General Surveillance Management Center

User's Manual

Foreword

General

This user's manual introduces the functions and operations of the general surveillance management center (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.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

⚠

- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Avoid heavy stress, violent vibration, and immersion during transportation.
- Transport the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the transporting temperature and humidity of the device.

Storage Requirements

⚠

- Store the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the storing temperature and humidity of the device.
- Avoid heavy stress, violent vibration, and immersion during storage.

Installation Requirements

⚠ DANGER

- Make sure that the power is off when you connect the cables, install or disassemble the device.
- For devices with earthing systems, make sure they are grounded to avoid being damaged by static electricity or induced voltage, and prevent electrocution from occurring.
- All installation and operations must conform to local electrical safety regulations.
- Use accessories suggested by the manufacturer, and installed by professionals.
- Do not block the ventilator of the device, and install the device in a well-ventilated place.
- Do not expose the device to heat sources or direct sunlight, such as radiator, heater, stove or other heating equipment, which is to avoid the risk of fire.
- Do not place the device in explosive, humid, dusty, extremely hot or cold sites with corrosive gas, strong electromagnetic radiation or unstable illumination.
- Avoid heavy stress, violent vibration, and immersion during installation.

⚠ WARNING

Safe and stable power supply is a prerequisite for proper operation of the device.

- Make sure that the ambient voltage is stable and meet the power supply requirements of the device.
- Prevent the power cord from being trampled or pressed, especially the plug, power socket and the junction from the device.
- For devices that can be powered by multiple supplies, do not connect them to two or more kinds of power supplies; otherwise, the device might be damaged.

● Refer to the specific user's manual for the power requirements of single device.

⚠

It is recommended to use the device with a lightning protector for better lightning-proof effect.

Operation Requirements

⚠

A suitable operating environment is the foundation for the device to work properly. Confirm whether the following conditions have been met before use.

● Use the device under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the operating temperature and humidity of the device.

● Use the device on a stable base.

● Do not let any liquid flow into the device to avoid damage to internal components. When liquid flows into the device, immediately disconnect the power supply, unplug all cables connected to it, and contact after-sales service.

● Do not plug or unplug RS-232, RS-485 and other ports with the power on, otherwise, the ports will be easily damaged.

● Back up data in time during deployment and use, in an effort to avoid data loss caused by abnormal operation. The company is not liable for data security.

● The company is not responsible for damages to the device or other product problems caused by excessive use or other improper use.

Maintenance Requirements.

⚠ WARNING

● Contact professionals for regular inspection and maintenance of the device. Do not disassemble or dismantle the device without a professional present.

● Use accessories suggested by the manufacturer, and maintain the device by professionals.

Table of Contents

1 Overview

1.1 Introduction

DSS General Surveillance Management Center is a high-performance security management platform based on Linux OS and pre-installed DSS software. It provides higher performance in the low-end and mid-end market, offering a reasonably low price for a highly efficient and carefully designed system.

1.2 Highlights

- Easy to Use

  All-in-One, plug & play.
- Cost-effective
  - ◇ One-time payment for hardware and whole software capacity.
  - ◇ Lower price per channel.
- Stable and Reliable
  - ◇ Linux OS based design with high efficiency and reliability.
  - ◇ Less maintenance investment.

2 Installation and Deployment

The system supports standalone deployment, and LAN to WAN mapping.

Standalone Deployment

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

Figure 2-1 Standalone deployment
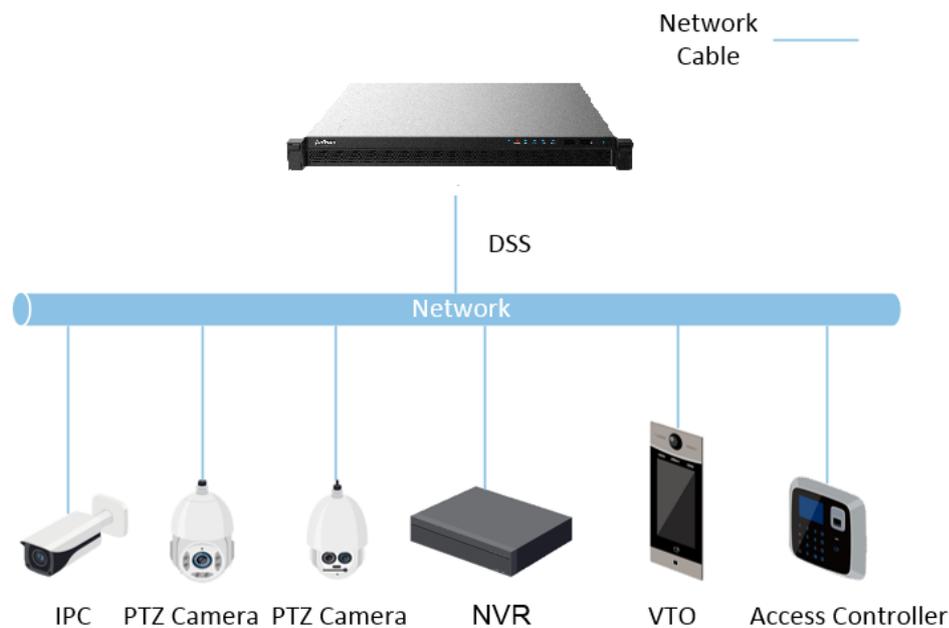
LAN to WAN Mapping

Perform port mapping when:
- The server of the platform and devices are on a local area network, and the DSS client in on the internet. To make sure that the DSS client can access the platform server, you need to map the platform IP to the Internet.
- The platform is on a local area network, and the devices are on the Internet. If you want to add devices to the platform through automatic registration, you need to map the IP address and ports of the platform to the Internet. For devices on the Internet, the platform can add them by their IP addresses and ports.

⚠

The configuration system does not differentiate service LAN ports and WAN ports. Make sure that the WAN ports and LAN ports are the same.

2.1 Configuring Single-server Deployment

Whichever deployment mode you use, you need to configure network settings and server working mode for each server before deployment.

Step 1   Log in to the Config system.

1) In the address bar of browser, enter DSS IP address/config, and then press the Enter key.

2) Enter username and password, and then click **Login**.
The default username is admin, password 123456.

Figure 2-2 Login

    For the first-time login, follow the onscreen prompts to change the password and set security questions.

Step 2   Configure network.

1) Select **Quick Guide** > **Network Card Config**, or select **Network Config** > **NIC Config**.

Figure 2-3 Network card config

2) Configure parameters of network card.

Table 2-1 Network card parameter description

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

Parameter	Description
IPv4	After selecting a network card, you can set its IP address, subnet mask, default gateway and DNS server address.
IPv6	Enable IPv6 and configure the parameters to connect the platform to an IPv6 network, you can add devices with IPv6 address to the platform.
Default Network Card	Select the default NIC. This NIC will be used as the default NIC to forward data package between non-consecutive network segments such as WAN or public network.

3) Click **Apply and Restart**.

Step 3   Set server time zone and time.

📖

For distributed deployment, N+M deployment or hot standby deployment, you need to set NTP time synchronization. For details, see "8.2.3 Time Synchronization".

1) Select **Basic Config** > **Time Config**.

Figure 2-4 Time config

2) Set time parameters.

Table 2-2 Parameters description

Parameter	Description
Time Mode	● GMT: Greenwich Mean Time. ● UTC: Coordinated Universal Time.
Time Zone	Select time zone of the server.
Date/Time	Click the box to select date and time.
Sync PC	Click **Sync PC** to sync PC time with system time.

3) Click **Application**.

The platform will restart.

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 or Domain Name

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

Step 1   Log in to the Config system.

Step 2   Select **Network Config** > **Network Mode**.

Figure 2-5 Network mode

Step 3   Enter a fixed WAN IP address or a domain name in the **Mapping IP | Domain** box, and then click **OK**.

If you want to use a domain name, you need to make corresponding configurations on the domain name server.

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

3 Configuring Basic Settings

Log in to the Config system (configuration system) to quickly configure network parameters, basic parameters, safety parameters , as well as system update and self-check.

3.1 Login and Password Initialization

Step 1 Go to https://*DSS platform IP address*/config in the browser.
The password resetting interface is displayed.

Figure 3-1 Reset password
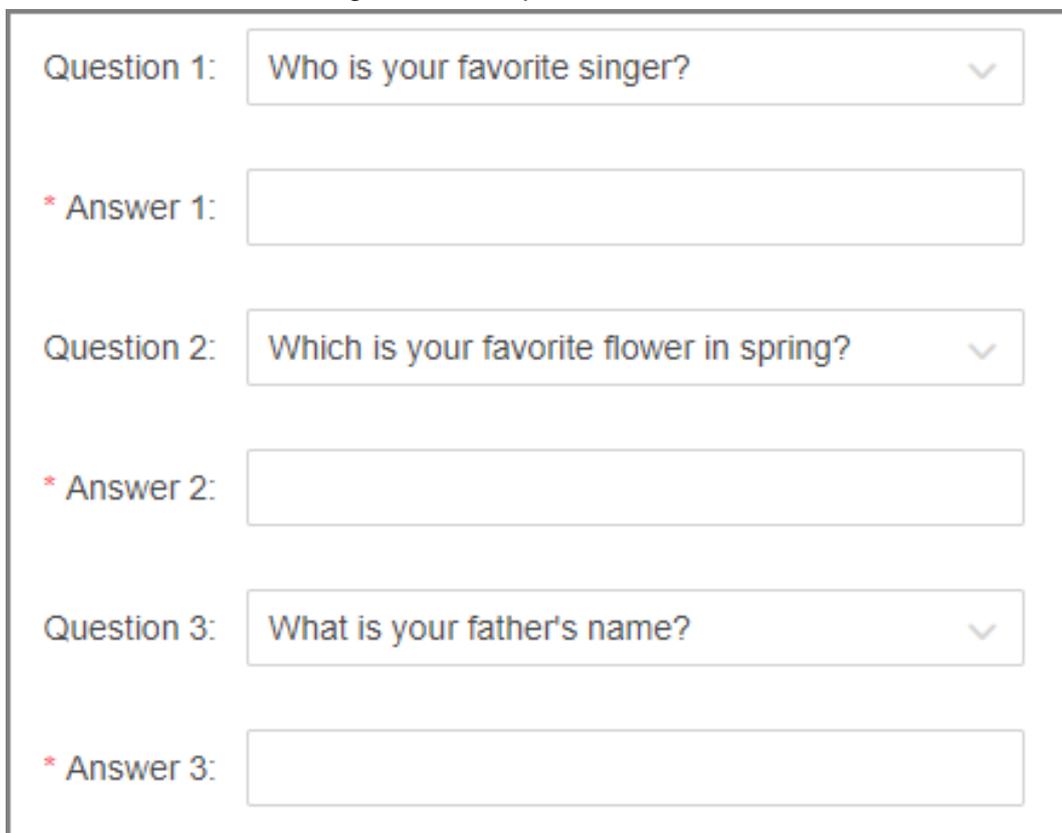
Step 2 Enter a password and confirm it, and then click **Next**.
Step 3 Set security questions, and then click **Next**.
Step 4 Configure the time and time zone, and then click **Finish**.
Service is restarted and you need to log in to the system again.

3.2 Quick Guide

On the **Quick Guide** interface, you can quickly configure network settings, and LAN to WAN mapping.

Step 1 Log in to the Config system, and then select **Quick Guide** > **Network Card Config**.

Figure 3-2 Network card configuration

Step 2 Configure the parameters.

Table 3-1 Network card parameter description

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

Parameter	Description
IPv4	After selecting a network card, you can set its IP address, subnet mask, default gateway and DNS server address.
IPv6	Enable IPv6 and configure the parameters to connect the platform to an IPv6 network, you can add devices with IPv6 address to the platform.
Default Network Card	Select the default NIC. This NIC will be used as the default NIC to forward data package between non-consecutive network segments such as WAN or public network.

Step 3   Click **Apply and Restart**.

Step 4   Log in to the Config system, and then select **Quick Guide** > **Network Mode**.

Figure 3-3 Network mode
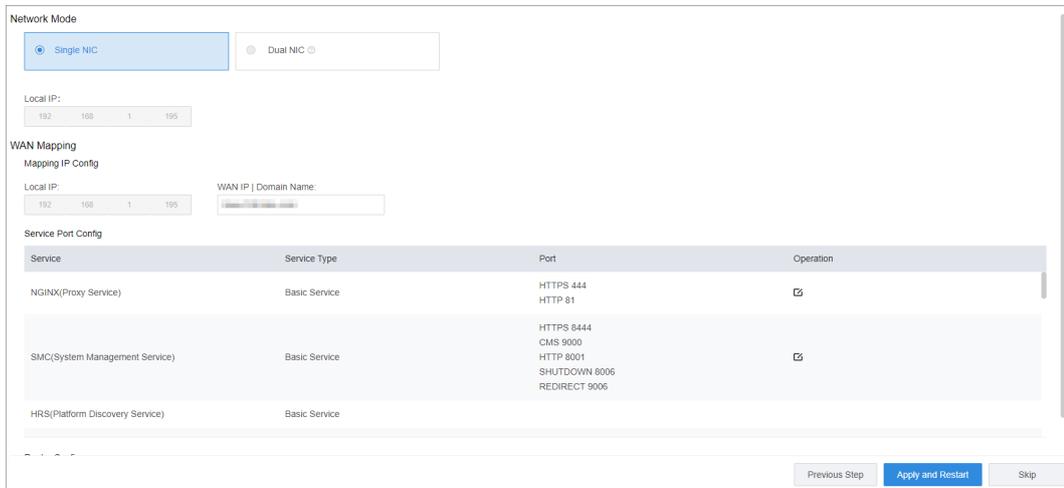
Step 5   Configure the parameters.

Table 3-2 Network mode parameter description

Mode	Parameter	Description
Network Mode	Single NIC	The platform will only use the default network card, and you can only access the platform through the IP address of this network card.
	Dual NIC	If the platform has more than one network cards, you can configure an additional one so that the platform can access more devices on another network segment. 📖 To use Dual NIC, you must set the network mode to multi-IP address mode, and then configure the parameters of the network cards.
WAN Mapping	WAN IP | Domain Name	Map the LAN IP to a WAN IP, so that you can access the platform through the WAN IP. If the WAN IP changes frequently, you can map it to a domain name, and use it to access the platform.
	Service Port Config	Displays all services used by the platform and their ports. Click 📝 to change their port numbers as needed. For introduction to each service, see "Appendix 1 Service Module Introduction".

Step 6   Click **Apply and Restart**.

3.3 Self-check

Click **System Status** and then select **Service Status**, **CPU Status**, **Network Status**, or **Local Disk Status**, or click [icons] to check the status of service, CPU, network and disk.

3.4 Network Config

3.4.1 NIC Config

Configure the parameters so that the platform can connect to the network.

Step 1   Select **Network Config** > **NIC Config**.

Figure 3-4 Network card configuration
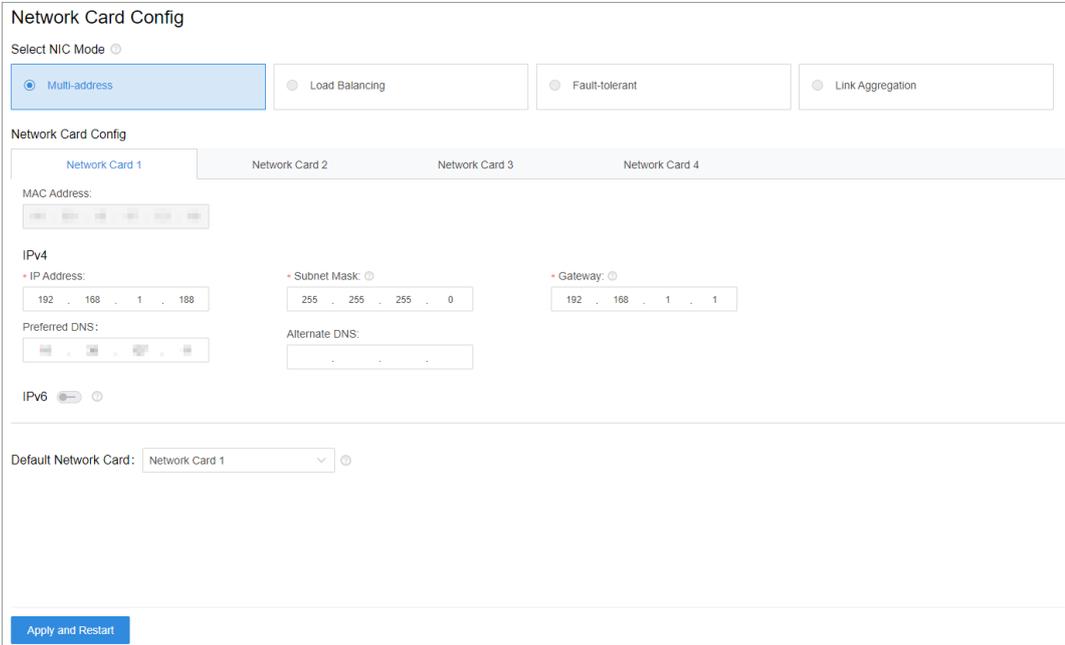
Step 2   Configure the parameters, and then click **Apply and Restart**.

Table 3-3 Network card parameter description

Parameter	Description
Select NIC Mode	● Multi-address Multiple network card (hereinafter referred to as NIC) mode. You can configure different network parameters for different NIC to access to multiple network segments and achieve high network reliability. For example, ISCSI storage expansion solution. When setting ISCSI storage expansion, NIC 1 can be used for communication, NIC 2 is reserved and NIC 3 and NIC 4 can be used for ISCSI storage. ● Load Balancing Multiple NICs share one IP and work at the same time to share the network load, providing greater network capacity than the single NIC mode. When one of them fails, the network load will be re-distributed among the rest NICs to ensure network stability. ● Fault-tolerant Multiple NICs share one IP. Normally, one of them works. When the working NIC fails, another one will automatically take over the job to ensure network stability. ● Link Aggregation Bind NICs so that all the bound NICs work at the same time and share network load. For example, bind two NICs and set multi-address for the other two NICs. Then the server has three IPs. The bandwidth of the two bound NICs is 2K and the other two are 2K respectively. This is applicable to stream forwarding, not storage.
Add Network Card	When the NIC mode is fault tolerance, load balance or link aggregation, you need to add network card. Select NIC to bind. You can bind 2 NICs as needed.
Network Card Config	After NIC is selected or added, its information will be displayed.
MAC Address	Displays the MAC address of the server.
IPv4	After selecting a network card, you can set its IP address, subnet mask, default gateway and DNS server address.
IPv6	Enable IPv6 and configure the parameters to connect the platform to an IPv6 network, you can add devices with IPv6 address to the platform.
Default Network Card	Select the default NIC. This NIC will be used as the default NIC to forward data package between non-consecutive network segments such as WAN or public network.

3.4.2 Network Mode

You can set the platform to work in mapping mode or multi-IP mode. In mapping mode, you can configure LAN IP to WAN IP mapping, or LAN IP to domain name mapping, so that you can use the WAN IP or domain name to visit the platform deployed in a local network. In multi-IP mode, you can

assign an IP address to the platform and use it to visit and operate the platform.

Step 1   Select **Network Config** > **Network Mode**.

Figure 3-5 Network mode
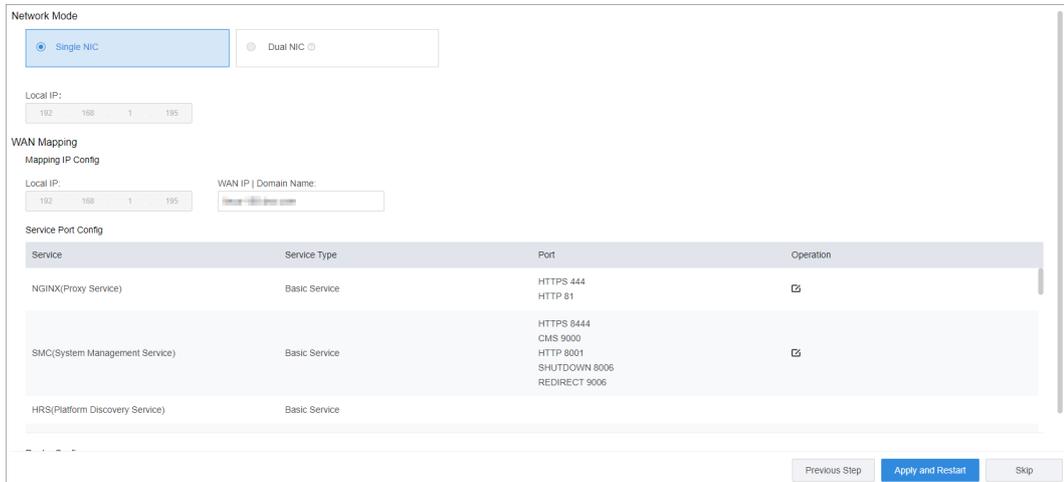
Step 2   Configure the parameters.

Table 3-4 Network mode parameter description

Mode	Parameter	Description
Network Mode	Single NIC	The platform will only use the default network card, and you can only access the platform through the IP address of this network card.
	Dual NIC	If the platform has more than one network cards, you can configure an additional one so that the platform can access more devices on another network segment. 📖 To use Dual NIC, you must set the network mode to multi-IP address mode, and then configure the parameters of the network cards.
WAN Mapping	WAN IP | Domain Name	Map the LAN IP to a WAN IP, so that you can access the platform through the WAN IP. If the WAN IP changes frequently, you can map it to a domain name, and use it to access the platform.
	Service Port Config	Displays all services used by the platform and their ports. Click ✏ to change their port numbers as needed. For introduction to each service, see "Appendix 1 Service Module Introduction".

Step 3   Click **Apply and Restart**.

3.4.3 Connection Detection

Check whether the IP address or URL is connected normally to validate the network interconnection between servers or between the devices and the server.

Step 1   Select **Network Config** > **Connection Detection**.

Figure 3-6 Connection detection
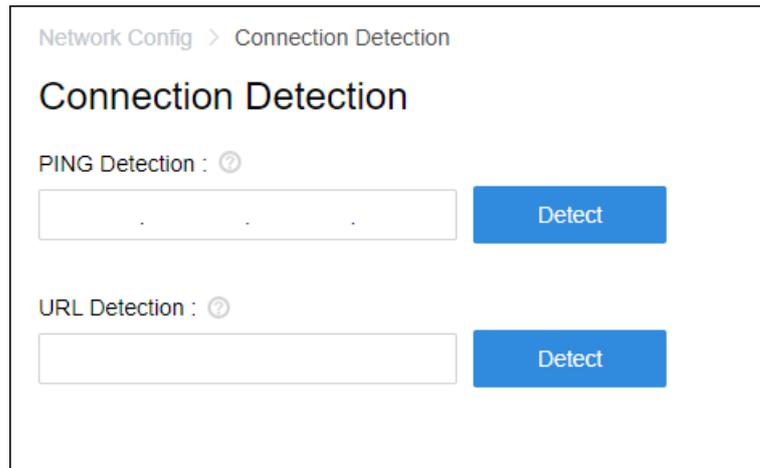
Step 2   Enter IP address or URL, and then click **Detect**.

3.4.4 Route Setup

Add static route to establish access between servers in different network segments.

Step 1   Select **Network Config** > **Routing Settings**.

Figure 3-7 Route setup

Step 2   Click **Manually Add**.

Figure 3-8 Add statistic router
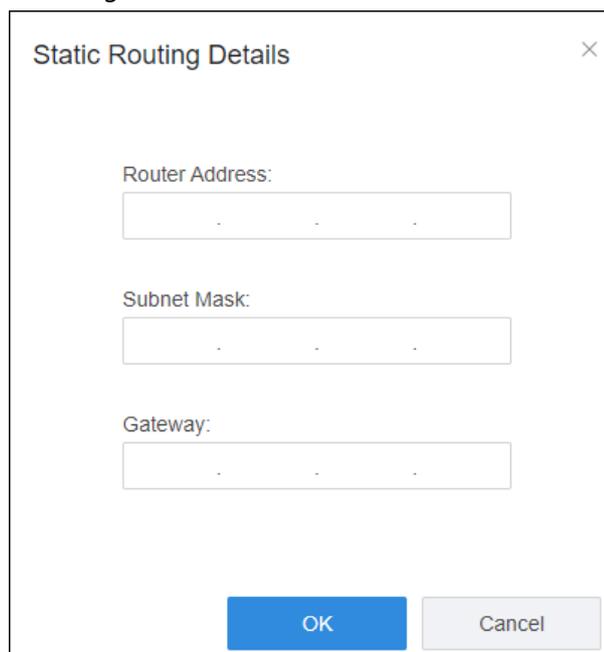
Step 3   Enter router IP address, subnet mask and default gateway.

Table 3-5 Parameter description

Parameter	Description
Router Address	The IP address or the network segment of the host you want to access.
Subnet Mask	The subnet mask of the network you want to access.
Gateway	The IP address of the default gateway or the next hop.

Step 4   Click **OK**.

3.5 Security Setup

3.5.1 SSH Connection Setup

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

Step 1   Select **Security Config** > **SSH Connection Service**.

Figure 3-9 SSH connection
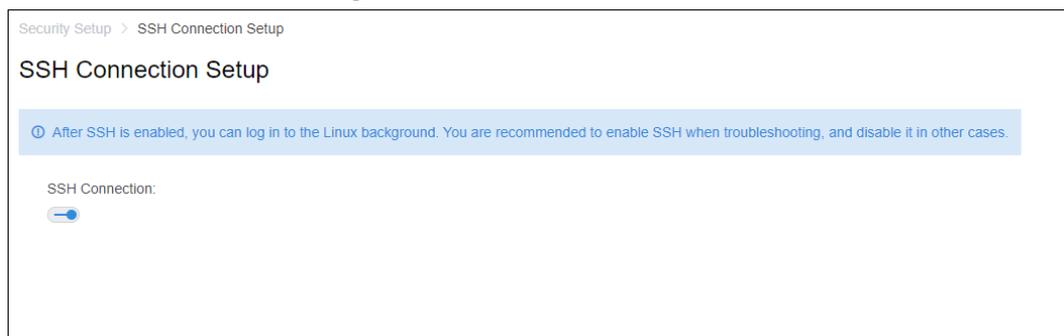
Step 2   Enable **SSH Connection**.

Disable **SSH Connection** after debugging.

3.5.2 Enabling TLS

By default, the platform only supports TLS1.2. You must enable TLS1.2 according to the on-screen instructions to normally access the Config system. If you must use TLS1.0 or TLS1.1, you must enable TLS self-adaptive mode on the platform. Please be advised that TLS1.0 and TLS1.1 poses security risks. We recommend you disable TLS self-adaptive mode and enable TLS1.2 to avoid unnecessary risks to your system.

Step 1   Select **Security Config** > **TLS Config**.

Figure 3-10 TLS self-adaptive mode
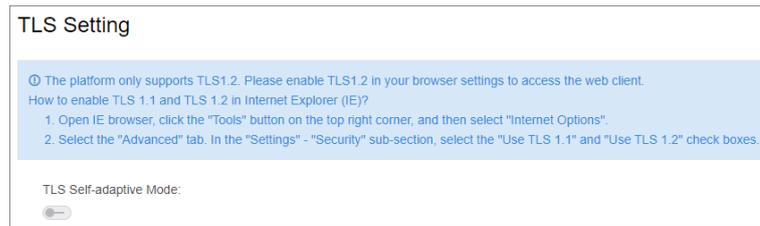
Step 2   Click ⬤▬, and then click **OK**.

The platform will restart.

Step 3   Open Internet Explorer, click ⚙ on the upper-right corner, and then select **Internet Options** > **Advanced**.

Step 4   In the **Security** section, select **TLS1.0** or **TLS1.1**, click **Apply**, and then click **OK**.

3.6 System Maintenance

3.6.1 Basic Maintenance

Restart, shut down and reset the server. You can also reset password.

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

Figure 3-11 Maintenance
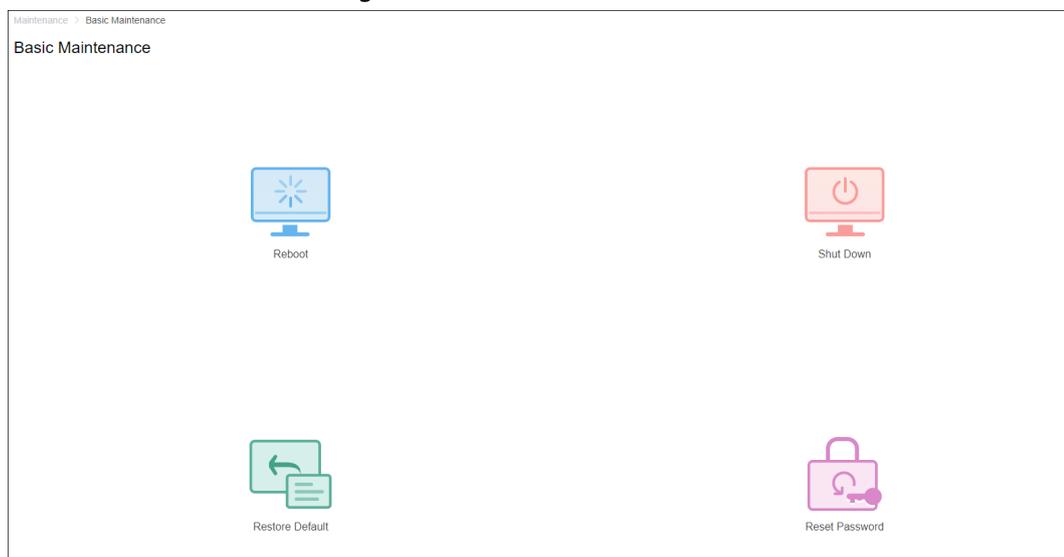
Step 2   Click the icons for various functions.

- **Reboot**: Restart the server.
- **Shut Down**: Shut down the server.
- **Restore Default**: Restore the server to default settings.
- **Reset Password**: Verify your current password to reset the password. Wait for the server to restart, and then log in to the config system again to set a new password.

3.6.2 Log

You can download CMS, DMS, MTS, SS and other service logs from the system.

Step 1　　Select **System Maintenance** > **Service Log**.

Figure 3-12 Log

Maintenance > Server Log

Server Log

* Log Time:

| ▦ 2021-06-29 | Download |
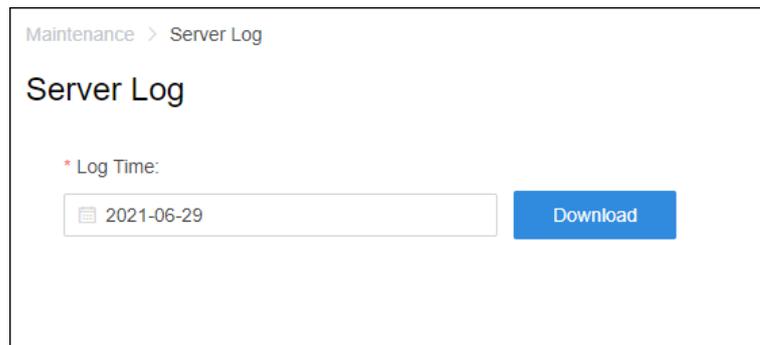
Step 2　　Select date, and then click **Download** to download log file.

3.6.3 Updating System

We recommend you update the system regularly to enjoy enhanced performance and functions.
Before updating your system, contact technical support to get the software package.

Step 1　　Select **System Maintenance** > **System Update**.

Step 2　　Click 📁 , and then select the update package.

Figure 3-13 Update

Maintenance > System Update

System Update

ⓘ Current Program Version: V8.000.0000004.0.R.20211129.1638197138
　　Please make sure the target version is newer than the current version. Otherwise,
update might fail.

Update through Web

Update Package Path

| 📁 |
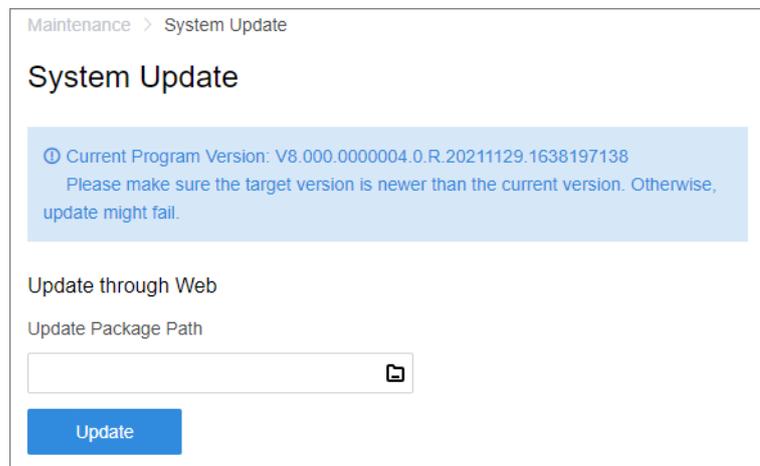
Update

Step 3　　Click **Update**.

3.7 Basic Config

3.7.1 Time Setup

Set time zone and time where the server is located.

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

Figure 3-14 Time configuration

Step 2   Configure time parameter.

Table 3-6 Parameters description

Parameter	Description
Time Mode	- GMT: Greenwich Mean Time. - UTC: Coordinated Universal Time.
Time Zone	Select time zone of the server.
Date/Time	Click the box to select date and time.
Sync PC	Click **Sync PC** to sync PC time with system time.

