after the alarm event ends.	
Record	When an alarm happens, it will trigger video recording immediately. It requires the device to have recording schedules already. See device manual for detailed instruction.	Click **Set** next to **Record** and select an alarm output channel.
Record Delay	After the alarm event ends, the video recording continues for a while.	
Snapshot	The system will take snapshots automatically when an alarm happens. It requires the device to have snapshot schedules already. See device manual for detailed instruction.	Click **Set** next to **Snapshot** to select the snapshot channel.
Send Email	The system will send an email to the related mail address when an alarm happens. It requires the device to have email configured already. See device manual for detailed instruction.	–

4) Click **Save**.

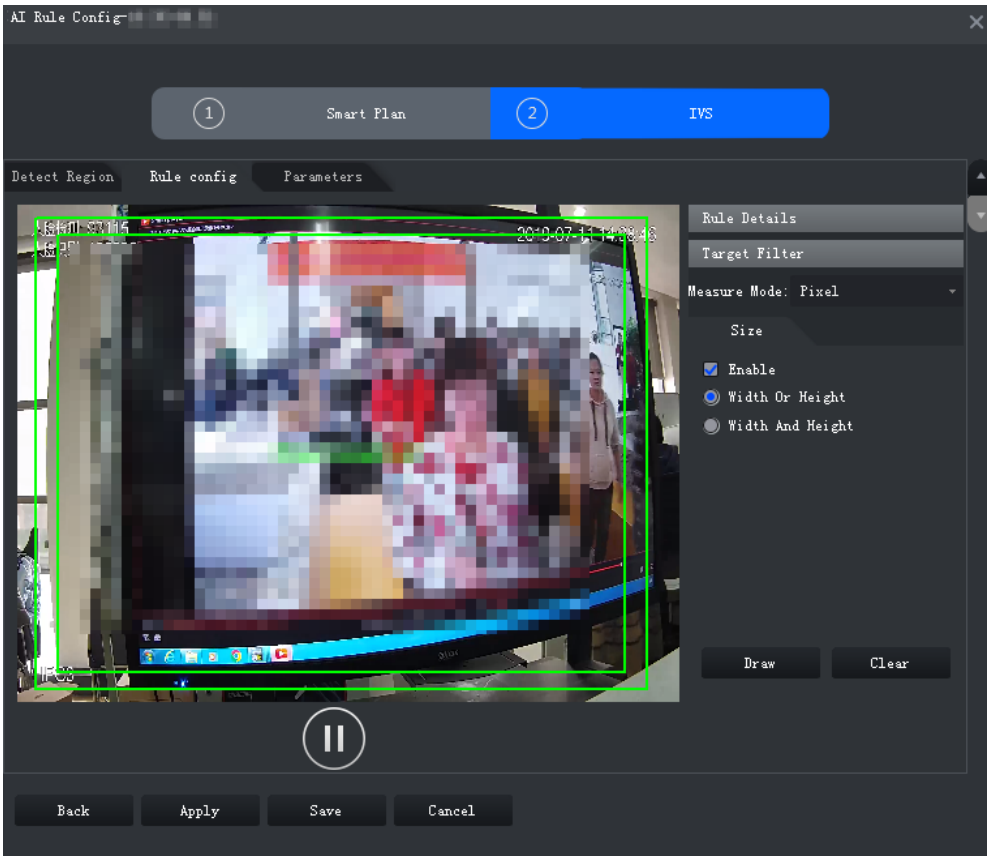
Step 6 Draw target-filtering frame.

The filtering frame is used to filter targets that are too big or too small. When the target size is within the preset value, it can trigger alarm.

1) Click **Target Filter**.

2) Select **Enable**.
3) Select a filtering method, **Width or Height** or **Width and Height**. Select filtering frame and drag the frame corners to adjust the size.

Figure 3-63 Target filtering



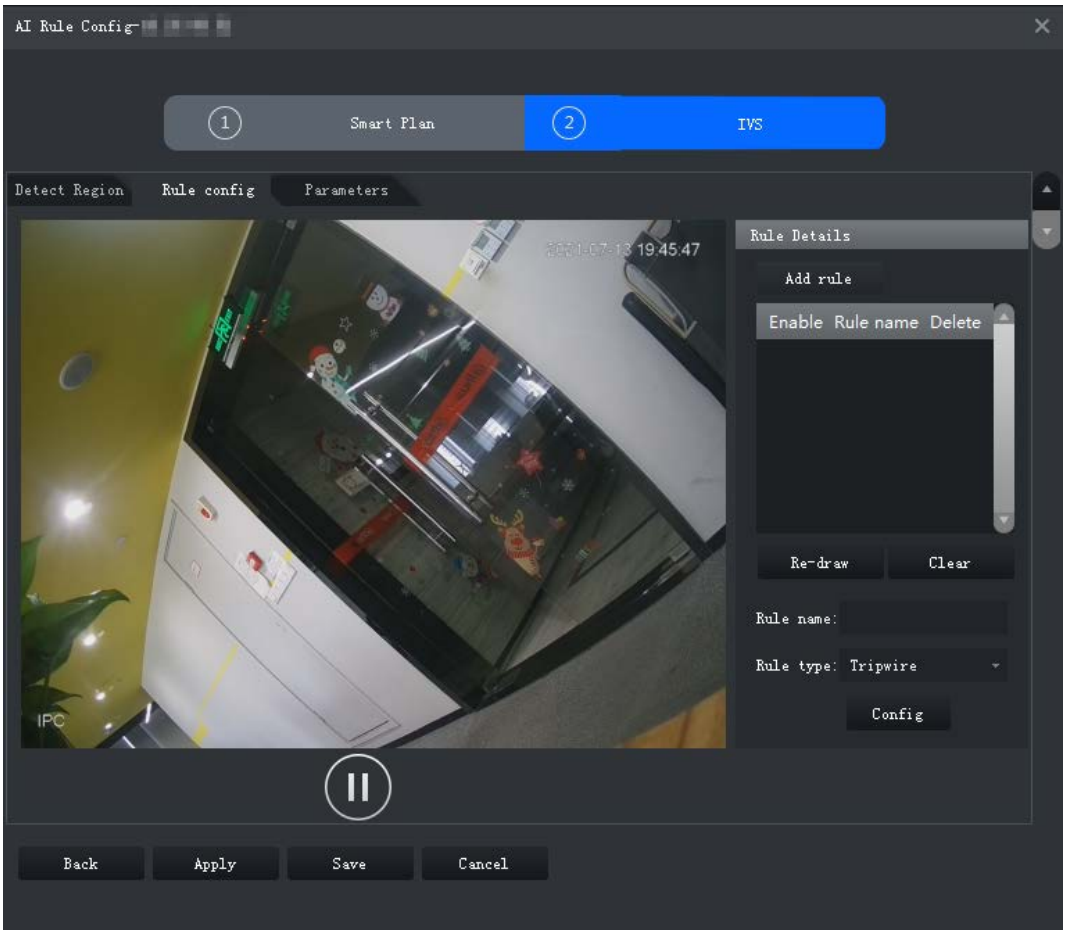
Step 7 Click **Apply**.

3.2.9.4.2 Intrusion

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

Step 1 On the **AI Rule Config** interface, click **Rule config**.

Figure 3-64 Rule configuration interface



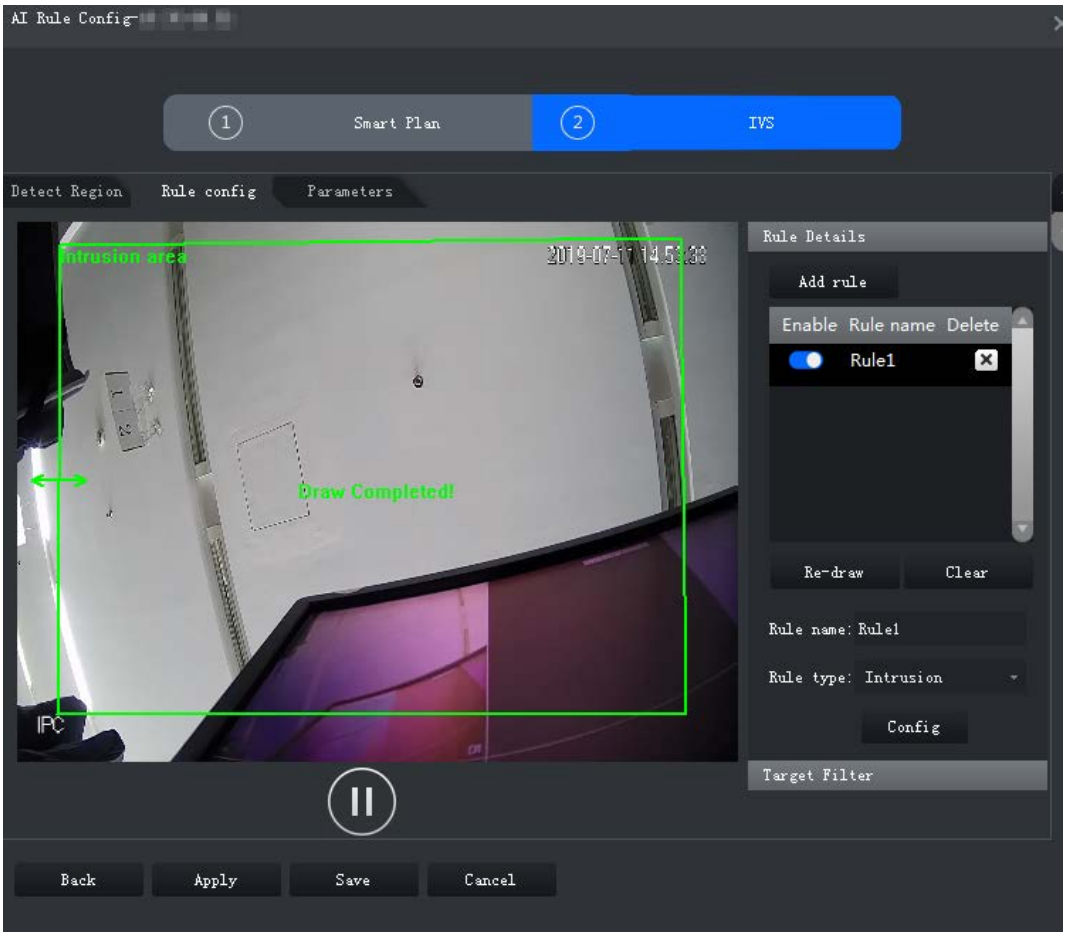
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

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

Step 4 Draw a detection zone on the video and right-click to finish.

Figure 3-65 Intrusion



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.2.9.4.1 Tripwire".

Figure 3-66 Set parameters

Table 3-16 Parameters

Parameter	Description
Object Type	Only human or vehicle can trigger alarm.
Action List	Appear and cross

Parameter	Description
Direction	When **Cross** in **Action List** is selected, **Direction** setting will be effective. Direction includes entering zone, leaving zone and two-way.

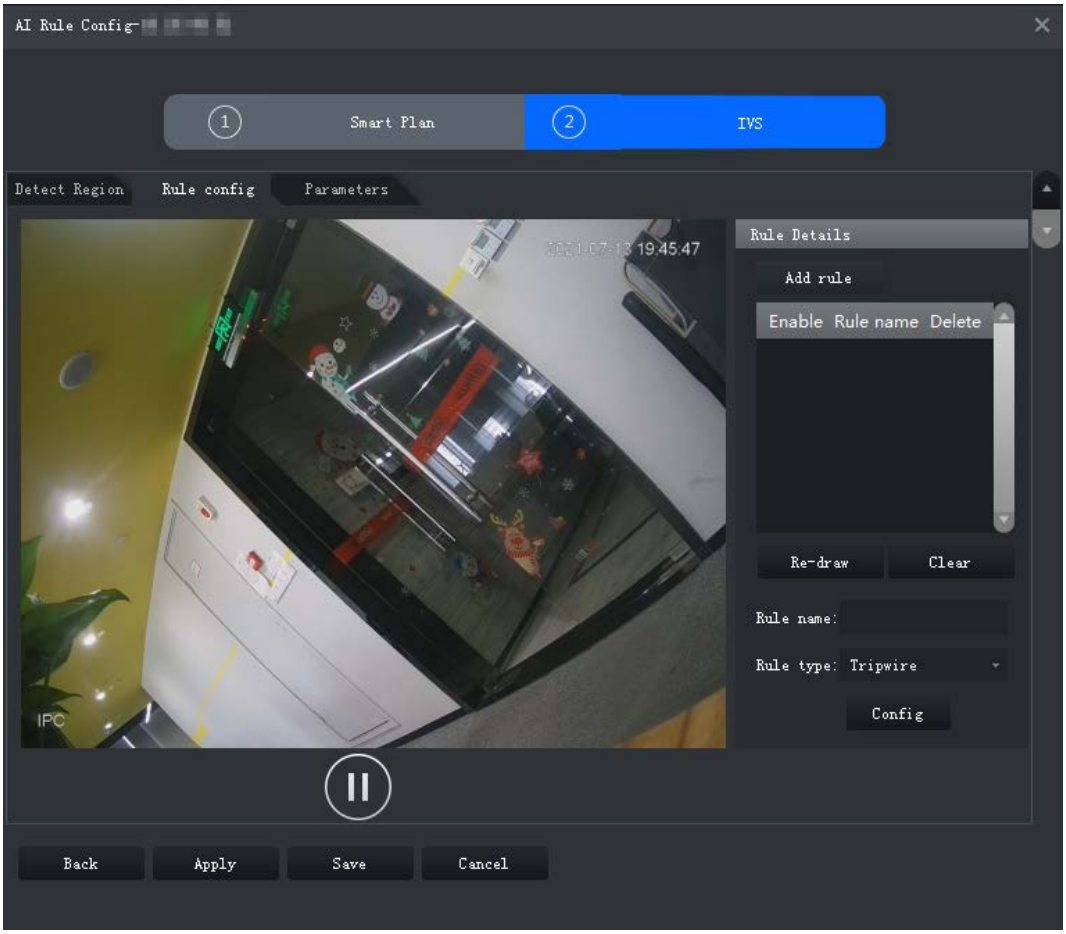
Step 6 Click **Apply**.

3.2.9.4.3 Abandoned Object

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

Step 1 On the **AI Rule Config** interface, click **Rule config**.

Figure 3-67 Rule configuration interface



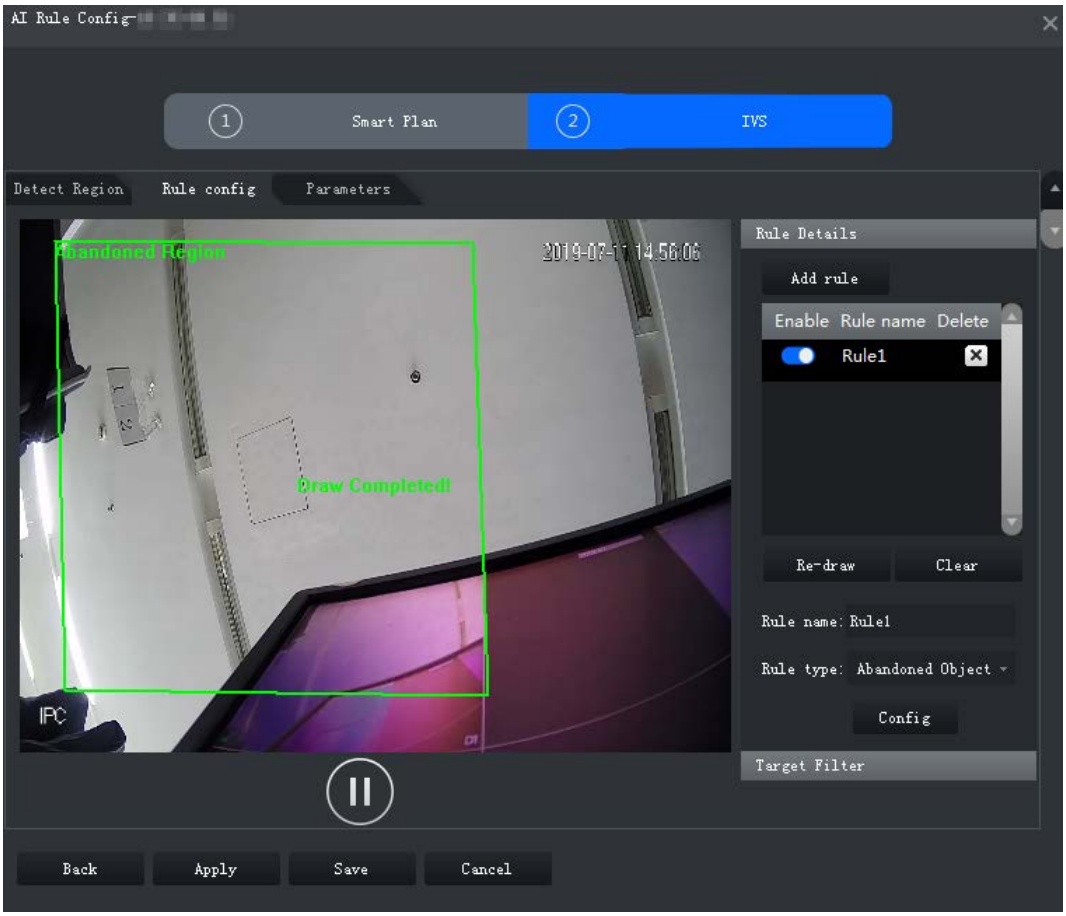
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

1) Enable rule. indicates the rule is enabled.
2) Modify the rule name.
3) Select **Abandoned Object** in the drop-down list of **Rule type**.

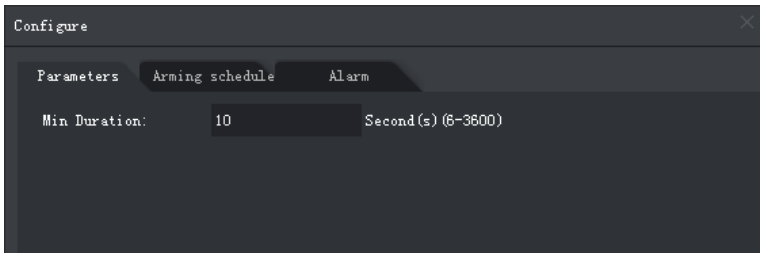
Step 4 Draw a detection zone on the video and right-click to finish.

Figure 3-68 Abandoned Object



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.2.9.4.1 Tripwire".

Figure 3-69 Set parameters



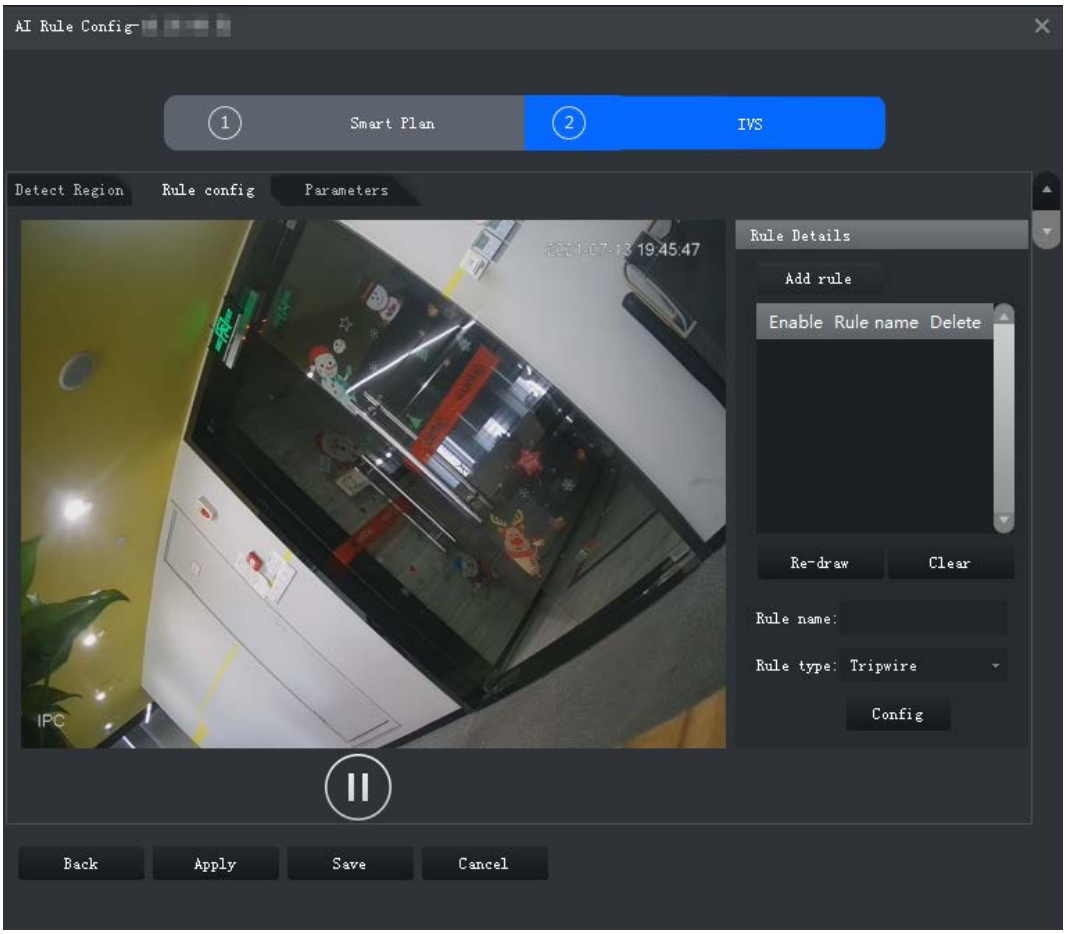
Step 6 Click **Apply**.

3.2.9.4.4 Fast-Moving

When a target appears and its moving speed is or exceeds the preset value for the preset time period, system will trigger an alarm.

Step 1 On the **AI Rule Config** interface, click **Rule config**.

Figure 3-70 Rule configuration interface



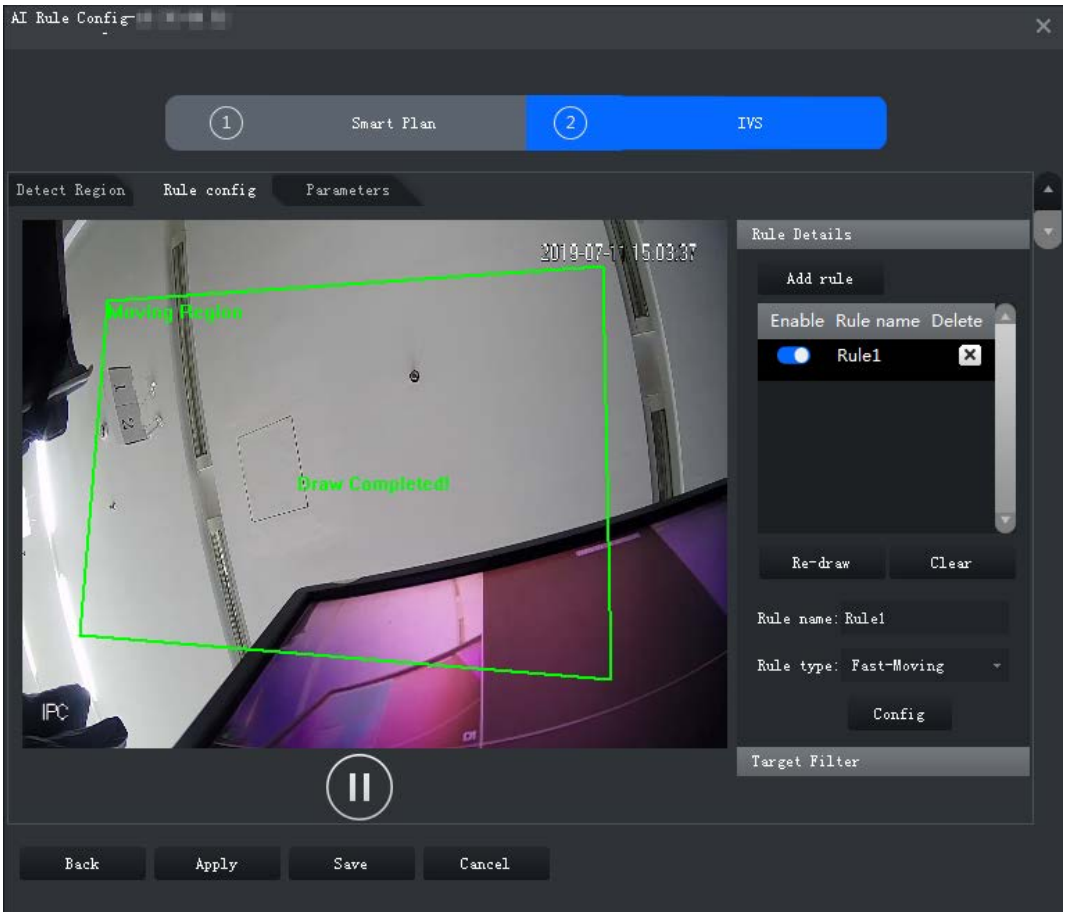
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

1) Enable rule. indicates the rule is enabled.
2) Modify the rule name.
3) Select **Fast-Moving** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish.

Figure 3-71 Fast-moving



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.2.9.4.1 Tripwire".

Figure 3-72 Set parameters

Table 3-17 Parameters

Parameter	Description
Object Type	Only human or vehicle can trigger alarm.
Min Duration	The minimum duration of fast-moving in the detection zone.
Sensitivity	Keep it default.

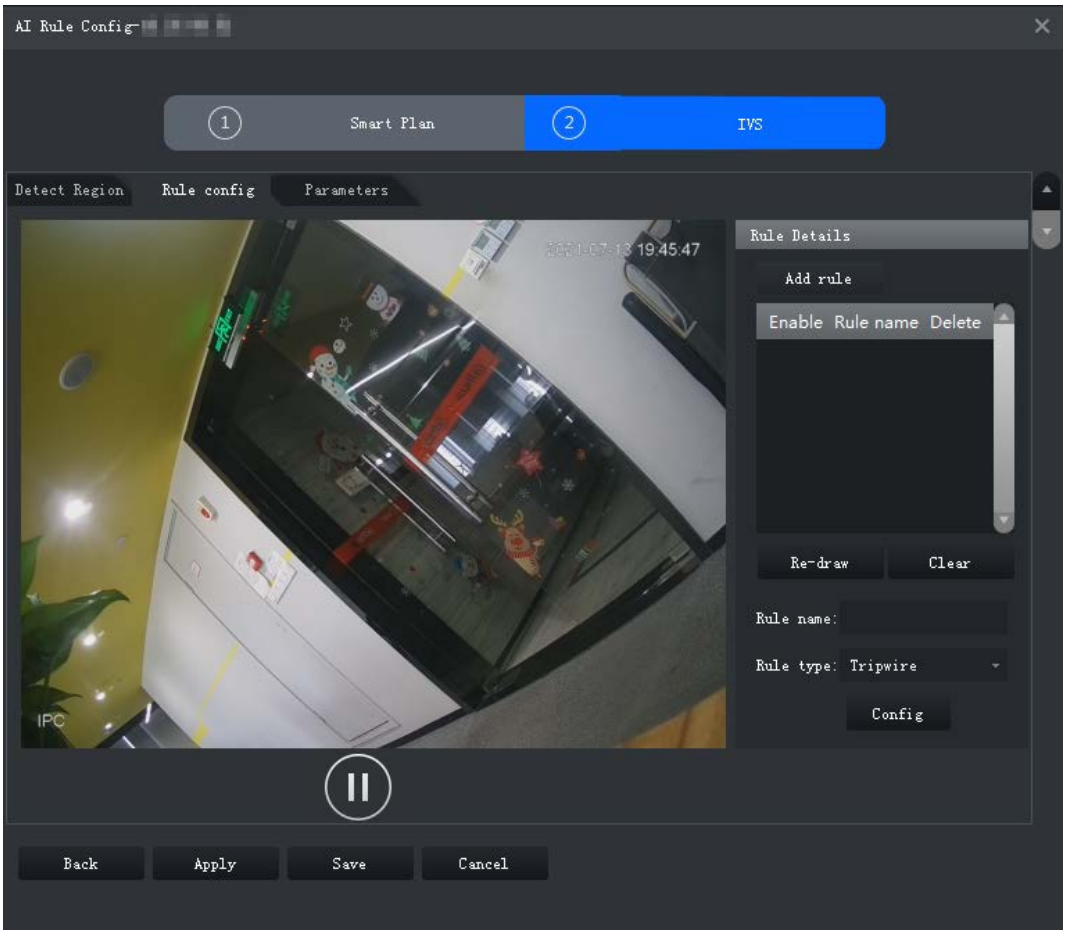
Step 6 Click **Apply**.

3.2.9.4.5 Parking Detection

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

Step 1 On the **AI Rule Config** interface, click **Rule config**.

Figure 3-73 Rule configuration interface



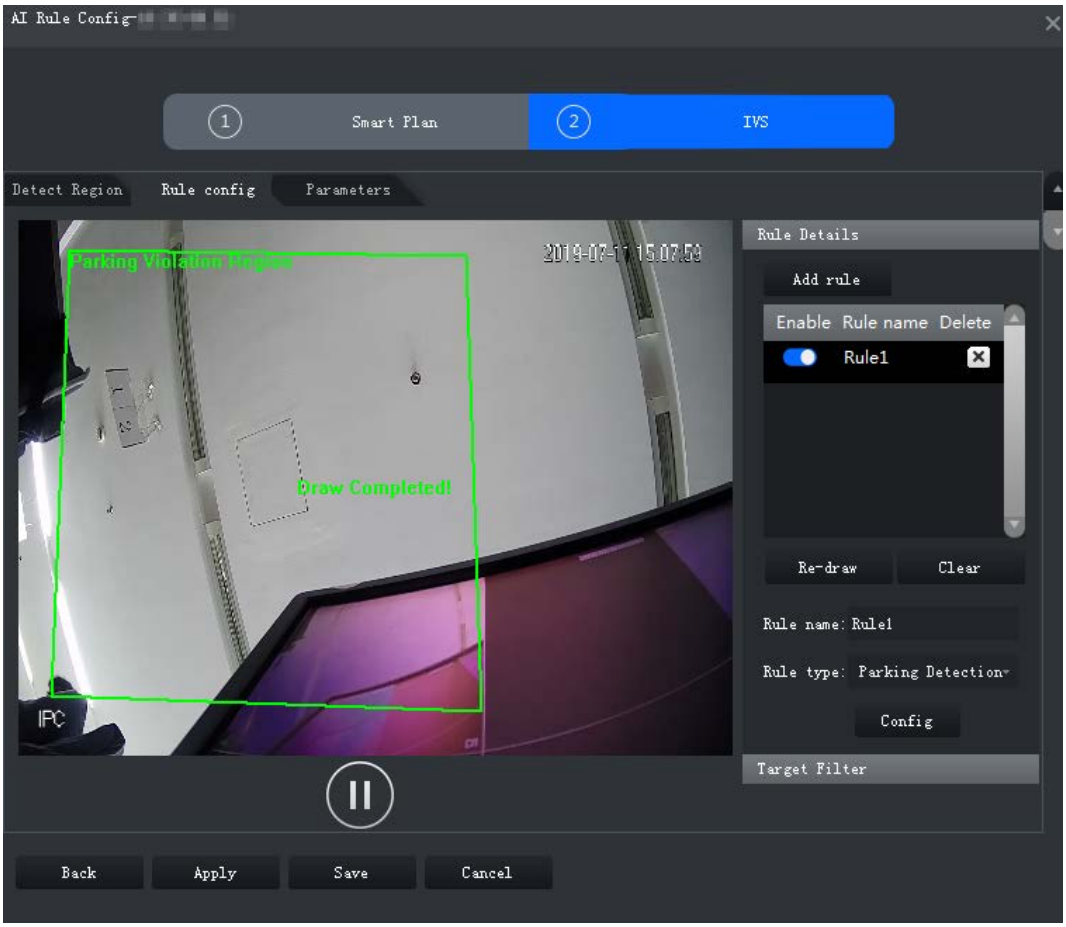
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

1) Enable rule. indicates the rule is enabled.
2) Modify the rule name.
3) Select **Parking Detection** in the drop-down list of **Rule type**.

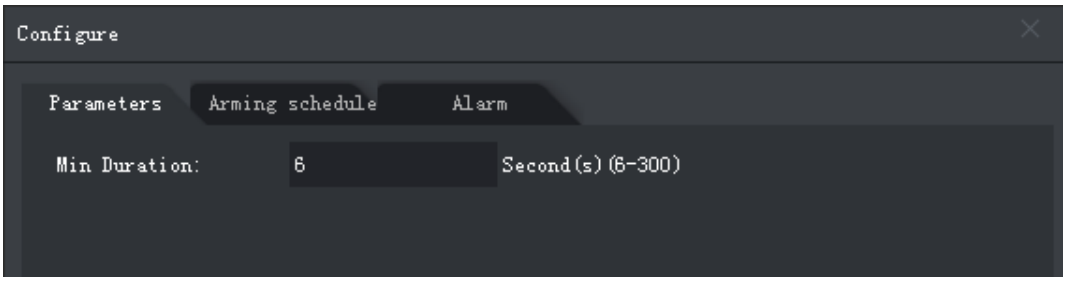
Step 4 Draw a detection zone on the video and right-click to finish.

Figure 3-74 Parking detection



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.2.9.4.1 Tripwire".

Figure 3-75 Set parameters



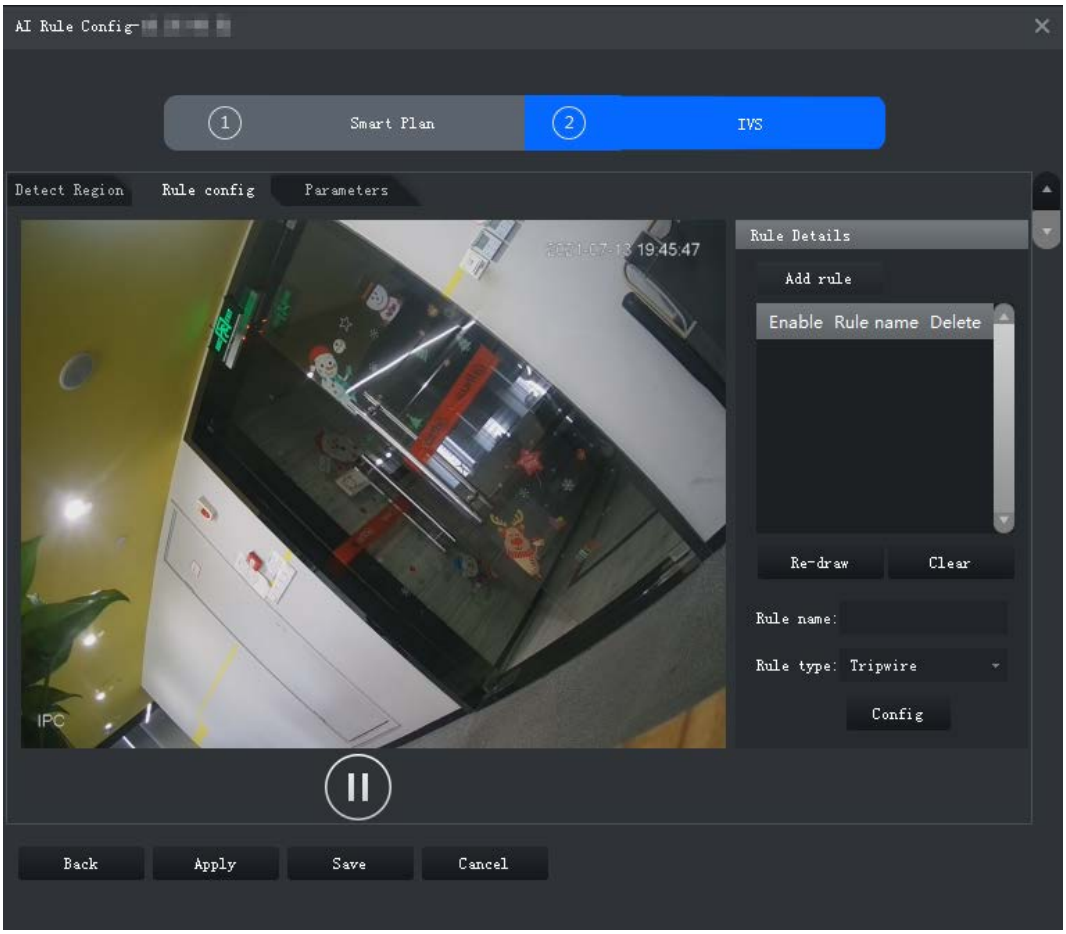
Step 6 Click **Apply**.

3.2.9.4.6 Crowd Gathering

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

Step 1 On the **AI Rule Config** interface, click **Rule config**.

Figure 3-76 Rule configuration interface



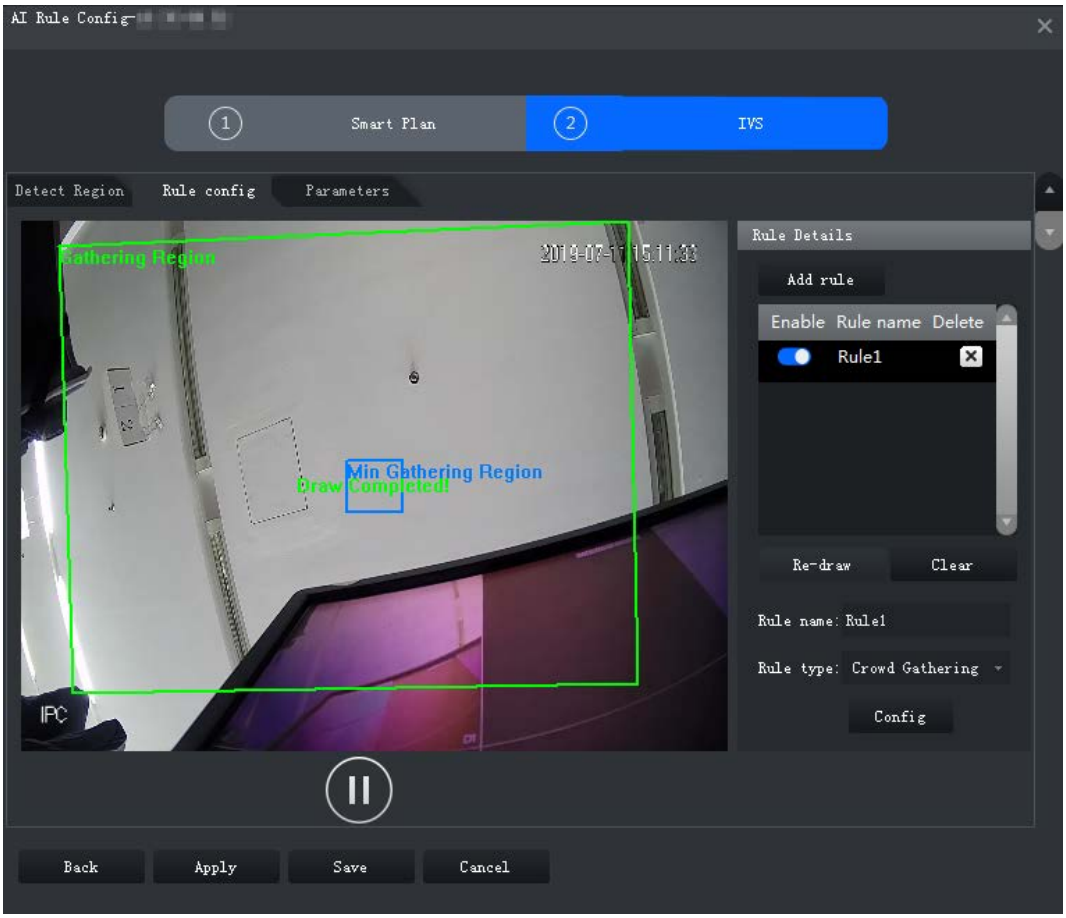
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

1) Enable rule. indicates the rule is enabled.
2) Modify the rule name.
3) Select **Crowd Gathering** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish. Click the **Min Gathering Region** and drag the zone corners to adjust the size.

Figure 3-77 Crowd gathering



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.2.9.4.1 Tripwire".

Figure 3-78 Set parameters

Table 3-18 Parameters

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

Step 6 Click **Apply**.

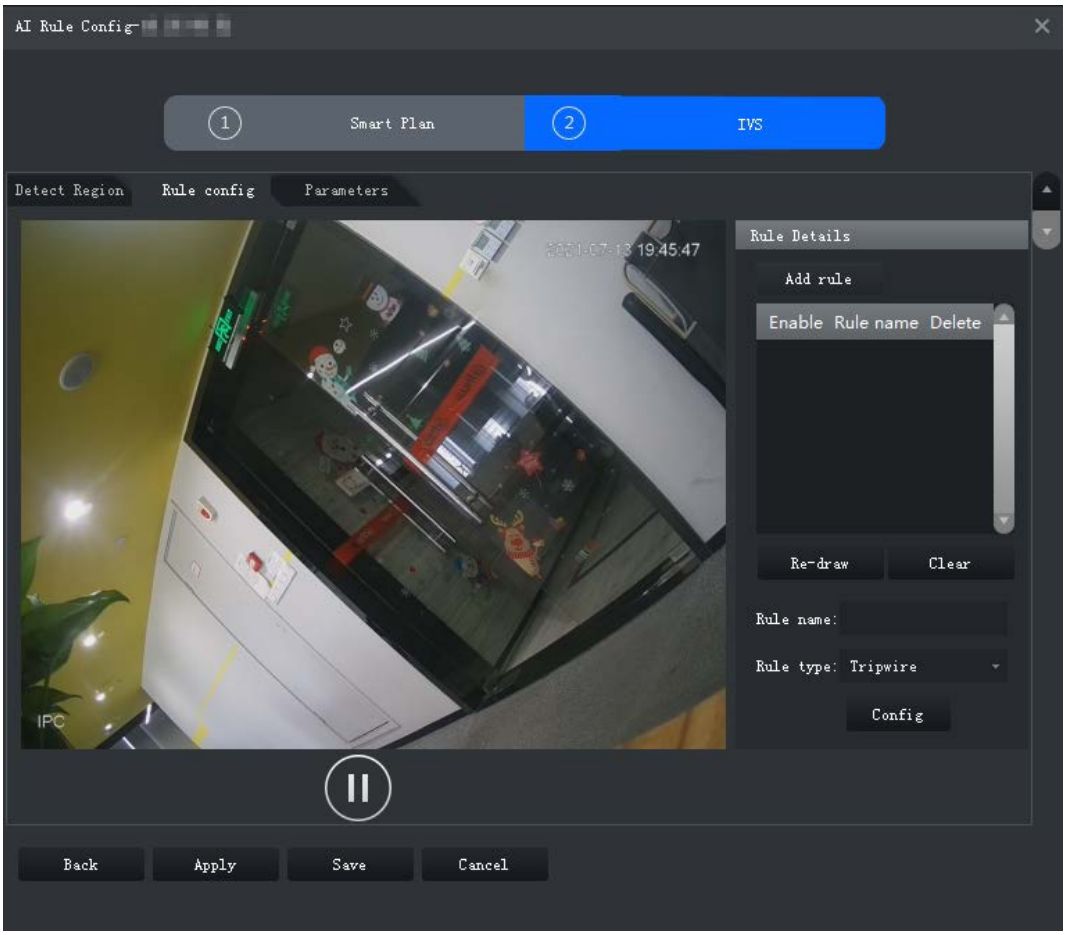
3.2.9.4.7 Missing Object

If an object has been moved out of the detection zone and not put back anymore for a time period,

system will trigger an alarm.

Step 1 On the **AI Rule Config** interface, click **Rule config**.

Figure 3-79 Rule configuration interface



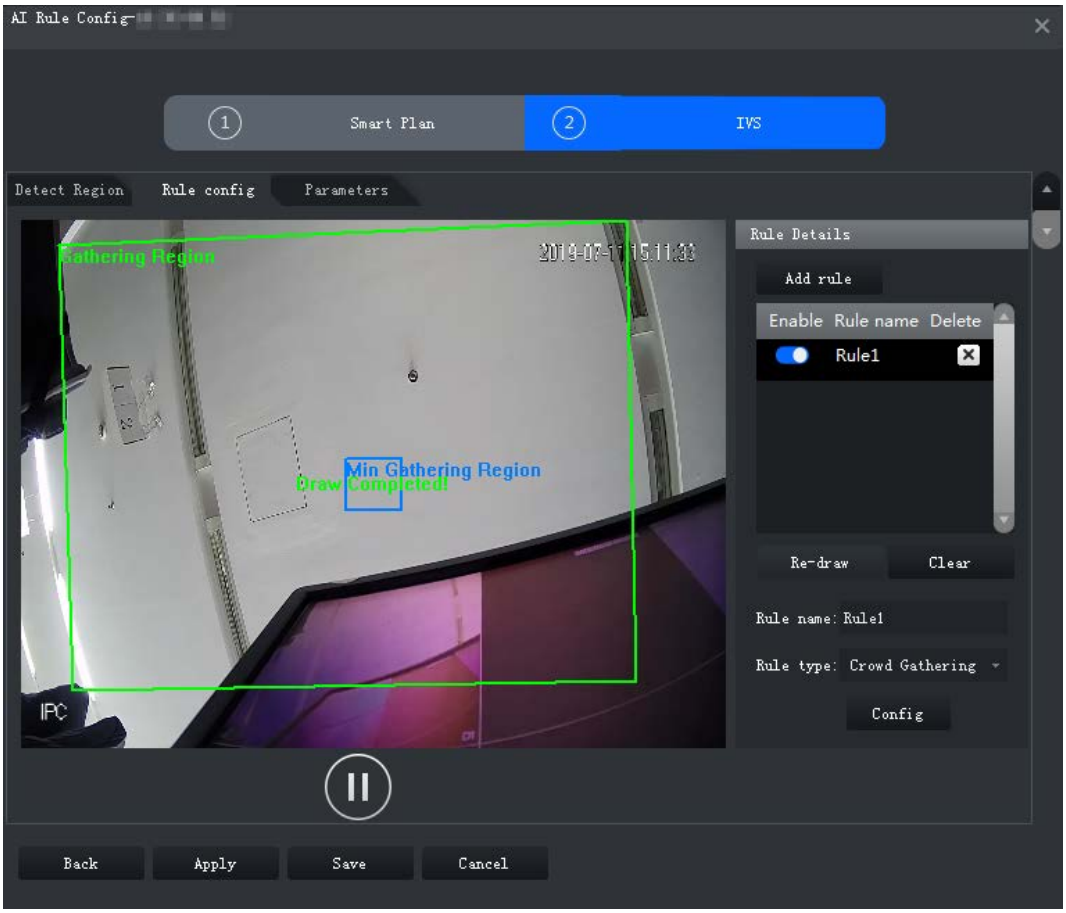
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

1) Enable rule. indicates the rule is enabled.
2) Modify the rule name.
3) Select **Missing Object** in the drop-down list of **Rule type**.

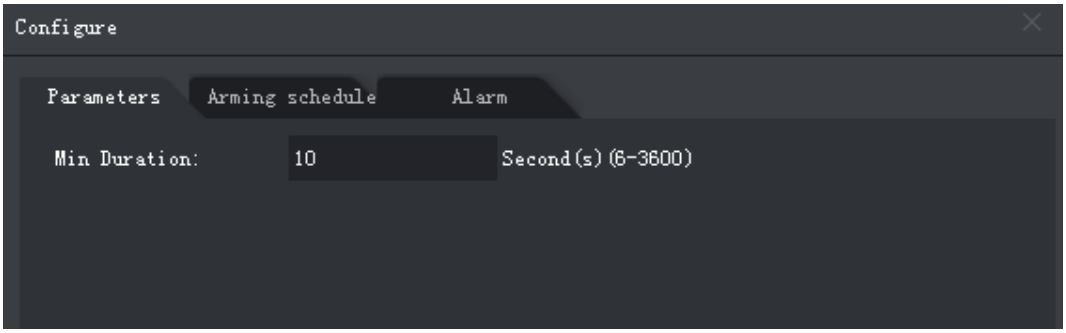
Step 4 Draw a detection zone on the video and right-click to finish.

Figure 3-80 Missing object



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.2.9.4.1 Tripwire".

Figure 3-81 Set parameters



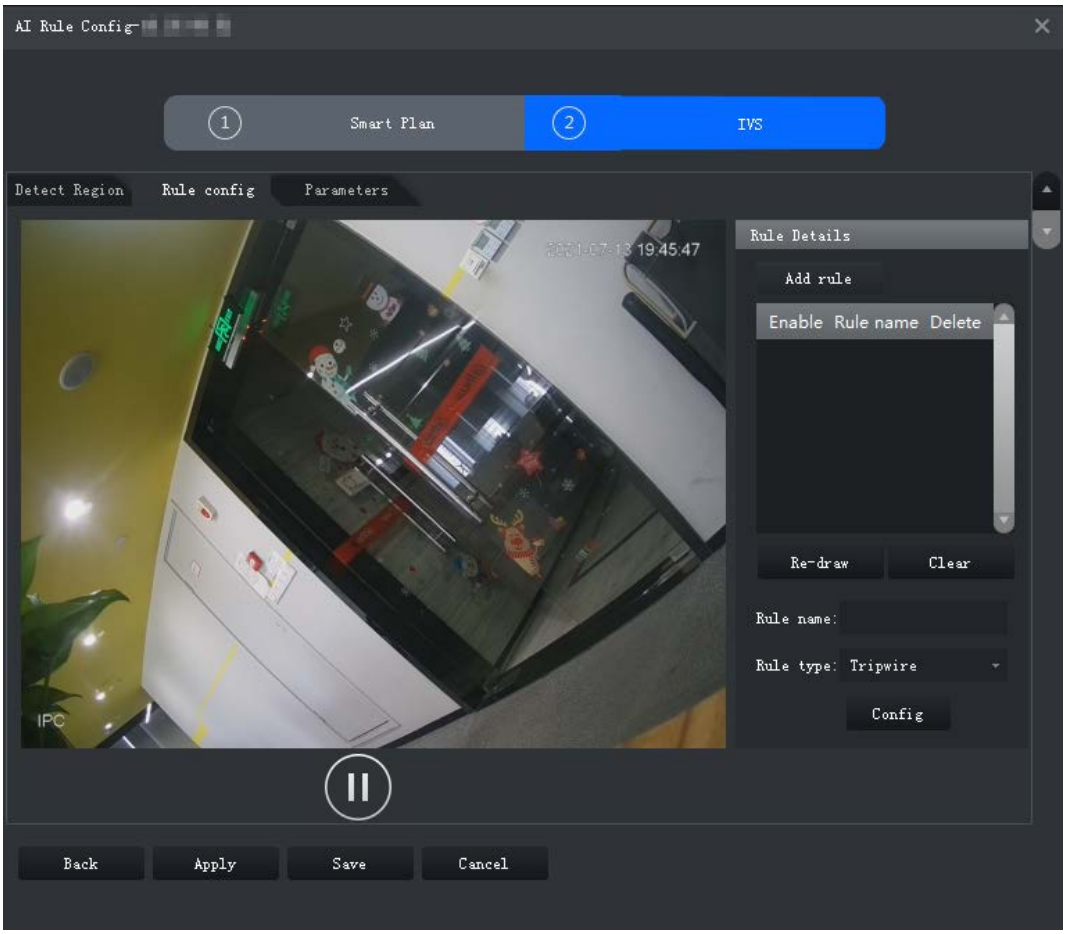
Step 6 Click **Apply**.

3.2.9.4.8 Loitering Detection

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

Step 1 On the **AI Rule Config** interface, click **Rule config**.

Figure 3-82 Rule configuration interface



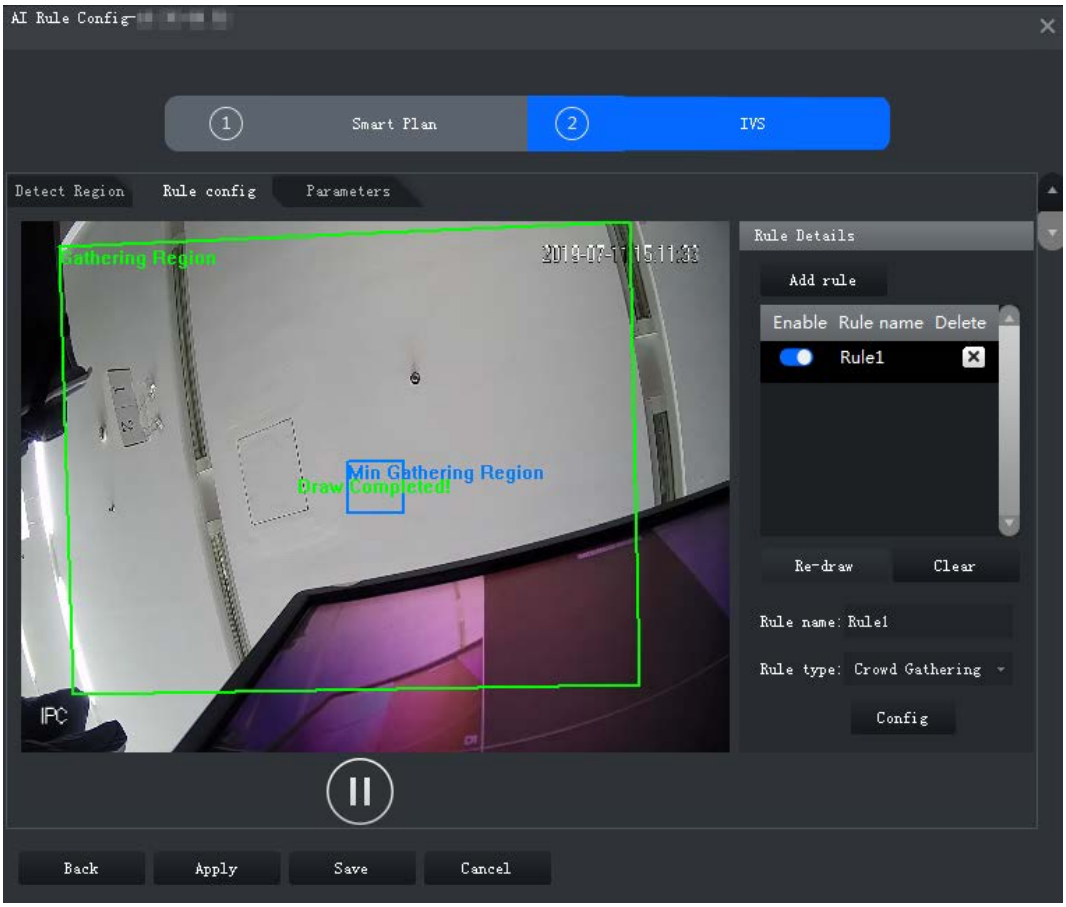
Step 2 Click **Add rule**.

Step 3 Enable rule and modify the name and type.

1) Enable rule. indicates the rule is enabled.
2) Modify the rule name.
3) Select **Loitering Detect** in the drop-down list of **Rule type**.

Step 4 Draw a detection zone on the video and right-click to finish.

Figure 3-83 Loitering detection



Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "3.2.9.4.1 Tripwire".

Figure 3-84 Set parameters

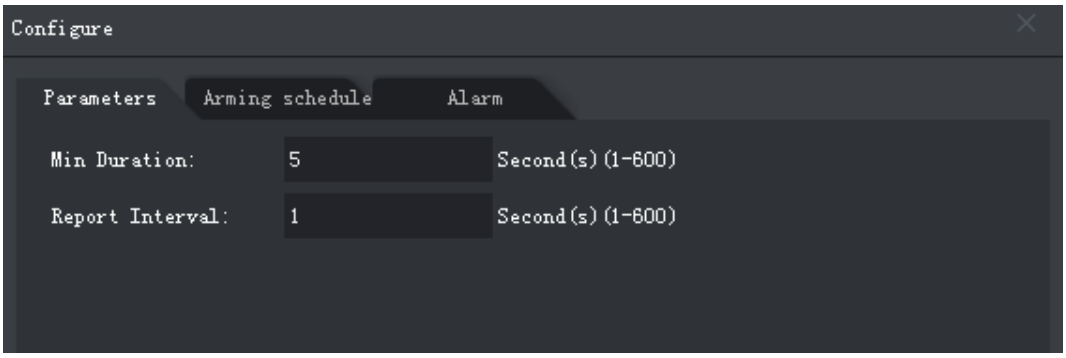


Table 3-19 Parameters

Parameter	Description
Min Duration	The minimum time duration from target appearing to alarm triggering.
Report Interval	If the event still exists after the first alarm, system will trigger more alarms by the preset alarm interval.

Step 6 Click **Apply**.

3.2.9.5 Configuring Parameters

Set common parameters for the IVS, including disturbance filter and sensitivity.

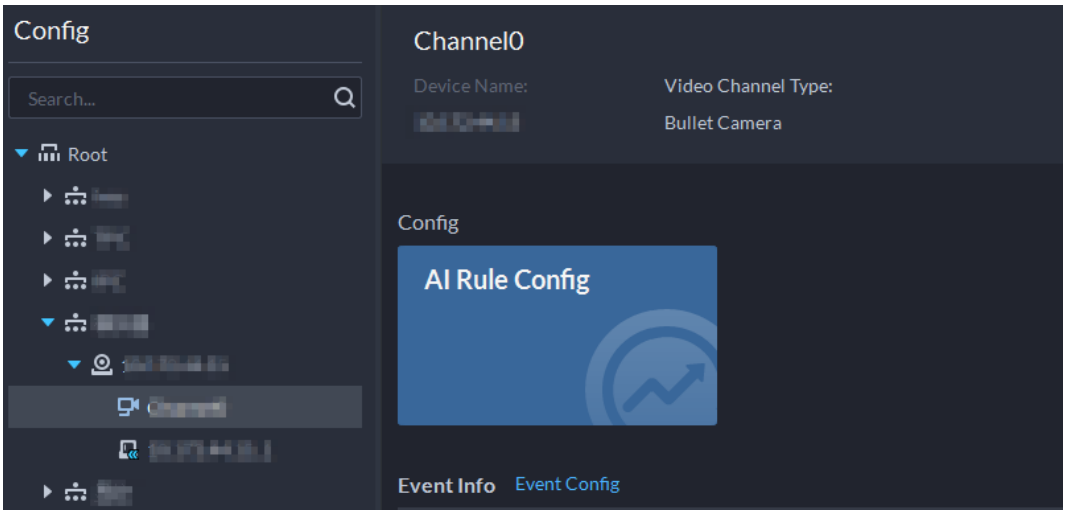
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config**

section, select **Device**.

Step 2 Click .

Step 3 Select a channel, and then click **AI Rule Config**.

Figure 3-85 Go to AI rule config interface



Step 4 After selecting the IVS smart plan in the **Smart Plan** interface, click **Next**.

Step 5 Click twice.

Step 6 Click **Parameters** after configuring rules on the **Rule config** interface.

Step 7 Set parameters.

Figure 3-86 Parameters

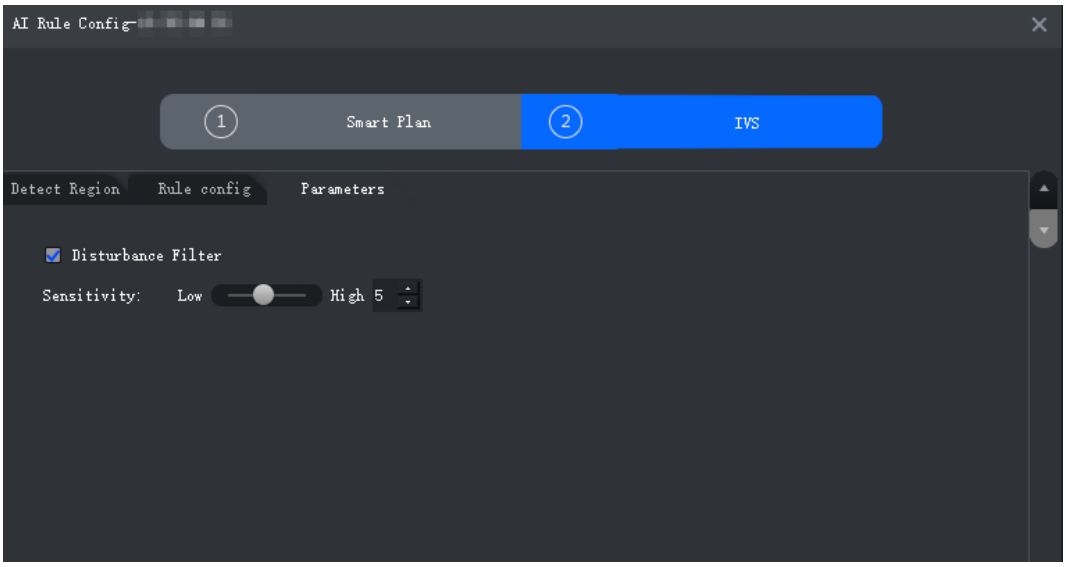


Table 3-20 Parameters

Parameter	Description
Disturbance Filter	Filter false targets including waving plants and water waves. This function may cause target omissions as some parts of a true target may be judged as false factors.
Sensitivity	Control detection sensitivity. The smaller the value is, the lower the false detection rate will be and the higher omission rate will happen. The bigger the value is, the higher false detection rate will be and the lower the omission rate will happen.

Step 8 Click **Save**.

3.2.10 Synchronizing People Counting Rules

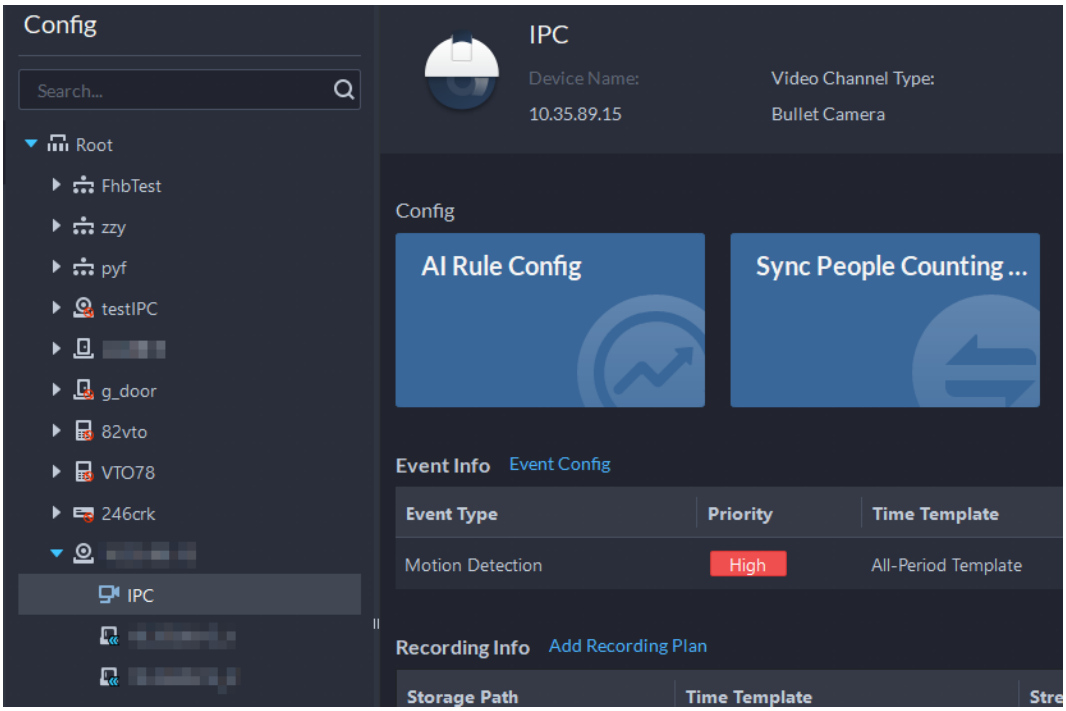
If you create, edit or delete people counting rules on a device, you have to manually synchronize them to the platform.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

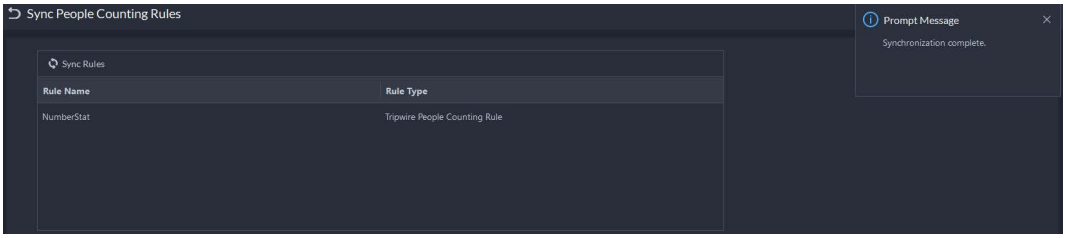
Step 3 Select a channel, and then click **Sync People Counting Rules**.

Figure 3-87 Synchronize people counting rules from the device



Step 4 Click **Sync Rules**, and then the system prompts **Synchronization Complete**.

Figure 3-88 Synchronize people counting rules from the device



3.3 Adding Role and User

Users of different roles have different menus and permissions of device access and operation. When creating a user, assign a role to it to give the corresponding permissions.

3.3.1 Adding User Role

A role is a set of permission. Classify users of the platform into different roles so that they can have different permissions for operating the devices, functions and other system resources.

- Super administrator: A default rule that has the highest priority and all the permissions. This role

cannot be modified. A super administrator can create administrator roles and common roles. The system supports 3 super administrators at most.

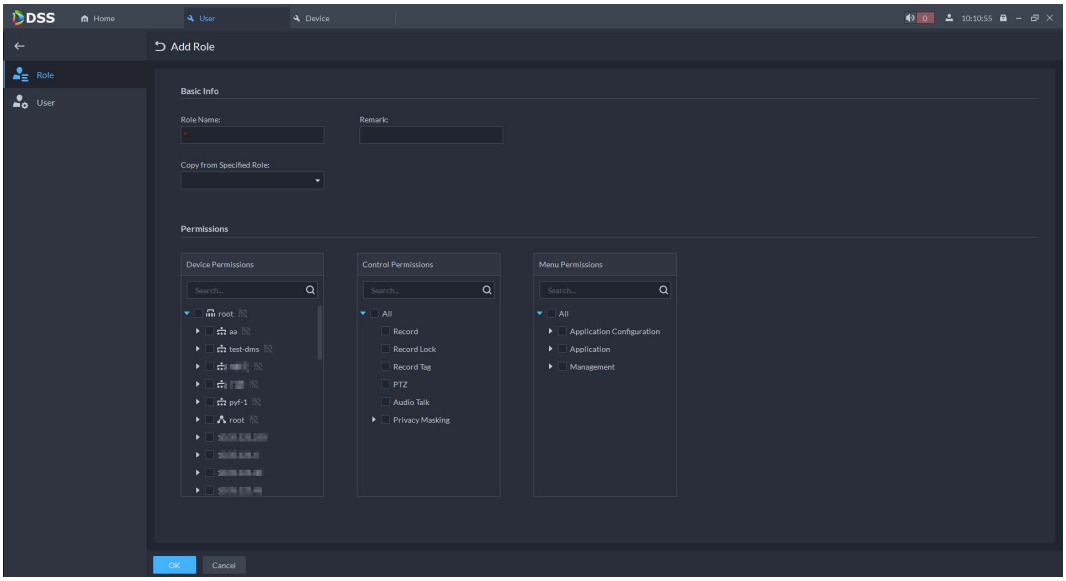
- Administrator: A default rule that cannot be modified and has no permission of authorization, backup and restore. An administrator can create other administrators.
- Common role: A common role has no permission of authorization, backup and restore, user management, and storage management.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **User**.

Step 2 Click .

Step 3 Click **Add**, set role information, and then select device and control permissions and assign the rule to users.

Figure 3-89 Add a role



Step 4 Click **OK**.

3.3.2 Adding User

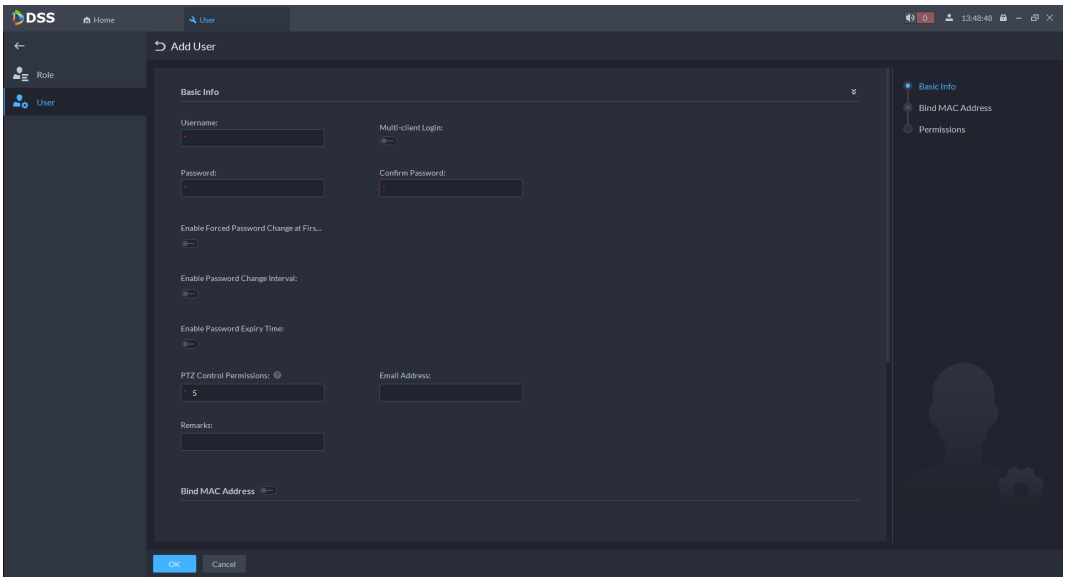
Create a user account for logging in to the platform.

Procedure

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **User**.

Step 2 Click **Add**, and then configure user information.

Figure 3-90 Add a user



- **Enable Forced Password Change at First Login**: Force to change the password for first-time login.
- **Enable Password Changing Interval**: Force users to change the password on time.
- **Enable Password Expiry Time**: The password should be changed after it expires on this date.
- **PTZ Control Permission**: The PTZ control priority of the user. The larger the value, the higher the priority.
- **Email Address**: User email address to receive alarms.
- **Multi-client Login**: Whether the user can be logged in to multiple clients at the same time.
- **Bind MAC Address**: To limit the user to log in from specific computers. One user can be bound to 5 MAC addresses at most.
- Role: Assign a role to the user to give the corresponding permissions.

Step 3 Click **OK**.

Related Operations

- Click to freeze user. The frozen user cannot log in to the DSS Client and App.
- Click to modify user information except username.
- Click to delete user.

3.3.3 Password Maintenance

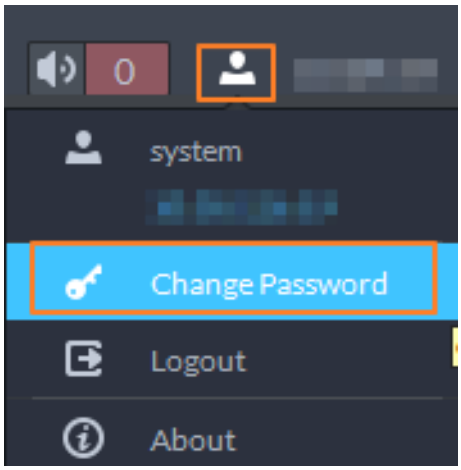
The platform supports modifying user password, and resetting system user password when it is forgotten. Only the system user can reset password. Other users, when their passwords are forgotten, can ask the system user to modify the passwords.

3.3.3.1 Changing Online User Password

We recommend changing your password regularly for account safety.