Step 3   Click **Application**.

3.7.2 Managing Account

You can change the login password of admin user.

All services will be restarted after changing the password. Check if the services have been restarted successfully during use.

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

Figure 3-15 Manage account

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

Step 3   Click **Apply and Restart**.

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

4 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.

4.1 Preparations

4.1.1 Installing and Logging into DSS Client

Install the DSS client before licensing it.

4.1.1.1 Installing DSS Client

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

4.1.1.1.1 DSS Client Requirements

To install and use the DSS Client, we recommend you prepare a computer that meets the following requirements.
● CPU: Intel Core i7, 64 bits 4 Core Processor
● Memory: 16 GB
● Graphics card: NVIDIA® GeForce® GTX 1060 3 GB
● Network card: 1000 Mbps
● Hard drive capacity: 200 GB for the DSS client

4.1.1.1.2 Downloading and Installing DSS Client

Step 1   Go to https://*IP address of the platform* in the browser
Step 2   Click **PC**, and then **Download**.
            If you save the program, go to Step3.
            If you run the program, go to Step4.

Figure 4-1 Download DSS Client
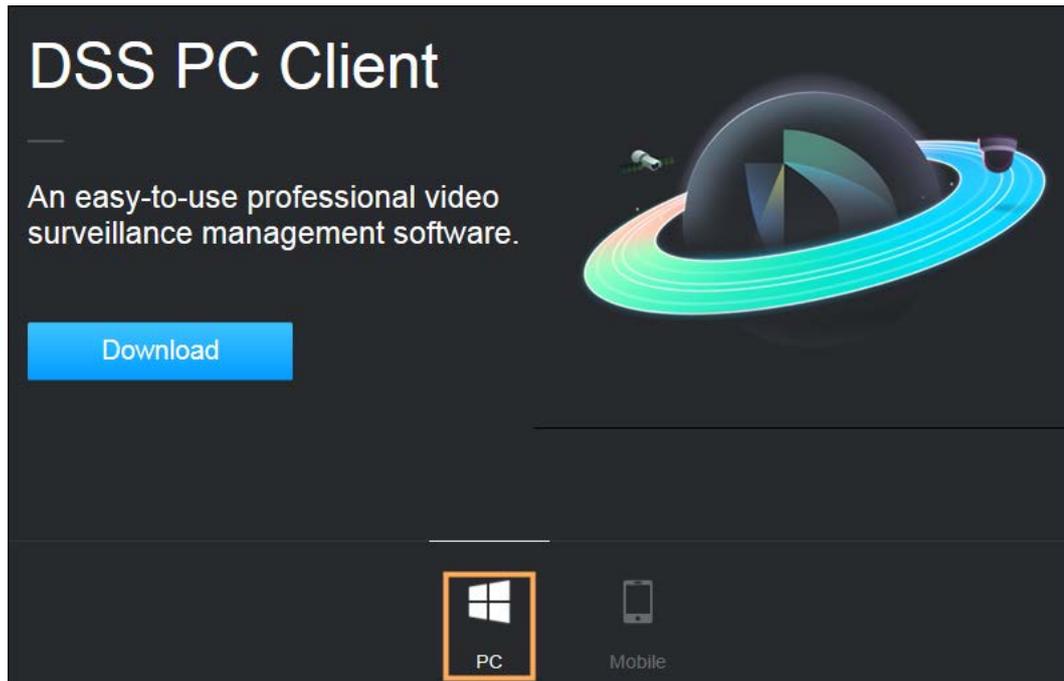
Step 3   Double-click the DSS Client program.

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.

4.1.1.2 Logging in to DSS Client

Step 1   Double-click [icon] on the desktop.

Step 2   Select a language.

Step 3   Enter the IP address and port number of the platform.

On the drop-down list, platforms that are in the same network as your computer will be shown.

📖

If you want to log in to the platform using its domain name, you must link its IP address to a domain name first. See "2.2.2 Mapping IP or Domain Name".

Figure 4-2 Automatically discovered platform
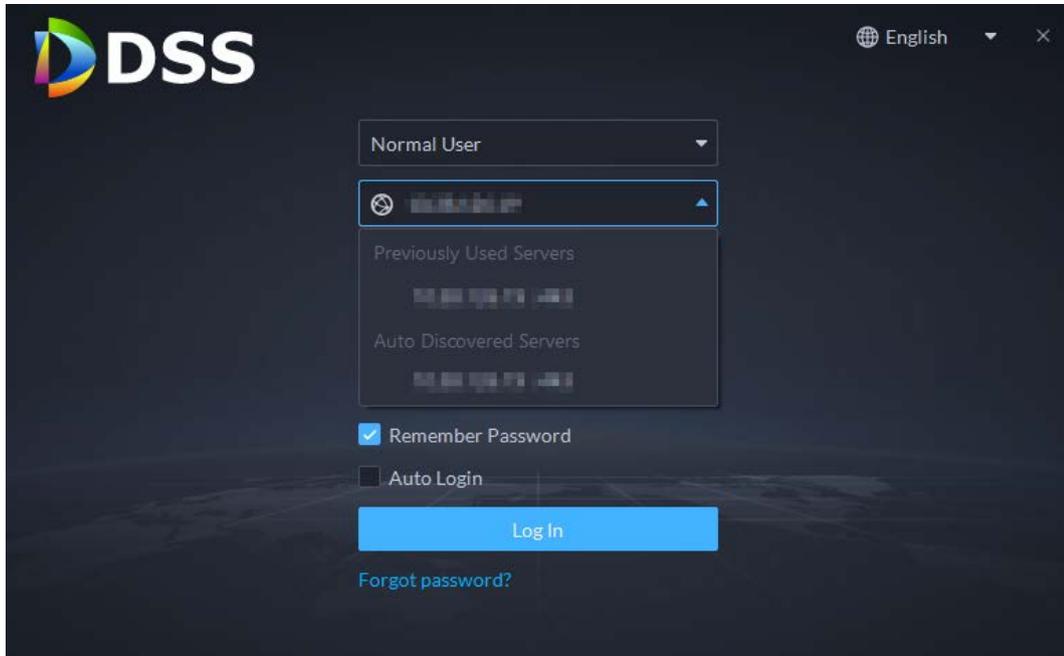
Step 4   Initialize the platform.

For first-time login, you have to initialize the platform by setting a login password for the default user **system**, and security questions for resetting the password.

If you are not logging in for the first time, enter the IP address, port number of the platform, username, and password, and then click **Login**.

1) Enter **system** in the **Username** input area, enter any character in the **Password** input area, and then click **Login**.

2) Set up a password for the system user.

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 ' " ; : &).

3) Select your questions and enter their answers, and then click **OK**.

The client will automatically log in to the platform by using the password you just set.

4.1.2 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 4-3 Download App by scanning QR code
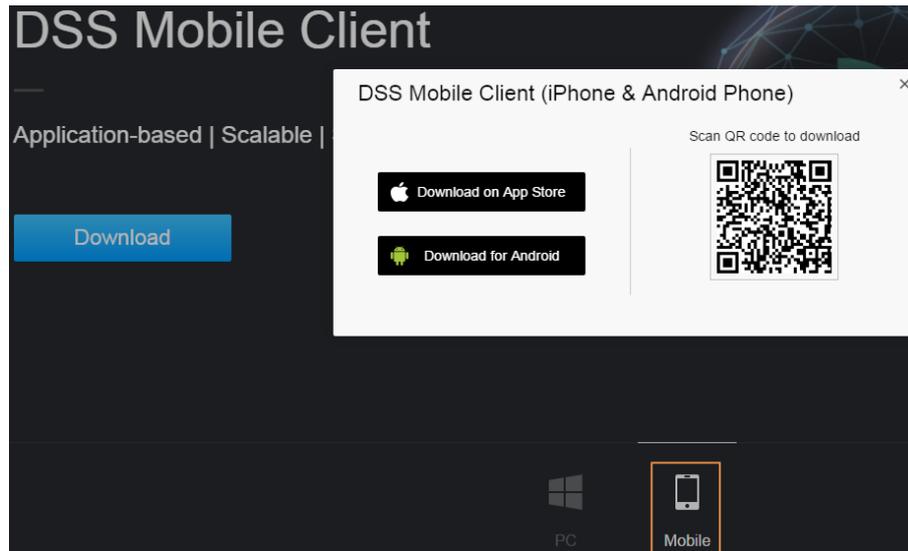
4.2 Managing Resources

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

4.2.1 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** page, click [icon], and then in the **Basic Config** section, select **Device**.

Step 2   Click [icon]

Step 3   Add an organization.

1) Select a parent organization.

2) Click [icon].

Figure 4-4 Add an organization
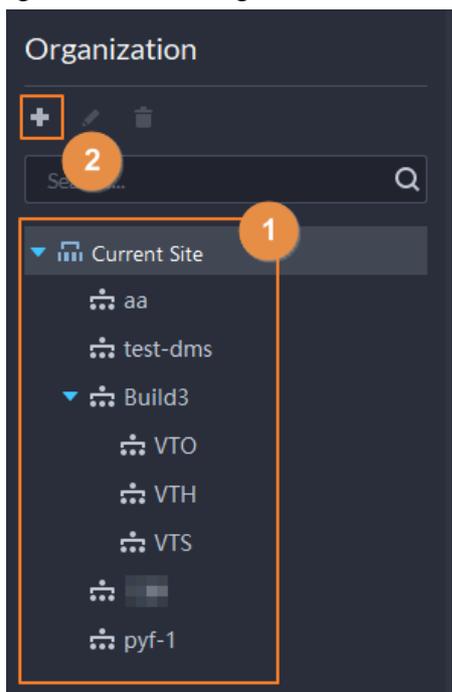
3) Enter the name of the organization, and then click **OK**.

Figure 4-5 Add an organization

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

Related Operations

- Change 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**.

- Change the organization of devices

    Select one or more devices, and then click **Move To** to move them to another organization.

4.2.2 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.

4.2.2.1 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** page, click ![icon], and then in the **Basic Config** section, select **Device**.

Step 2   Click ![icon].

Step 3   Click ![icon].

The icon changes to ![icon] when devices are searched.

📖

- When using the platform for the first time, the platform automatically searches for devices on 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 4-6 Search for devices
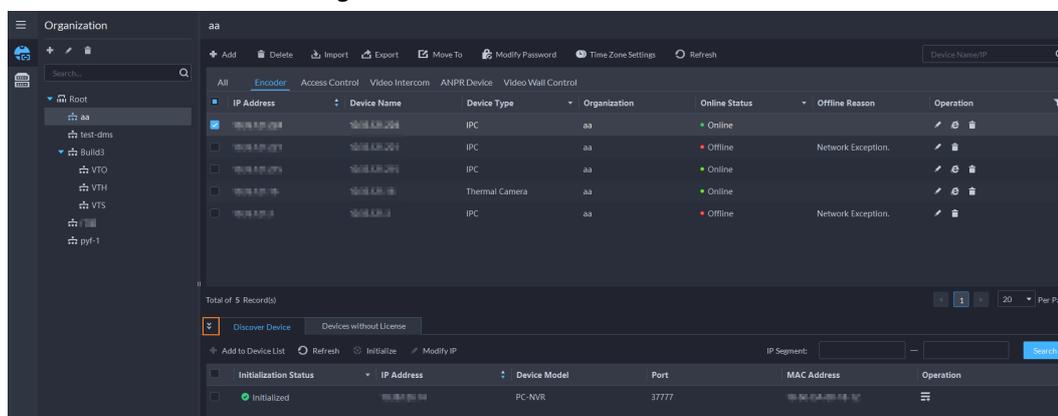
Step 4   Specify **IP Segment**, and then click **Search**.

Figure 4-7 IP segment search
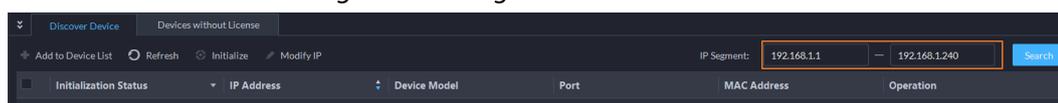
4.2.2.2 Initializing Devices

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

Step 1   Search for devices. For details, see "4.2.2.1 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. The information of these devices will be the same after initialization, such as password and email address.
- Click ▼ next to **Initialization Status** to quickly sort out devices in certain status.

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.

4.2.2.3 Changing Device IP Address

You can change IP addresses of the devices that have not been added to the platform. For the devices that have been added to the platform, and their IP addresses have been changed, you can edit their IP addresses directly on the platform so that they can connect to the platform normally.

Step 1   Search for devices. For details, see "4.2.2.1 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 4-8 Change IP address
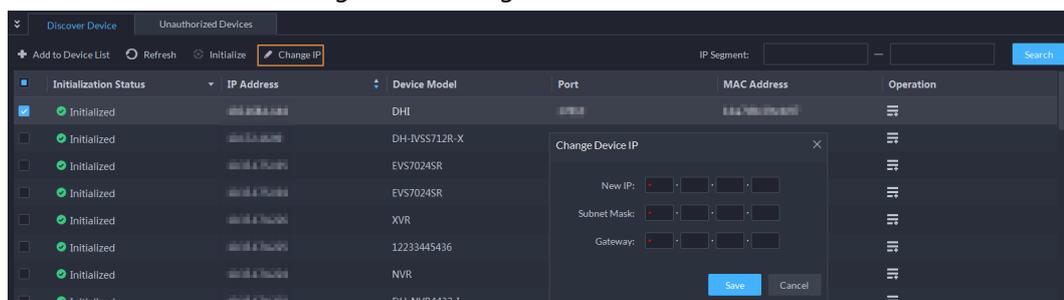
Step 3   Enter **New IP**, **Subnet Mask** and **Gateway**, and then click **Save**.

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

4.2.2.4 Adding Devices

You can add different types of devices, such as encoder, decoder, ANPR device, access control, and video intercom. This section takes adding an encoder as an example. The configuration pages shown here might be different from the ones you see for other types of devices.

📖

When you add devices by using automatic registration, IP segment, or importing, some devices will fail to be added if they exceed the number of devices or channels allowed to be added to the platform. These devices will be displayed in **Devices without License**.

4.2.2.4.1 Adding Devices One by One

There are multiple ways you can add devices to the platform, including using domain names, serial numbers, IP addresses, IP segments, and automatic registration.

Step 1   Log in to the DSS Client. On the **Home** page, 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. If you want to add devices to the platform through IPv6 addresses, you must first configure an IPv6 address for the platform. For details, see "3.4.1 NIC Config".

- **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.

- **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.

- **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 change the auto register port number, log in to the config system, select **Network Config** > **Network Mode**, and then change the port number of DSS_ARS service.

- **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.

📖

The parameters vary with the selected protocols.

Figure 4-9 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 manager of a device, click 🅔 .

4.2.2.4.2 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 "4.2.2.1 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 4-10 Add in batches

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

4.2.2.4.3 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 4-11 Download template
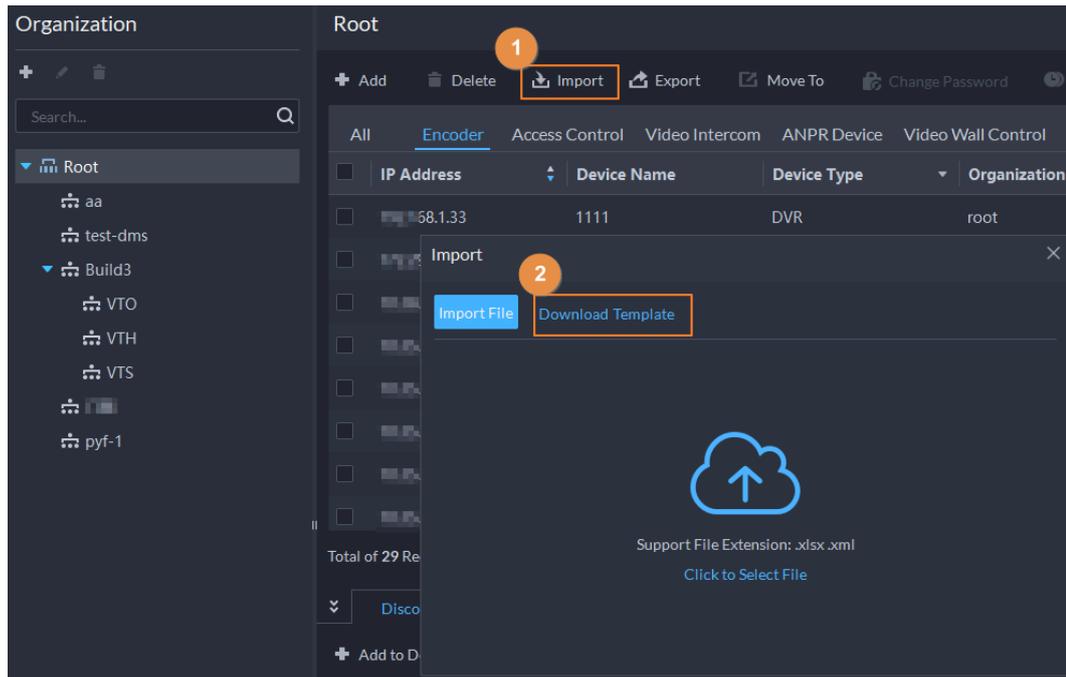
Procedure

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

Step 2   Click .

Step 3   Click **Import**.

Figure 4-12 Import devices

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

Step 5   Click **OK**.

4.2.2.5 Editing Devices

Modify device information and organization.

4.2.2.5.1 Modifying Device Information

Step 1   Log in to the DSS Client. On the **Home** page, 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 4-13 Basic information

Step 4   Click **Video Channel**, and then configure the channel information, such as the channel name and channel features.

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 device do not 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 edit 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**.

4.2.2.5.2 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** page, 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 4-14 Move a device
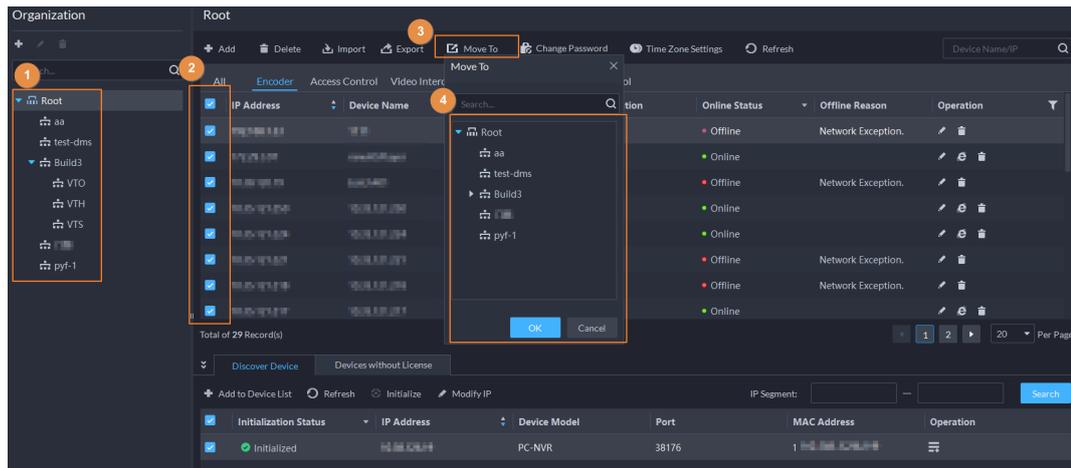
4.2.2.5.3 Changing Device Password

You can change device usernames and passwords in batches.

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

Step 2　Click .

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

⊙⚷

You can select multiple devices and change their passwords at the same time.

Figure 4-15 Change device password
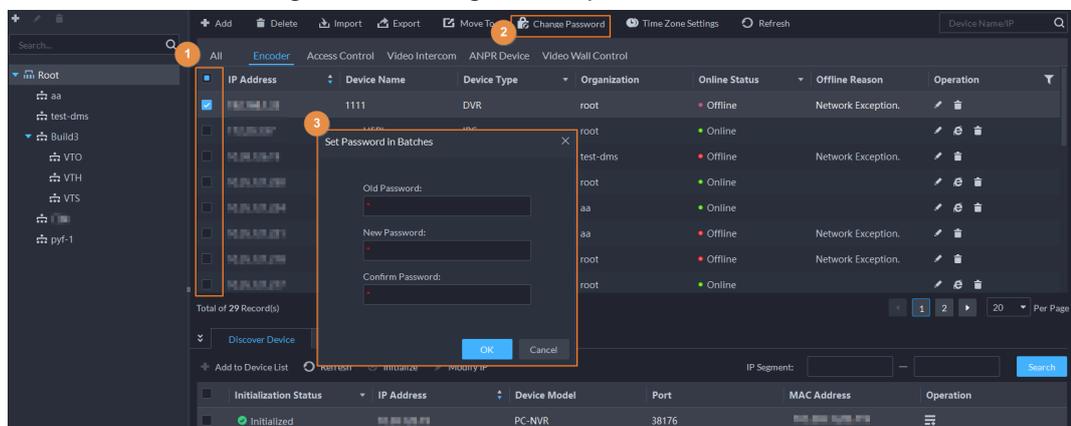
Step 4　Enter the old and new passwords, and then click **OK**.

4.2.2.6 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** page, 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 4-16 Modify device time zone
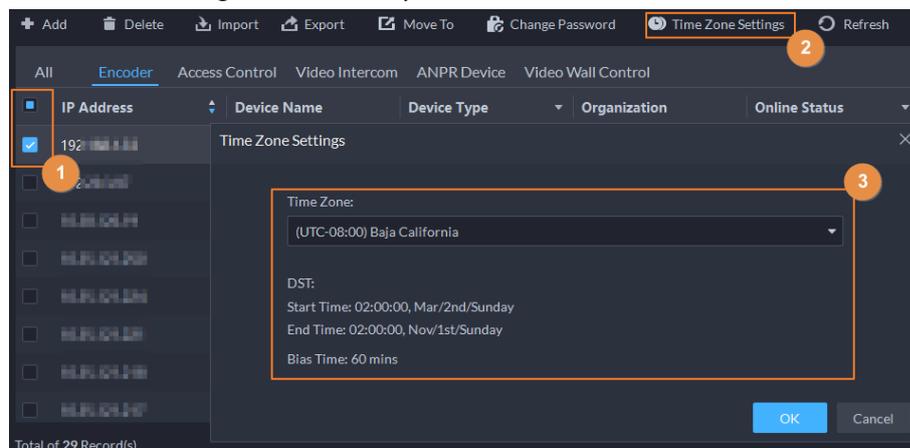
Step 4   Select a time zone.

Step 5   Click **OK**.

4.2.2.7 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** page, click 🔧, and then in the **Basic Config** section, select **Device**.

Step 2   Click 🖥️.

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

Figure 4-17 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**.

4.2.3 Binding Resources

The platform supports binding resources for linked actions. You can link 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** page, click 🔧, and then in the **Basic Config** section, select **Device**.

Step 2 Click ⌨.

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

Figure 4-18 Bind channel
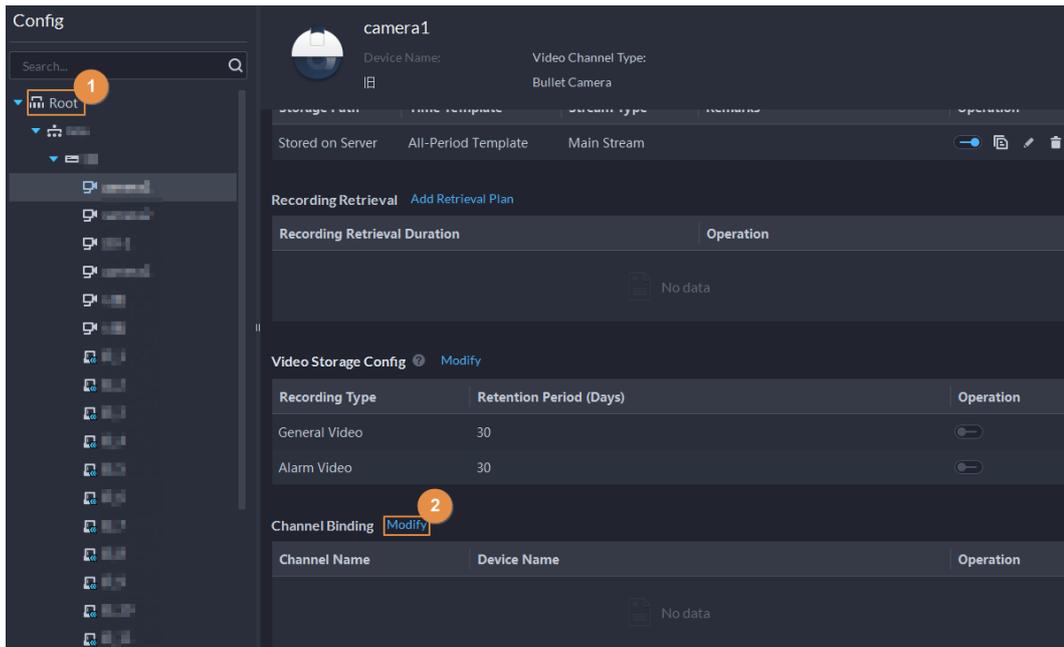
Step 4   Select a channel, and then click **OK**.

📖

Multiple channels can be selected.

Figure 4-19 Select the channels you want to bind to the camera
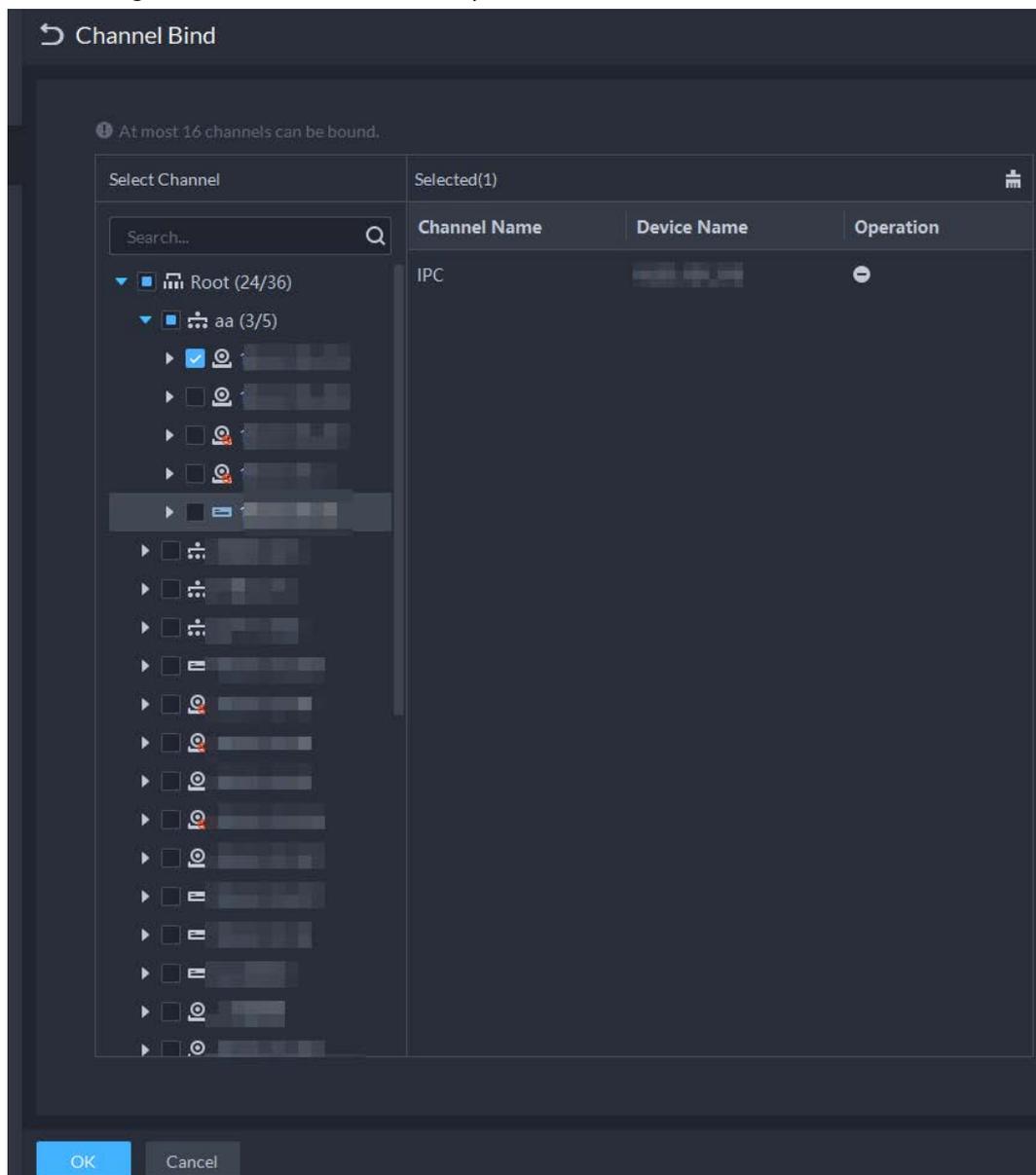
Step 5   Click **OK**.

4.2.4 Adding Recording Plan

Configure recording plans for video channels so that they can record videos accordingly.
You can configure 2 types of recording plans for a channel. One is general recording plan, and a device will continuously record videos during the defined period. The other is motion detection recording plan, and a device will only record videos when motion is detected.

4.2.4.1 Adding Recording Plan One by One

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

motion detection videos within the defined period.

Procedure

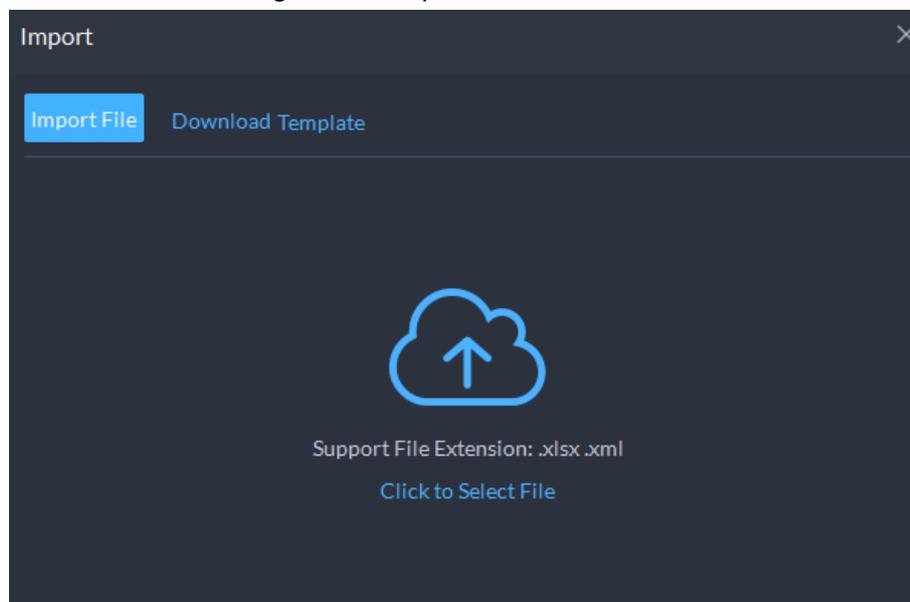Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **Basic Config** section, select **Device**.

Step 2   Click ![icon].

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 4-20 Add a center recording plan (1)
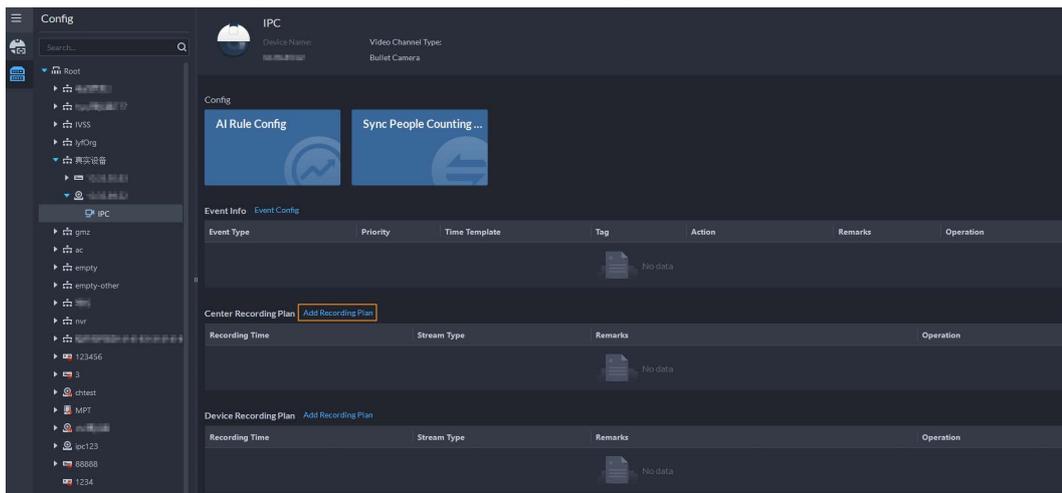
2) Configure the parameters, and then click **OK**.

Table 4-1 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.
Recording Type	• General recording: The device will continuously record videos within the defined periods. • Motion detection recording: Record videos within the defined periods on motion detections. A video can be up to 60 seconds on each motion detection. For example: ◇ Motion A starts, recording will stop after 60 seconds even if motion A has not stopped. ◇ Motion A starts, and motion B starts in 10 seconds. Recording will be made on motion B, and a countdown of 60 seconds start from the beginning. If motion B stops anywhere before 60 seconds is over, recording will stop. But if motion B does not stop in 60 seconds, recording will also stop.
Stream Type	Select **Main Stream**, **Sub Stream 1** or **Sub Stream 2**. Videos recorded on the main stream will have the best quality, but they require more storage.
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 "4.2.5 Adding Time Template".

3) Click **OK**.

● Configure a device recording plan.

If it is an latest EVS, the platform can obtain and display the recording plan that has been configured on the device.

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

Figure 4-21 Add a device recording plan (1)
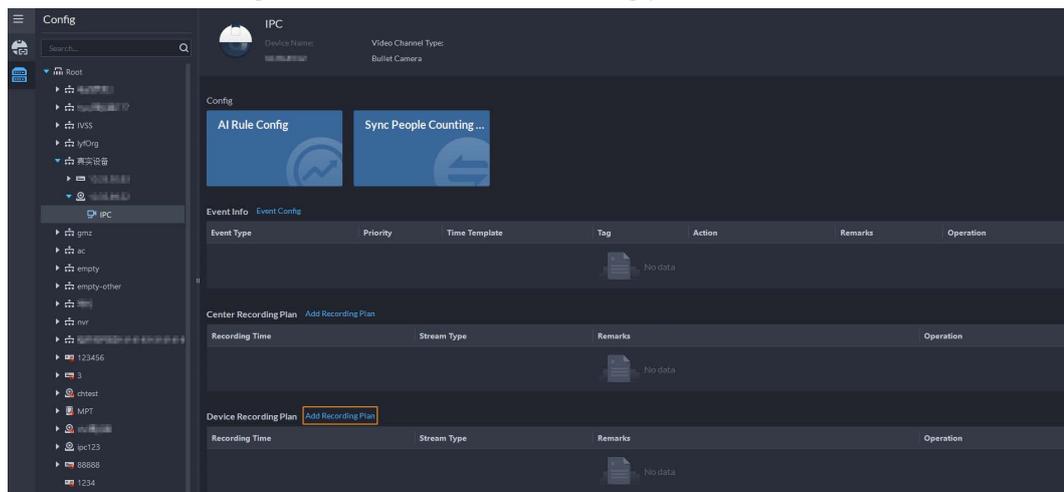
2) Configure the parameters, and then click **OK**.

Table 4-2 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.
Recording Time	Select a default time template or click **Create Time Template** to add a new time template. See "4.2.5 Adding Time Template".

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.

● Edit a recording plan

Click of corresponding plan to edit the plan.

● Click to delete recording plans one by one.

4.2.4.2 Adding Center Recording Plans in Batches

Add a center recording plan of general or motion detection videos for multiple channels at the same time.

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

Figure 4-22 Center recording plan
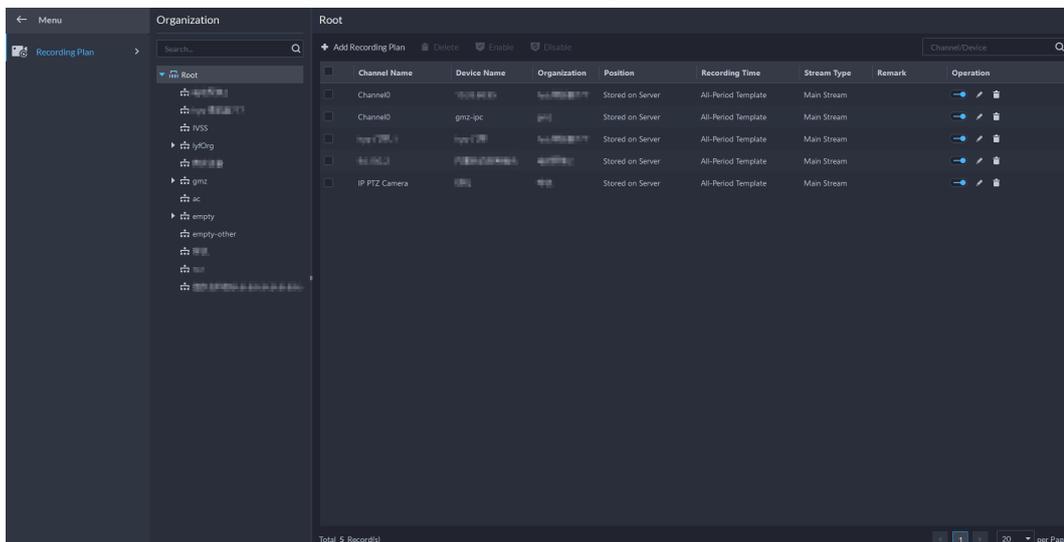
Step 2 Select **General Recording Plan** > **Add General Recording Plan**.

Step 3 Configure the parameters, and then click **OK**.

Table 4-3 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**. Videos recorded on the main stream will have the best quality, but they require more storage.
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 "4.2.5 Adding Time Template".
Recording Channel	Select the channels you want to add the recording plan for.

Step 4 Select **Motion Detection Recording Plan** > **Add Motion Detection Recording Plan**.

Step 5 Configure the parameters, and then click **OK**.

Table 4-4 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.

Parameter	Description

Recording Type	• General recording: The device will continuously record videos within the defined periods.
	• Motion detection recording: Record videos within the defined periods on motion detections. A video can be up to 60 seconds on each motion detection. For example:
	  ◇ Motion A starts, recording will stop after 60 seconds even if motion A has not stopped.
	  ◇ Motion A starts, and motion B starts in 10 seconds. Recording will be made on motion B, and a countdown of 60 seconds start from the beginning. If motion B stops anywhere before 60 seconds is over, recording will stop. But if motion B does not stop in 60 seconds, recording will also stop.

Stream Type	Select **Main Stream**, **Sub Stream 1** or **Sub Stream 2**. Videos recorded on the main stream will have the best quality, but they requires more storage.
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 "4.2.5 Adding Time Template".
Recording Channel	Select the channels you want to add the recording plan for.

- 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.

4.2.5 Adding Time Template

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

Step 2   Click 🖩.

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

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

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

Figure 4-23 Create time template
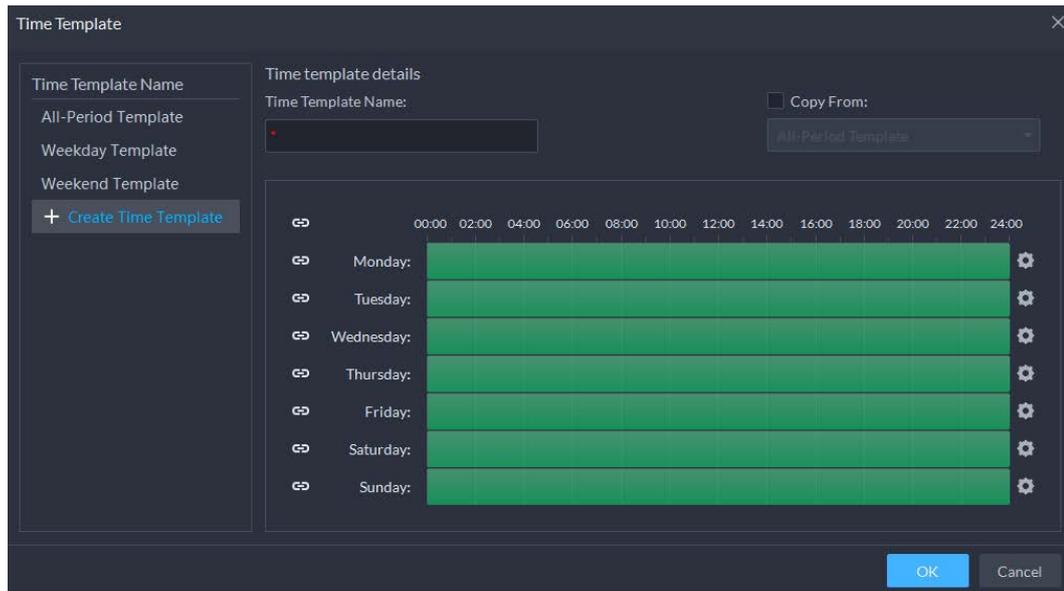
Step 5　　Configure name and periods. You can set up to 6 periods in one day.

　　　　　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 🔗, and then draw the periods for multiple days.
- You can also click ⚙ to configure periods.

Step 6　　Click **OK**.

4.2.6 Configuring Video Retention Period

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

Procedure

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

Step 2　　Click ⌨.

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

Figure 4-24 Go to recording storage configuration page
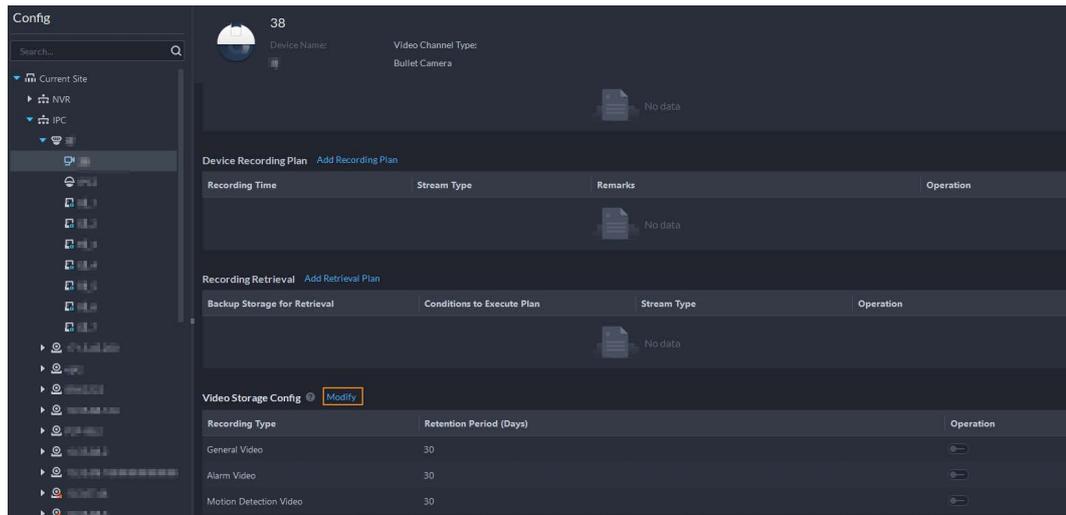
Step 4   Click [toggle] to enable the storing of different type of video, and then configure the retention period.

Step 5   Click **OK**.

Related Operations

Enable/disable record plan

In the operation column, [toggle on] means that the recoding storage configuration has been enabled.

Click the icon and it becomes [toggle off], meaning that the configuration has been disabled.

4.2.7 Configuring Events

You need to set up the event configuration on a device or its channels to receive alarms on the platform.

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

Step 2   Click [icon]

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

Figure 4-25 Go to the event configuration (device)
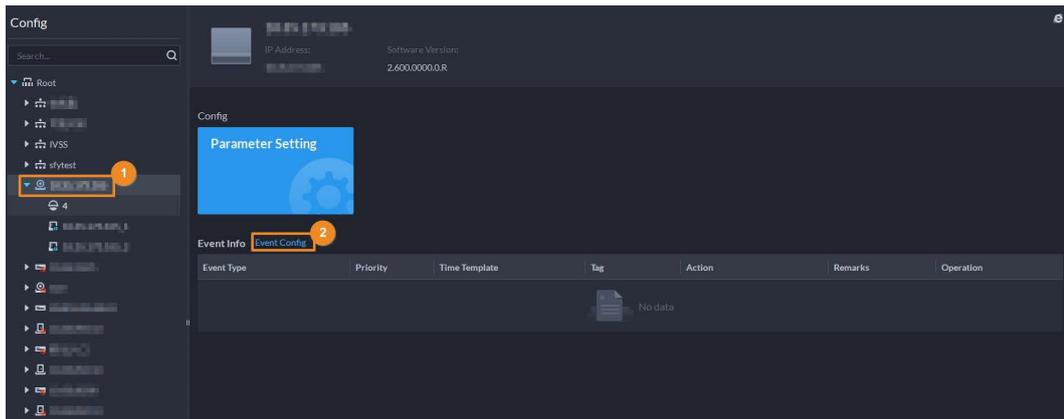
Figure 4-26 Go to the event configuration (channel)
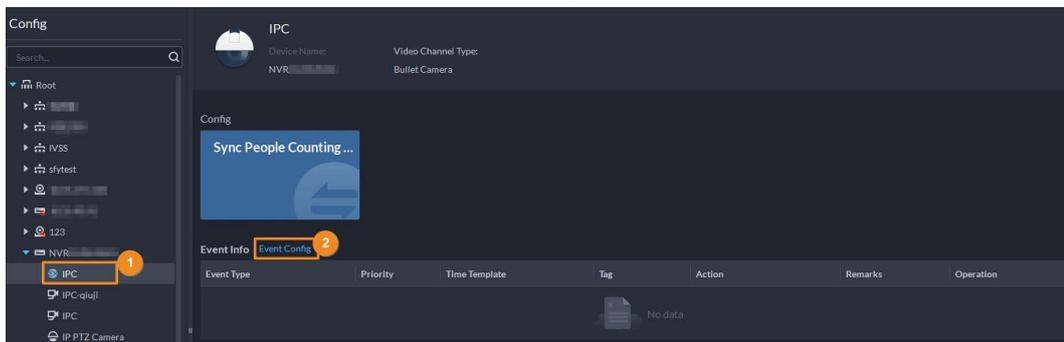
Step 4   Configure events. See "5.1 Configuring Events".

4.2.8 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 pages in the section are for reference only, and might differ from the actual ones.

4.2.8.1 Configuring Camera Properties

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

4.2.8.1.1 Configuring Property Files

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

Step 2   Click .

Step 3   Select a device, and then click **Parameter Setting**.

Figure 4-27 Device configuration
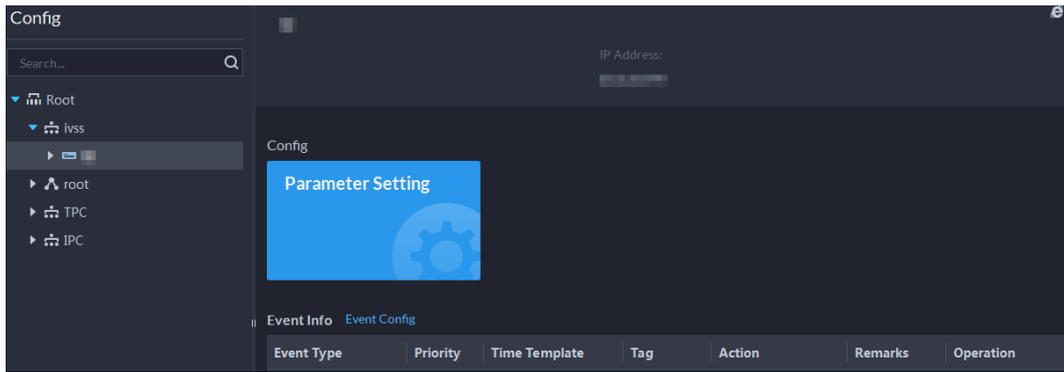
Step 4　　Select **Camera** > **Camera** > **Properties** > **Image**.

Figure 4-28 Image
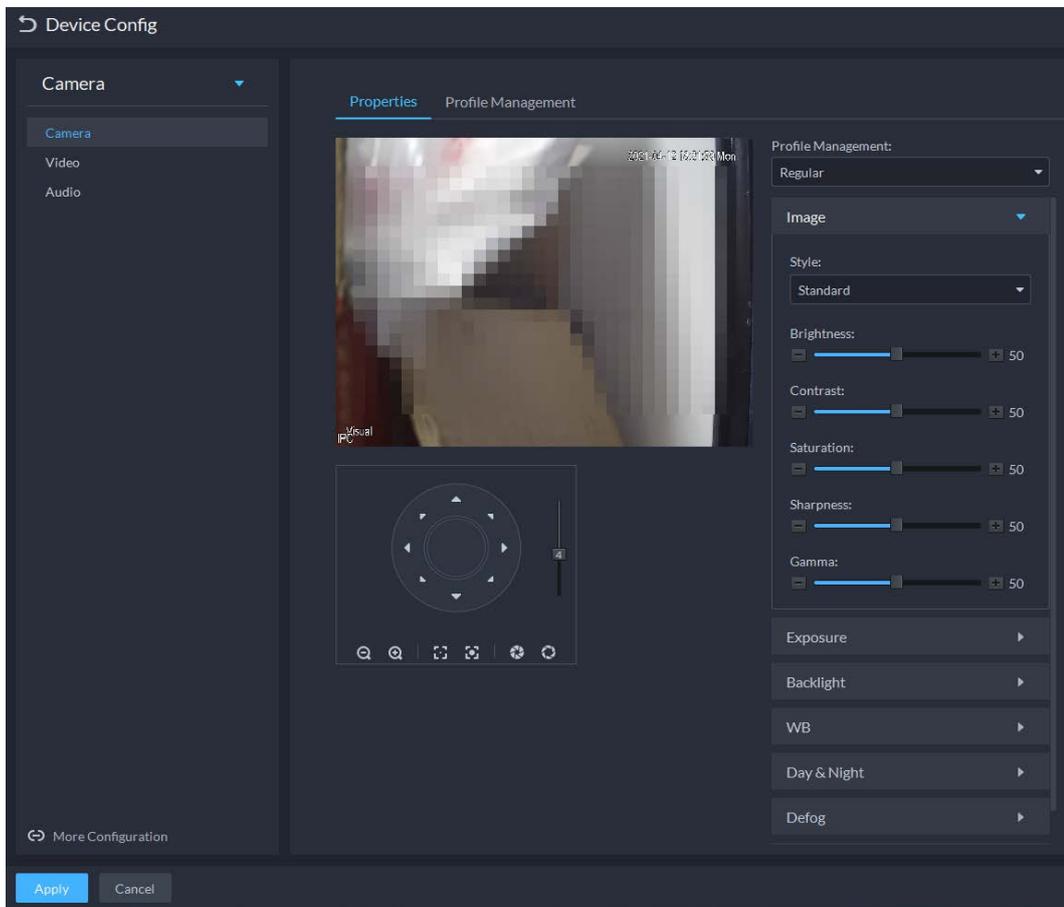
- To go to the device web page, you can click **More configuration**.
- PTZ will be displayed if the device has PTZ function.

Table 4-5 PTZ operation

Icon/Function	Description
Arrow keys	Click it and the camera will rotate to the corresponding direction.

Icon/Function	Description
	Adjust the speed. The higher the value, the faster the camera rotates.
	Zoom in and out.
	Adjust the focus level.
	Adjust the aperture.

Step 5 Select a mode from the drop-down list for **Profile Management**.

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

Table 4-6 Image parameters

Parameter	Description
Style	You can set the image style to be **Standard**, **Soft**, or **Vivid**.
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 result in noises in images.
Gamma	Changes image brightness by non-linear tuning to expand the dynamic display range of images. The higher the value, the brighter the image and vice versa.

Step 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 4-29 Exposure
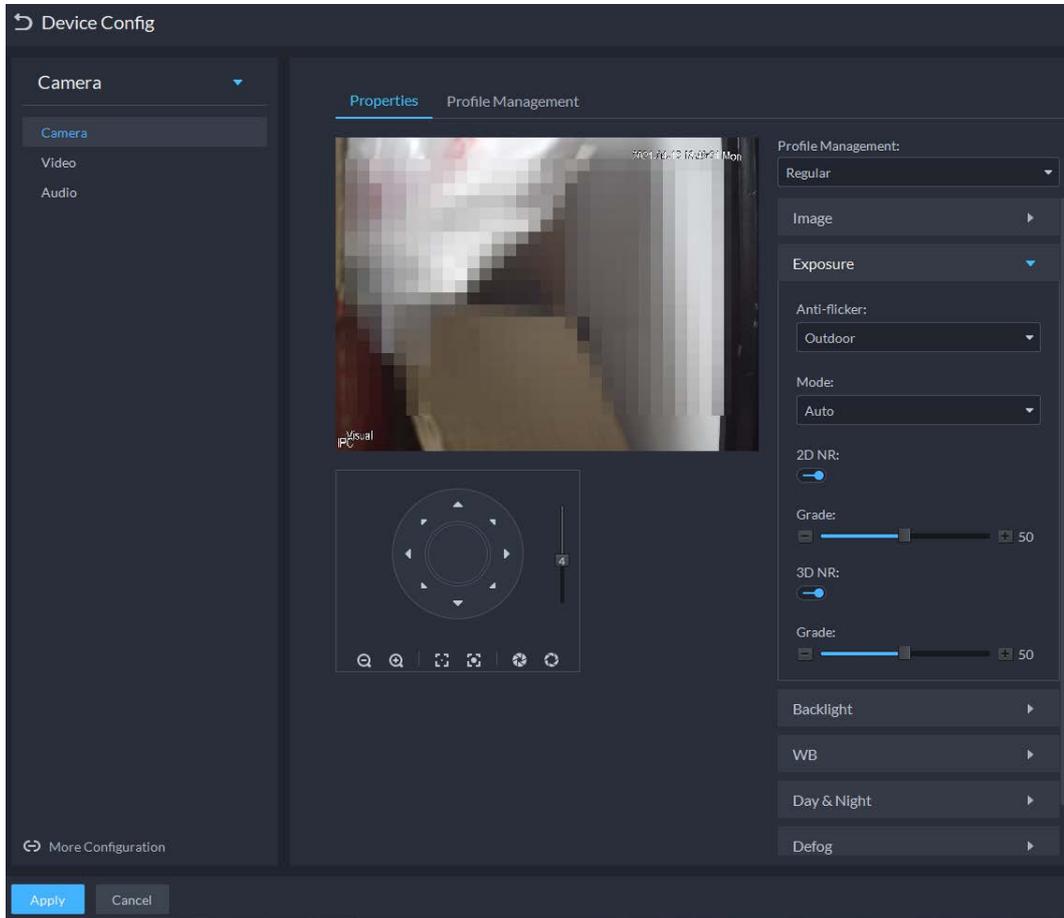
Table 4-7 Exposure parameters

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 no horizontal stripe appears 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 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 pages 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 4-30 Backlight
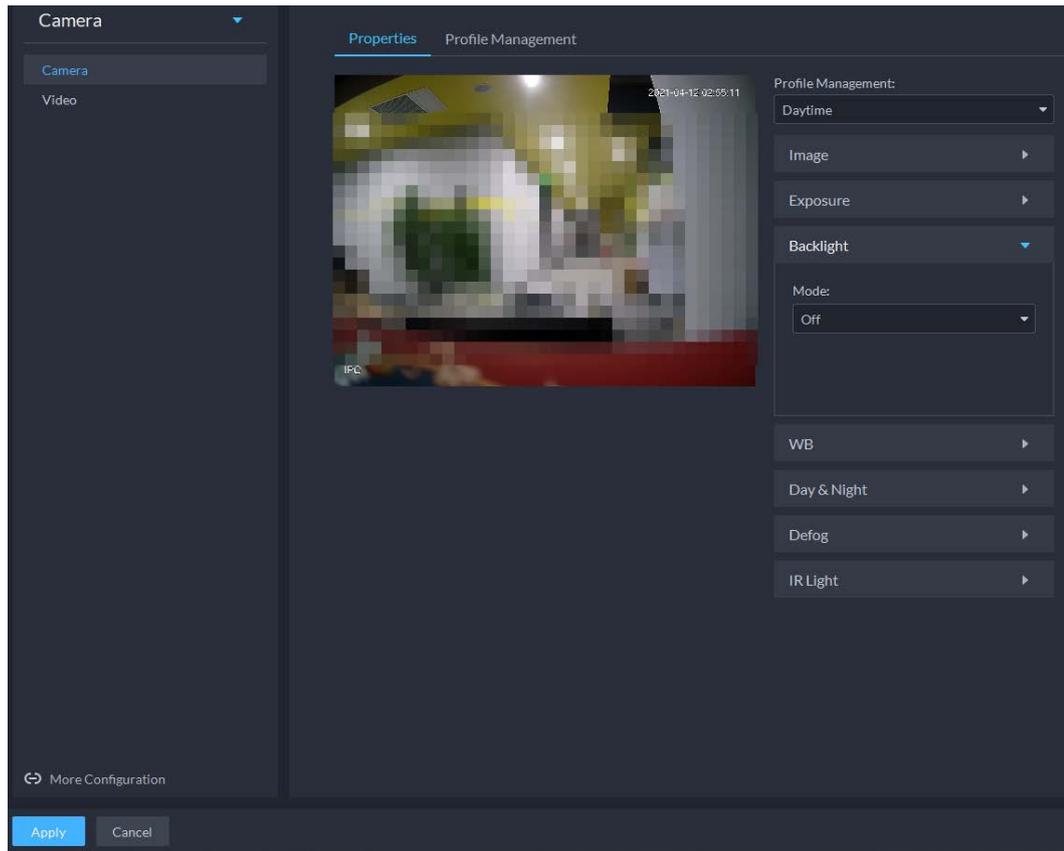
Table 4-8 Backlight parameters

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 4-31 WB
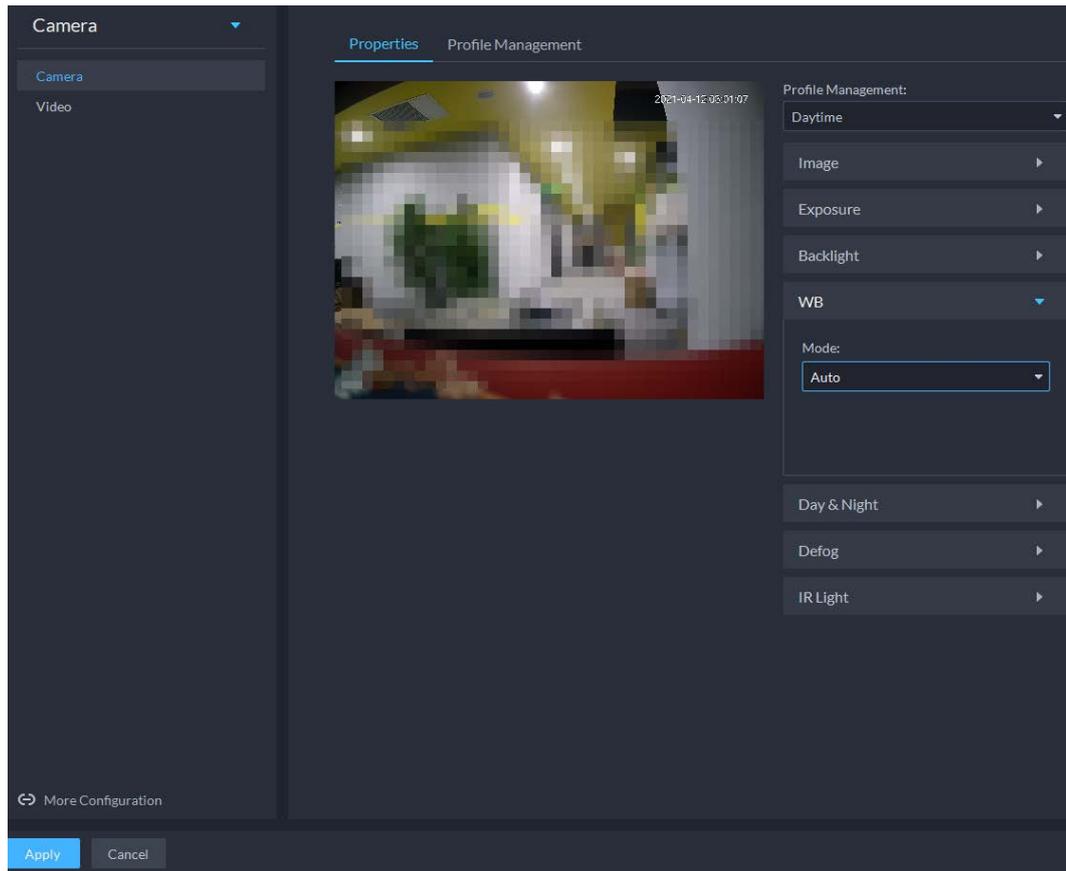
Table 4-9 WB parameters

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 4-32 Day & night
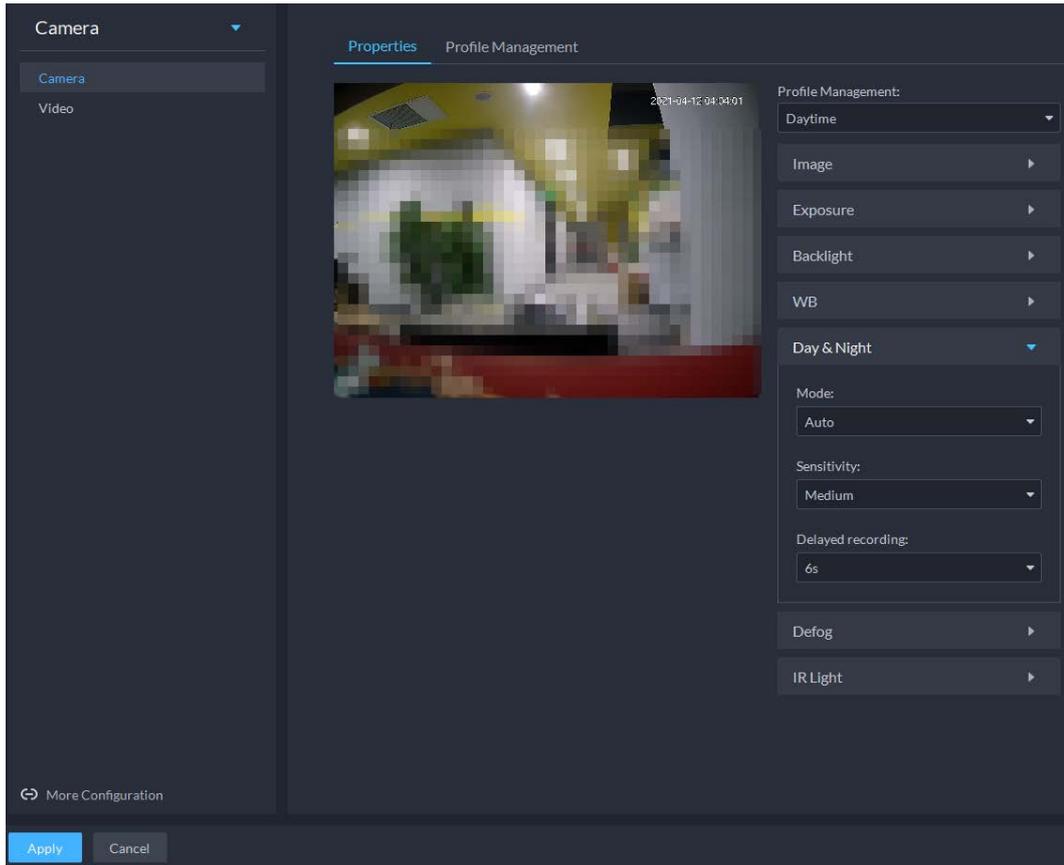
Table 4-10 Day & night parameters

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 Figure 4-33. For details of the parameters, see Table 4-11.