Step 1 Log in to the DSS Client, click at the upper-right corner, and then select **Change Password**.

Figure 3-91 Change password



Step 2 Enter the old password, new password, and then confirm the new password. Click **OK**.

3.3.3.2 Changing Offline User Password

Only system user can change offline user password.

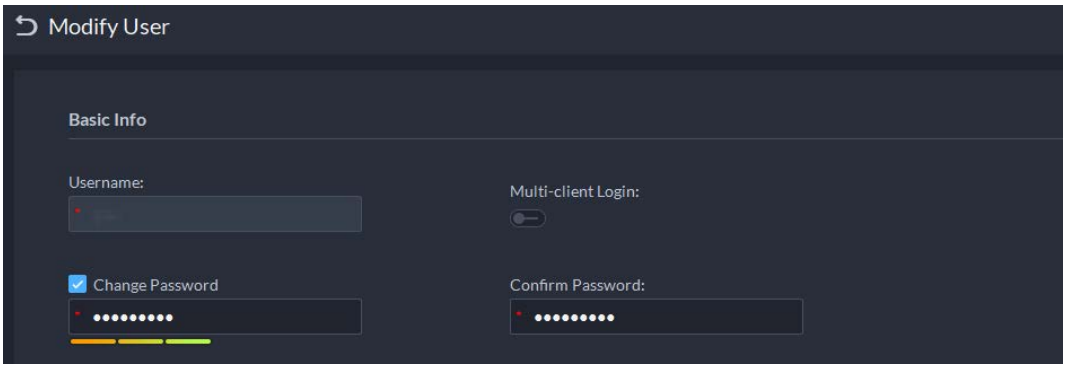
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **User**.

Step 2 Click .

Step 3 Select a user, and then click .

Step 4 Enable **Change Password**, enter the new password and confirm password, and then click **OK**.

Figure 3-92 Change user info



3.3.3.3 Resetting System User Password

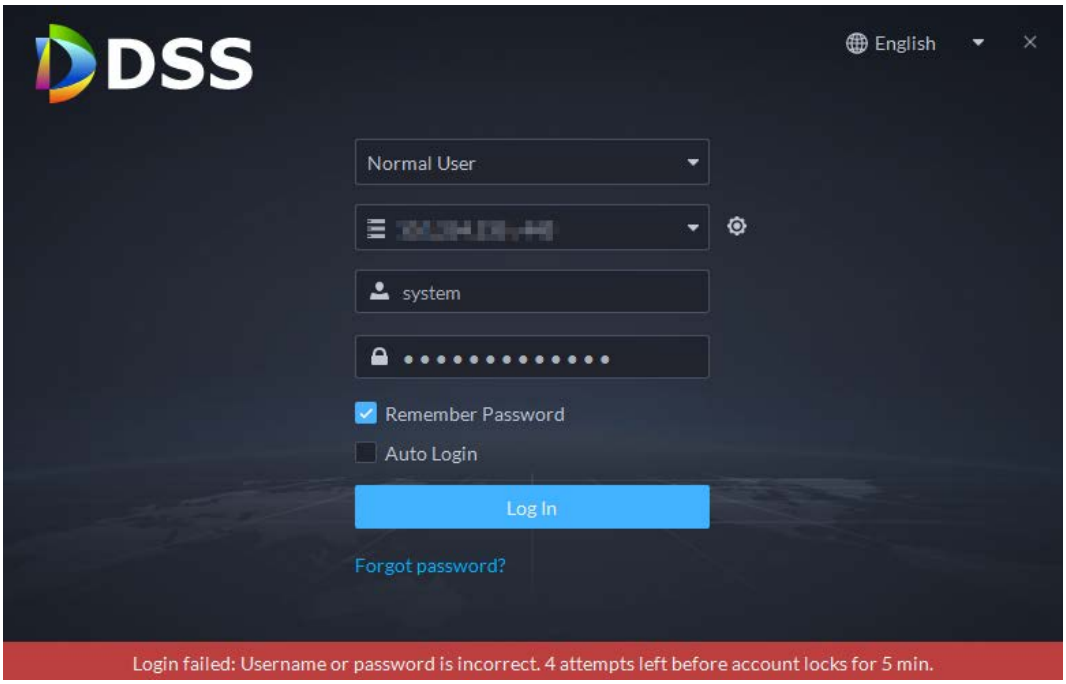
When the system user password is forgotten, you can reset the password by answering security questions.

Step 1 On the login interface of the DSS Client, enter system username and a wrong password, and then click **Login**.

Step 2 Click **Forgot password?**.

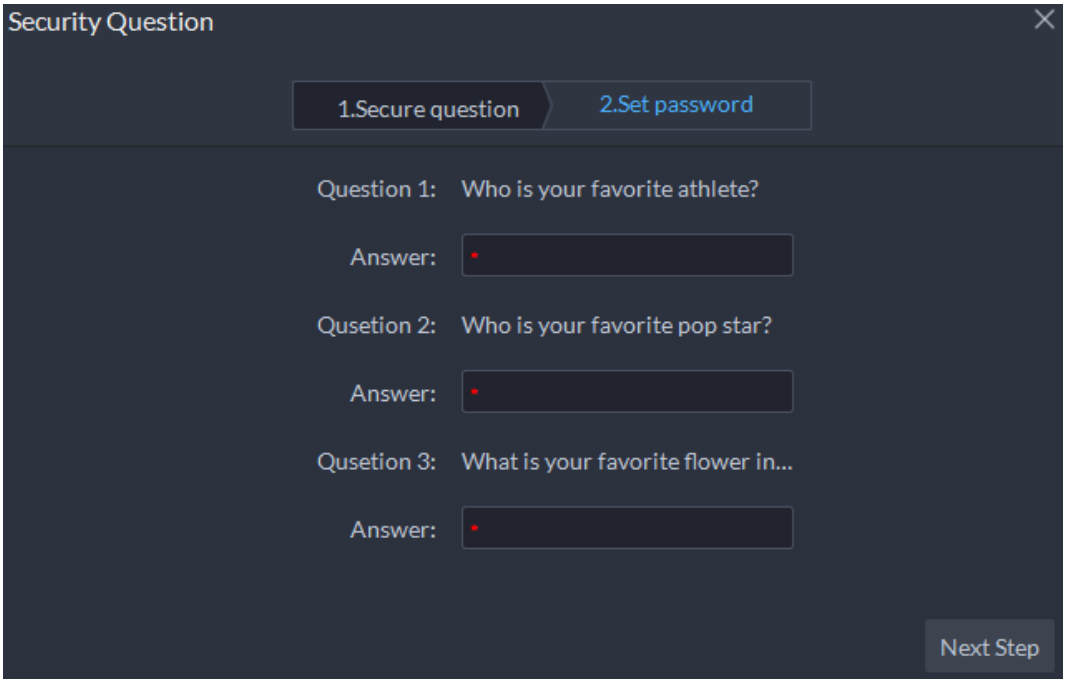
Forgot password? only displays when the system user logs in with a wrong password.

Figure 3-93 Forgot password



Step 3 Answer the questions, and then click **Next**.

Figure 3-94 Security questions



Step 4 Enter the new password, and then click **OK**.

3.4 Configuring Server Disk

Configure local disk to store different types of files, including videos, images, and normal files. In addition to the local disks, you can also connect an external disk to the platform server, but you have to format the external disk before using it.

- To set up local storage, you need a physical disk with only one volume or any volume of one physical disk. Back up the data of the disk or volume before setting its disk type, which will format and erase all data from it.
- One physical disk with only one volume or any volume of one physical disk can only store one type of files. If you need to store more than one type of files, you need more than one physical disks or volumes, but it cannot be the one where you installed the operating system of the server or the DSS server. See "2.1.2 Installing DSS".

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Storage**.

Step 2 Select .

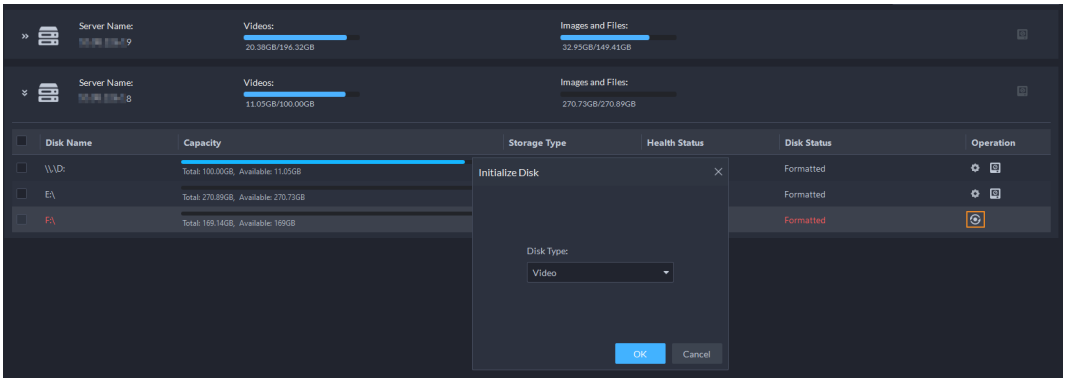
Step 3 Format local disk.

Format the disk to set disk type. This operation will clear all data on the disk. Be cautious.

1. Select user volume, and then click .
2. Select format disk type, and then click **OK**.

If you do not set up one or more disk types, you will not be able to properly use corresponding functions. For example, if you do not set up an **Image and File** disk, you will not see images in all alarms.

Figure 3-95 Initialize local disk



Disk types:

- **Video**: Stores videos.
- **Images and Files**: Stores all types of images and video files from MPT devices.

If no **Image and File** disk is configured, the client will give corresponding prompt when an admin logs in.

Step 4 Manage local disks.

- To configure disk type: Click .
- To format a disk: Select a disk or user volume, click .

4 Businesses Configuration

This chapter introduces the basic businesses, such as storage plan, video monitoring, access control, alarm controller, video intercom, target detection, face recognition, and ANPR.

4.1 Configuring Events

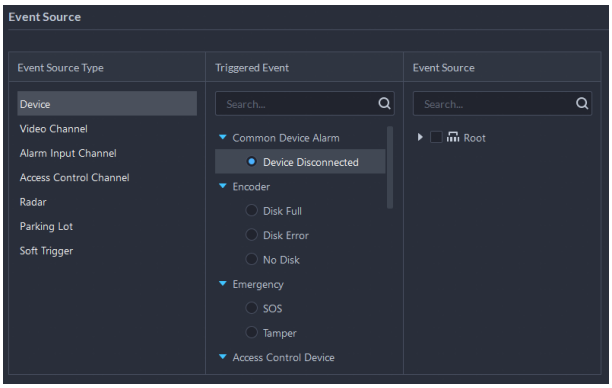
Configure events first if you want to display alarm event notifications on the platform.

Procedure

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **App Config** section, select **Event**.

Step 2 Click **Add**.

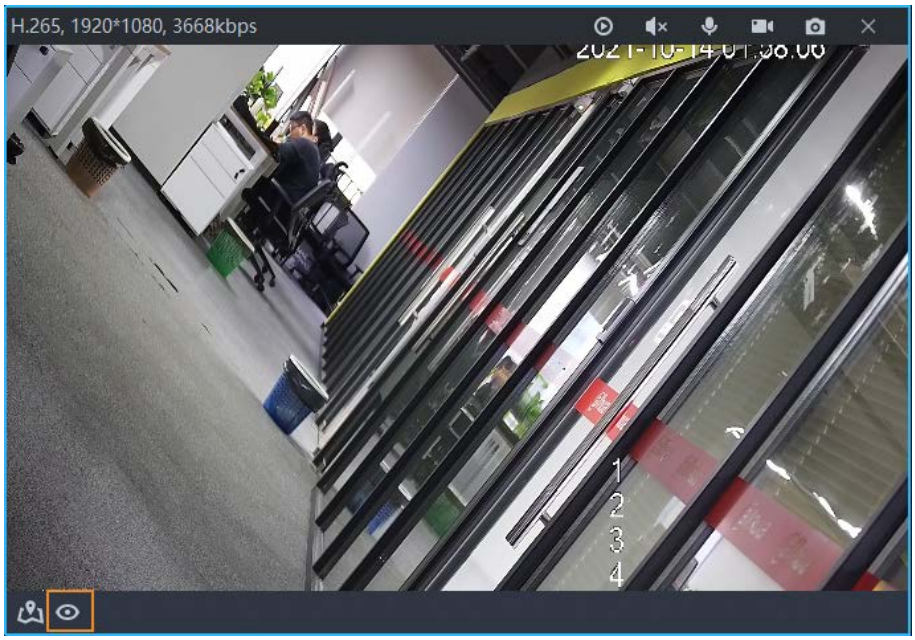
Figure 4-1 Configure the event source



Step 3 Configure the event source.

- Before configuring the event, check whether the channel features match the event type; otherwise the event type cannot be selected as the alarm source. To configure channel features, see "3.2.2.5.1 Modifying Device Information".
- If **Alarm Input Channel** is selected, check whether the **Triggered Event** that you select matches the alarm input channel you select; otherwise, the event will not be triggered.
- **Soft Trigger** is a type of event that is manually triggered. You can customize its name and button type. When viewing the live video image of the configured channel in the **Monitoring Center**, you can click its button to trigger an alarm manually.

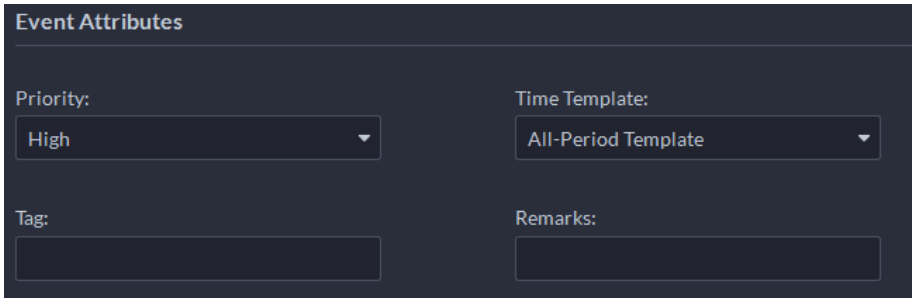
Figure 4-2 Manually trigger an alarm by clicking the button



Step 4 Configure parameters under **Event Attribute**.

Configure alarm priority as needed, so that you can quickly know the priority of alarm when receiving an alarm on the DSS Client.

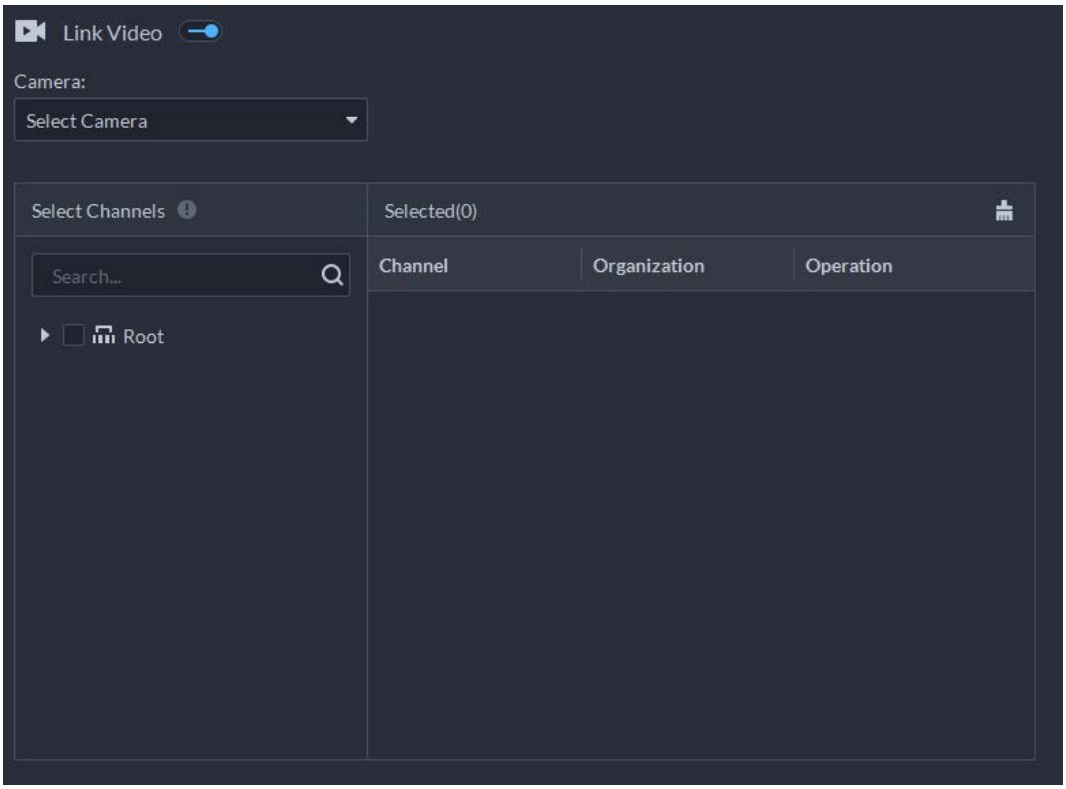
Figure 4-3 Event attributes



Step 5 Configure alarm linkage actions.

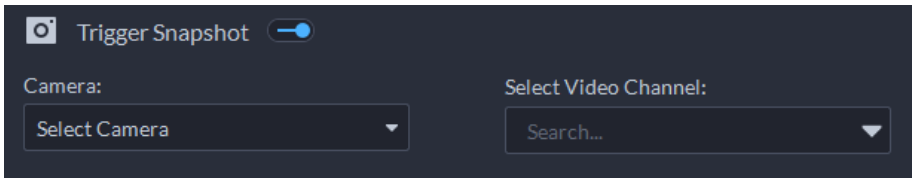
- To link video, enable **Linked Action** > **Link Video**, and then select a camera.

Figure 4-4 Link video



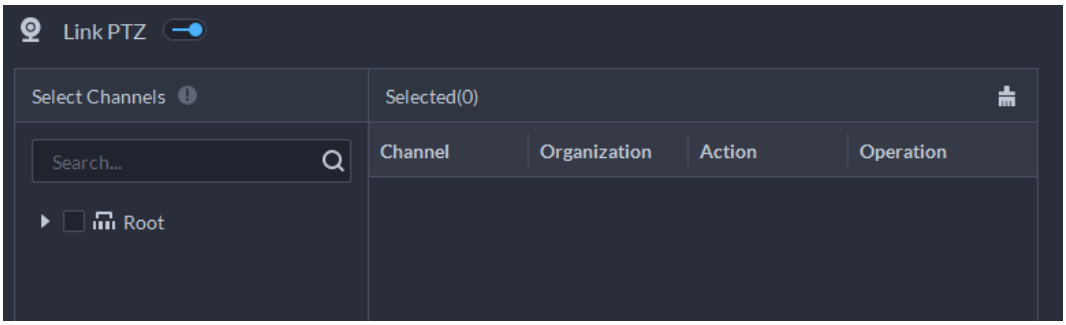
- Alarm source: The camera of the alarm itself is linked when the alarm occurs.
- Bind camera: If the alarm channel is bound to a video channel, you can view the video of the bound channel. To bind a channel, see "3.2.3 Binding Resources".
- Select a camera: Select a camera so that you can view the camera video when the associated alarm is triggered.
- Position: Whether to record when the alarm is triggered.
- **Stream Type**: The stream type of recordings. Main stream has higher quality than sub stream, but consumes more storage and bandwidth.
- **Record Time**: The duration of recording when the alarm is triggered.
- **Prerecord Time**: Where the alarm video starts to play. It is the length of video prior to the alarm.
- To trigger a snapshot, enable **Trigger Snapshot**, and then select a camera and video channel.

Figure 4-5 Trigger a snapshot



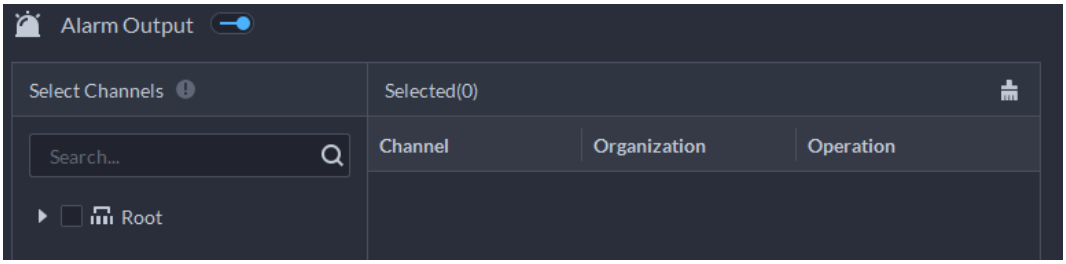
- To link a PTZ action, click **Link PTZ**, and then select the PTZ channels and presets to be linked.

Figure 4-6 Link PTZ



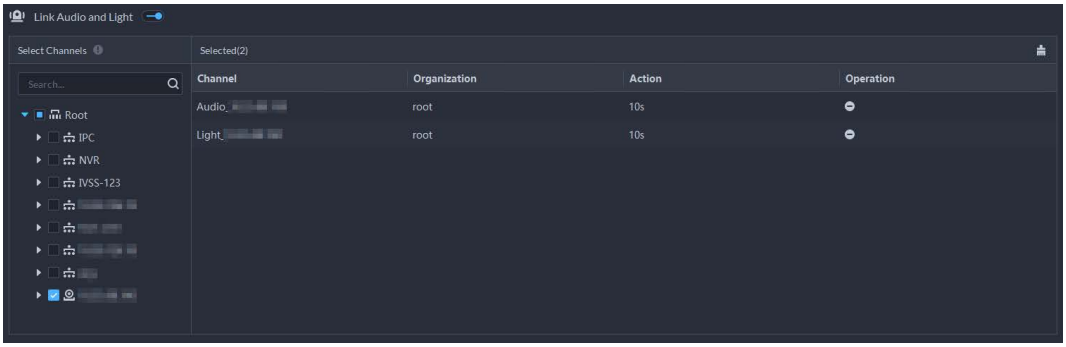
- Click **Alarm Output**, select an alarm output channel, and then set duration.

Figure 4-7 Alarm output



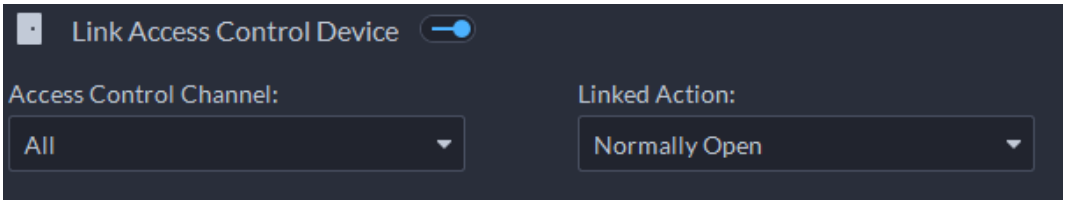
- To link audio and light, click **Link Audio and Light**, select the audio and light channels, and then select the action duration.

Figure 4-8 Link audio and light



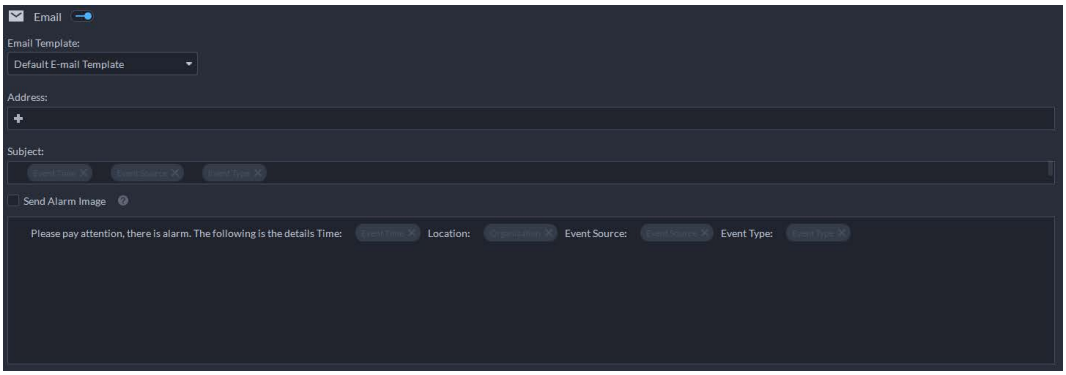
- Click **Link Access Control Device**, select access control channels, and then select a linked action.

Figure 4-9 Link access control device



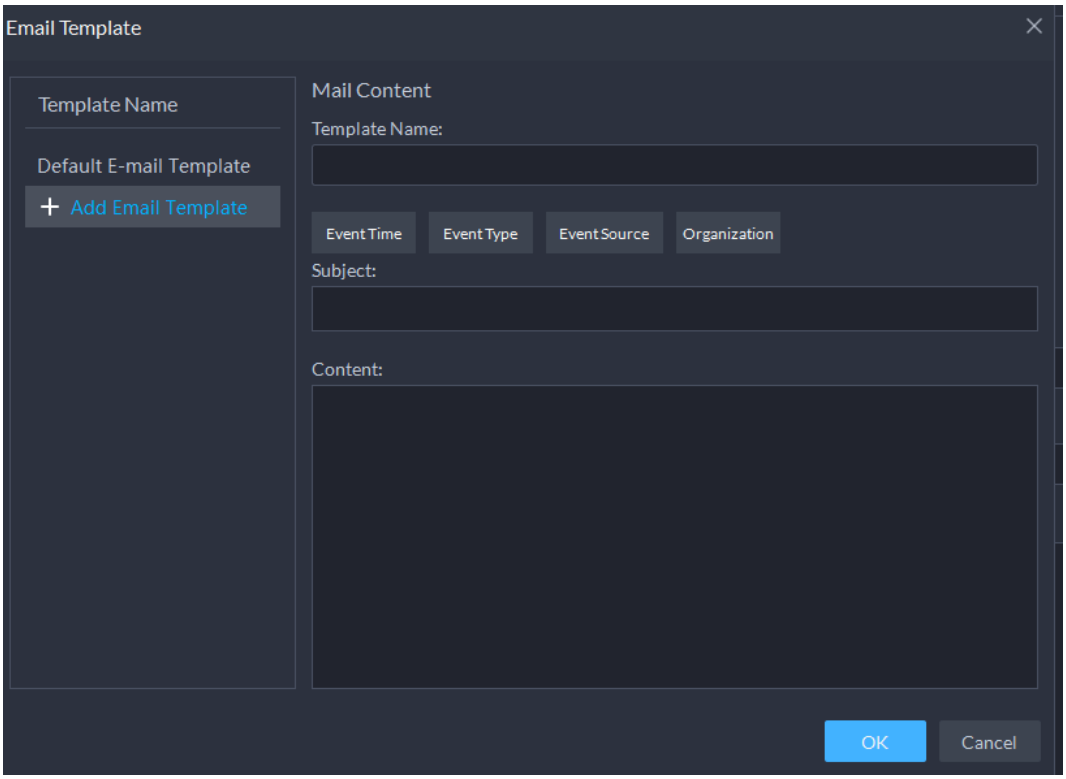
- To link emails, enable **Email**, and click + to add the email address, and then an email will be sent to the selected email address when an alarm is triggered.

Figure 4-10 Link email



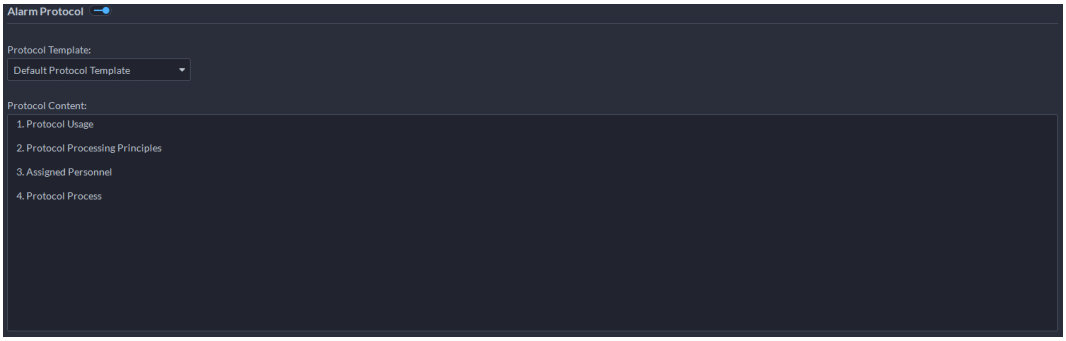
To configure the email template, select **Add Email Template** from the **Email Template** drop-down list.

Figure 4-11 Email template



- Apply an alarm protocol to help users process alarms when they are triggered . Click **Alarm Protocol**, and then select a protocol from the **Protocol Template** drop-down list.

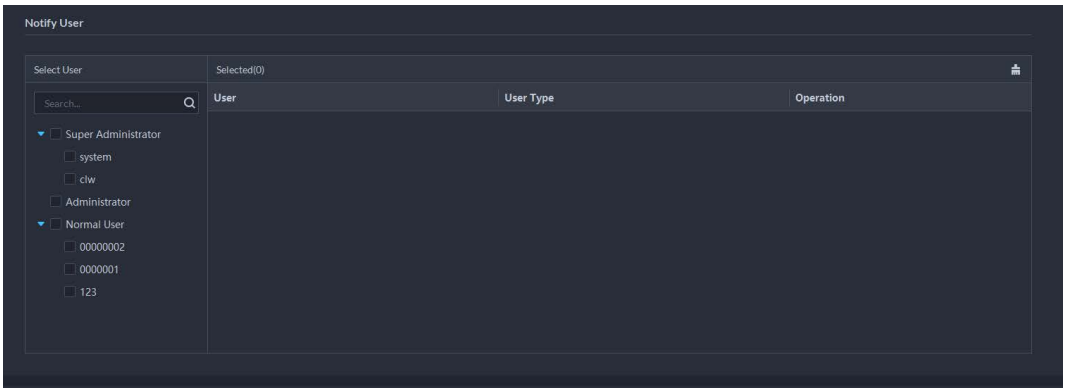
Figure 4-12 Alarm protocol



Click **Add protocol template** to create a new protocol; click  to edit the content of a protocol.

- To inform a user, click **Notify User**, and then select the user to be informed.

Figure 4-13 Notify user



Related Operations

- To edit an event, click .
- To delete an event, click .
- To disable an event, click .

4.2 Configuring Map

4.2.1 Preparations

- Devices are deployed. For details, see device user's manuals.
- Basic configurations of the platform have been finished. For details, see "3 Basic Configurations".
- A map picture is prepared.
- To show device alarms on the map, make sure that **Map flashes when alarm occurs** is enabled in **Home** > **Management** > **Local Settings** > **Alarm**.

4.2.2 Adding Map

Import a raster map. You can add cameras, access control channels, and alarm channels onto the map to directly show them on the map.

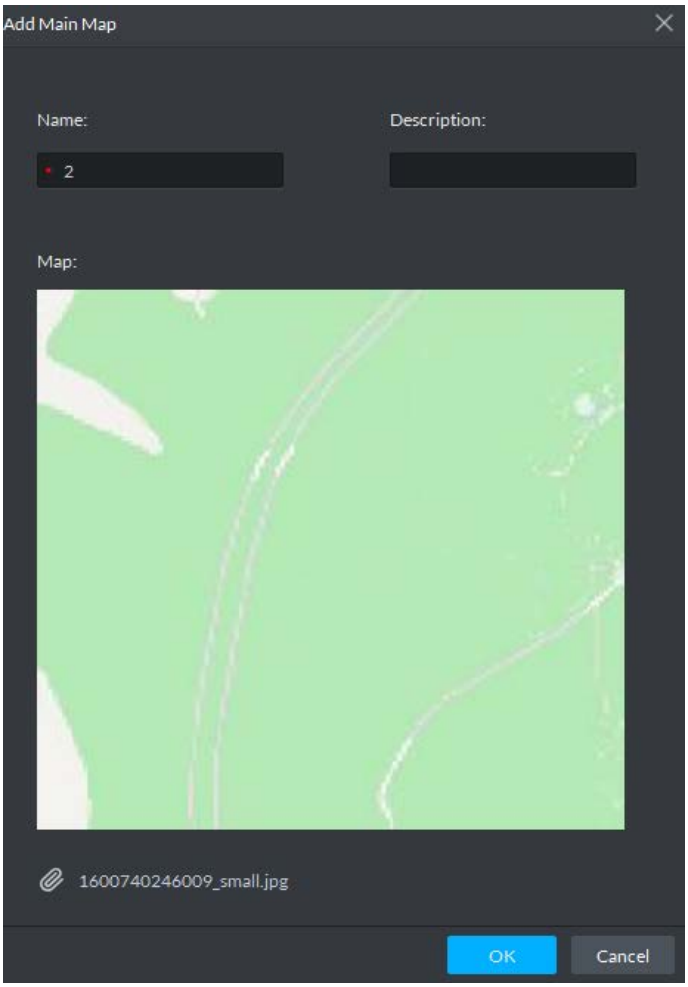
Procedure

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Map**.

Step 2 Select the **Main Map**, and then click **Add Map**.

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

Figure 4-14 Add main map



Step 4 Add a sub map.

1) Click the added raster map, and then click **Add Sub Map**.
2) Enter the map name, upload the picture, and then click **Next Step**.
3) Drag the picture to the desired position and click **OK**.

Related Operations

- Delete device
  To delete a device from the map, click it and then click **Delete Device**.
- Show device
  Select to display cameras, alarm inputs, and zone alarms.
- Move
  To move a device, click **Move** and then drag the device on the map.
- Select
  To select one or more devices, click **Select**, and then click the devices on the map one by one.
- Pane
  To select devices in batches, you can click **Pane**, and then draw a frame on the devices to select the device.
- Clear
  To clear all markings on the map, click **Clear**.
- Add a submap
  To add a submap on the current map, click **Add Sub Map**, click on the map to locate it, name the map, upload map picture and then click **OK**.

- Length
  Select **Box** > **Length**, connect two points with a line on the map (double-click to finish drawing), and then the distance between the points is shown.
- Area
  Select **Box** > **Area**, select a region on the map (double-click to finish drawing), and then the area is measured.
- Add Mark
  Select **Box** > **Add Mark**, and then mark information on the map.
- Reset
  Select **Box** > **Reset** to restore the map to its initial position and zoom level.

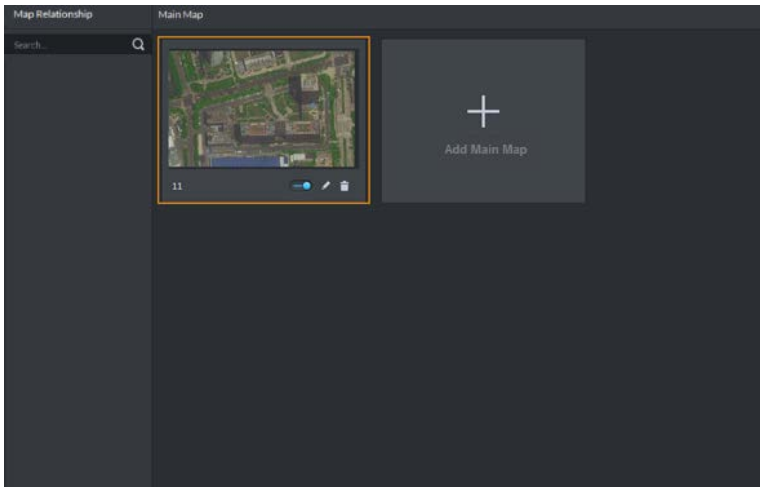
4.2.3 Marking Devices

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

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Map**.

Step 2 Click the map.

Figure 4-15 Map



Step 3 Drag the device channel from the left device tree to the corresponding location of the map.

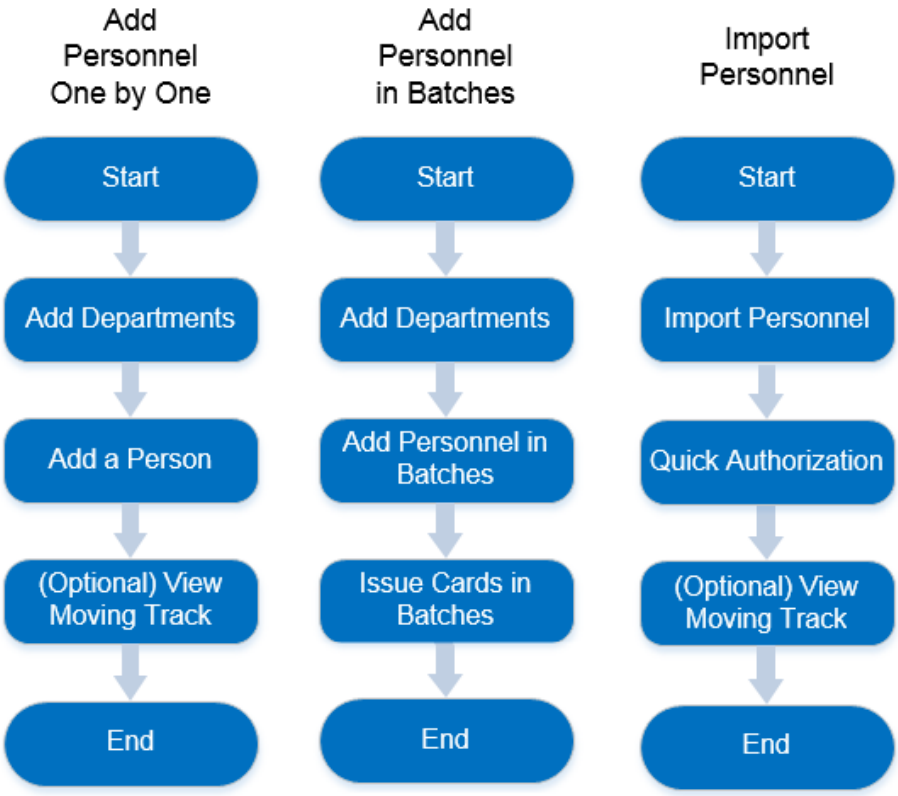
4.3 Personnel and Vehicle Information Management

Configure personnel and vehicle information for the applications of access control, vehicle control, and video intercom.

- Personnel information contains card number, password, face picture, and more. People bound with vehicle information will be displayed in the vehicle list.
- Vehicle information helps to confirm the entry of the vehicle into a certain area. Vehicle bound with personnel information will be displayed in the personnel list.

4.3.1 Configuring Personnel Information

Figure 4-16 Personnel Management



4.3.1.1 Adding Person Group

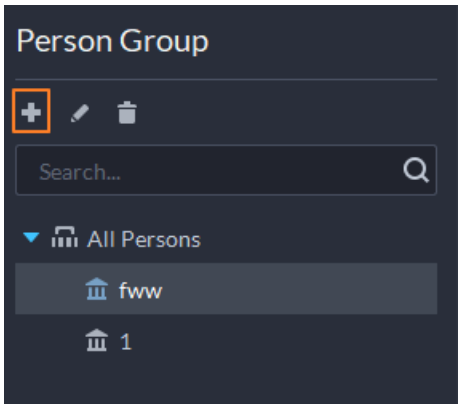
Add groups and you can manage people and assign permission by group.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Personal and Vehicle Infor**.

Step 2 Click .

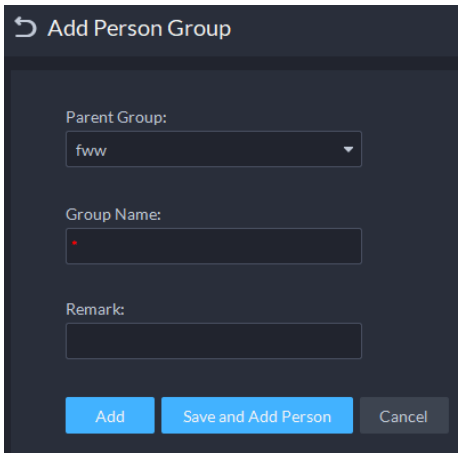
Step 3 Click .

Figure 4-17 Added person group (1)



Step 4 Enter person group name and click **OK**.

Figure 4-18 Added person group (2)



Related Operations

- To delete a person group, select it, and then click . All permissions associated with the people in the group will also be deleted.
- To rename a person group, select it, and then click .
- To move a person into a different group, select the person, and then click **Move To**.

4.3.1.2 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.

- Person ID shall be the same on the platform and access control devices; otherwise person data could be wrong.
- To collect fingerprints or card number, connect a fingerprint collector or card reader first.

4.3.1.2.1 Adding a Person

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Personal and Vehicle Info**.

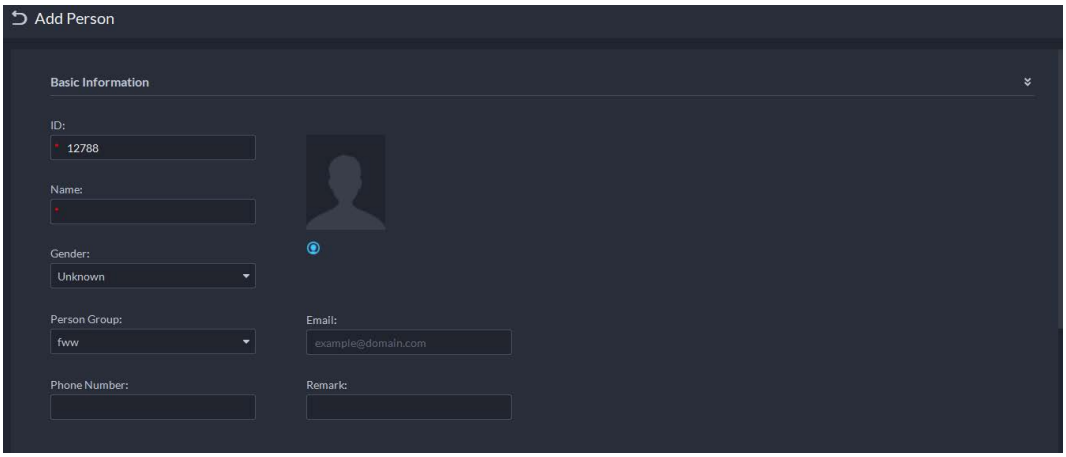
Step 2 Click .

Step 3 Click **Add**.

Step 4 Click the **Basic Info** tab to configure person information.

1) Hover over the profile, and then click **Upload** to select a picture or click **Snapshot** to take a photo.
   Click on the **Snapshot** interface, and then you can select camera, pixel format, resolution, and image quality. This is only effective with the current client.
2) Enter personnel information as necessary. ID is required and must be unique. It can be up to 30 characters, and letter-number combination is also supported.

Figure 4-19 Personnel information



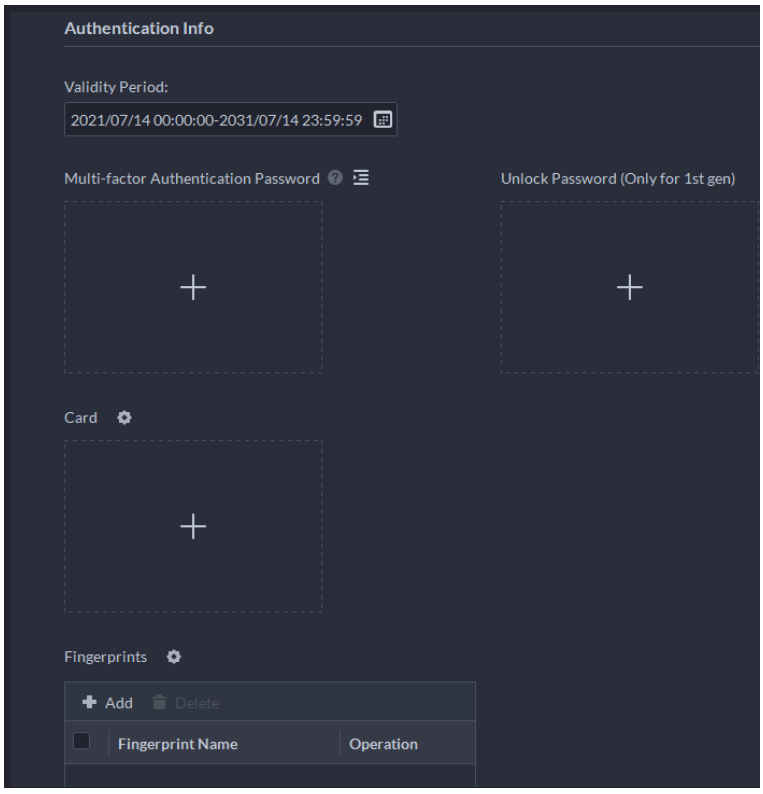
Step 5 Click », and then set person details as required, including nickname, ID, address, birthday, region, company, job title, and more.

Step 6 If the person is resident, Click » next to **Resident Info**, and then bind room number.

- **Room No.**: The number of the apartment in which this person lives. The room number is displayed in the access records and video intercom operation records. Access permission of the corresponding VTO is also included when authorizing access control permission to this person.
- **Householder**: When several people live in one apartment, you can set one of them as the householder. The householder will be taken as the only contact of video intercom.

Step 7 Click the **Authentication Info** tab, and then set validity period and access control information.

Figure 4-20 Authentication Info



1) Configure effective periods, within which the card, password, and fingerprint are

effective.

2) When access controllers are added and passwords are required to unlock the door, configure the password first.

Click , and then **Unlock Password** interface is displayed.

- Directly uses password to unlock the door: On the **Unlock Password** interface, click , enter password, and then click .
- Uses multi-factor authentication password, combining with card, or fingerprint, to unlock the door: In the **Multi-factor Authentication Password** interface, click , enter password, and then click .

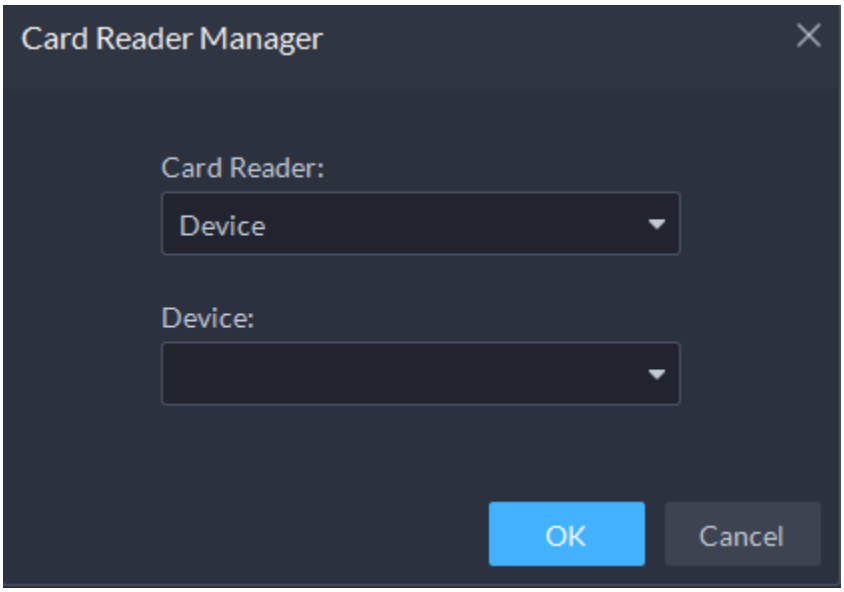
- The unlocking password here is only effective to the first- generation access controller.
- Click to display the password.

Step 8 Issue cards to personnel.

One person can have up to 5 cards. There are two ways to issue cards: by entering card No. and by card reader. A card number is 8-16 numbers. Only second-generation access control devices support 16-digit card numbers. When a card number is less than 8 numbers, the system will automatically add zeros prior to the number to make it 8 digits. For example, if the provided number is 8004, it will become 00008004. If there are 9-16 numbers, the system will not add zero to it.

1) Click next to card, select device or card issuer, and then click **OK**.

Figure 4-21 Reader manager



2) Go back to **Card** interface, enter card number, and then click .

Figure 4-22 Reader manager

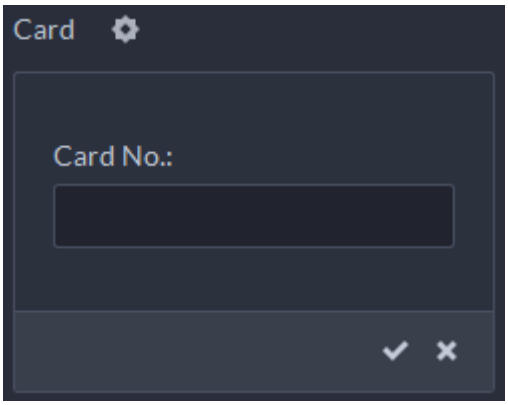


Table 4-1 Card operations

Icon	Description
	If a person has more than one card, only the main card can be issued to the first-generation access control device. The first card of a person is the main card by default. Click on an added card, the icon turns into , which indicates that the card is a main card.
	Set a card as duress card. When opening door with a duress card, there will be a duress alarm. Click this icon, it turns into , and is displayed at upper right, which indicates that the card is set as a duress card. To cancel the duress setting, click .
	Change card for the person when the current card does not work.
	Remove the card, and then it has no access permissions.

Step 9 Collect fingerprint.

To open door with fingerprint, you need to collect personnel fingerprints. A person can have up to 3 fingerprints.

1) Click next to **Fingerprint**.
2) Click **Add**.
1) Select a fingerprint collector from the **Fingerprint Collector** drop-down list, and then click **OK**.
2) Click **Add**

Figure 4-23 A collected fingerprint

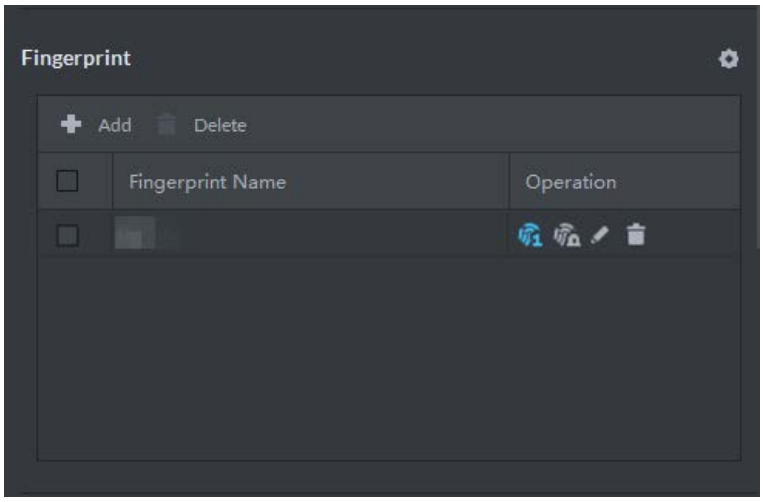


Table 4-2 Fingerprint operations

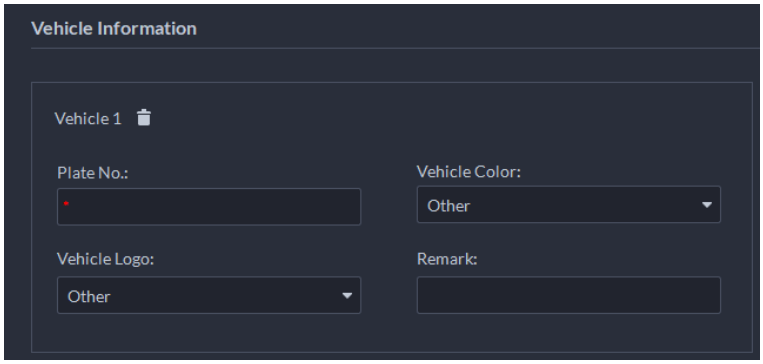
Icon	Description
	One can have 3 fingerprints, but only these fingerprints can be issued to devices. Click this icon, and then it turns into , which indicates that this fingerprint has been set as a main one. To cancel the main fingerprint setting, click .
	Set a fingerprint as duress fingerprint. When opening door with a duress fingerprint, there will be a duress alarm. Click this icon, it turns into , which indicates that the fingerprint has been set as a duress fingerprint. To cancel the duress setting, click .
	Modify fingerprint name.
	Remove the fingerprint, and then it has no access permission.

Step 10 If the person has a vehicle, click next to **Vehicle Information** to add vehicle information.

Click , and then enter plate No., select vehicle color and logo.

Add vehicle information to a person, so as to enable vehicle access permission for this person.

Figure 4-24 Add vehicle information



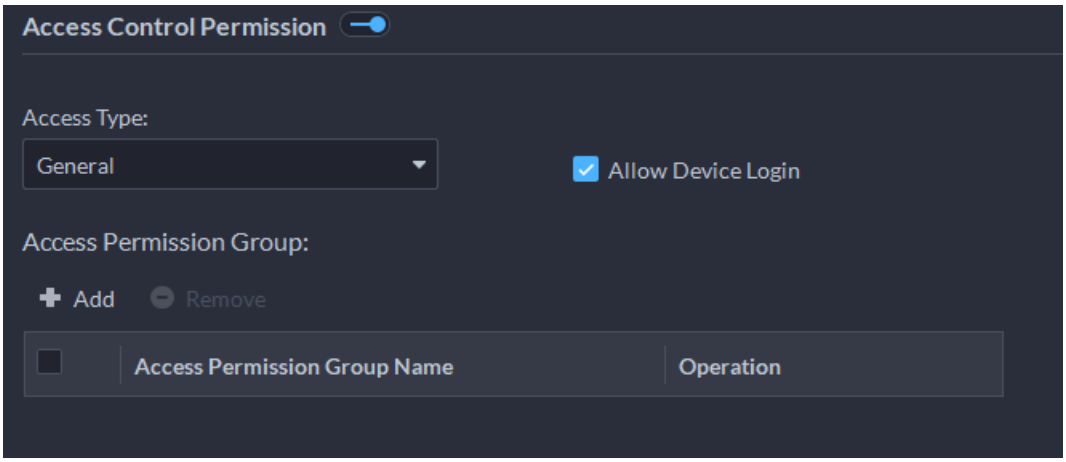
Step 11 If the person need access control permission, enable the permission first.

1) Click next to **Access Control Permission**.
2) Select **Access Type**, and select **Allow Device Login** check box as needed.
   - **Allow Device Login**: People have permission to go into web interface from the device.

- Select **General** if it is the first time for the person to use the card to unlock the door.

3) Click **Add**, and then select access control permission group. For details, see "4.4.1.1 Creating Face Comparison Group".

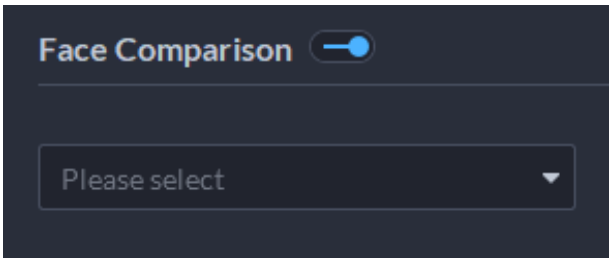
Figure 4-25 Add to access control permission group



Step 12 Enable **Face Comparison** to recognize the person by images.

1) Click next to **Face Comparison**.
2) Select a face comparison group.

Figure 4-26 Face comparison

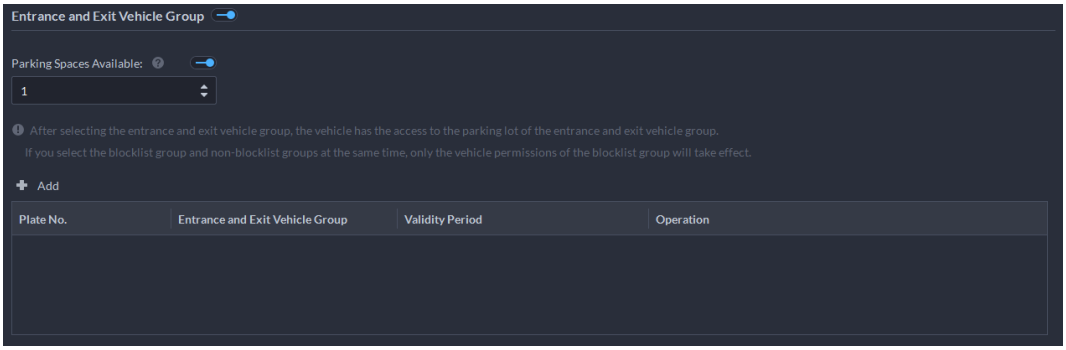


You need to create a face comparison group first.

Step 13 If the vehicle needs access to the parking lot, enable and configure **Entrance and Exit Vehicle Group** first.

1) Click next to **Entrance and Exit Vehicle Group**.
2) Enable **Parking Space Available** and configure the number of the parking space for the vehicle owner.
3) Select **Entrance and Exit Vehicle Group** and **Validity Period**.

Figure 4-27 Entrance and exit vehicle group



Step 14 Click **OK**.

To delete a person, you can select the person, and then click ; to delete all people on this page, select the **Select All** check box, and then click **Delete**.

Related Operations

- To edit basic information of a person, select the person, and then click .
- To delete a person, select the person, and then click . Or select multiple people, and then click **Delete** to delete them in batches.
- To view authorization exception, click .
- To search for a person, enter key words in the .

4.3.1.2.2 Importing Personnel

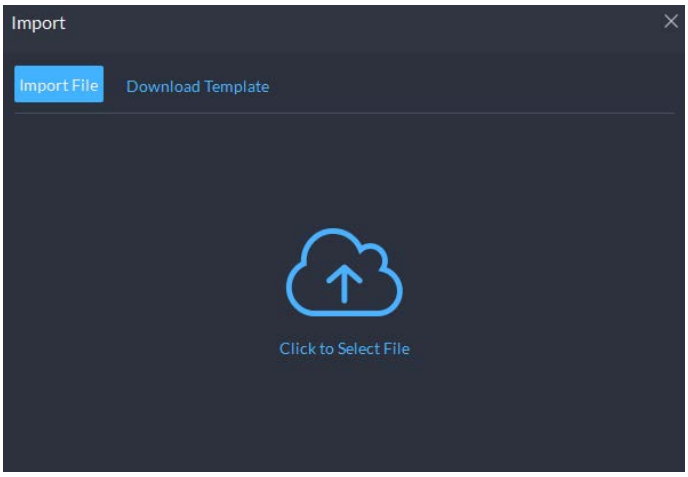
To quickly add a number of personnel, you can download a personnel template, fill in it and then import it to the platform. You can also import an existing personnel file.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Personal and Vehicle Info**.

Step 2 Click .

Step 3 Select **Import** > **Inport from File**.

Figure 4-28 Import personnel information



Step 4 Import the personnel information file.

If there is no personnel information file, click **Template Download** and follow the instructions on the interface to create personnel information.

Step 5 Click **OK**.

The following cases might occur during an import:

- If there are failures, you can download the failures list to view details.
- Read carefully the instructions in the template to make sure all the information is correct.
- Cannot read the contents with a parsing error reported directly.

- Export personnel information.
  Select an organization, click **Export**, and then follow the instructions on the interface to save the exported information to a local disk.
- Download template

To add personnel information in batches, you can download the template, fill in the information, and then import it.

4.3.1.2.3 Extracting Personnel Information

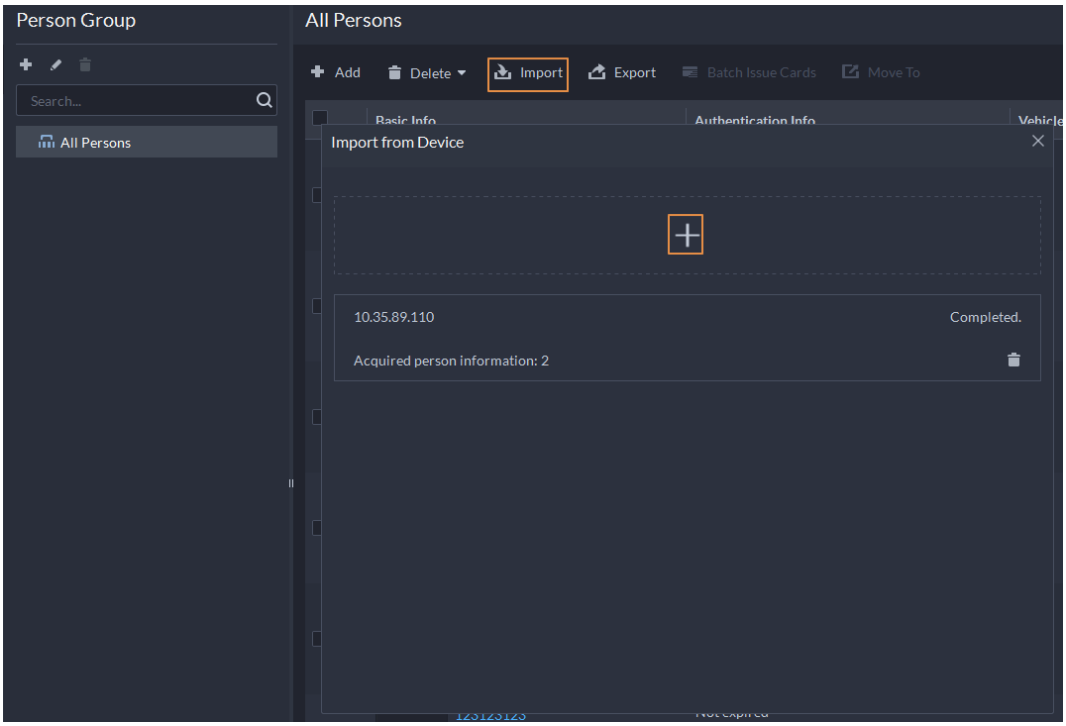
When personnel information has been configured on the devices, you can directly synchronize personnel information from the devices.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Personal and Vehicle Info**.

Step 2 Click .

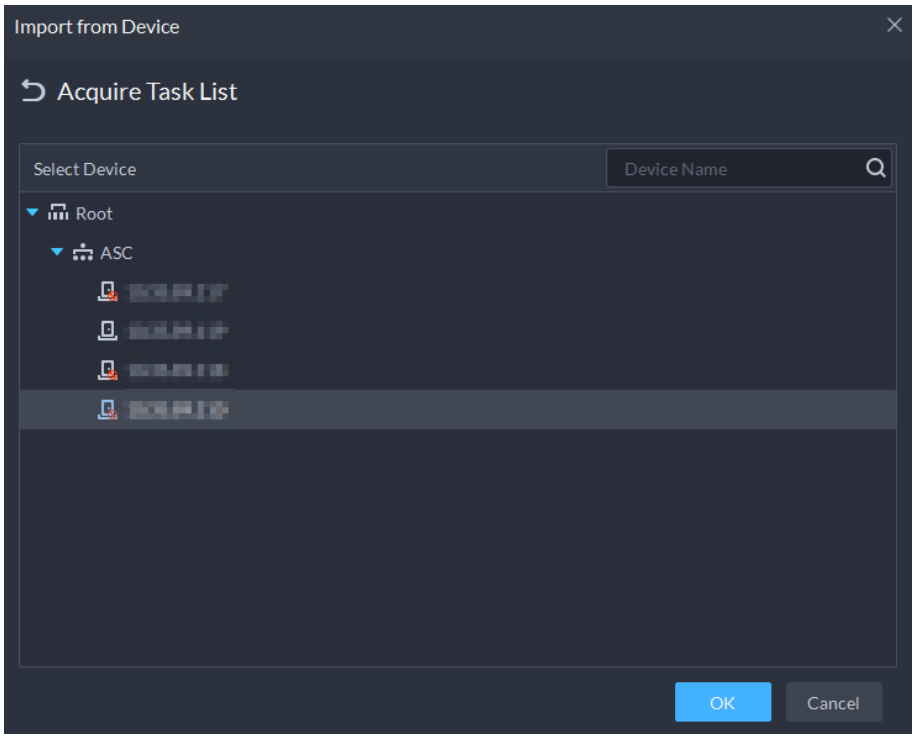
Step 3 Click **Import**, and then select **Import from Device**.

Figure 4-29 Import from device



Step 4 Click , select devices need to be extracted, and then click **OK**.

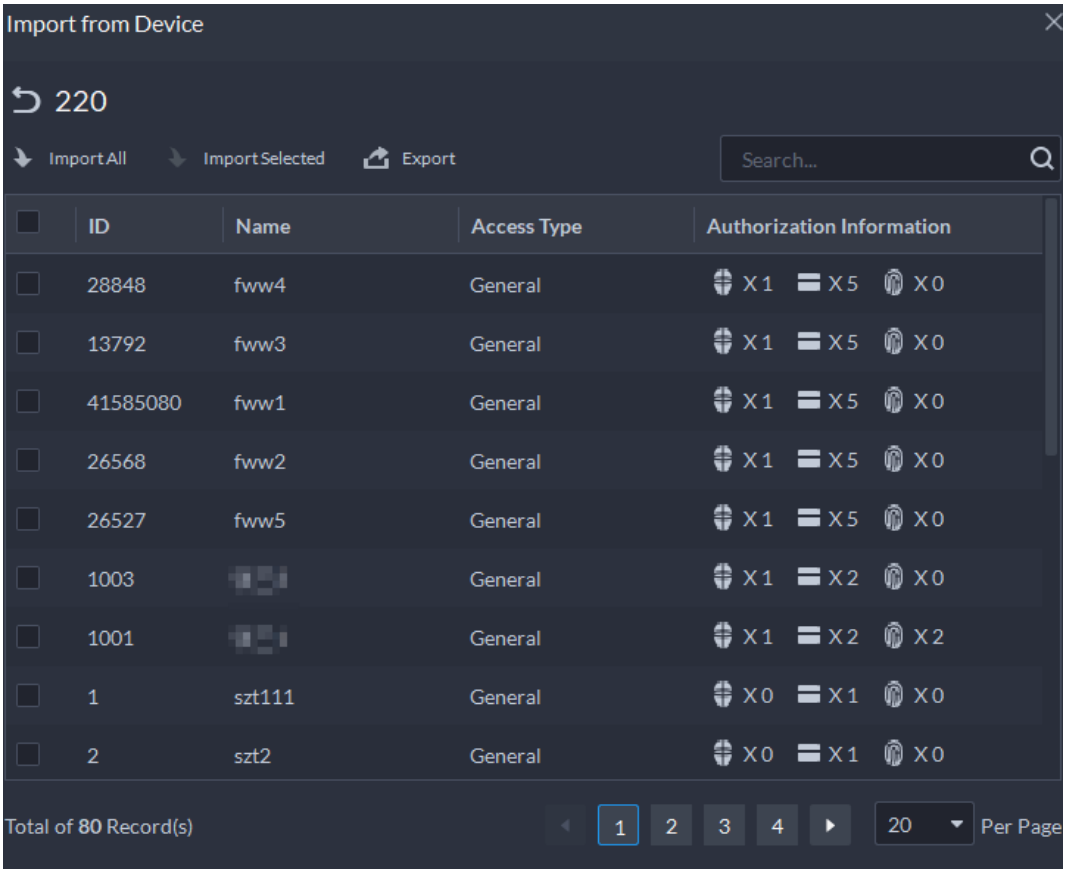
Figure 4-30 Extract task list



Step 5 Double-click a result to view the detailed information.

Step 6 Synchronize personnel information to the platform, or export information.

Figure 4-31 Personnel extraction results



- To add all the personnel information to the platform, click **Import All**.
- To add part of the information, select the people of interest, and then click **Import selected.**

- To export information, select the people you want, and then click **Export**.

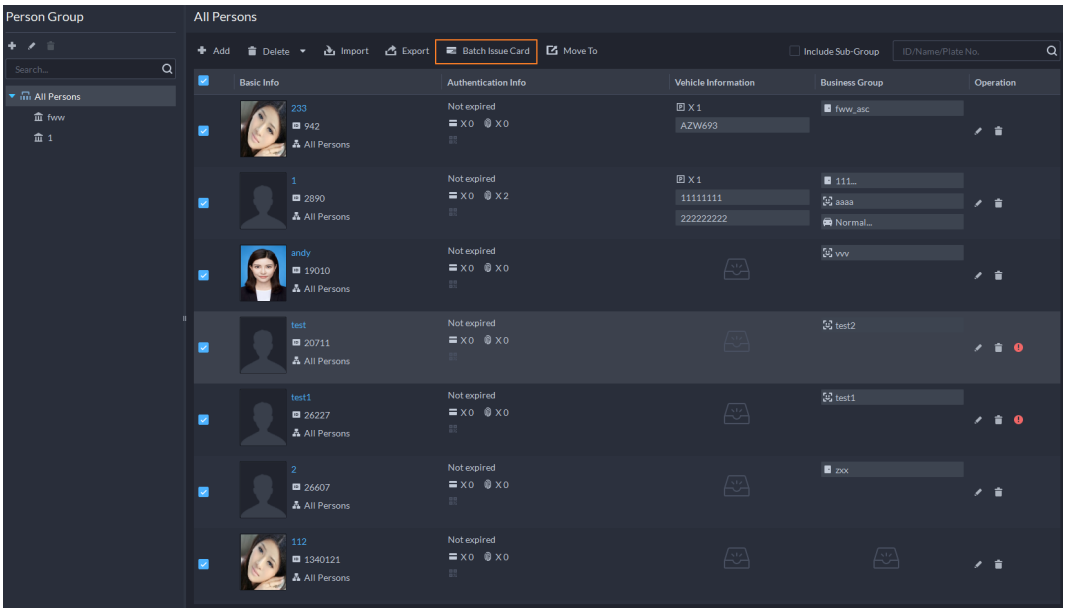
4.3.1.3 Issuing Cards in Batches

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Personal and Vehicle Info**.

Step 2 Click .

Step 3 Select the people to issue card to, and then click **Batch Issue Card**.

Figure 4-32 Issue card in batches



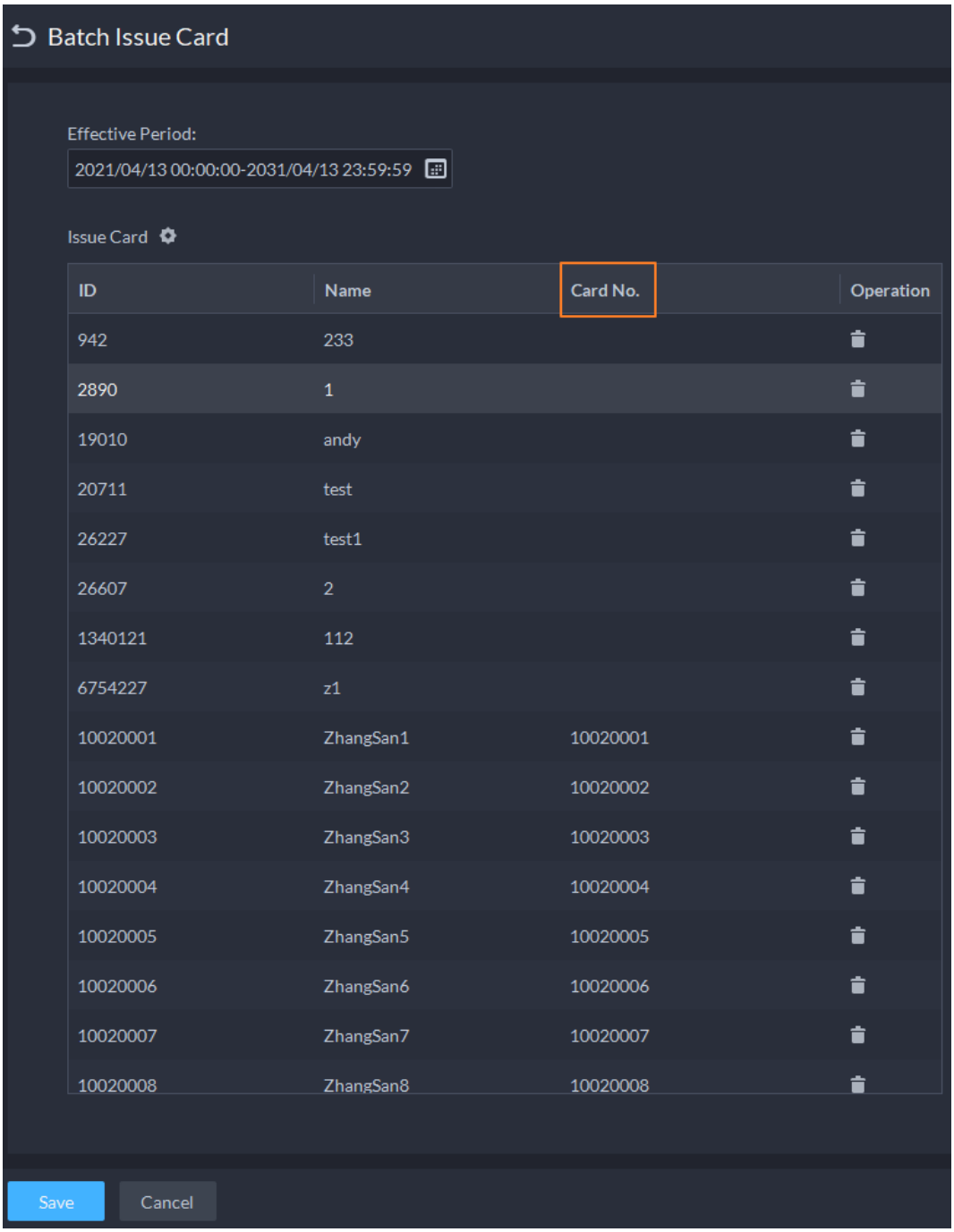
Step 4 Set term of validity.