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

Figure 4-33 Defog
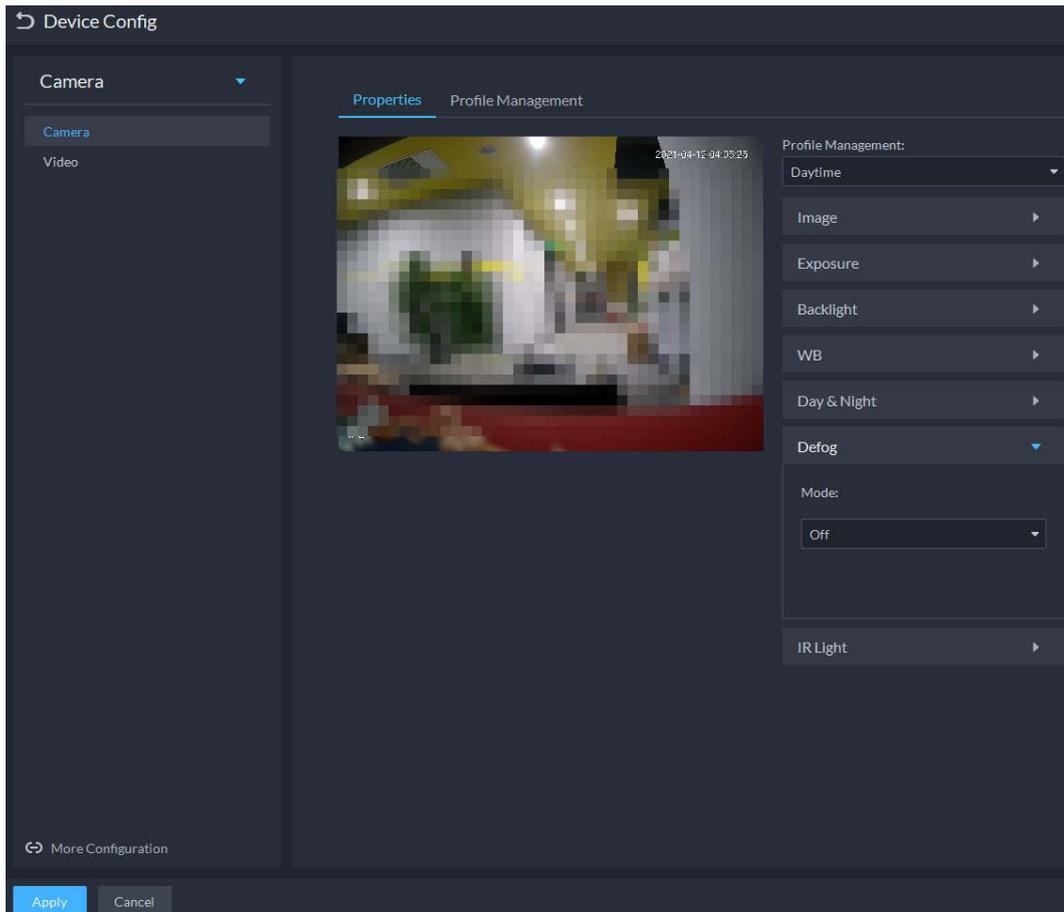
Table 4-11 Defog parameters

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 4-34 IR light
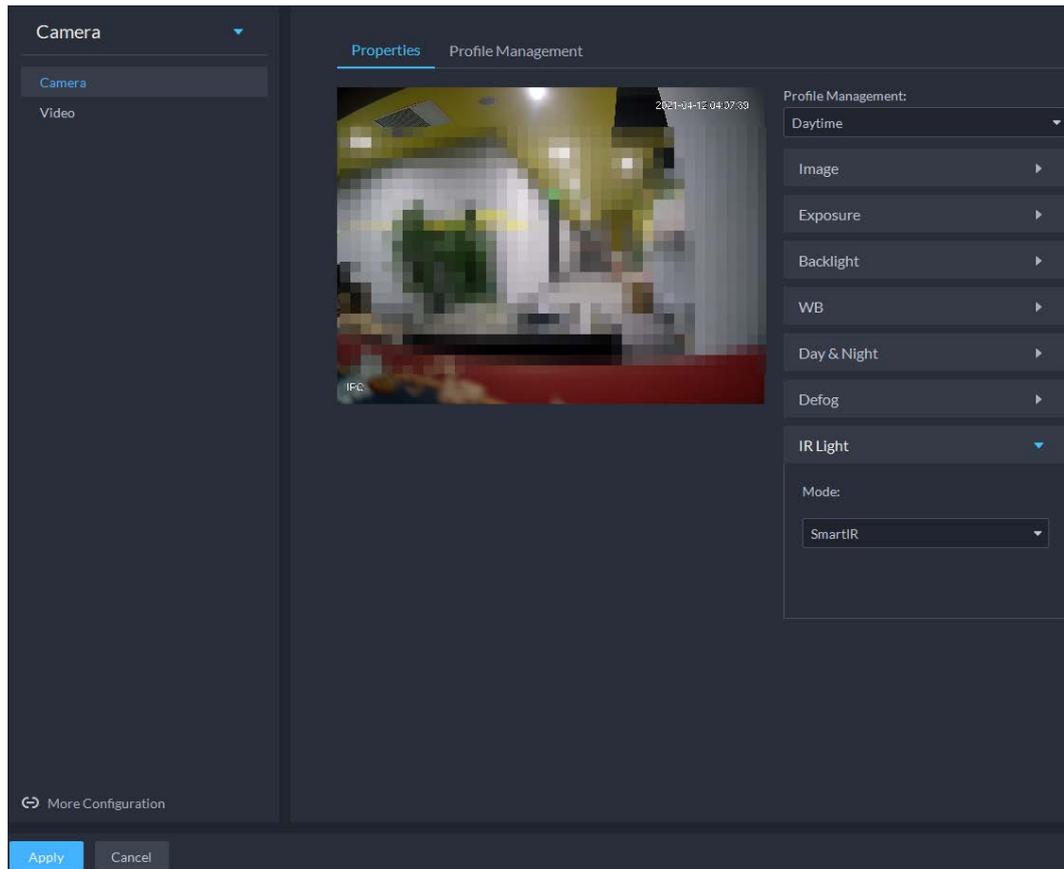
Table 4-12 IR light parameters

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.
Zoom Priority	The system adjusts the illuminator according to the lighting condition. ● When the environment turns dark, the low beam will be used first. If the low beam is not enough, the high beam will be used. ● When the environment turns bright, the high beam will be adjusted or turned off first. If it is still too bright, the low beam will be adjusted or turned off. ● When the focal length is adjusted to a wide angle value, the high beam will not be used to avoid overexposure on the objects near the camera, but you can manually adjust the brightness of the low beam by reducing or increasing the light compensation value.
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.

4.2.8.1.2 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** page, click ![icon], and then in the **Basic Config** section, select **Device**.

Step 2   Click ![icon].

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

Figure 4-35 Device configuration
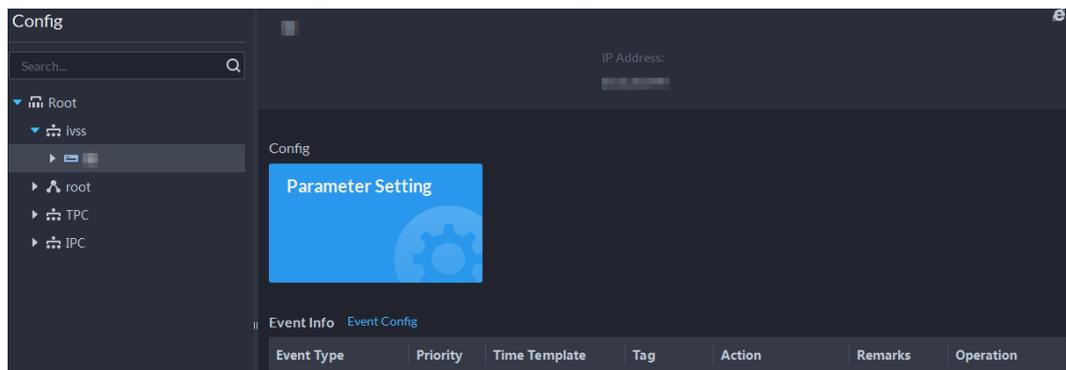
Step 4   Click **Profile Management**, and set configuration files.

● When the mode is set to **Regular**, the system monitors the objects as per regular configurations.

Figure 4-36 Set configuration files as regular
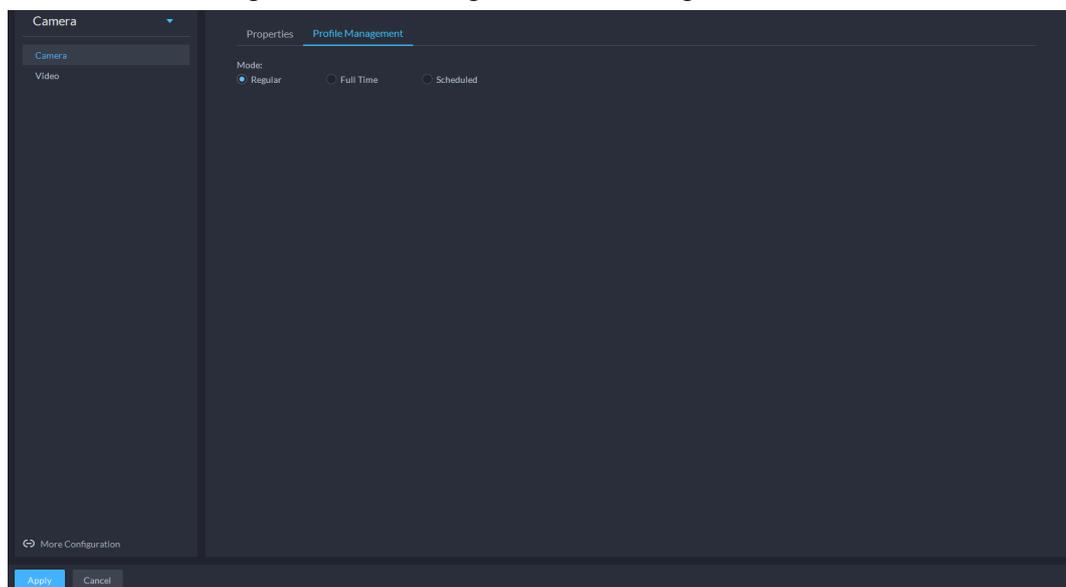
● When the mode is set to **Full Time**, you can set **Always Enable** to **Daytime** or **Night**. The system monitors the objects as per the **Always Enable** configurations.

Figure 4-37 Set configuration files as full time
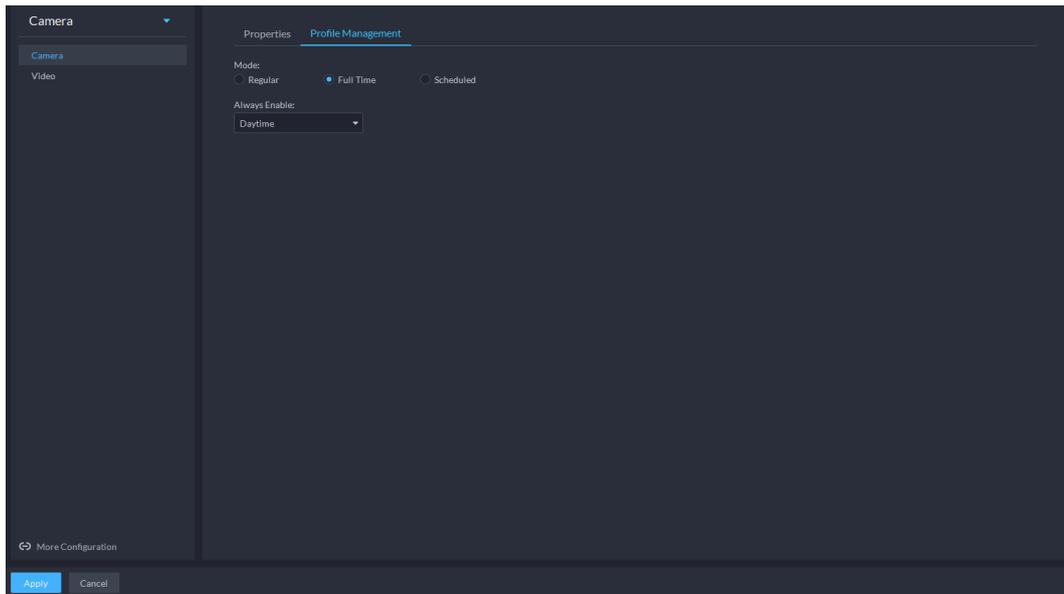
- When the mode is set to **Shift by time**, you can drag the slider to set a period of time as daytime or night. For example, you can set 8:00–18:00 as daytime, 0:00–8:00 and 18:00–24:00 as night. The system monitors the objects in different time periods as per corresponding configurations.

Figure 4-38 Set configuration files as shift by time
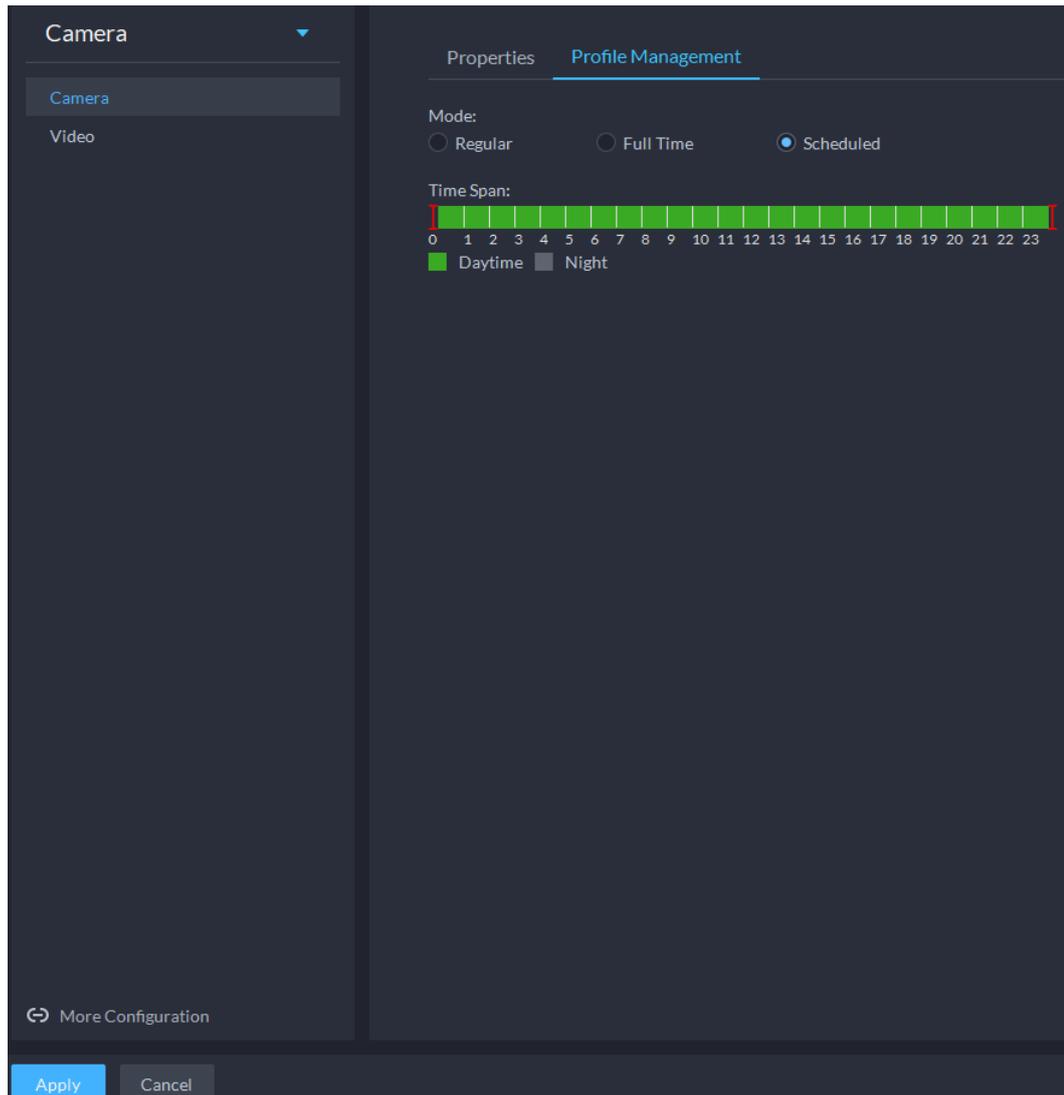
Step 5 Click **OK** to save the configurations.

4.2.8.2 Video

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

4.2.8.2.1 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** page, click 🔧, and then in the **Basic Config** section, select **Device**.

Step 2 Click 🖳.

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

Figure 4-39 Device configuration
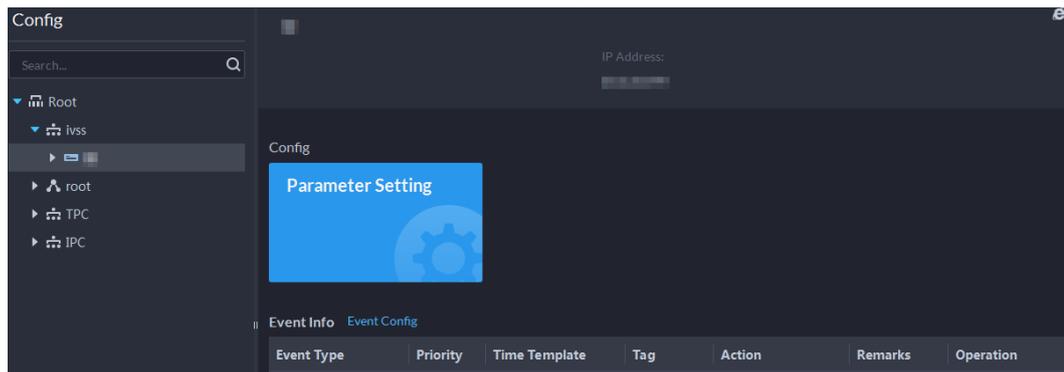
Step 4   Select **Camera** > **Video** > **Video Stream**.

Step 5   Set **Video Stream**.

Figure 4-40 Configure video stream settings
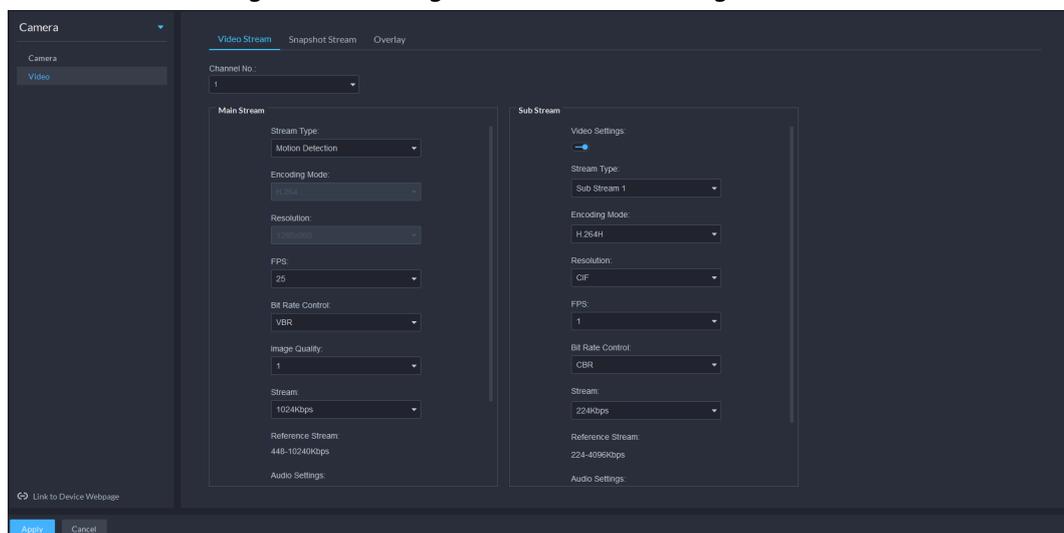
The default values of streams are for reference only, and the actual pages might be different.

Table 4-13 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. ● SVAC (Surveillance Video and Audio Coding): It is a standard for security surveillance applications in China.

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. Characters for watermark verification. The default value is DigitalCCTV.

Step 6   Click **Apply**.

4.2.8.2.2 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** page, click ▣, and then in the **Basic Config** section, select **Device**.

Step 2   Click ▣.

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

Figure 4-41 Device configuration
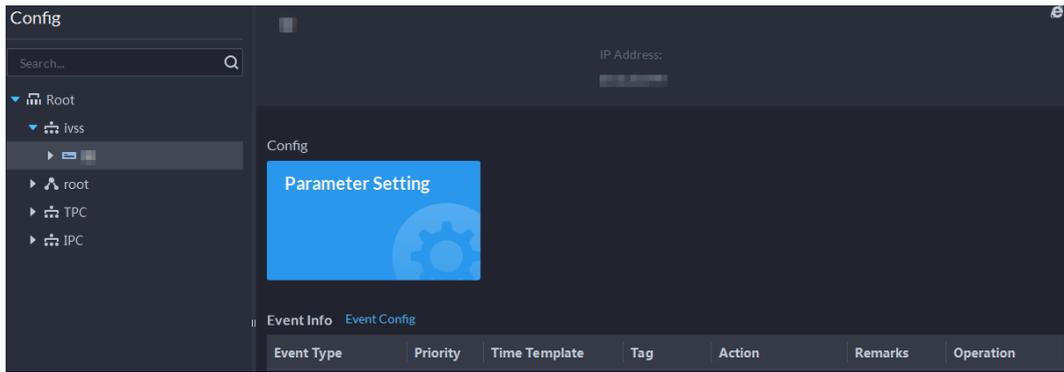
Step 4   On the **Device Config** page, select **Camera** > **Video** > **Snapshot Stream**.

Figure 4-42 Configure snapshot stream settings

Step 5   Set **Snapshot Stream**.

Table 4-14 Snapshot stream parameters

Parameter	Description
Snapshot Type	It includes **General** 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**.
Image Quality	Sets up image quality. It is divided into six grades: Best, better, good, bad, worse and worst.

Parameter	Description
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 page of the device.

Step 6   Click **OK**.

4.2.8.2.3 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** page, click ![icon], and then in the **Basic Config** section, select **Device**.

Step 2   Click ![icon].

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

Figure 4-43 Device configuration
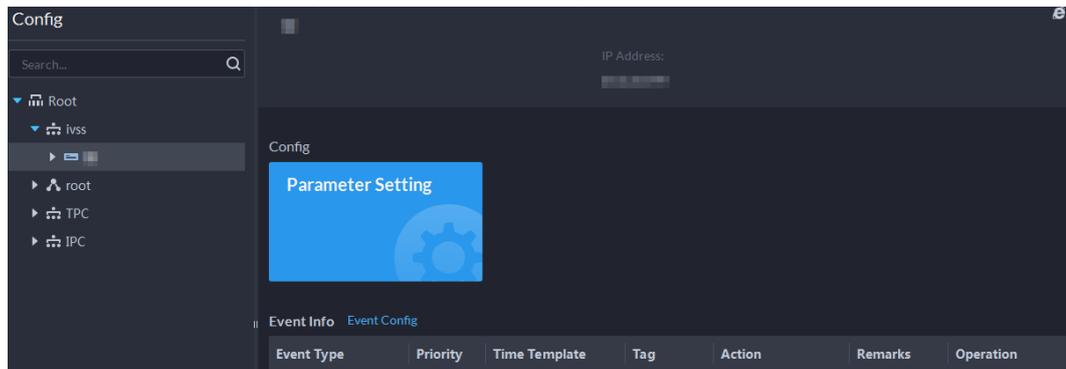
Step 4   On the **Device Config** page, select **Camera** > **Video** > **Overlay**.

Step 5   Set privacy mask.

Figure 4-44 Overlay
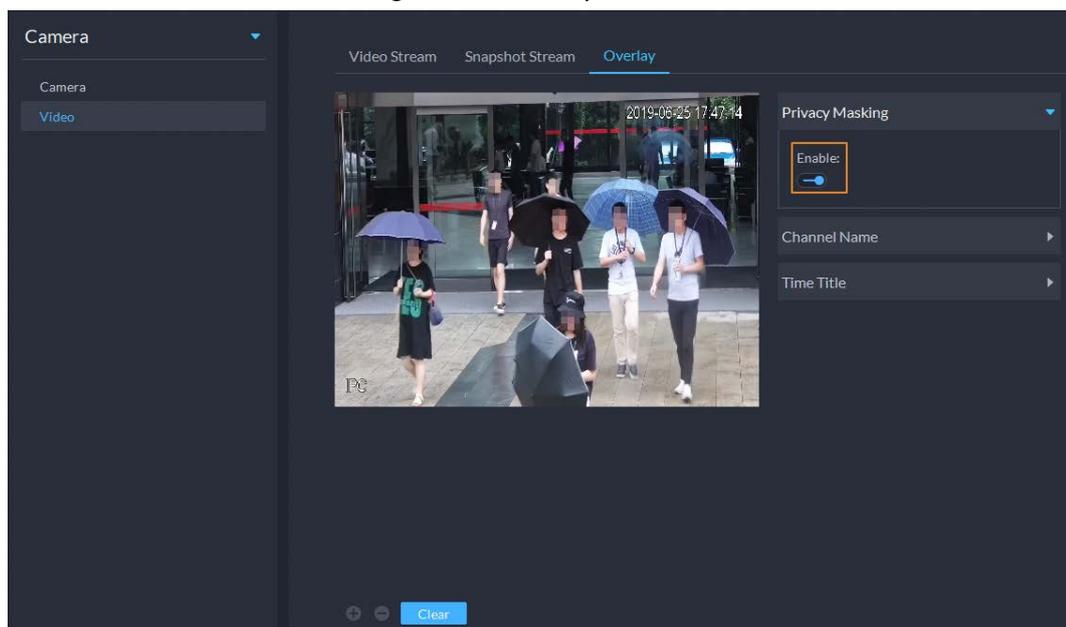
1) Click the **Privacy Mask** tab.

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 4-45 Set channel name
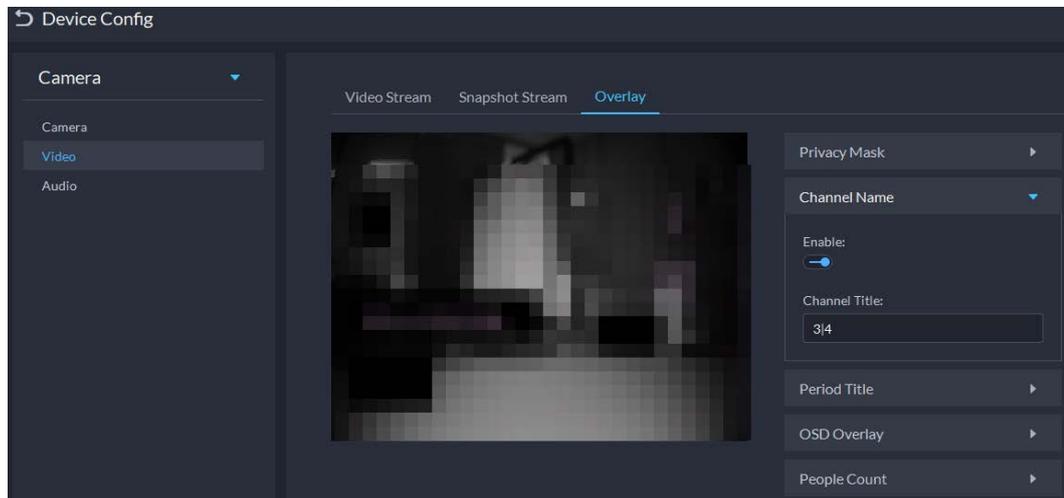
2) Click ⬤━ to enable the function.

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 4-46 Set period title
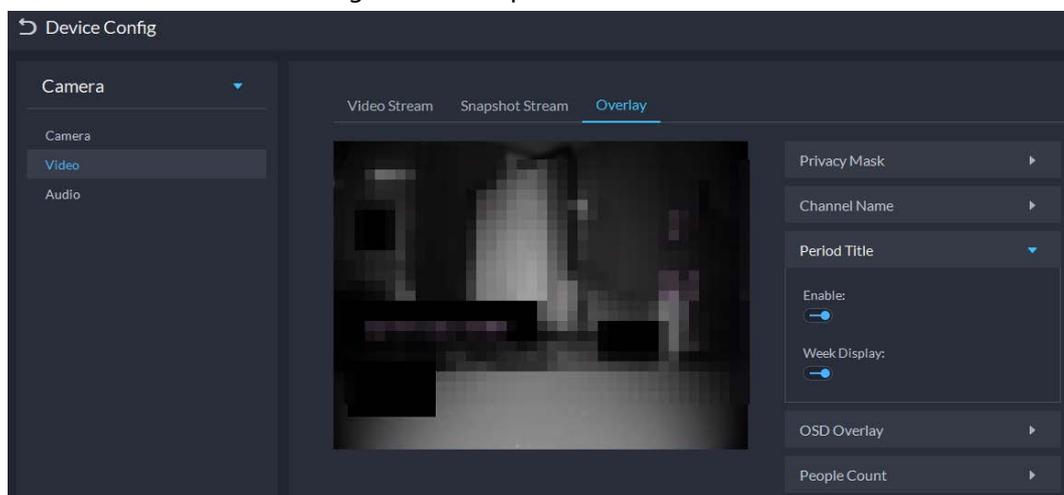
2) Click ⬤━ to enable the function.

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   OSD overlay.

1) Enable **Geographic Position**, and then enter the geographic information of the camera.

2) Select a text alignment method.

Figure 4-47 OSD overlay
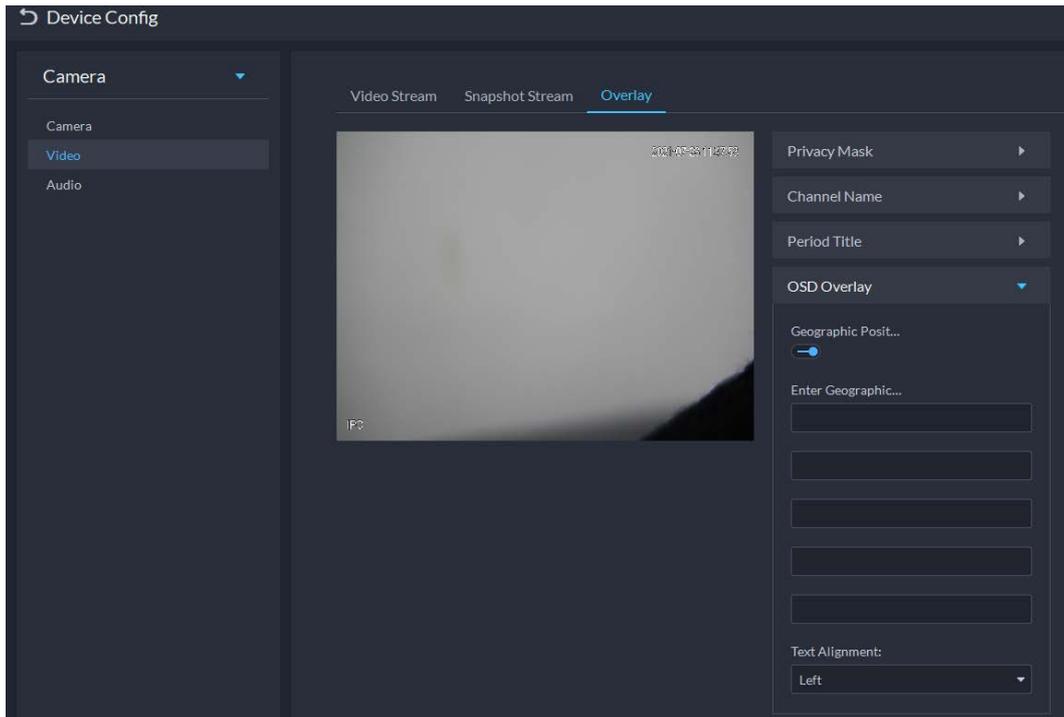
Step 9   Click **OK**.

4.2.8.3 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** page, click ![icon], and then in the **Basic Config** section, select **Device**.

Step 2   Click ![icon].

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

Figure 4-48 Device configuration
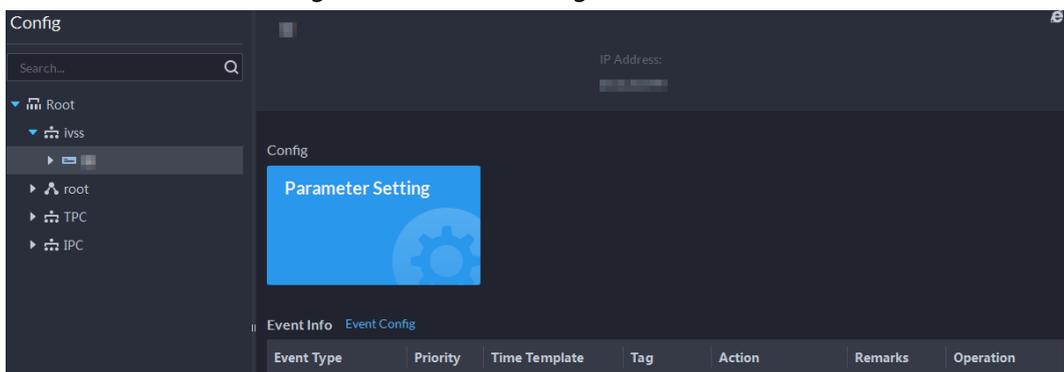
Step 4   On the **Device Config** page, select **Camera** > **Audio**.

Step 5   Set parameters.

Figure 4-49 Configure audio settings
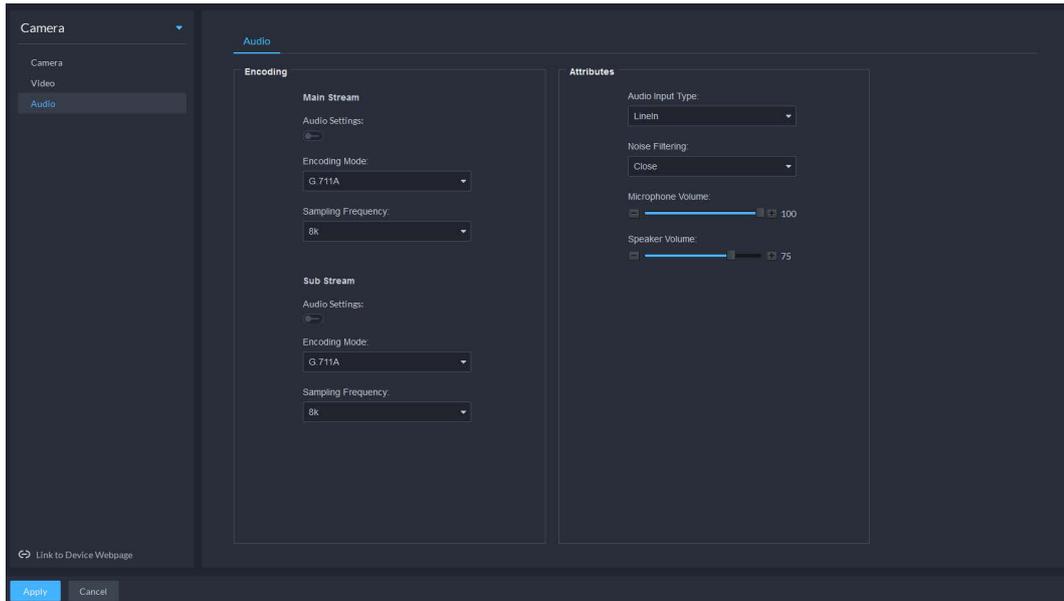
Table 4-15 Audio parameters

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: ● Lineln: 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**.

4.2.9 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.