Step 5 Issue cards to personnel.

Step 6 Support issuing cards by entering card number or by using a card reader.

- By entering card number

Figure 4-33 Enter card number

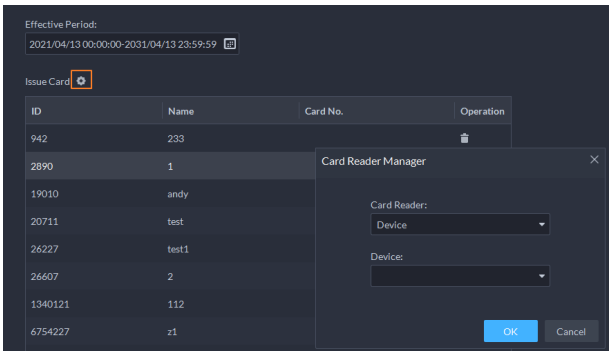


1) Double-click the **Card No.** input boxes to enter card numbers one by one.
2) Click **OK**.

- By using a card reader

1) Click .
2) Select a card reader or device, and then click **OK**.

Figure 4-34 Reader manager



3) Select people one by one and swipe cards respectively until everyone has a card number.
4) Click **OK**.

4.3.1.4 Editing Personnel Information

Modify personnel information including basic information, authentication details, and authorization. Person ID cannot be modified.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Configuration** section, select **Personal and Vehicle Info**.

Step 2 Click .

Step 3 Click to edit information. For details, see "4.3.1.2.1 Adding a Person".

4.3.2 Vehicle Management

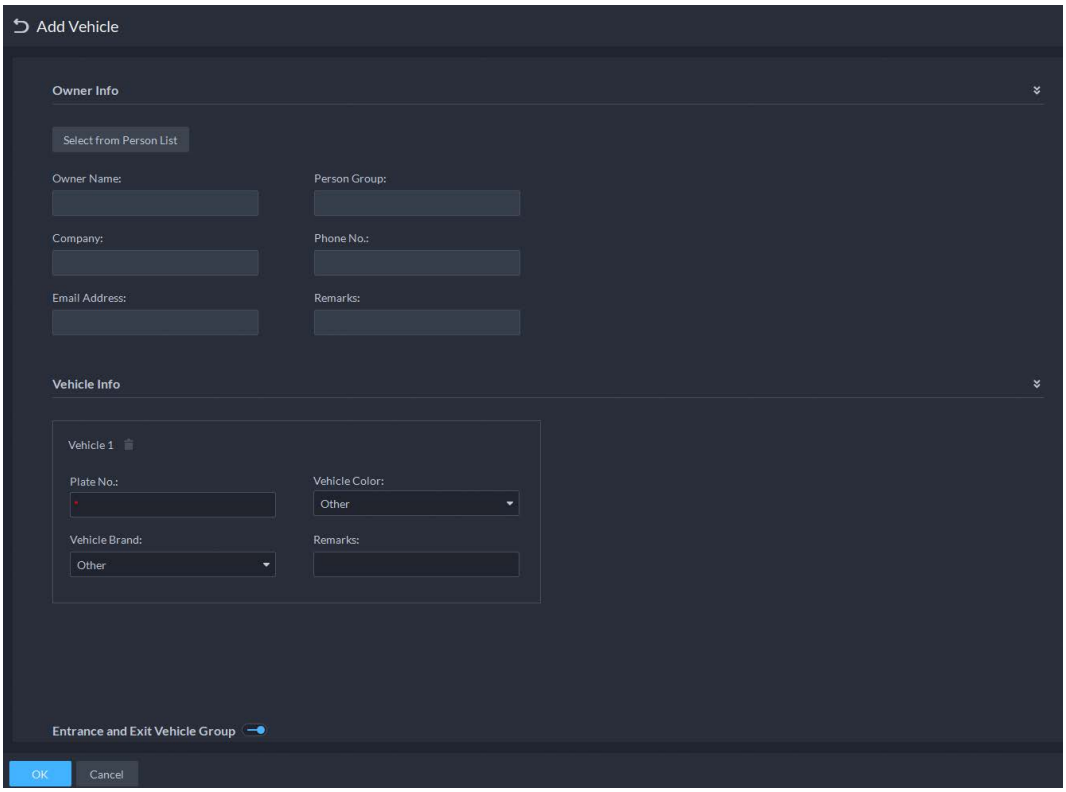
Manage vehicle information including vehicle type, owner, entry and exit permissions and arming groups.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Configuration** section, select **Personal and Vehicle Info**..

Step 2 Click .

Step 3 Click **Add** to add vehicle information.

Figure 4-35 Add vehicle information

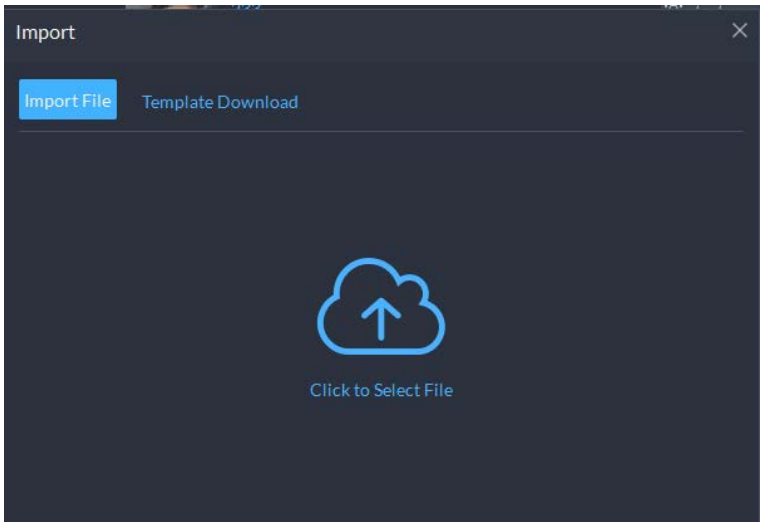


- Add vehicles one by one
  1. Enter **Owner Info** of the vehicle by clicking **Select from Person List**.
  2. Enter **Vehicle Information** such as plate number (required and unique), vehicle color, brand and more. After selecting owner, you can add multiple vehicles.
  3. Click to enable **Entrance and Exit Vehicle Group**, and then you can set the available parking spots for the selected person, and grant access permissions by adding vehicles into entrance and exit vehicle groups.

     If the owner has more vehicles than the set parking spots, once no parking spots available, owner cannot access the parking lot.
  4. Click to enable **Vehicle Arming Group**, and then click **Add** to arm the vehicles you have just added.

     For arming group details, see "4.4.2.1 Creating Vehicle Arming Group".
- Add vehicles in batches
  1. Click **Import** at the top, and then click **Template Download**.

Figure 4-36 Download template



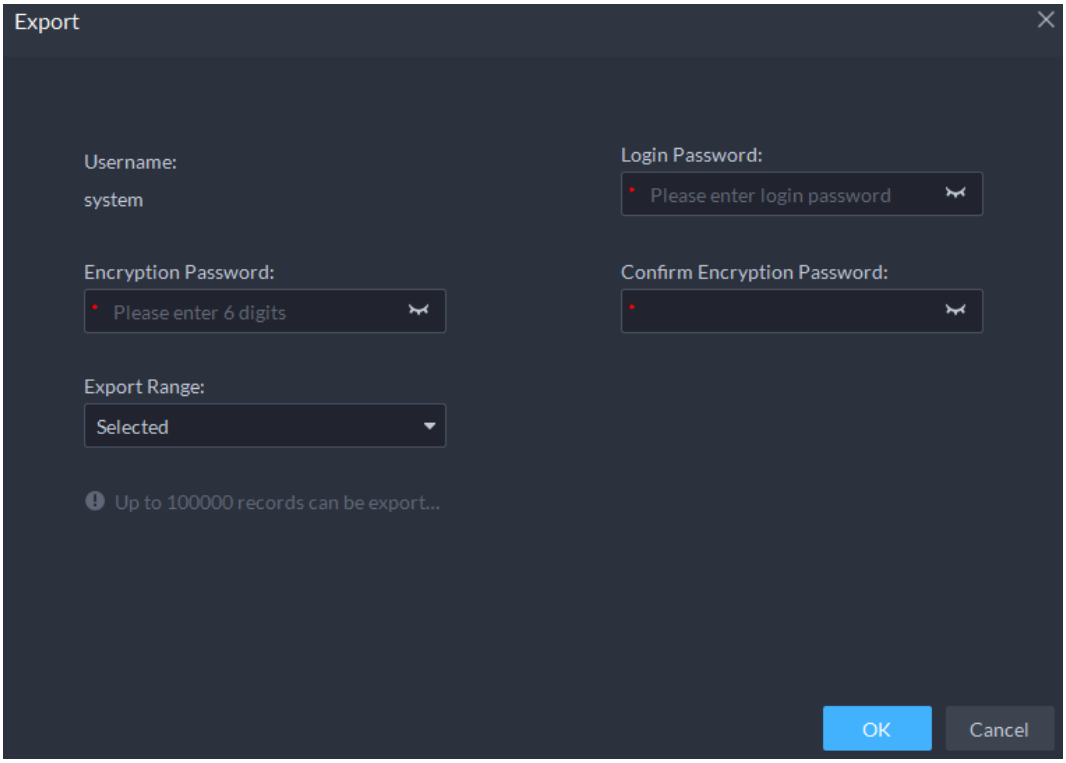
2. Fill in the template, and then select **Import** > **Import File**. Click to select the file and import.

   The platform supports downloading files that failed to import for you to check and fix.

Step 4 Click **OK**.

Step 5 (Optional) You can export vehicle information to local storage as needed.

Figure 4-37 Export vehicle information



- Click **Export** and then enter required information, such as passwords for login and encryption, to export all the items.
- Select vehicles, and then click **Export** to export only the selected information.

Related Operations

- You can search vehicles by entering keywords in search box at the upper-right corner.

- Click or double-click the column to edit the vehicle information.
- Click to delete vehicles one by one. You can also select multiple vehicles and then click **Delete** at the top to delete in batches.

4.4 Watch List Configuration

Configure face and vehicle watch list for future investigation.

- For face watch list, you can create and arm face comparison groups to recognize faces.
- For vehicle watch list, you can create vehicle comparison groups, add vehicles and then link devices for plate recognition.

4.4.1 Face Watch List

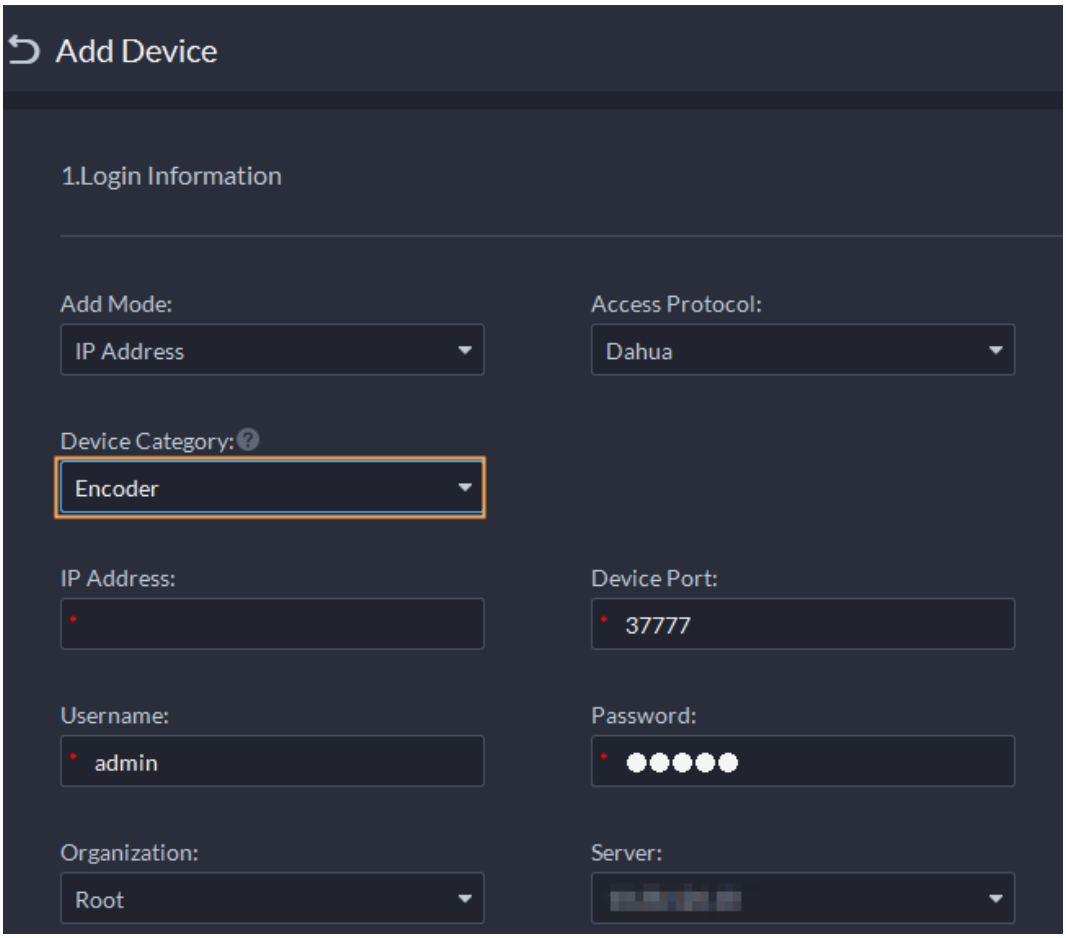
Configure face watch list and issue the list to devices for recognition and alarm.

4.4.1.1 Creating Face Comparison Group

Prerequisites

- Make sure that the devices for face recognition have been successfully configured onto the Platform.
- Make sure that the basic configuration of the Platform has completed. For details, see "3 Basic Configurations". During the configuration, you need to pay attention to following parts.
  - ◇ When adding devices on the **Device** interface, set the **Device Category** to **Encoder**.

Figure 4-38 Device category



◇ When adding devices like NVR or IVSS which supports face recognition, set the device feature to **Face Recognition**. For details, see "3.2.2.5 Editing Devices".

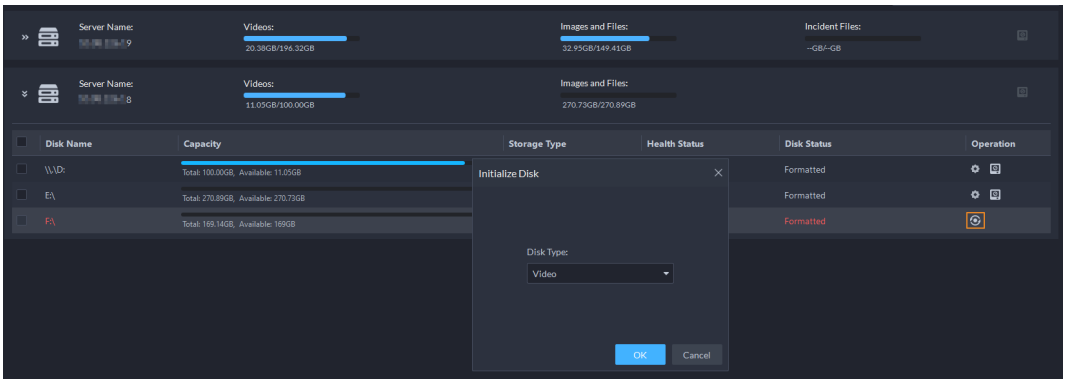
Figure 4-39 Feature configuration

◇ When adding face recognition or face detection camera, edit the camera properties and set the camera feature to **Face Recognition**. For details, see "3.2.2.5 Editing Devices".

The platform reads the camera feature after successfully added.

◇ Make sure that you have configured at least one disk with the type of **Face/Alarm and Other Pictures** to store face images. Otherwise, the snapshots cannot be displayed.

Figure 4-40 Disk type configuration

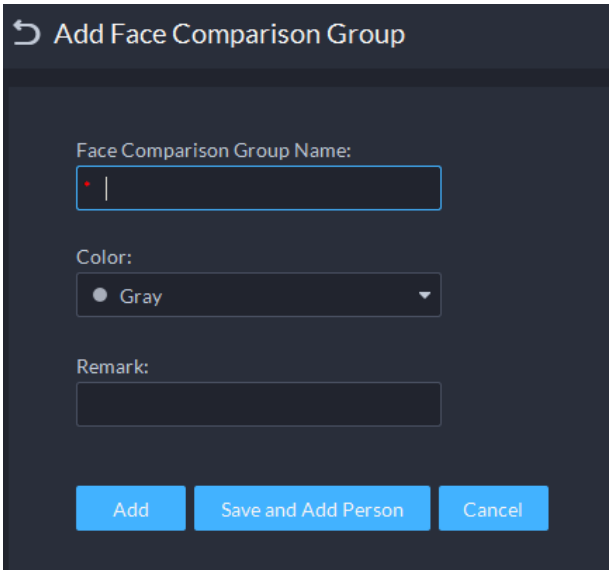


Procedure

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then click **Watch List**.

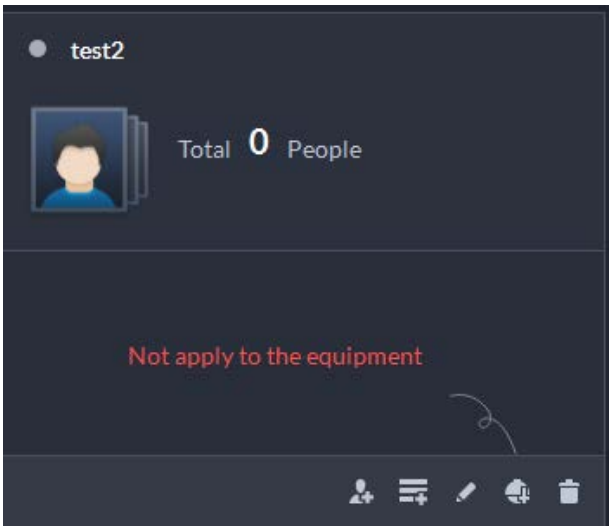
Step 2 Click , and then click **Add** at the upper-left corner to add face comparison group.

Figure 4-41 Add face comparison group



Step 3 Enter the required information, and then click **Add**.

Figure 4-42 Group added



Related Operations

- You can search groups by entering key words in the search box at the upper-right corner.

- Click to edit the group.
- Click to delete the group.

4.4.1.2 Adding Face

Add person in the created comparison group.

Procedure

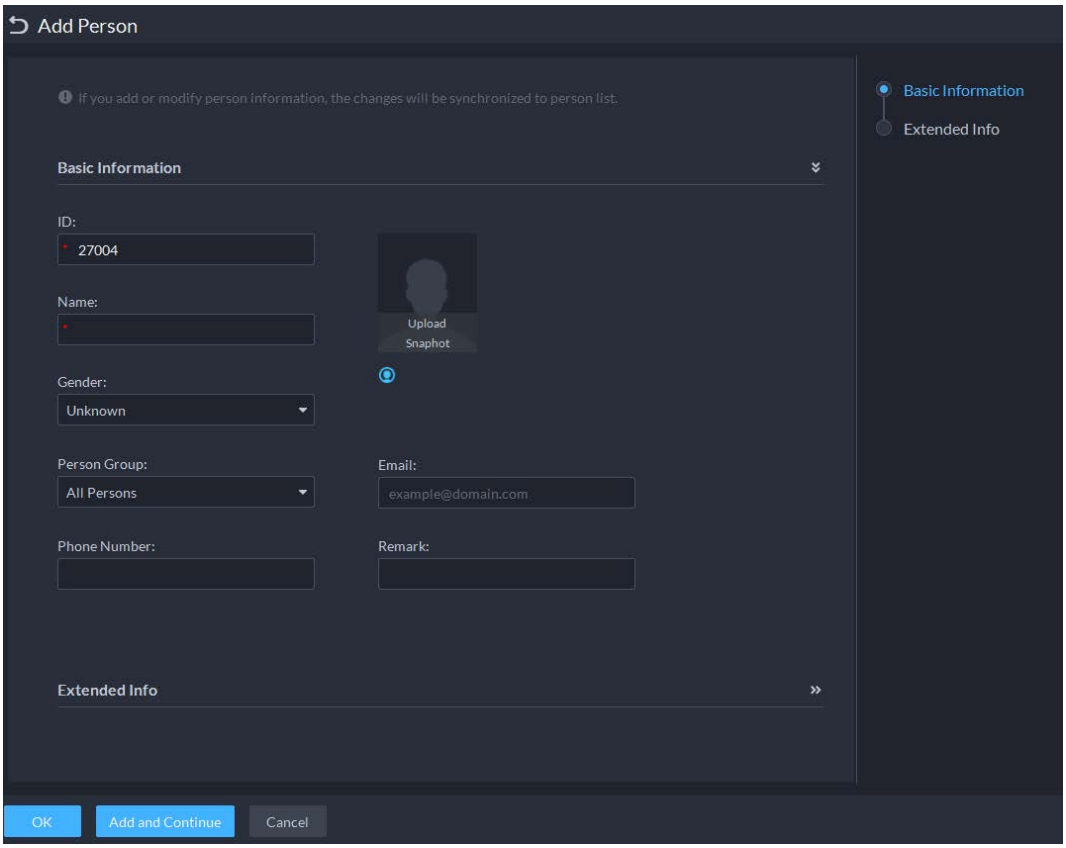
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then click **Watch List**.

Step 2 Click , and then double-click the created group to add people.

Step 3 Click **Add** at the upper-left corner, enter required information and then click **OK** to add faces into the group or click **Add and Continue** to add more people.

- Enter basic information of the person such as ID (required and unique), name, gender and more.
- Move your mouse to the image section, click **Upload** to select an image from local storage. You can also click **Snapshot** to take a face photo on the spot if your PC supports camera function.
  - You can configure the capture parameters on the **Snapshot** interface, such as camera, resolution and more. The configurations are only effective for the current client.
  - Certain devices support two face images for more accurate recognition. means no uploaded face image and means uploaded.

Figure 4-43 Add a person

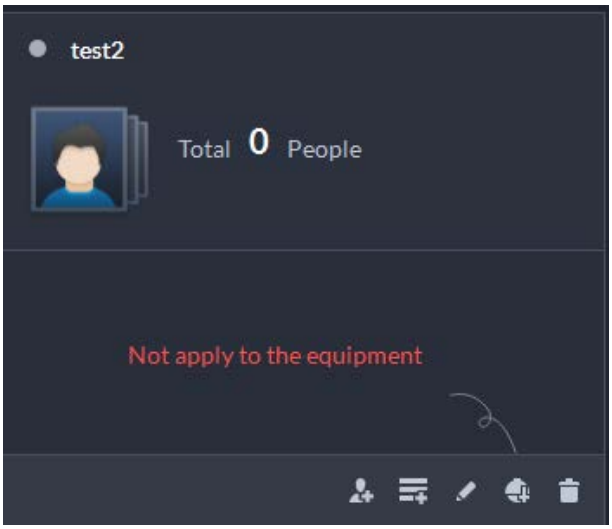


Step 4 Click to display and enter the **Expanded Info**, including nickname (display in VTO contact), address, ID type and more.

Step 5 Click **OK**.

- Click at the bottom of the created group to add one by one.
- Click at the bottom of the created group to **Select from Person List**.

Figure 4-44 Person added



Related Operations

- You can search faces by entering key words in the search box at the upper-right corner.
- Click to edit the person information.
- Click to delete person from the group and face library one by one.
- Click to remove person from the group but keep it in the face library. You can also select multiple people and then click **Remove** at the top to remove in batches.

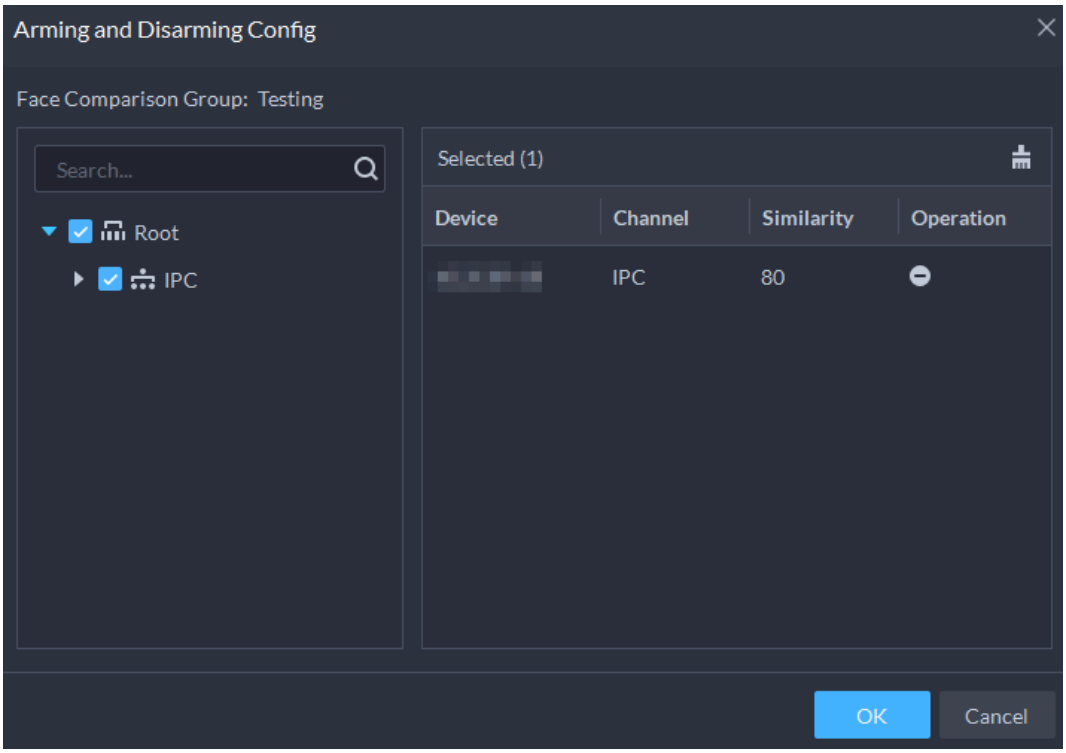
4.4.1.3 Arming Face

Arm the added faces to specified devices for future recognition and alarm.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then click **Watch List**.

Step 2 Click , and then click of a group to arm faces.

Figure 4-45 Arm faces



Step 3 Select devices, and set similarity for each device.

When the device captures a face which exceeds the defined similarity, an alarm is triggered and reported to the Platform.

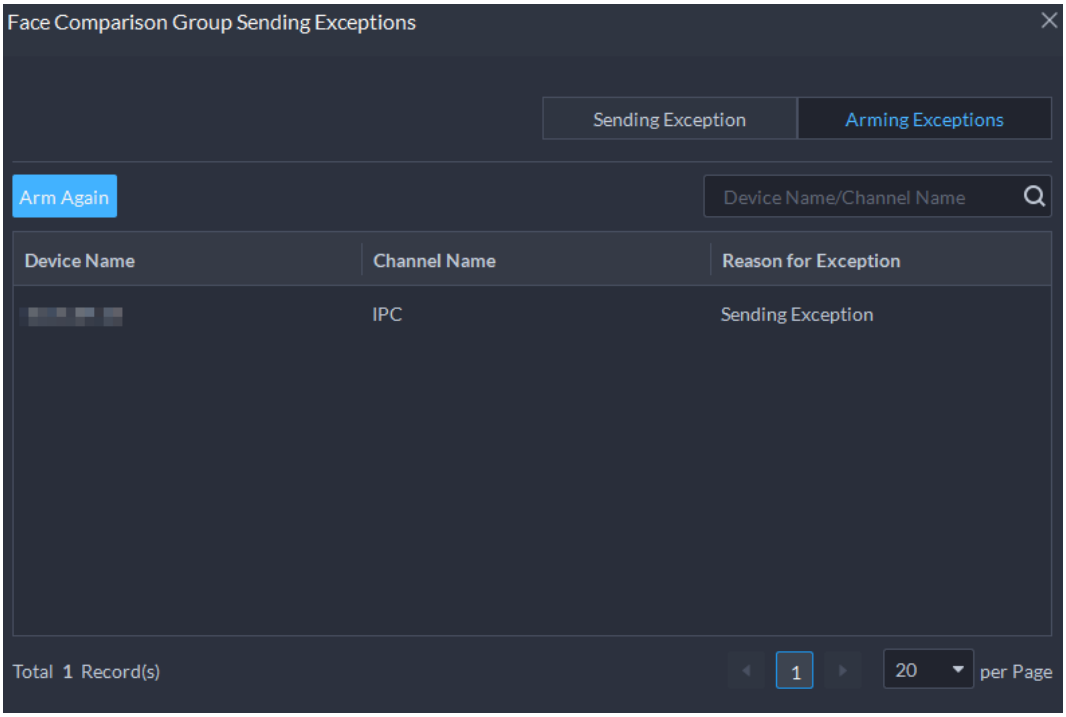
Step 4 Click **OK**.

The platform issues the faces to the added devices.

Step 5 (Optional) If appears at the bottom of the group. It means that the platform failed to issue faces or there are arming exceptions.

1. Click to view the failures.

Figure 4-46 Failure



2. Click **Arm Again** to arm the faces in the group again.

You can also see handle the exception on **Person and Vehicle Info** > **Person List**. Click of a person you failed to arm to view the reason.

4.4.2 Vehicle Watch List

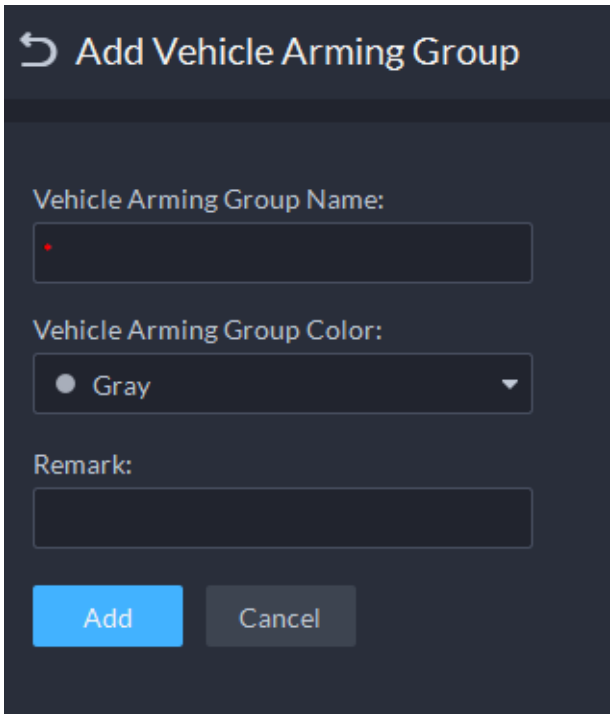
Create vehicle comparison group and add vehicles in, together with **Event** configuration, you can link devices like ANPR camera to recognize and reports to the Platform.

4.4.2.1 Creating Vehicle Arming Group

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then click **Watch List**.

Step 2 Click , and then click **Add** on the upper-left corner to add a vehicle arming group.

Figure 4-47 Add a vehicle arming group



Step 3 Enter the required information, and then click **Add**.

Related Operations

- You can search groups by entering key words in the search box at the upper-right corner.
- Click to edit the group.
- Click to delete groups one by one. You can also select multiple groups and then click **Delete** at the top to delete in batches.

4.4.2.2 Adding Vehicles

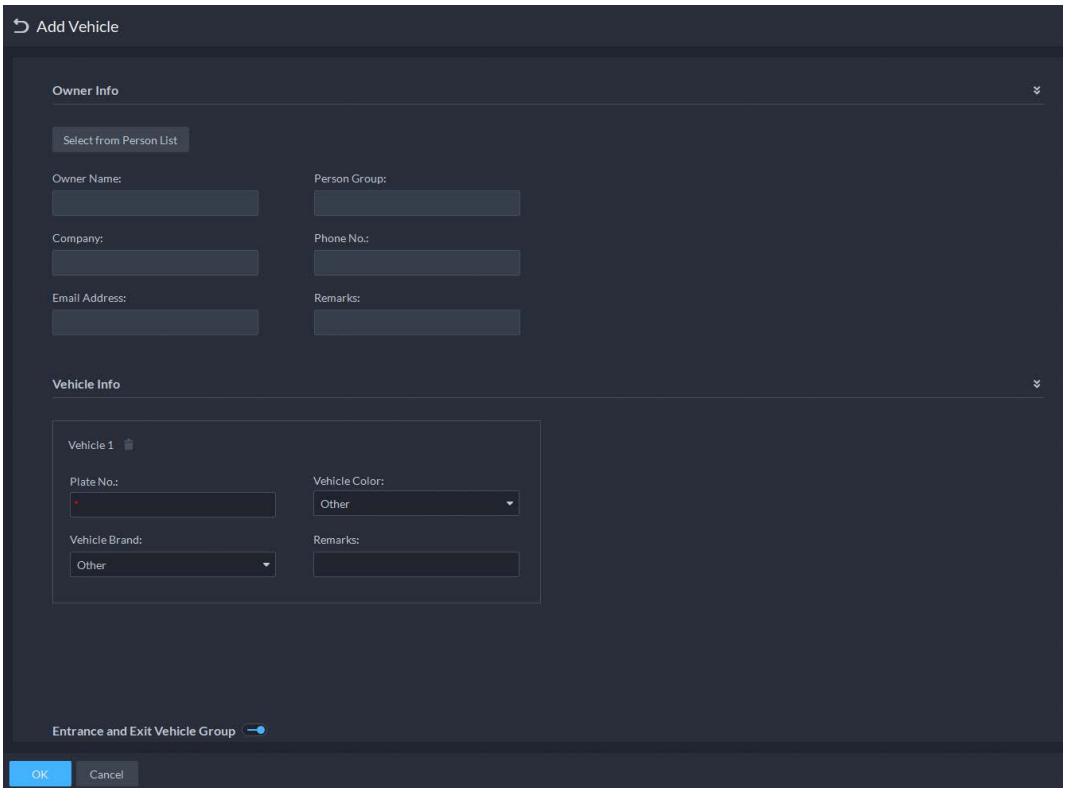
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then click **Watch List**.

Step 2 Click , and then double-click the created group to add vehicles.

- Click at the bottom of the created group to add one by one.
- Click at the bottom of the created group to **Select from Vehicle List**.

Step 3 Click **Add** at the upper-left corner, enter required information and then click **OK** to add vehicles into the group.

Figure 4-48 Add vehicles



1. Enter owner information of the vehicle by clicking **Select from Person List**.
2. Enter vehicle information such as plate number (required and unique), vehicle color, brand and more. After selecting owner, you can add multiple vehicles.
3. Click to enable **Vehicle Arming Group**, and then click **Add** to arm the vehicles you have just added.

Step 4 Click **OK**.

Related Operations

- You can search vehicles by entering search conditions on the left side.
- Click to edit the vehicle information.
- Click to delete vehicles from the group and vehicle database one by one. You can also select multiple vehicles and then click next to **Remove** at the top to delete in batches.
- Click to remove vehicles from the group but keep it in the vehicle database. You can also select multiple vehicles and then click **Remove** at the top to remove in batches.
- Click **Operation** at the upper-right corner to select displaying items of vehicle information.

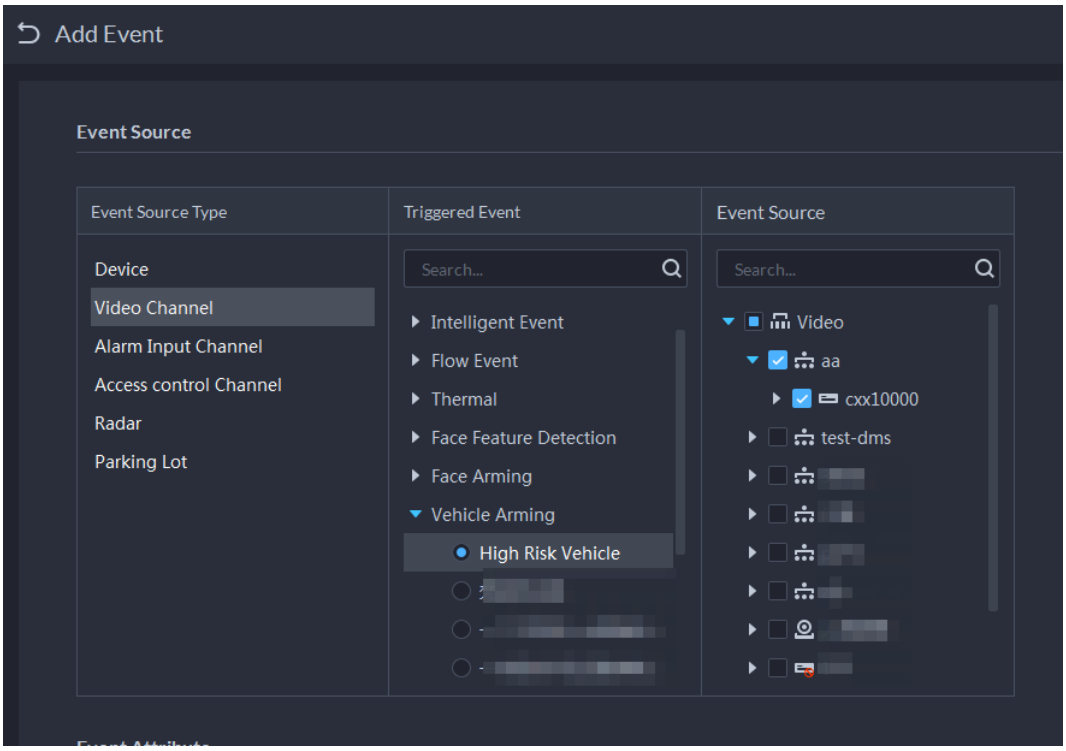
4.4.2.3 Arming Vehicles

Link ANPR camera or other devices which support plate recognition to arm watched vehicles in real time. Once matched vehicles are detected, an alarm is triggered and reported to the Platform.

Log in to the DSS Client. On the **Home** interface, click , and then arm the vehicle on the **Event** interface. For details, see "4.1 Configuring Events".

Click **Add**.

Figure 4-49 Arm vehicle event



4.5 Access Control

- Access control
  Issue cards, collect fingerprints and face data, and apply permissions, so that the authorized people can open door by using card, face or fingerprint.
- Advanced functions
  Configure advanced access control rules such as First-card Unlock, Multi-card Unlock, Anti-pass Back and Interlock to enhance security.

4.5.1 Preparations

Make sure that the following preparations have been made:

- Access control devices are correctly deployed. For details, see the corresponding user's manual of the device.
- Basic configurations of the platform have been finished. See "3 Basic Configurations" for details.
  - When adding access control devices, select **Access Control** for device category.
  - (Optional) On the **Bind Resource** interface, bind video channels for access control channels.
  - Personnel information is added correctly. For details, see "4.3 Personnel and Vehicle Information Management".

4.5.2 Configuring Door Groups

Configure door groups to include access permission of one or more access control devices.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Access Control**.

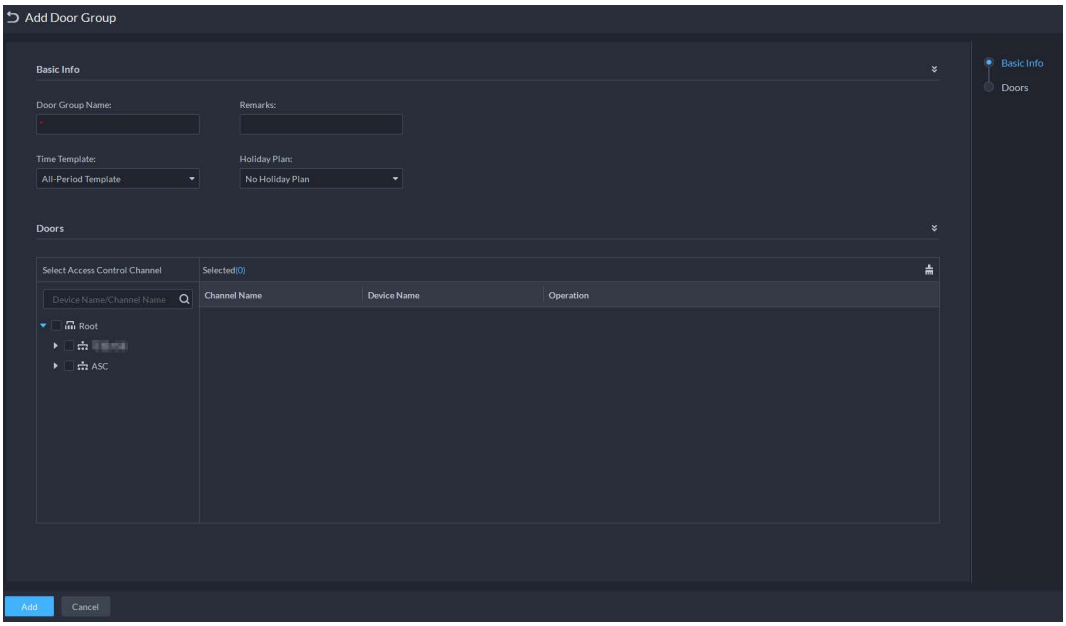
Step 2 Click .

Step 3 Create a door group.

1) Click **Add** at the upper-left corner, or the **Add Door Group** tab.
2) Enter the group name, select a time template and a holiday schedule, select a device channel, and then click **OK**.

   After the time template and device channel are selected, the permission assigned to personnel is valid only for period of the selected time template of the selected device channel.

Figure 4-50 Add a door group



Step 4 Authorize.

1) On the **Access Permission Group** interface, select a door group, and then click the corresponding icon.
2) Select personnel, and then click **OK**.

4.5.3 Configuring Access Permission Groups

Configure access permission groups so that you can quickly assign access permissions by door groups.

Procedure

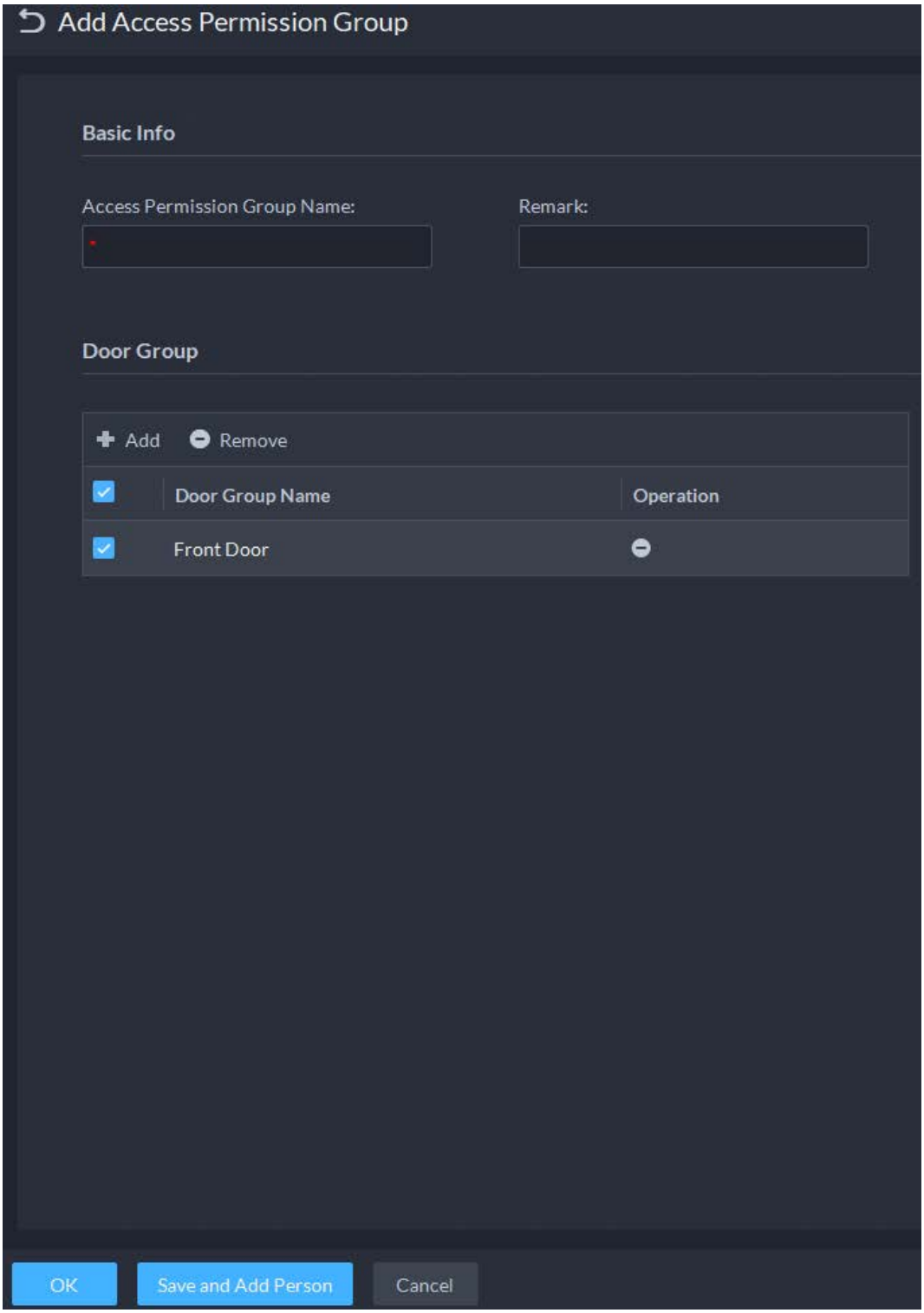
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Access Control**.

Step 2 Click .

Step 3 Create an access permission group.

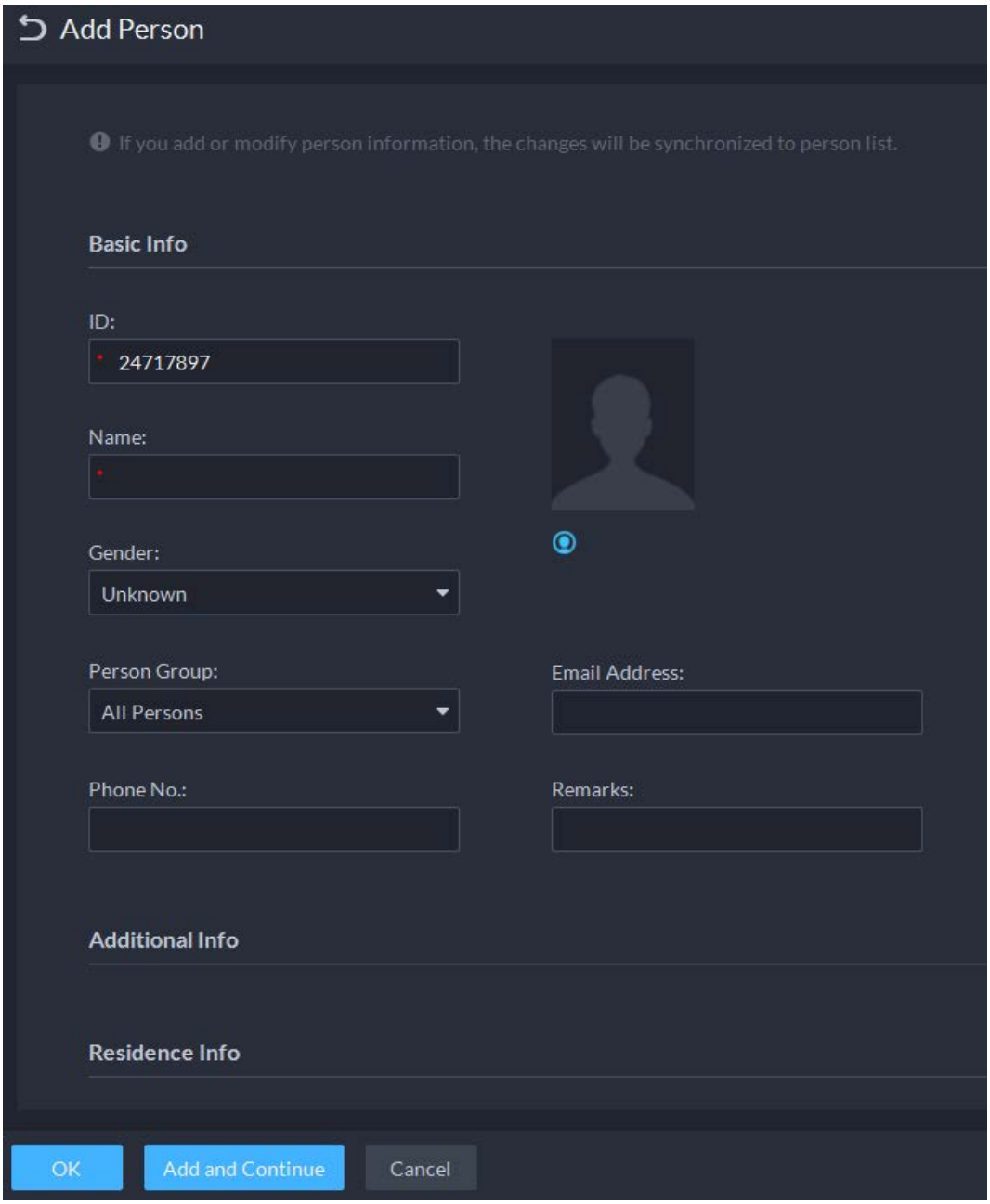
1) Click **Add** at the upper-left corner.

Figure 4-51 Add an access permission group



2) Enter the group name, and then select the door groups as needed.
3) Click **Save and Add Person**.

Figure 4-52 Add a person



4) Enter the information from different sections. See "4.3.1.2.1 Adding a Person" for details.
5) Click **Add and Continue**, and then click **OK**.

Related Operations

- Enter keywords in the search box at the upper-right corner, and then press the Enter key to search for the groups you want.
- Double-click a group, and then click **Add** to add people. You can also click or to add people to a group.
- Click to edit the name and door groups of a group.
- Click to delete a group; select the groups as needed, and then click **Delete** to delete them all.

4.5.4 Configuring Public Passwords

Anyone with a pubic password can unlock associated doors. You can add up to 100 passwords.

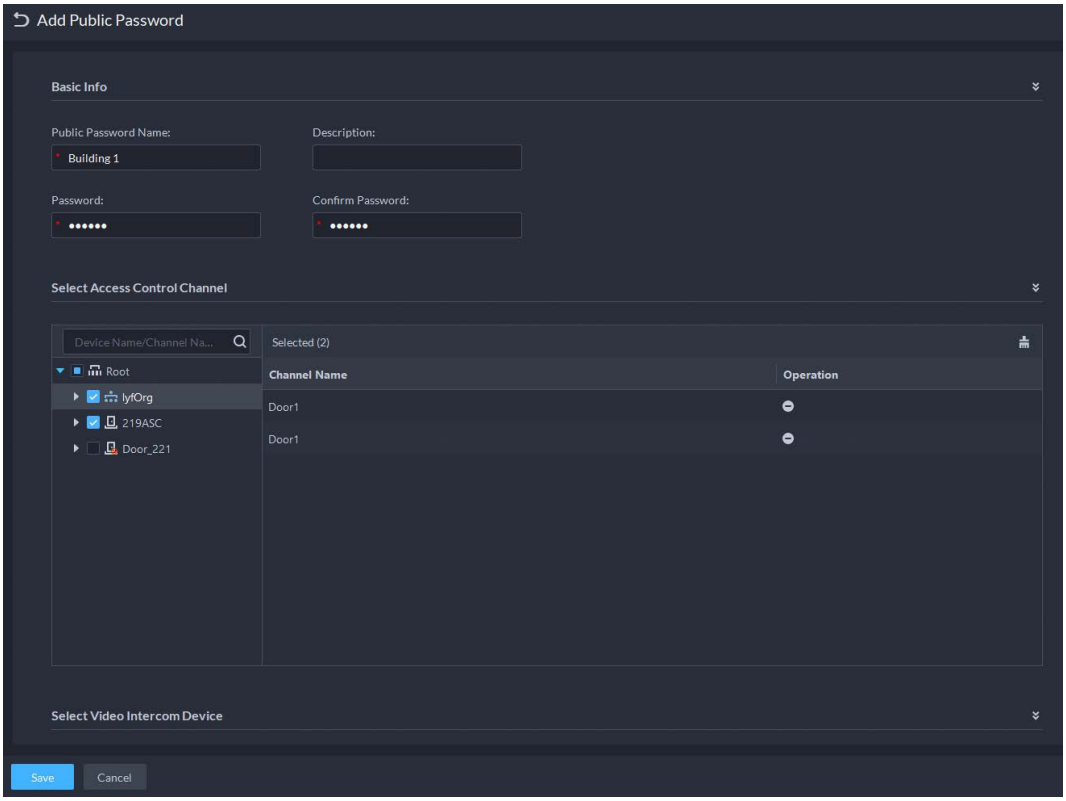
Only second-generation access control devices and video intercom devices support this function.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Access Control**.

Step 2 Click .

Step 3 Click **Add**, enter a name, set password, and then select access control channels.

Figure 4-53 Add a public password



Step 4 Click **Save**.

4.5.5 Configuring Time Templates

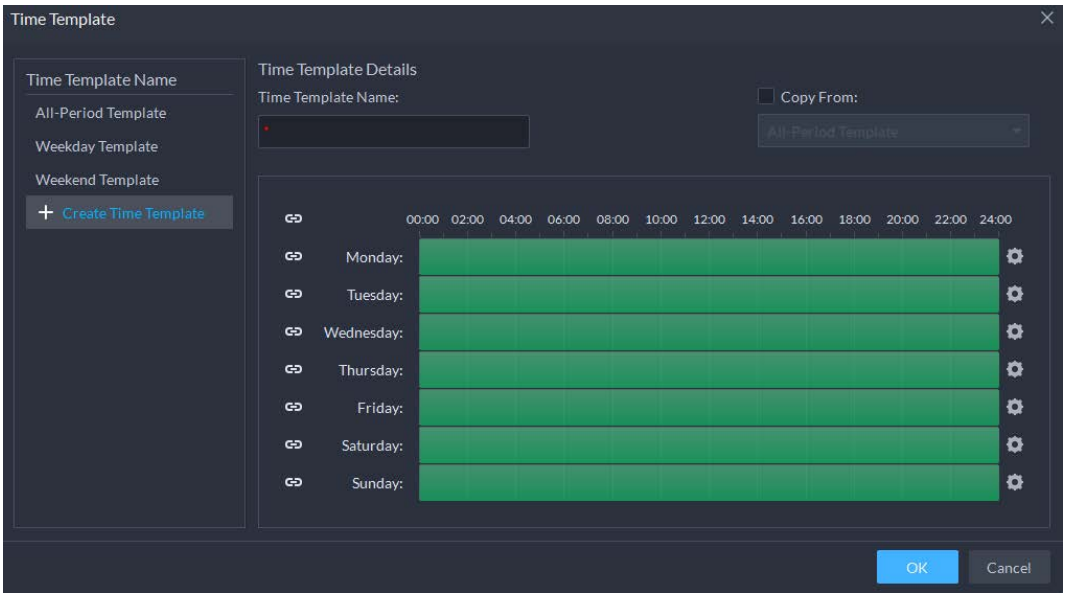
Configure time templates for different access control strategies. For example, you can create a template that first-card unlock is only valid within the periods you defined.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Access Control**.

Step 2 Click .

Step 3 Click **Create Time Template** from the **Time Template** drop-down list when adding or editing a door group.

Figure 4-54 Time template



Step 4 Enter the template name, set time periods, and then click **OK**.

There are two ways to set time periods:

- Drag your mouse cursor on the time bars to select time sections. To remove a selected time section, click on the time bar and drag.
- Click , and then set time periods in the **Period Setup** dialog box. You can add up to 6 periods.

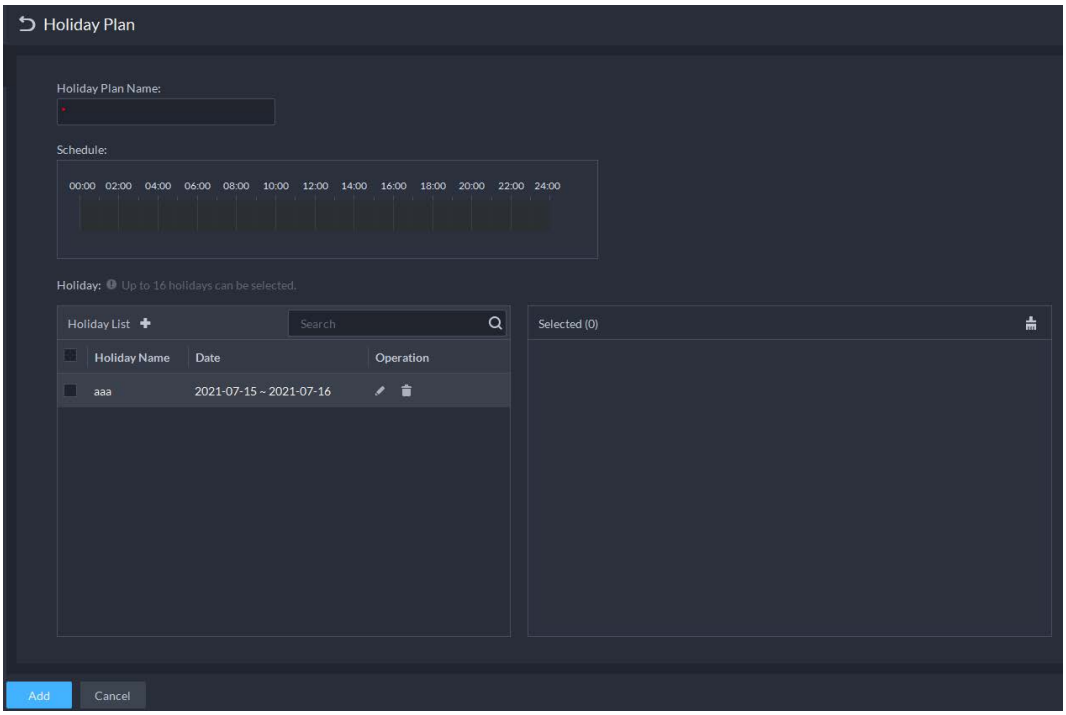
To use an existing template, select the **Copy From** check box and then select a template in the drop-down list.

4.5.6 Configuring Holidays

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Access Control**.

Step 2 Click **Add Holiday Schedule** from the **Holiday Schedule** drop-down list when adding or editing a door group.

Figure 4-55 Add a holiday schedule



Step 3 Configure the parameters.

1. Enter a holiday schedule name.
2. Configure the periods in the **Schedule** section.
3. Click to add a holiday: Enter the holiday name, set a start date, and how many days this holiday lasts, and then this holiday will be effective within the periods you set from the previous step.

Step 4 Click **Add**.

4.5.7 Configuring Access Control Devices

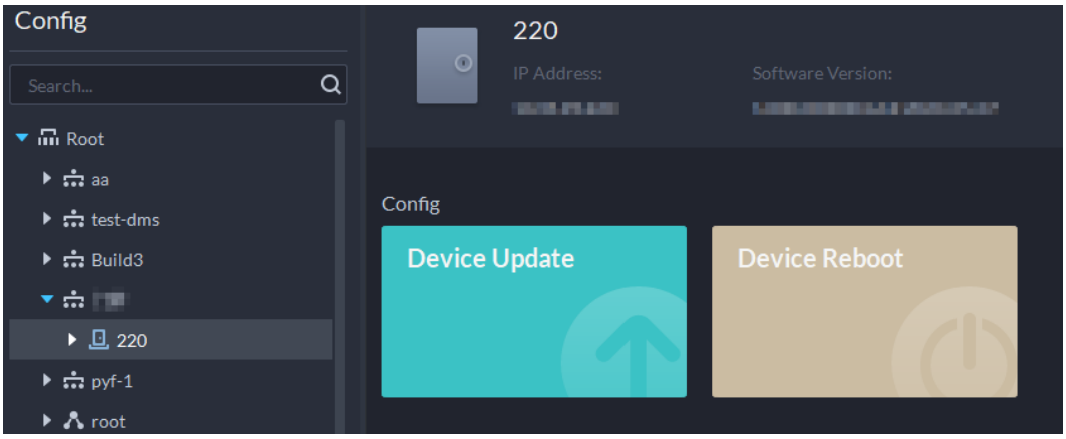
After an access control device is added, and if it is online, you can restart and upgrade it, and synchronize device time.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Select an access control device from the device tree.

Figure 4-56 Select an access control device



Step 4 Configure access control devices.

- Click **Device Reboot** to restart the device.
- Click **Device Update**, select the update file, and then click **Upgrade** to update the device.

To go to the configuration interface of an access controller, click at the upper-right corner.

4.5.8 Configuring Door Information

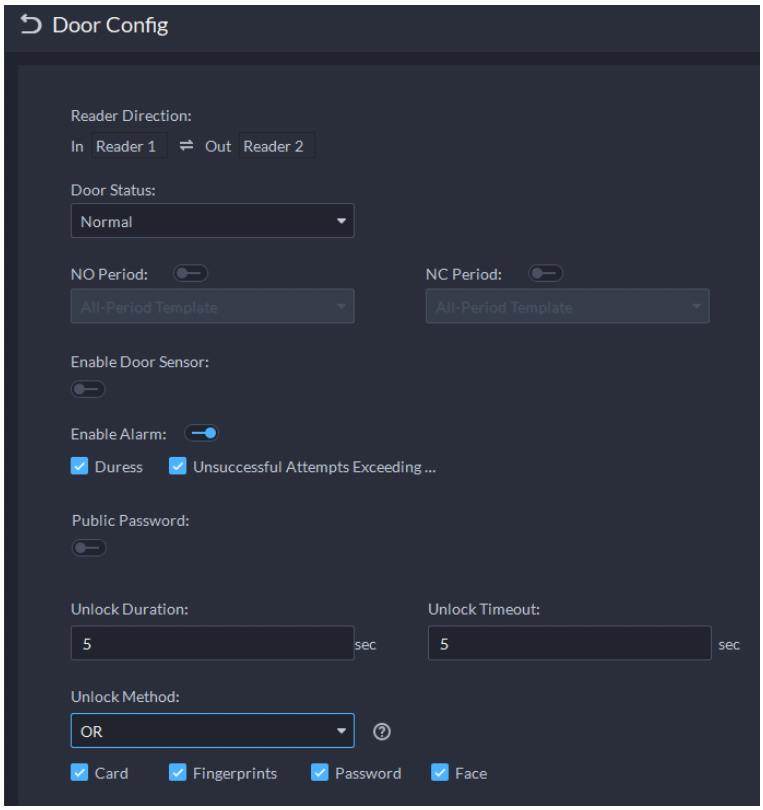
You can configure door status, Always-Open or Always-Close period, alarm and more.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Basic Config** section, select **Device**.

Step 2 Select a door channel in the device tree, and then click **Door Config** on the right.

Step 3 Configure door information, and then click **OK**.

Figure 4-57 Door configuration



The interface is only for reference, and might vary with different access control devices.

Table 4-3 Parameters

Parameter	Description
Set reader direction	Indicates the in/out reader based on the wiring of ACS.
Door Status	Set 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 closed.
Door Sensor Enable	You can only enable intrusion and timeout alarms when the door sensor is enabled.
Enable Alarm	• Intrusion: If the door is unlocked by methods you have not configured, the door contact is split and triggers an intrusion alarm. • Unsuccessful Attempts Exceeding Limit: If failed to unlock the door for certain times, an alarm will be triggered. • Duress: Entry with the duress card, duress password, or duress fingerprint triggers a duress alarm. • Timeout: Unlock duration timeout triggers a timeout alarm.
Public Password	Enable this function, and then you can use a public password to unlock the door. For how to configure a public password, see "4.5.4 Configuring Public Passwords".
Unlock Duration	Sets up for how long the door will unlock. The door locks automatically after the duration.
Unlock Timeout	Unlock duration exceeding the **Unlock timeout** triggers a timeout alarm.

Parameter	Description
Unlock Method	You can use any one of the methods, card, fingerprint, face, and password, or their combinations to unlock the door. ● Select **And**, and select unlock methods. You can only open the door using all the selected unlock methods. ● Select **Or** and select unlock methods. You can open the door in one of the ways that you configured. ● Select **Unlock by period** and select unlock mode for each time period. The door can only be opened by the selected method(s) within the defined period.

4.6 Video Intercom

4.6.1 Preparations

Make sure that the following preparations have been made:

- Access control devices are correctly deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
  - ◇ When adding video intercom devices on the **Device** interface, select **Video Intercom** as the device category.
  - ◇ When adding access control devices that support intercom, select **Device Category** to **Access Control** in **Login Information**, and then select **Door Station access Controller** or **Fence Station Access Controller** according to the type of your device.

- The system creates personnel information automatically when you add VTH. It extracts room number from VTH SIP. This number is used as person ID.
- Any configuration modification on the device will not be reported to the platform. You need to go to the device modification interface of Web Manager to manually synchronize the modification.

4.6.2 Configuring Building/Unit

Make sure the status of building and unit of the DSS client is the same as the VTO. If building and unit are enabled on the platform, they must also be enabled on the device, and vice versa; otherwise, the VTO will be offline after being added. That also affects the dialing rule. Take room 1001 unit 2 building 1 as an example, the dialing rule is as follows after it is enabled:

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

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Video Intercom**.

Step 2 Click .

Step 3 Enable or disable building and unit as required, and then click **OK**.

4.6.3 Setting Private Password

Set room door passwords so that the room door can be opened by entering password on the VTO (outdoor station).

Make sure that contacts are sent to the VTO; otherwise you cannot set private password.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Video Intercom**.

Step 2 Click .

Step 3 Select a VTO, and then you can see all the VTHs linked to this VTO.

Step 4 Select a VTH and click , or select several VTHs and click **Change Password**.

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

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

4.6.4 APP User

You can view information of APP users, freeze user, modify login password and delete user.

APP user can register by scanning the QR code on VTH. For details, see DSS APP User's Manual.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Video Intercom**.

Step 2 Click .

Table 4-4 Parameter description

Operation	Description
Freeze APP user	The APP user cannot log in for 600 s after being frozen. The account will be frozen when invalid password attempts exceeds 5 by an APP user.
Change APP user login password	Click and enter a new password on the **Reset Password** interface, and then click **OK**. ● The password must be 8 to 16 characters and must include numbers and letters. ● Click to display password, or to mask password.
Delete APP user	Click to delete APP users one by one, or select multiple APP users, click **Delete**, and then follow the instructions to delete the users.

4.6.5 Synchronizing Contacts

Synchronize contacts information to VTO and then you can view contacts on the VTO or its web interface.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications**

Config section, select **Video Intercom**.

Step 2 Click .

Step 3 Select an organization node (VTO), and then click **Send Contacts**.

Step 4 Select one or more VTHs as needed, and then click **OK**.

Now you can view contacts on the VTO or web interface.

4.6.6 Call Management

Create device group, management group and relation group respectively and define restricted call relations. This function is only available for the system account user.

Click on the interface of device group, management group or relation group, the system will restore management group and relation group to their original status.

4.6.6.1 Configuring Device Group

VTOs and VTHs can only call each other when they are added into the same device group. DSS will automatically generate corresponding device group when VTO, second confirmation station and fence station are added.

- Add VTOs and access control devices that support intercom, and then a device group will be automatically generated. Add VTHs from the same unit into the group, and realize mutual call between VTH and VTO within the group.
- Add second confirmation stations and automatically generate a device group. Add them to the group together with the VTHs of the same room, and realize mutual call between VTHs and second confirmation stations within the group.
- Add fence stations and automatically generate a device group. Add all the VTHs into the group to realize mutual call between fence stations and all the VTHs.
- Add VTHs. If the VTHs are connected to unit VTO, second confirmation station, fence station, they will be automatically added to the device group, and realize mutual call among unit VTOs, second confirmation stations and fence stations.

  VTHs from different device groups can call each other.

4.6.6.2 Adding Management Group

Management group is to make groups for administrators, and realize relation binding of one to one, one to many or many to many. Administrators include DSS administrator and VTS. If there is a default management group, VTS will be automatically added to the management group when it is added.

- Before configuring management group, you need to create users, select video intercom menu permission and device permission, and add new users to the management group.
- After using system user account to configure group relation, you need to switch to new user to log in. If the system account is logged in on multiple clients, you cannot use it to make calls.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications**

Config section, select **Video Intercom**.

Step 2 Click .

Step 3 Click **Manage** **Group Config**.

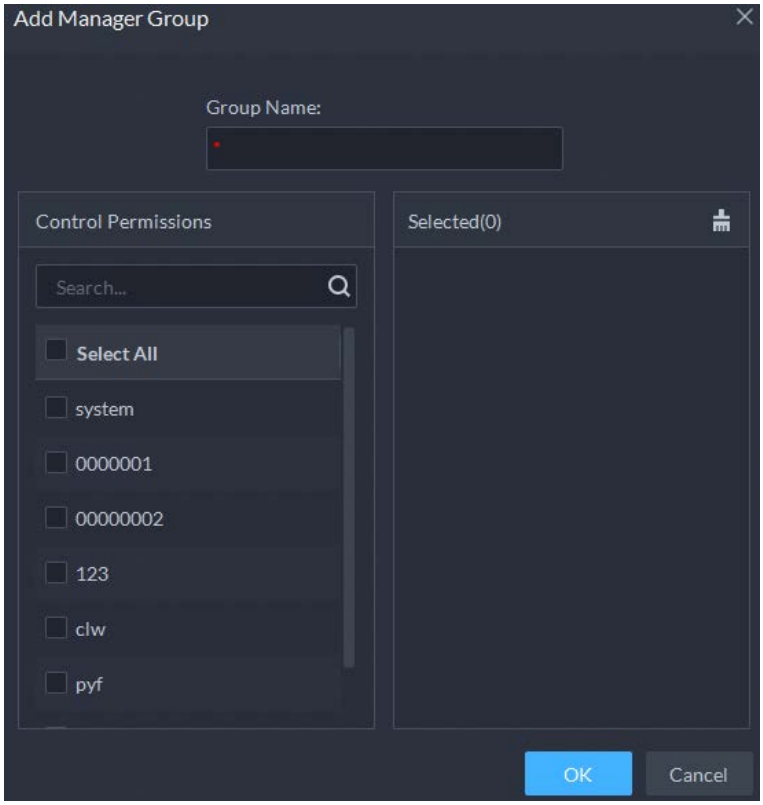
Step 4 Click **Add Group**.