4.2.9.1 Enabling IVS Smart Plan

Enable IVS functions.

Step 1 Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **Basic Config** section, select **Device**.
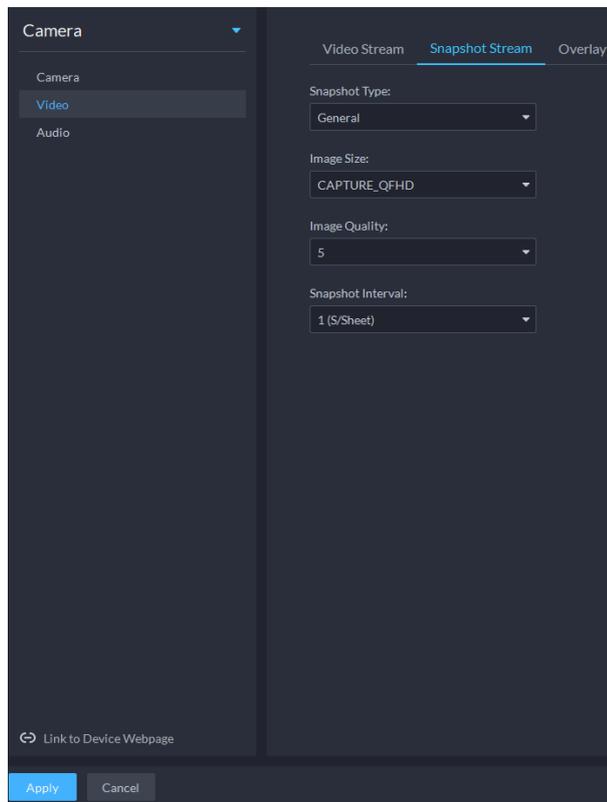
Step 2 Click ![icon].

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

Figure 4-50 Go to AI rule configuration page
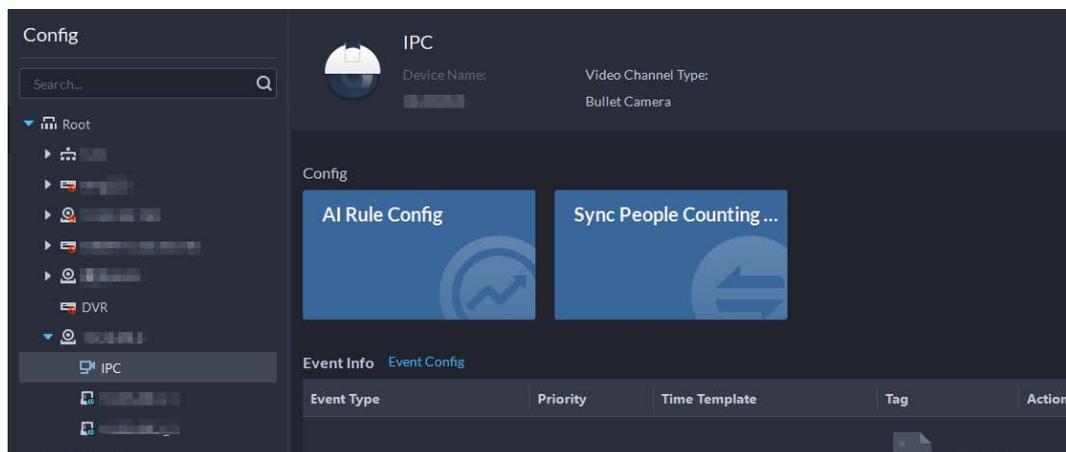
Step 4 Click ![icon] on the smart plan page to enable IVS smart plan.
When the icon is displayed in the white frame, it means the smart plan is selected. If another smart plan has been selected, click that smart plan icon to deselect it and then click ![icon] to select IVS.

Figure 4-51 IVS smart plan
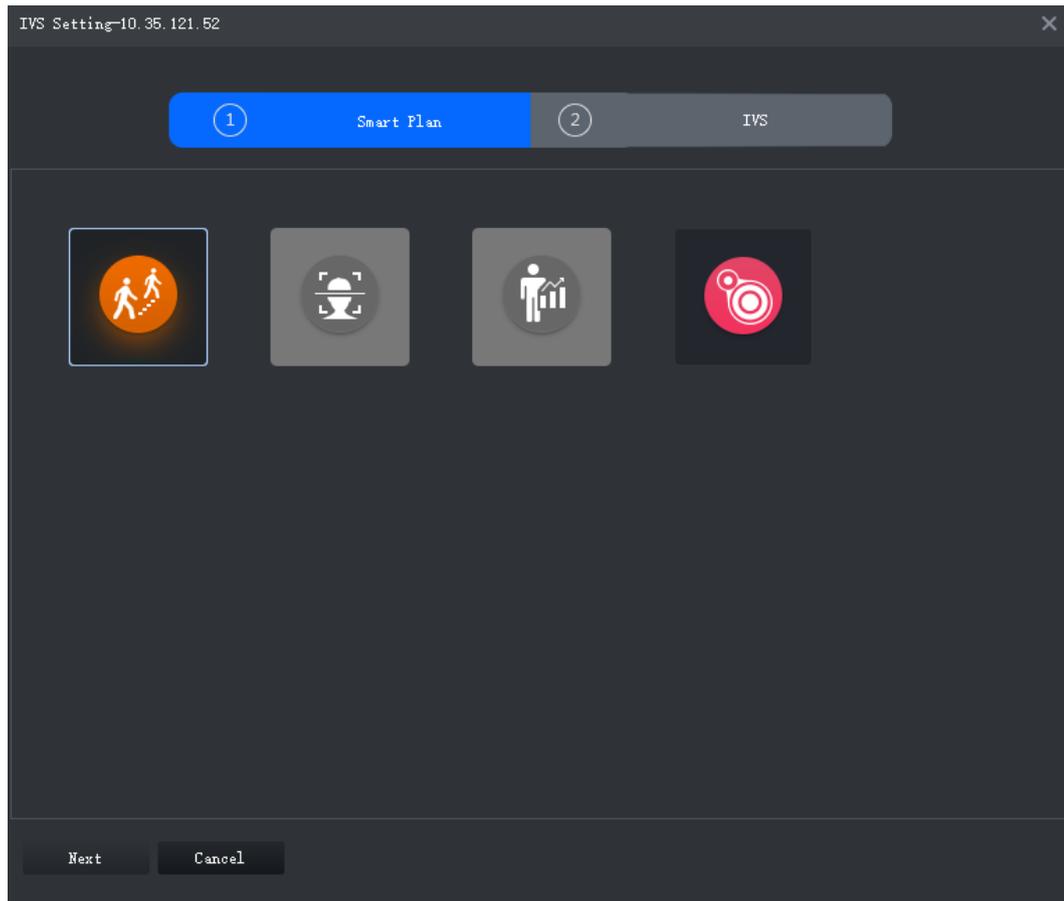
Step 5   Click **Next** to go to the **IVS** page.

4.2.9.2 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** page, 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 4-52 Go to AI rule configuration page
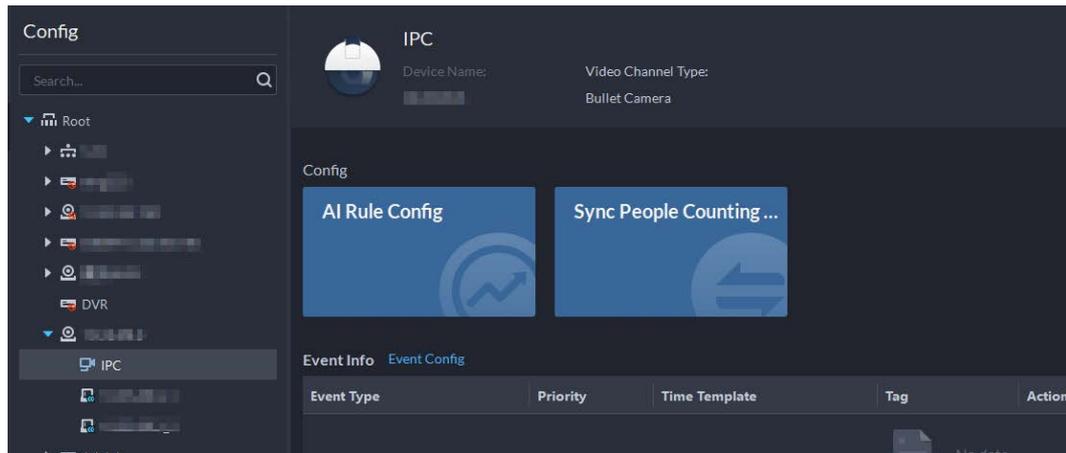
Step 4   After selecting the IVS smart plan on the **Smart Plan** page, click **Next**.

Step 5   Click ▾ to go to the calibration page.

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 4-53 Calibrating depth of field
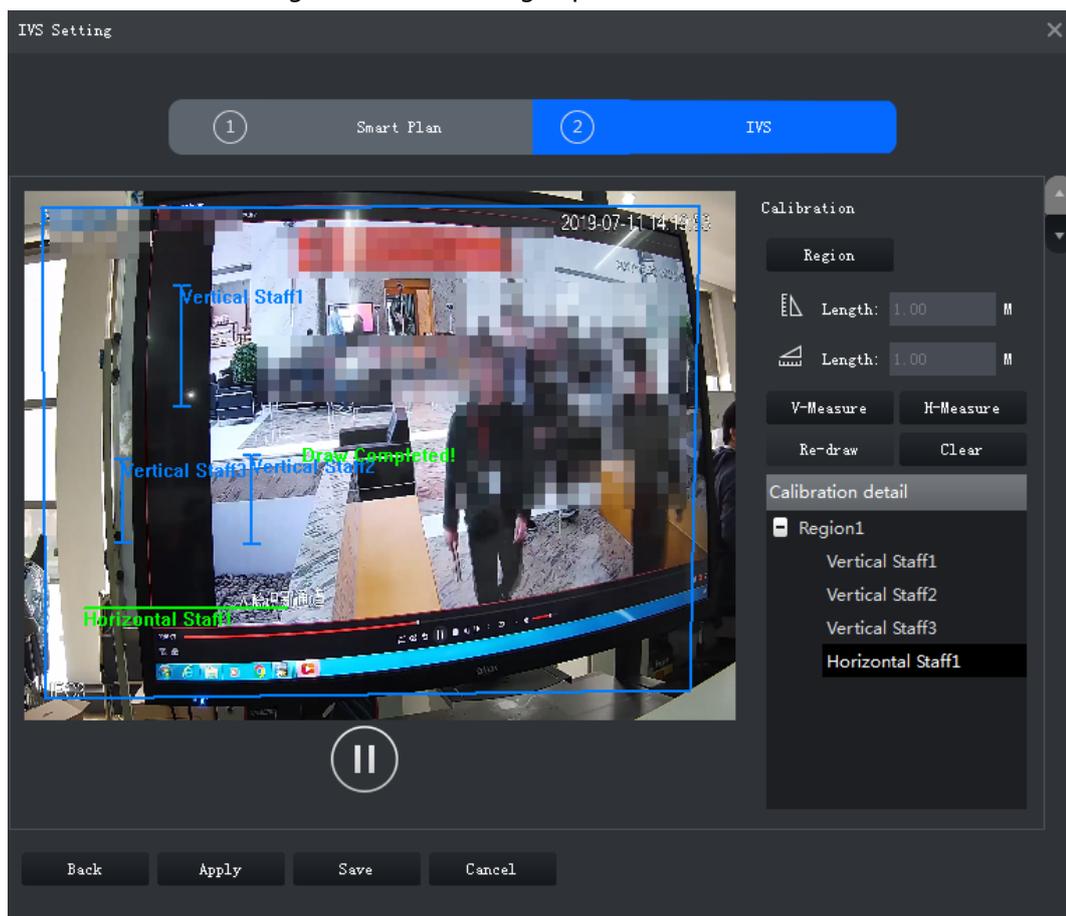
Step 8   Set length value of horizontal gauge. Click ◿ and then draw a horizontal gauge in the calibration area. Click to finish.

- 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.

4.2.9.3 Configuring Detection Region

Configure the detection zone of IVS.

Step 1 Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **Basic Config** section, select **Device**.

Step 2 Click ![icon].

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

Figure 4-54 Go to AI rule configuration page
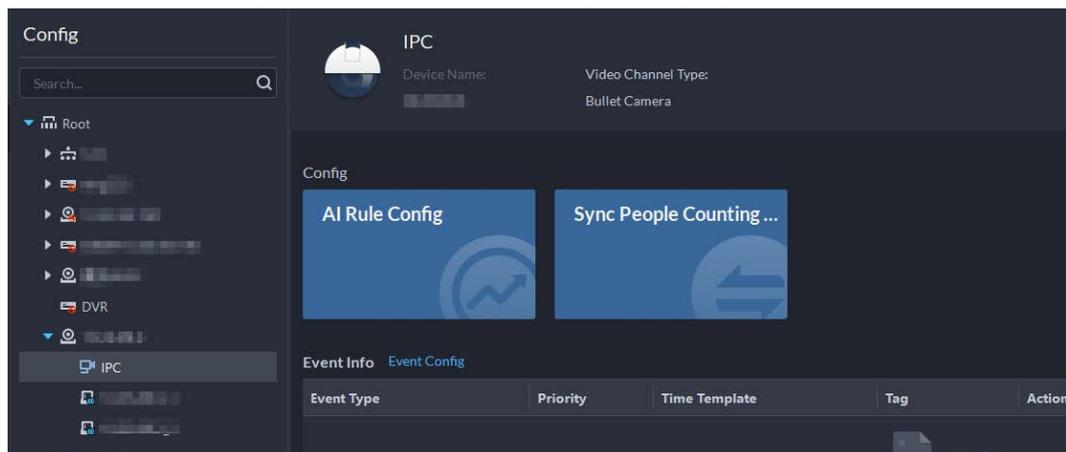
Step 4 After selecting the IVS smart plan in the **Smart Plan** page, click **Next**.

Step 5 Click ![icon].

Figure 4-55 Detection region
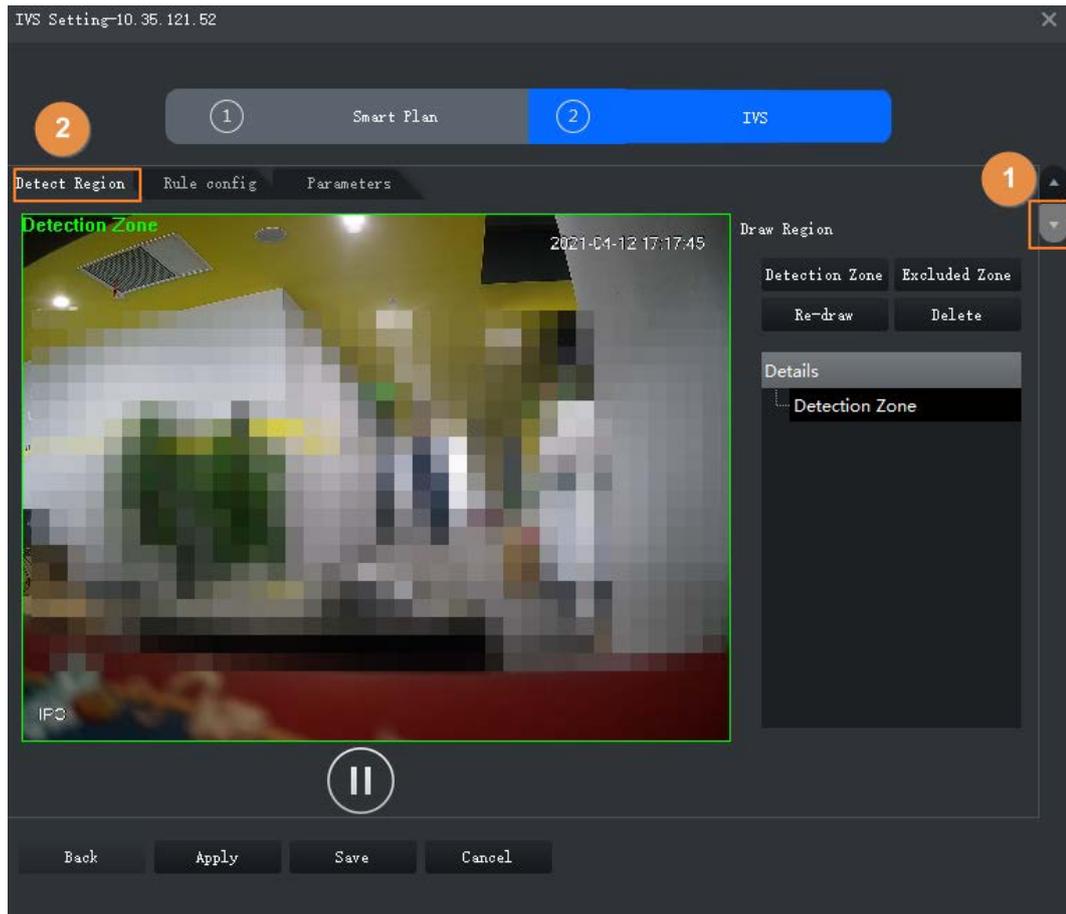
Step 6   Click **Detection Zone**, and then draw the frame of the detection zone on the video and right-click to finish.

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

4.2.9.4 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.

4.2.9.4.1 Tripwire

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

Step 1   On the **IVS** page, click **Rule config**.

Figure 4-56 Rule configuration
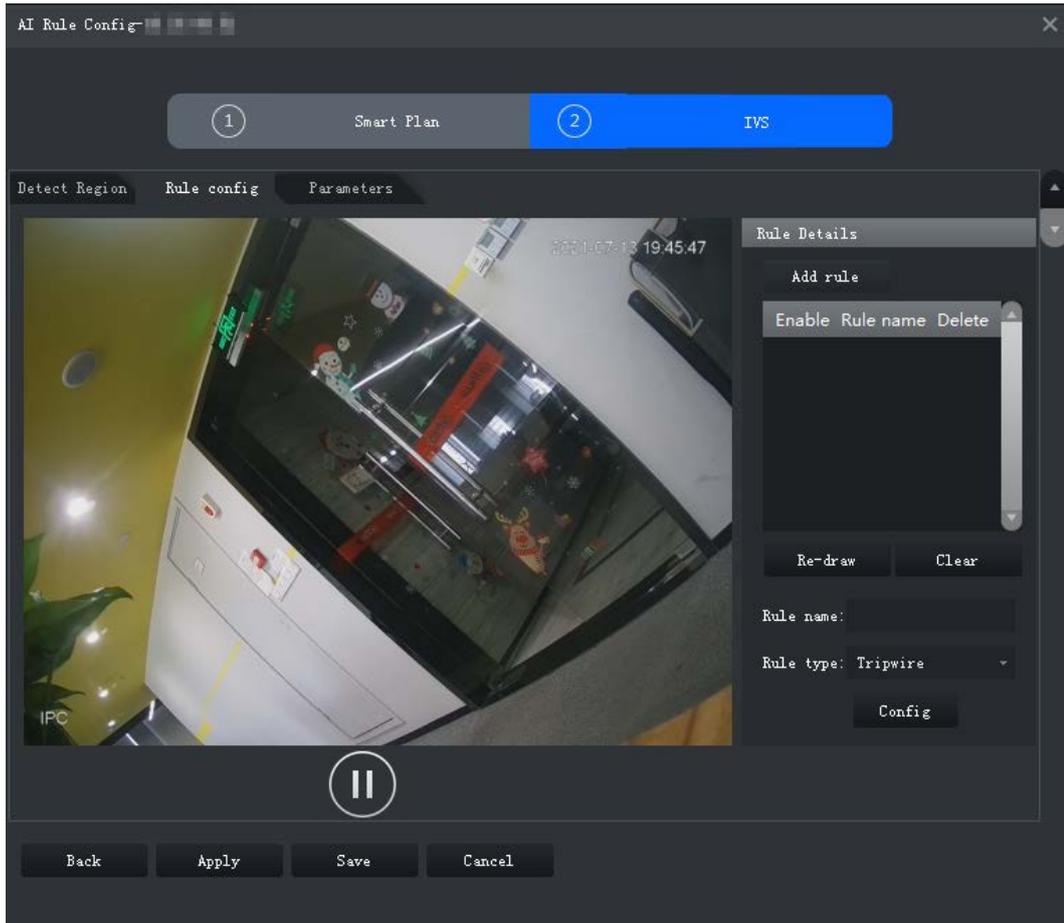
Step 2   Click **Add rule**.

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 4-57 Tripwire
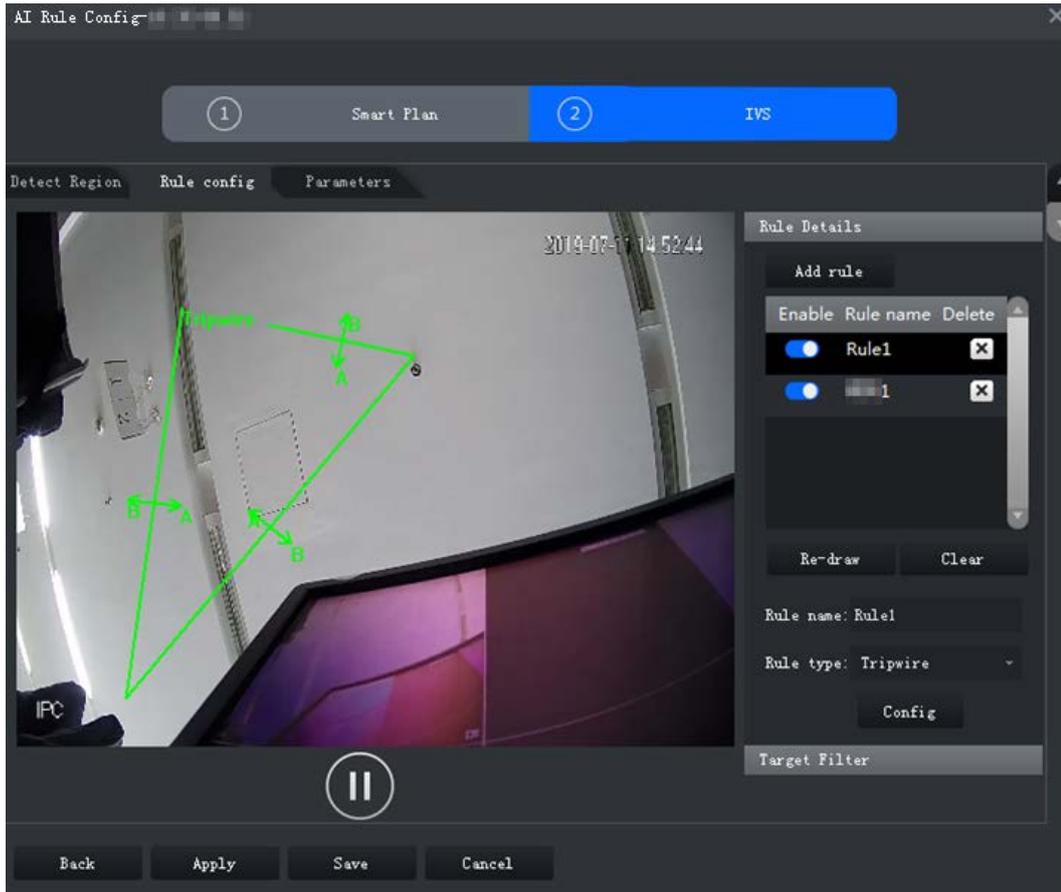
Step 5   Set parameters, arming schedule and alarm linkage.

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

Figure 4-58 Set parameters
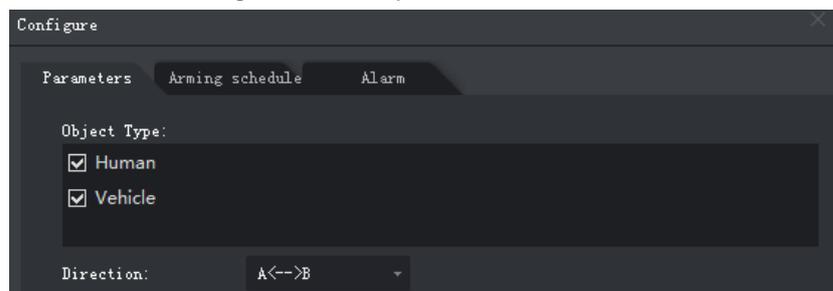
Table 4-16 Parameters

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 4-59 Arming schedule

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

Figure 4-60 Alarm linkage
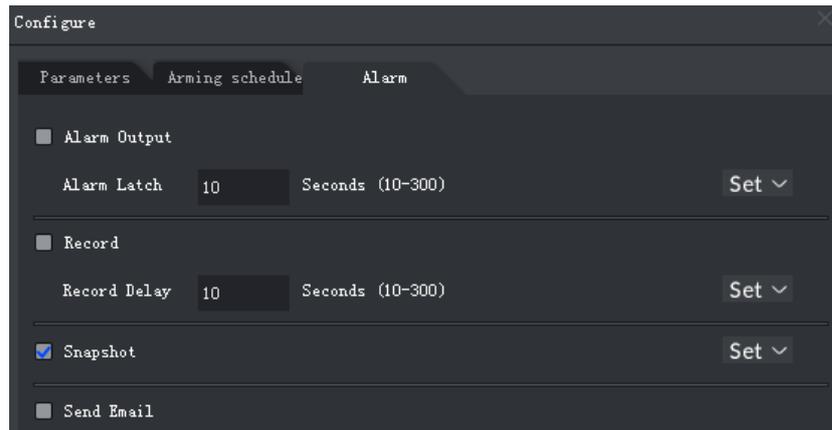
Table 4-17 Parameters

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 4-61 Target filtering
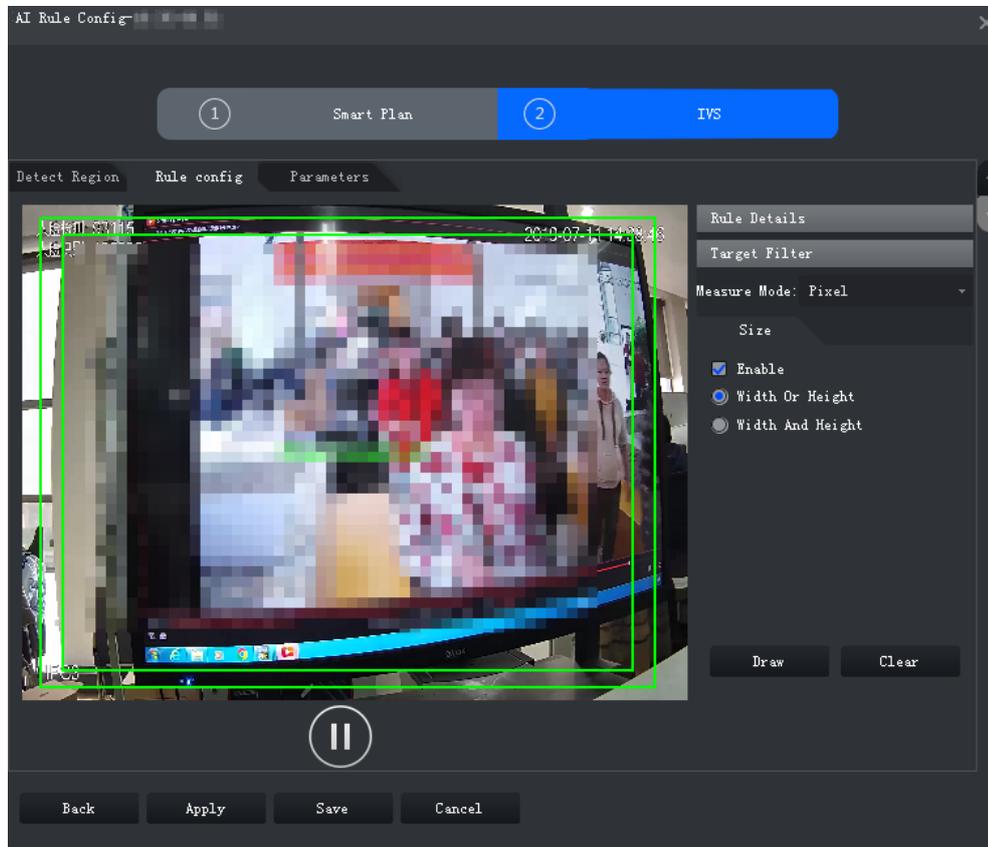
Step 7 Click **Apply**.

4.2.9.4.2 Intrusion

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

Step 1 On the **IVS** page, click **Rule config**.

Figure 4-62 Rule configuration
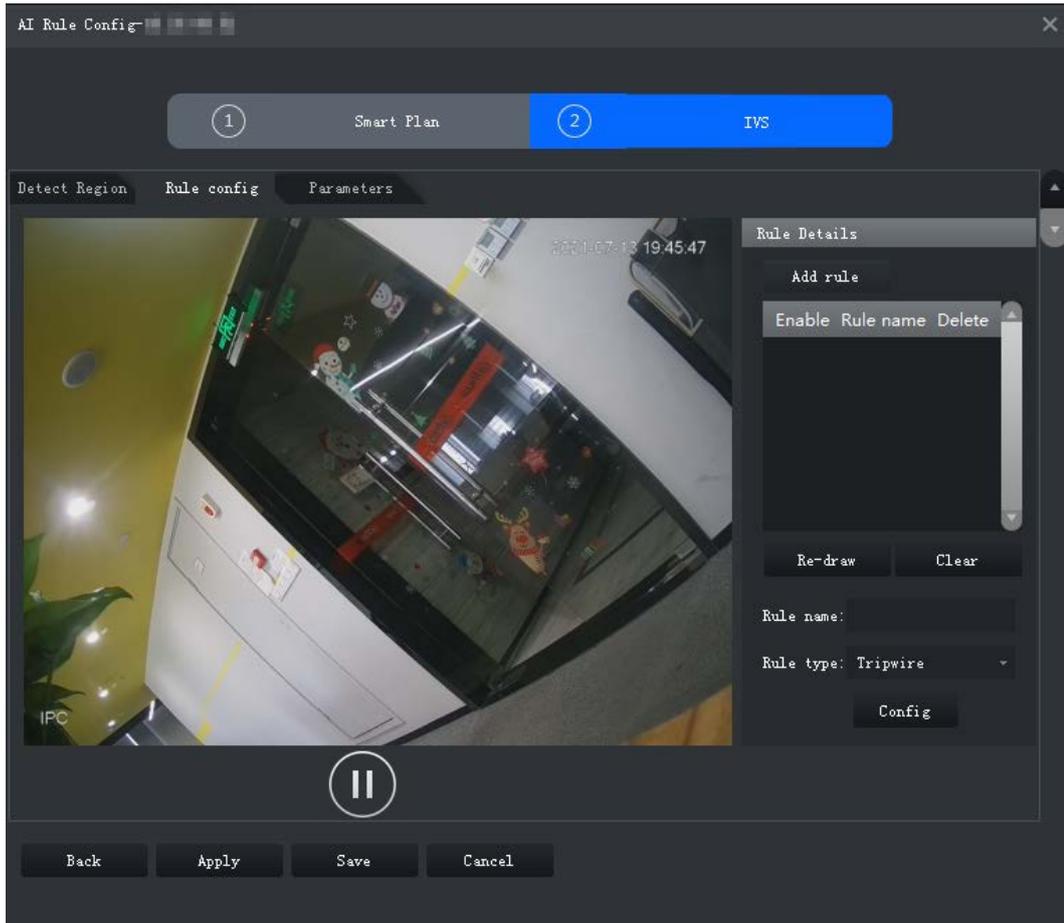
Step 2   Click **Add rule**.

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 4-63 Intrusion
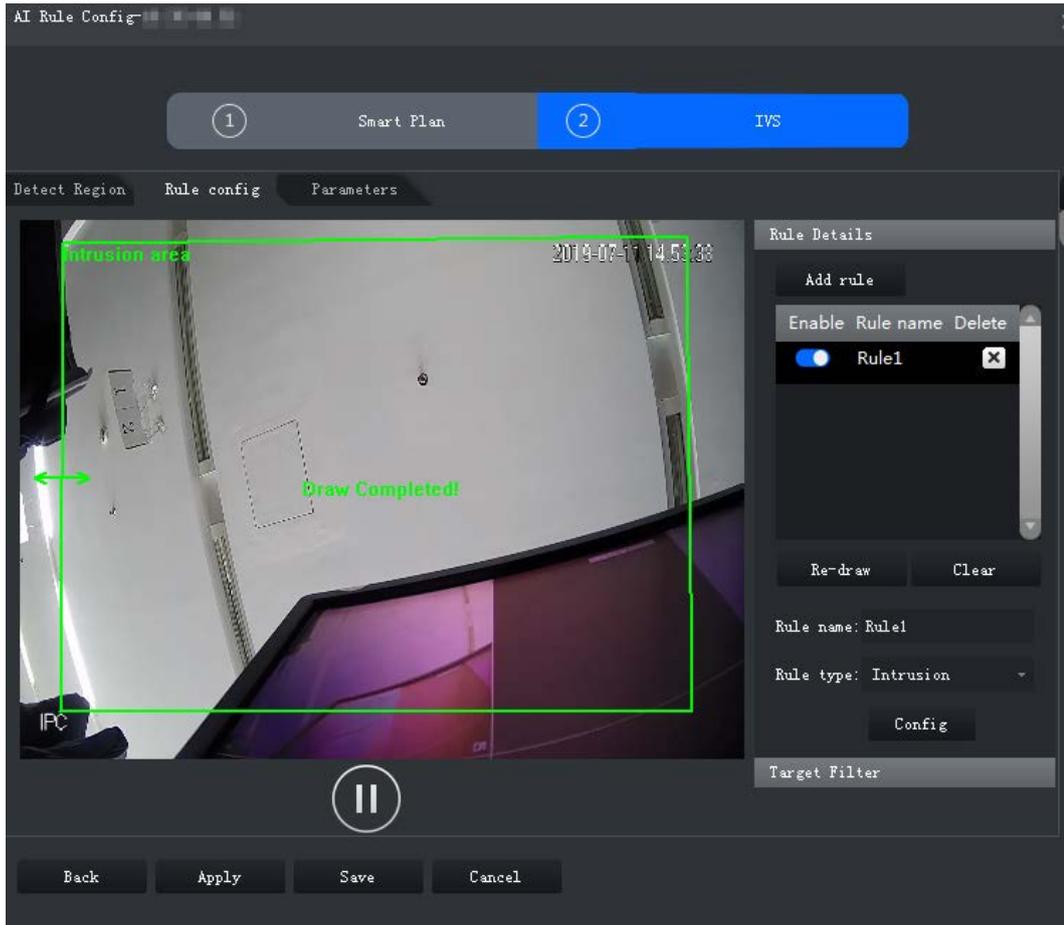
Step 5   Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.2.9.4.1 Tripwire".

Figure 4-64 Set parameters
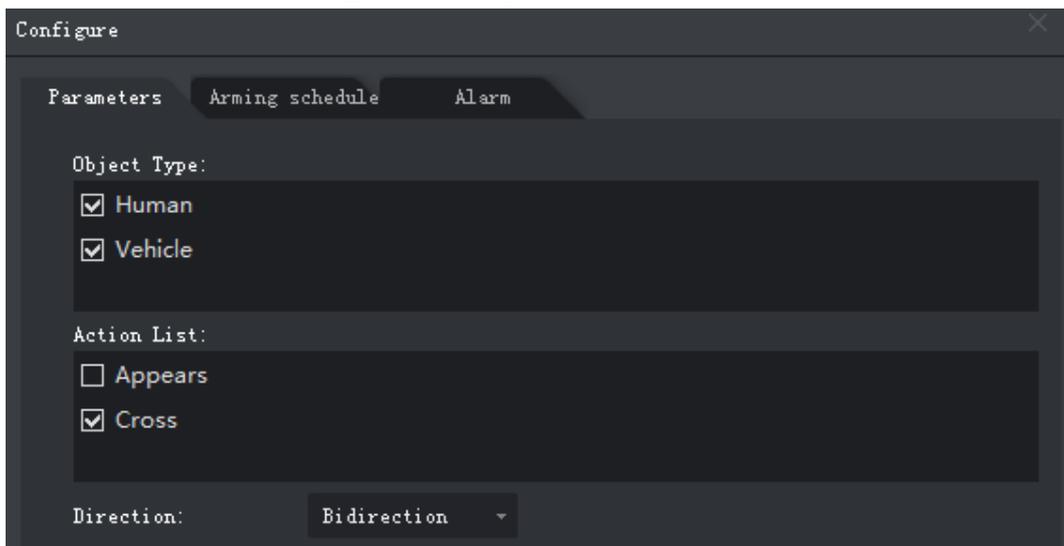
Table 4-18 Parameters

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**.

4.2.9.4.3 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 **IVS** page, click **Rule config**.

Figure 4-65 Rule configuration
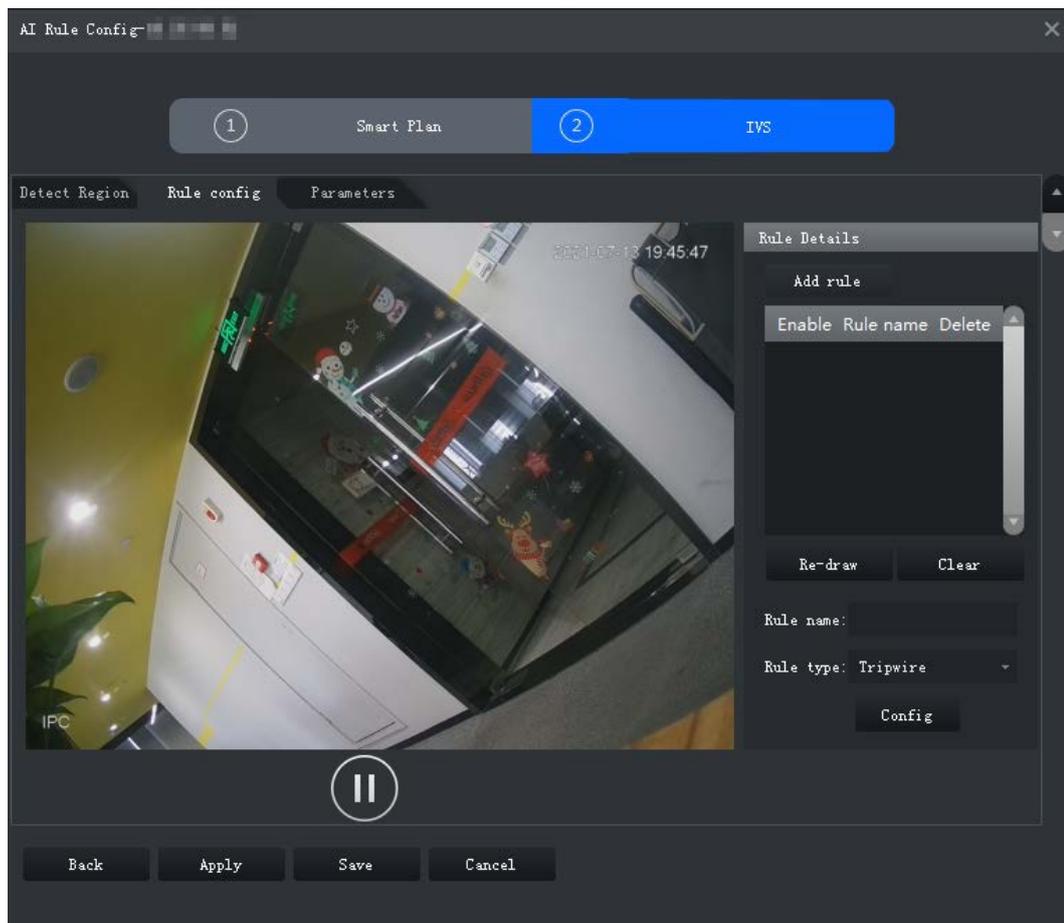
Step 2   Click **Add rule**.

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 4-66 Abandoned Object
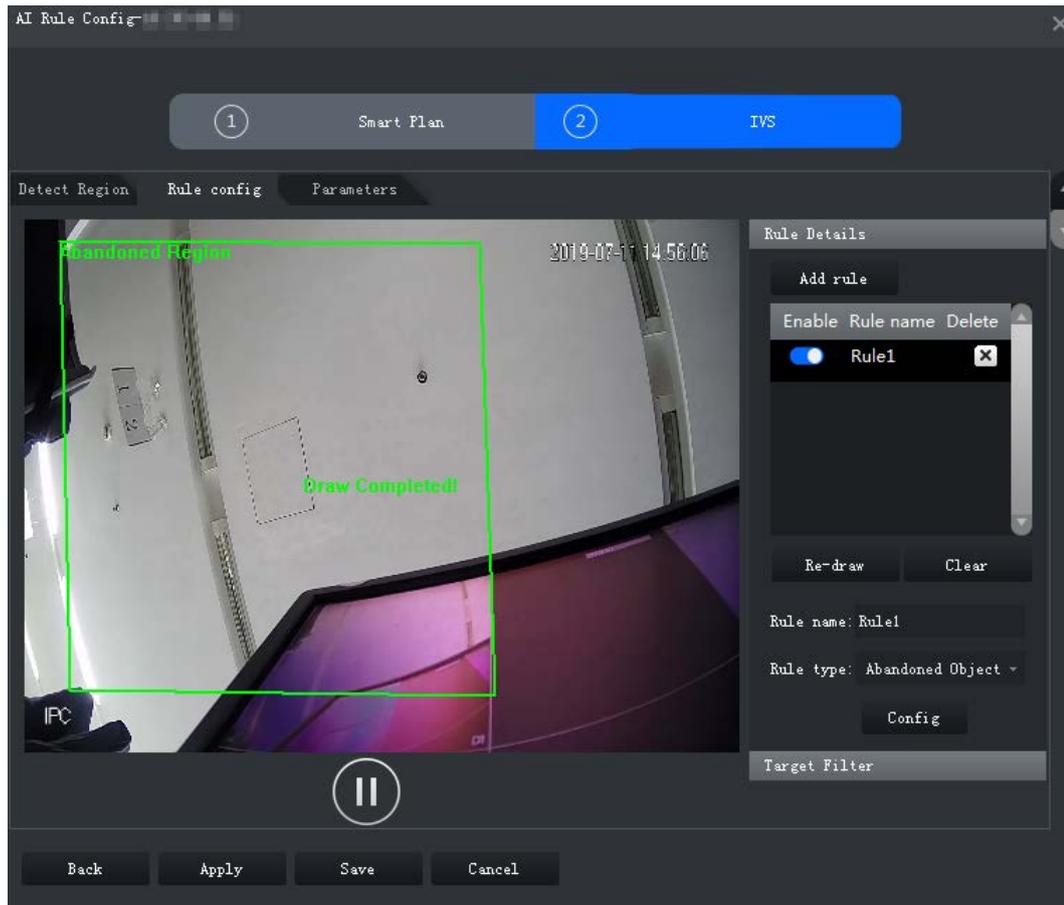
Step 5　　Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.2.9.4.1 Tripwire".

Figure 4-67 Set parameters
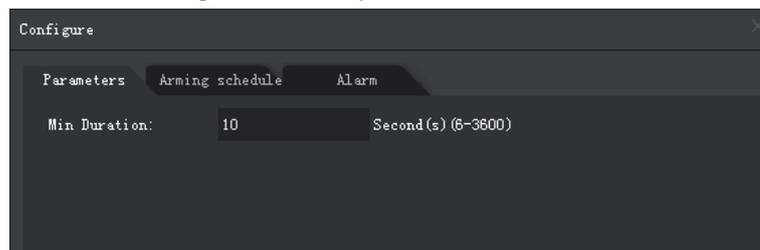
Step 6　　Click **Apply**.

4.2.9.4.4 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 **IVS** page, click **Rule config**.

Figure 4-68 Rule configuration
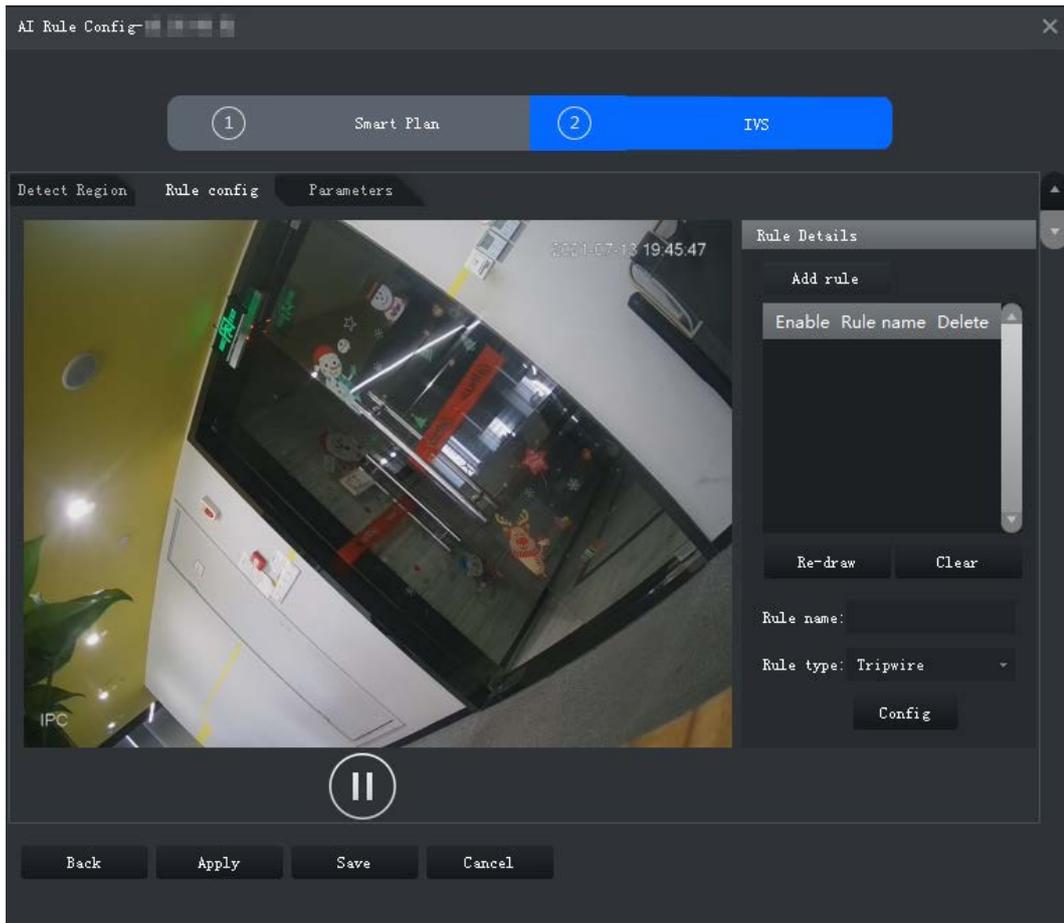
Step 2   Click **Add rule**.

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 4-69 Fast-moving
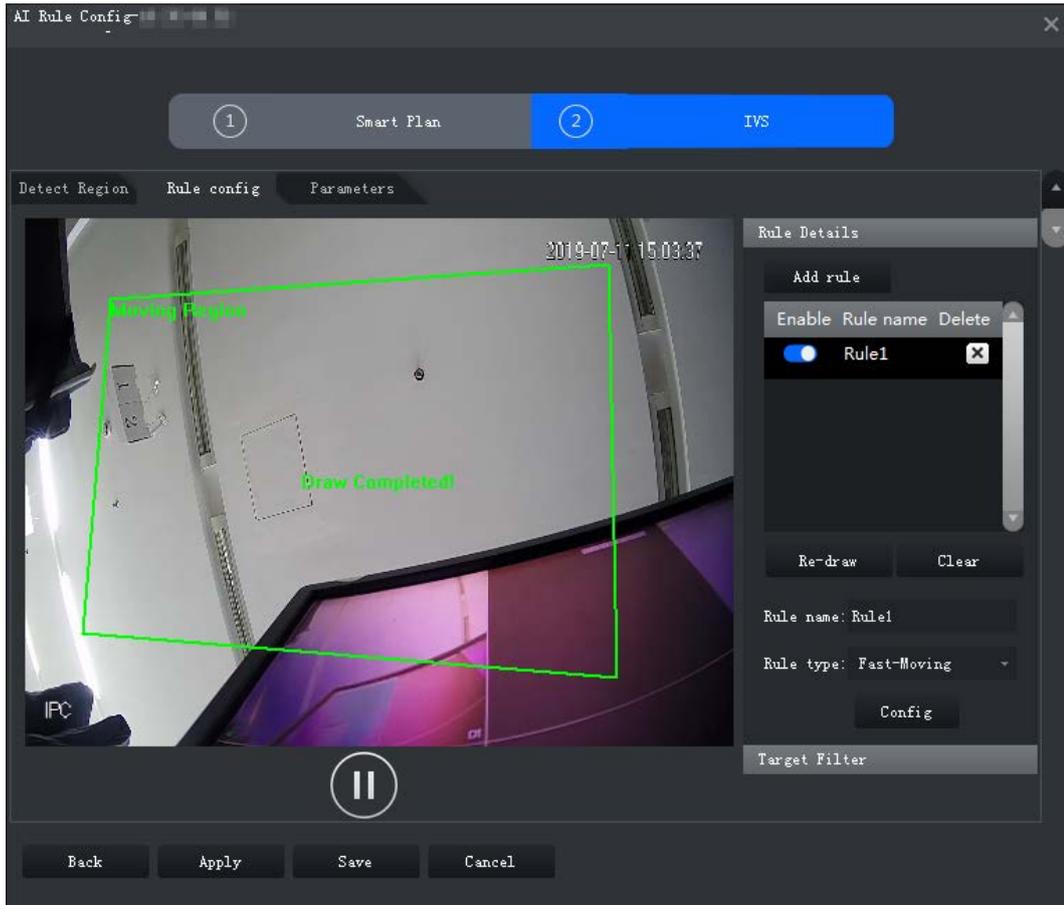
Step 5   Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.2.9.4.1 Tripwire".

Figure 4-70 Set parameters
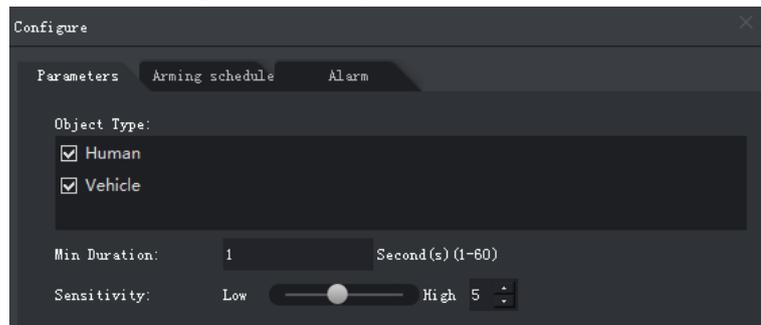
Table 4-19 Parameters

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**.

4.2.9.4.5 Parking Detection

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

Step 1   On the **IVS** page, click **Rule config**.

Figure 4-71 Rule configuration
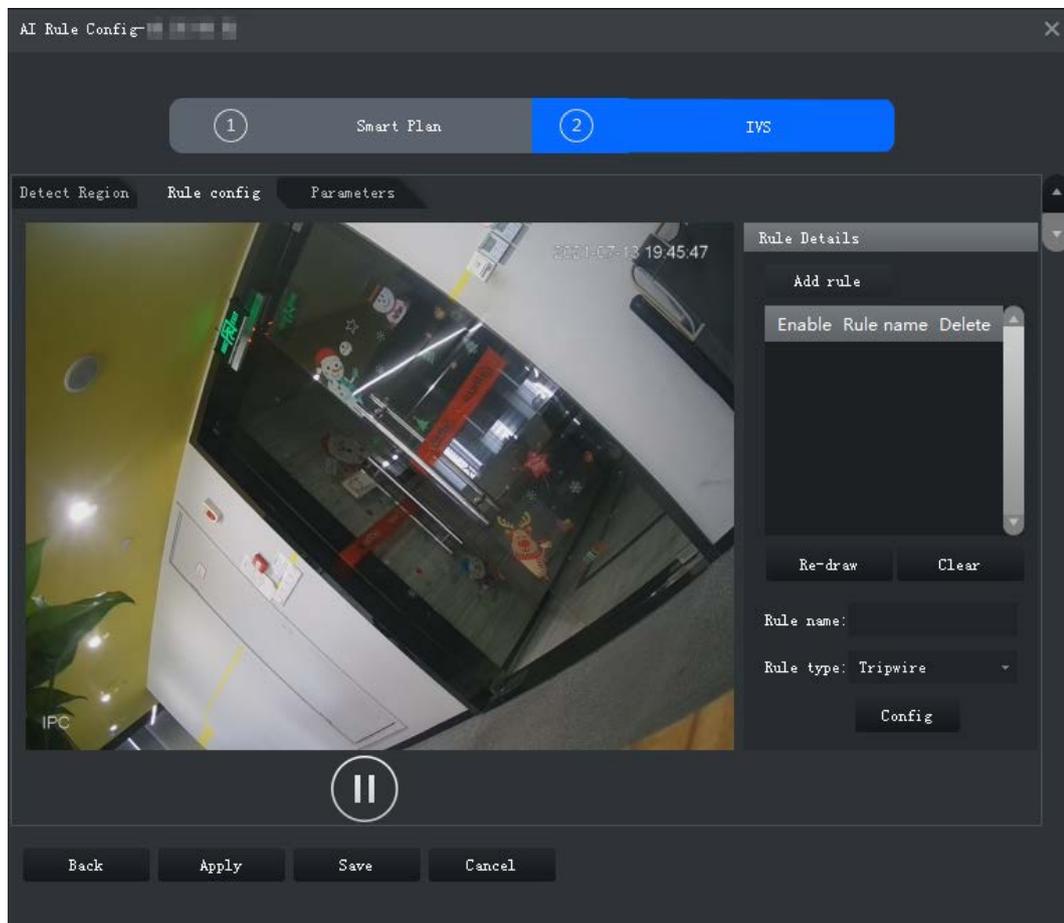
Step 2   Click **Add rule**.

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 4-72 Parking detection
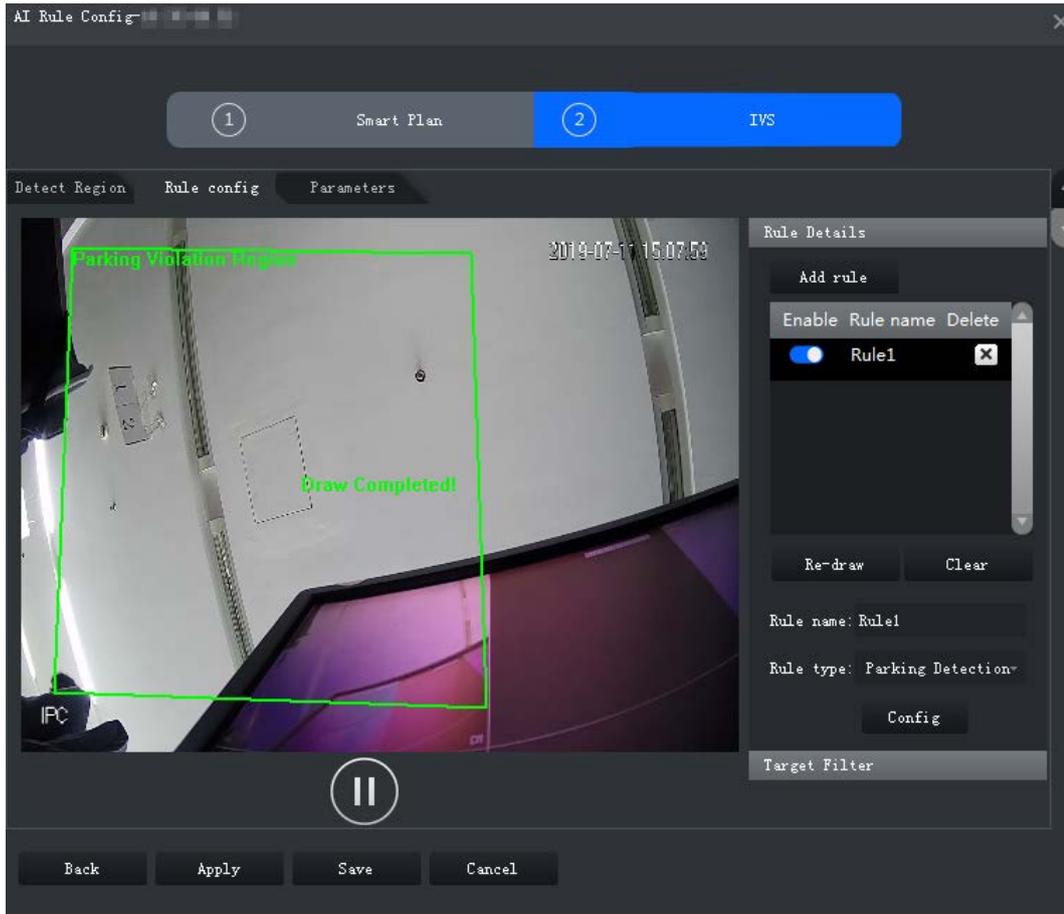
Step 5 Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.2.9.4.1 Tripwire".

Figure 4-73 Set parameters
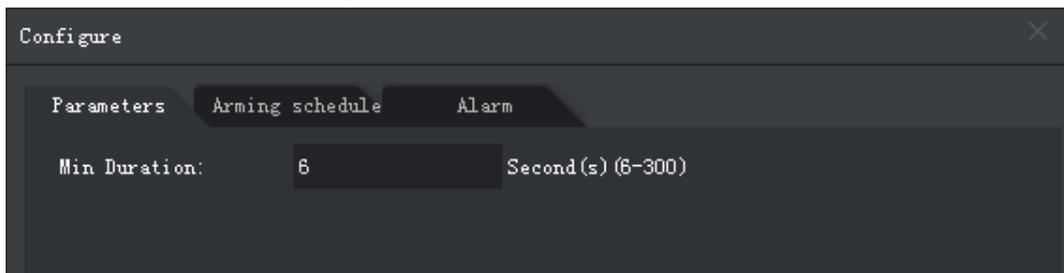
Step 6 Click **Apply**.

4.2.9.4.6 Crowd Gathering

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

Step 1 On the **IVS** page, click **Rule config**.

Figure 4-74 Rule configuration
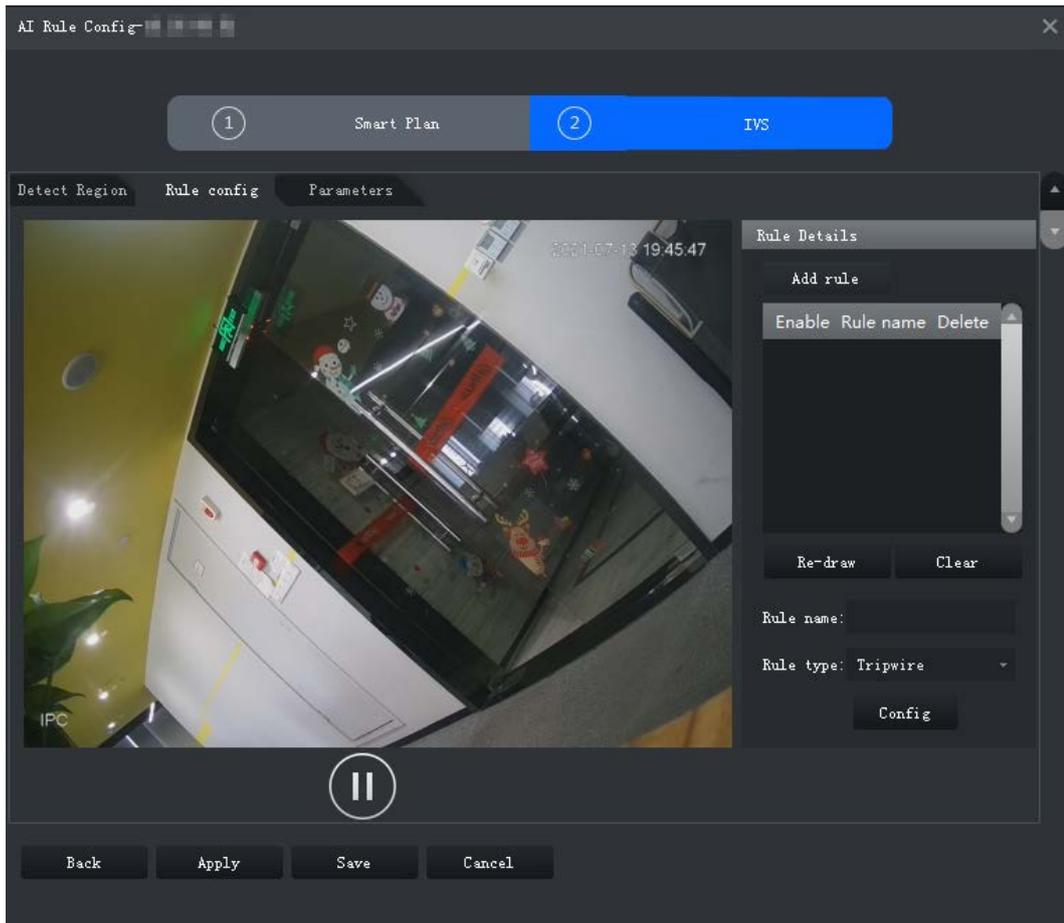
Step 2 Click **Add rule**.

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 4-75 Crowd gathering
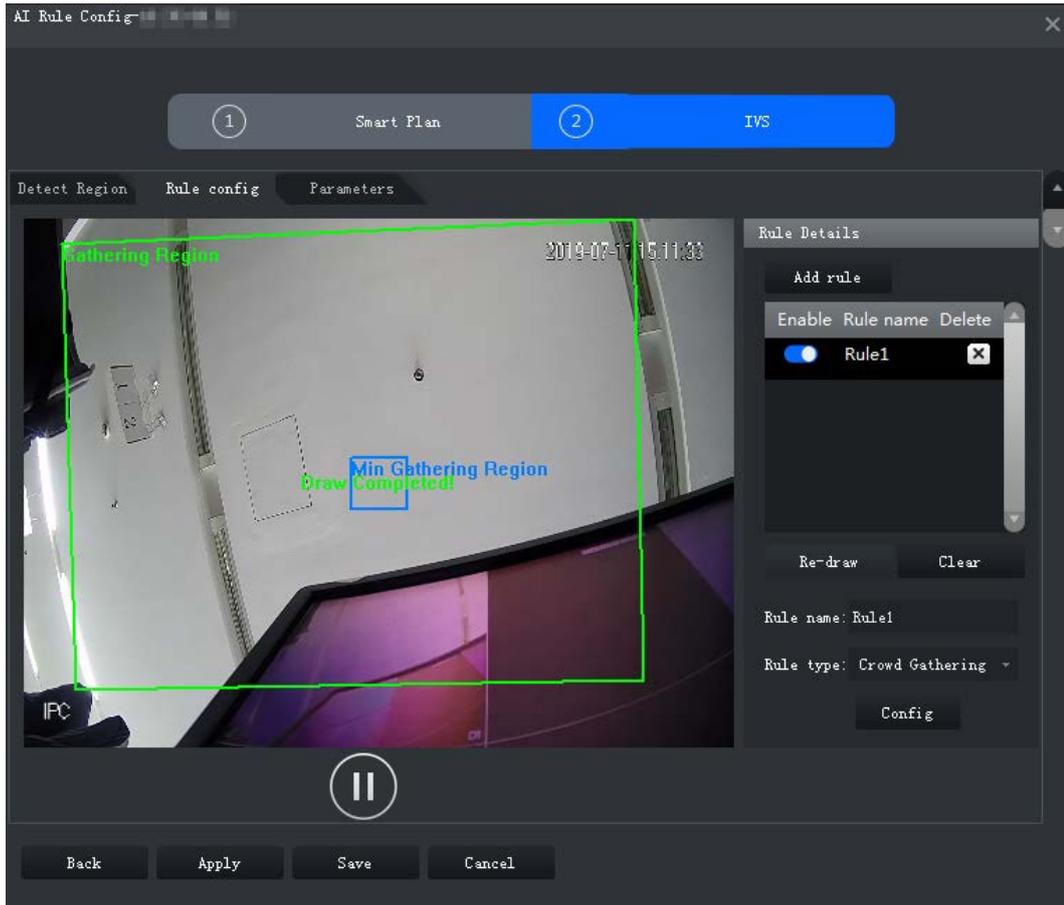
Step 5   Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.2.9.4.1 Tripwire".

Figure 4-76 Set parameters
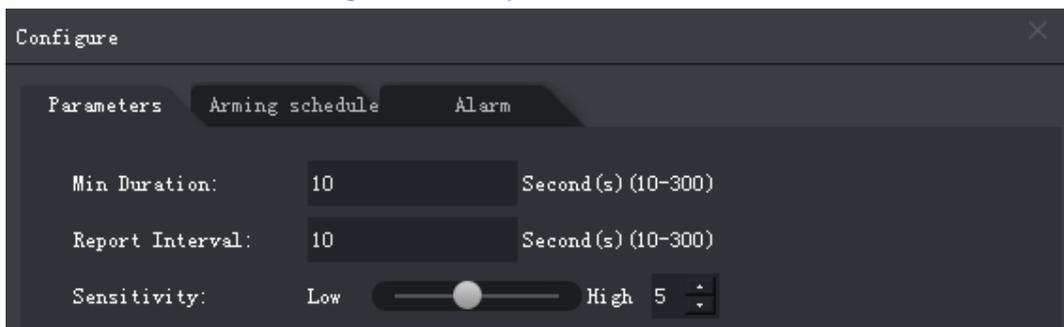
Table 4-20 Parameters

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**.

4.2.9.4.7 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 **IVS** page, click **Rule config**.