Step 5 Enter group name, select administrator account or VTS, and click **OK**.

The added management group is displayed in the list.

- To transfer members, click and move the member to other groups.
- To manage group members, click to add or delete group members.

Figure 4-58 Edit manager group



4.6.6.3 Configuring Group Relation

Link device groups and management groups, and VTOs or VTHs in a device group can only call administrators or VTSs of a linked management group. There are two situations for creating relation:

- A device group only links to 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 bells will stop as long as there are no administrator answers. The device call request can be rejected as long as all the administrators reject to answer.
- A device group links to 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 no administrator answers, then it will call next management group. The interval between two calls is 30 seconds; it can skip up to one management group. If neither of two groups answer, then the device prompts call overtime, no

response.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Video Intercom**.

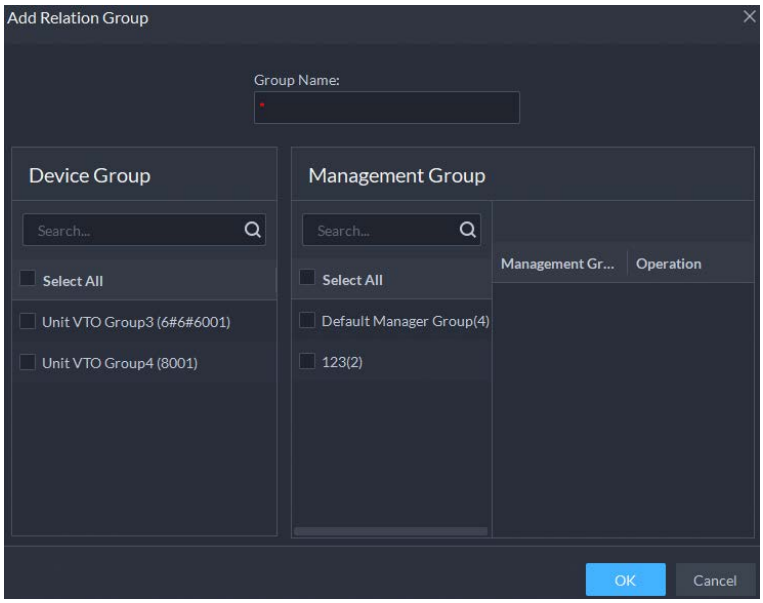
Step 2 Click .

Step 3 Click **Relation Group Config**.

Step 4 Click **Add**.

Step 5 Enter a name, select device group and management group, and then click **OK**.

Figure 4-59 Add a group relation



Added relation group is displayed in the list. If there are several relation groups, you can click or to adjust priority level. When there is a call, the online administrators with the highest priority will generate ring bell first.

4.7 Visitor Management

After appointment is made on platform, and visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves.

4.7.1 Preparations

- Access control devices have been added into the DSS client.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".

4.7.2 Configuring Visit Settings

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Visitor**.

Step 2 Configure the parameters.

- Automatic visit
  Enable the function, and then select the channels as needed. Visitors with appointment

can verify their identities on the selected channels without registering.

- Automatic leave
  - Enable the function, and then select the channels as needed. Visitors who are visiting can verify their identities on the selected channels to end their visits automatically.
  - Sign out regularly: Expired visits will be automatically ended at the defined time point.
  - Daily sign-out time: For visitors who do not arrive for their appointment before the daily sign-out time, their appointment will be cancelled.
  - Sign out now: For visitors who missed their appointment when you click this button, their appointment will be cancelled.
- Default visitor permissions: Set default access permissions for visitors.
- Email template: You can set up an email template and automatically send emails when visitors make an appointment, arrive for their appointment, and end their visit. You can customize the email subject and content with the visitor information, such as visitor's name and ID number.
- Visitor pass remarks: Customize the content of remarks on a visitor pass.

Figure 4-60 Customize visitor pass remarks

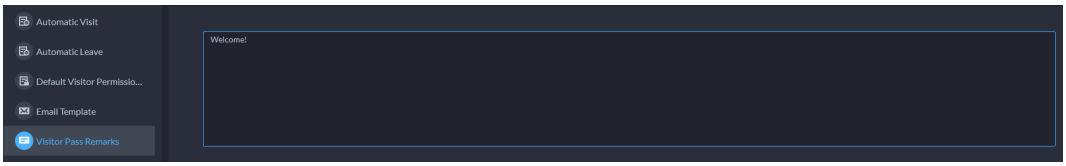
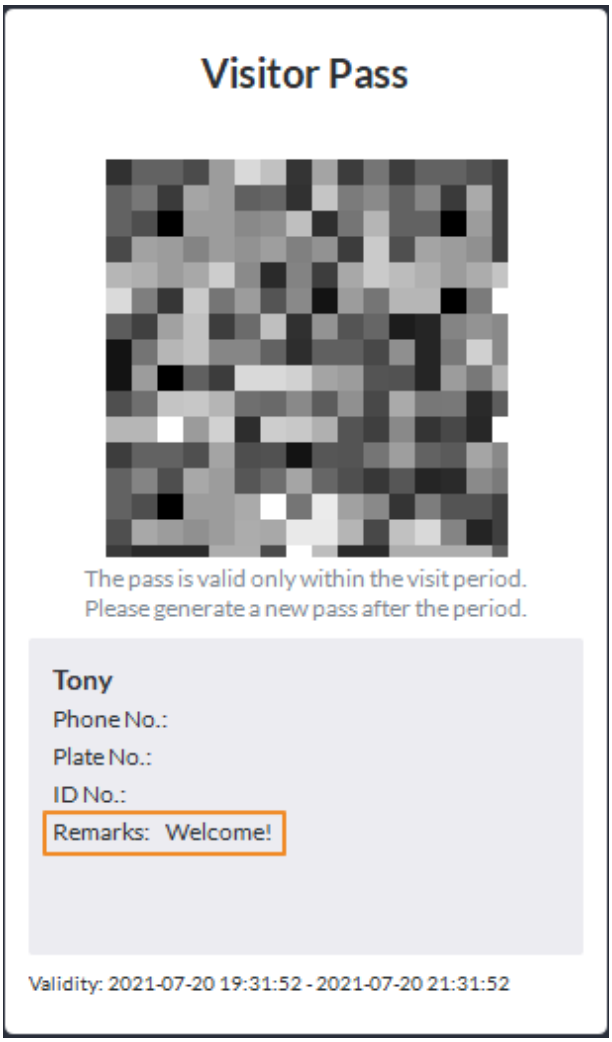


Figure 4-61 Visitor pass remarks



Step 3 Click **Save**.

4.8 Entrance and Exit

Achieve vehicle entrance and exit control with the functions such as ANPR, number of parking space, alarm, and search. In case the vehicle is not recognized by the ANPR camera, visitors can use VTO to call the management center by entering password, swiping a card, fingerprint or face recognition, and then the management center can remotely open the barriers after verifying visitors' identity.

4.8.1 Preparations

Make sure that the following preparations have been made:

- ANPR cameras, VTO, barrier gate, general screen, display for available parking spot, and NVR are deployed. ANPR cameras are correctly added to NVR. For details, see the corresponding user's

manuals.

- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
  - When adding an ANPR camera, select **Access ANPR Device** as the device category.
  - When adding an NVR, select **Encoder** as the device category.
  - Select **Access Snapshot** from **Features** for the corresponding NVR channels.
  - When adding VTO, select **Video Intercom** as the device category.

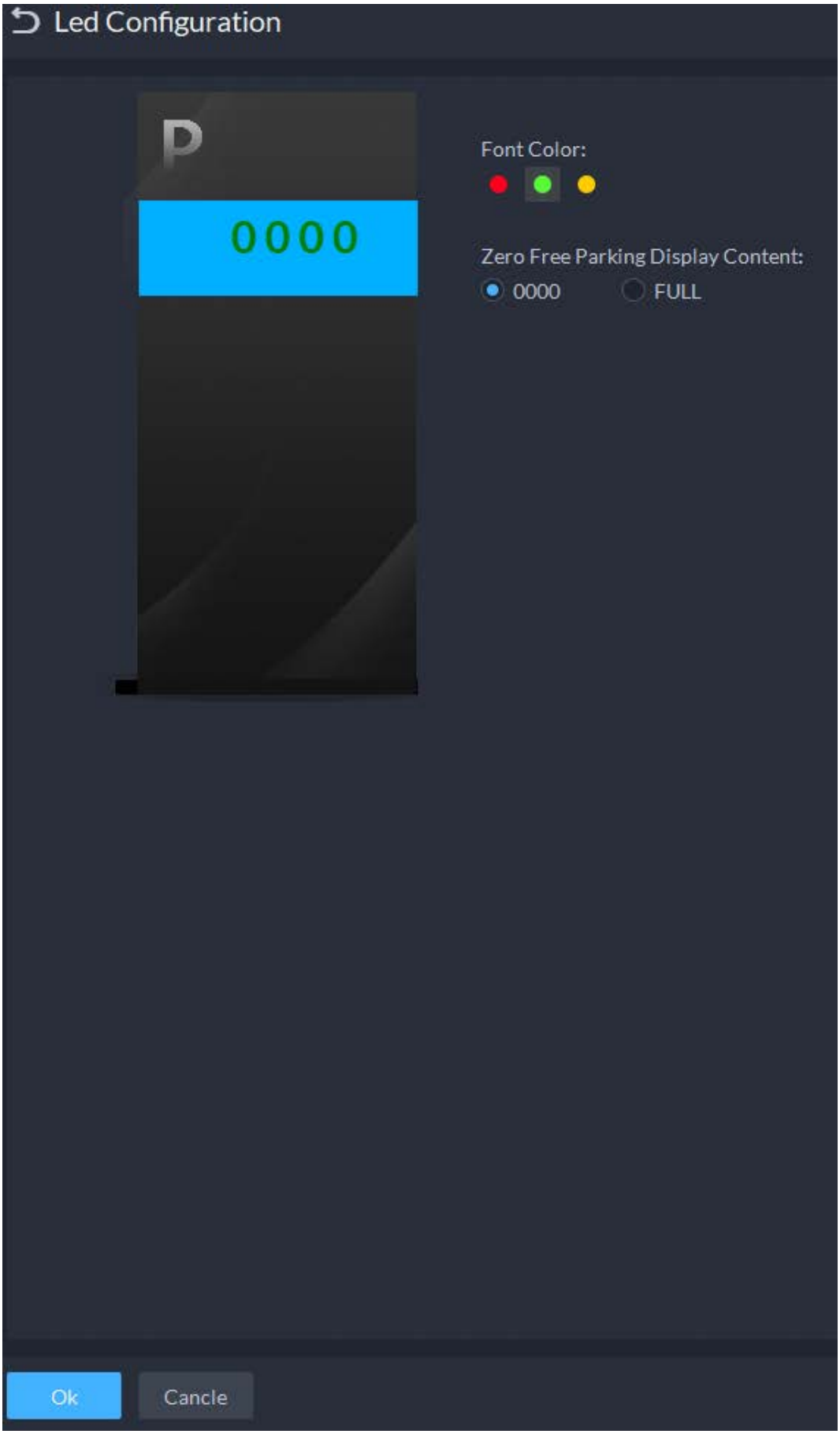
    

    Make sure the status of building and unit of the DSS client is the same as the device. If building and unit are enabled on the platform, they must also be enabled on the device, and vice versa.; otherwise, the VTO will be offline after being added. For details, see "4.6.2 Configuring Building/Unit".
  - Add a screen.

    Add a general LED screen or display for available parking space. Select **LED Device** as the device category. Dahua screen and Jiuzhou screen are supported as the display for available parking space.

    On the **Device Config** interface, select the display for available parking space, and then select character color and the contents to be displayed. The contents you select here will be displayed on the screen when there is no parking space left in the parking lot.

Figure 4-62 Configure the display for available parking space



- Log in to the DSS Client. On the **Home** interface, click , and then select **Device** > **Device Config**. Select the camera as needed, click **Modify** next to **Channel Bind** on the right, and

then you can bind video channels for the ANPR channel. See "3.2.3 Binding Resources" for details.

This is useful when you have installed other cameras at the entrance to view and record the video of the entire background, not just the vehicle part. You can view video from the bound camera when checking the alarm details.

- ◇ The ANPR snapshots are stored in the **ANPR Picture** disks. On the **Storage** interface, configure at least one **ANPR Picture** disk. Otherwise vehicle pictures cannot be viewed.

- If you need the VTO feature, you need to configure personnel information and assign permissions. See "4.3 Personnel and Vehicle Information Management" for details.

4.8.2 Configuring Parking Lot

Generally, one parking lot is considered as an area. Parking lot configuration includes setting parking space quantity, barrier control rules and other information. Bind an ANPR camera for recognizing vehicles, and a VTO (outdoor station) for recognizing human.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Entrance and Exit**.

Step 2 Click .

Step 3 Click **Add**, and then configure the basic information of the parking lot.

Figure 4-63 Basic information

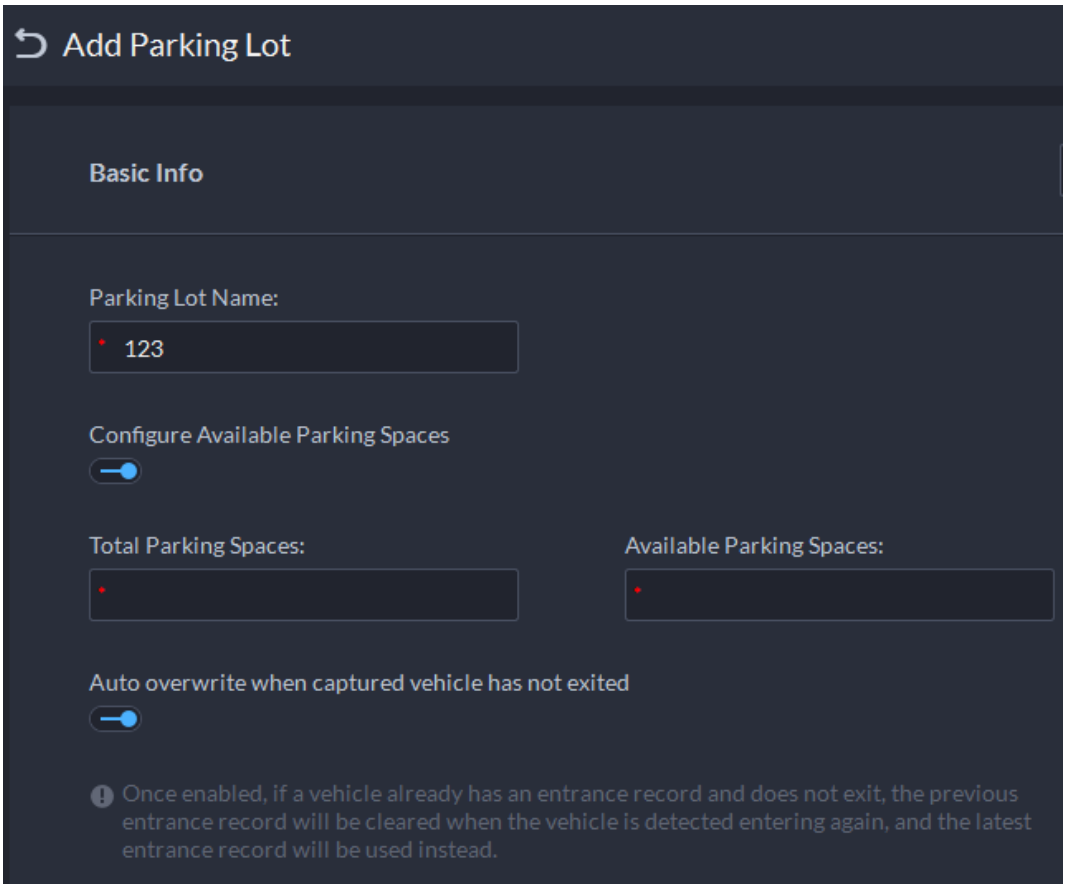


Table 4-5 Parameter description

Parameter	Description
Parking Lot Name	To differentiate from other parking lots.

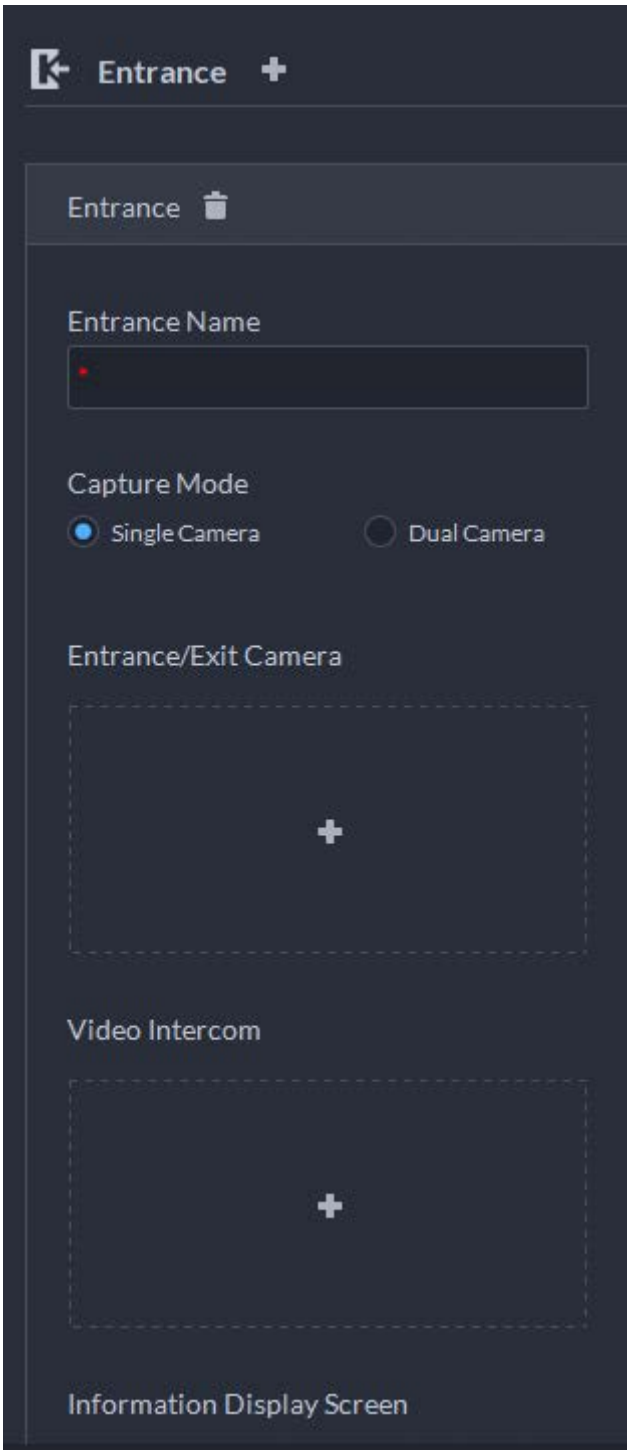
Parameter	Description
Configure Available Parking Space	Enable and then configure the total and available parking space.
Overwrite when captured vehicle does not exist	If a vehicle has entered but not exited, a new entry record will be generated when the vehicle is recognized to have entered again.

Step 4 Click **Next**, and then configure **Entrance/Exit Point**.

You can add more than one entrance or exit points. The total number of entrance and exit points of all parking lots are 30 respectively.

1) Click ➕ or **Add Entrance and Exit Point**.
2) Enter a name, and then click **OK**.
3) If there is an entrance point, click ➕ next to **Entrance**. Enter a name for the point, select a capture mode, and then add a camera, video intercom device (optional), or information display screen (optional).
   - If limited by the environment, you can install two cameras for this point, and then set **Capture Mode** to **Dual Camera** to improve the recognition rate of number plate.
   - In **Dual Camera** mode, the vehicles captured by the two cameras within the defined **Dual Camera Coordinative Time** will be considered as the same vehicle. You must properly configure the time according to the installation positions of the cameras and the distance between them.

Figure 4-64 Entrance point configuration

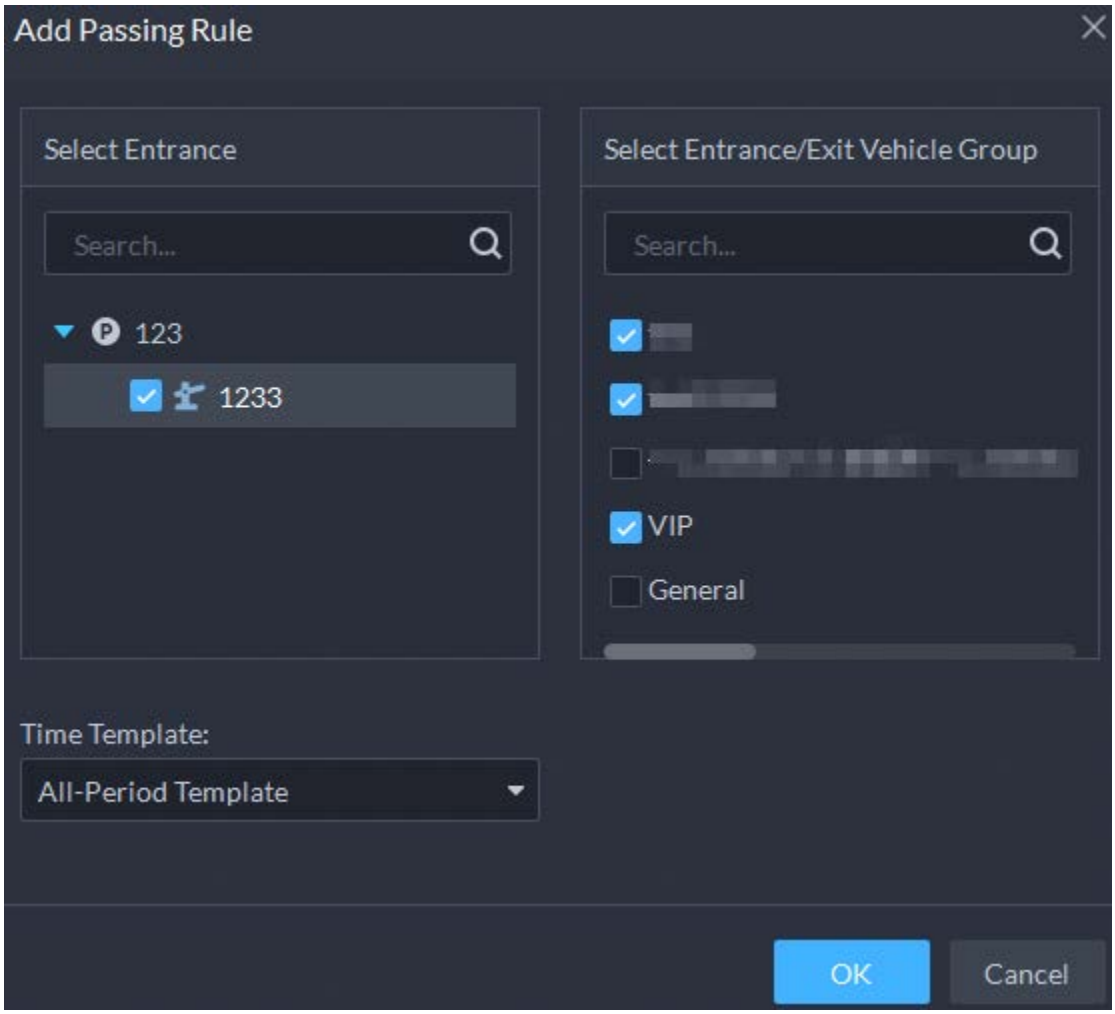


4) If there is an entrance point, click next to **Exit**. Enter a name for the point, select a capture mode, and then add a camera, video intercom device (optional), or information display screen (optional).

Step 5 Click **Next**, and then configure passing rules.

1) Click **Add** in the **Entrance** section. Select **By Point** or the **By Parking Lot** as needed, and then select a time template within which the vehicles from the selected vehicle groups are allowed to pass. For how to create a vehicle group, see "4.8.3 Managing Vehicle Group" for details.

Figure 4-65 Add passing rule



2) Enable **All Vehicles Allowed to Pass** as needed, and then select a time template. Except for vehicles in the blocklist, all vehicles are also allowed to pass.
3) Enable **Allow passage while available space is 0** as needed, and then select a time template. Vehicles from the vehicle groups that you have added from previous steps are allowed to pass even when parking space is 0 within the defined period.
4) Select a passing rule for **Exit** as needed. For vehicle group, see "4.8.3 Managing Vehicle Group" for details.
5) If you select the passing rule as **Allowlist for Registered Vehicles Allowed to Pass** or **Passing According to Setting Rule**, you can enable **Allow unregistered vehicle to exit**.
6) Enable **Send Plate Number to Device**, and then devices can determine which vehicles to let in when the platform is offline.

Step 6 Click **Next**, and then configure the display for available parking space.

1) Click **Add**, and then select all the displays.
2) Select the character color and the contents to be displayed on the right.

Step 7 Click **Save and Exit**.

- : Edit the passing rules of the parking lot.
- : Edit the available parking space of the parking lot.
- : Edit the information of the parking lot.
- : Delete the parking lot.

4.8.3 Managing Vehicle Group

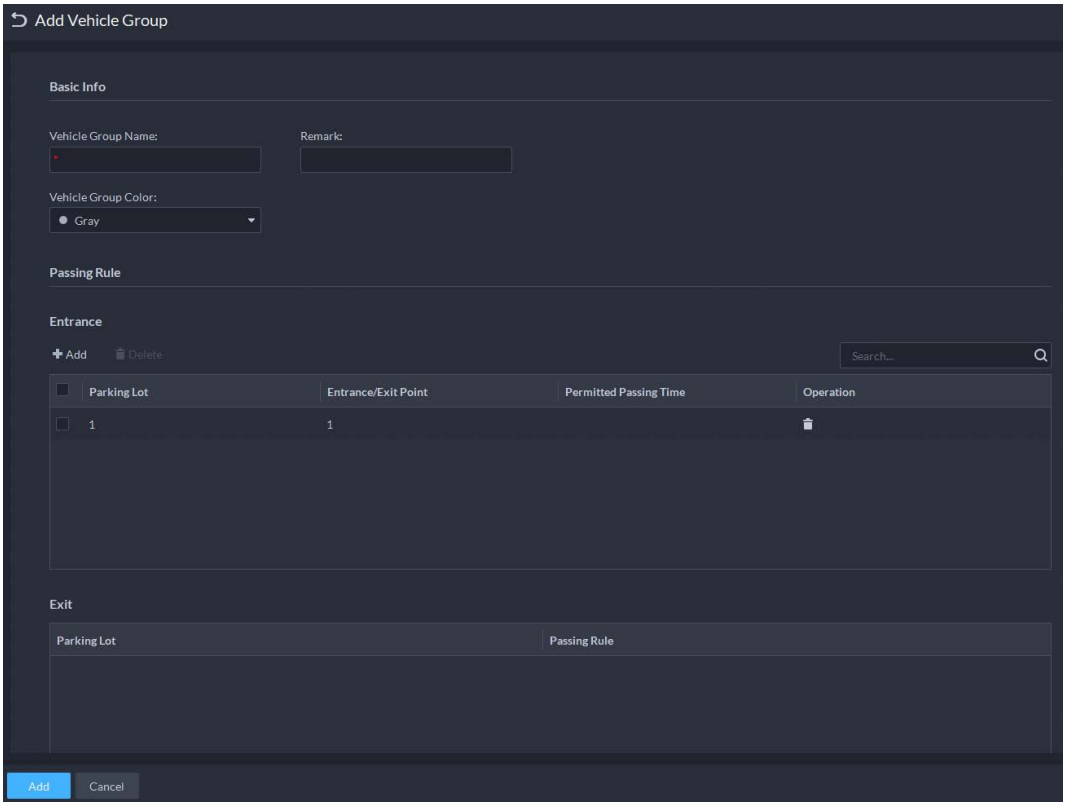
Add similar vehicles to the same group to assign permissions by group.

General, VIP, and blocklist are three default groups. Add vehicles in them as needed.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Config** section, select **Entrance and Exit**.

Step 2 Click , and then click **Add**.

Figure 4-66 Add a vehicle group



Step 3 Configure the vehicle group information.

1) Enter a name for the group, and then select a color.
2) Click **Add** to add a parking lot or entrance/exit point, and then select a time template from **Permitted Passing Time**.

   The information in the **Exit** section is automatically displayed. If you want to configure passing rules, go to **Parking Lot**.

Step 4 Add vehicles.

1) Click , or double-click a group, and then click **Select from Vehicle List**.
2) If you want to link to a person, click on the right of **Owner Info**, and then click **Select from Person List** to select the person as needed. For details, see "4.3.1 Configuring Personnel Information".
3) In the **Vehicle Information** section, enter the vehicle information. If you have linked the vehicle to a person, you can click to add multiple vehicles.
4) Enable **Entrance and Exit Vehicle Group**, click **Add**, select the vehicles as needed, and then configure **Entrance and Exit Vehicle Group** and **Validity Period**.

4.8.4 Configuring Alarms

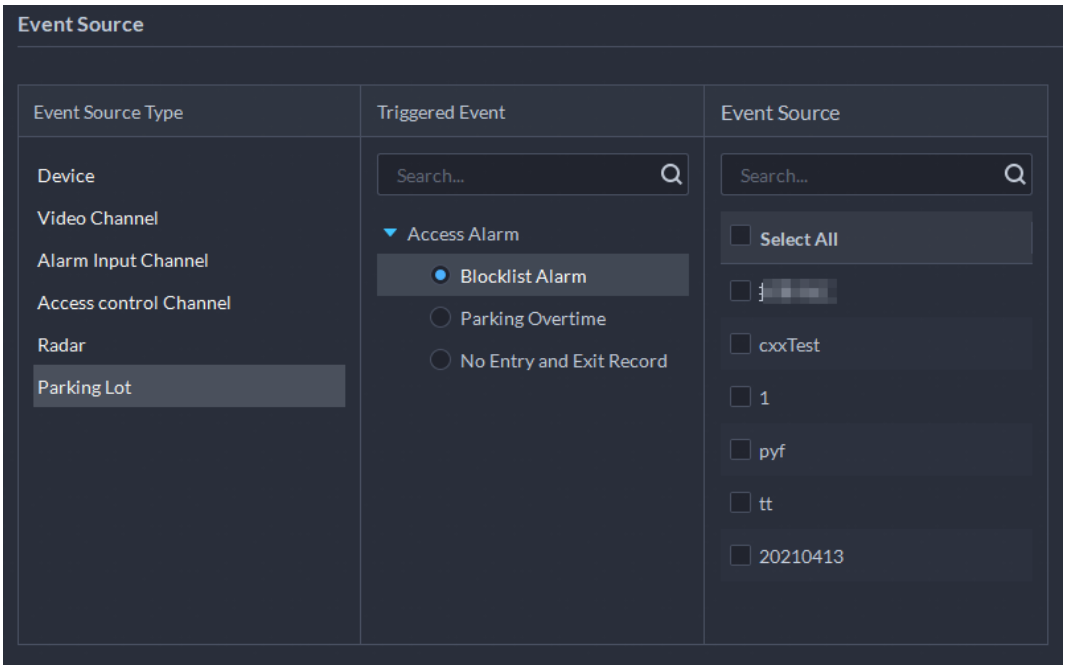
Alarm type includes:

- Blocklist alarm
  Group vehicles to the blocklist as needed. An alarm is triggered when a vehicle in the blocklist is captured by an ANPR camera.

  To add vehicles to the blocklist, see "4.3.2 Vehicle Management" and x"4.3.2 Vehicle Management".
- Parking overtime
  Alarm is triggered when the parking time of a vehicle reaches the threshold.
- No entry and exit record
  Alarm is triggered when vehicles in the defined group have only entrance or exit record within the defined period.

For details, see "4.1 Configuring Events".

Figure 4-67 Add an event



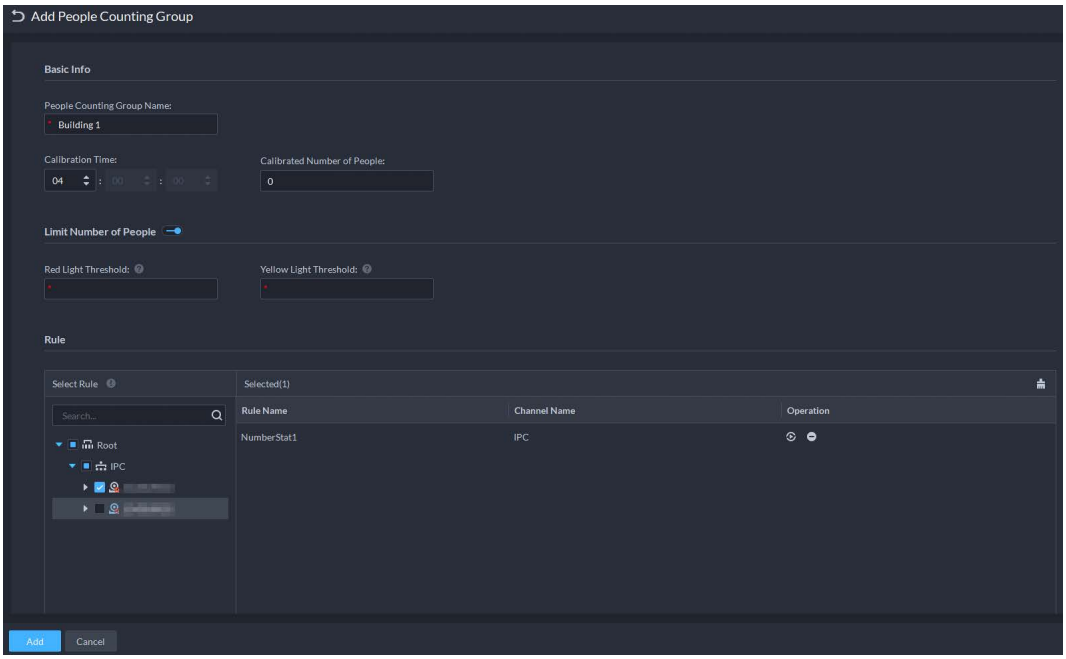
4.9 People Counting Group

Create a people counting group, and then add multiple people counting rules from one or more devices. You can view the real-time and history number of people of the group.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **Applications Configuration** section, select **Intelligent Analysis**.

Step 2 Click **Add** at the upper-left corner.

Figure 4-68 Add a people counting group



Step 3 Configure the parameters.

Table 4-6 Parameter description

Parameter	Description
People Counting Group Name	Name of the people counting group.
Calibration Time	The number of the people in this group will be reset to the defined value at the defined time every day. The defined time also means the start of a counting cycle.
Calibrated Number of People	
Limit Number of People	When enabled, you can configure the red and yellow light threshold of the people in the group.
Red Light Threshold	When the number of people in the group reaches the defined value, the light will turn red.
Yellow Light Threshold	When the number of people in the group reaches the defined value but smaller than the red light value, the light will turn yellow.
Rule	Select the devices whose people counting rules you want to include in the group, and then their data will be combined together.

Step 4 Click **Save**.

5 Businesses Operation

5.1 Monitoring Center

The monitoring center provides integrated real-time monitoring applications for scenarios such as CCTV center. The platform supports live video, license plate recognition, target detection, access control, emap, snapshots, events, video playback, video wall, and more.

5.1.1 Main Interface

Provides frequently used functions such as video and event and alarm.

Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

Figure 5-1 Monitoring center

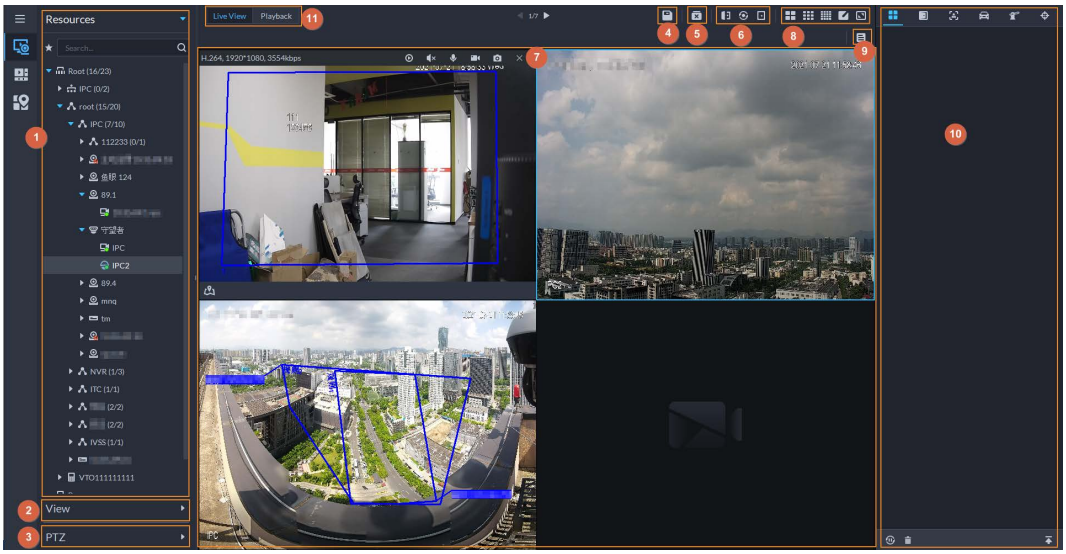


Table 5-1 Interface description

No.	Parameter	Description
1	Favorites and device tree	• List of resources including devices, and maps. • You can search for a device or channel in the search field. Fuzzy search is supported so that you can simply enter part of the name and then select the exact one from the provided name list. • Add, delete or rename the favorites. You can also tour the channels in favorites.
2	View	• Save the current view of window split and video channels in the live view section, and name the view. You can directly select the view from the **View** tab to display it quickly next time. • Channels under a view or view group can be displayed by tour (in turn). You can set the tour interval to be 10 s, 30 s, 1 min, 2 min, 5 min or 10 min. Maximum 100 views can be created.

No.	Parameter	Description
3	PTZ	PTZ control panel.
4	Save view	Click to save current video window as a view.
5	Close all windows	Close all windows in live view.
6	Channel control	Control the door channels in live view.
7	Real-time videos	Drag a channel to the windows and view its real-time video.
8	Window split mode and full screen	• Set window split mode. Supports 1, 4, 6, 8, 9, 13, 16, 20, 25, 36 or 64 splits, or click to set a customized split mode. If the live-view channel number is more than the number of current windows, then you can turn page(s) by clicking at the bottom of the interface. • Switch the video window to **Full Screen** mode. To exit **Full Screen**, you can press the Esc key or right-click on the video and select **Exit Full Screen**.
9	Event panel button	Display or hide the event panel.
10	Event and alarms	Events and alarms.
11	Live view and playback	• Live view: View real-time videos. • Playback: View recordings. See "5.1.3 Playback"。

5.1.2 Video Monitoring

View live videos. For ANPR and face cameras, you can view information of ANPR, face detection and face recognition. For video metadata cameras, you can view metadata information.

5.1.2.1 Viewing Live Video

View the live video of connected devices.

This section only introduces viewing live video. For map live view, see "4.2 Configuring Map".

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then click **Monitoring Center**.

Step 2 Click .

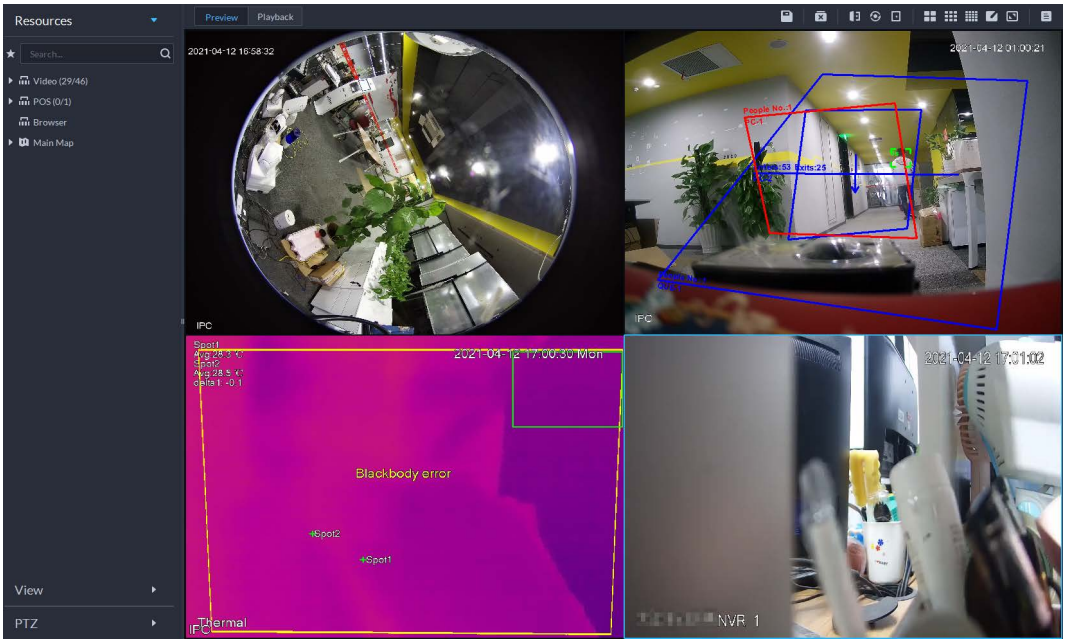
Step 3 View real-time video.

You can view live video in the following ways:

- Double-click a channel or drag the channel from the device list on the left to one window on the right.
- Double-click a device to view all channels under the device.
- Right-click a node, select **Tour**, and then set tour interval. The channels under this node will play in turn according to the defined interval.

- If the number of splits in the window is more than the number of online channels, video of all channels will be displayed in the window. Otherwise, click 1/6 on the top of the interface to turn pages.
- Close the on-going tour before starting live view.

Figure 5-2 Live view



Step 4 You can perform the following operations during live view.

- Display intelligent snapshots.
  When viewing live video of face detection cameras, face recognition cameras, ANPR cameras, or target detection cameras, right-click the monitoring image, and then select **Start Picture Overlay**. The snapshot will be displayed on the upper-right corner of the live window. If no more images are captured, a snapshot will be displayed up to 5 s by default, and it will disappear after 5 s.
  Point to the live window, and then select type of images to be displayed.
- Point to the video window, and then you can see the shortcut menu on the upper right.

Figure 5-3 Live window

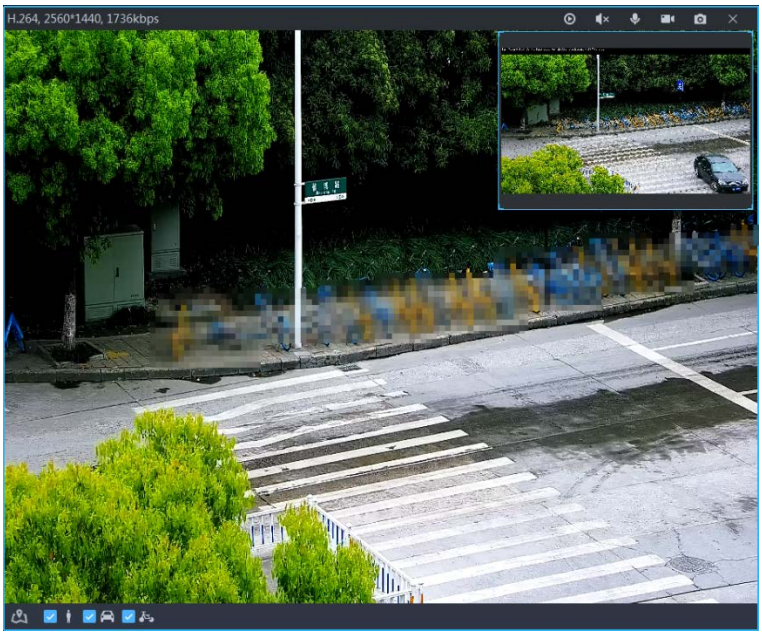


Table 5-2 Description

Icon	Name	Description
	Instant playback	Open/close instant playback.
	Audio	Open/close audio.
	Audio communication	Open/close two-way audio.
	Local record	Click it, and then the system begins to record local file and you can view the record time on the upper left. Click again, and then system stops recording and saves the file to your PC. The recorded video is saved to ..*DSS**DSS Client**Record* by default. To change the storage path, see "8.3.5 Configure File Storage Settings".
	Snapshot	Take a snapshot. The snapshots are saved to ..*DSS**DSS Client**Picture* by default. To change the snapshot storage path, see "8.3.5 Configure File Storage Settings".
	Zoom	Zoom in, and it supports mouse wheel zooming after zooming in the image.
	Close	Close the video.

- Right-click the live video, and then the shortcut menu is displayed.

The menu varies depending on device functions.

Figure 5-4 Live video operation menu

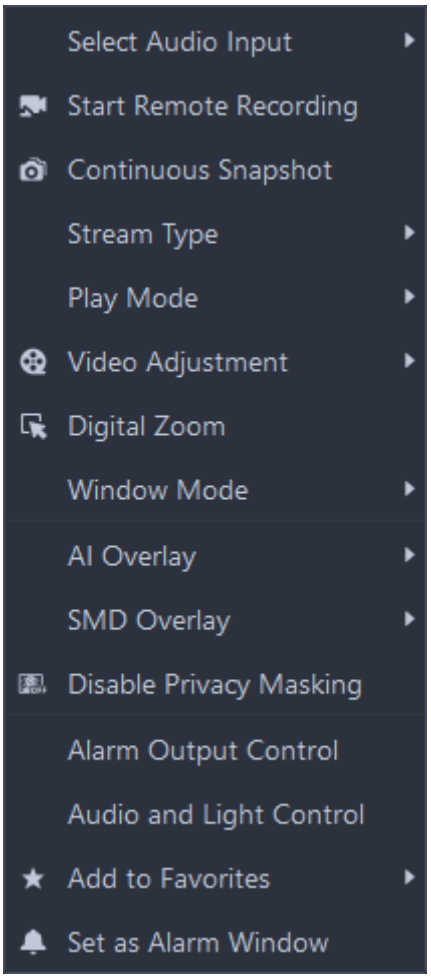


Table 5-3 Description

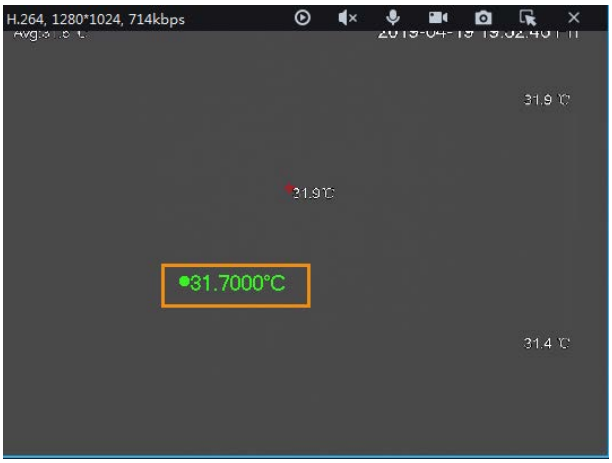
Parameters	Description
Audio Input Selection	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Start Remote Record	Record the audio and video in the current window, and save the recordings to the path defined when configuring record plan. If a channel already has recorded within the same period, the video status will be overlaid over the live view. If video storage disk is configured on the platform, the videos will be saved to the platform server.
Continuous Snapshot	Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to ..*DSS\DSS Client\Picture* by default. To change the snapshot storage path, see "8.3.5 Configure File Storage Settings".
Stream Type	Select stream type as required. Generally, main stream requires the most bandwidth, and sub stream 2 the least. The smaller the bandwidth is required by the stream, the smoother the video image.

Parameters	Description
Play Mode	● Real-Time Priority: The video is in real-time, but video quality might be reduced. ● Fluency Priority: The video is fluent, but video lagging might occur. ● Balance Priority: Real-time priority or fluency priority, depending on actual conditions. ● Custom: Configure the video buffer time from **Local Settings > Video**. The larger the value, the more stable the video quality.
Video Adjustment	Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement.
Digital Zoom	Click it, and then click and hold the video image to zoom in on the image. Right-click the image, and then select **Digital Zoom** again to exit zooming in.
Window Mode	Divide one window into 4 (**1+3** mode), 6 (**1+5** mode). One window plays live video, and the others play local views. To play the video in normal mode, select **Normal Mode**.
AI Overlay	The client does not show rule lines on the live video by default. If needed, you can click **AI Overlay** and enable **Rule Overlay** and **Bounding Box Overlay**, and then the live video shows rule lines if the AI detection rules are enabled on the device. This configuration is effective with the current selected channel both in live view and playback.
SMD Overlay	Enable **SMD Overlay** to show target bounding box over live video. When SMD is enabled on the device, you can enable **SMD Overlay** for the device channel, and then the live video will display dynamic target bounding boxes. This configuration is effective with the current selected channel both in live view and playback.
Disable Privacy Masking	For a camera that supports privacy masking of human face, you can disable the masking here to view the face image.
Alarm Output Control	Enable or disable channel alarm input/output.
Audio and Light Control	You can turn on or off the audio and light channels one by one or at the same time.
Add to Favorite	You can add the active channel or all channels into Favorite.
Set as Alarm Window	When selecting open alarm linkage video **In Preview** (in live window) from **Local Settings > Alarm**, then the video will be displayed on the window which is set to alarm window. If multiple alarms are triggered, the video linked to the latest alarm will be opened. If the number of alarm windows is fewer than the number of linkage videos, the video linked to the earliest-triggered alarm will be opened. After enabling **Set as Alarm Window**, the window frame is displayed in red.

Parameters	Description
Fisheye View	This function is available on fisheye cameras only. When changing the video stream, the fisheye view mode will maintain the current configuration. According to different installation methods, the fisheye view can be varied. ● In-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.

- To view real-time temperature of a point on the thermal camera view, hover over that point.

Figure 5-5 View temperature



- If a channel supports electronic focus, you can enable electronic focus for it on the platform to adjust video definition and size.

The interface might vary according to the lens types of cameras. Lens types include embedded zoom lens and external CS electronic lens. The following figure is for reference only.

Figure 5-6 Live view

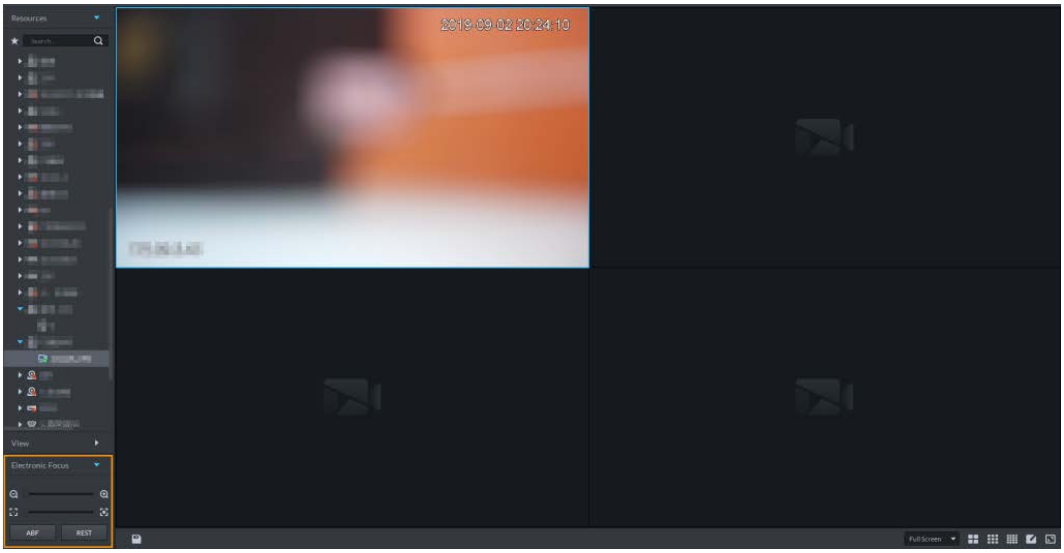


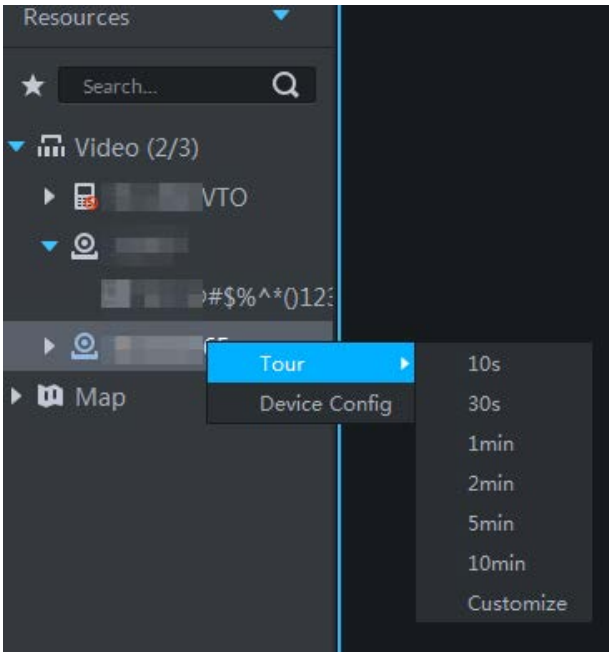
Table 5-4 Description

Parameters	Description
Zoom +/- (for embedded zoom lens)	Zoom in/out. Click or click and hold or , or drag the slider to the left or right to zoom in/out.
Focus +/-	Adjust camera focus to achieve the best video definition. Click or click and hold or , or drag the slider to the left or right to adjust focus.
Auto Focusing (for embedded zoom lens) ABF (auto back focusing, for external CS electronic lens)	Adjust image definition automatically. Other focusing operations are unavailable during auto focusing.
Reset	When image definition is imperfect, or after many times of zooming or focusing operations, you can click **Reset** to reset the lens, so as to eliminate lens deviation.

- Tour

  On the live view interface, right-click a device or node, select **Tour**, and then select an interval. The channels under this device or node will be played in turn at the pre-defined interval. You can also customize the interval.

Figure 5-7 Start tour



- ◇ To view remaining time of a channel during tour, check 00:02.
- ◇ To pause, click .
- ◇ To exit tour play, click .

- Region of interest (RoI)

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

  On the live view interface, right-click the window, select **Window Mode**, and then select a mode. For example, select 1+3 mode.

To exit the **Window Mode**, right-click and select **Normal Mode**.

Figure 5-8 Split mode

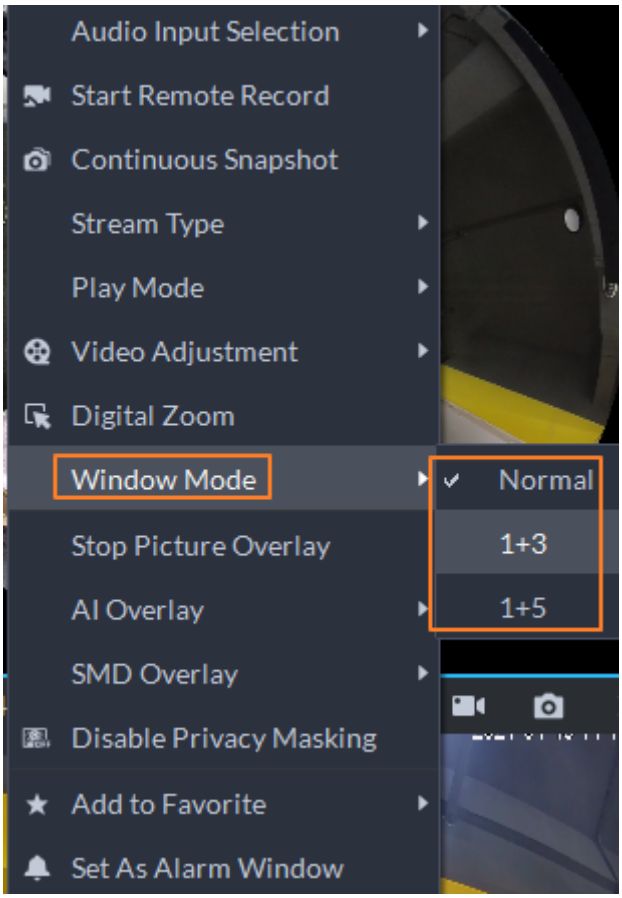
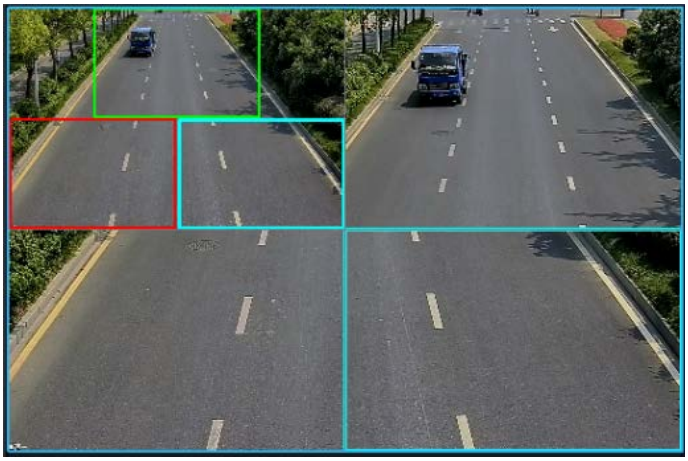


Figure 5-9 1+3 mode



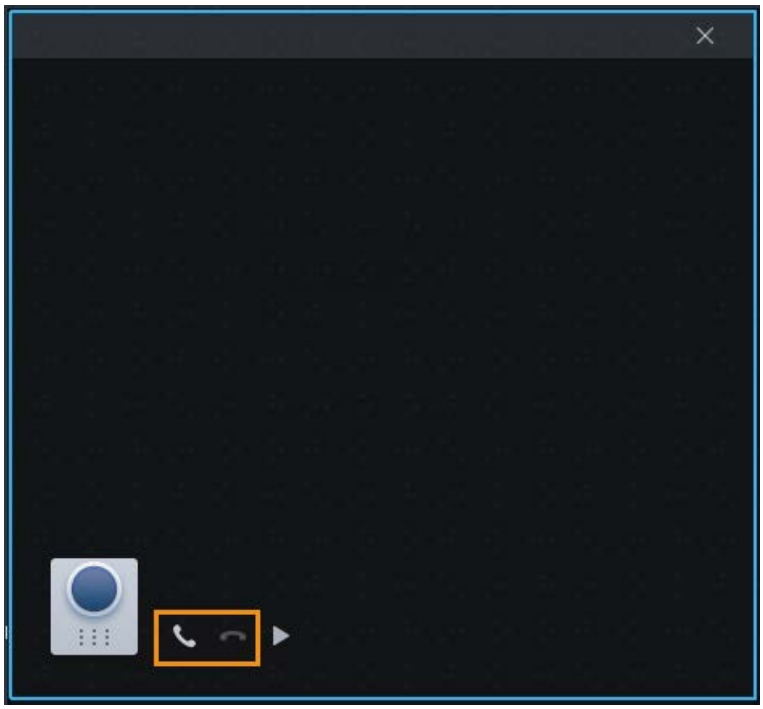
- View real-time events.
  Click to open the event panel, which displays the real-time alarm events of the channel.
  - Click the event type on the top of the event panel to view the corresponding event.
  - Click event record to view the snapshot. Video playback is also supported. Operations related to different events might be different.
  - : Refreshes events in real time. : Stops refreshing.
  - Click to clear the events in the event panel.
  - Click to quickly view the latest events.

- Remotely unlock the door.
  When viewing the access control channel, you can remotely control the status of the door on the upper right: Normally open ( ), normally closed ( ), or normal status ( ). You need to enter the login password of the current user before operation. Restore the door to normal status first, and then the door can be opened and closed according to defined period or through face recognition.
  In the video window of the access control channel, you can remotely lock or unlock the door.

Figure 5-10 Lock/unlock the door

- Video intercom.
  When viewing the video intercom channel, you can answer or hang up the call.

Figure 5-11 Video intercom



5.1.2.2 View

The current layout and resources can be saved as a view for quick play next time. Views are categorized into different groups, which include three levels: First-level root node, second-level grouping and third-level view. Tour is supported for first-level root node and second-level grouping. The tour time can be 10 s, 30 s, 1 min, 2 min, 5 min, 10 min, or customized (5 s–120 min). Up to 100 views can be created.

5.1.2.2.1 Creating View

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

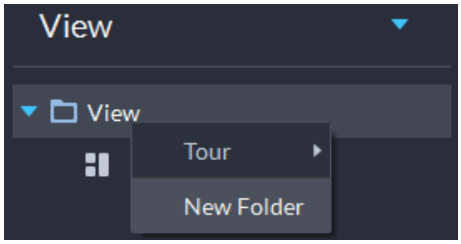
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

Step 2 Click .

Step 3 Create a view group.

1) Click the **View** tab.
2) Right-click **View**, select **New Folder**.

Figure 5-12 Create a new folder



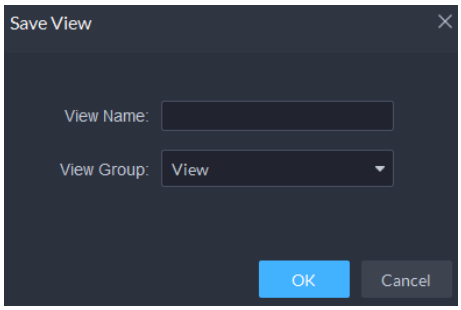
3) Enter a folder name, click **OK**.

Step 4 Create view.

1) Click on the upper right corner as needed.

2) Enter **View Name**, select **View Group** and click **OK**.

Figure 5-13 Save view



5.1.2.2.2 Viewing View

- Live view
  On the **Monitoring Center** interface, select a view, double-click or drag it to the window to start viewing.
- Tour
  On the **Monitoring Center** interface, right-click view group or root node, select **Tour** and tour period.

Figure 5-14 Go to video tour interface

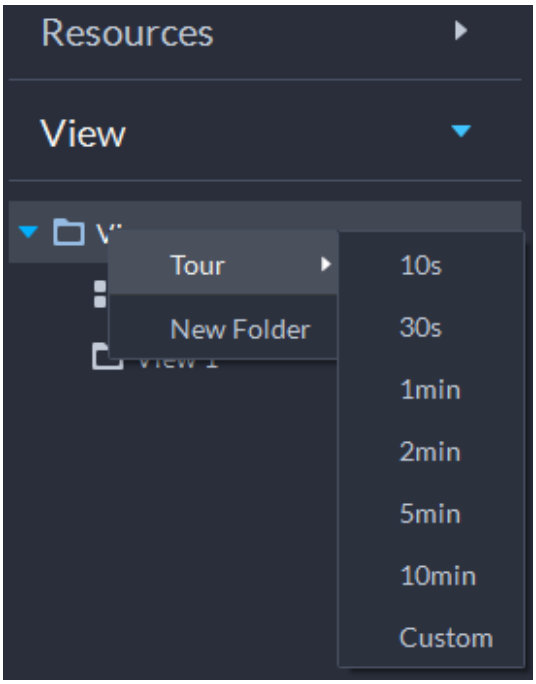
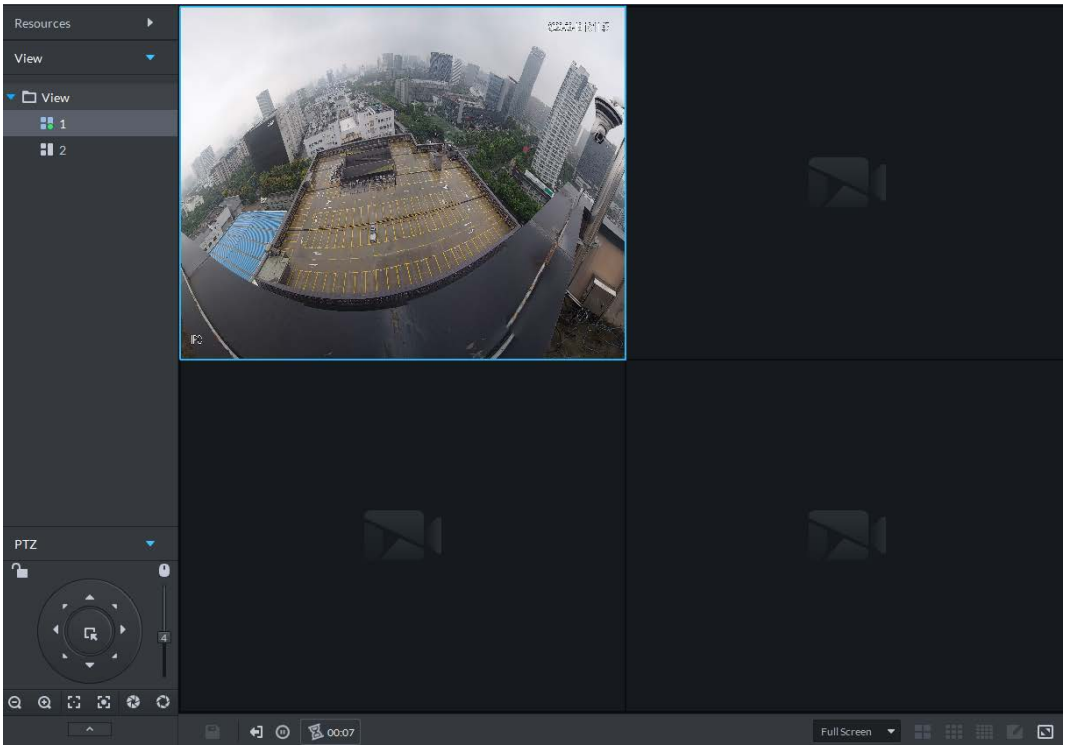


Figure 5-15 View tour



- To view remaining time of a channel during tour, check 00:02.
- To pause, click .
- To exit tour play, click .

5.1.2.3 Favorites

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

5.1.2.3.1 Creating Favorites

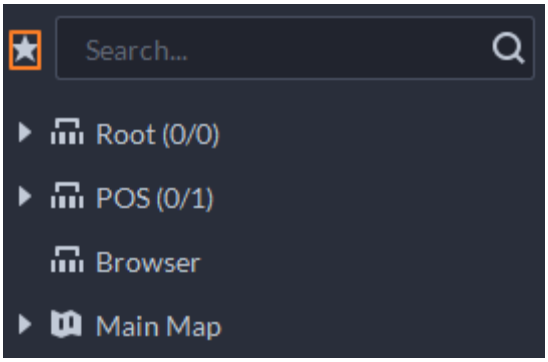
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

Step 2 Click .

Step 3 Create favorites.

1) Click .

Figure 5-16 Favorites



2) Right-click root node or created favorites, and then select **New Folder**.

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

Lower-level favorites are generated under the selected root node or favorites.

4) Click .

The system goes back to the device list.

Step 4 Add channels to favorites.

- In the device list, right-click a channel, and then select **Add to Favorite**.
- Right-click the window with live video, and then select **Add to Favorite**.

5.1.2.3.2 Viewing Favorites

- Live view

  On **Monitoring Center** interface, click , open favorites list, select favorites or channels, double-click or drag to video window and the system starts to play live video.
- Tour

  On **Monitoring Center** interface, click , open favorites list, select the root node or favorites, select **Tour** and then set duration. The system starts to play the channels in tour.
  - To view remaining time of a channel during tour, click 00:02.
  - To pause, click .
  - To exit tour play, click .

5.1.2.4 PTZ

Operate PTZ cameras during live view on the DSS Client.

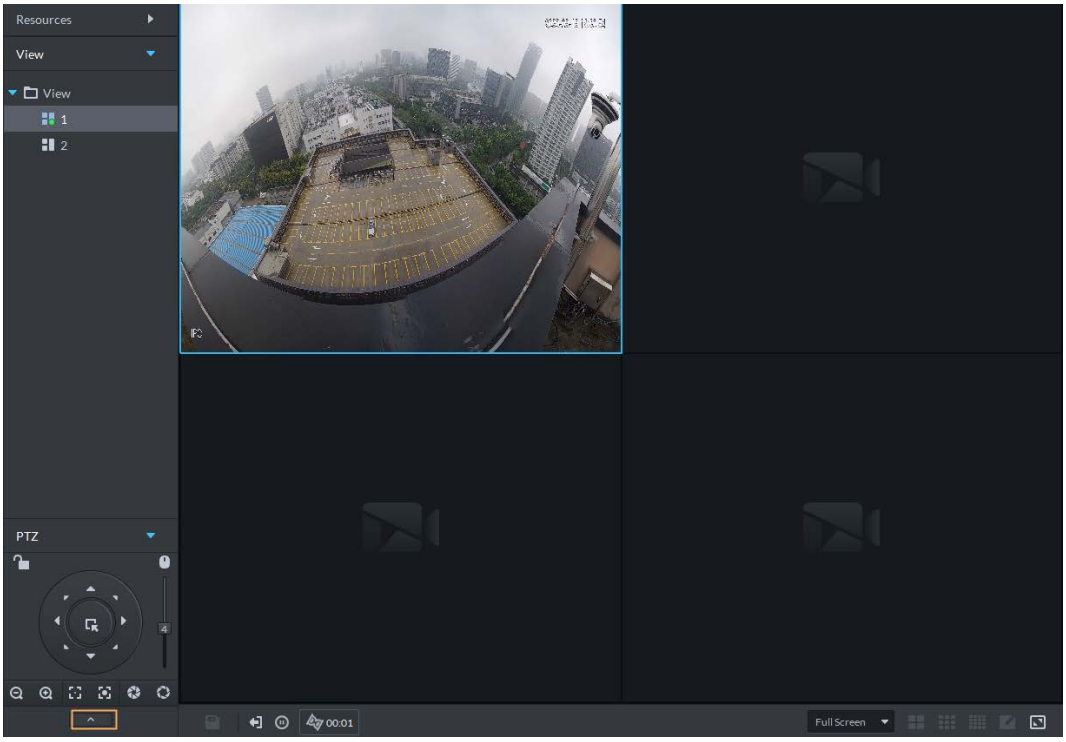
5.1.2.4.1 Configuring Preset

A preset is a set of parameters involving PTZ direction and focus. By calling a preset, you can quickly rotate the camera to the pre-defined position.

Step 1 On the **Monitoring Center** interface, open the video of a PTZ camera.

Step 2 Click .

Figure 5-17 Go to PTZ control panel



Step 3 Click .

Step 4 Add a preset.

1) Rotate the PTZ camera to a specific point.
2) Click , enter the preset name, and then click .

Related Operations

Call a preset: Click of a specific preset, and then camera will rotate to the related position.

5.1.2.4.2 Configuring Tour

Set Tour to enable an camera to go back and forth among different presets. Set tour to enable camera to automatically go back and forth between different presets.

Prerequisites

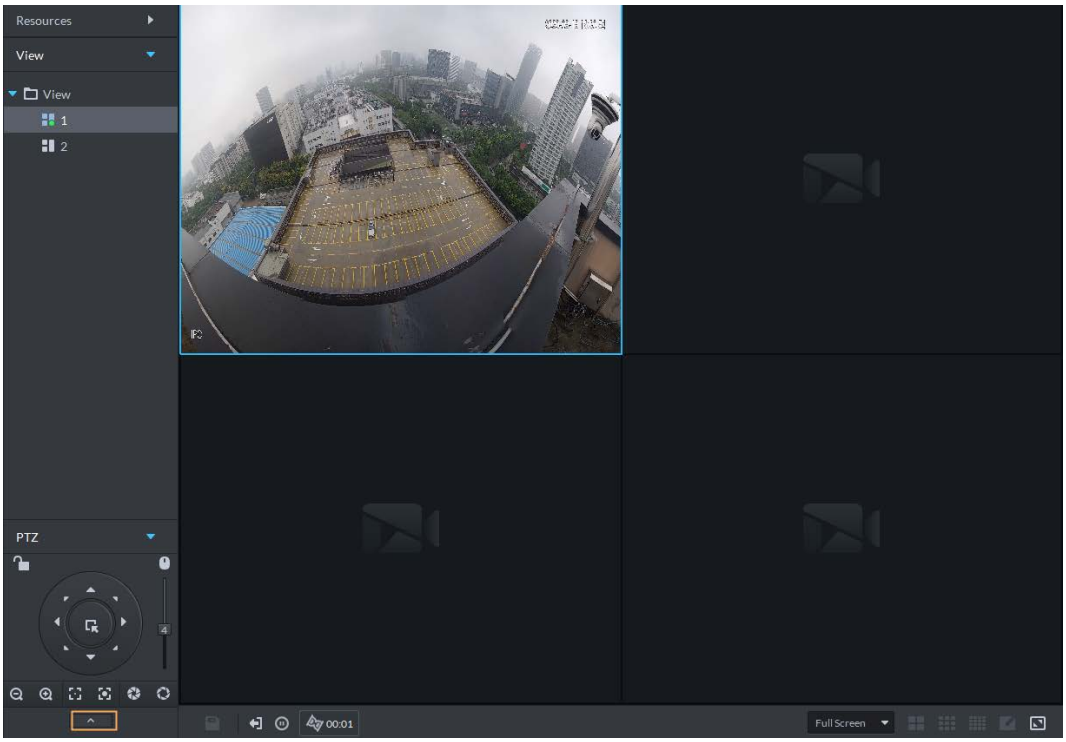
You have added at least 2 presets.

Procedure

Step 1 On the **Monitoring Center** interface, open the video of a PTZ camera.

Step 2 Click .

Figure 5-18 Go to PTZ control panel



Step 3 Click .

Step 4 Click .

Step 5 Add tours.

1) Enter tour name, and click .
2) Select a preset from the drop-down list on the left.
3) Repeat the previous 2 steps to add more presets.
4) Click **OK**.

Related Operations

To start tour, click , then camera goes back and forth among the presets.

5.1.2.4.3 Configuring Pattern

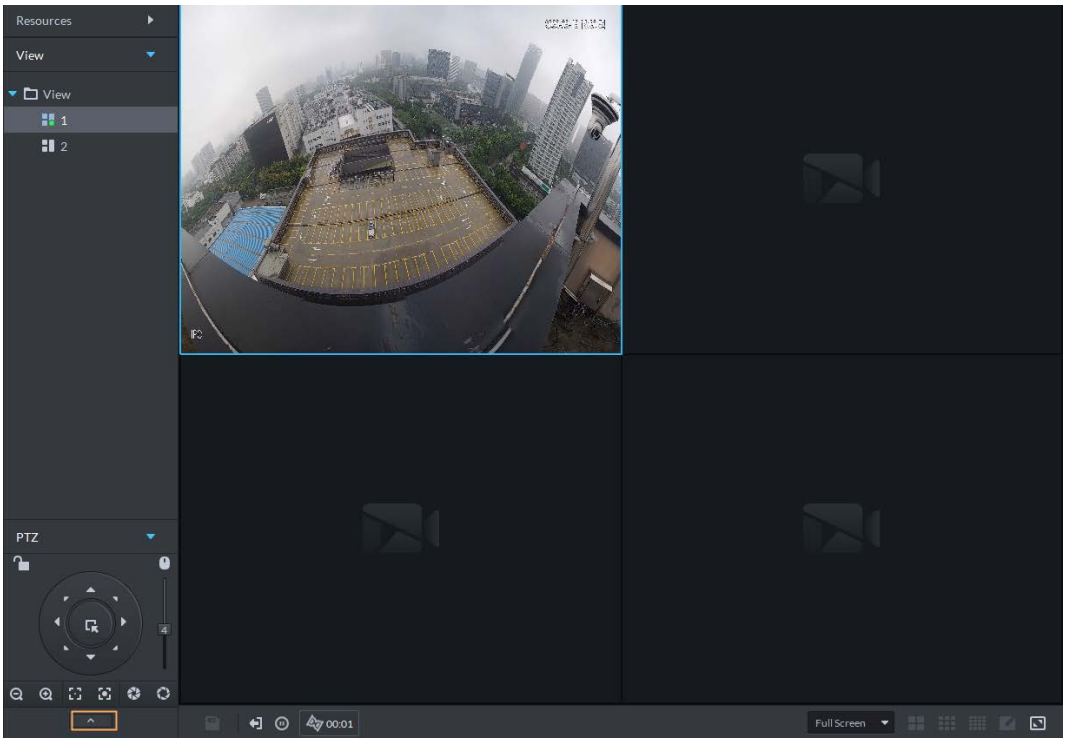
A pattern is a record of a consecutive series of PTZ operations. You can select a pattern to repeat the corresponding operations quickly. See pattern configuration instructions as follows.

Procedure

Step 1 On the **Monitoring Center** interface, open the video of a PTZ camera.

Step 2 Click .

Figure 5-19 Go to PTZ control panel



Step 3 Click .

Step 4 Click , and then operate the 8 PTZ buttons of PTZ to set pattern.

Step 5 Click .

Related Operations

Call pattern: Click , and then the camera will automatically repeat the pattern that you have configured.

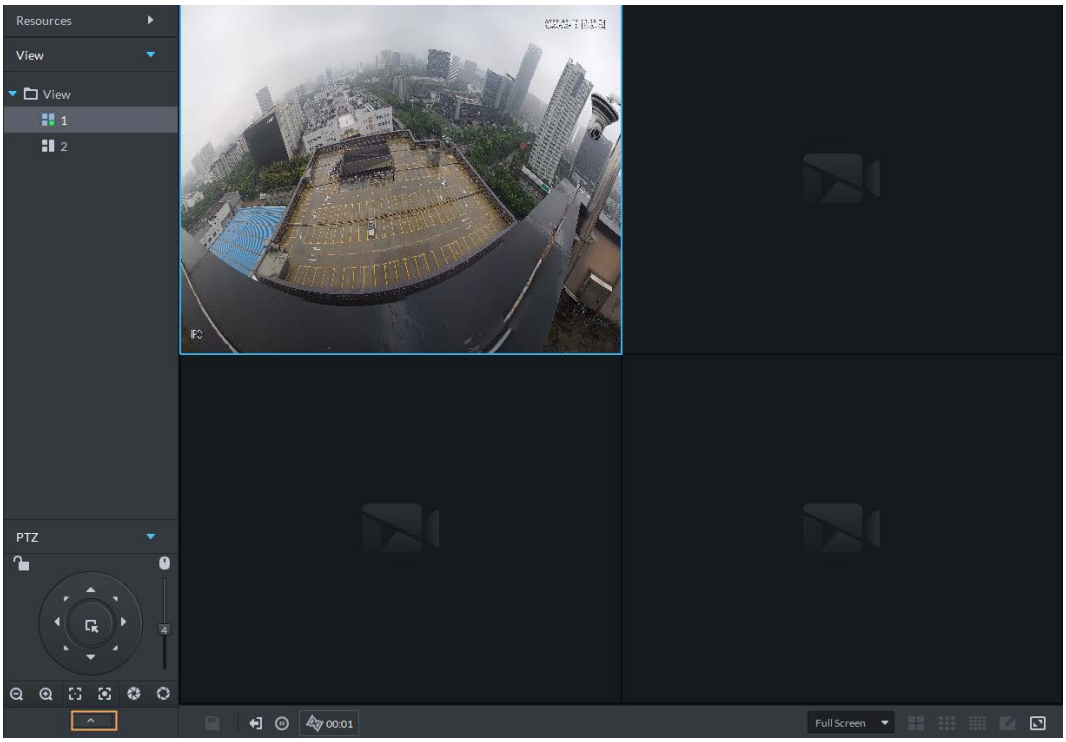
5.1.2.4.4 Configuring Scan

The camera automatically scans horizontally at a certain speed.

Step 1 On the **Monitoring Center** interface, open the video of a PTZ camera.

Step 2 Click .

Figure 5-20 Go to PTZ control panel



Step 3 Click ••• .

Step 4 Click PTZ button, and rotate PTZ to the left to a position, and then click to set the left boundary.

Step 5 Continue to rotate PTZ to the right to a position, and then click to set the right boundary.

Step 6 Click to start scanning, then PTZ will rotate back and forth automatically within the two boundaries.

5.1.2.4.5 Enabling/Disabling Pan

On the **Monitoring Center** interface, open the video of a PTZ camera. Click •••, and then click . PTZ rotates 360° at a specified speed. Click to stop camera rotation.

5.1.2.4.6 Enabling/Disabling Wiper

Enable/disable the PTZ camera wiper. Make sure that the camera supports wiper function.

On the **Monitoring Center** interface, open the video of a PTZ camera. Click •••, and then click to turn on wiper. Click to turn off wiper.

5.1.2.4.7 Enabling/Disabling Light

Turn on/off camera light . Make sure that the camera supports light.

On the **Monitoring Center** interface, open the video of a PTZ camera. Click •••, and then click to turn on light. After enabling light, click to turn off light.

5.1.2.4.8 Enabling/Disabling IR Light

Turn on/off IR light. Make sure that the camera is connected to or supports IR light.

On the **Monitoring Center** interface, open the video of a PTZ camera. Click •••, and then click

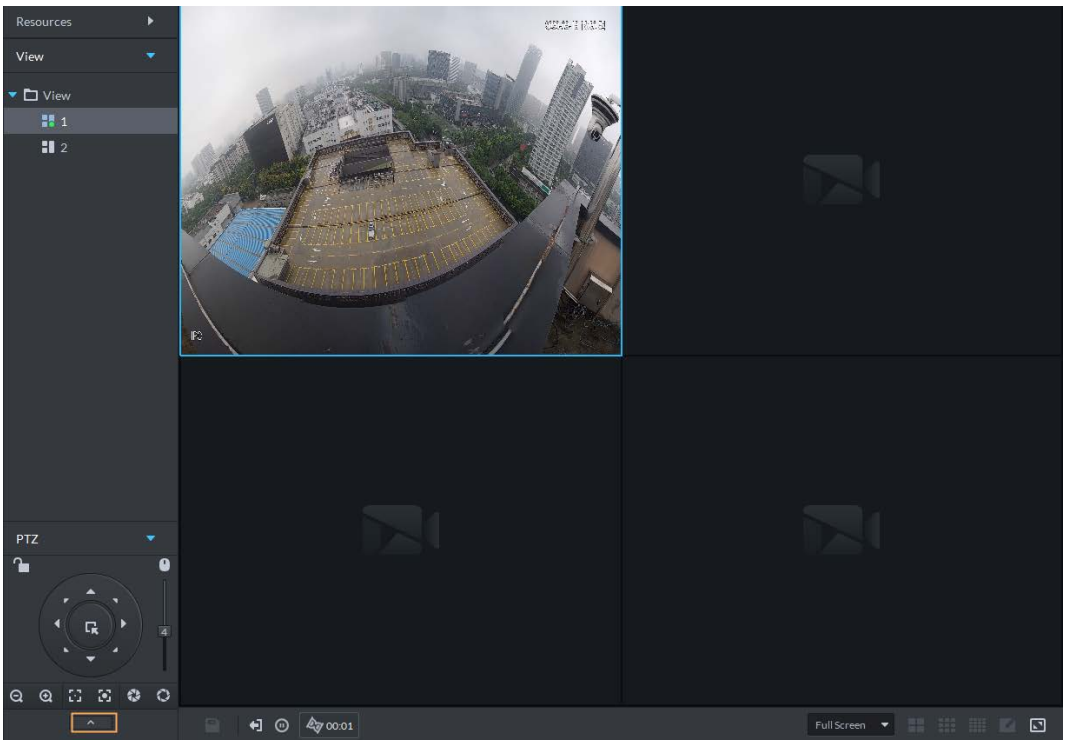
to enable IR light. After enabling IR light, click to disable.

5.1.2.4.9 Configuring Custom Command

Step 1 On the **Monitoring Center** interface, open the video of a PTZ camera.

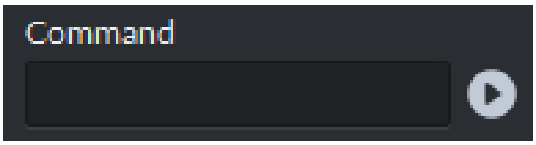
Step 2 Click .

Figure 5-21 Go to PTZ control panel



Step 3 Enter your command in the **Command** box.

Figure 5-22 Custom command



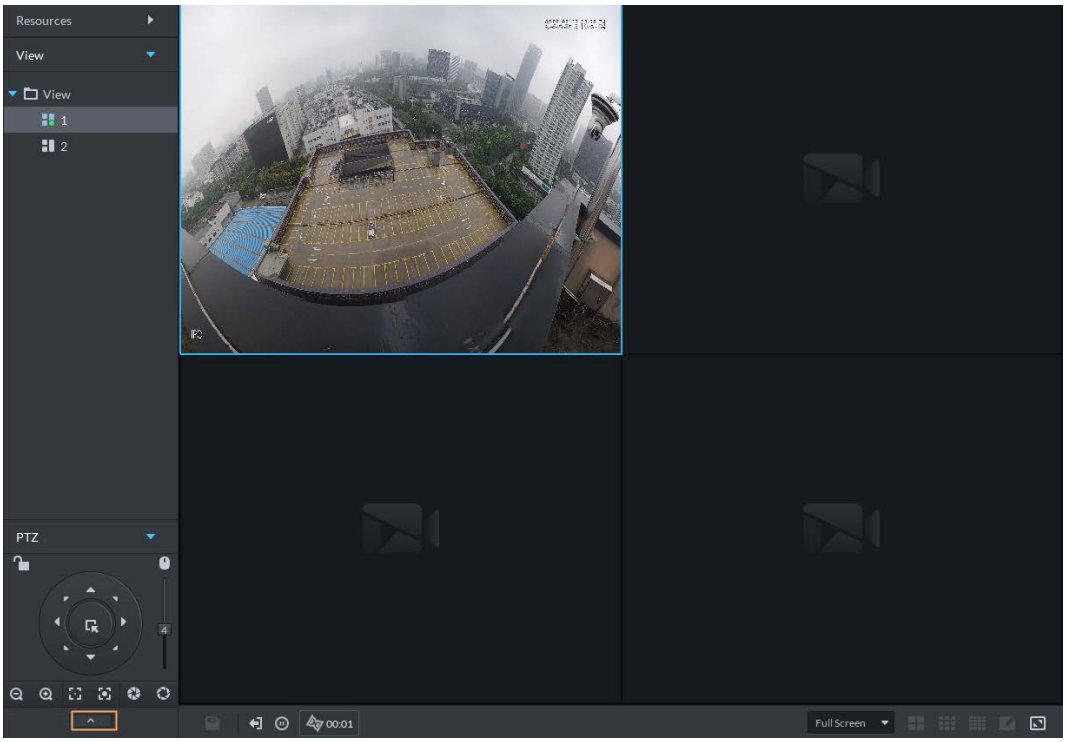
Step 4 Click to show the command functions.

5.1.2.4.10 PTZ Menu

Step 1 On the **Monitoring Center** interface, open the video of a PTZ camera.

Step 2 Click .

Figure 5-23 Go to PTZ control panel



Step 3 Click .

Step 4 Click .

Step 5 Use the panel to go to the menu configuration interface.

Figure 5-24 Go to PTZ menu configuration interface

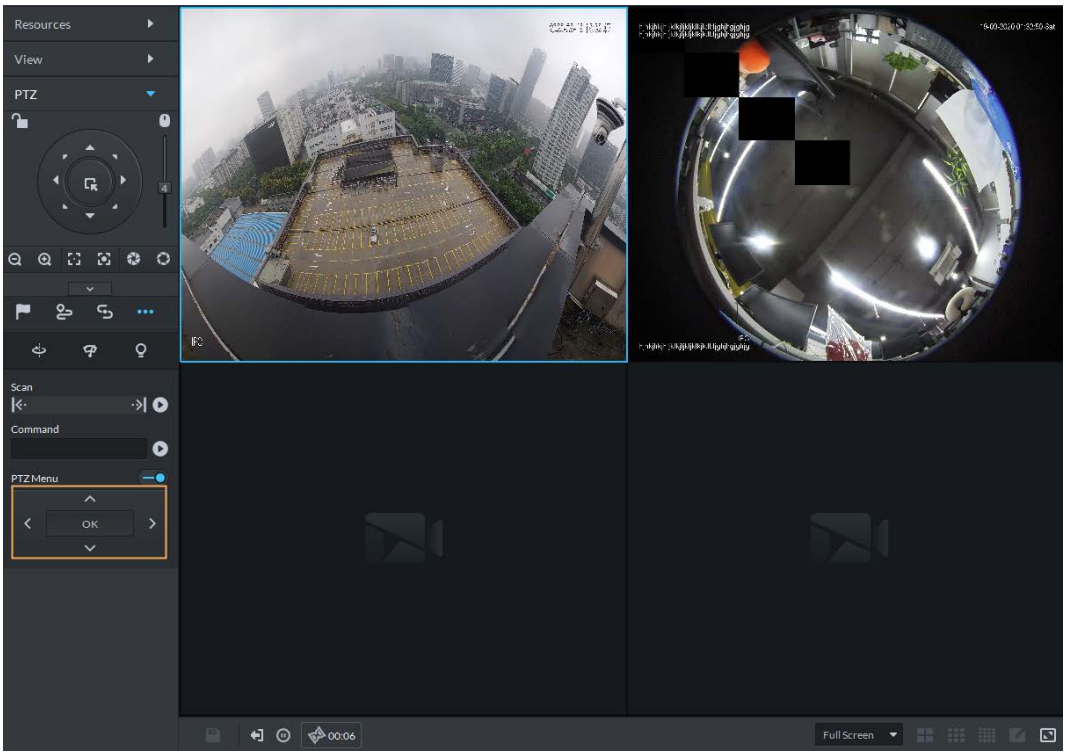


Table 5-5 PTZ menu description

Parameters	Description
/	Up/down button.
/	Left/right. Point to set parameters.

Parameters	Description
	Click  to enable PTZ menu function. System displays main menu on the monitor window.
	Click  to close PTZ menu function.
OK	It is the confirm button. It has the following functions. ● If the main menu has the sub-menu, click **OK** to enter the sub-menu. ● Point to **Back** and then click **OK** to go to go back to the previous menu. ● Point to **Exit** and then click **OK** to exit the menu.
Camera	Point 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, and default.
PTZ	Point to **PTZ** and then click **OK** to go to PTZ sub-menu interface. Set PTZ functions. It includes preset, tour, scan, pattern, rotation, PTZ restart, and more.
System	Point to **System** and then click **OK** to go to system sub-menu interface. Set PTZ simulator, restore camera default settings, video camera software version and PTZ version.
Return	Point to the **Return** and then click **OK** to go back to the previous menu.
Exit	Point to the **Exit** and then click **OK** to exit PTZ menu.

5.1.2.5 Fisheye-PTZ Smart Track

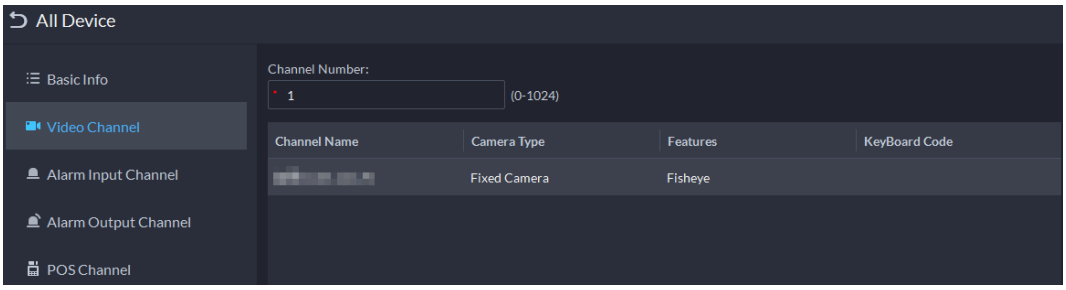
Link a PTZ camera to a fisheye camera so that when the fisheye camera detects a target, the PTZ camera automatically rotates to it and track.

5.1.2.5.1 Preparations

Make sure the following preparations have been completed:

- Fisheye camera and PTZ camera are well deployed. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. For details, see "3 Basic Configurations".
  - When adding cameras, select **Encoder** from **Device Category**.
  - **Features** of fisheye camera is set to **Fisheye**. For details, see "3.2.2.5.1 Modifying Device Information".

Figure 5-25 Set fisheye camera features



5.1.2.5.2 Configuring Fisheye-PTZ Smart Track

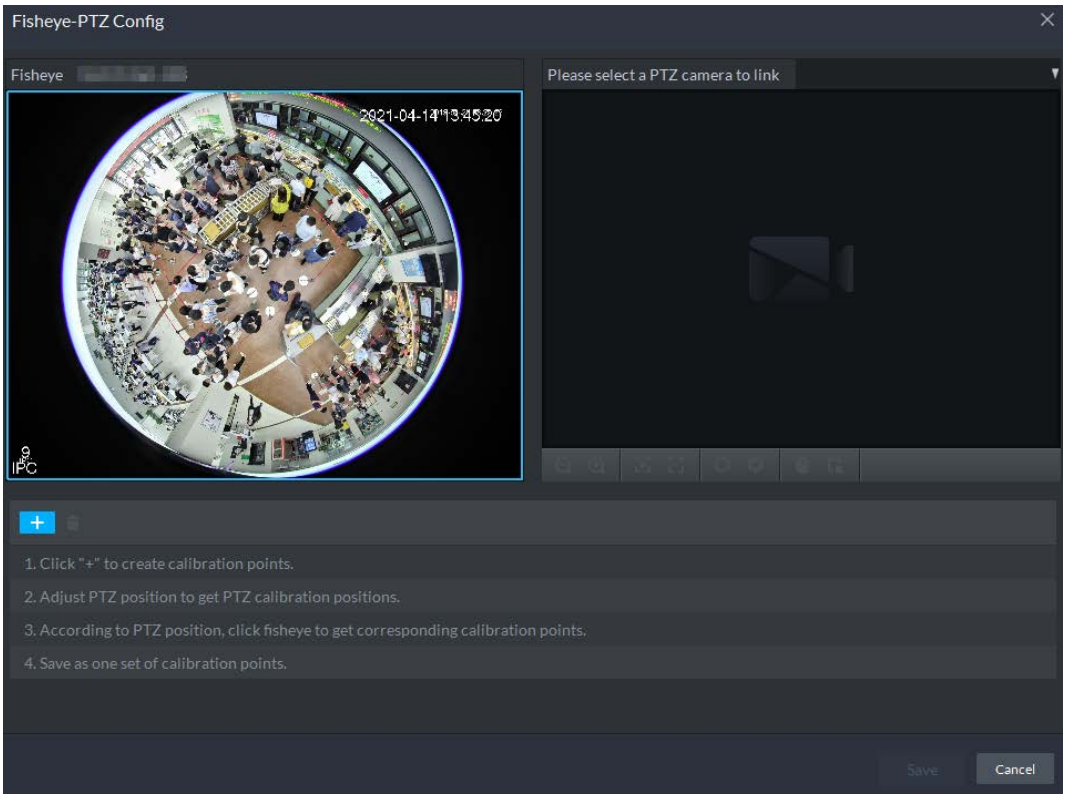
Step 1 Log in to the DSS Client. On the **Home** interface, click  , and then click **Monitoring Center**.

Step 2 Click  .

Step 3 In the device tree on the left, right-click a fisheye camera, and then select **Modify Smart Track**.

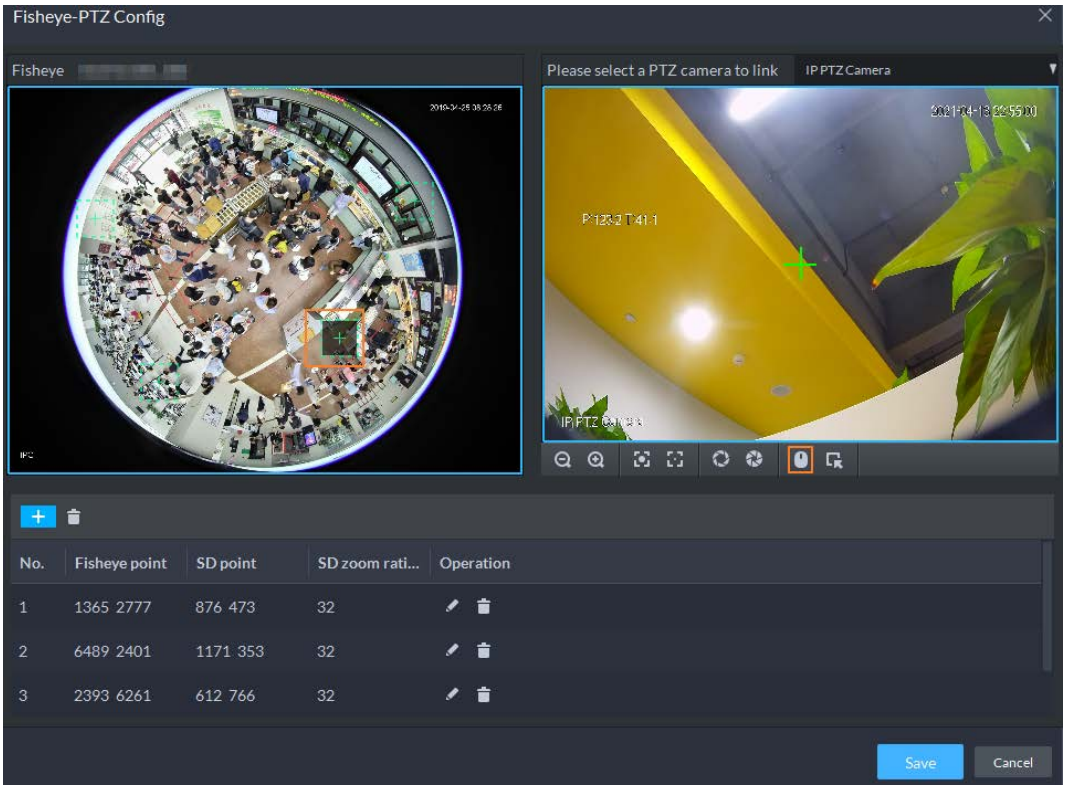
Step 4 Click next to **Please select a PTZ camera to link**, and then select a PTZ camera.

Figure 5-26 Set smart track rules (1)



Step 5 Click and then move the of the fisheye on the left to select a position. Click of the PTZ camera to find the position. Adjust the PTZ camera to find the position and move the PTZ to the center position (The green cross on the image).

Figure 5-27 Set smart track rules (2)



- Select 3-8 mark points on fisheye camera.
- When you find mark point on the right side of the 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 6 Click to save the calibration point.

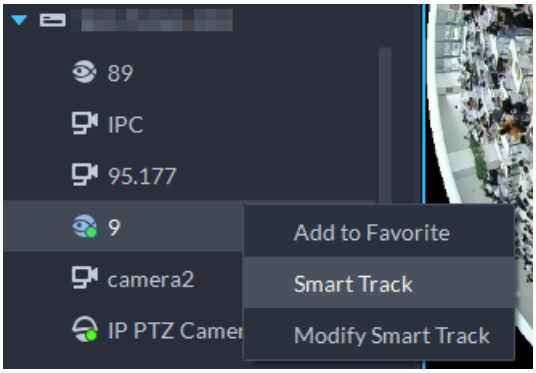
See above steps to add at least three calibration points. These three points shall not be on the same straight line.

Step 7 Click **Save**.

5.1.2.5.3 Applying Fisheye-PTZ Smart Track

Step 1 Log in to the DSS Client. On the **Monitoring Center** interface, select the fisheye camera on the device tree and then right-click to select **Smart Track**.

Figure 5-28 Select a smart track channel



Step 2 Click any point on the left of fisheye, PTZ camera on the right will automatically rotate to

corresponding position.

5.1.2.6 Bullet-PTZ Smart Track

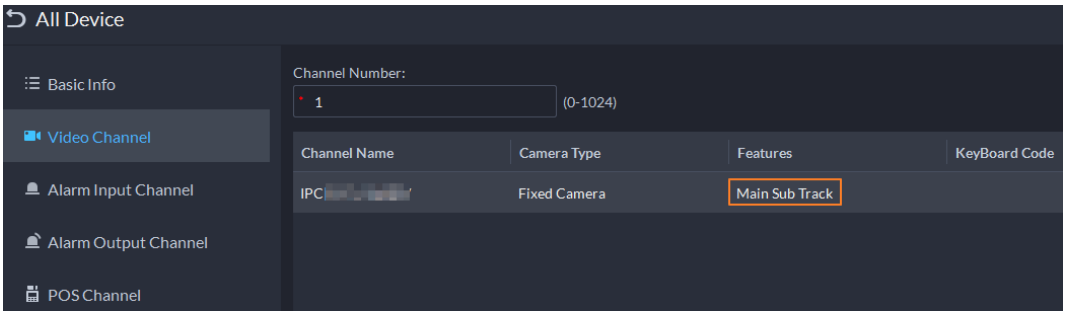
When a target is detected in the bullet camera view, the PTZ camera can automatically go to track the target.

5.1.2.6.1 Preparations

Make sure that the following preparations have been completed:

- Cameras are well deployed. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. For details, see "3 Basic Configurations". During configuration, note that:
  - When adding cameras, select **Encoder** from **Device Category**.
  - **Features** of the panoramic + PTZ camera, starlight smart capture camera, or bullet-PTZ camera is set to **Main Sub Track**. For details, see "3.2.2.5.1 Modifying Device Information".

Figure 5-29 Set camera features



5.1.2.6.2 Configuring Bullet-PTZ Smart Track

Relate bullet camera view to PTZ camera view. Skip this section if you use panoramic + PTZ camera.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

Step 2 Click .

Step 3 Right-click the bullet camera, and then select **Bullet-PTZ Smart Track Config**.

Step 4 Set bullet camera and PTZ camera parameters.

- Separate mode: The bullet camera and PTZ camera are separate. Their login information is different. The bullet camera information is already displayed. Specify PTZ camera information as needed.
- Bullet-PTZ camera: The bullet camera and PTZ camera are integrated in one camera. Their login information is the same.

Step 5 Click **Login and Link** to open the smart track calibration interface.

Step 6 Use the PTZ control panel to rotate the PTZ camera view on the left side to the position where the bullet camera is overlooking.

Step 7 Click **Start**.

During the calibration, PTZ control is unavailable to ensure accuracy of calibration. To operate PTZ during the calibration, click **Pause**. To resume calibrating, click **Start**.

Step 8 Calibrate coordinates.

1) Click **Add** next to **Coordinate 1**, and then two frames appear in the bullet view. Move the two frames to the same positions, and then the coordinate values appear in the boxes of the **Coordinate 1**.
2) Repeat the previous step to finish the remaining 3 coordinate groups.
3) Click **Save**.
4) Click **OK** on the confirmation dialogue box.
5) Complete the calibration of all coordinates.
   The **Apply** button is highlighted on the finishing interface.
6) Click **Apply**.

5.1.2.6.3 Applying Bullet-PTZ Smart Track

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

Manual Positioning

Click any position on the bullet image, and the PTZ will position the image to the area. Click the red spot on the bullet image, and the PTZ central point will move to the corresponding location automatically.

Figure 5-30 Manual positioning

Before Positioning

After Positioning

3D Positioning

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

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

camera.

Figure 5-31 3D positioning (1)

Figure 5-32 3D positioning (2)

Before Positioning

After Positioning

Manual Track

Bullet PTZ all-in-one camera, panoramic + PTZ camera and individual bullet have been configured with smart rules. For detailed operation, see device user's manual.

IVS Overlay is required to be selected on the bullet image, enable target box overlay. Target box will be displayed only when a moving target appears in the image.

Manual track priority is higher than auto track.

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

Figure 5-33 Manual track

Before Tracking

After Tracking

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, see device user's 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 **Video Surveillance** interface, select individual bullet, bullet PTZ all-in-one camera or panoramic + PTZ camera, right-click and select **Auto Track** > **On** and enable auto track. When there is moving target in the image, then PTZ camera will track the target

automatically.

Figure 5-34 Select automatic track

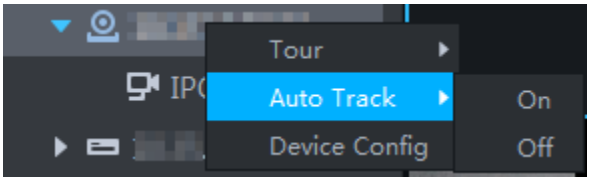


Figure 5-35 Automatic track

Before Tracking

After Tracking

Preset Return

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

5.1.3 Playback

Play back recorded videos.

5.1.3.1 Playback Interface

Log in to the DSS Client. On the **Home** interface, click , and then click **Monitoring Center**. Click

the **Playback** tab.

Figure 5-36 Playback interface

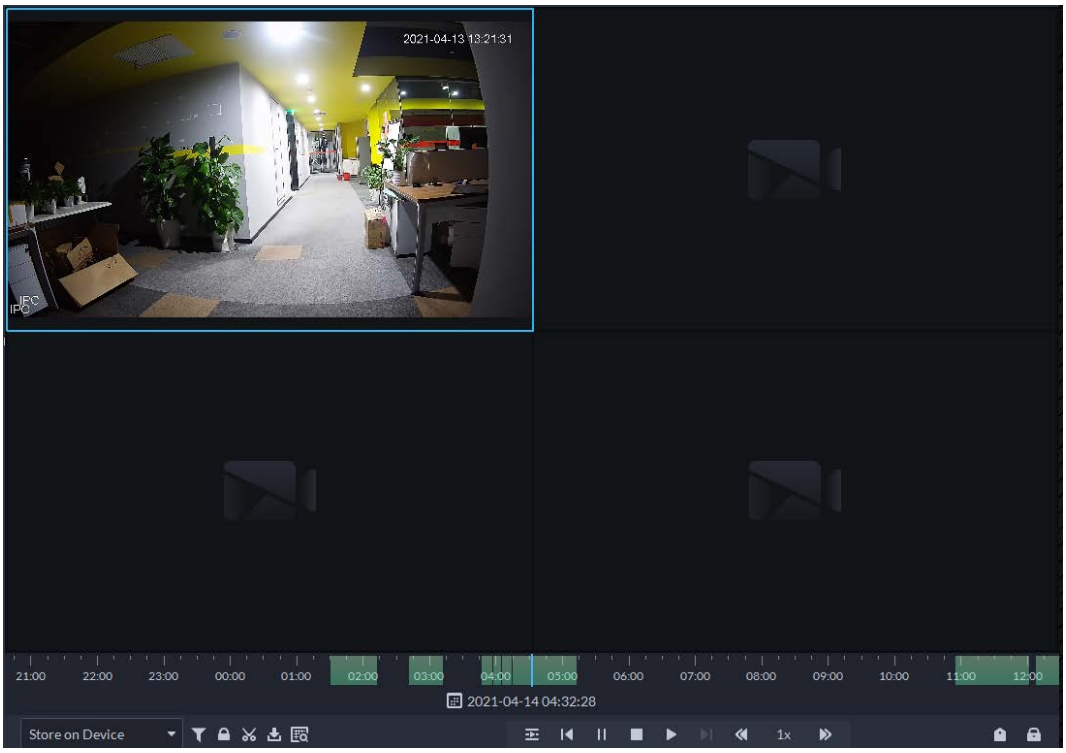


Table 5-6 Description

Icon	Description
	Lock the video stored to the 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, and it only plays back the video with dynamic image in the detection area.
	Play back recording 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.
Store on Server	Select the storage location of the video to be searched. Supports searching for the video on the platform server or storage device.
	Tag records.
	Lock records.

5.1.3.2 Playing Back Recorded Videos

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

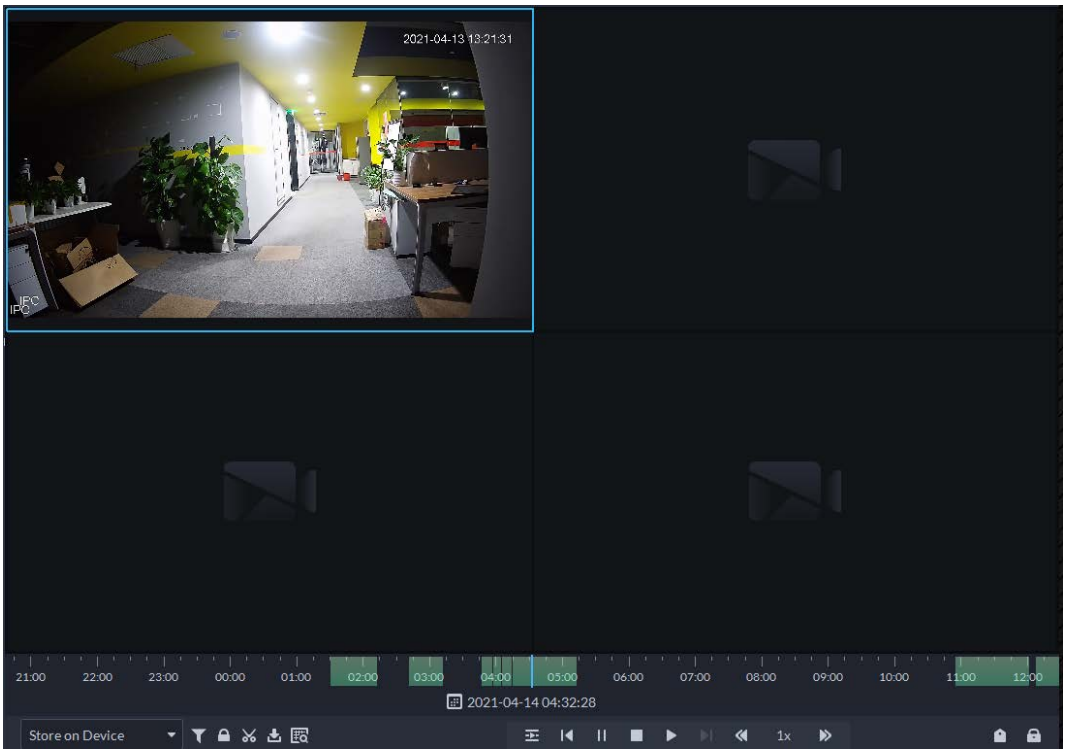
Step 2 Click the **Playback** tab.

Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Select the storage path of recorded video from Store on Server, and then click to select the date.

Dates with blue dot means there are video recordings.

Figure 5-37 Playback interface



Step 5 Click to play the video.

Step 6 Hover over the video, and then the icons appear. You can perform the following actions.

Figure 5-38 Video playback

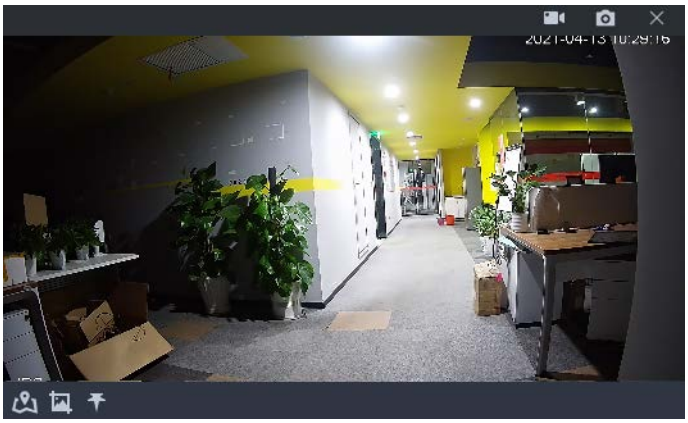


Table 5-7 Description

Icon	Name	Description
	Local recording	Click this icon to start recording. The recorded video is stored locally. The saving path is C:\DSS\DSS Client\Record\ by default.
	Snapshot	Take a snapshot of the current image and save it locally. The saving path is C:\DSS\DSS Client\Picture\by default.
	Close	Close the window.
	Map location	If the device has been marked on the map, click the icon to open the map in a new window to display map location of the device.
	Search by snapshot	Capture the target in the playback window. Click to select the search method, and then the system goes to the interface with search results. More operations: ● : Move the selection area. ● : Adjust the size of the selection area. ● Right-click to exit search by snapshot.
	Tag	Tag the videos of interest for easy search in the future.

Right-click the video, and then you can perform the following actions.

Figure 5-39 Shortcut menu

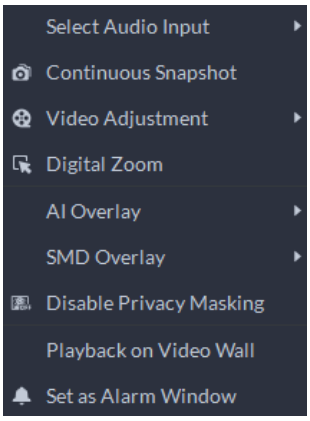


Table 5-8 Description

Parameters	Description
Select Audio Input	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Continuous Snapshot	Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to *..\DSS\DSS Client\Picture* by default. To change the snapshot saving path, see "8.3.5 Configure File Storage Settings".
Video Adjustment	Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement.
Digital Zoom	Click it, and then double-click the video image to zoom in the image. Double-click the image again to exit zooming in.
AI Overlay	The client does not show rule lines over live video by default. When needed, you can click **AI Overlay** and enable **Rule Overlay** and **Bounding Box Overlay**, and then the live video shows rule lines if the AI detection rules are enabled on the device. This configuration is effective with the current selected channel both in live view and playback.
SMD Overlay	Enable **SMD Overlay** to show target bounding box over live video. When SMD is enabled on the device, you can enable **SMD Overlay** for the device channel, and then the live video will display dynamic target bounding boxes. This configuration is effective with the current selected channel both in live view and playback.
Disable Privacy Masking	For a camera that supports privacy masking of human face, you can disable the masking here to view the face image.
Playback on Video Wall	Play the video of the current channel on video wall. Make sure that video wall is configured (see "5.1.5 Video Wall").
Set as Alarm Window	When selecting open alarm linkage video **In Preview**(in live window) from **Local Settings > Alarm**, then the video will be displayed on the window which is set to alarm window. If multiple alarms are triggered, the video linked to the latest alarm will be opened. If the number of alarm windows is fewer than the number of linkage videos, the video linked to the earliest-triggered alarm will be opened. After enabling **Set as Alarm Window**, the window frame is displayed in red.

5.1.3.3 Locking Videos

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

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

Step 2 Click the **Playback** tab.

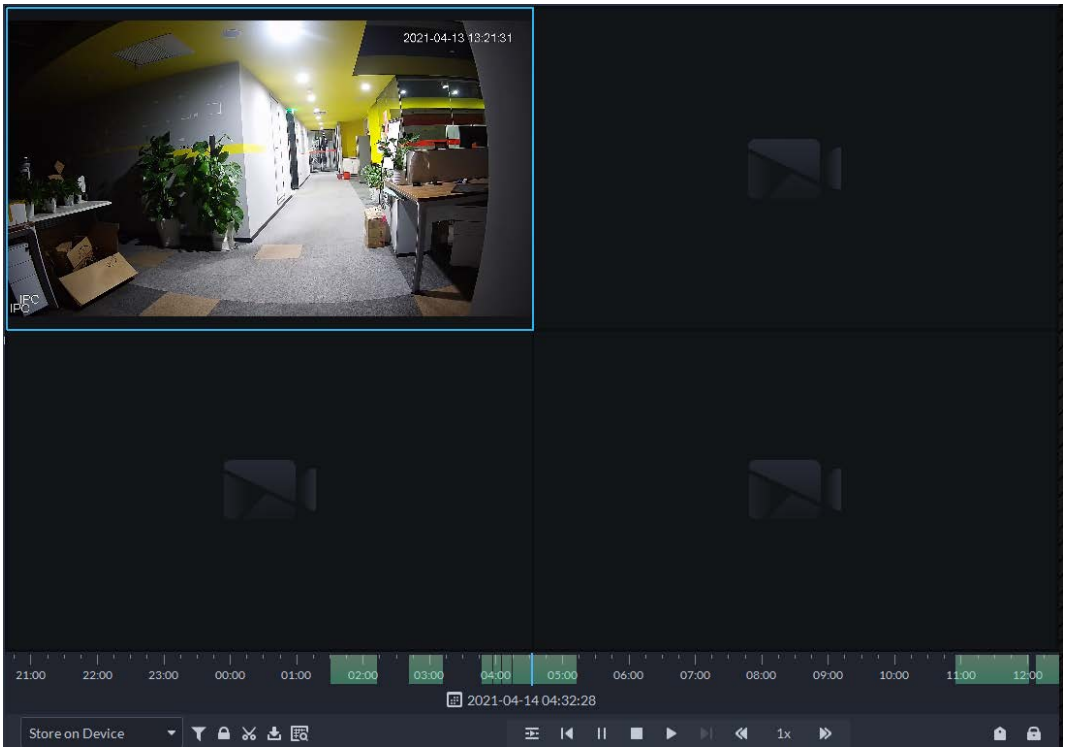
Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Select the storage path of recorded video from Store on Server, and then click to select the date.

The search results are displayed.

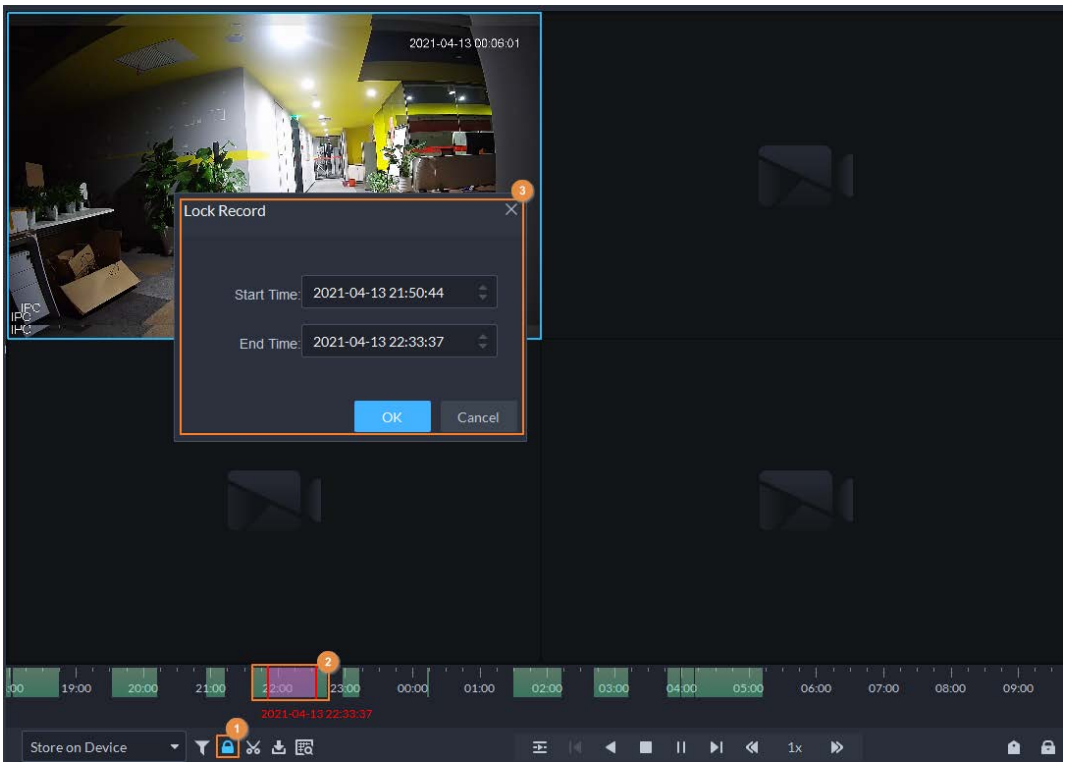
Dates with blue dot means there are video recordings.

Figure 5-40 Playback interface



Step 5 Select a window that has recorded video, and then click on the bottom of the interface, and then click on the timeline to mark the start point and end point of the video clip you need.

Figure 5-41 Lock record



Step 6 Confirm the start and end time, and then click **OK**.

5.1.3.4 Tagging Videos

You can tag records of interest for quick search.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

Step 2 Click the **Playback** tab.

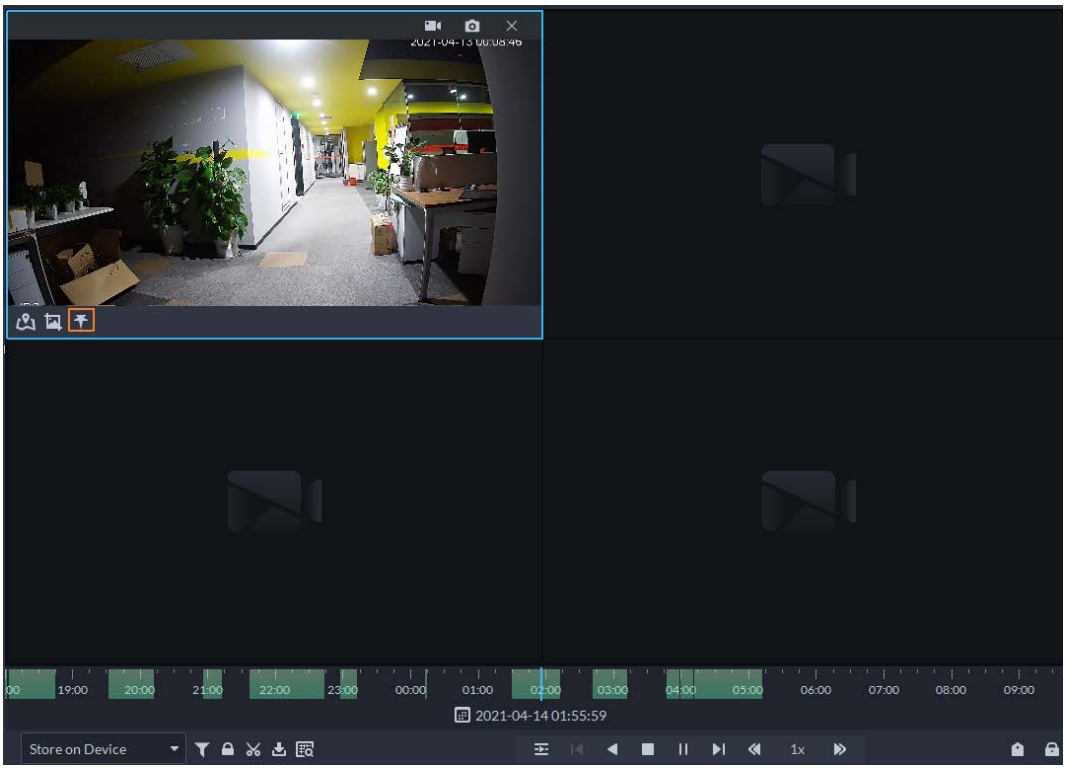
Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Select the storage path of recorded video from Store on Server, and then click to select the date.

The search results are displayed.

Dates with blue dot means there are video recordings.

Figure 5-42 Playback interface



Step 5 Point to the window that is playing record, and then click .

Step 6 Name the tag, and then click **OK**.

5.1.3.5 Filtering Record Type

Filter video according to record type, record type includes scheduled record, alarm record, and motion detection record.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

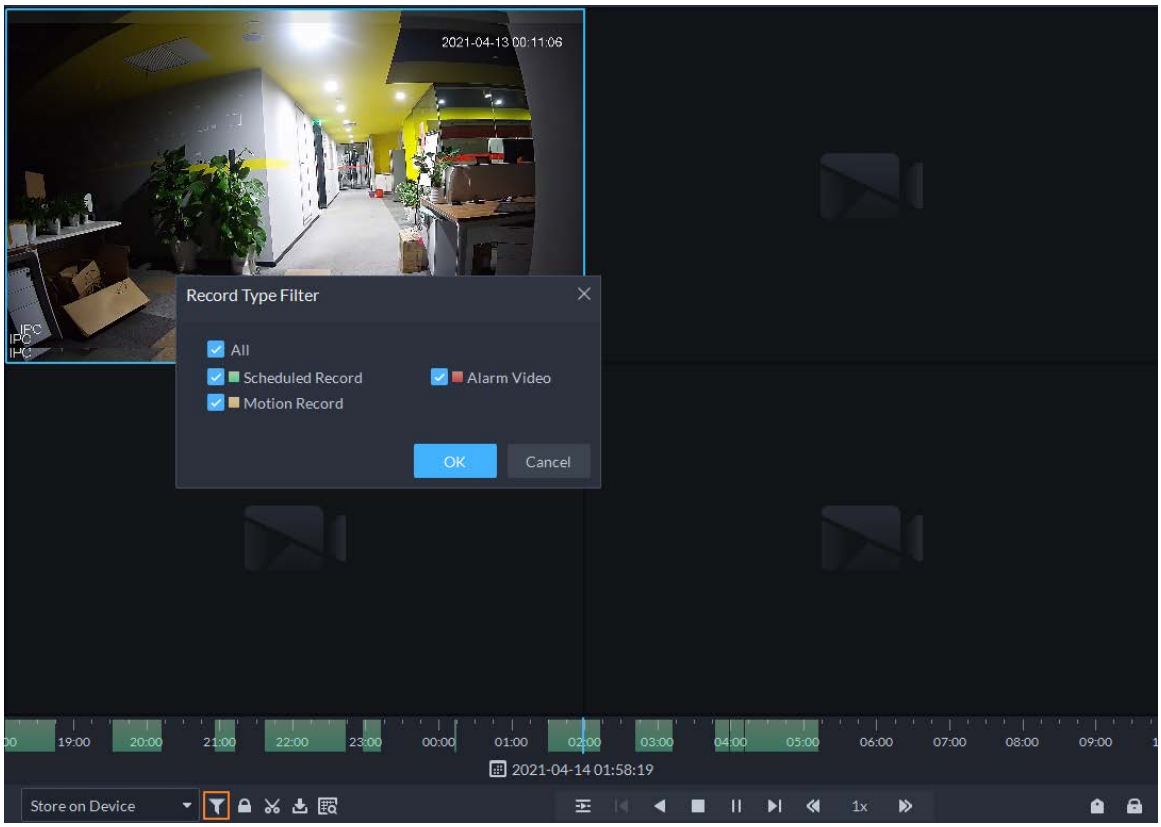
Step 2 Click the **Playback** tab.

Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Click , select a record type (or types), and then click **OK**.

The system only displays videos of the selected type.

Figure 5-43 Filter record type



5.1.3.6 Clipping Videos

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

Step 2 Click the **Playback** tab.

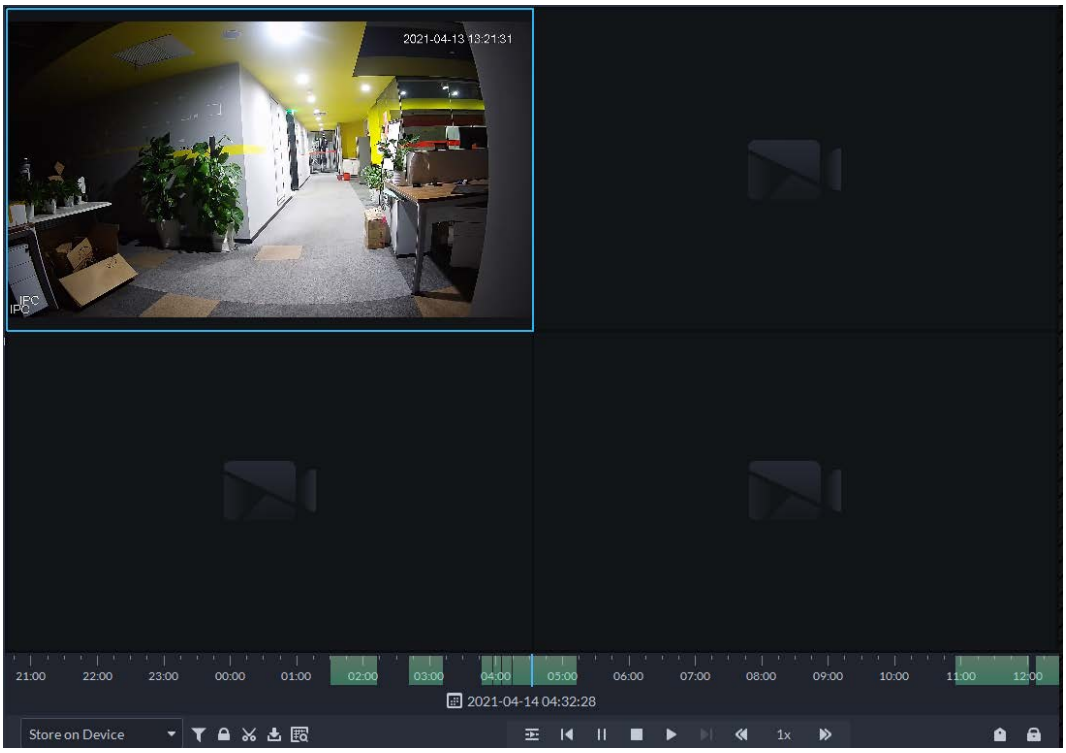
Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Select the storage path of recorded video from Store on Server, and then click to select the date.

The search results are displayed.

Dates with blue dot means there are video recordings.

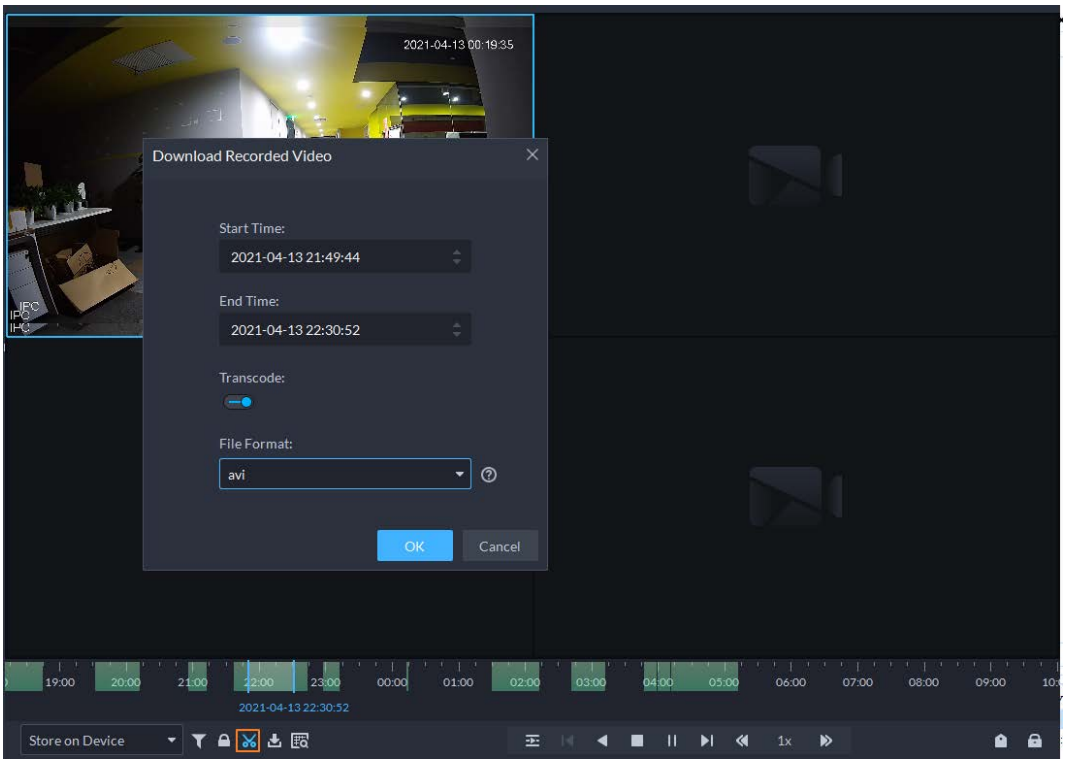
Figure 5-44 Playback interface



Step 5 Select a date with video recordings, and then click .

Step 6 On the timeline, click the point with green shade to start clipping, drag your mouse, and then click again to stop clipping.

Figure 5-45 Download recorded video



Step 7 Enter the password for logging in to the DSS client.

Step 8 (Optional) Enable **Transcode**, and then select the file format.

Step 9 Click **OK**.

5.1.3.7 Smart Search

With the smart search function, you can select a zone of interest on the video image to view motion records within this section. The relevant camera is required to support Smart Search; otherwise the search result will be empty.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center**.

Step 2 Click the **Playback** tab.

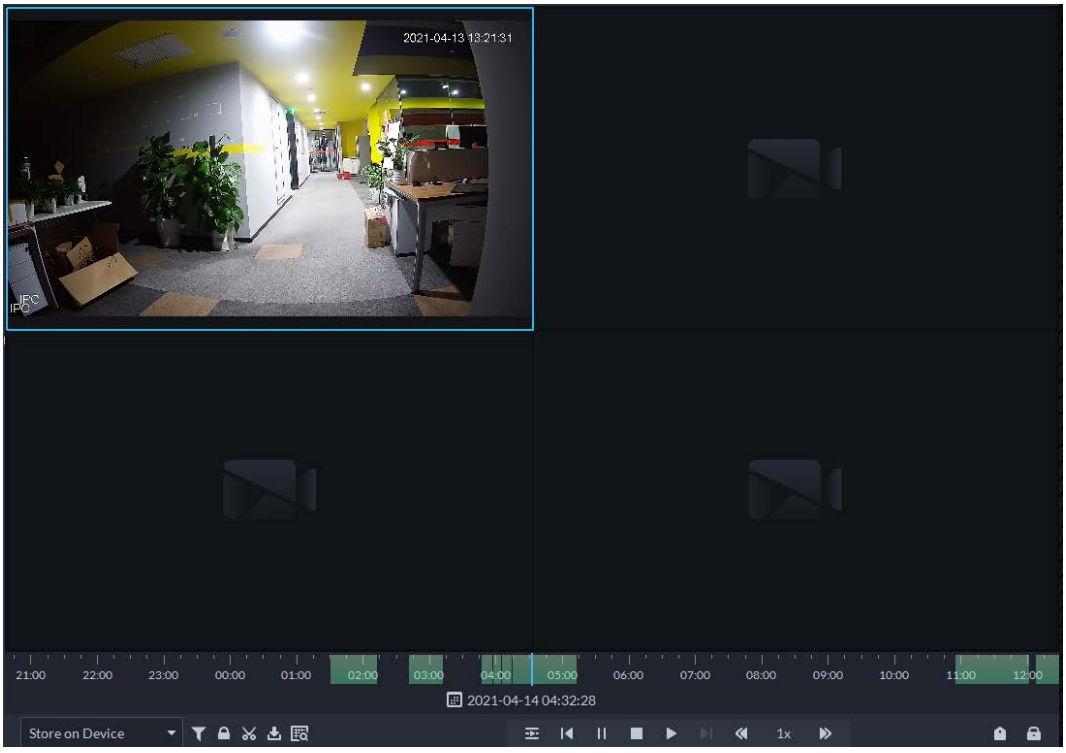
Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

Step 4 Select the storage path of recorded video from Store on Server, and then click to select the date.

The search results are displayed.

Dates with blue dot means there are video recordings.

Figure 5-46 Playback interface



Step 5 Select a window that has videos, click , and then select a type.

The smart search interface is displayed, with 22×18 squares in the window.

Figure 5-47 Smart search

Step 6 Click the squares and select detection areas.

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

Step 7 Click to start smart search analysis.

- If there are search results, the time progress bar will become purple and display dynamic frame.
- It will prompt that the device does not support smart search if the device you selected does not support the function.

Click to select the detection area again.

Step 8 Click the play button on the image or control bar.

The system plays search results, which are marked purple on the timeline.

Step 9 Click to exit smart search.

5.1.4 Map Applications

You can view video, cancel alarms, and view device locations on the map.

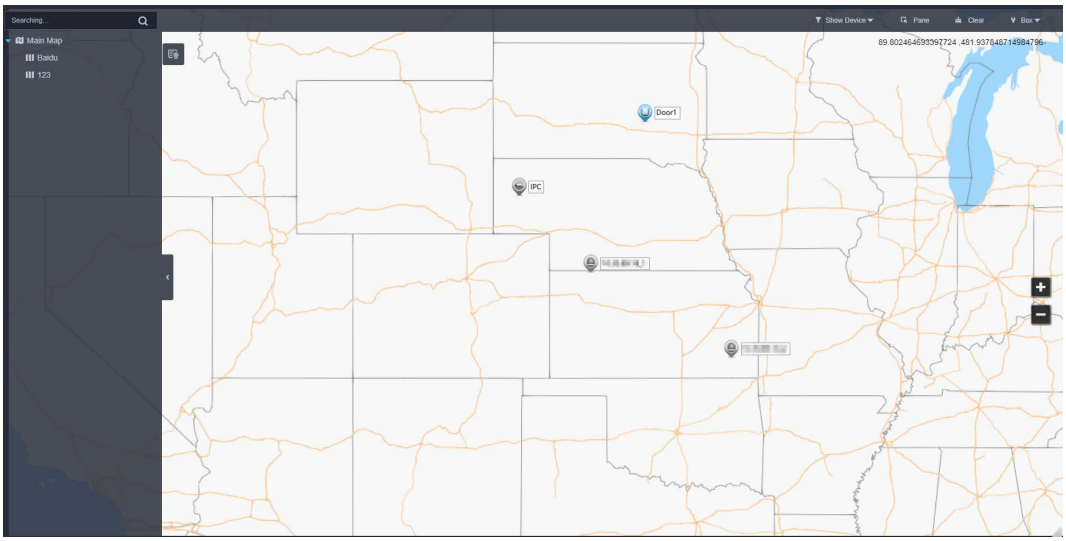
Make sure that you have configured a map. For details, see "4.2 Configuring Map".

Step 1 Log in to the DSS Client, and on the **Home** interface, select > **Monitoring Center**.

Step 2 Click .

Step 3 In the map list, double-click a map.

Figure 5-48 View map



Step 4 Click a device on the map, and then you can view video, cancel alarms, view longitude and latitude, and more.

Related Operations

There might be differences between the actions supported by different devices and map types.

- View live video
  Click **Pane**, select devices from the device tree, and then click to view videos in batches; or click on the map, and then select to view videos.
- Playback
  Click **Pane**, select devices from the device tree, and then click to view videos in batches; or click on the map, and then select to view videos.
- Cancel alarms
  Click a device on the map, and then select .
- Show devices
  On a raster map, you can select to display video channels, access control channels, alarm input channels, and defense zone alarms.
- Clear
  To clear all markings on the map, click **Clear**.
- Add marks
  Select **Box** > **Add Mark**, and then mark information on the map.
- Reset
  Select **Box** > **Reset** to restore the map to its initial position and zoom level.
- Click the hot zone to modify the map information of the hot zone.
- Double-click the hot zone, and then the system will automatically go to the hot zone map, where you can drag channels to the map.

5.1.5 Video Wall

A video wall, which consists of multiple video screens, is used for displaying videos on the wall, instead of small PC displays.

Complete video wall settings before you can view videos on the wall.

5.1.5.1 Configuring Video Wall

5.1.5.1.1 Preparations

To display video on the wall, make sure that:

- Cameras, decoders and video wall are well deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. For details, see "3 Basic Configurations". During configuration, make sure that:
  - When adding a camera, select **Encoder** from **Device Category**.
  - When adding a decoder, select **Video Wall Control** from **Device Category**.
- A glimpse of the video wall configuration interface

Figure 5-49 Video wall interface

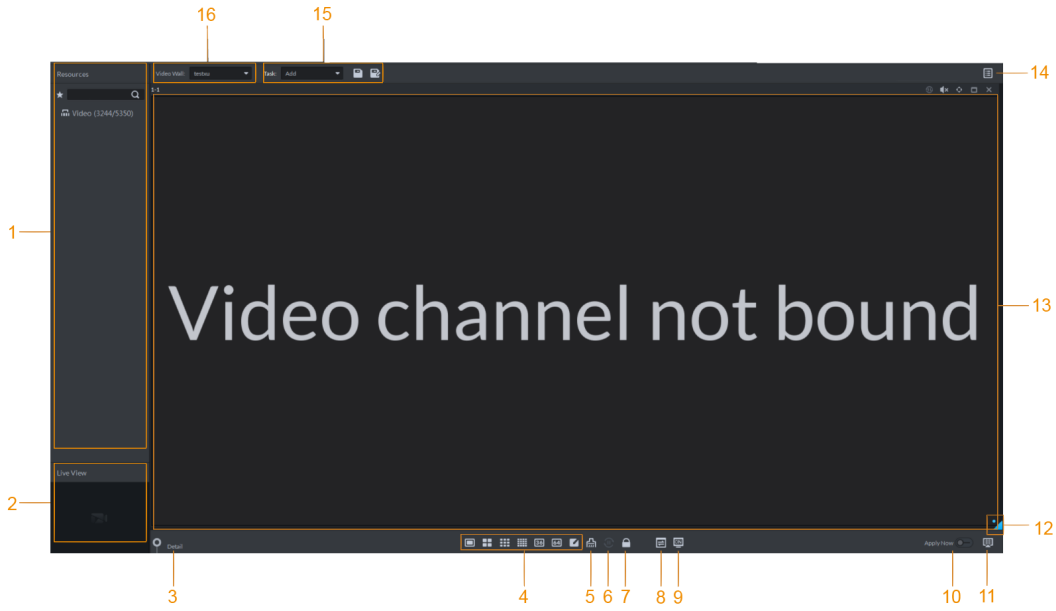


Table 5-9 Description

No.	Name	Function
1	Device tree	If you enable **Show device node** in **Local Settings** > **Basic**, the device tree will display devices and all channels. If you clear the **Show device node** check box, the device tree will only display channels. Click ★ to view the channels in the **Favorites** folder. Support searching for devices or channels by entering device name or channel name in Search.. .
2	Live view	View channel video.

No.	Name	Function
3	Detailed information	View the screen, window, and channel bound information. ● Click to view live video of the current channel at the bottom left. ● Click to adjust sequence. ● Click to delete the video channel on the current window. ● Click the **Stay Time(s)** column or click to modify the video play duration of the current channel during tour. ● Click the **Stream** column or to modify stream type.
4	Window split	Set window split mode.
5	Clear	Clear all screens.
6	Start/stop all tours	Start or stop all tours.
7	Lock window	Click to lock the window. Operation is not allowed on a locked window.
8	Back display	View video image of the selected channel window.
9	Screen on/off	Turn a screen on or off.
10	Apply now	If you enable the function, system automatically outputs the video to the wall after you set the task.
11	Decode to wall	Click it to manually output the video to the wall.
12	Eagle eye	View current video wall layout.
13	Video wall	Video wall area.
14	Video wall task	Configure scheduled tasks and tour tasks.
15	Task management	Add, save or delete a task.
16	Video wall selection	Select a video wall.

5.1.5.1.2 Adding Video Wall

Add a video wall layout on the platform.