Figure 4-77 Rule configuration
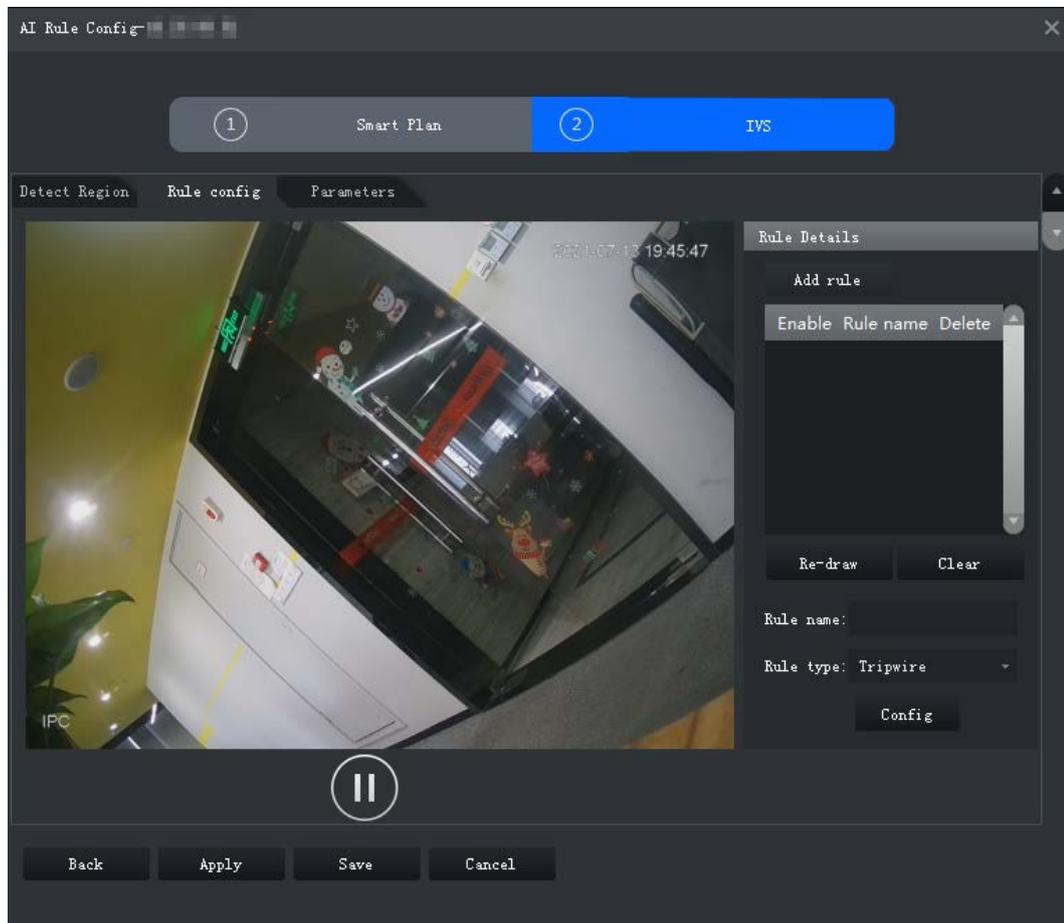
Step 2   Click **Add rule**.

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 4-78 Missing object
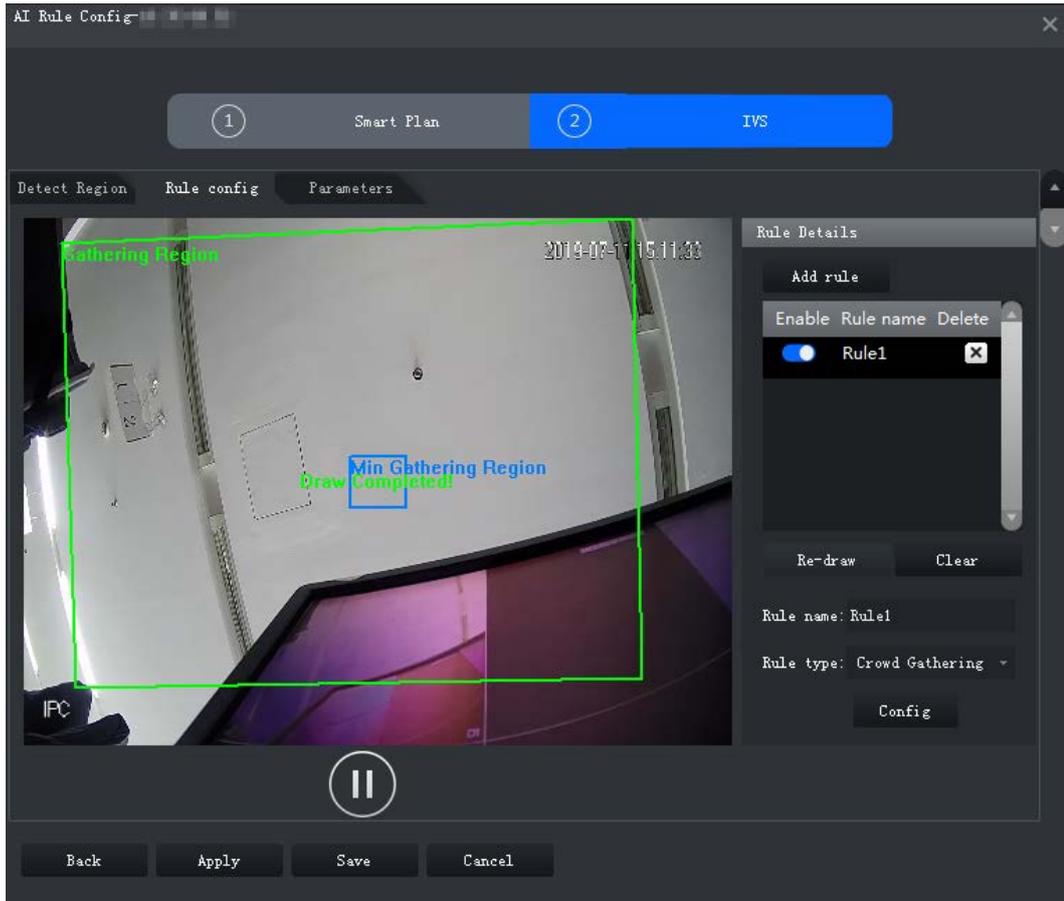
Step 5   Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.2.9.4.1 Tripwire".

Figure 4-79 Set parameters
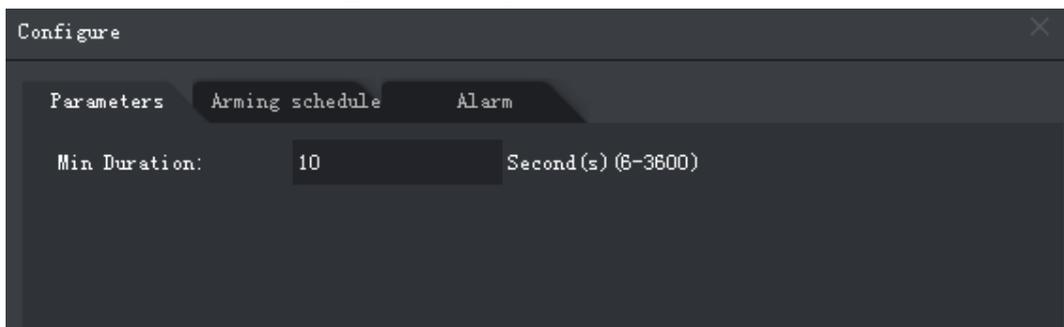
Step 6   Click **Apply**.

4.2.9.4.8 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 **IVS** page, click **Rule config**.

Figure 4-80 Rule configuration
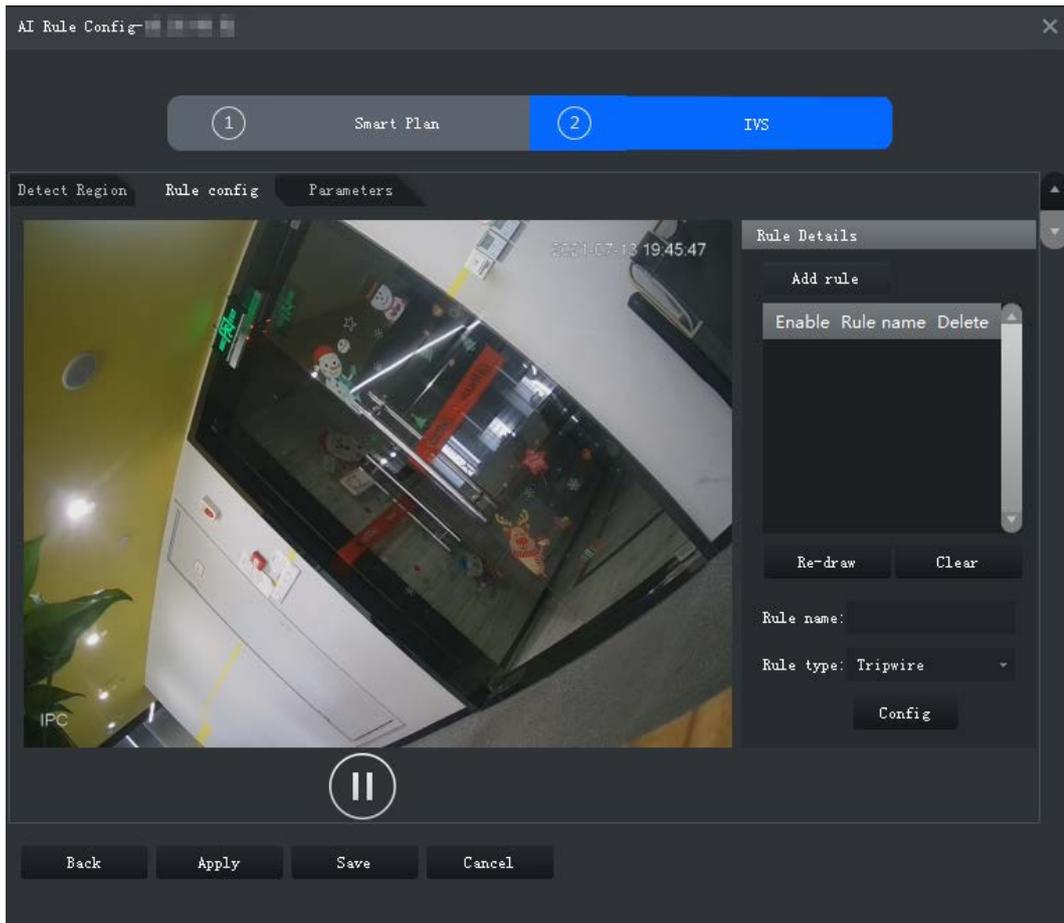
Step 2   Click **Add rule**.

Step 3   Enable rule and modify the name and type.

1) Enable rule. [toggle] 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 4-81 Loitering detection
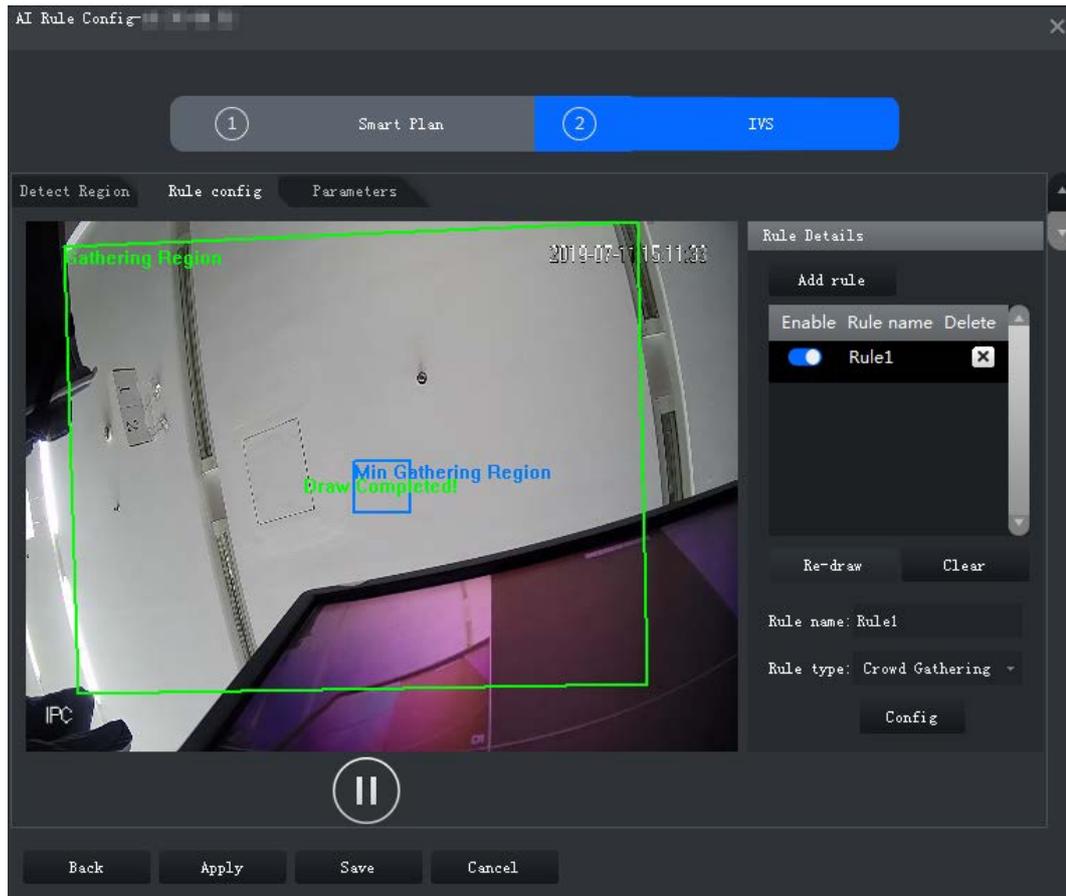
Step 5   Set parameters, arming schedule and alarm linkage. Draw a target-filtering frame. See "4.2.9.4.1 Tripwire".

Figure 4-82 Set parameters
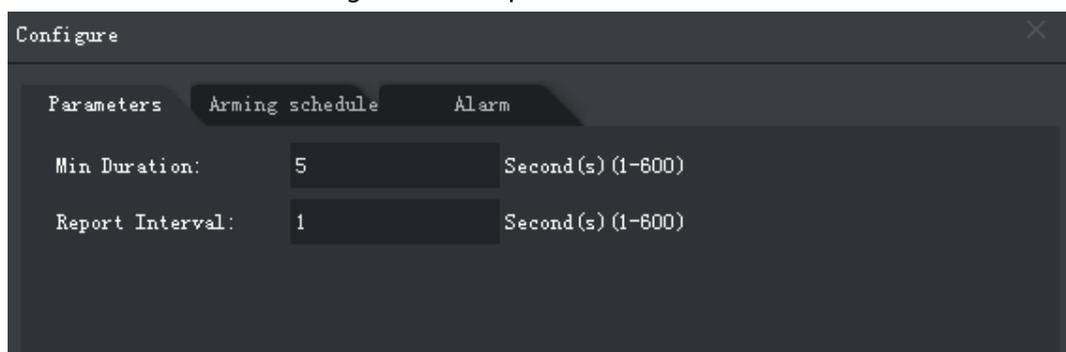
Table 4-21 Parameters

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**.

4.2.9.5 Configuring Parameters

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

Step 1   Log in to the DSS Client. On the **Home** page, 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 4-83 Go to AI rule configuration page
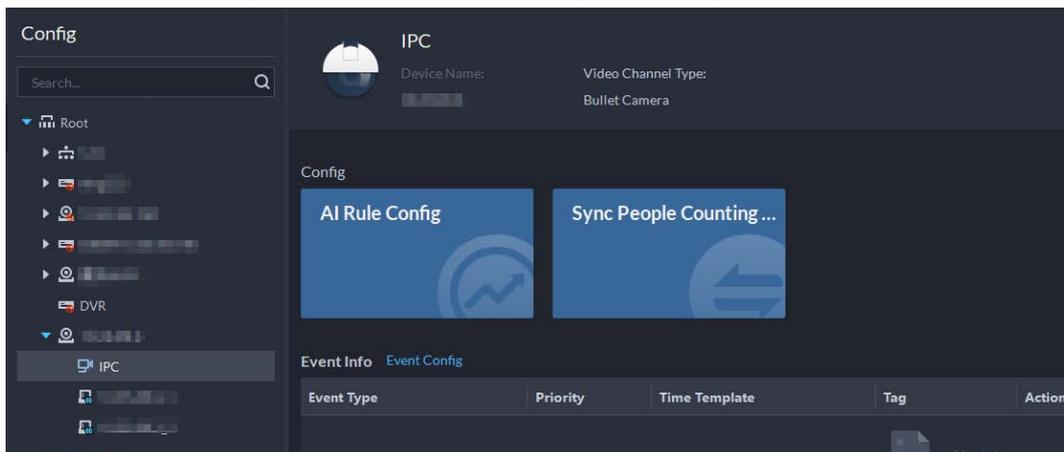
Step 4   After selecting the IVS smart plan in the **Smart Plan** page, click **Next**.

Step 5   Click   twice.

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

Step 7   Set parameters.

Figure 4-84 Parameters
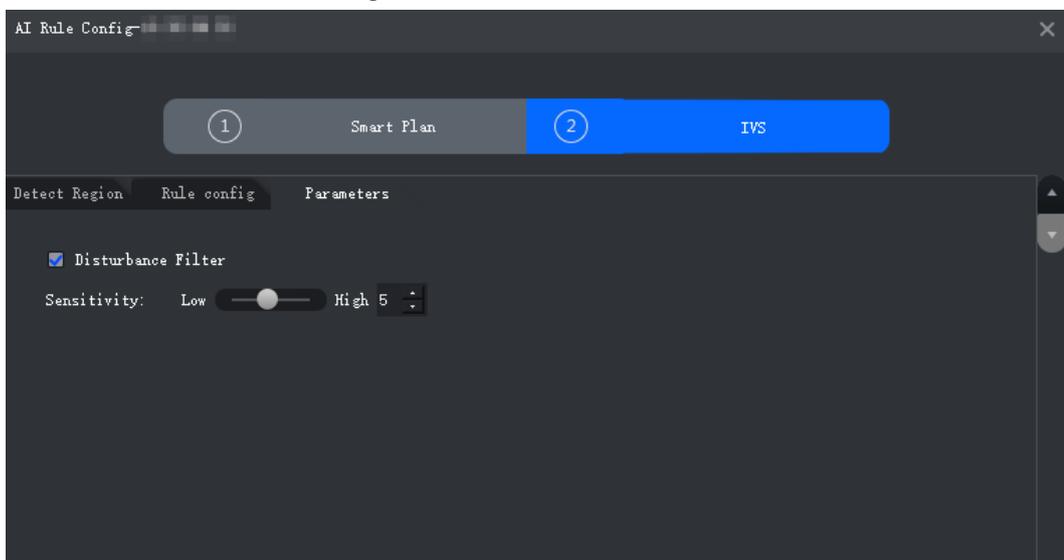
Table 4-22 Parameters

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.

Parameter	Description
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**.

4.2.10 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** page, click ![icon], and then in the **Basic Config** section, select **Device**.

Step 2   Click ![icon].

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

Figure 4-85 Synchronize people counting rules from the device
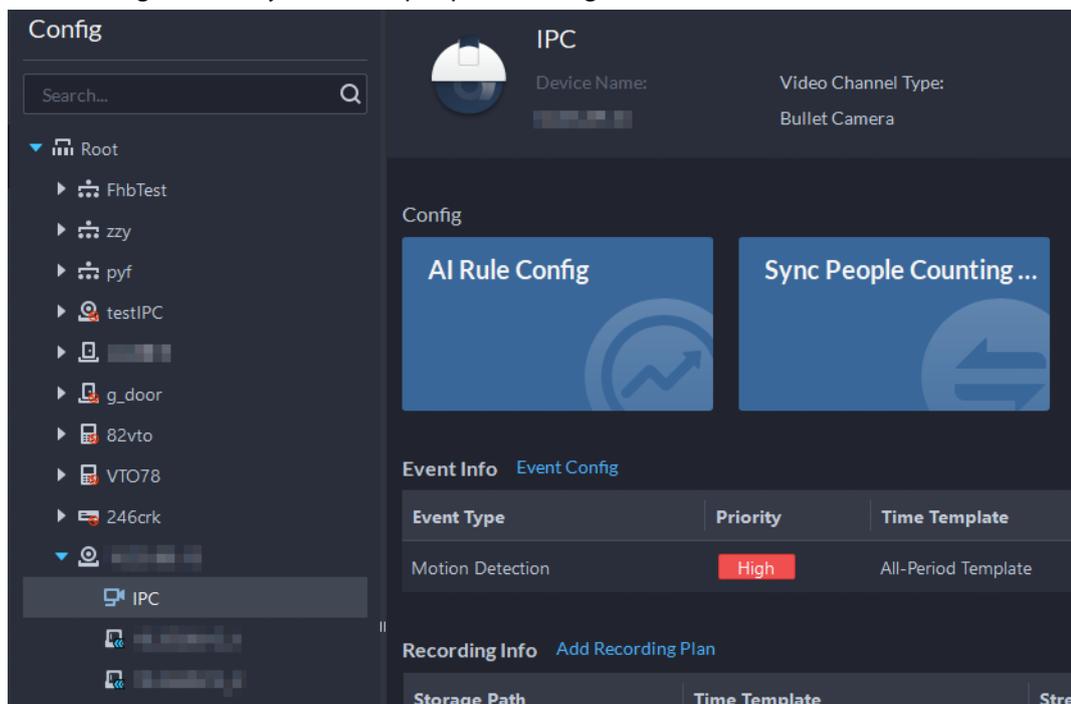
Step 4   Click **Sync Rules**, and then the system prompts **Synchronization Complete**.

Figure 4-86 Synchronize people counting rules from the device
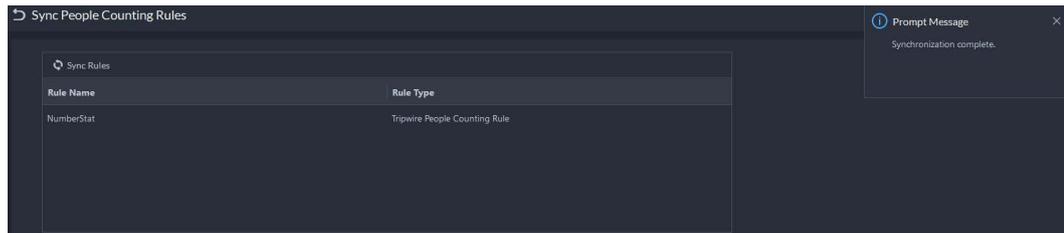
4.3 Adding Role and User

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.

4.3.1 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 restoring. An administrator can create other administrators.
- Common role: A common role that has no permission of authorization, backup and restoring, user management, and storage management.

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **Basic Config** section, select **User**.

Step 2   Click ![icon].

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

Figure 4-87 Add a role
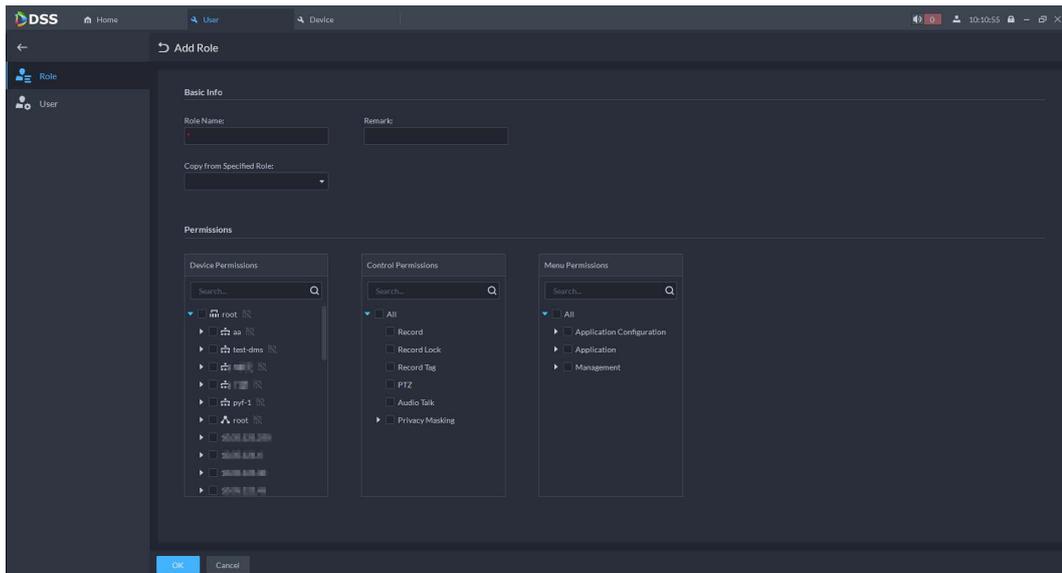
- If a device is not selected under **Device Permissions** or a menu not selected under **Menu Permissions**, all users assigned with this role will not be able to see the device or menu.
- Click 🏢 of a selected organization. All permissions of subsequently added devices under this organization will also be assigned to users of this role.

Step 4 Click **OK**.

4.3.2 Adding User

Create a user account for logging in to the platform.

Procedure

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

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

Table 4-23 Parameter description

Parameter	Description
Username	Used to log in to the client.
Multi-client Login	Allow the user to log in to multiple clients at the same time.
Password	Used to log in to the client.
Confirm Password	
Enable Forced Password Change at First Login	The user is required to change the password at first-time login.
Enable Password Change Interval	Force the user to change the password regularly.

Parameter	Description
Enable Password Expiry Time	The password must be changed after it expires on the defined date.
PTZ Control Permissions	The PTZ control priority of the user. The larger the value, the higher the priority. For example, User A has a priority of 2 and User B has a priority of 3. When they operate on the same PTZ camera at the same time, the PTZ camera will only respond to the operations from User B.
Email Address	Used to reset password and receive alarm emails.
Bind MAC Address	Limit the user to log in from specific computers. One user can be bound to 5 MAC addresses at most.
Role	Select one or more roles to assign the user permissions, such as which devices are allowed to be operated.

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 information of a user except the username.
- Click 🗑 to delete a user.

4.3.3 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.

4.3.3.1 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 4-88 Change password
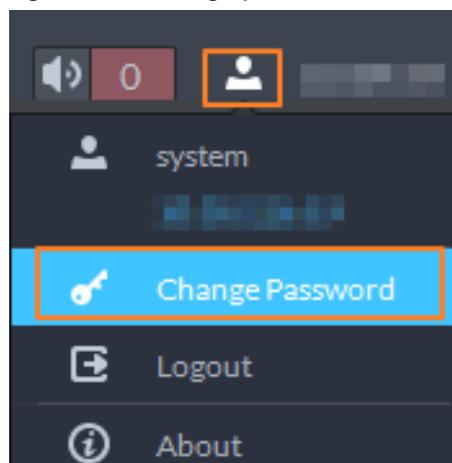
Step 2   Enter the old password, new password, and then confirm the new password. Click **OK**.

4.3.3.2 Changing Offline User Password

Only system user can change offline user password.

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **Basic Config** section, select **User**.

Step 2   Click ![icon].

Step 3   Select a user, and then click ![icon].

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

Figure 4-89 Change user info
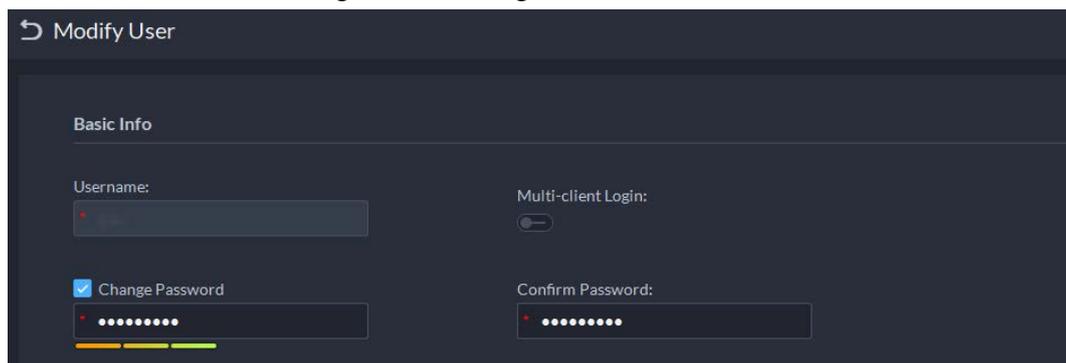
4.3.3.3 Resetting User Password

You can reset the password of a user by security questions or email address, but only the system account supports resetting the password by security questions.

Step 1   On the login page, click **Forgot password?**.

Step 2   Enter the account that you want to reset the password for, and then click **Next Step**.

Step 3   Select how you want to reset the password.

● By security questions. This is only applicable to the system account.

1. Click **Reset Password through Security Questions**.
2. Answer the questions, and then click **Next Step**.

● By email address. This is applicable to all accounts, but an email address must be configured first. For details, see "4.3.2 Adding User".

1. Click **Reset Password through Email Verification**.
2. Click **Send Verification Code**.
3. Enter the verification code that you received from the email address, and then click **Next Step**.

Step 4   Set a new password and confirm it, and then click **Next Step**.

The password has been reset.

4.4 Configuring Storage

Manage the storage of the platform, including adding network disks, setting storage types to store different types of files, and setting the storage location and retention period of the images and recorded videos from devices.

4.4.1 Configuring Network Disk

- The storage server is required to be deployed.
- One user volume of the current network disk can only be used by one server at the same time.
- User volume must be formatted when adding network disk. Check if you have backed up the data.

Procedure

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

Step 2   Select 🌐.

Step 3   Click **Add**.

Step 4   Select server name and mode, enter the IP address of network disk, and click **OK**.
- Normal mode: All volumes of the network disk will be added. Those used by any user will be in red.
- User mode: Enter the username and password of a user. Only volumes of the network disk assigned to this user will be added.

Figure 4-90 Add network disk (normal mode)

Figure 4-91 Add network disk (user mode)

Step 5   Select disk, and then click 🖥 to format the corresponding disk.
1. Select user volume, and then click 🔄.
2. Select format disk type, and then click **OK**.

- **Video**: Stores videos.
- **Image and File**: Stores all types of images.

Figure 4-92 Format disk
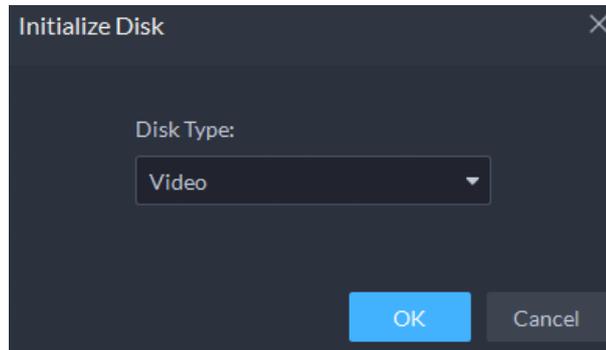
Related Operations

- To configure disk type, click ⚙.
- To format a disk, click 🖳.

📖

Formatting will clear all data on the disk. Please be advised.

4.4.2 Configuring Server Disk

Configure local disk to store different types of files, including videos, ANPR snapshots, and face or alarm snapshots. 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.

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

Step 2   Select 🖫.

Step 3   Format a disk to set a storage type

⚠

This operation will clear all data on the disk. Please be advised.

1) Select user volume, and then click 🔘.

1) Select storage type, and then click **OK**.

- **Video**: Stores videos.
- **Images and Files**: Stores all types of images.

$\square$

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.

Step 4   Manage local disks.

- Initialize disk

  Click ⊙.

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

4.4.3 Configuring Device Storage

When there are a large number of devices on the platform, it will put too much pressure on the local disks because they might produce a lot of images and videos that need to be stored. The platform supports setting the storage location and retention period of the images and videos for storage devices, such as an IVSS, to reduce the pressure on the server.

The types of images include face captures, video metadata, and events.

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

Only organizations with storage devices are displayed.

Step 2   Select an organization, click ⚙ of a device on the right.

Step 3   Configure the parameters, and then click **OK**.

Table 4-24 Parameter description

Parameter	Description
Event Image Storage Location	**Save to Central Storage**: All images produced by the channels connected to this device will be stored on the local disks of the platform. **Link to Images on Device**: All images produced by the channels connected to this device will be stored on the device itself. The platform will obtain images from the device.

Parameter	Description
Event Video Storage Location	• **Save to Central Storage**: All alarm videos produced by the channels connected to this device will be stored on the local disks of the platform. • **Link to Videos on Device**: All alarm videos produced by the channels connected to this device will be stored on the device itself. The platform will obtain videos from the device. 📖 To make sure that alarms videos are complete, we recommend you set a 24-hour recording plan for the device. Otherwise, the platform might not be able to obtain videos. For example, a recording plan of 00:00–14:00 has been configured on the device so that the channels connected to it will record videos during that period. If an alarm is triggered on 14:01, the platform will not be able to obtain videos for this alarm.
Retention Time of Images and Videos on Device	This function is applicable to the images and videos stored on the device. After enabled, the platform will obtain the value from the device, and you can change it to 1–180. The images and videos that have been stored longer than this value will be automatically deleted. ⚠ Deleted files cannot be recovered. Please be advised.

5 Businesses Configuration

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

5.1 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** page, click ![icon], and then in the **App Config** section, select **Event**.

Step 2   Click **Add**.

Figure 5-1 Configure the event source
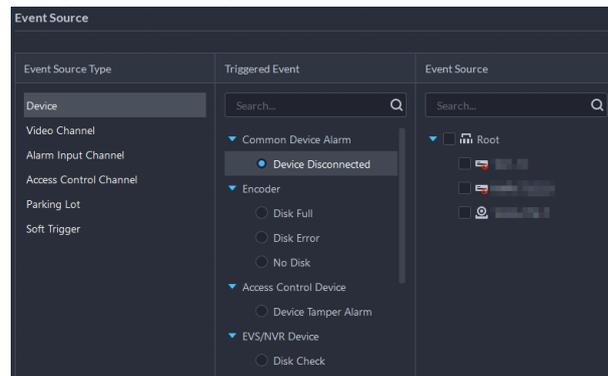
Step 3   Configure the event source.