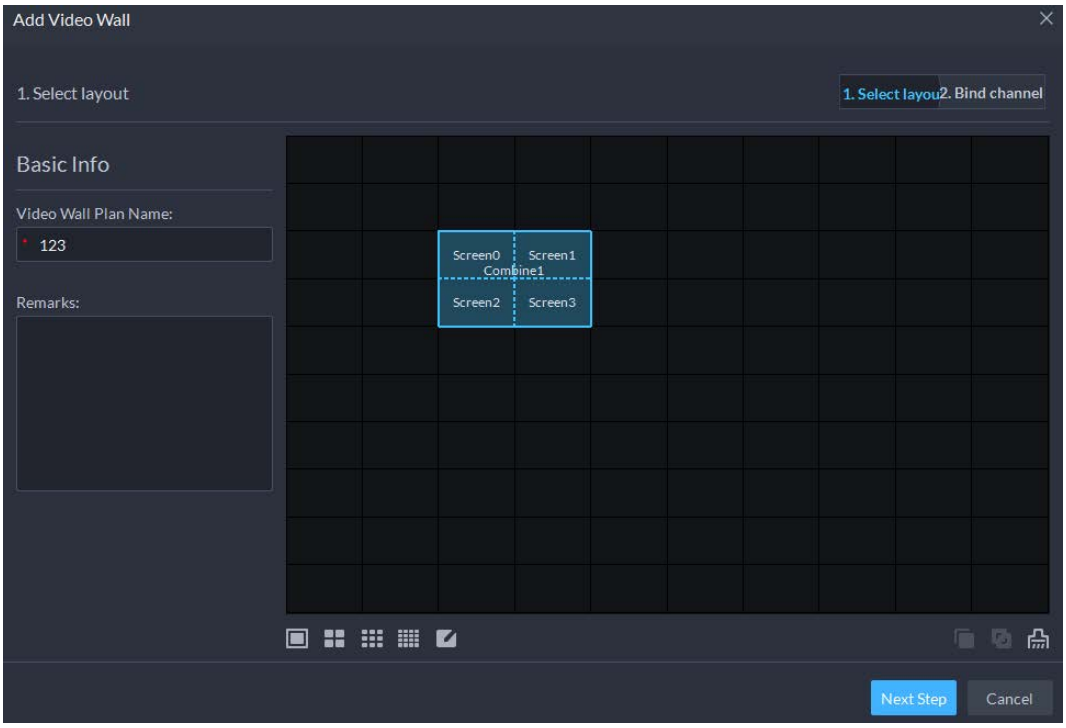
Step 1 Log in to the DSS Client, and on the **Home** interface, select **Monitoring Center** > .

Step 2 From the **Video Wall** drop-down list, select **Add New Video Wall**.

Step 3 Enter **Video Wall Name**, and then select a window splicing mode.

- Select a splicing mode from among 1×1, 2×2, 3×3, 4×4 or set a custom mode by clicking .
- A multi-screen splicing mode is a combined screen by default. You can perform video roaming on it. For example, with a 2×2 combined screen, if you close 3 of them, the other one will be spread out on the combined screen. To cancel combination, click the combined screen, and then click .
- To create a combined screen, press and hold Ctrl, select multiple screens, and then click .
- To clear the created screen, click .

Figure 5-50 Add a video wall



Step 4 Click **Next Step**.

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

- You can set whether to show ID in the screen, Show Screen ID means that the screen ID is disabled; click the icon and it becomes Show Screen ID, which means that screen ID is enabled.
- Each screen in a combined screen must be bound with a decoding channel.

Step 6 Click **Finish**.

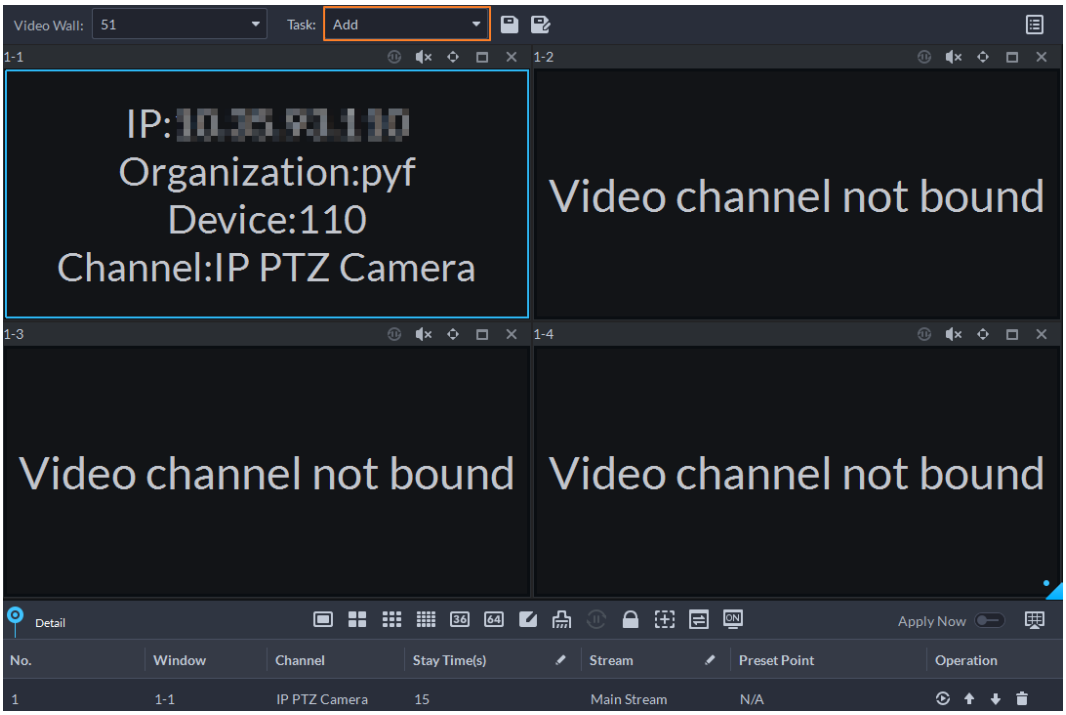
5.1.5.1.3 Configuring Video Wall Display Tasks

Display videos on the wall manually or in accordance with the pre-defined configuration.

Step 1 Log in to the DSS Client, and on the **Home** interface, select **Monitoring Center** > .

Step 2 In the **Task** drop-down list, select **Add**.

Figure 5-51 Add a video wall task



Step 3 From the device tree, select a camera, and then drag it to a screen, or select a window, drag the camera to the **Detail** section.

If you do not close video wall display in advance, this action will delete the bound camera and play the selected camera on the wall.

Step 4 Click .

If you have selected an existing task in the **Task** drop-down list, after dragging the video channel to the window, click to save it as a new task, which will be played on the wall immediately.

Step 5 Name the task, and then click **OK**.

- During video wall display of a task, if you have rebound the video channel, click to start video wall display manual.
- During video wall display, click or to stop or start tour display.

Step 6 Click to start video wall display.

5.1.5.1.4 Configuring Video Wall Plans

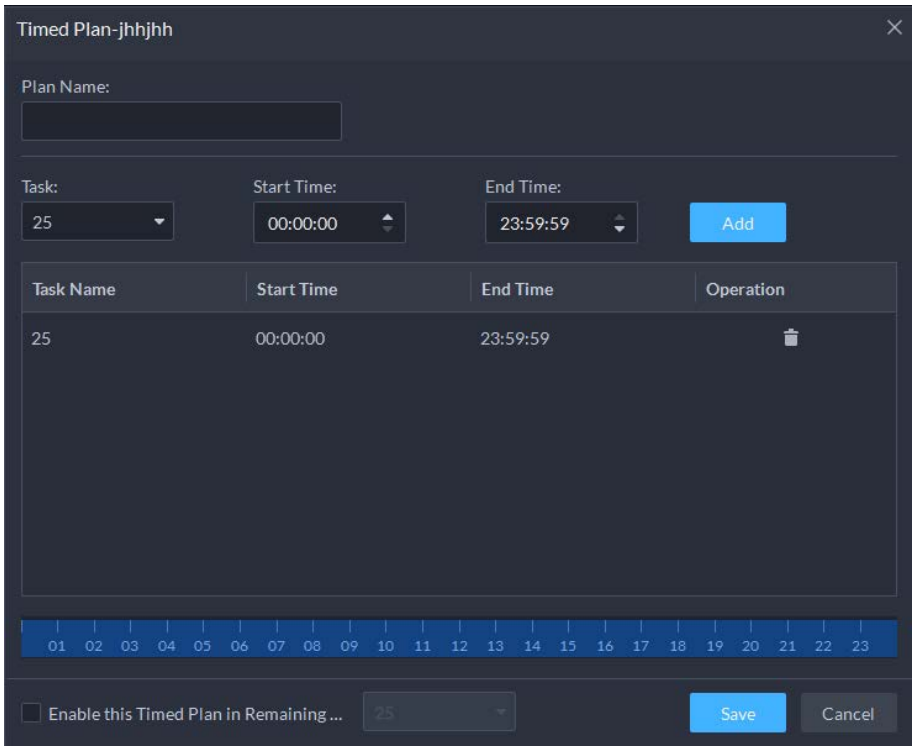
Configuring Timed Plans

Step 1 Log in to the DSS Client, and on the **Home** interface, select **Monitoring Center** > .

Step 2 Click on the upper-right corner.

Step 3 Hover over , and then select .

Figure 5-52 Set timed plan



Step 4 Enter the plan name.

Step 5 Select a video task, set start time and end time, and then click **Add**.

Repeat this step to add more tasks. The start time and the end time of tasks cannot be repeated.

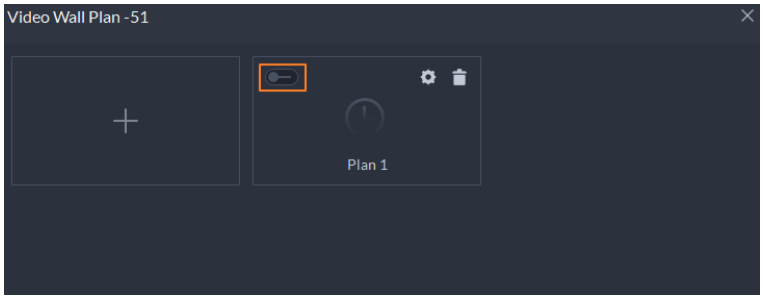
Select the **Enable This Timed Plan in Remaining Time** check box, and then set the task. The video wall displays the selected task during the remaining period.

Step 6 Click **Save**.

Step 7 Click to start the plan.

You cannot display multiple plans on the wall at the same time. When a plan is enabled, the previous plan on the wall is automatically terminated.

Figure 5-53 Enable timed plan



- Modify plan: .
- Delete plan: .

Configuring Tour Plans

After setting video wall tasks, you can configure the sequence and interval of tasks so that they can

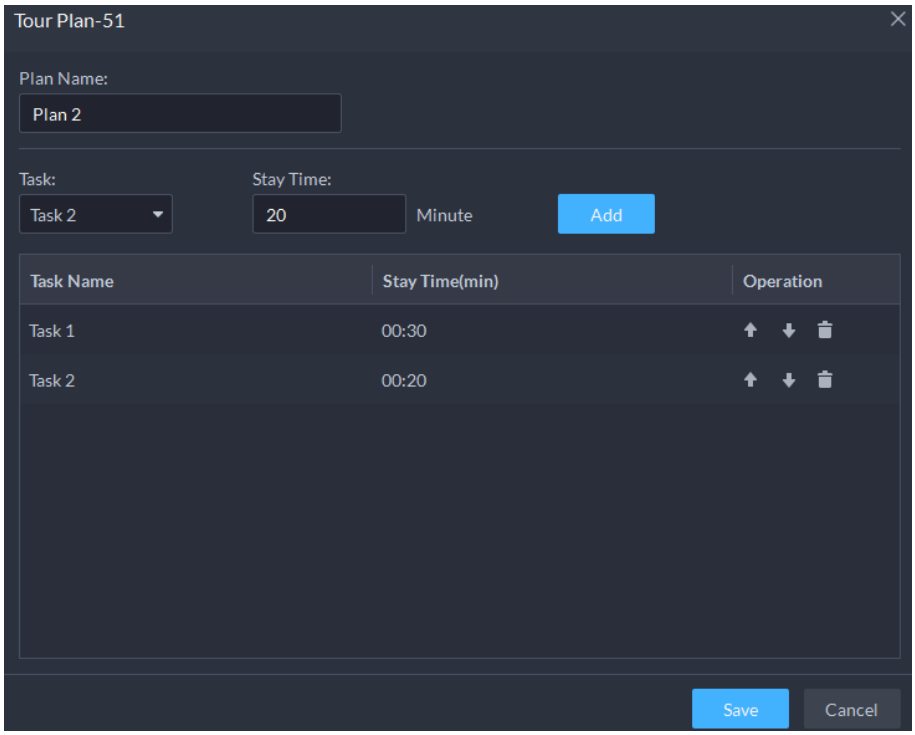
automatically play in turn on the wall.

Step 1 Log in to the DSS Client, and on the **Home** interface, select **Monitoring Center** > .

Step 2 Click on the upper-right corner.

Step 3 Hover over , and then select .

Figure 5-54 Tour plan

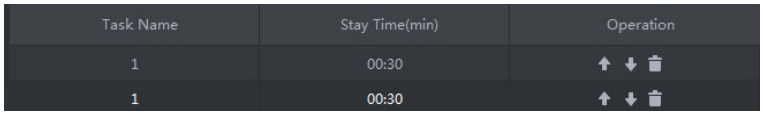


Step 4 Enter task name, select a video task and then set stay time. Click **Add**.

Repeat this step to add more tasks.

Click to adjust task sequence; click to delete a task.

Figure 5-55 Tour information

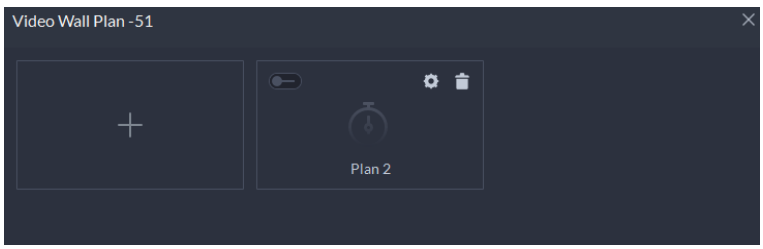


Step 5 Click **Save**.

Step 6 Click to start the tour plan.

You cannot display multiple plans on the wall at the same time. When a plan is enabled, the previous plan on the wall is automatically terminated.

Figure 5-56 Enable tour plan



- Modify plan: Click .
- Delete plan: Click .

5.1.5.2 Video Wall Applications

Make sure that decoder video ports are connected to the video wall screens.

5.1.5.2.1 Instant Display

Drag a camera to the video wall screen for instant display on the wall.

The video wall display task is configured. For details, see "5.1.5.1.3 Configuring Video Wall Display Tasks".

Step 1 Log in to the DSS Client, and on the **Home** interface, select **Monitoring Center** > .

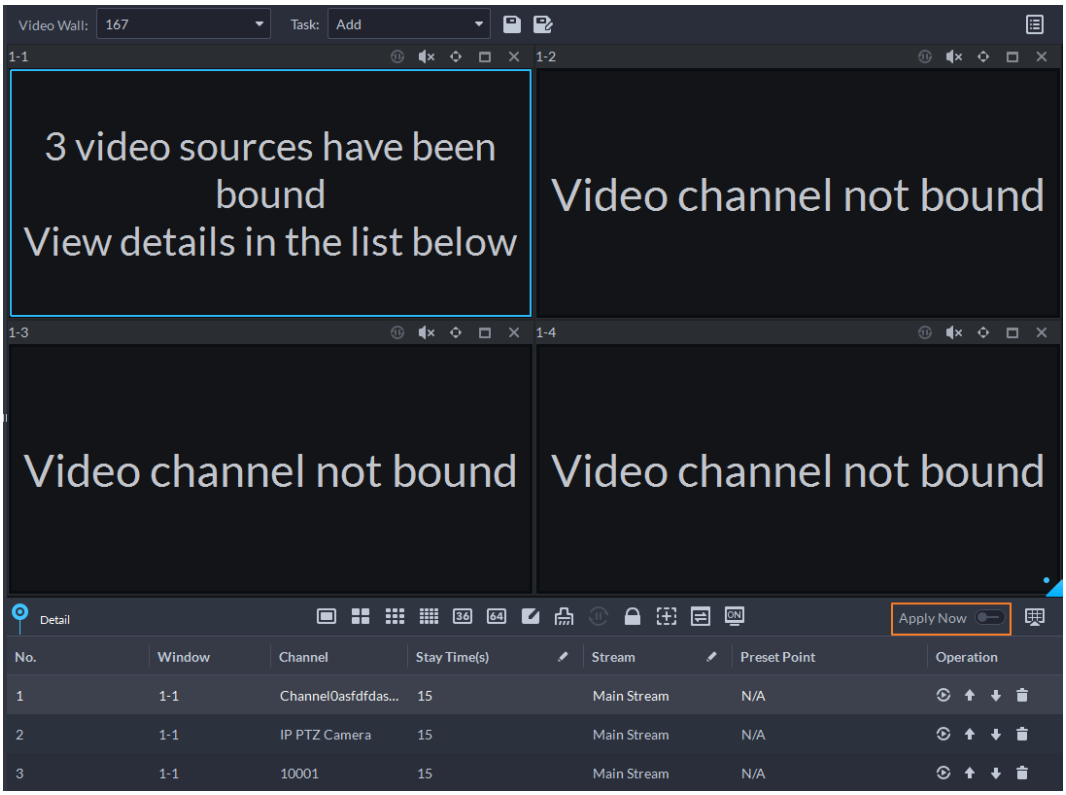
Step 2 In the **Video Wall** drop-down list, select a video wall.

Step 3 Click Apply Now to start video wall display.

Step 4 Drag a camera from the device tree to a screen, or select a window and drag the camera to the **Detail** section.

- A window can be bound to multiple video channels.
- The binding mode, which includes **Tour**, **Tile**, and **Inquiry**, can be set in **Local Settings** > **Video Wall**. For details, see "8.3.3 Configuring Video Wall Settings".
- For a fisheye camera, right-click it to select the installation mode for fisheye dewarping.

Figure 5-57 Bind video channel



Step 5 Select a screen, and then click **Detail** to view detailed information about the screen and channel, including stream type, preset and display sequence.

- Click to view live video of the current channel on the lower left.
- Click to adjust sequence.
- Click to delete the video channel on the current window.

5.1.5.2.2 Video Wall Task Display

Display a pre-defined task on video wall.

Step 1 Log in to the DSS Client, and on the **Home** interface, select **Tools** > **Video Wall**.

Step 2 In the **Task** drop-down list, select a task.

Step 3 Operations available.

- After changing the video channel that is being displayed, click at the lower-right corner before you can see the effect on video wall.
- Click / to pause or stop.
- Select a screen, and then click **Detail** to view detailed information about the screen and channel, including stream type, preset and display sequence.

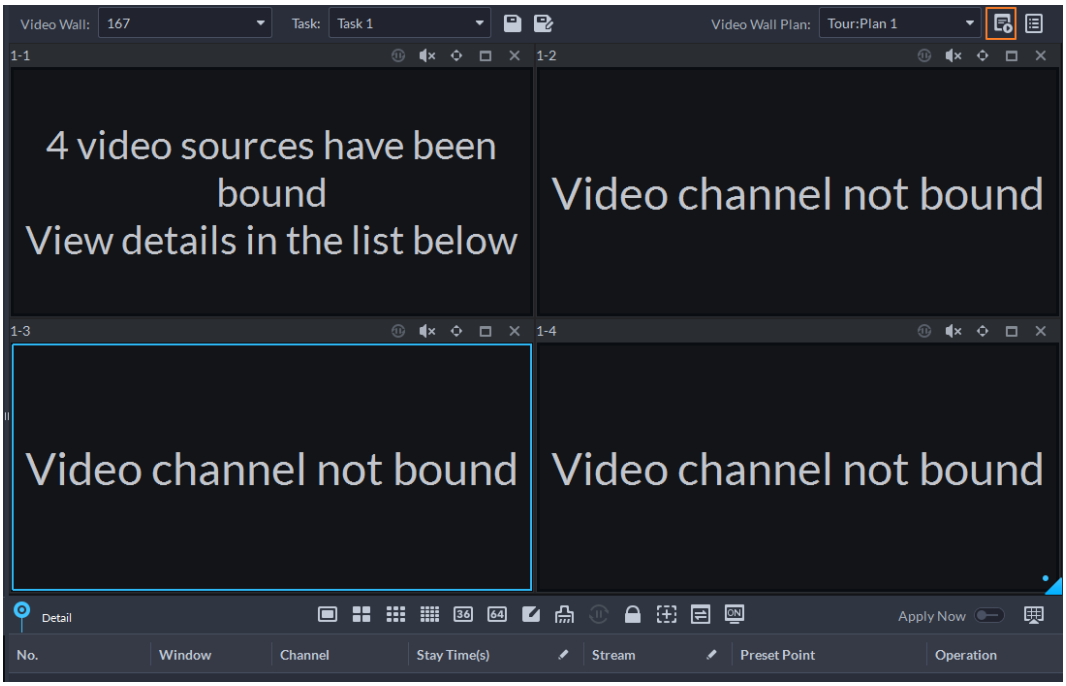
5.1.5.2.3 Video Wall Plan Display

Display a pre-defined plan on video wall.

Make sure that there are pre-defined plans. For details, see "5.1.5.1.4 Configuring Video Wall Plans".

The video wall automatically works as the plans have been configured. To stop the current plan, click on the upper-right corner of the **Video Wall** interface, and then it changes to . Click to start displaying video on wall again.

Figure 5-58 Display video wall plan



5.2 Event Center

You can view real-time alarms, and history alarms.

Make sure you have configured and enabled alarm events. To configure, see "4.1 Configuring Events".

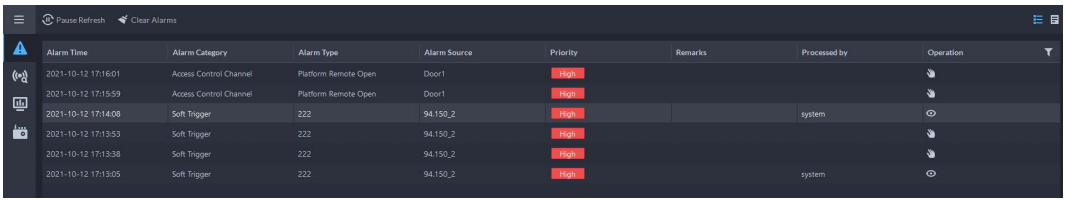
5.2.1 Real-time Alarms

View and process real-time alarms.

Step 1 Click .

The alarm list is refreshed in real time. To stop refreshing, click Pause Refresh; to resume refreshing, click Start Refresh.

Figure 5-59 Real-time alarms



Step 2 Click to claim an alarm.

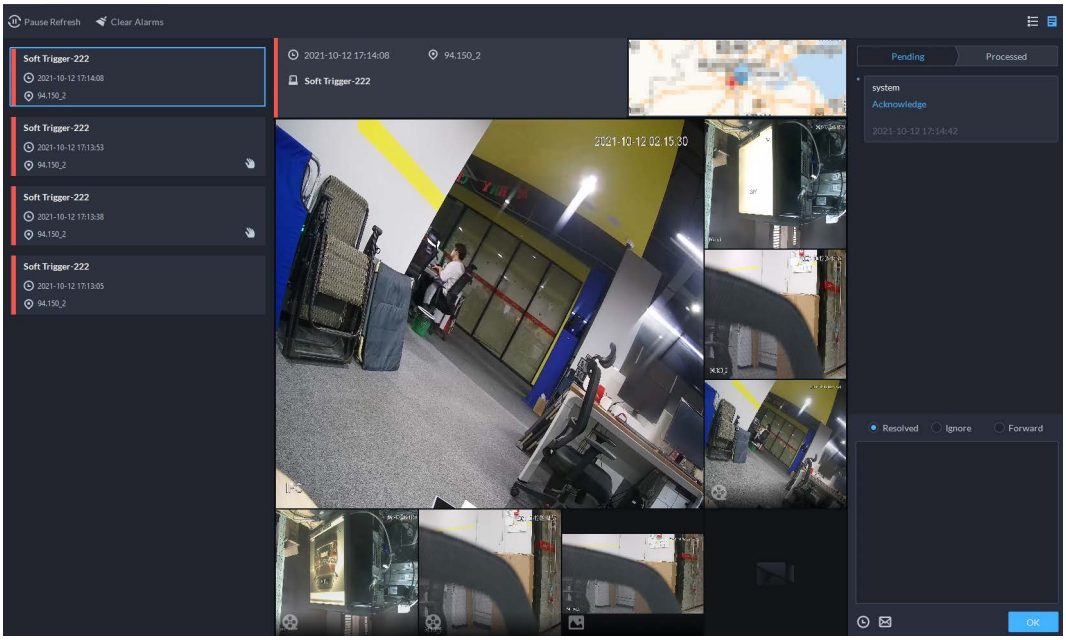
After an alarm has been claimed, the username of your account will be displayed under the **Processed by** column.

Step 3 Process alarms.

You can use the up and down arrow keys on the keyboard to quickly select other alarms.

1. Click or double-click the alarm.

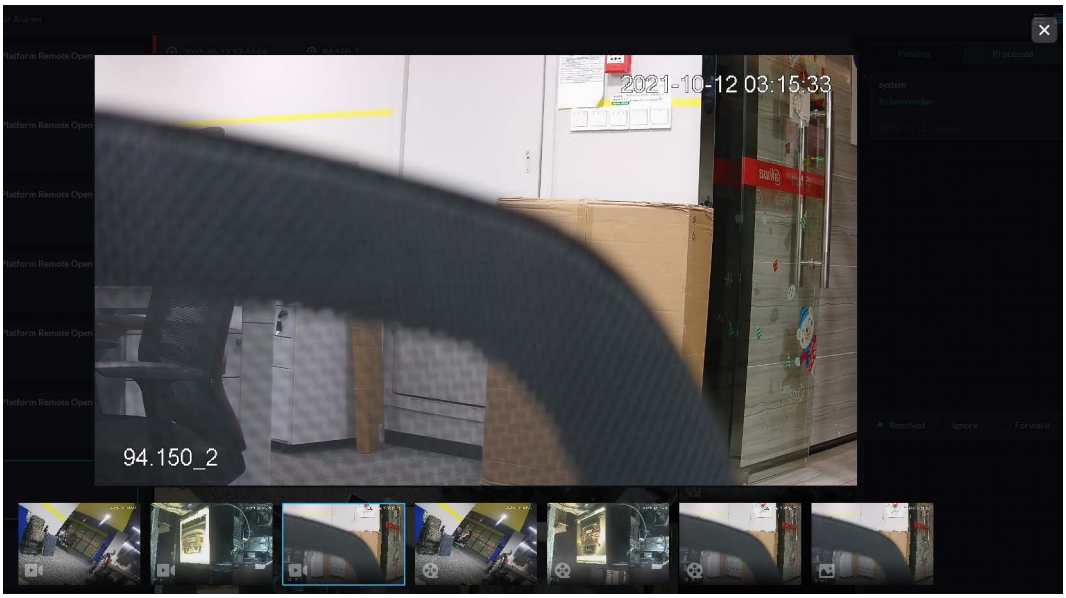
Figure 5-60 Alarm details



2. The middle area displays the time when the alarm was triggered, name and location of the alarm source, alarm type, and the live video images of linked channels, alarm videos, and alarm snapshots.

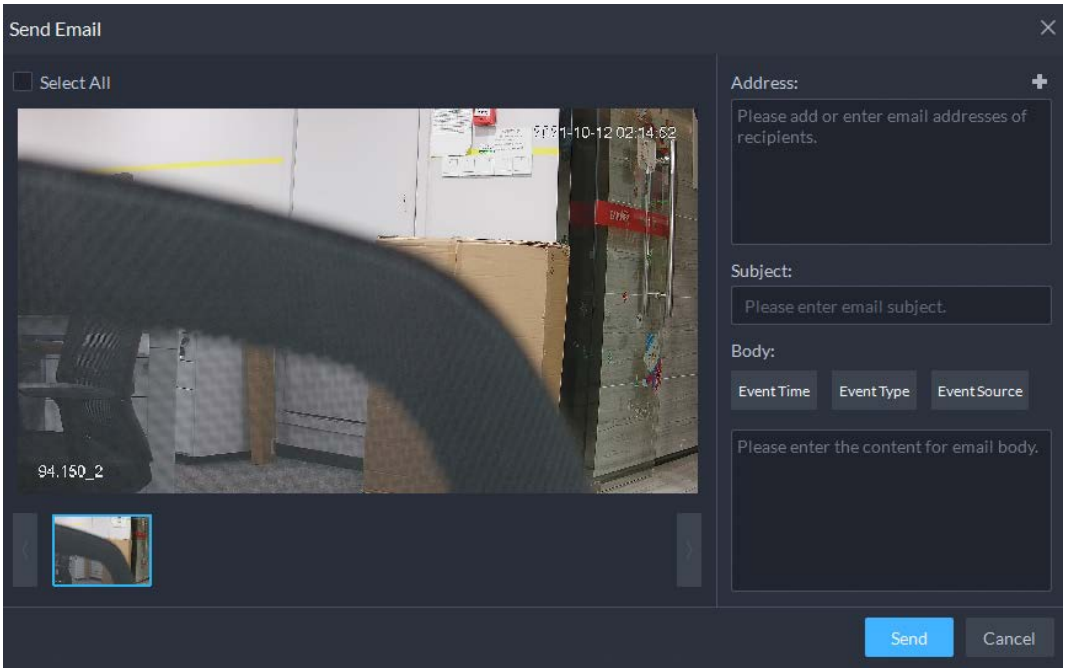
   Double-click a window to view them in larger size. Click to go back.

Figure 5-61 Alarm linkage media



3. On the right side, select how to process the alarm from **Resolved**, **Ignore**, or **Forward**. Enter comments, and then click **OK**.
   Forward allows you to forward the alarm to another user who will process it.
4. (Optional) Click to disarm the alarm. This alarm will not be triggered within the defined period.
5. (Optional) Click to send the alarm information to other users as a prompt or an email.

Figure 5-62 Send email



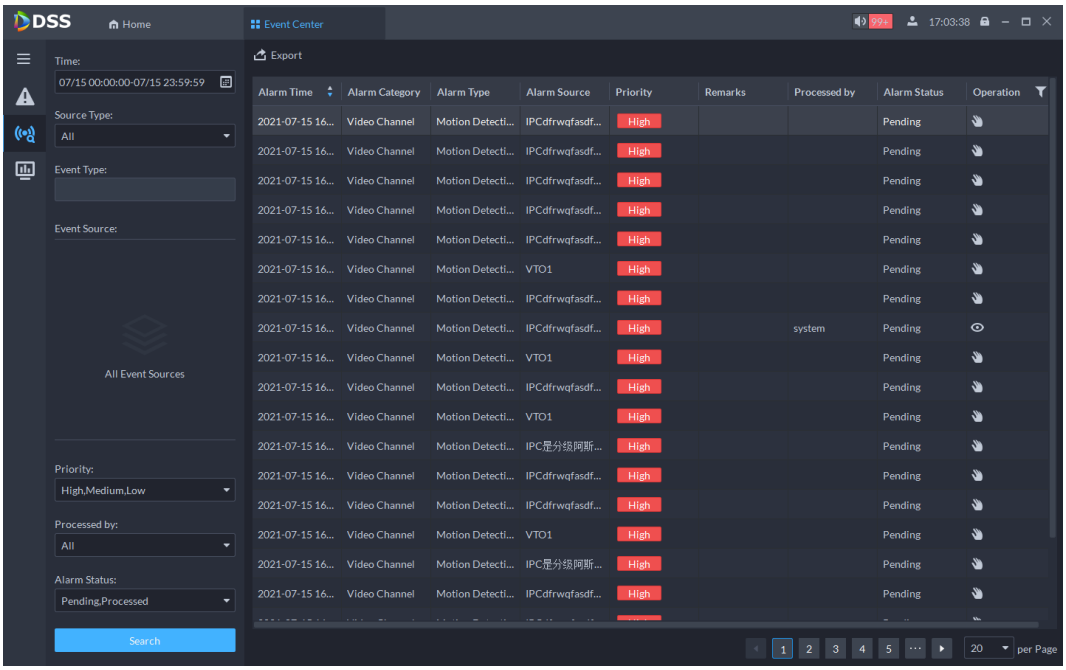
5.2.2 History Alarms

Search for and process history alarms.

Step 1 Click .

Step 2 Set search conditions, and then click **Search**.

Figure 5-63 history alarms



Step 3 Claim and process alarms, see "5.2.1 Real-time Alarms".

You can use the up and down arrow keys on the keyboard to quickly select other alarms.

5.3 DeepXplore

You can set multiple search conditions to view records of people, vehicle snapshots and access.

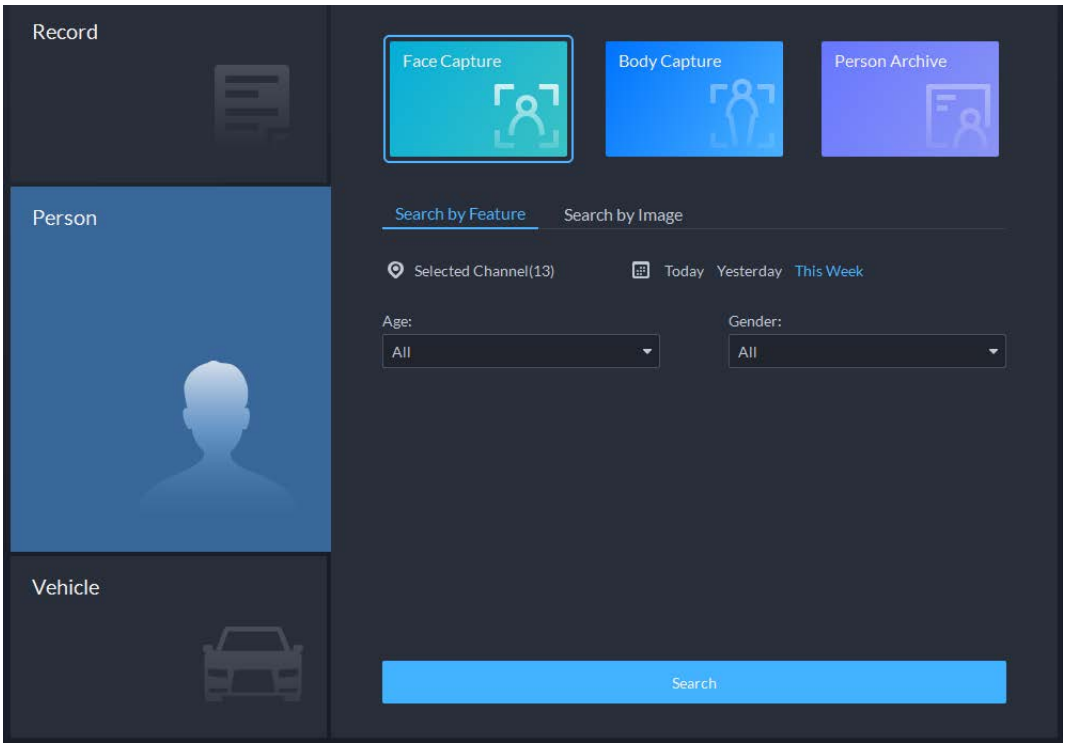
5.3.1 Searching for People

Based on the defined search conditions, you can view records of people face, body and related information from corresponding database.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **DeepXplore**.

Step 2 click , and then select **Person**.

Figure 5-64 Person search



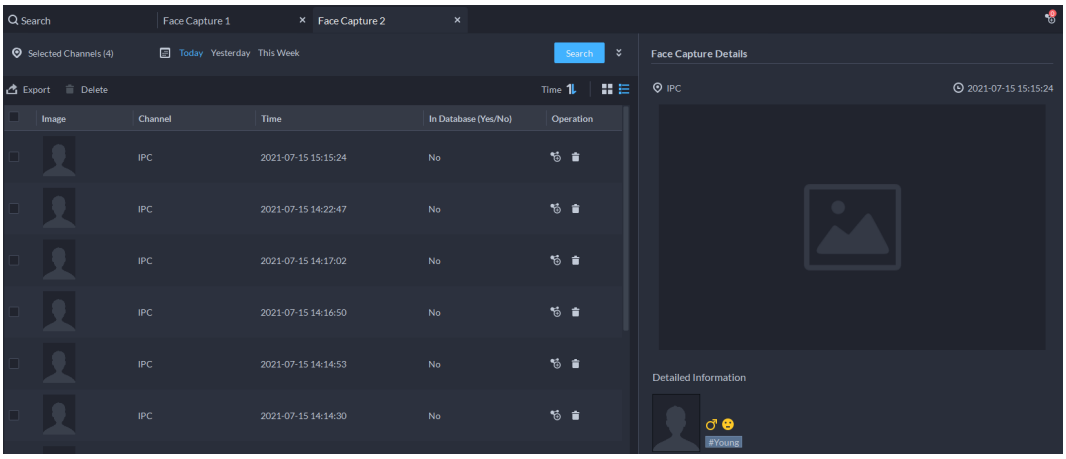
- Search object
  - **Face Capture**: Search for records in face capture database.
  - **Body Capture**: Search for records in body capture database.
  - **Person Archive**: Search for records in person information database.
- Search type
  - **Search by Feature**: Search for records by the defined features such as age, gender, clothes color, ID and more.
  - **Search by Image**: Search for records by the uploaded image, and only records above the set **Similarity** will be displayed.

    Only new versions of IVSS devices support displaying similarity.
  - Search channel: Select device channels of the records by clicking **Selected Channel**.
  - Search time: Select time period of the records from **Today**, **Yesterday** and **This Week**.

    Only available for face and body capture modules.
- Search conditions: Set search conditions such as age, gender, top color, ID, name and more to search for specific records.

Step 3 Set the search object, type and conditions, and then click **Search**.

Figure 5-65 Search result



For the search result, you can perform following operations.

- Click next to **Search** to change search conditions.
- Click Time to change records arrangement.
- Click next to the record to add it to case bank temporarily.
- Click next to the record to delete it one by one, or you can select records, and then click **Delete** to delete them in batches.
- Click **Export** to export records to the local storage.

Step 4 Select a record, and on the right side, you can see the details. Click the video image to view the linked recording.

click at the upper-right corner to view all records added to the case bank. Inside it, you can click to view the target track, and click to remove the record form the bank.

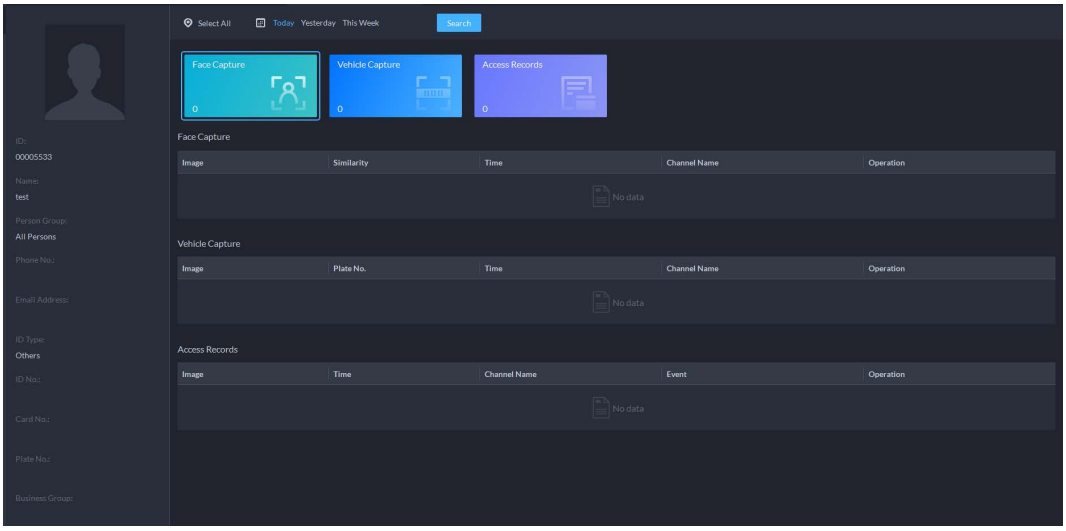
Step 5 Go back to Step2, and then click **Person Archive**.

Step 6 Enter the ID, name or card number of the person you want to search for.

Step 7 Double-click the record.

You can see the face capture, vehicle capture, access records and other information of the corresponding person.

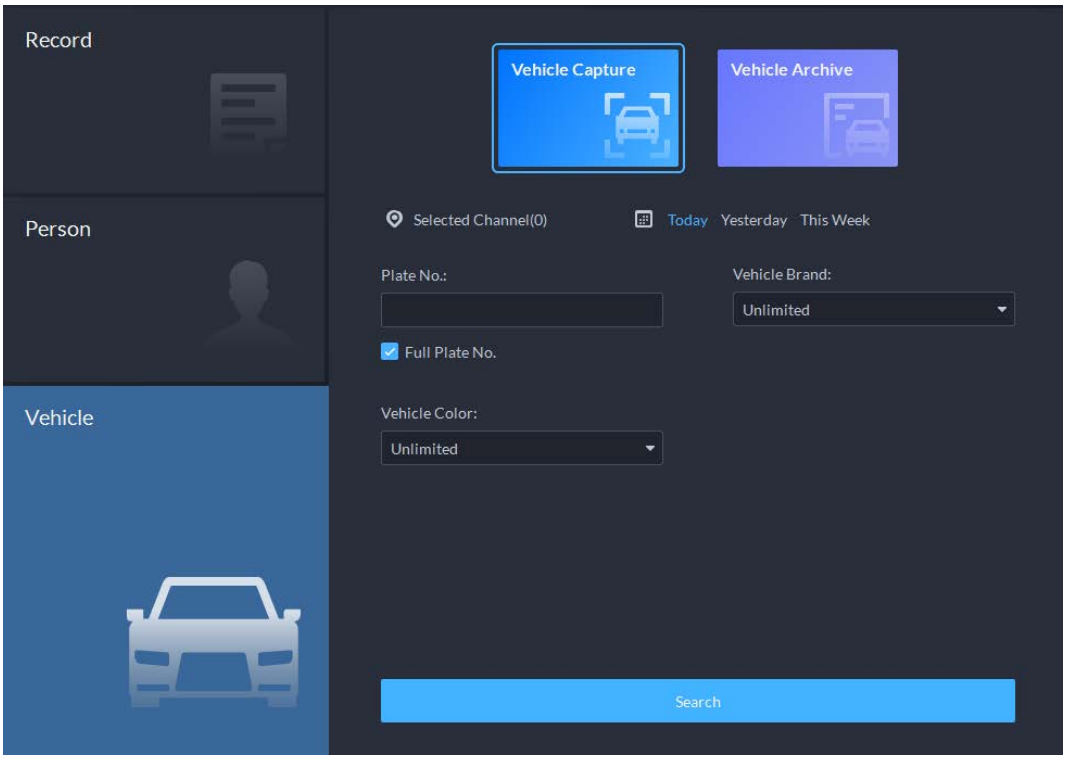
Figure 5-66 Person information



5.3.2 Searching for Vehicles

Step 1 click , and then select **Vehicle**.

Figure 5-67 Vehicle search



- Search object
  - **Vehicle Capture**: Search for records in vehicle capture database.
  - **Vehicle Archive**: Search for records in vehicle information database.
- Search type
  - Search channel: Select device channels of the records by clicking **Selected Channel**.
  - Search time: Select time period of the records from **Today**, **Yesterday** and **This Week**.

  Only available for vehicle capture module.
- Search conditions: Set search conditions such as plate number (full plate number optional), vehicle brands, owner name and more to search for specific records.

Step 2 Set the search object, type, channel and time, and then click **Search**.

For the search result, you can perform following operations.

- Click next to **Search** to change search conditions.
- Click Time to change records arrangement.
- Click next to the record to add it to case bank temporarily.
- Click next to the record to delete it one by one, or you can select records, and then click **Delete** to delete them in batches.
- Click **Export** to export records to the local storage.

Step 3 Select a record, and on the right side, you can see the details. Click on the video image to view the linked recording.

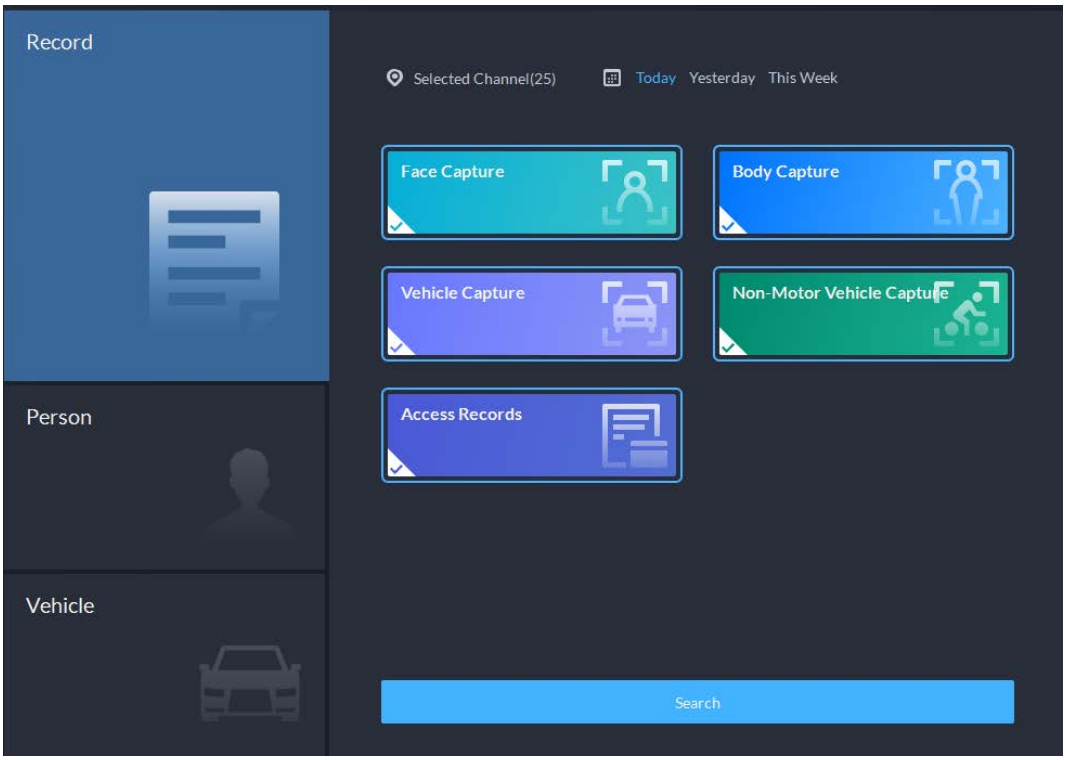
click at the upper-right corner to view all records added to the case bank. Inside it, you can click to generate target track, and click to remove the record form the bank.

5.3.3 Searching for Records

In this section, you can view integrated records of people, vehicle, access.

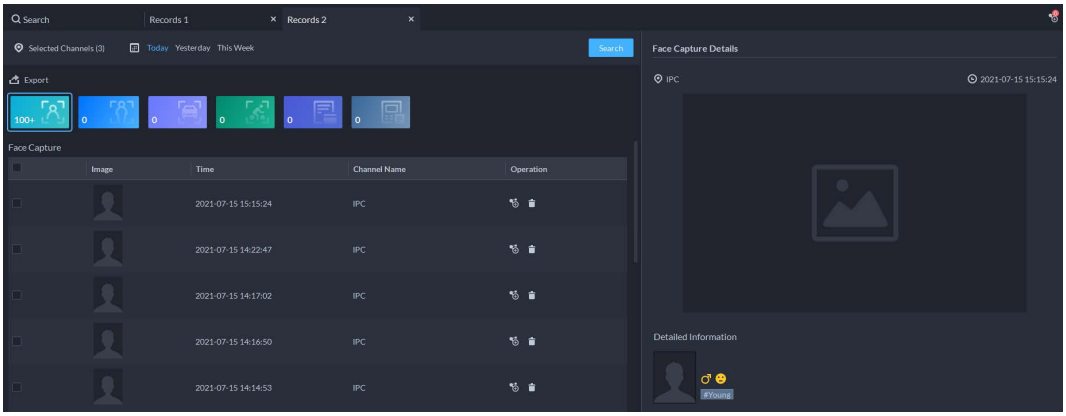
Step 1 click , and then select **Record**.

Figure 5-68 Record search



Step 2 Set the search object, channel and time, and then click **Search**.

Figure 5-69 Search result



For the search result, you can perform following operations.

- Click next to the record to add it to case bank temporarily.
- Click next to the record to delete it one by one.

  Access records cannot be deleted.

- Click **Export** to export records to the local storage.

Step 3 Select a record, and on the right side, you can see the details. Click on the video image to view the linked recording.

click at the upper-right corner to view all records added to the case bank. Inside it, you can click to generate target track, and click to remove the record form the bank.

5.4 Access Management

On the **Access Management** interface, you can do operations on access control, video intercom, attendance, and visitor.

5.4.1 Access Control Application

You can unlock and lock doors, view details of bound videos and event, and the access control logs. Make sure that you have finished the access control configuration before application. For details, see "4.5 Access Control". You can also click Access Control Configur... to go to the access control configuration interface.

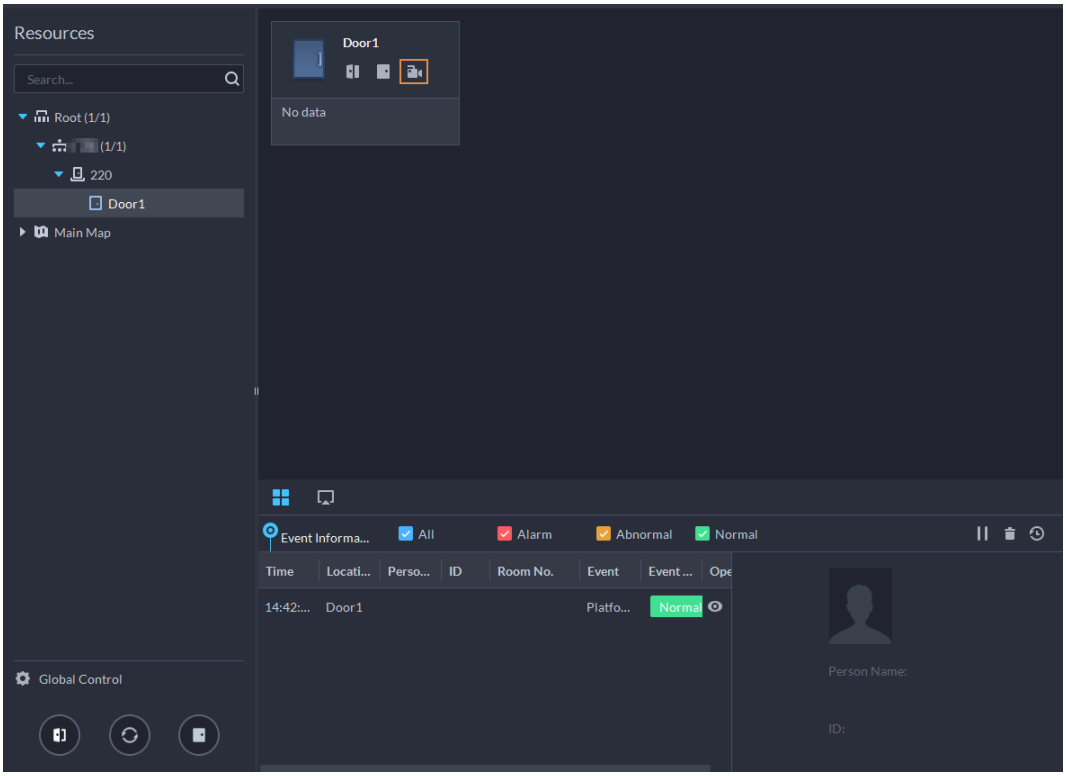
5.4.1.1 Viewing Videos

If you have already bound a video channel to the access control channel, you can view the real-time videos of the channels on the console. To bind video channels, see "3.2.3 Binding Resources".

Log in to the DSS Client. On the **Home** interface, click > **Access Management** > > **Access Control Console**, and then bind videos through the following two methods.

- On the right side of the console interface, click in the access control channel list.

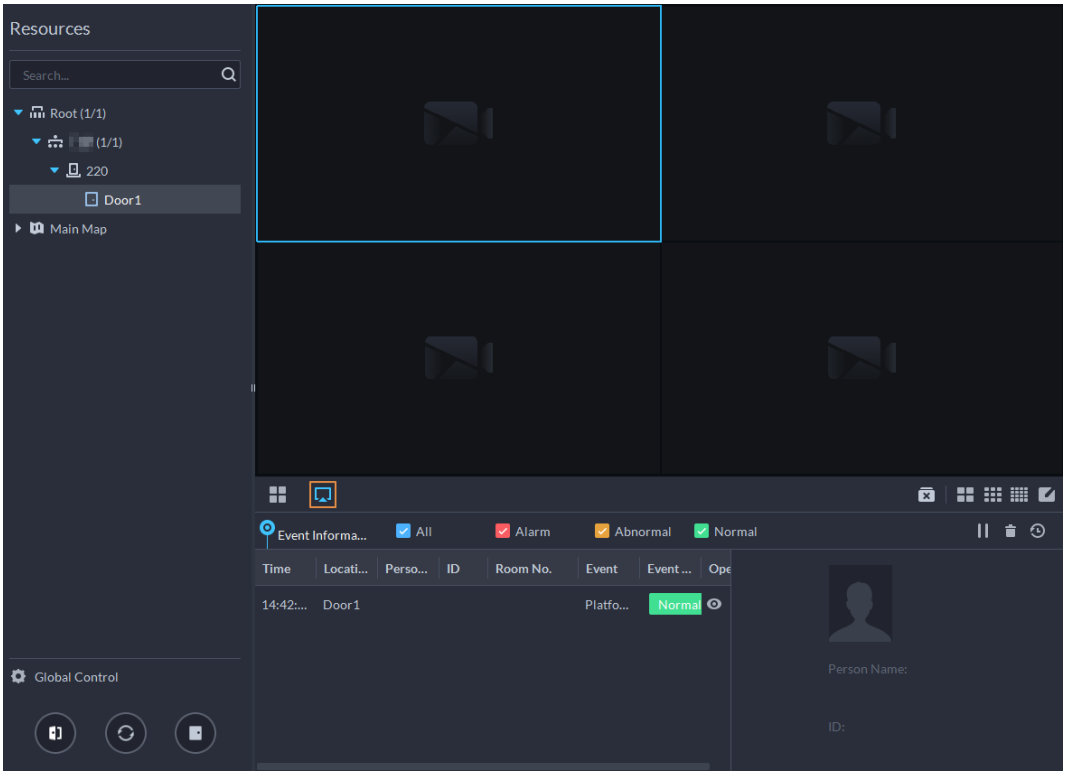
Figure 5-70 Viewing video (1)



- Click on the console interface. The video interface is displayed. Drag the access control channel on the left side of the screen to the live view interface on the right side. The system

displays videos in real time.

Figure 5-71 Viewing video (2)



5.4.1.2 Unlocking Door

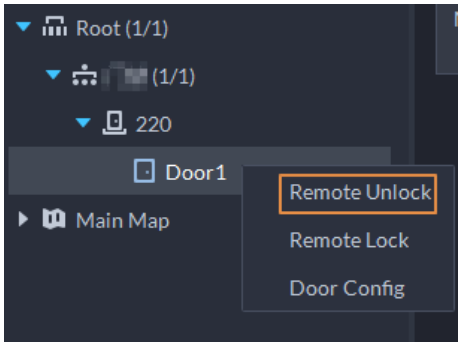
In addition to Always Open or linked unlock in specified periods, the console also supports unlocking by manually controlling the access control channel. After unlock, the door automatically locks up after a specified period (5 s by default, and 10 s in this example) set up in **Door Config**.

This section introduces the unlocking operations on DSS client. For unlocking by fingerprint, card, and face recognition, you can operate on devices. If advance functions are configured, unlock doors according to the requirements of advance functions.

There are the following ways to unlock door:

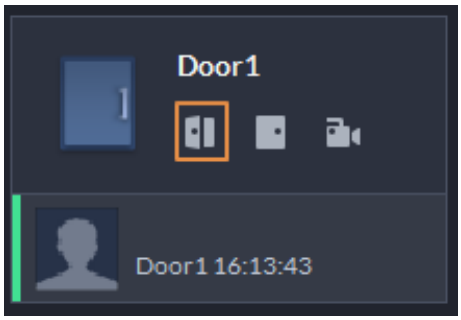
- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Unlock** in the pop-up menu. After unlocking, the door status in the access control channel list on the right side of the interface changes to open, as .

Figure 5-72 Unlock door (1)



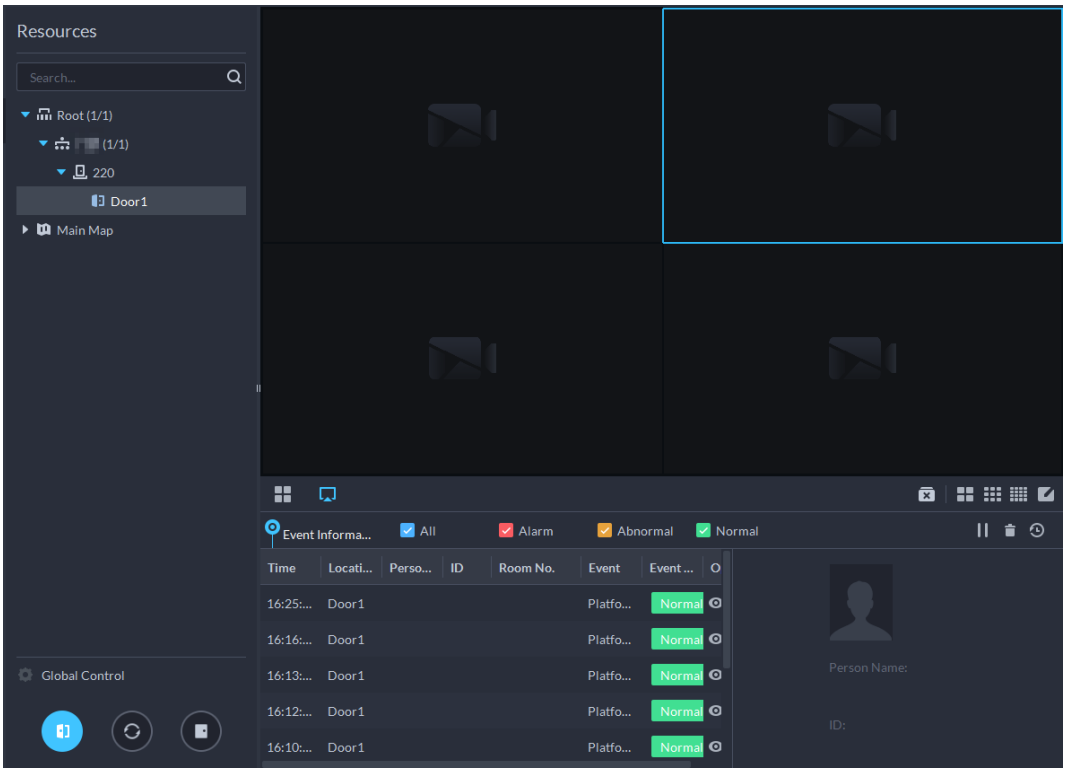
- Click on the door channel interface to unlock the door.

Figure 5-73 Unlock door (2)



- When viewing videos bound to the channel, click on the video interface to unlock the door.

Figure 5-74 Unlock door (3)



- Temporary Always Open of multiple doors

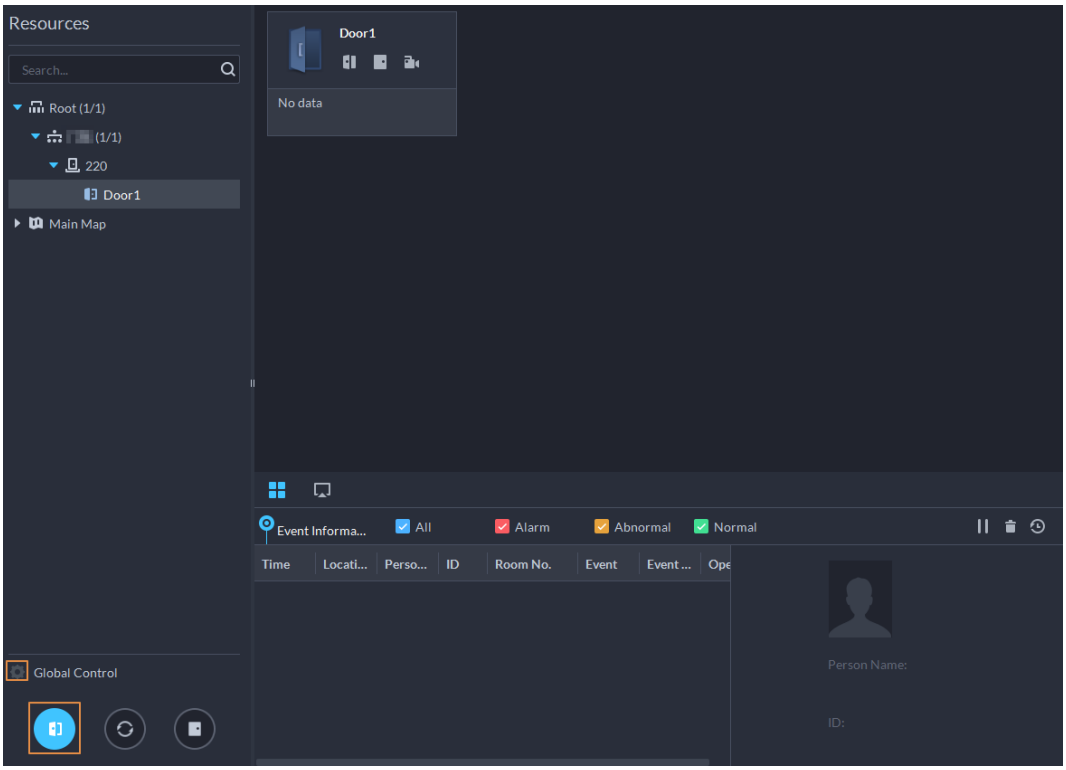
  Select door channels through global control, and then you can set the door to be Always Open.

Step 1 Click on the lower left of the console interface of the **Access Control Console** module.

Step 2 Select an access control channel to be set to Always Open through global control, and click **OK**.

Step 3 Click on the lower-left corner of the interface.

Figure 5-75 Global control



Step 4 Click **OK**.

All the doors of the selected access control channels are set to Always Open.

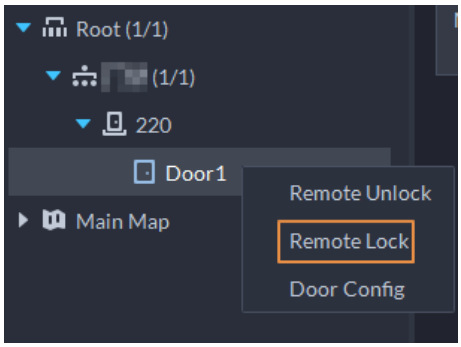
Click to restore the door from the Always Open or Always Closed status before the scheduled door control or face-recognition access control takes effect.

5.4.1.3 Locking Door

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:

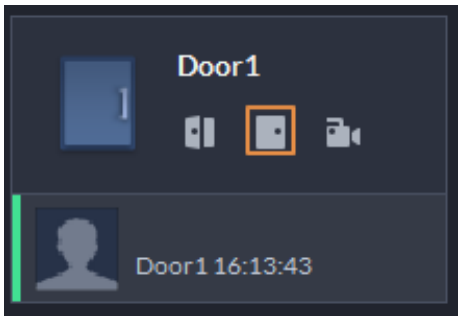
- On the left side of the interface, right-click an access control channel in the device list, and select **Remote Lock** in the pop-up menu. After locking, the door status in the access control channel list on the right side of the interface changes to closed, as .

Figure 5-76 Lock door (1)



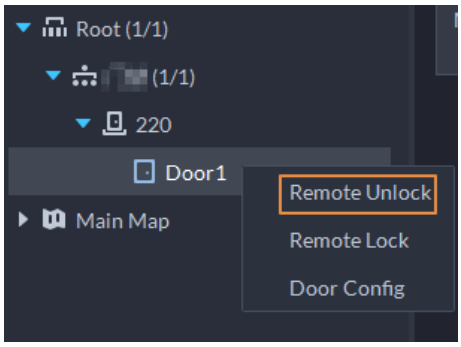
- Click on the door channel interface to unlock the door.

Figure 5-77 Lock door (2)



- When viewing videos bound to the channel, click on the video interface to lock the door.

Figure 5-78 Lock door (3)



- Temporary Always Close of multiple doors

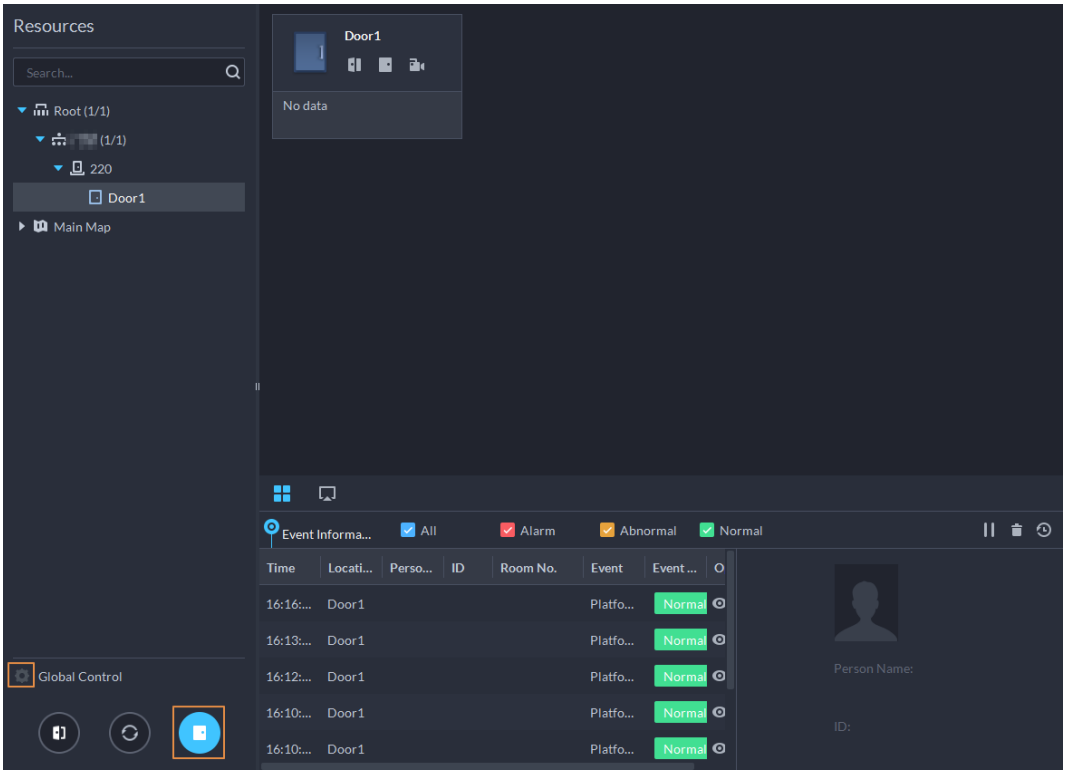
  Select a door channel through global control and you can set the door to be Always Close.

Step 1 Click on the lower left of the console interface of the **Access Control Console** module.

Step 2 Select an access control channel to be set to Always Close via global control, and click **OK**.

Step 3 Click at lower left of the interface.

Figure 5-79 Global control



Step 4 Enter current user's password, and click **OK**.

All the doors of the selected access control channels are set to Always Close.

Click to restore the door from the Always Open or Always Closed status before the scheduled door control or face-recognition access control takes effect.

5.4.1.4 Viewing Event Details

View details of the events reported on door locking and unlocking, including event information, 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 "3.2.3 Binding Resources".
- To see snapshots and videos of access control, you need to configure video linkage action for the access control channels. For details, see "4.1 Configuring Events".
- Details except locking door are displayed on the console, such as unlocking door, entry with the duress card, and no right.

Step 1 In the event list below the console interface, click next to the event records.

For a face recognition controller, the face snapshots will be displayed in the records; for other controllers, the records display people profiles.

Figure 5-80 Event information

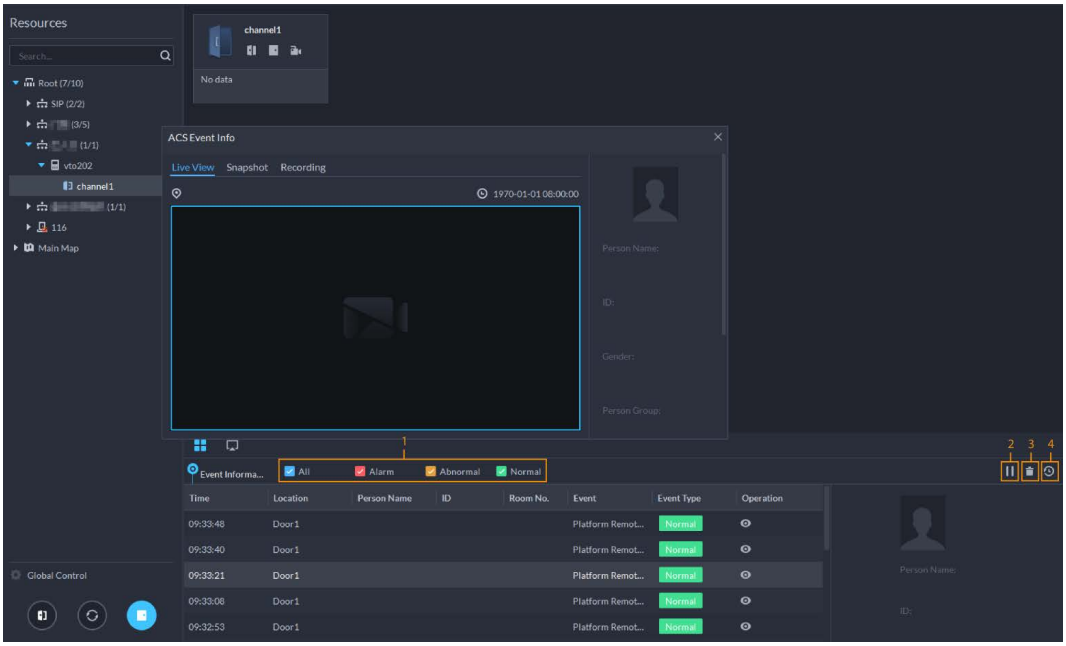


Table 5-10 More operations

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	Clear the events from the current event list without removing them from the log.
4	Click to view access control records.

Step 2 Click the corresponding tab to view the live view, snapshots, and video recordings of the linked video channel.

5.4.1.5 Viewing Access Control Records

You can view access control records on the platform or directly on a device. For records on a device, see "8.1 Managing Logs".

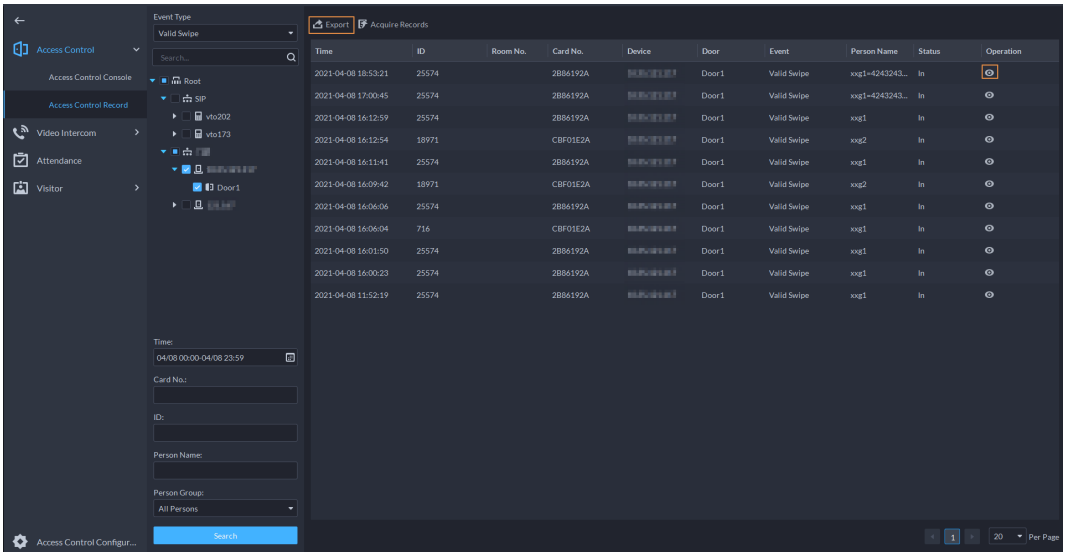
5.4.1.5.1 Online Records

The access control records stored on the platform.

Step 1 Log in to the DSS Client. On the **Home** interface, click ⊞ > **Access Management** > 🚪 > **Access Control Record**.

Step 2 Set search conditions, and then click **Search**.

Figure 5-81 Search result



Step 3 Manage event records.

- Click 👁, and you can view live view, snapshot and recording, and person information access control events.
- Click **Export** at the upper-left corner of the interface, and then export records as the screen instructs.

5.4.1.5.2 Offline Records

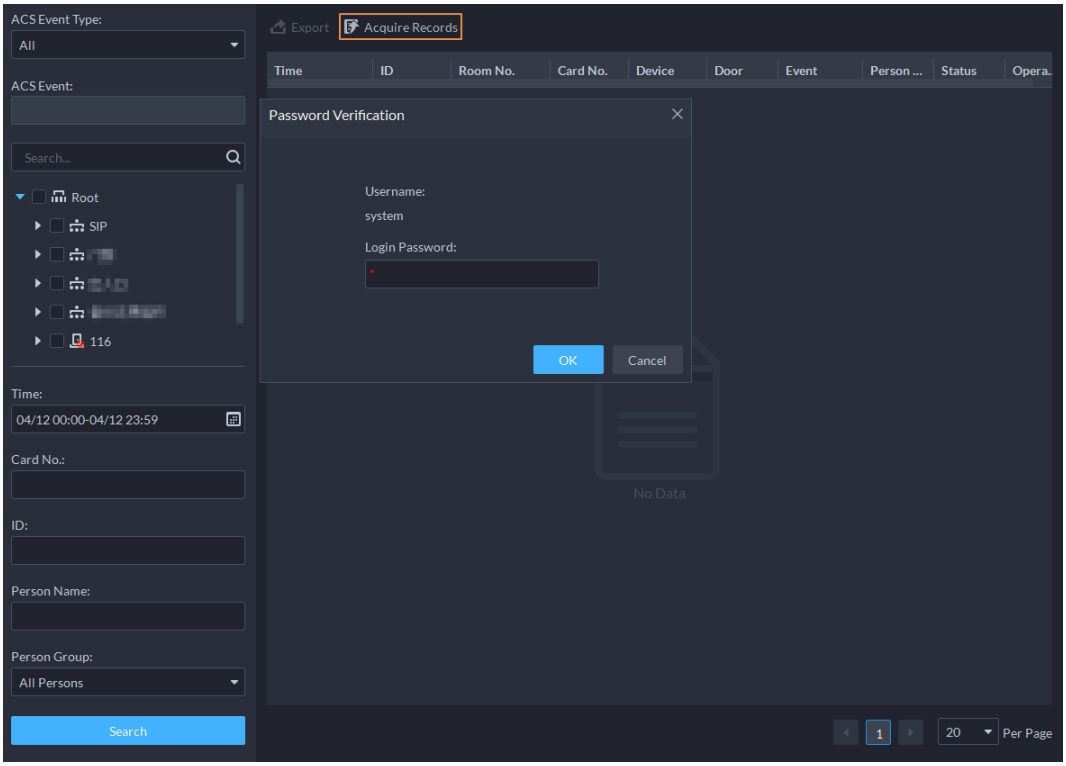
The access control records stored in the device when it was disconnected from the platform. After

the device gets reconnected to the platform, you can retrieve the records generated during the disconnection.

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Access Management** > > **Access Control Record**.

Step 2 Click Acquire Records at the upper-left corner.

Figure 5-82 Extract records during disconnection



Step 3 Enter the login password for verification.

Step 4 Click to set period, select **Card-swiping Records** or **Alarm Log**, and then select device.

You can select up to one week.

Step 5 Click **OK**.

5.4.2 Video Intercom Application

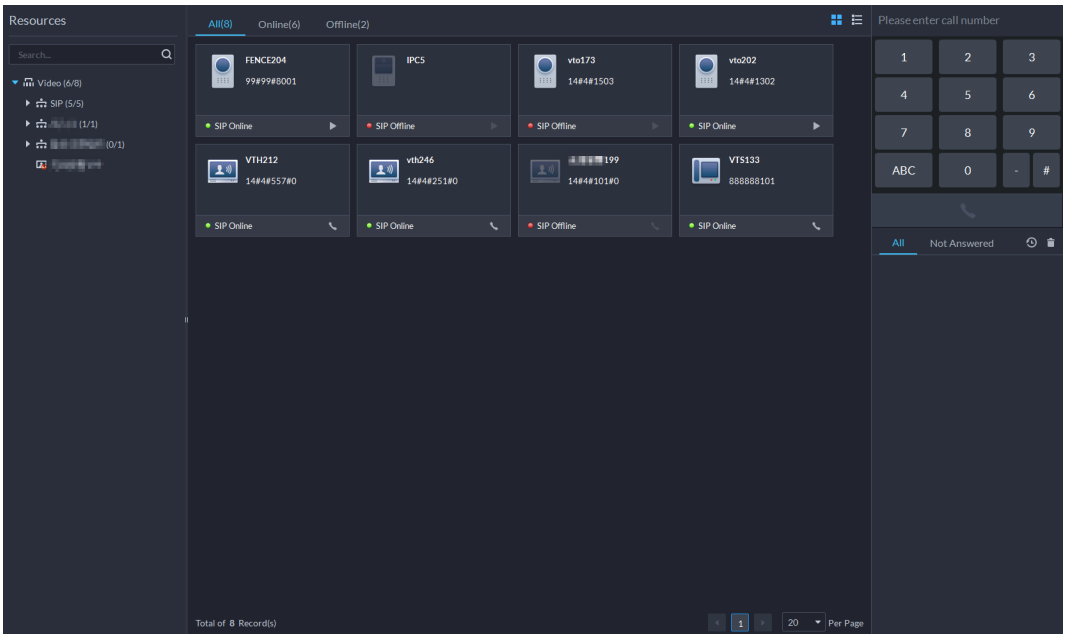
- You can call, answer, release information and view video intercom records.
- Make sure that you have configured the video intercom configuration before application. For details, see "4.6 Video Intercom". You can also click Video Intercom Configur... to go to the video intercom configuration interface.

5.4.2.1 Call Center

The platform, VTOs, VTHs, second-generation door station access controllers, and second-generation fence station access controllers can call each other.

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Access Management** > > **Call Center**.

Figure 5-83 Call center



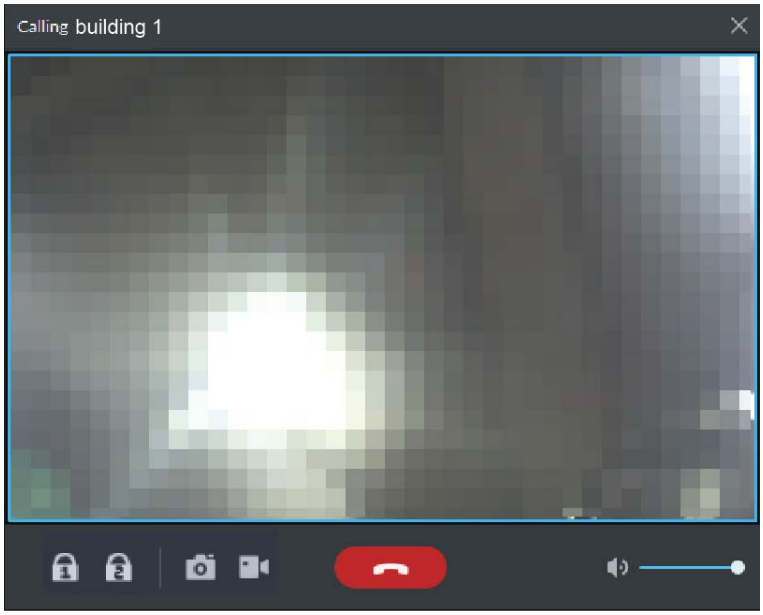
Step 2 You can call VTO and VTH.

- Call from the platform to VTO

  Select VTO in the device list; click ▶ corresponding of VTO and call VTO. The system pops out call interface. The following operations are supported during call.

  - 🔒: If VTO is connected to lock, click this icon to unlock.
  - 📷: Click this icon to capture picture, the snapshot is saved into the default directory. To change the path, see "8.3.5 Configure File Storage Settings".
  - 🎥: Click this icon to start record, click again to stop record. The video is saved in default path. To change the path, see "8.3.5 Configure File Storage Settings".
  - 📞: Click this icon to hang up.

Figure 5-84 Call

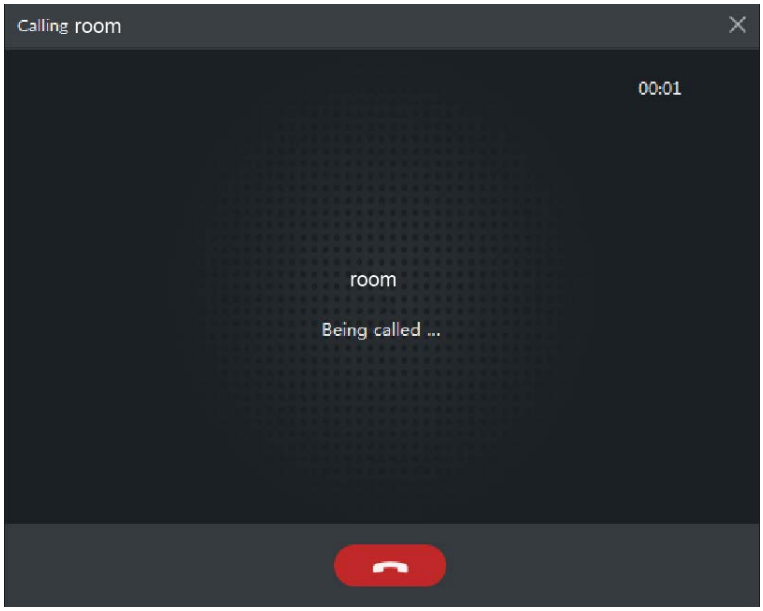


- Call from the platform to VTH

  Select VTH from the device list, click 📞 on the VTH or dial corresponding VTH on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait...**. There are two modes for answering the call.

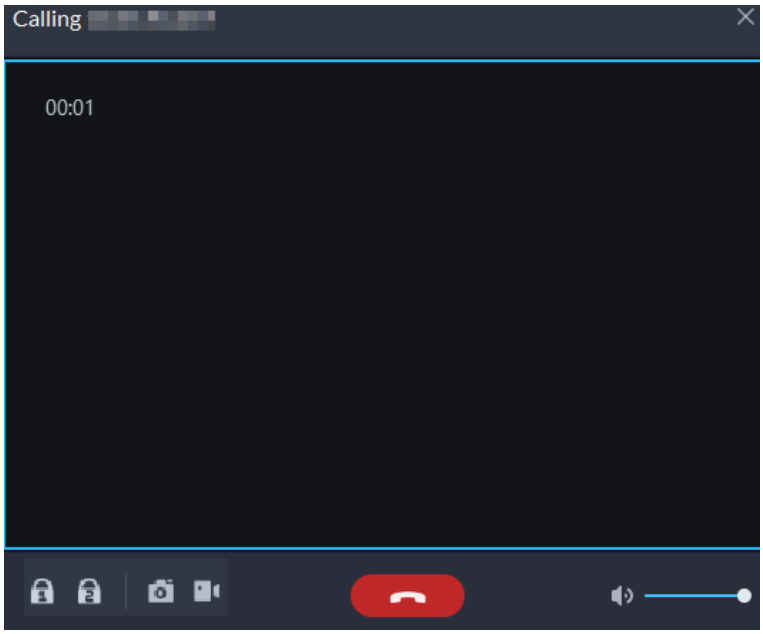
- Answer by VTH, bidirectional talk between client and VTH. Press to hang up when you answer the call.
- If VTH fails to answer over 30 s, hangs up directly or is busy, then it means the call is busy.

Figure 5-85 Calling



- Call from the platform to an access control device
  Select an access control device from the device list, click on the it or dial its number on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait…**. There are two modes for answering the call.
  - Answer by the access control device, bidirectional talk between client and the device. Press to hang up when you answer the call.
  - If the device fails to answer over 30 s, busy or hang up directly, then it means the call is busy.

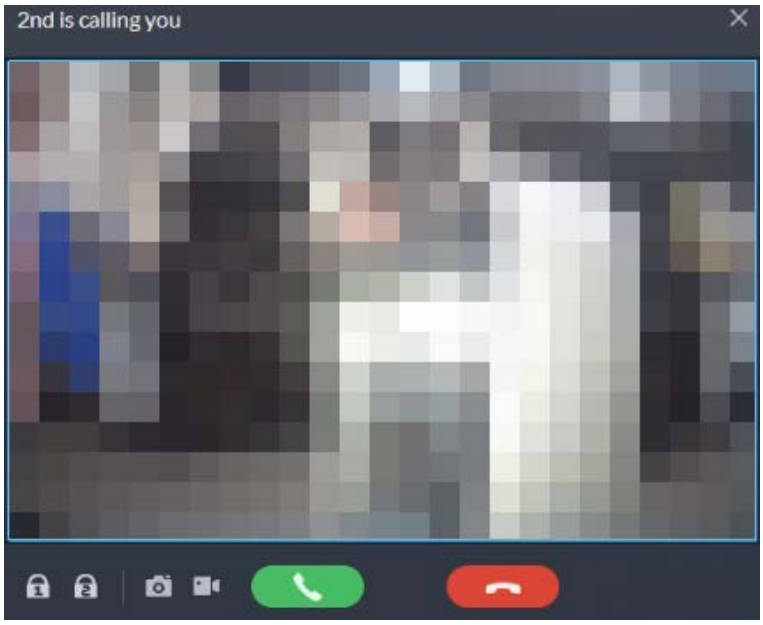
Figure 5-86 Calling



- Call from VTO to the platform
  VTO calls Pro, client pops up the dialog box of VTO calling.

- ◇ : If VTO is connected to lock, click this icon to unlock the door.
- ◇ : Click this icon to answer VTO, realize mutual call after connected.
- ◇ : Click this icon to hang up.

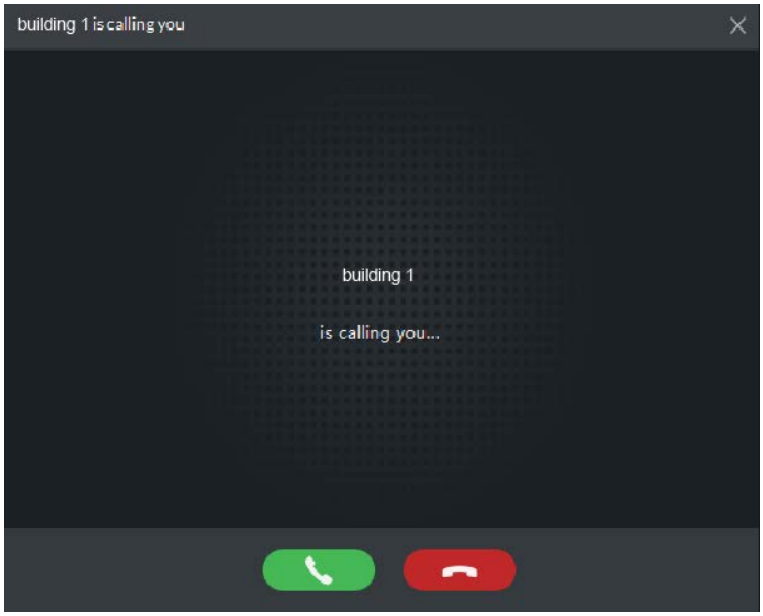
Figure 5-87 VTO Call



- When VTH is calling the platform

  The client pops out the dialog box of VTH calling. Click to talk with VTH.
  - ◇ Click to answer VTO, realize mutual call after connected.
  - ◇ Click to hang up.

Figure 5-88 VTH call

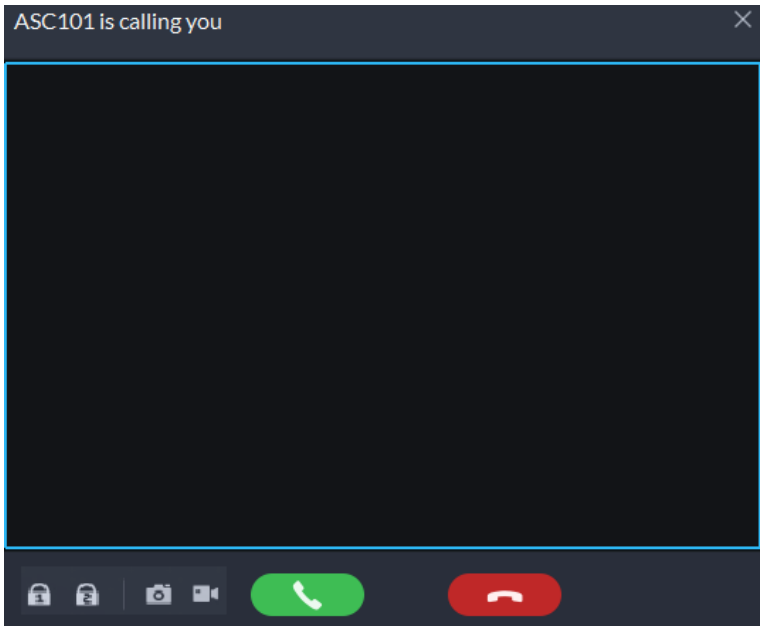


- When an access control device is calling the platform

  The client pops out the dialog box. Click to talk with the device.

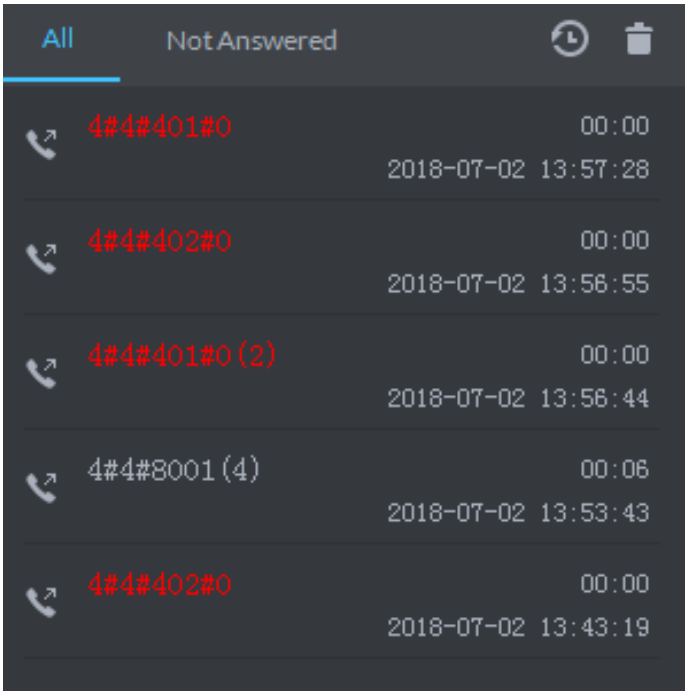
  Click to hang up.

Figure 5-89 An access control device call



- Call through call records
  All the call records are displayed in the **Call Record** at the lower-right corner of the interface of **Video Intercom**. Click the record to call back.

Figure 5-90 Call records

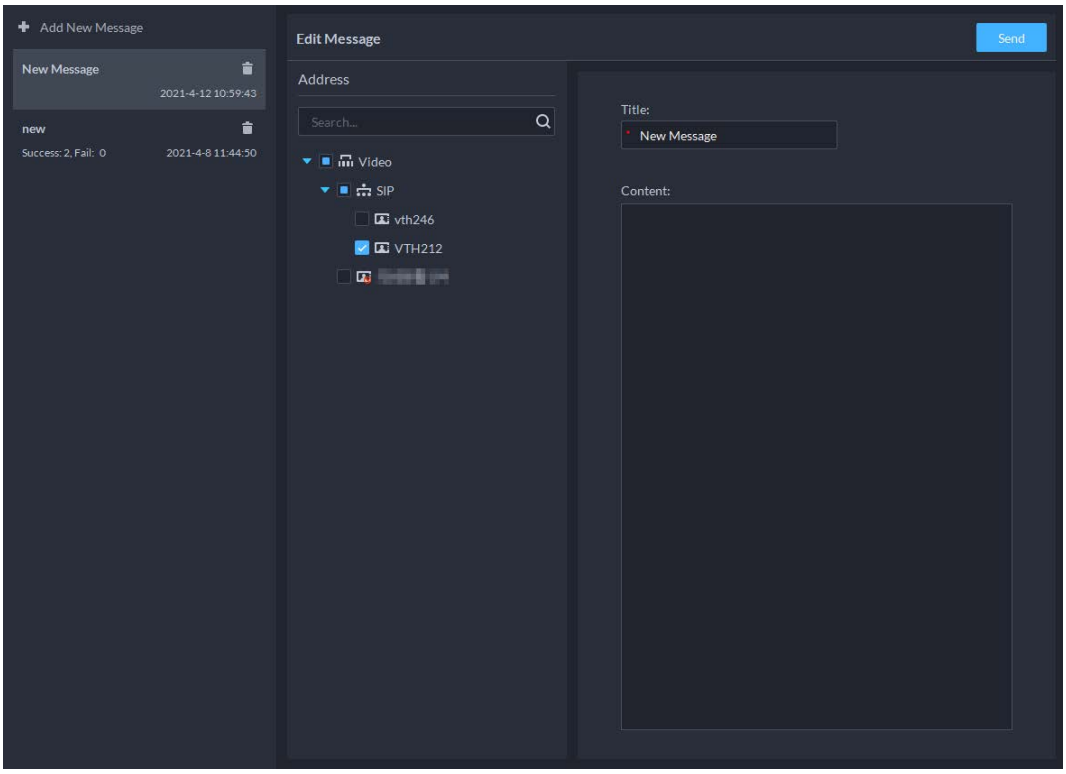


5.4.2.2 Information Release

Send message to designated VTH.

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Access Management** > > **Release Information**.

Figure 5-91 Information release



Step 2 Click **Add New Message**, select VTH, and then add release information.

Step 3 Click **Send**.

The VTH will receive the message after it is sent successfully.

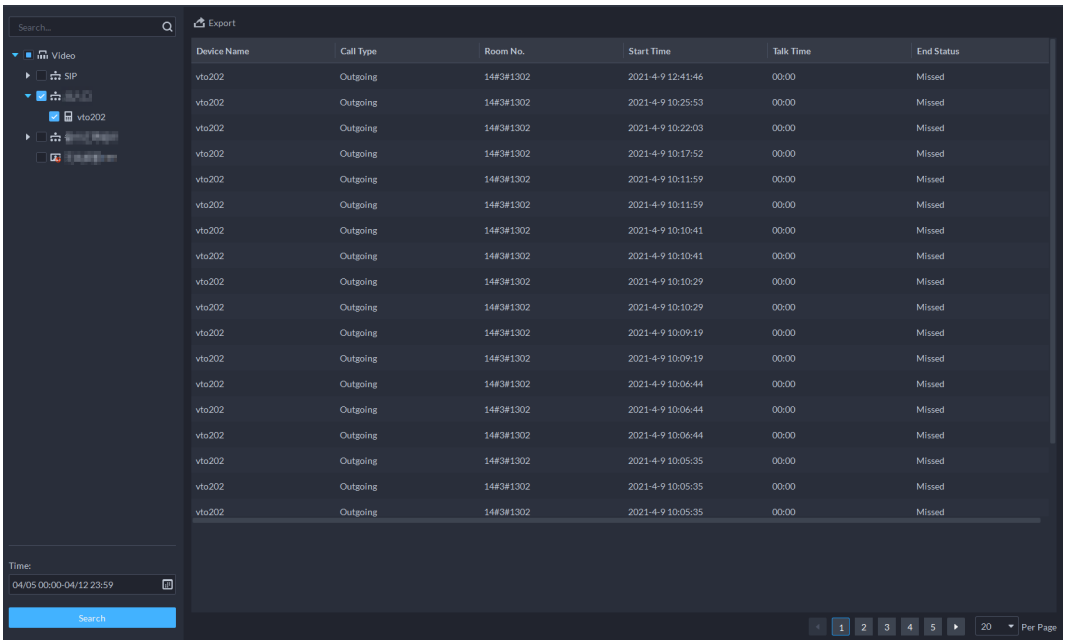
5.4.2.3 Video Intercom Records

View log records and you can trace recorded calls.

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Access Management** > > **Video Intercom Record**.

Step 2 Set conditions, and then click **Search**.

Figure 5-92 Video intercom records



Step 3 Click **Export** and the records will be saved locally according to system prompt.

5.4.3 Visitor Application

After appointment is made on platform, and visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves.

5.4.3.1 Preparations

- You have configured the deployment of the video intercom devices, access control devices and entrance and exit device. For details, see the corresponding user's manual.
- You have configured the basic configuration of the platform. For details, see "3 Basic Configurations".
- Make sure that you have configured the visitor configuration before application. For details, see "4.7 Visitor Management". You can also click Visitor Configuration to go to the video intercom configuration interface.

5.4.3.2 Visitor Appointment

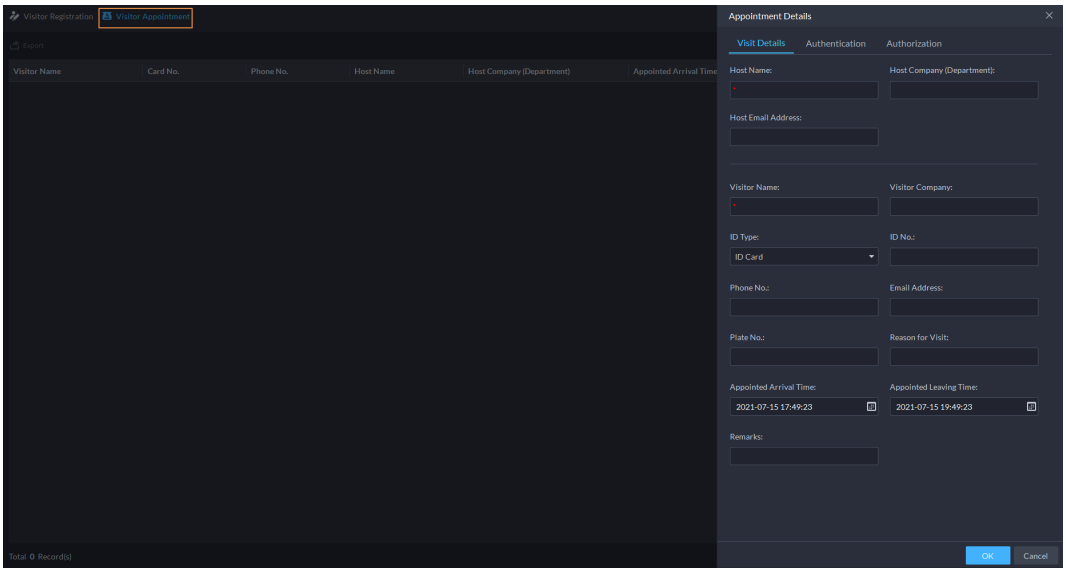
Register visitor information on the platform.

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Access Management** > > **Visitor Management**.

Step 2 Click **Visitor Registration**.

Step 3 Click the **Visitor Details** tab, enter the information of the visitor and the one to be visited.

Figure 5-93 Visitor details

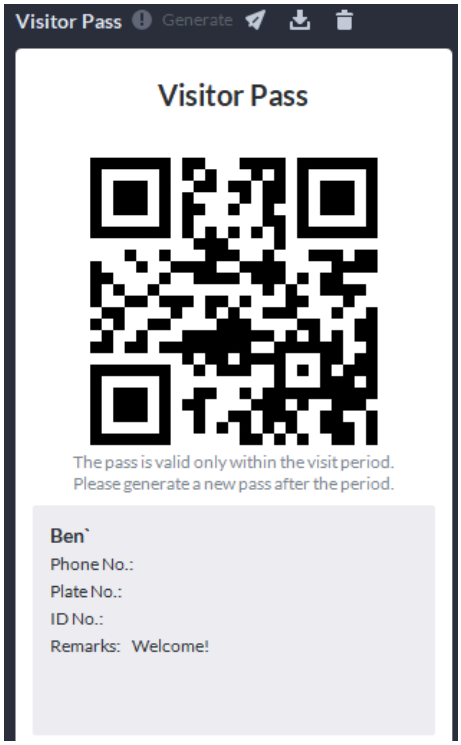


Click in the appointment list to enter the **Visitor Details** tab.

Step 4 (Optional) Click the **Authentication** tab, select the room number to be visited, and then click **Generate** to generate the QR code of the pass.

You can click to download the QR code, and click to send it to the visitor by email.

Figure 5-94 Authentication



Step 5 Click **OK**.

5.4.3.3 Checking In

When a visitor with an appointment arrives, you need to confirm their information and give them access permission. On-site registration is supported when there is a walk-in visitor. Visitors can get

access by card swipe or face recognition.

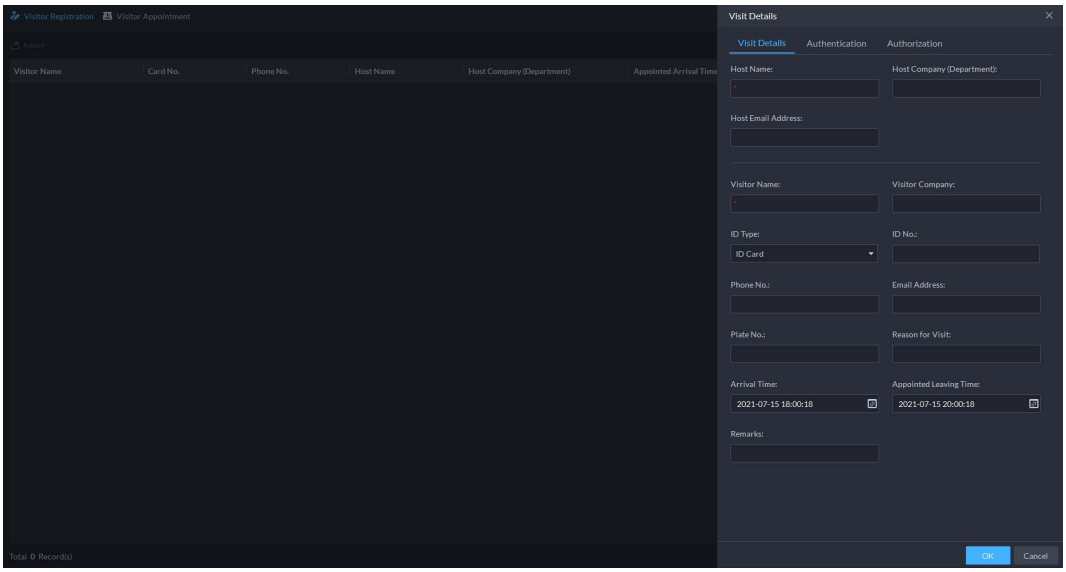
Step 1 Log in to the DSS Client. On the **Home** interface, click > **Access Management** > > **Visitor Management**.

Step 2 Record visitor details.

1) Go to the visit registration information interface.
   - If a visitor has an appointment, find their visitor information, and then click .
   - If a visitor does not have an appointment, click **Visit Registration**.
2) Confirm or enter visitor information.

Step 3 On the **Access Management** interface, select **Visitor** > **Visitor Management**.

Figure 5-95 Visitor information



Step 4 (Optional) Click the **Authentication** tab, and then set authorization information.

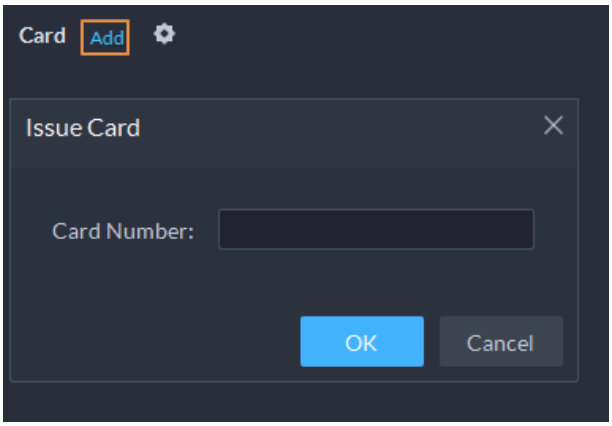
1) Select the room number.
2) Issue cards.

   You can issue cards by entering card number manually or by using a card reader. A card number is 8-16 numbers. Only second-generation access control devices support 16-digit card numbers. When a card number is less than 8 numbers, the system will automatically add zeros prior to the number to make it 8 digits. For example, if the provided number is 8004, it will become 00008004. If there are 9-16 numbers, the system will not add zero to it.

   - Issue cards by entering card numbers manually

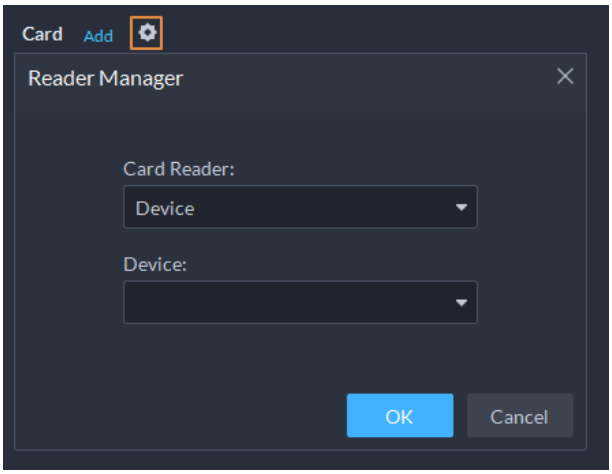
     Click **Add** next to **Card**, enter the card number, and then click **OK**.

Figure 5-96 Issue card



- Issue card by using a card reader
  Click , select a card reader or device, and then click **OK**. Swipe card through the reader or device, and then a new card will be issued.

Figure 5-97 Reader manager

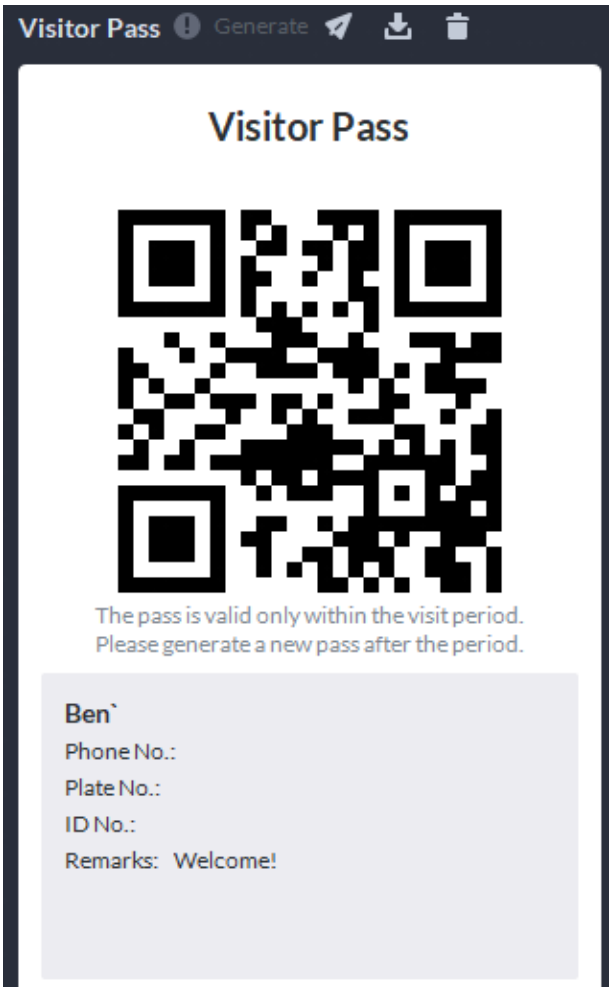


3) Set face picture. Position your face in the snapshot area, and click **Upload Picture** to select a picture or click **Snapshot** to take a photo.

Figure 5-98 Take a face photo

4) Click **Generate** to generate a QR code for the pass.
   You can click to download the QR code, and click to send it to the visitor by email.

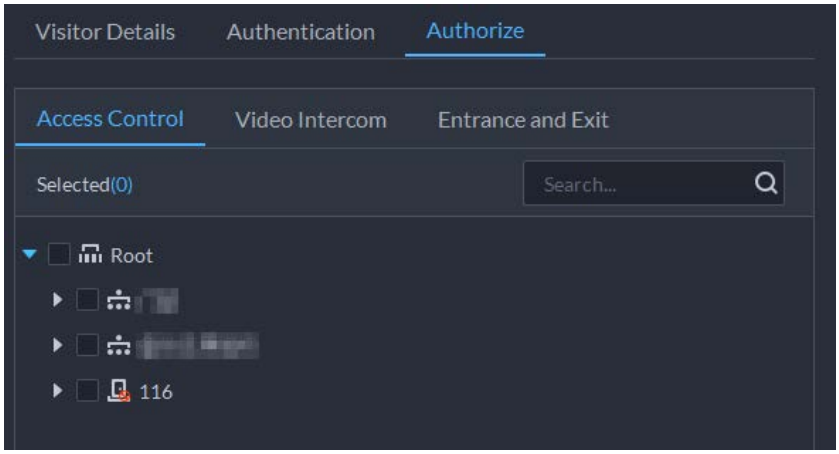
Figure 5-99 Authentication



Step 5 Click the **Authorize** tab, and then select access permissions for the visitor.

If you want to set video intercom devices and entrance and exit permissions, you must set host room number and number plate for the visitor.

Figure 5-100 Authorize



Step 6 Click **OK**.

Related Operations

- End visit.
  Click to end a visit.

- View card swiping records.
  Click the **Card-swiping Record** tab, or click in visitor record to view visitor card swiping records.
- Cancel appointment.
  Click , and cancel the appointment as the screen instructs.

5.4.3.4 Checking Out

When visitors are leaving, remove their access permissions.

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Access Management** > > **Visitor Management**.

Step 2 Find the appointment record of the visitor, and then click .

Step 3 Click **OK** to remove access permission.

If you have issued a card to a visitor, make sure the visitor returns the card before leaving.

5.4.3.5 Searching for Visit Records

Search for visit records, and view visitor details and card swiping records.

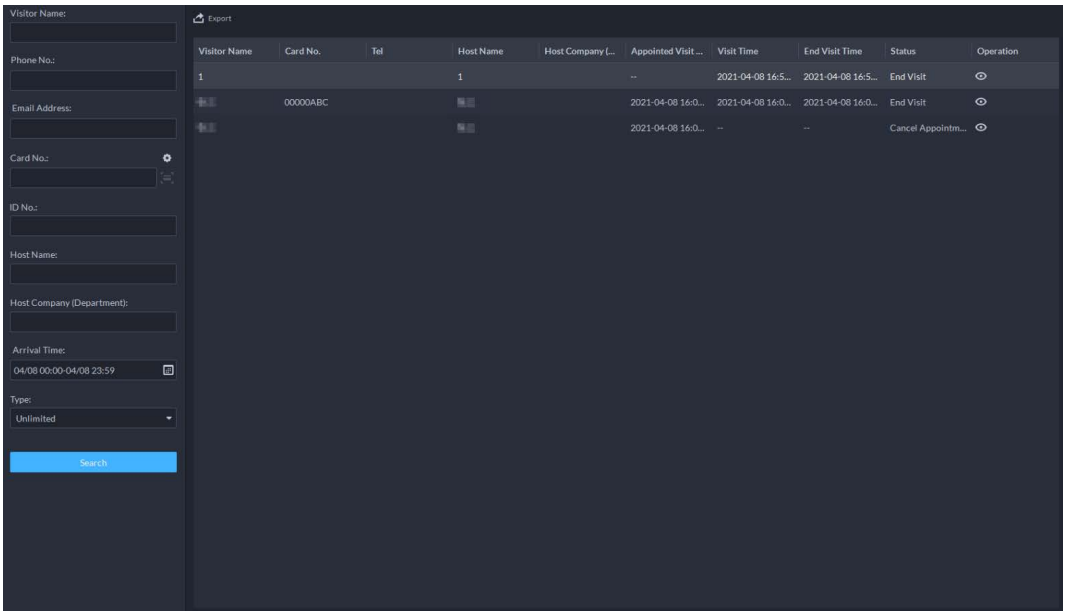
Step 1 Log in to the DSS Client. On the **Home** interface, click > **Access Management** > > **Visitor Record**.

Step 2 Set search conditions, and then click **Search**.

The results are displayed.

In addition to entering the card number, you can also click , select a card reader and then get the card number by swiping card.

Figure 5-101 Search for visit result



Step 3 Click to view visitor details and card swiping records.

5.5 Vehicle Entrance and Exit Application

You can monitor vehicles that enter and exit in real time, view vehicle information, and search on-site vehicle, exit vehicle and snapshot records.

Make sure you have configured the entrance and exit configuration before the application process. For details, see "4.8 Entrance and Exit". You can also click Entrance and Exit Config... to go to the entrance and exit configuration interface.

5.5.1 Entrance and Exit Monitoring

Procedure

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Vehicle Entrance and Exit** > .

Step 2 Select an ANPR channel, double-click it or drag it to the window.

Figure 5-102 ANPR

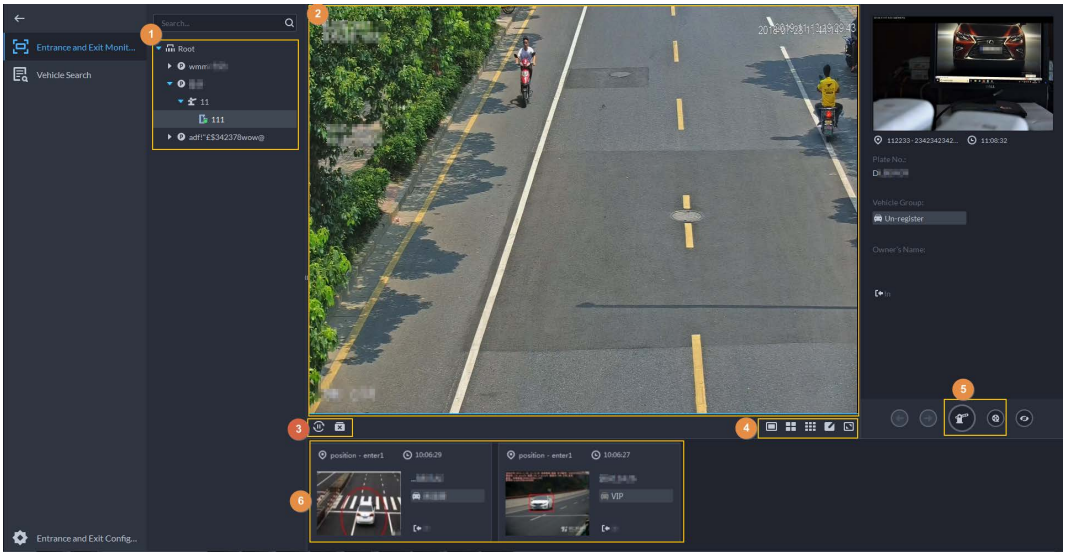


Table 5-11 ANPR interface description

No.	Description
1	Device list. Displays channel information.
2	Live view. Select windows, and double-click the channel as needed, or drag it to the window. The live view interface will be displayed. Point to the image, and is displayed. Click it to open barrier.
3	• /: Update or stop updating ANPR information. • : Close all windows.
4	• : Set the split mode of the window, which includes 1 window, 4 windows, and 9 windows, or click to customize the splits. • : Full screen mode. Press the Esc key to exit full scree mode.
5	Displays the latest ANPR snapshot of the vehicles with drivers who need to open the barrier manually and vehicle details. More operations: • Click to open the barrier for the vehicle. • Click to view the video of the corresponding channel.

No.	Description
6	Displays the 5 latest ANPR snapshots. Double-click a snapshot to view vehicle details, including vehicle information, the snapshot and license plate image. You can play back the video and download it.

Related Operations

Right-click a video, and then you can set audio input, stream type, and more.

5.5.2 Vehicle Entrance and Exit

Search for entry and exit records, forced exit records and snapshot records.

Log in to the DSS Client. On the **Home** interface, click , and then select **Vehicle Entrance and Exit**. Click Entrance and Exit Config... to go to the entrance and exit configuration interface.

5.5.2.1 Searching for Entrance Records

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Vehicle Entrance and Exit** > .

Step 2 Click the **Entrance Records** tab.

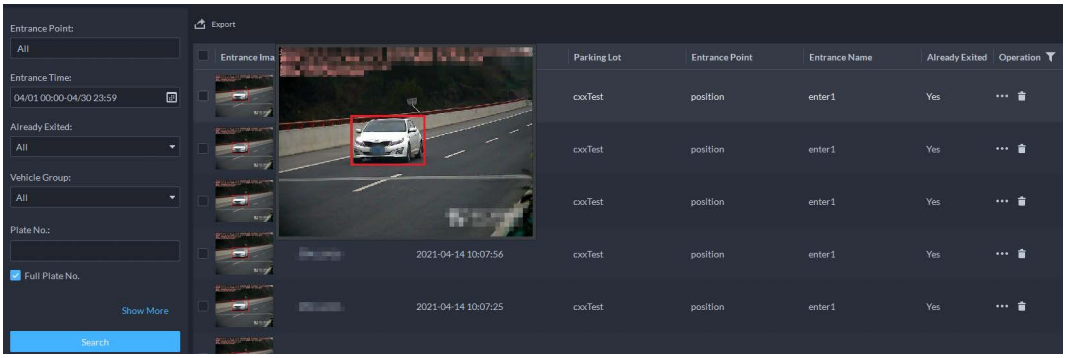
Step 3 Set search conditions, and then click **Search**.

Click **Show More** and you can search by vehicle owner, company, person group, and more.

Step 4 Mange records.

- Click the entry image, and then a bigger image will be displayed.

Figure 5-103 View bigger picture



- Double-click the record or click , and detailed information is displayed on the right, including entry and exit records. Click the play icon to play the video, and then click to download it. Click **Edit** to modify vehicle information such as plate number, vehicle logo and vehicle color.

  For the dual camera mode, snapshots from both cameras are displayed.
- Forced exit.

  If **No** is displayed in **Already Exited** when the vehicle has exited, click to change the status to **Yes**.
- Export records.

  Select records to be exported, click **Export**, and then export records as the screen instructs; or click **Export**, and the then export all records as the screen instructs.

.● Set record display item.
Click , and then select items to be displayed.
- Click **Next** to display the next record. Click **Previous** to go to the previous record.

5.5.2.2 Searching for Exit Records

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Vehicle Entrance and Exit** > .

Step 2 Click the **Exit Records** tab.

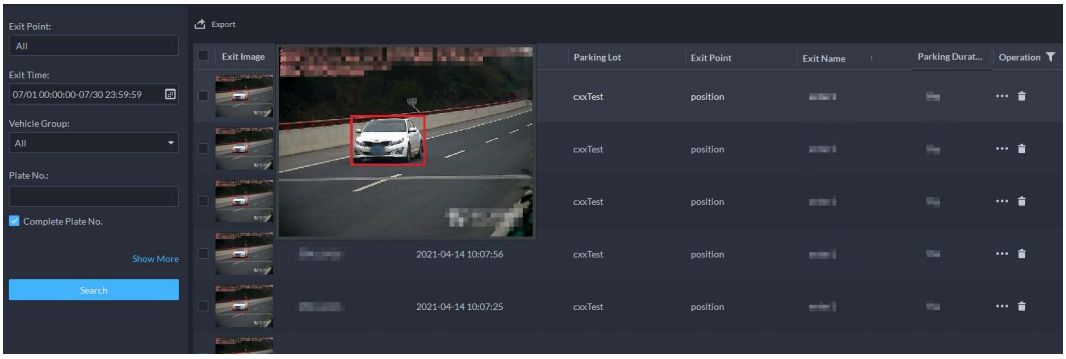
Step 3 Set search conditions, and then click **Search**.

Click **Show More** and you can search by vehicle owner, company, person group, and more.

Step 4 Mange records.

- Click the exit picture, and then a bigger picture will be displayed.

- Figure 5-104 View bigger picture



- Double-click the record or click , and detailed information is displayed on the right, including entry and exit records. Click the play icon to play the video, and then click to download it. Click **Edit** to modify vehicle information such as plate number, vehicle logo and vehicle color.
For the dual camera mode, the snapshots from both the cameras are displayed.
- Export records.
Select the records to be exported, click **Export**, and then export records as the screen instructs; or click **Export**, and the then export all records as the screen instructs.
- Set record display item
Click , and then select items to be displayed.
- Click **Next** to display the next record. Click **Previous** to go to the previous record.

5.5.2.3 Searching for Forced Exit Records

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Vehicle Entrance and Exit** > .

Step 2 Click the **Forced Exit Records** tab.

Step 3 Set search conditions, and then click **Search**.

Click **Show More** and you can search by vehicle owner, company, person group, and more.

Step 4 Mange records.

- Click the exit picture, and then a bigger picture will be displayed.
- Double-click the record or click , and detailed information is displayed on the right, including entry and exit records. Click the play icon to play the video, and then click to download it. Click **Edit** to modify vehicle information such as plate number, vehicle logo and vehicle color.
  For the dual camera mode, snapshots from both cameras are displayed.
- Export records.
  Select records to be exported, click **Export**, and then export records as the screen instructs; or click **Export**, and the then export all records as the screen instructs.
- Set record display item
  Click , and then select items to be displayed.
- Click **Next** to display the next record. Click **Previous** to go to the previous record.

5.5.2.4 Searching for Capture Records

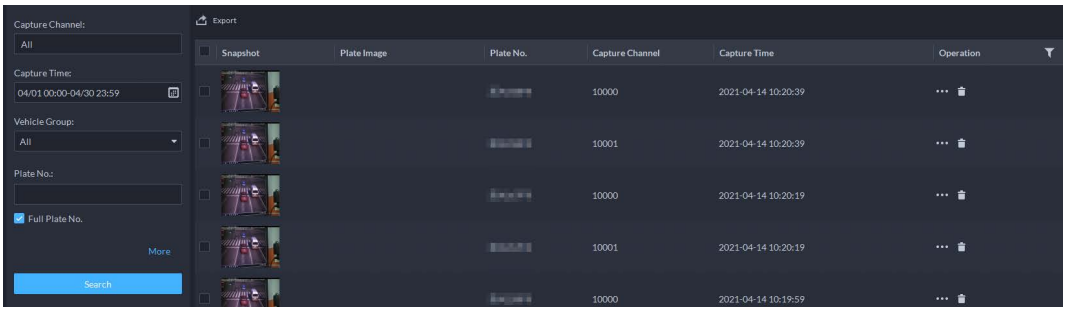
Step 1 Log in to the DSS Client. On the **Home** interface, click > **Vehicle Entrance and Exit** > .

Step 2 Click the **Capture Records** tab.

Step 3 Set search conditions, and then click **Search**.

Click **Show More** and you can search by vehicle owner, company, person group, and more.

Figure 5-105 Capture record



Step 4 Mange records.

- Click the exit picture, and then a bigger picture will be displayed.
- Double-click the record or click , and detailed information is displayed on the right, including entry and exit records. Click the play icon to play the video, and then click to download it. Click **Edit** to modify vehicle information such as plate number, vehicle logo and vehicle color.
  For the dual camera mode, snapshots from both cameras are displayed.
- Restore entry
  If **Yes** is displayed in **Exited** when the vehicle is still in the area, click to change the state to **No**.
- Export records.
  Select records to be exported, click **Export**, and then export records as the screen instructs; or click **Export**, and the then export all records as the screen instructs.
- Set record display item
  Click , and then select items to be displayed.

- Click **Next** to display the next record. Click **Previous** to go to the previous record.

5.6 Intelligent Analysis

View real-time and history people counting data, heat maps, and number of people in an area.

5.6.1 People Counting

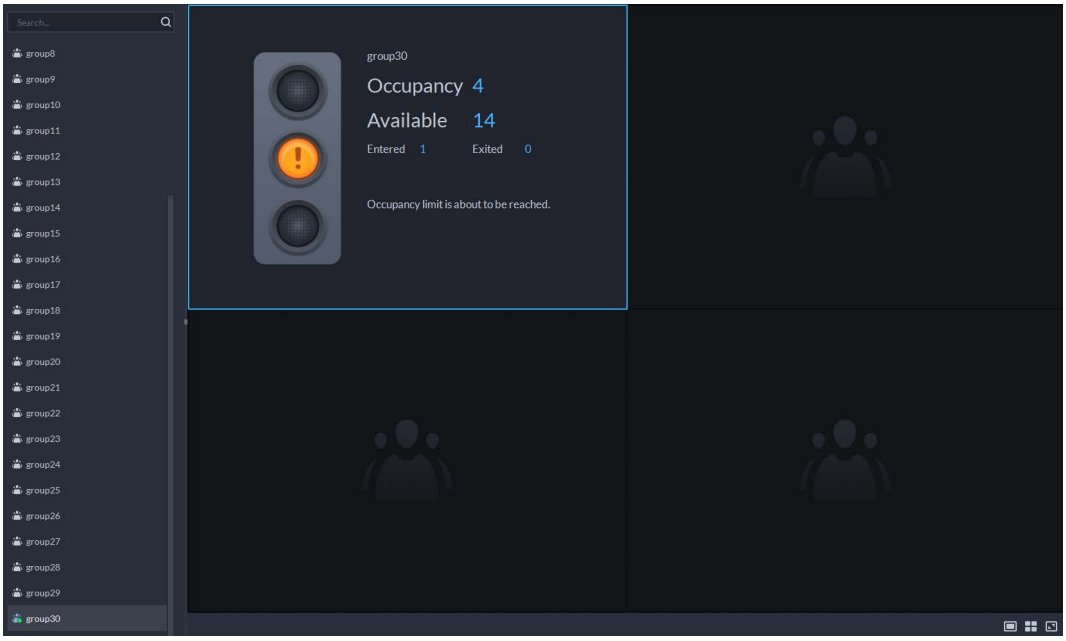
5.6.1.1 Real-time Count

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Intelligent Analysis** > > **Real-time Count**.

Step 2 Double-click a group or drag it to a window on the right to display its real-time data.

- **Occupancy**: The number of people currently inside this group, which will be reset to the defined value at the defined calibration time.
- **Entered**: The number of people entered this group, which will be reset to zero at the defined calibration time.
- **Exited**: The number of people who left this group, which will be reset to zero at the defined calibration time.
- Color of the light:
  - `
  - Red light: Occupancy≥ red light threshold.
  - Yellow light: Yellow light threshold≤ occupancy < red light threshold.
  - Green light: Occupancy < yellow light threshold.

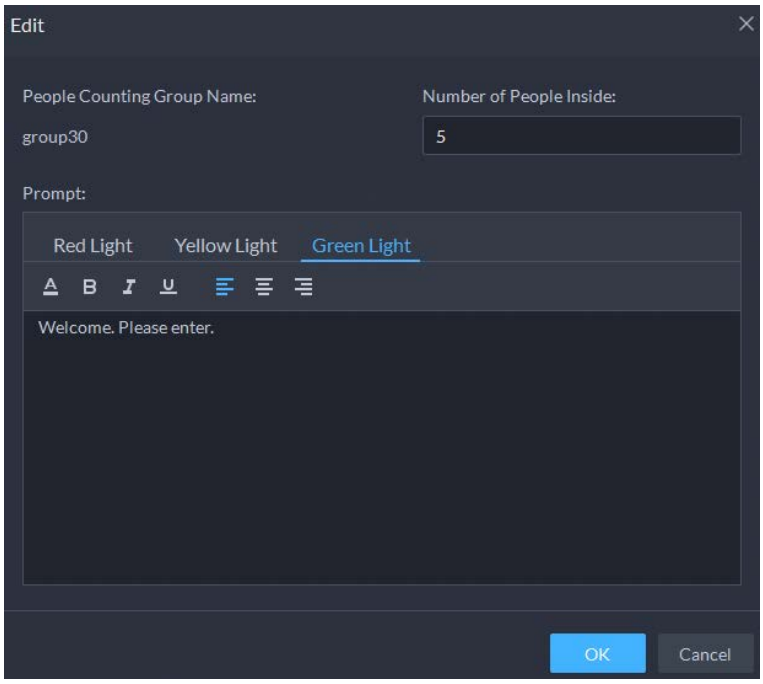
Figure 5-106 Real-time count



Step 3 Hover you mouse on the window displaying real-time data, and then click .

Step 4 You can enter a number of people to overwrite the current data, and customize the content to be displayed for green, yellow and red light.

Figure 5-107 Edit the content and data



Step 5 Click **OK**.

5.6.1.2 Historical Count

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Intelligent Analysis** > > **Historical Count**.

Step 2 Select the groups you want in **Groups**, or select the channels in **Resources**.

Step 3 Configure the search settings, and then click **Search**.

- **Groups**: Groups are people counting groups, which allow you to combine and calculate the people flow data from multiple rules across different devices and channels. You can search for historical people flow data from one or more people counting groups.
- **Resources**: Search for historical people flow data from one or more channels. The data from all the rules of a channel will be included.

Figure 5-108 Historical people counting data

Related Operations

- : Change the display format of the data.

  Only weekly report supports will display the number of retention.

- **Export**: Export the data into a .zip file to your PC.

5.6.2 Heat Maps

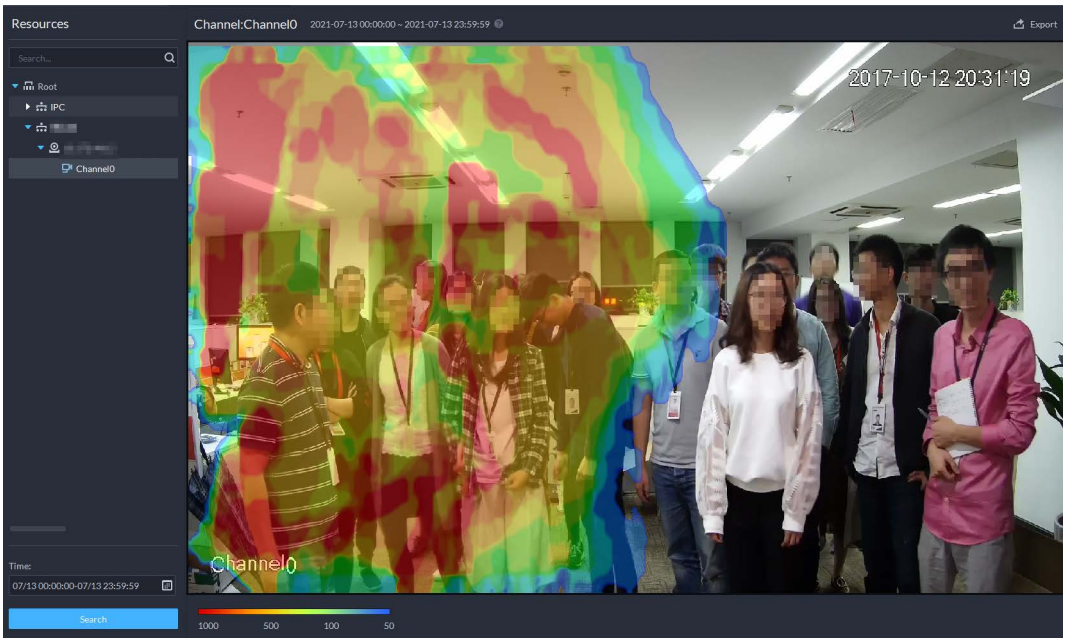
View heat maps generated by devices. A heat map shows the distribution of people flow by different colors, such red for many people have visited an area and blue for few people have visited an area.

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Intelligent Analysis** > .

Step 2 Select a channel and a time period, and then click **Search**.

You can select up to one week.

Figure 5-109 Heat map



Click **Export** at the upper-right corner to export the heat map as a .bmp file to your PC.

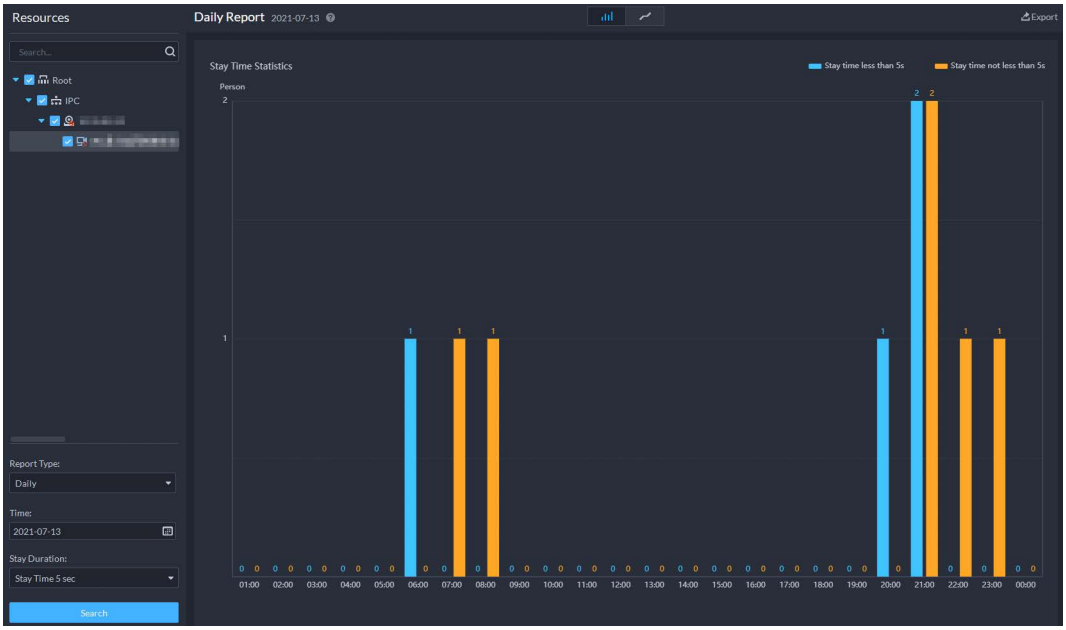
5.6.3 In-area People Counting

View the in-area people number statistics of one or more channels.

Step 1 Log in to the DSS Client. On the **Home** interface, click > **Intelligent Analysis** > .

Step 2 Select a channel and configure the search settings, and then click **Search**.

Figure 5-110 In-area people number statistics



Related Operations

- : Change the display format of the data.

- **Export**: Export the data to your PC.

6 General Application

This chapter introduces the general businesses, including target detection, face recognition, and ANPR.

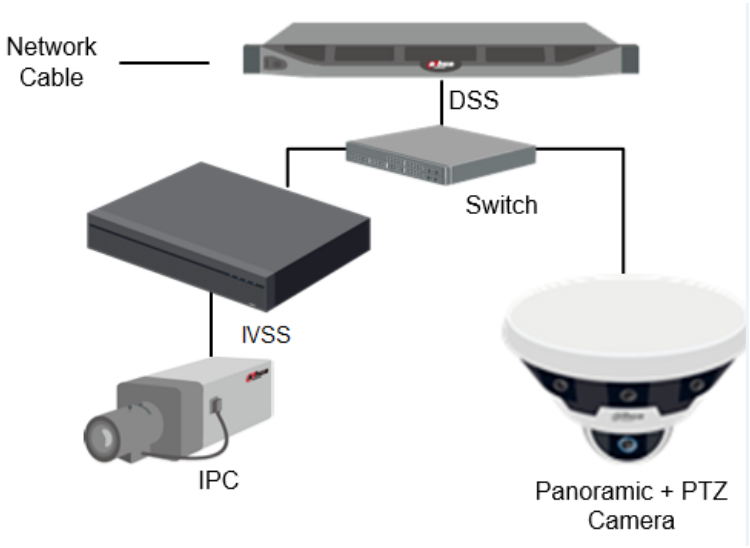
6.1 Target Detection

View and search for metadata of people, vehicle and non-motor vehicle.

Target detection can be done by video metadata cameras + a platform, or IPCs + IVSSs + platform.

6.1.1 Typical Topology

Figure 6-1 Typical topology



- General cameras record videos.
- Video metadata cameras such as panoramic + PTZ camera record videos and analyze people, and motor and non-motor vehicles.
- IVSS manages cameras and analyzes people, and motor and non-motor vehicles.
- The platform centrally manages IVSS and cameras, receives analysis results from cameras and displays the reports.

6.1.2 Preparations

Make sure the following preparations have been completed:

- Cameras and IVSS are correctly deployed, and video metadata is enabled on them. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic

Configurations".

- ◇ When adding a camera or IVSS, select **Encoder** for device category.
- ◇ After adding the camera or IVSS to the platform, select **Target Detection** from **Features** of the device.

6.1.3 Live Target Detection

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitoring Center** > **Monitor**.

Step 2 Select a window, double-click the channel or drag the channel to the window.

Figure 6-2 Live view

Step 3 Click and then click to view live metadata events.

Step 4 View live video, and human body, vehicle, and non-motor vehicle information.

- Click an event record to view the event snapshot. You can play back the video of the event. Different events support different operations.
- When playing back video, click to download the video to a designated path.
- Click to play back the video before and after the snapshot.
- Click to refresh events; click to pause refreshing.
- Click to delete event information.
- Click to view the most recent events.

6.1.4 Searching for Metadata Snapshots

Search for metadata snapshots by setting search criteria or uploading images.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **DeepXplore**.

Step 2 Click .

Step 3 Set search criteria.

You can search for metadata snapshots in the **Record**, **Person** or **Vehicle** section. For details, see "5.3 DeepXplore".

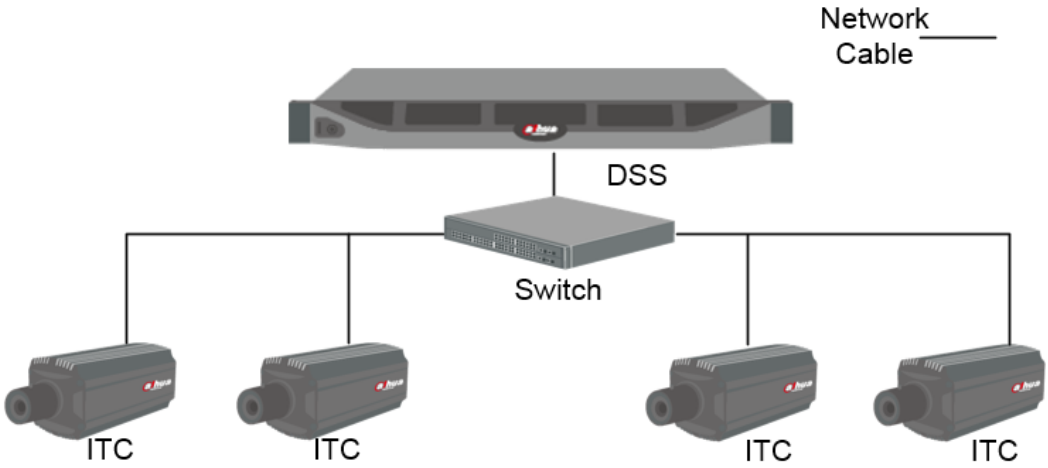
6.2 ANPR

View automatic number plate recognition in real time or search for records.

- Automatic number plate recognition
  DSS displays vehicle snapshots and ANPR results in real time.
- Vehicle records
  Search for vehicle records according to the filtering conditions you have set.

6.2.1 Typical Topology

Figure 6-3 Typical topology



- ANPR cameras (ITC camera) capture and recognize vehicles.
- DSS centrally manages ANPR cameras, receives and displays vehicle snapshots and information uploaded from the cameras.

6.2.2 Preparations

Make sure that the following preparations have been made:

- ANPR cameras are deployed, and the ANPR function is configured. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
  - ◇ When adding an ITC camera, select **ANPR** for device category, and then select **ANPR Device** for **Device Type**.
  - ◇ ANPR snapshots are only stored on **ANPR Picture** disks. On the **Storage** interface, configure at least one **ANPR Picture** disk. Otherwise vehicle pictures cannot be viewed.

6.2.3 Live ANPR

View ANPR live video and plate snapshots.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitor Center** > **Monitor**.

Step 2 Select a window, double-click the channel or drag the channel to the window.

Figure 6-4 Live view

Step 3 Click and then click .

Step 4 View live ANPR events.

- Click an event record to view event snapshots. You can also play back the video of the event. Different events support different operations.
- When playing back a video, click to download the video to a designated path.
- Click to play back the video before and after the snapshot.
- Click to refresh events; click to pause refreshing.
- Click to delete event information.
- Click to view the most recent events.

6.2.4 Searching for Vehicle Snapshot Records

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **DeepXplore**.

Step 2 Click .

Step 3 Set search criteria.

You can search for vehicle snapshots in the **Record** or **Vehicle** section. For details, see "5.3 DeepXplore".

6.3 Face Recognition

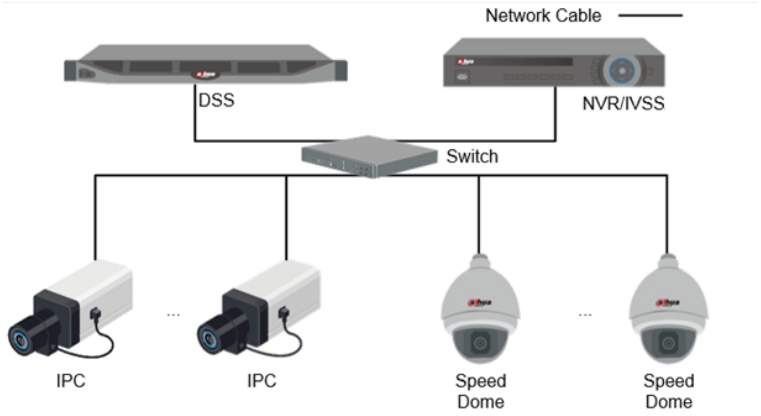
Configure face recognition settings on the device and the platform before you can view face recognition results on the platform.

6.3.1 Typical Topology

The face recognition feature is available on select models of NVR, IVSS and FR camera.

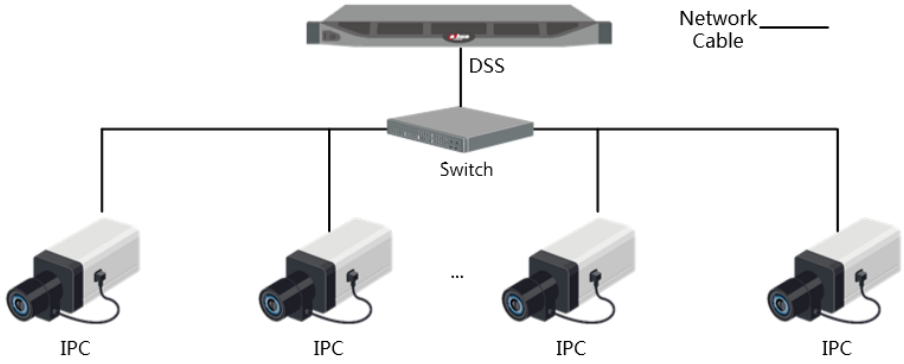
- Face recognition by NVR/IVSS

Figure 6-5 Typical topology (NVR/IVSS)



  - Cameras record videos.
  - NVR/IVSS is used for face recognition and storage.
  - DSS centrally manages cameras, NVRs, and the face database, and provides live view and face search.
- Face recognition by camera

Figure 6-6 Typical topology (camera)



  - Cameras record face videos, and detect and recognize faces.
  - DSS centrally manages cameras, NVRs, and the face database, and provides live view and face search.

6.3.2 Preparations

Make sure that the following preparations have been made:

- Face recognition devices are correctly deployed. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
  - When adding face recognition devices, select **Encoder** for device category.
  - After adding a face recognition NVR or IVSS, select **Face Recognition** for **Features** of the corresponding channels.
  - After adding face recognition cameras or face detection cameras, select **Face Recognition** or **Face Detection** for **Features**.
  - Face snapshots are stored in the **Face/Alarm and Other Pictures** disk. Configure at least one

local disk for picture storage. Otherwise, the platform cannot display snapshots.

6.3.3 Arming Faces

Before arming faces, you need to add the persons to face recognition group. For details, see "4.4.1 Face Watch List".

6.3.4 Live Face Recognition

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **Monitor Center** > **Monitor**.

Step 2 Select a window, double-click the channel or drag the channel to the window.

Figure 6-7 Live view

Step 3 Click and then click to view live face recognition information.

Step 4 View live video, and human body, vehicle, and non-motor vehicle information.

- Click an event record to view event snapshots. You can play back the video of the event. Different events support different operations.
- When playing back video, click to download the video to designated path.
- Click to play back the video before and after the snapshot.
- Click to refresh events; click to pause refreshing.
- Click to delete event information.
- Click to view the most recent events.

6.3.5 Searching for Face Snapshots

Search for face snapshots by setting search criteria or uploading images.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then select **DeepXplore**.

Step 2 Click .

Step 3 Set search criteria.

You can search for vehicle snapshots in the **Record** or **Person** section. For details, see "5.3 DeepXplore".

7 System Configurations

Introduce system parameters configuration, license, service management and backup and restore.

7.1 License

The system controls channel and function availability through the license. User can buy a license according to the channels and functions as needed.

The platform is unlicensed by default after being deployed.

License Types

- Trial
  A trial license is limited in capacity and expires in 90 days.
- Paid
  To acquire full control of the features and permanent use, you need to buy a formal license. After activating the first paid license, if you might want to increase your license capacity, you can buy more license codes. For example, if you have 500 channels currently, you can buy another 500 channels. After activating the new 500 channels, you will have 1,000 channels in total.
- Unlicensed
  Lack permissions to use the system. This occurs after deactivating.

For expired trial version and unlicensed version, all modules are displayed as unauthorized, except for the resources, license, tools, and management modules.

Activation Methods

- Normal online activation
  When the platform server is connected to the Internet, it can connect to the license server, which supports online license activation by verifying the activation code.
- Normal offline activation
  When the platform server is on a local area network, it cannot connect to the license server. You need to obtain the license file from a computer with Internet access, and then import the license file to the platform to activate it.

7.1.1 Activating License

You can get the desired features or number of channels only after you load the corresponding license.

For details about activating a license, see "2.1.6.2 Activating License".

7.1.2 Deactivating License

After deactivation, the platform will go back to the unauthorized state. A deactivated license can be activated again on other servers, allowing users to change servers. The license can be deactivated with online and offline deactivation. If the server is connected to the network, use online deactivation, otherwise use offline deactivation.

- After you deactivate the license, the system returns to the inactive status.
- Deactivated license can be used again. Keep it safe.

7.1.2.1 Online Deactivation

Background Information

Select this method if your platform sever is connected to a network.

Procedure

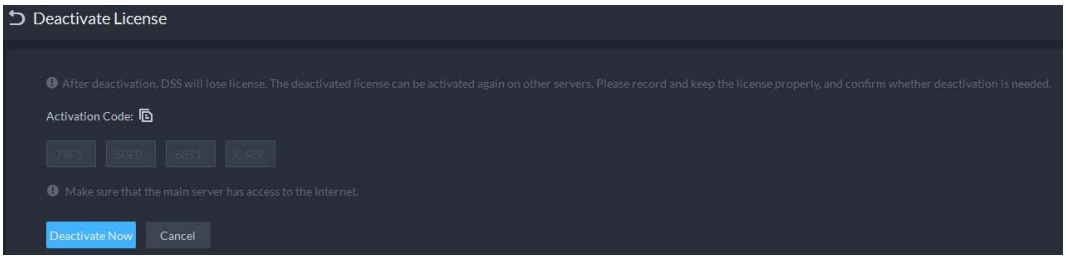
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **License**.

Step 2 In the **Deactivate License** section, click **Online Deactivate License**.

The license is reusable. We recommend copying the license code by clicking and then saving it locally.

Step 3 Click **Deactivate Now**, and then follow the onscreen instructions to finish deactivation.

Figure 7-1 Online deactivation



7.1.2.2 Offline Deactivation

Background Information

Select this method if your platform server has no Internet access.

Procedure

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **License**.

Step 2 In the **Deactivate License** section, click **Offline Deactivate License**.

Figure 7-2 Offline deactivation

Step 3 Click **Export** to export and save the license deactivation file locally.

Step 4 Move the request file to a computer with Internet access. On that computer, open the system email that contains your license, and then click the attached webpage address to go to the license management page.

Step 5 Upload the license request file obtained from step 1, and then follow onscreen instructions to finish deactivation.

7.2 System Parameters

Configure storage retention duration, email server, time sync, remote log, login method, and more.

7.2.1 Configuring System Data Retention Period

Set the retention periods for logs, alarm messages, face recognition records, vehicle passing records, access snapshot records, video communication records, visitor records, and more. Records beyond the defined retention period will be automatically deleted.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **System Parameter**.

Step 2 Click **Message Retention Period**.

Step 3 Double-click numbers to modify the values.

Step 4 Click **Save**.

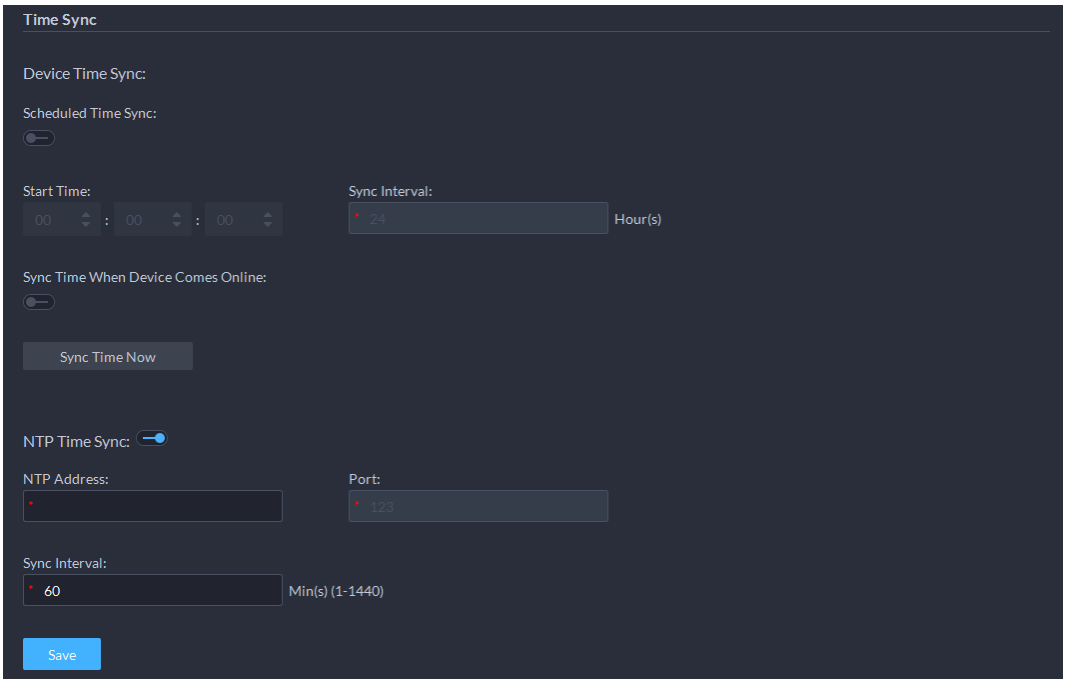
7.2.2 Time Synchronization

Synchronize the system time of all connected devices with that of the platform; otherwise the system might malfunction. For example, video search might fail. The platform supports synchronizing the time of multiple devices connected through the Dahua protocol and ONVIF. You can synchronize manually or automatically.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **System Parameter**.

Step 2 Click the **Time Sync** tab. Enable the sync methods, and then set parameters.

Figure 7-3 Enable time synchronization



- Scheduled Time Sync: Enable the function, enter the start time in time sync for each day, and the interval.
- Sync Time When Device Comes Online: Syncs device time when the device goes online.
- NTP Time Sync: If there is an NTP server in the system, you can enable this function to let the system enable time with the NTP server.

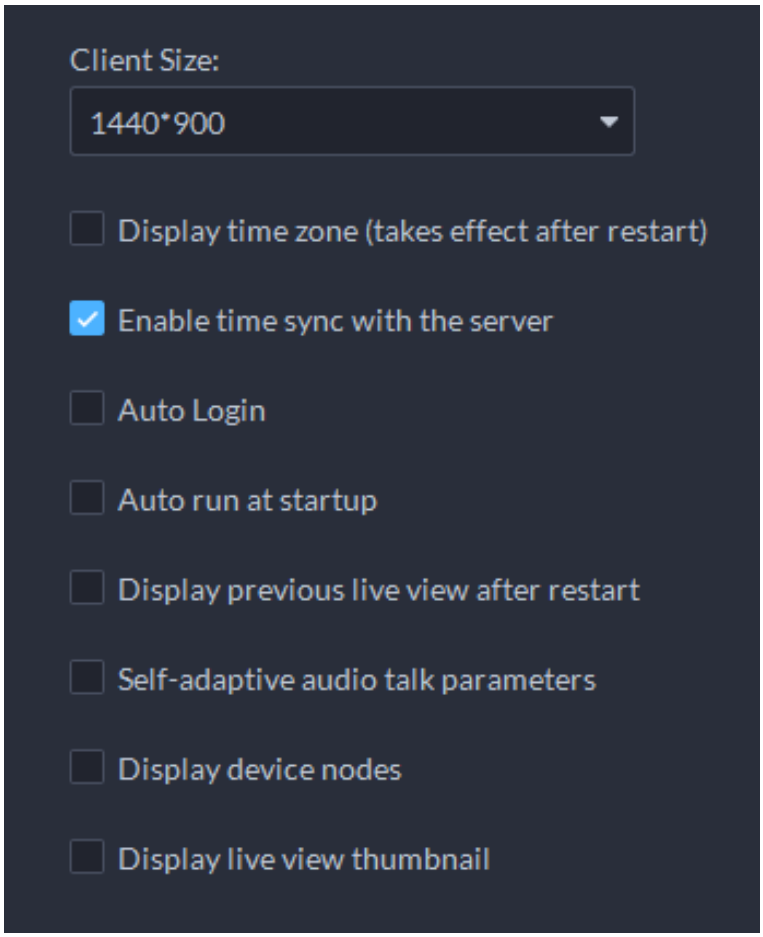
Step 3 Click **Save**.

Step 4 (Optional) Enable time synchronization on DSS Client.

1) Log in to the DSS Client, and then in the **Management** section, click **Local Settings**.
2) Click the **Basic** tab, select the check box next to **Enable time sync with platform server**, and then click **Save**.

The system immediately synchronizes the time after you enable the function.

Figure 7-4 Enable time sync



3) Restart the client for the configuration to take effect.

7.2.3 Configuring Email Server

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **System Parameter**.

Step 2 Click the **Email Server** tab, enable **Email Server**, and then configure parameters as required.

Figure 7-5 Set email server

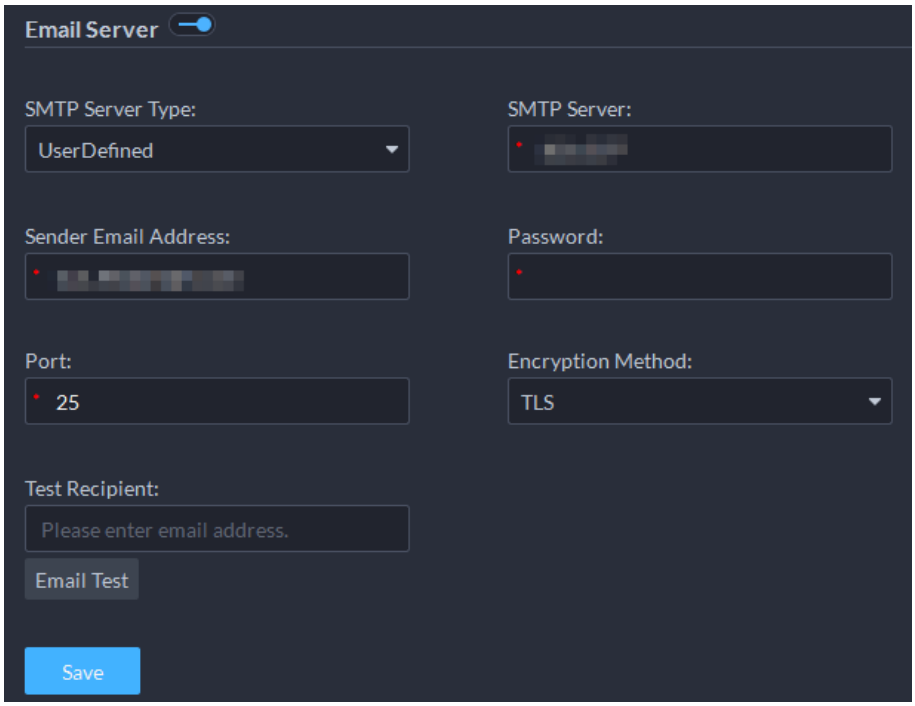


Table 7-1 Description of email server parameters

Parameter	Description
SMTP Server Type	Select according to the type of SMTP server to be connected. The types include **Yahoo**, **Gmail**, **Hotmail**, and **UserDefined**.
Sender Email Address	The sender displayed when an email is sent from DSS.
SMTP Server	IP address, password, and port number of the SMTP server.
Password	
Port	
Encryption Method	Supports no encryption, TLS encryption, and SSL encryption.
Test Recipient	Set the recipient, and then click **Email Test** to test whether the mailbox is available.
Email Test	

Step 3 Click **Save**.

7.2.4 Importing HTTPS Certificate

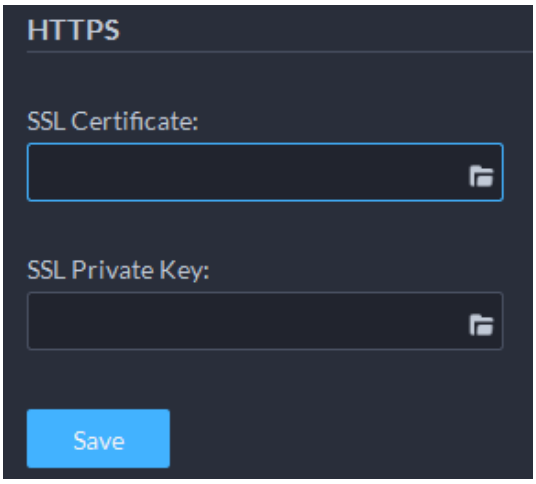
HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is a safe HTTP transmission protocol. It is safe and stable, and guarantees the security of user information and devices. When HTTPS certificate is configured, you can log in to the platform through HTTPS protocol to ensure transmission security.

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **System Parameter**.

Step 2 Click the **HTTPS** tab.

Step 3 Click to select the SSL certificate, and then enter the password.

Figure 7-6 HTTPS certificate



Step 4 Click **Save**.

7.2.5 Configuring Device Login Mode

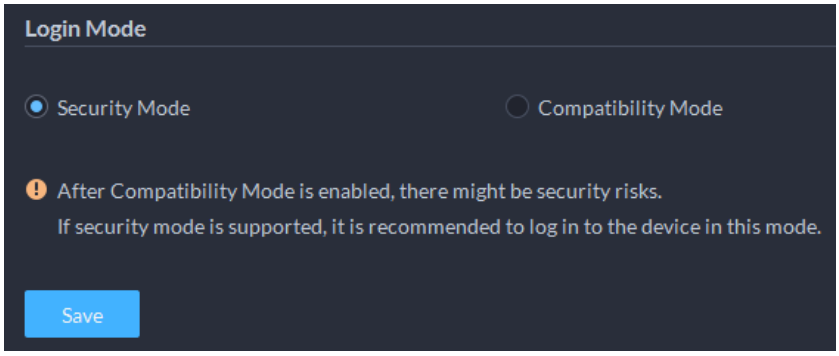
To ensure that you can use the device safely, we recommend using the security mode (if the device supports this mode. Otherwise, select compatibility mode).

Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **System Parameter**.

Step 2 Click the **Login Mode** tab.

Step 3 Select a mode.

Figure 7-7 Select a login mode



Step 4 Click **Save**.

7.2.6 Remote Log

To ensure safe use of the platform, the system sends administrator and operator logs to the log server for backup at 3 A.M. every day.

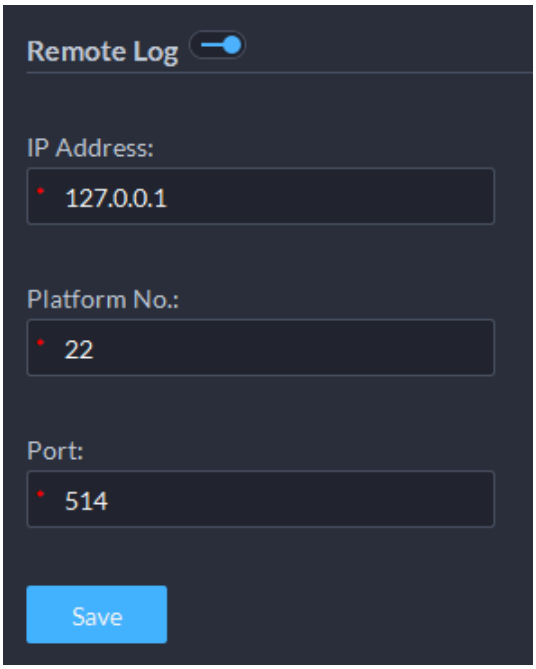
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **System Parameter**.

Step 2 Click the **Remote Log** tab.

Step 3 Enable the function, and then set parameters as required.

The **Platform No.** must be the same on the remote server and the platform.

Figure 7-8 Enable remote log



Step 4 Click **Save**.

7.3 Backup and Restore

DSS supports backing up configuration information and saving it to a local PC or server, so that you can use the backup file for restoring settings.

7.3.1 System Backup

Use the data backup function to ensure the security of user information. Data can be manually or automatically backed up.

- Manual backup: Manually back up the data, and the DSS platform will save it locally.
- Automatic backup: The DSS platform automatically backs up the data at a defined time, and saves it to the installation path of the platform server.

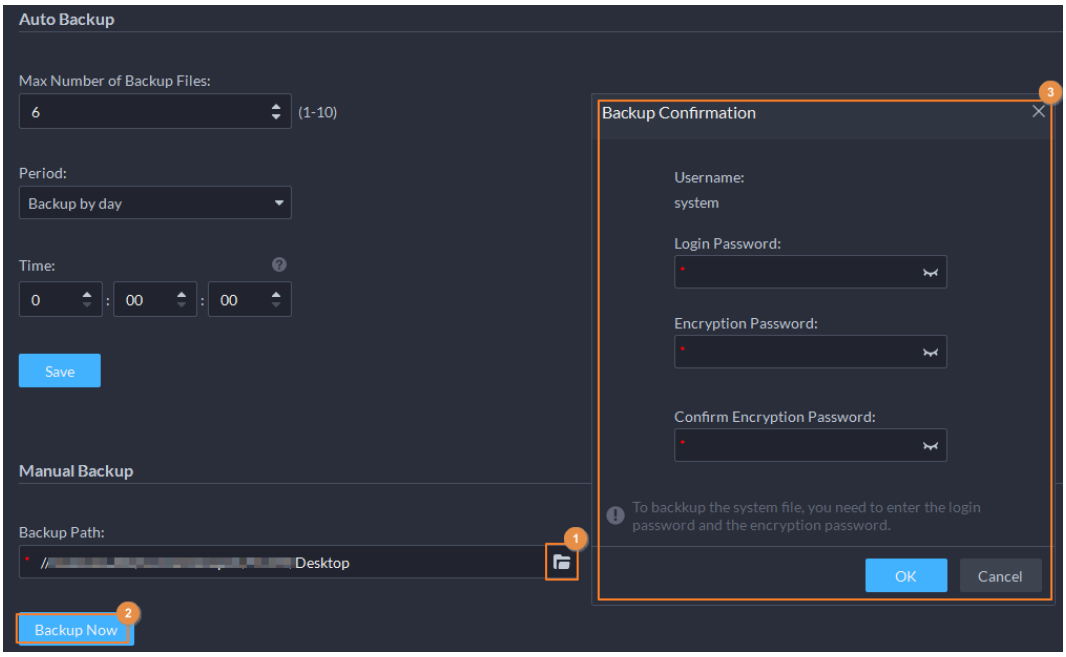
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **Backup and Restore**.

Step 2 Click the **Backup** tab.

Step 3 Back up data.

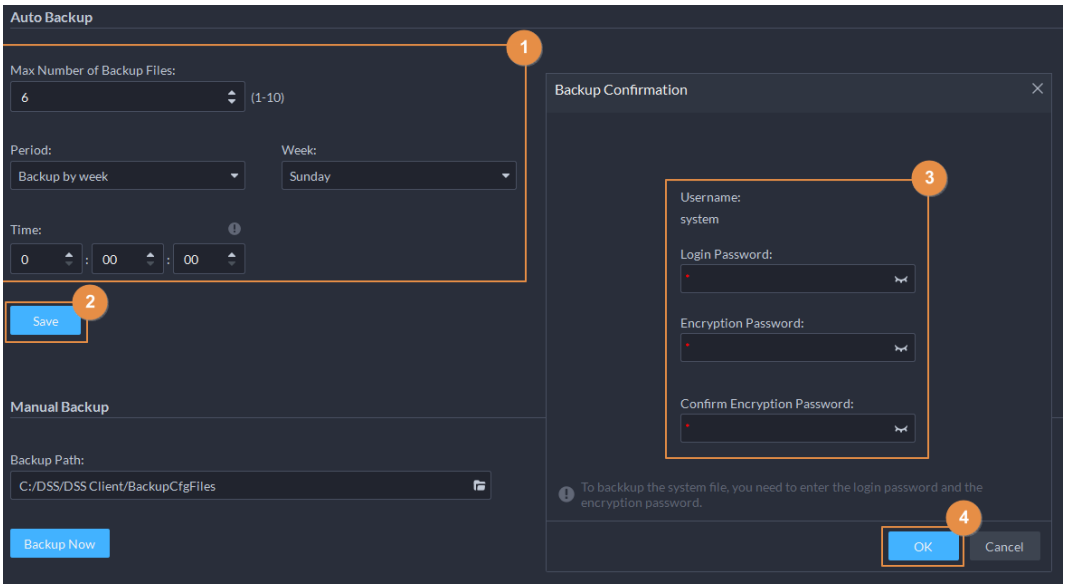
- Manual backup: In the **Manual Backup** section, select the data saving path, click **Backup Now**. The **Login Password** is the same as the system user's. Create an **Encryption Password** to protect data.

Figure 7-9 Manual backup



- Auto backup: In the **Auto Backup** section, configure backup parameters, and then click **OK**. The **Login Password** is the same as the system user's. Create an **Encryption Password** to protect the data. The platform automatically backs up data according to the defined time and period. The backup path is the installation path of the platform server by default.

Figure 7-10 Auto backup



7.3.2 System Restore

Restore the data of the most recent backup when the database becomes abnormal. It can quickly restore your DSS system and reduce loss.

- Local Restore: Import the backup file locally.
- Server Restore: Select the backup file from the server.

⚠

- Stop users from using the platform before performing system restore.
- Restoring the system will change system data. Be cautious.

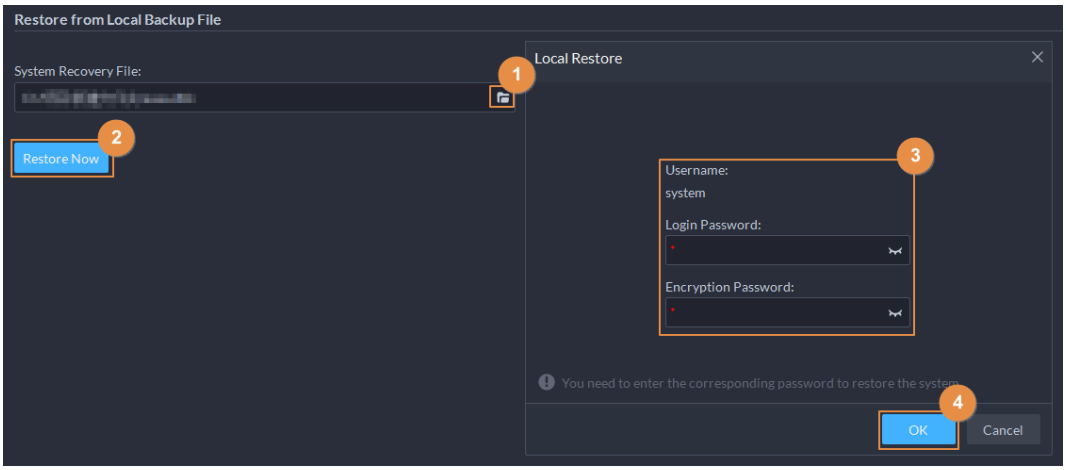
Step 1 Log in to the DSS Client. On the **Home** interface, click , and then in the **System Config** section, select **Backup and Restore**.

Step 2 Click the **Restore** tab.

Step 3 Restore data.

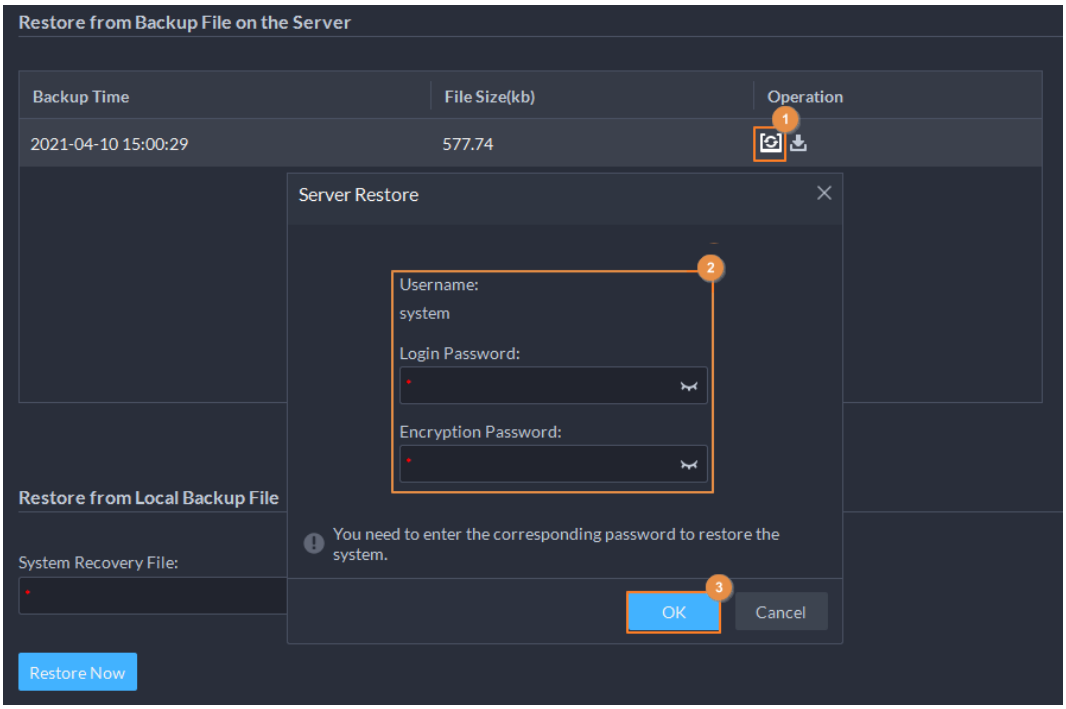
- Restore from local backup file: In the **Restore from Local Backup File** section, select the backup file path, click **Restore Now**, and then enter the passwords (the **Password** is the same as the system user's. The **Encryption Password** is the one created when the file was backed up).

Figure 7-11 Local restore



- Restore from backup file on the server: In the **Restore from Backup File on the Server** section, click , enter the passwords (the **Password** is the same as the system user's. The **Encryption Password** is the one created when the file was backed up), and then click **OK**. After restoration, the platform will automatically restart.

Figure 7-12 Server restore



You can click to download the backup file.

8 Management

8.1 Managing Logs

View and export operator logs, device logs and system logs, and enable service log debug mode for troubleshooting.

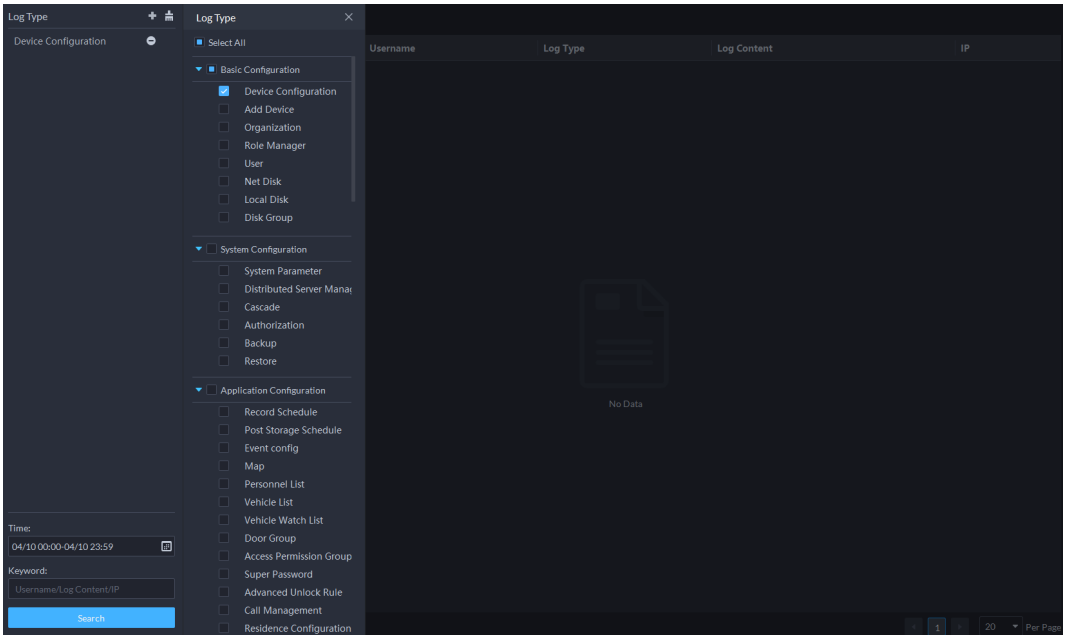
8.1.1 Operator Log

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Log**.

Step 2 Click .

Step 3 Click , select log type, specify time and keyword, and then click **Search**.

Figure 8-1 Search for operator log



Step 4 To export the logs, click **Export**.

8.1.2 Device Log

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Log**.

Step 2 Click .

Step 3 Select a device and time, and then click **Search**.

Step 4 To export the logs, click **Export**.

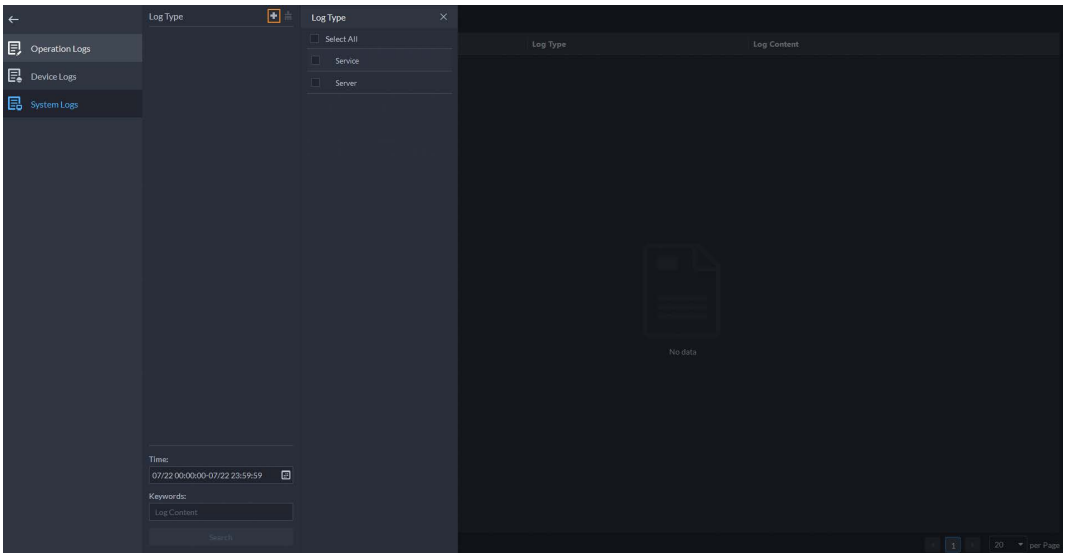
8.1.3 System Log

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Log**.

Step 2 Click .

Step 3 Click , and then select one or more types of logs you want to search for.

Figure 8-2 Search for system log



Step 4 Configure the time and enter keywords, and then click **Search**.

Step 5 (Optional) Click **Export**.

Follow the onscreen instruction to export logs to your PC.

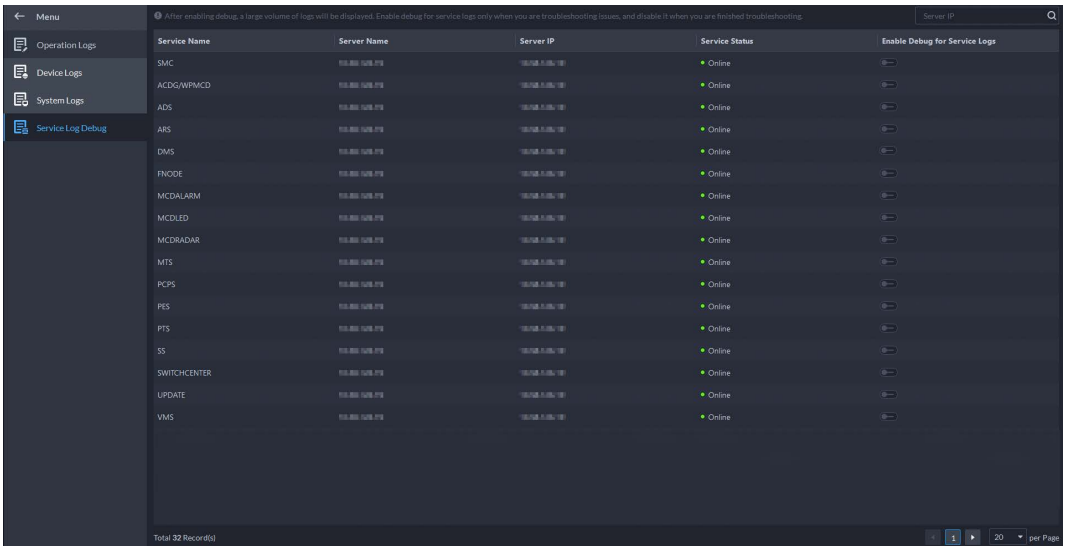
8.1.4 Service Log Debug

Enable the debug mode of a service, and then it generate logs that are more detailed for troubleshooting.

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Log**.

Step 2 Click .

Figure 8-3 Service log debug



Step 3 Enable the debug mode of one or more services.

After the debug mode of a service is enabled, the service will generate large amount of logs that take more disk space. We recommend you disable the debug mode after you have finish troubleshooting.

8.2 Downloading Videos

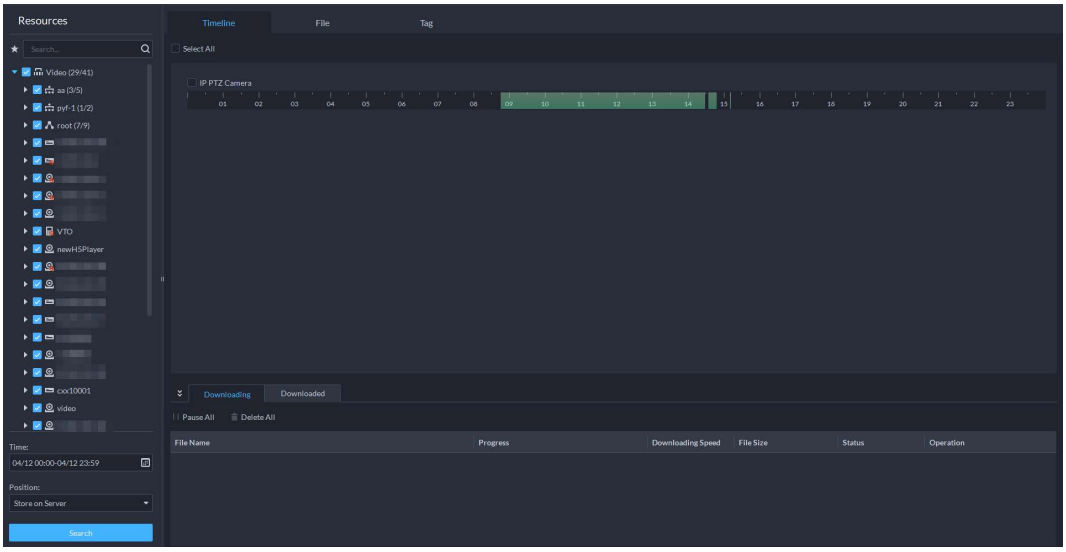
You can download videos of interest stored on the server or the device. The downloaded videos are in .avi, .mp4, or .asf format. Three ways to download videos are:

- Download clipped videos from the timeline.
- Download video files from the file list.
- Download videos by using video tags to search.

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Download Center**.

Step 2 Set search conditions, and then click **Search**.

Figure 8-4 Download center



Step 3 Select videos to download.

- To download videos by clipping the timeline, click the **Timeline** tab, and then select the start and end time of the video clip by clicking on the timeline.
- To download videos by selecting searched video files, click the **File** tab, and then click .
- To download tagged videos, click the **Tag** tab, and then click .

Step 4 In the password verification dialogue box that appears, enter the password, and then click **OK**.

Step 5 When downloading clipped videos, in the **Download Recorded Video** dialogue box, confirm the time span, and then, if necessary, click to select a video format. Click **OK**. After the download is finished, click in the prompt message at the upper-right corner to play the video directly in **Local Video**. See "8.4 Playing Local Videos".

8.3 Configuring Local Settings

After logging in to the client for the first time, you need to configure the following fields under system parameters: Basic settings, video parameters, record playback, snapshot, recording, alarm, security settings and shortcut keys.

8.3.1 Configuring General Settings

Configure client language, client size, time, and more.

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Local Settings**.

Step 2 Click **General**, and then configure the parameters.

Figure 8-5 General parameters

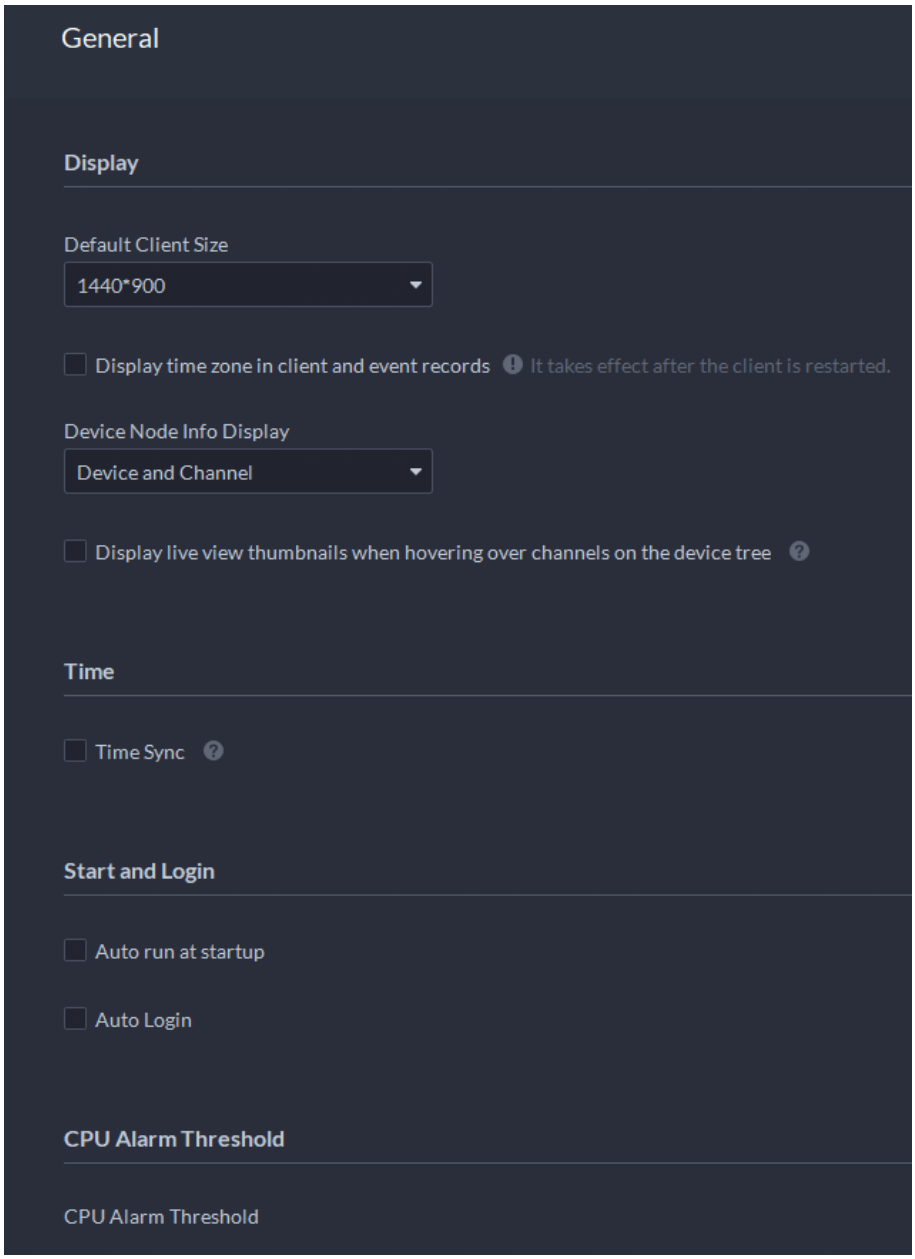


Table 8-1 Parameter description

Parameters	Description
Default Client Size	Select a proper resolution for the client according to PC display screen.
Display time zone in client and event records	When selected, the client and the time of alarms will show both the time and time zone.
Device Node Info Display	Select that the device tree displays devices and their channels or only channels.
Display live view thumbnails when hovering over channels on the device tree	When selected, you can hover the mouse over a channel in the device tree in **Monitoring Center** and a snapshot of its live video image will be displayed.
Time Sync	If enabled, the client starts to synchronize network time with the server to complete time synchronization.

Parameters	Description
Auto run at startup	• If **Remember Password** has been selected on the **Login** interface, select **Auto restart after reboot**, and the system will skip the login interface and directly open the homepage after you restart the PC next time. • If **Remember Password** is not selected on the **Login** interface, select **Auto restart after reboot**, the client login interface will appear after you restart the PC.
Auto Login	Enable the system to skip the login interface and directly open the homepage when logging in next time. • If **Remember Password** and **Auto Login** have been selected on the **Login** interface, the function is already enabled. • If **Remember Password** has been selected while **Auto Login** is not selected on the **Login** interface, select **Auto Login** on the **Basic** interface to enable this function. • If neither **Remember Password** nor **Auto Login** has been selected on the **Login** interface, select **Auto Login** on the **Basic** interface and you then to enter the password when logging in next time to enable the function.
CPU Alarm Threshold	The user will be asked to confirm whether to open one more video when the CPU usage exceeds the defined threshold.
Audio and video transmission encryption	Encrypt all audio and video to ensure information security.
Auto Lock Client	The client will be locked after the defined period and you cannot perform any operation. Click **Click to Unlock Client** and verify the password of the current account to unlock the client. You can configure up to 60 minutes.
Self-adaptive audio talk parameters	If enabled, the system automatically adapts to the device sampling frequency, sampling bit, and audio format for audio talk.

Step 3 Click **Save**.

8.3.2 Configuring Video Settings

Configure window split, display mode, stream type and play mode of live view, and instant playback length.

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Local Settings**.

Step 2 Click **Video**, and then configure the parameters.

Figure 8-6 Video parameters

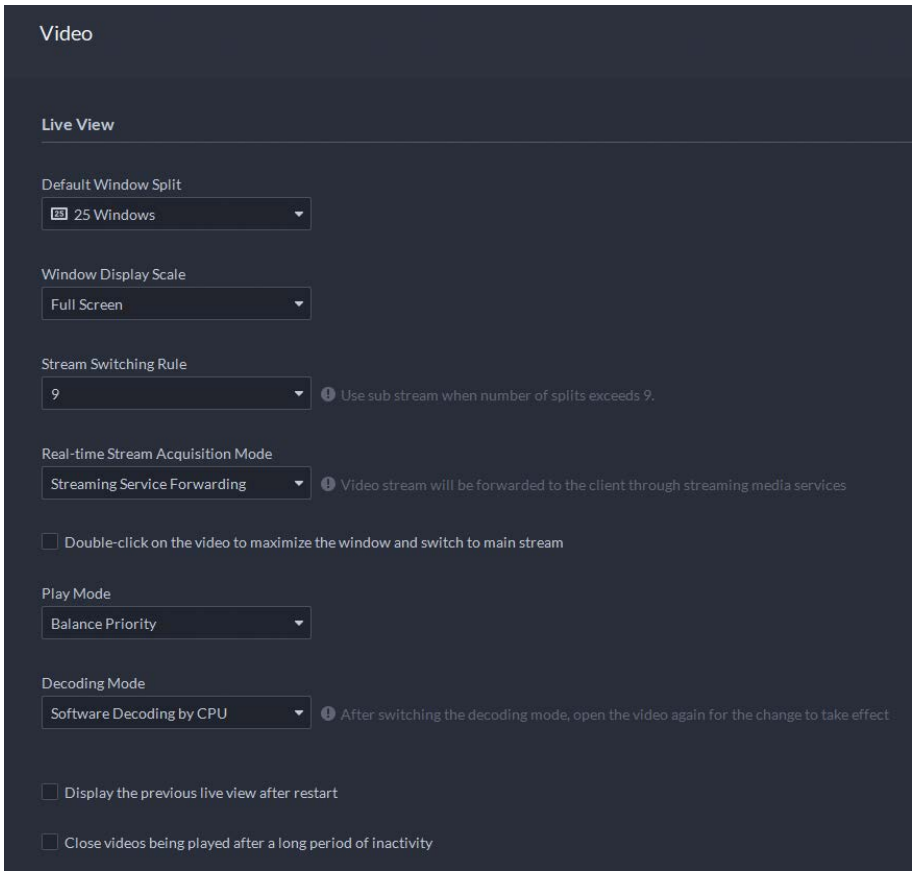


Table 8-2 Parameter description

Parameters	Description
Default Window Split	Set split mode of the video window.
Window Display Scale	Select from **Original Scale** and **Full Screen**.
Stream Switching Rule	When the number of window splits is greater than the defined value, the live video will switch from the main stream type to sub stream type.
Real-time Stream Acquisition Mode	Select the one according to your situation. If you select **Acquire directly from the device**, clients will acquire video streams directly from the channel. If direct acquisition fails, the platform will forward the video streams to clients. When the device and clients are properly connected to the network, direct acquisition can reduce the use of the platform's forwarding bandwidth. If too many clients are acquiring video streams from a channel, acquisition might fail due to insufficient performance of the device. Video streams will be forwarded to clients by the platform.
Double-click on the video to maximize the window and switch to main stream	If selected, you can double-click a video window to maximize it and switch from sub stream to main stream. Double-click again to restore the window size, and then the system will switch it back to sub stream.

Parameters	Description
Play Mode	• **Real-time Priority** The system might lower the image quality to avoid video lag. • **Fluency Priority** The system might lower the image quality and allow for lag to ensure video fluency. The higher the image quality, the lower the video fluency will be. • **Balance Priority** The system balances real-time priority and fluency priority according to the actual server and network performance. • **Custom** The system adjusts video buffering and lowers the impact on video quality caused by unstable network. The bigger the value, the more stable the video quality will be.
Decoding Mode CPU Threshold	• **Software Decoding by CPU**: All videos will be decoded by the CPU. When you are viewing live videos from large amount of channels, it will take up too much resources of the CPU that affects other functions. • **Software Decoding by GPU**: All videos will be decoded by the GPU. The GPU is better at concurrent operation than the CPU. This configuration will free up resources of the CPU significantly. • **Performance Mode (CPU First)**: All videos will be decoded by the CPU first. When the resources of the CPU is taken up to the defined threshold, the platform will use the GPU to decode videos.
Display previous live view after restart	If selected, the system displays the last live view automatically after you restart the client.
Close videos being played after long period of inactivity Inactivity Time	The system closes live view automatically after inactivity for a pre-defined period of time. Supports up to 30 minutes.
Instant Playback Time	Click on the live view interface to play the video of the previous period. The period can be user-defined. For example, if you set 30 seconds, the system will play the video of the previous 30 seconds.
Search Type of Device Video Stream	Select a default stream type when you play back recordings from a device. If **Only Sub Stream 2** is selected, but the device does not support sub stream 2, then recordings of sub stream 1 will be played.
Extract frames when playing back HD videos	If selected, when the playback stream is big due to high definition, certain frames will be skipped to guarantee fluency and lower the pressure on decoding, bandwidth and forwarding.
Continuous Snapshot Interval	Set the number and interval between each snapshot.

Parameters	Description
Number of Continuous Snapshots	For example, if the **Continuous Snapshot Interval** is 10 seconds and the **Number of Continuous Snapshots** is 4, when you right-click on the live/playback video and select **Snapshot**, 4 images will be taken every 10 seconds.

Step 3 Click **Save**.

8.3.3 Configuring Video Wall Settings

Configure the default binding mode and stream type of video wall.

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Local Settings**.

Step 2 Click **Video Wall**, and then configure the parameters.

Figure 8-7 Configure video wall settings

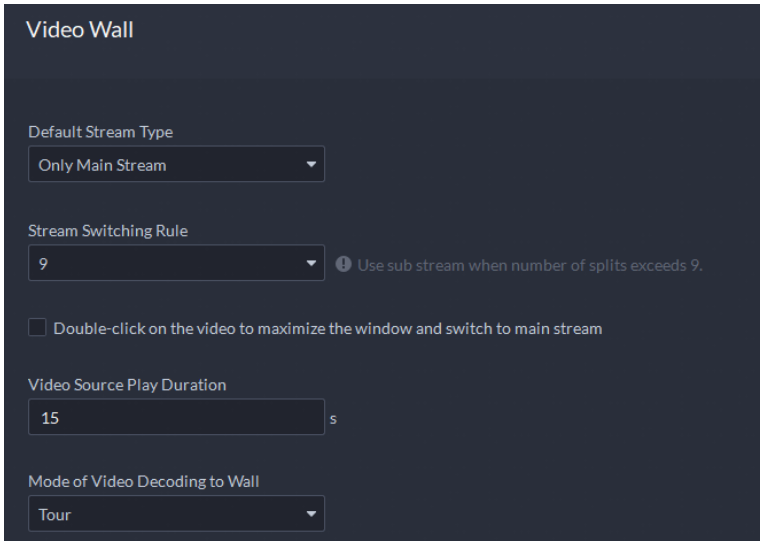


Table 8-3 Parameter description

Parameter	Description
Default Stream Type	Select **Main Stream**, **Sub Stream 1**, **Sub Stream 2** or **Local Signal** as the default stream type for video wall display.
Stream Switching Rule	When the number of window splits is greater than the defined value, the live video will switch from the main stream type to sub stream type.
Double-click on the video to maximize the window and switch to main stream	Double-click on the video to maximize the window, and then its stream type will switch to main stream.
Video Source Play Duration	Set the default time interval between the channels for tour display. For example, if 5 seconds is configured and you are touring 3 video channels, the live video image of each channel will be played 5 seconds before switching to the next channel.

Parameter	Description
Mode of Video Decoding to Wall	• **Tour**: Multiple video channels switch to decode in one window by default. • **Tile**: Video channels are displayed in the windows by tile by default. • **Ask Every Time**: When dragging a channel to the window, the system will ask you to select tour or tile mode.

Step 3 Click **Save**.

8.3.4 Configuring Alarm Settings

Configure alarm sound and alarm display method on the client.

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Local Settings**.

Step 2 Click **Alarm**, and then configure the parameters.

Figure 8-8 Configure alarm settings

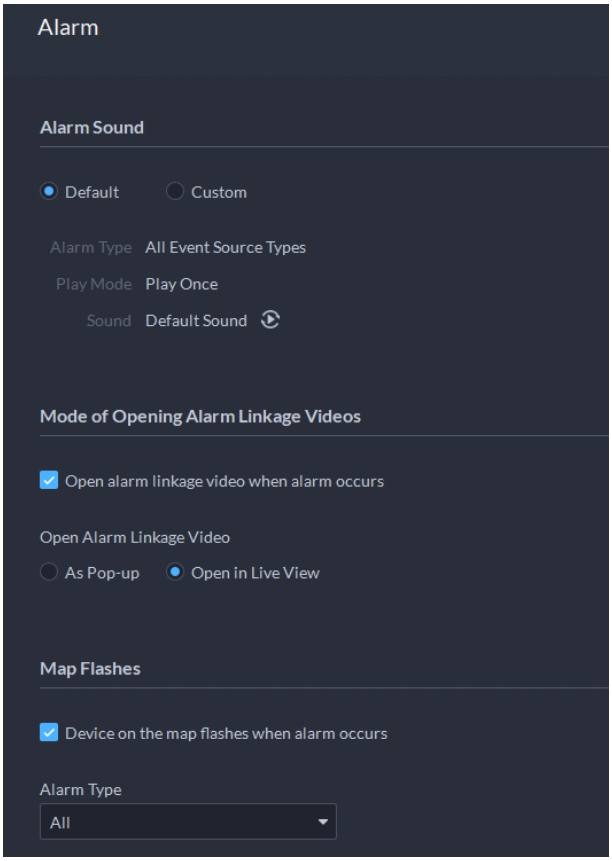


Table 8-4 Parameter description

Parameters	Description
Default	All types of alarms will use the same default alarm sound when triggered.
Custom	Click **Modify Alarm Sound**, and then you can change the alarm sound and its play mode of each type of alarm.
Open alarm linkage video when alarm occurs	If selected, the platform will automatically open linked video(s) when an alarm occurs.

Parameters	Description
Open Alarm Linkage Video	• **As Pop Up**:The alarm video will be played in an pop-up window. • **Open in Live View**: The alarm video will be played in a window in **Monitoring Center**.
Device on the map flashes when alarm occurs	Set one or more alarm types for alarm notification on the map. When an alarm occurs, the corresponding device will flash on the map.

Step 3 Click **Save**.

8.3.5 Configure File Storage Settings

Configure the storage path, naming rule, file size, and format of recordings and snapshots.

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Local Settings**.

Step 2 Click **File Storage**, and then configure the parameters.

Figure 8-9 Configure file storage settings

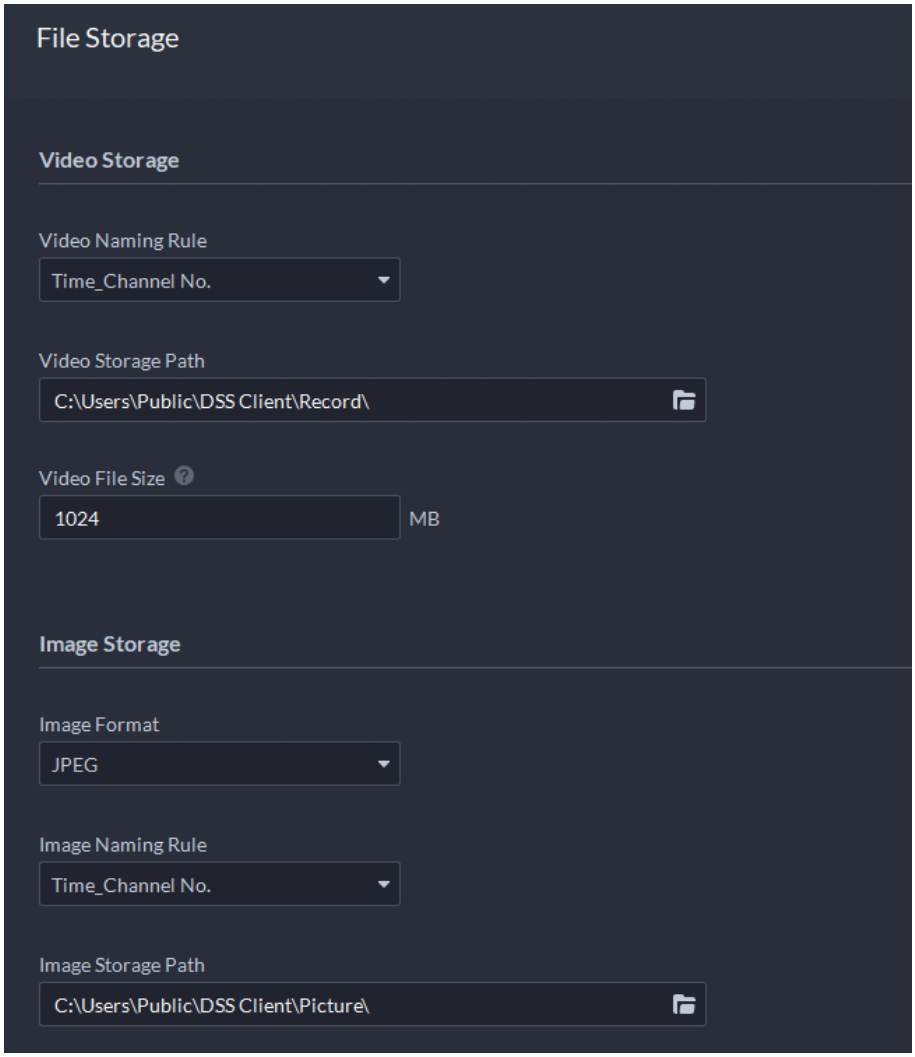


Table 8-5 Parameter description

Parameters	Description
Video Naming Rule	Select a naming rule for manual recordings.

Parameters	Description
Video Storage Path	Set a storage path of manual recordings during live view or playback. The default path is C:\Users\Public\DSS Client\Record.
Video File Size	Configure the maximum size of a single recording file.
Image Format	Select a format of snapshots.
Image Naming Rule	Select a naming rule for snapshots.
Image Storage Path	Set a storage path for snapshots. The default path is C:\Users\Public\DSS Client\Picture.

Step 3 Click **Save**.

8.3.6 Viewing Shortcut Keys

View shortcut keys for operating the client quickly.

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Local Settings**.

Step 2 Click **Shortcut Key** to view shortcut keys of the PC keyboard and USB joystick.

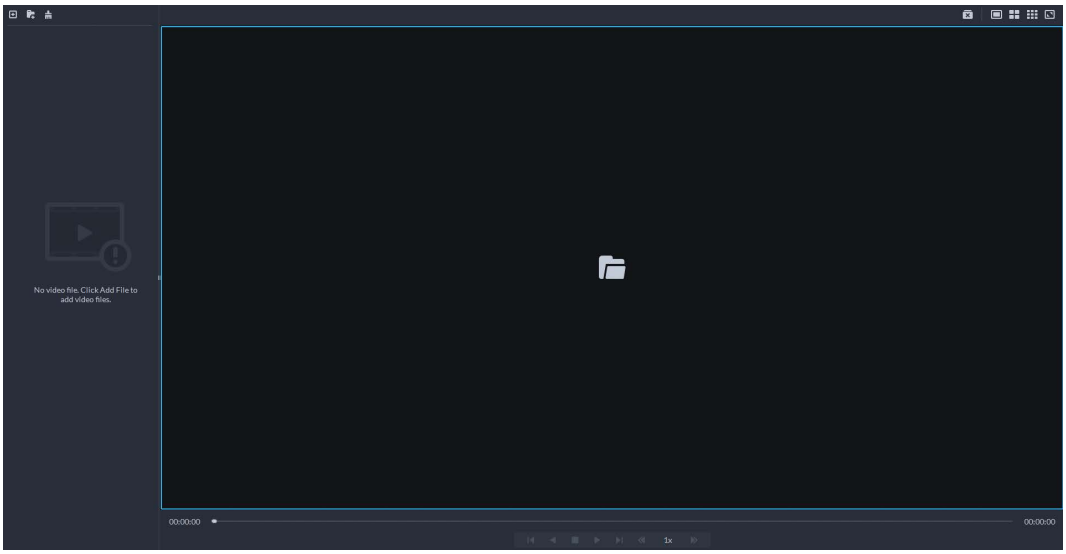
Figure 8-10 View shortcut keys

8.4 Playing Local Videos

You can play local videos directly on the platform.

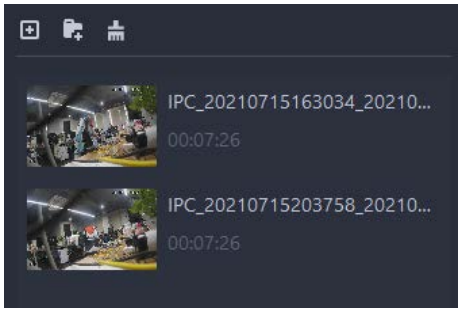
Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Local Video**.

Figure 8-11 Local video



Step 2 Click to select one or more files, or to open all files in a folder.

Figure 8-12 Playlist



Step 3 Drag a file to the window on the right or right click it to play.

Related Operations

Table 8-6 Interface operation

Icon/Function	Description
Right-click menu	• **Continuous Snapshot**: Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to ..*DSS**DSS Client**Picture* by default. To change the snapshot saving path, see "8.3.5 Configure File Storage Settings". • **Video Adjustment**: Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement. • **Digital Zoom**: Click it, and then double-click the video image to zoom in the image. Double-click the image again to exit zooming in.
	Close all playing videos.
	Split the window into multiple ones and play a video in full screen.
	Take a snapshot of the current image and save it locally. The path is C:\DSS\DSS Client\Picture\ by default.
	Close the window.
	Stop/pause the video.
1x	Fast/slow playback. Max. supports 64X or 1/64X.

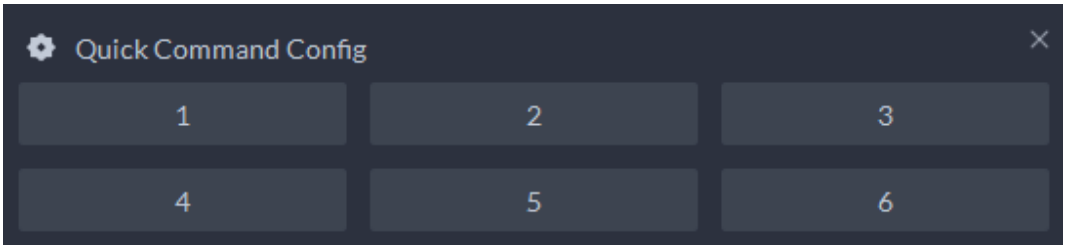
Icon/Function	Description
	Frame by frame playback/frame by frame backward.
	Capture the target in the playback window. Click to select the search method, and then the system goes to the interface with search results. More operations: • : Move the selection area. • : Adjust the size of the selection area. • Right-click to exit search by snapshot.

8.5 Quick Commands

Customize HTTP commands and execute them quickly. Request methods of GET, POST, PUT and DELETE are supported.

Step 1 Log in to the DSS Client. On the **Home** interface, select **Management** > **Quick Commands**.

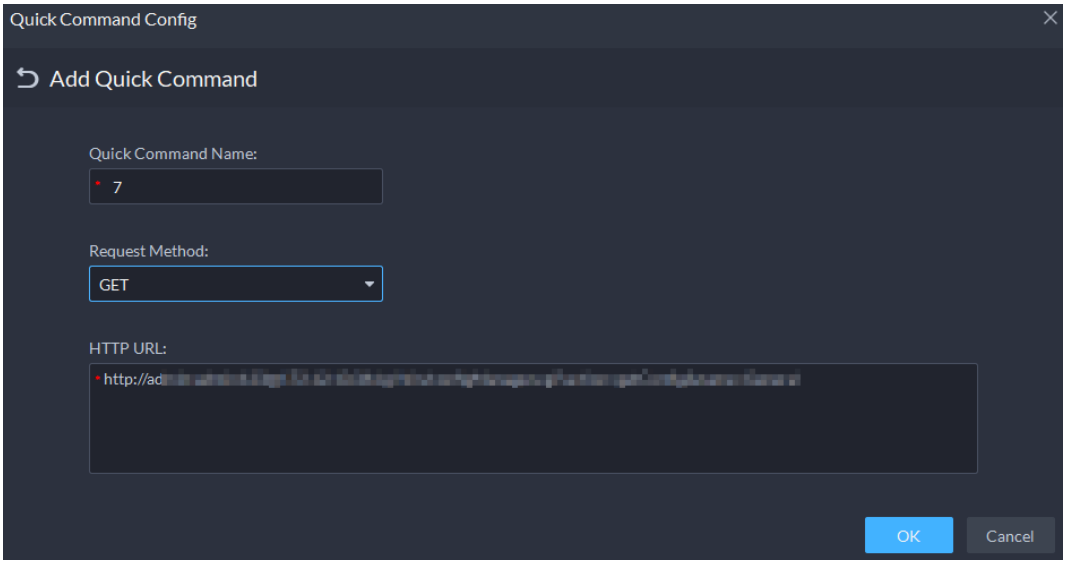
Figure 8-13 Quick commands



Step 2 Click .

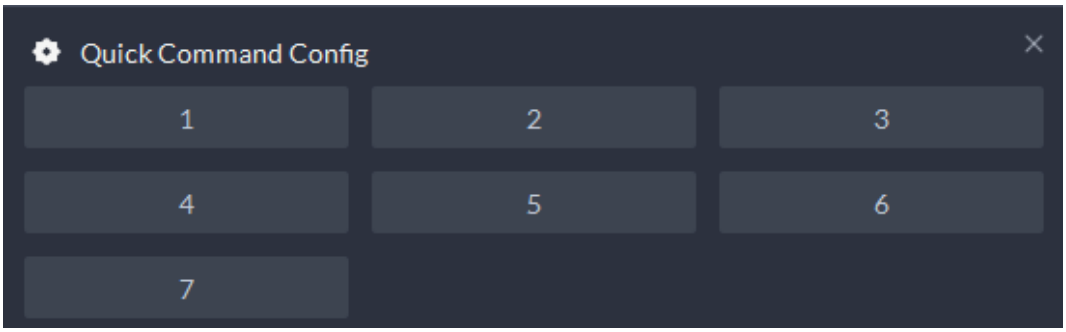
Step 3 Click **Add**.

Figure 8-14 Add a quick command



Step 4 Configure the parameters, and then click **OK**.

Figure 8-15 Execute a quick command



Step 5 Click the name of a quick command to execute it.

If successful, a prompt message will appear at the upper-right corner.

Appendix 1 Service Module Introduction

Appendix Table 1-1 Service module introduction

Service Name		Function Description
Access Service	DSS_NGINX	Reverses user requests to distributed system management services.
System Management Service	DSS_SMC	Manages services and provides access to various interfaces.
Device Discovery Service	DSS_HRS	Broadcasts platform information to discover devices.
Data Cache Service	DSS_REDIS	Platform temporary business data storage.
Database	MySQL	Stores platform business data.
Message Queue Service	DSS_MQ	Transfers messages between platforms.
Device Management Service	DSS_DMS	Registers encoders, receives alarms, transfers alarms and sends out the sync time command.
Media Transmission Service	DSS_MTS	Gets audio/video bit streams from front-end devices and then transfers the data to DSS, the client and decoders.
Storage Service	DSS_SS	Store, search and play back recordings.
Device Search Service	DSS_SOSO	Search for device information.
Video Matrix Service	DSS_VMS	Log in to the decoder and send tasks to the decoder to output on the TV wall.
Auto Register Service	DSS_ARS	Listens, logs in, or gets bit streams to send to MTS.
ProxyList control Proxy Service	DSS_PCPS	Logs in to ONVIF device, and then gets the stream and transfers the data to MTS.
Alarm Dispatch Service	DSS_ADS	Sends alarm information to different objects according to defined plans.
Access Control Service	DSS_ACDG	Manages access control and other related operations.
External LED Device Access Service	DSS_MCDLed	Manages LED access and other related operations.
External Alarm Controller Access Service	DSS_MCDAlarm	Manages alarm controller access and other related operations.
Power Environment Server	DSS_PES	Manages access of dynamic environment monitoring devices.
Video Intercom Switch Center	DSS_SC	Manages PC client and App client login as SIP client, and also forwards audio-talk streams.

Service Name		Function Description
Object Storage Service	DSS_OSS	Manages storage of face snapshots and intelligent alarm pictures.
Object Storage Service	DSS_SubOSS	Mainly manages storage evidence recordings and pictures.
Picture Transfer Service	DSS_PTS	Manages picture transmission.
Speed Measurement Service	DSS_EAS	Measures vehicle average speed and analyzes traffic data.
Media Gateway	DSS_MGW	Sends MTS address to decoders.
Configuration Service	DSS_CFGS	Manages disks, such as read-and-write operations.
Access Controller Access Service	DSS_MCDDOOR	Manages access controller access and related operations.

Appendix 2 Cybersecurity Recommendations

The necessary measures to ensure the basic cyber security of the platform:

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. **Customize the Answer to the Security Question**

   The security question setting should ensure the difference of answers, choose different questions and customize different answers (all questions are prohibited from being set to the same answer) to reduce the risk of security question being guessed or cracked.

Recommendation measures to enhance platform cyber security:

1. **Enable Account Binding IP/MAC**
   It is recommended to enable the account binding IP/MAC mechanism, and configure the IP/MAC of the terminal where the commonly used client is located as a whitelist to further improve access security.
2. **Change Passwords Regularly**
   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.
3. **Turn On Account Lock Mechanism**
   The account lock function is enabled by default at the factory, and it is recommended to keep it on to protect the security of your account. After the attacker has failed multiple password attempts, the corresponding account and source IP will be locked.
4. **Reasonable Allocation of Accounts and Permissions**
   According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.
5. **Close Non-essential Services and Restrict the Open Form of Essential Services**
   If not needed, it is recommended to turn off NetBIOS (port 137, 138, 139), SMB (port 445), remote desktop (port 3389) and other services under Windows, and Telnet (port 23) and SSH (port 22) under Linux. At the same time, close the database port to the outside or only open to a specific IP address, such as MySQL (port 3306), to reduce the risks faced by the platform.
6. **Patch the Operating System/Third Party Components**
   It is recommended to regularly detect security vulnerabilities in the operating system and third-party components, and apply official patches in time.
7. **Security Audit**
   - Check online users: It is recommended to check online users irregularly to identify whether there are illegal users logging in.
   - View the platform log: By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

8. **The Establishment of a Secure Network Environment**

   In order to better protect the security of the platform and reduce cyber security risks, it is recommended that:

   - Follow the principle of minimization, restrict the ports that the platform maps externally by firewalls or routers, and only map ports that are necessary for services.
   - Based on actual network requirements, separate networks: if there is no communication requirement between the two subnets, it is recommended to use VLAN, gatekeeper, etc. to divide the network to achieve the effect of network isolation.