◫

- 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 "4.2.2.5.1 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 5-2 Manually trigger an alarm by clicking the button
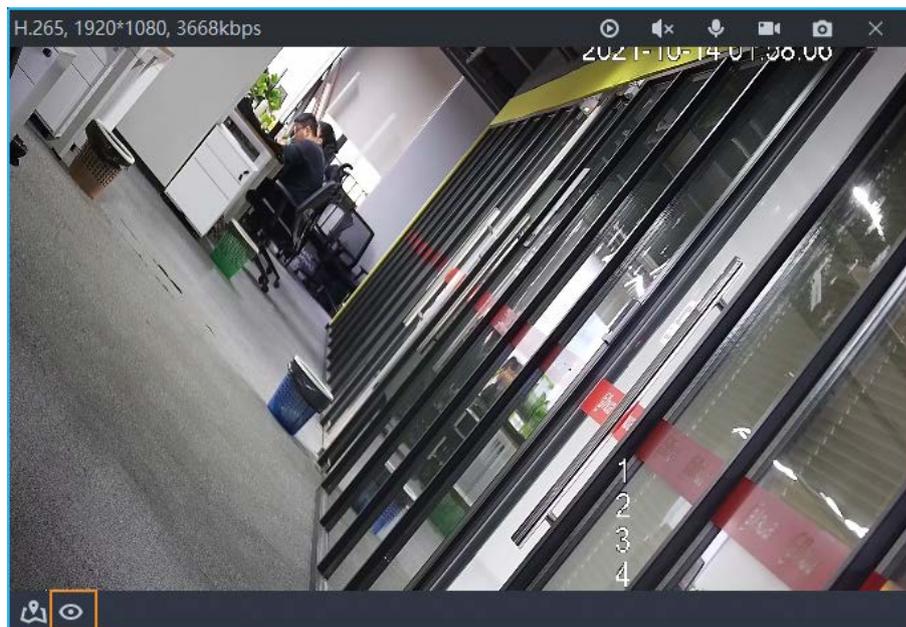
Step 4   Configure parameters under **Event Attribute**.

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

Figure 5-3 Event attributes
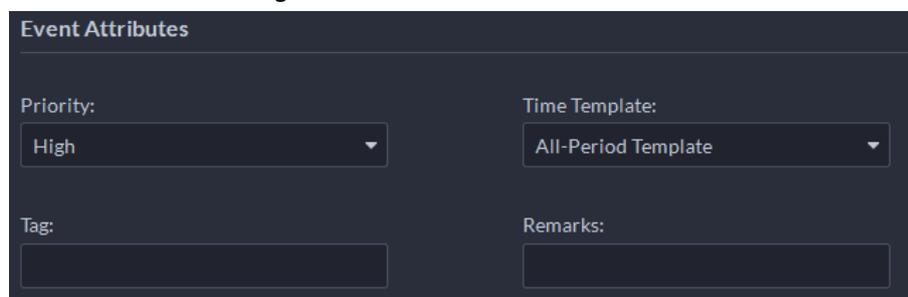
Step 5   Configure alarm linkage actions.

- To link video, enable **Linked Action** > **Link Video**.

Figure 5-4 Link video
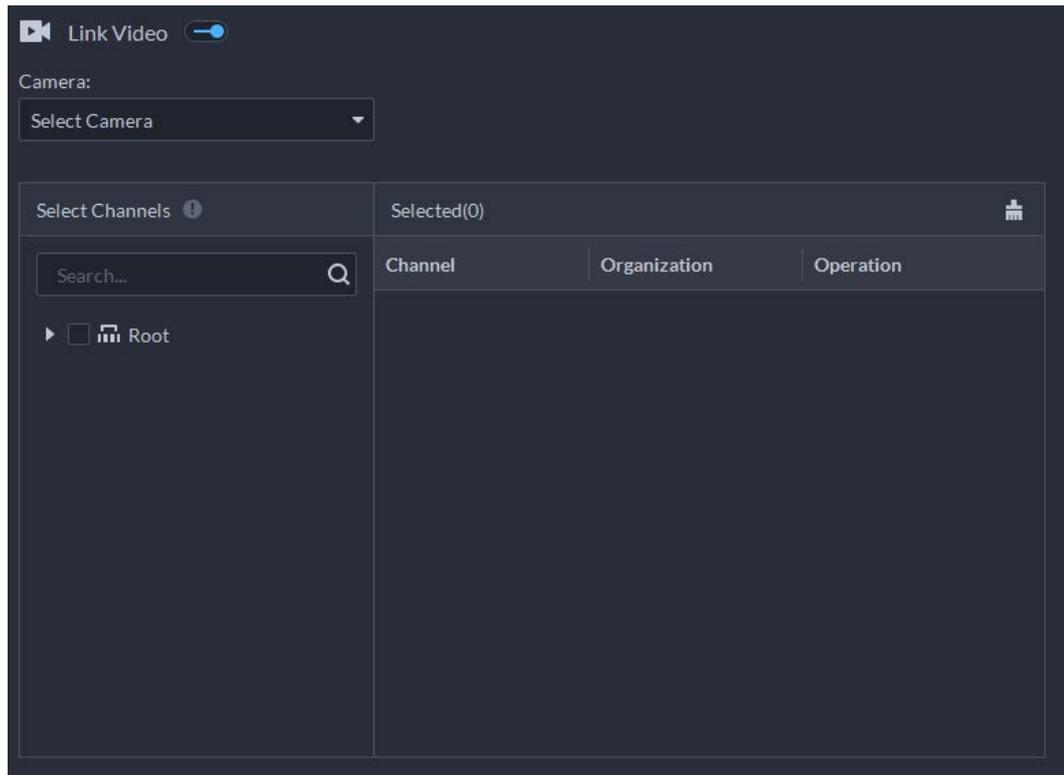
Table 5-1 Parameter description

Parameter	Description
Camera	● Event source: The camera of the alarm itself is linked when the alarm occurs. ● Bound 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 "4.2.3 Binding Resources". ● Select camera: Select a camera so that you can view the camera video when the associated alarm is triggered.
When an alarm is triggered, display camera live view on client	Enable this parameter, and then the platform will open the real-time video of the channel where an alarm is triggered, and play it in the defined stream type. 📖 After the event is configured, you must enable **Open Alarm Linkage Video** and select how the real-time video will be open in alarm settings. For details, see "9.3.4 Configuring Alarm Settings".
Event Recording	Start recording when an alarm is triggered.
Stream Type	Define the stream type of the recorded video. If you select main stream, the recorded video will be in higher quality than sub stream, but it requires more storage.
Recording Time	The duration of the recorded video.

Parameter	Description
Prerecording Time	When there is recorded video that is stored on the device or platform before the alarm is triggered, the platform will take the defined duration of that video, and then add it to the alarm video. 📖 ● If the alarm video is stored on the device, we recommend you configure a 24-hour recording plan to make sure that there is prerecorded content to add to the alarm video. ● If the alarm video is stored on the platform, the platform will record videos and use certain input bandwidth continuously. ● This parameter is not applicable to alarms in parking lots.

● To trigger a snapshot, enable **Trigger Snapshot**.

Select a video channel, and then it will take a snapshot when an alarm is triggered.

Figure 5-5 Trigger a snapshot
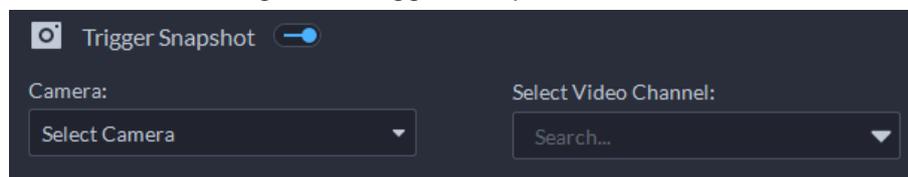
● To link a PTZ action, click **Link PTZ**, and then select the PTZ channels and presets to be linked.

Figure 5-6 Link PTZ
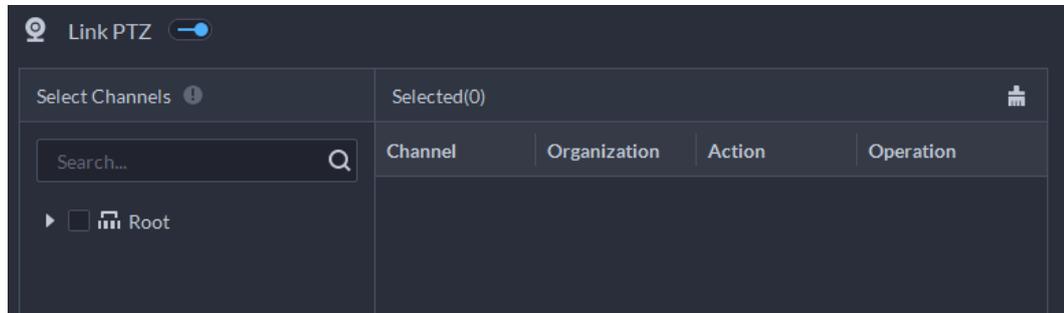
● Click **Alarm Output**, select an alarm output channel, and then set duration.

Figure 5-7 Alarm output
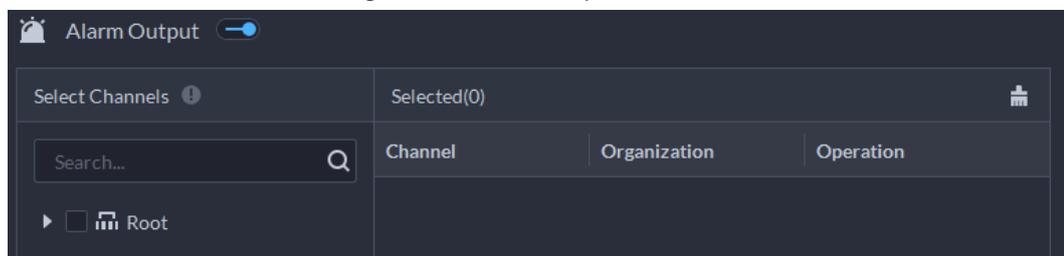
● To link audio and light, click **Link Audio and Light**, select the audio and light channels, and then select the action duration.

Figure 5-8 Link audio and light
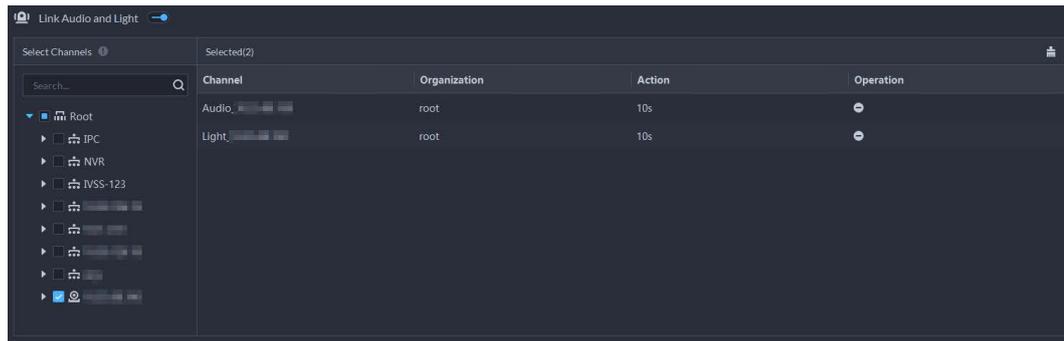
- Click **Link Access Control Device**, select access control channels, and then select a linked action.

Figure 5-9 Link access control device
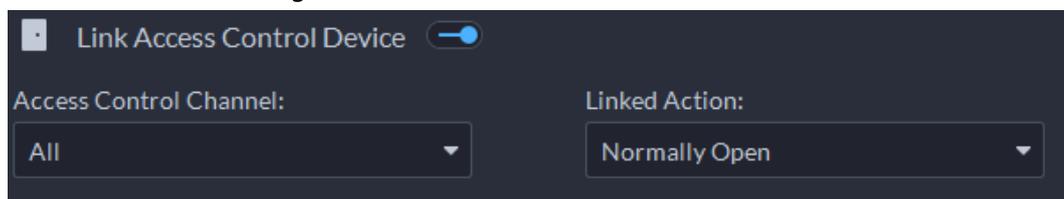
- To play alarm video on the video wall, click **Link Video Wall**, select a camera on the left of the page, and then select a video wall window on the right of the page.

📖

Make sure that you have added decoders to the platform, configured video wall and set alarm window.

- To execute an HTTP URL; command, click **Link HTTP URL Command**. Click **Add**, and then configure its request method, HTTP URL, and remarks. You can click [icon] to test if the command is valid.

Figure 5-10 Link HTTP URL command
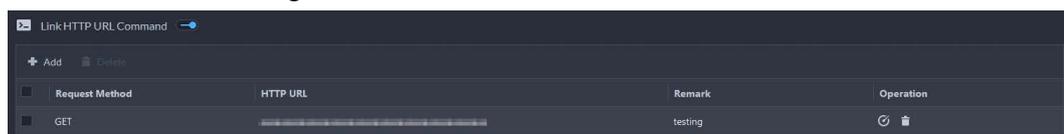
- To link emails, enable **Email**, and click [icon] to add the email address, and then an email will be sent to the selected email address when an alarm is triggered.

Figure 5-11 Link email
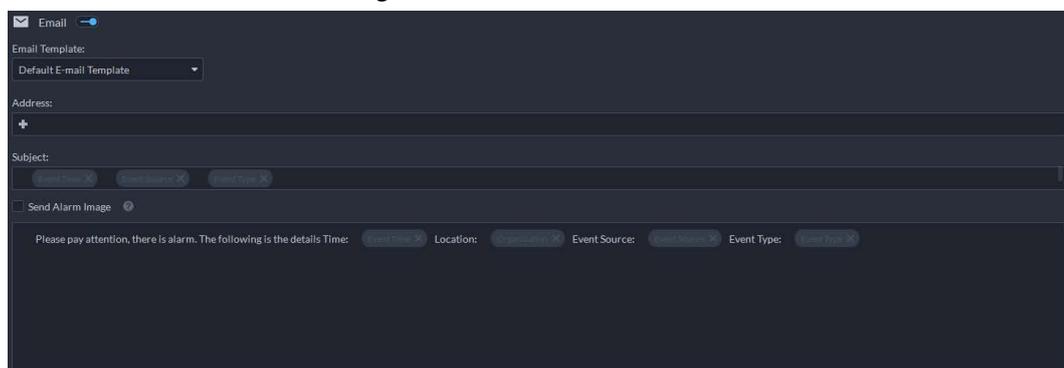
To configure the email template, select **Add Email Template** from the **Email Template** drop-down list.

Figure 5-12 Email template
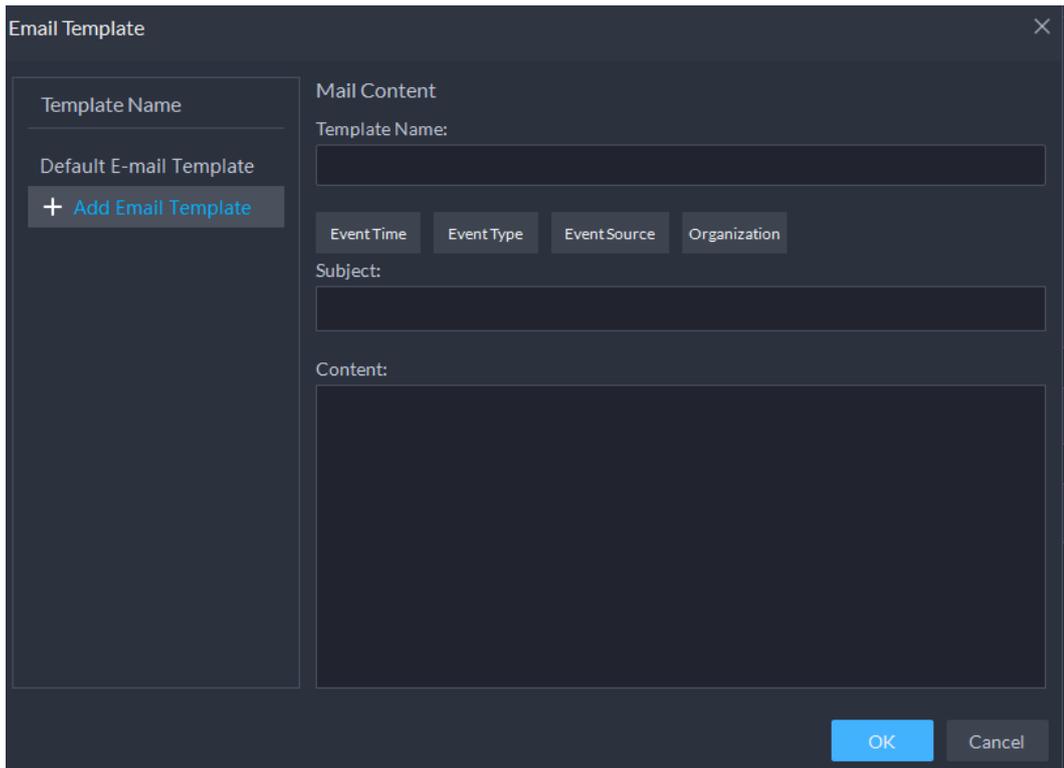
- Apply an alarm protocol to help users process alarms when they are triggered . Click **Alarm Protocol**, and then select a protocol from the **Protocol Template** drop-down list.

Figure 5-13 Alarm protocol
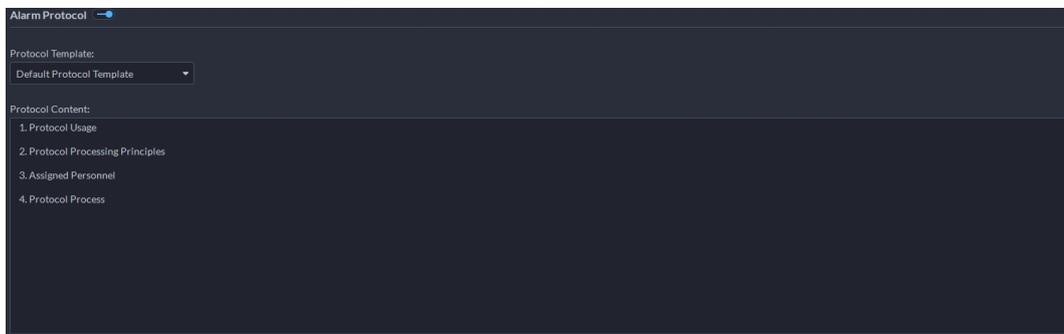
Click **Add protocol template** to create a new protocol; click ✎ to edit the content of a protocol.

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

Figure 5-14 Notify user
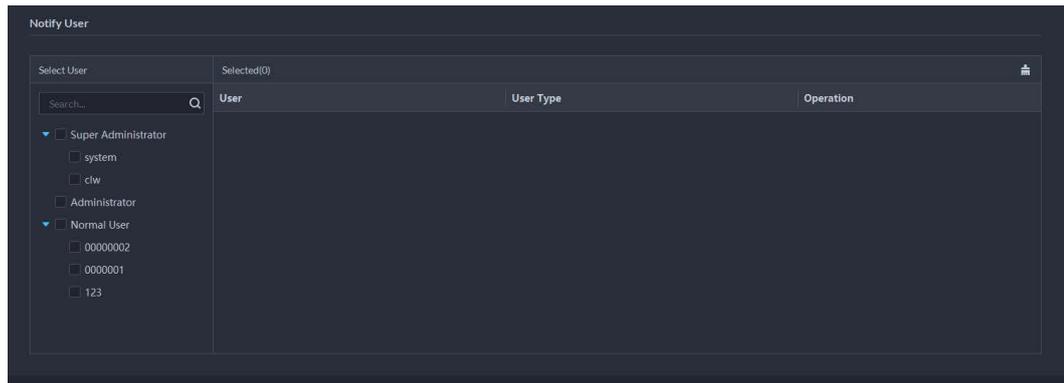
Related Operations

- To edit an event, click ![edit icon].
- To delete an event, click ![delete icon].
- To disable an event, click ![toggle icon].

5.2 Configuring Map

5.2.1 Preparations

- Devices are deployed. For details, see device user's manuals.
- Basic configurations of the platform have been finished. For details, see "4 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**.

5.2.2 Adding Map

Using a picture of a map, you can add cameras, access control channels, and alarm channels on it so that you can conveniently know where they are.

Procedure

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **App 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 5-15 Add main map
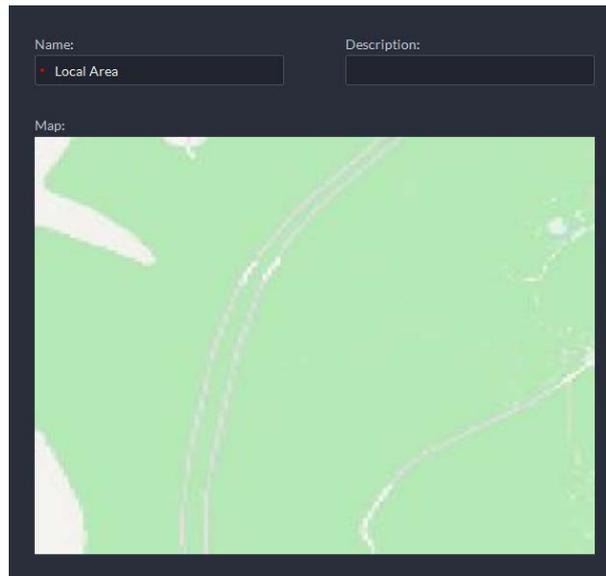
Step 4   Add a sub map.

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

- Hide Device Name

  Only display the icons of devices.

- Delete resources

  To delete a device from the map, click it and then click **Delete Device**.

- Show device

  Select which type of resources you want to display on the map.

- 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 Sub-map

  To add a sub map on the current map, click **Add Sub Map**, click on the map to locate it, enter a name, upload a 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.

5.2.3 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** page, click ![icon], and then in the **App Config** section, select **Map**.

Step 2 Click the map.

Figure 5-16 Map
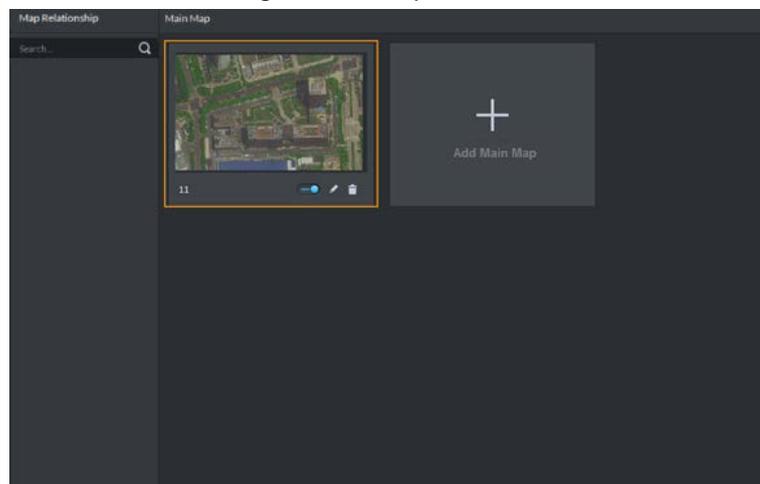
Step 3 Drag the device channel from the left device tree to the corresponding location of the map.

5.3 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.

5.3.1 Configuring Personnel Information

Figure 5-17 Personnel management
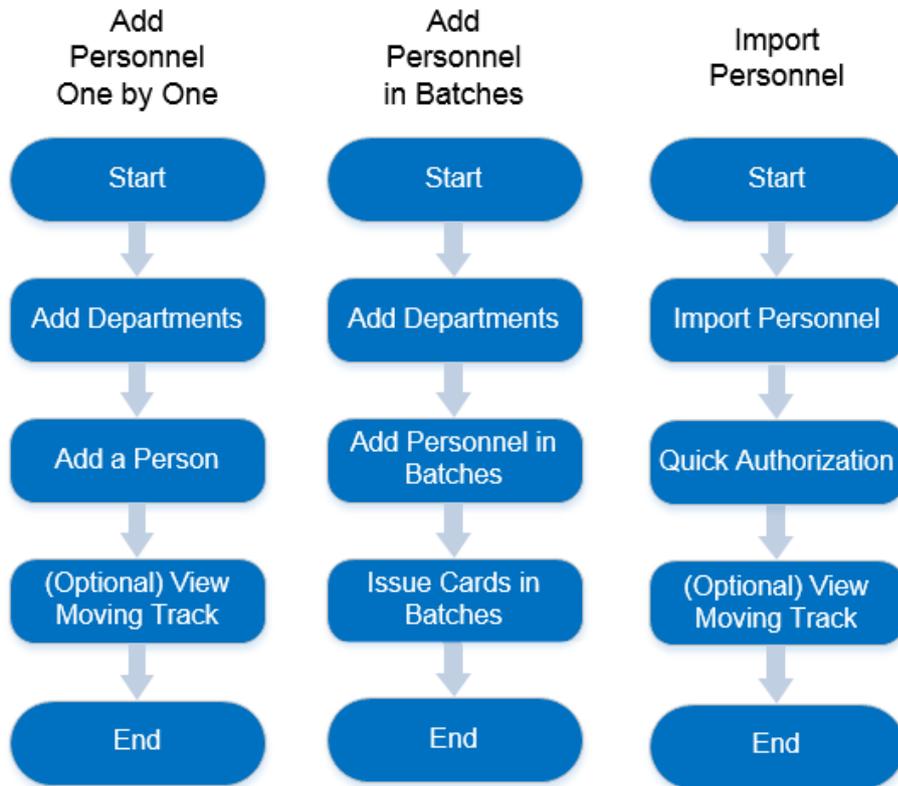
5.3.1.1 Adding Person Group

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

Procedure

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

Step 2 Click .

Step 3 Click .

Figure 5-18 Added person group (1)
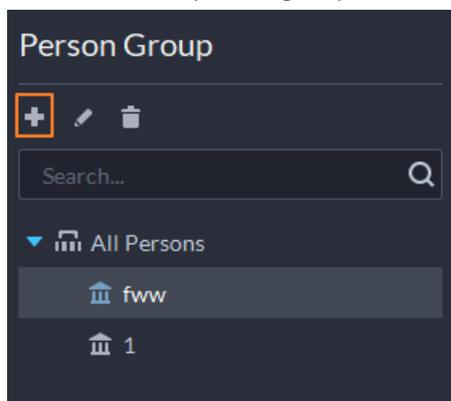
Step 4 Enter person group name and click **OK**.

Figure 5-19 Added person group (2)
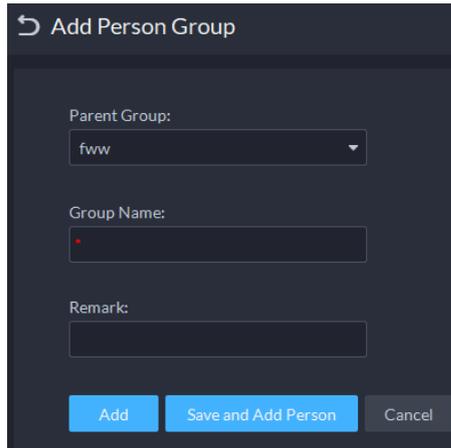
Related Operations

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

5.3.1.2 Adding Personnel

Add people to the platform and grant them access to different access control devices, entrance and exits permissions, and more.

📖

To collect fingerprints or card number, connect a fingerprint collector or card reader first.

5.3.1.2.1 Adding a Person

Procedure

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **App Config** section, select **Personal and Vehicle Info**.

Step 2   Click ![icon].

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.

           📖

        ●   You can upload 2 pictures or take 2 snapshots.

        ●   Click ![icon] on the **Snapshot** page, and then you can select camera, pixel format, resolution, and image quality. These settings are 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 5-20 Personnel information

📖

Only certain devices support the second picture or snapshot. The second picture or snapshot can be the person's face being blocked, such as wearing a mask or a hat.

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.
- **Homeowner**: When several people live in one apartment, you can set one of them as the homeowner.

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

Figure 5-21 Authentication Info
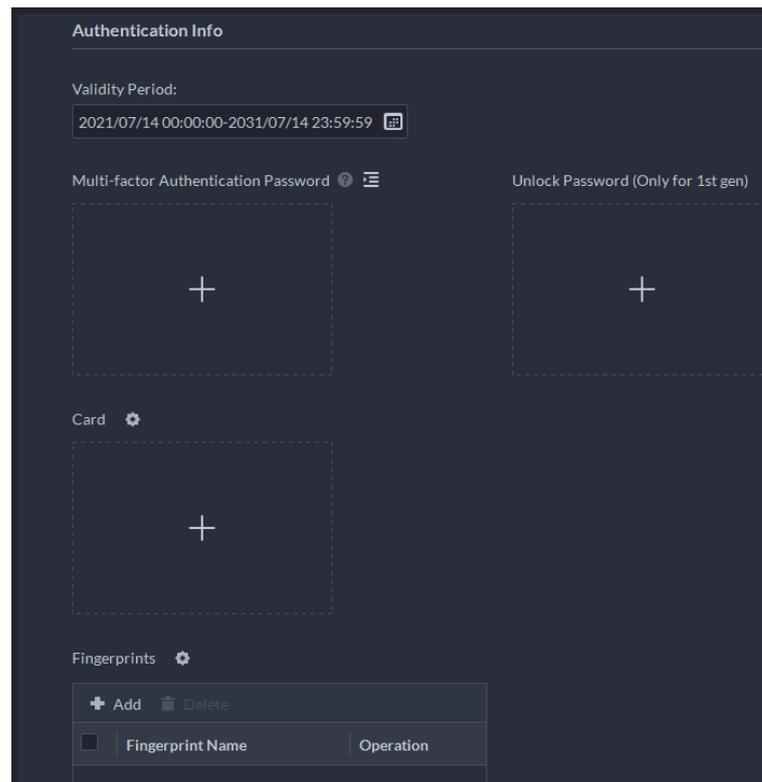
1) Configure effective periods, within which the face, card, password, and fingerprint are effective.
2) When access controllers are added and passwords are required to unlock the door, configure the password first.
   ● A multi-factor authentication password must be used with a card, person ID, or fingerprint to unlock the door. It is only applicable to second-generation access control devices.
   ● Click ▤ and you can set up an unlock password that can be used to directly unlock the door. It is only applicable to first-generation access control devices.

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. or by 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 a card through a card issuer or a device with a card reader.
   1. Click 🔧 next to **Card**, select a card issuer or a reader of a device, and then click **OK**.

Figure 5-22 Card reader manager
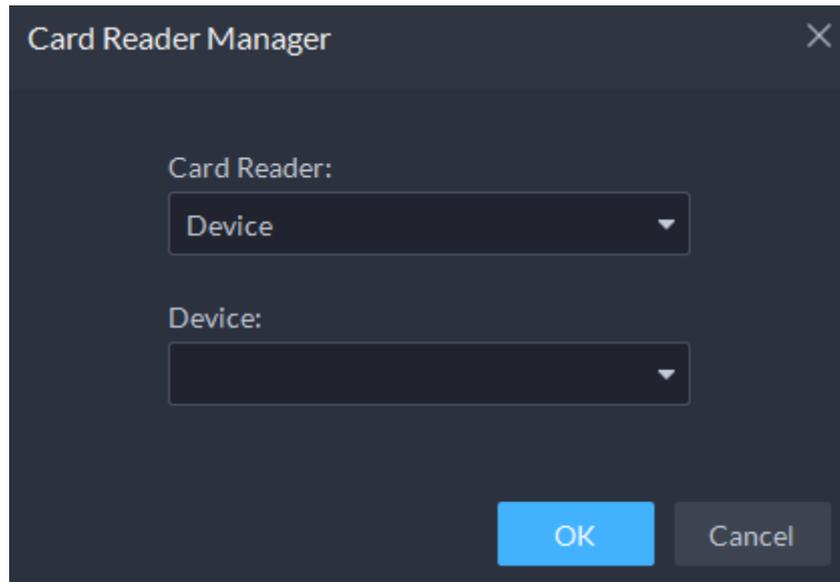
2. Click ![icon], swipe a card on the device you select, the card number will be recognized and displayed.

3. Click ![icon].

- Manually enter the card number.

  Click ![icon], enter card number, and then click ![icon].

Figure 5-23 Reader manager
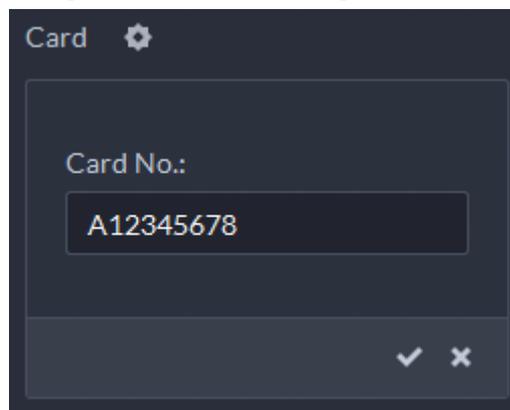
Table 5-2 Card operations

Icon	Description
![icon]	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 ![icon] on an added card, the icon turns into ![icon], which indicates that the card is a main card.
![icon]	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 ![icon], and ![icon] is displayed at upper right, which indicates that the card is set as a duress card. To cancel the duress setting, click ![icon].
![icon]	Change card for the person when the current card does not work.
![icon]	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**.

3) Select a fingerprint collector from the **Fingerprint Collector** drop-down list, and then click **OK**.

4) Click **Add**

Figure 5-24 A collected fingerprint
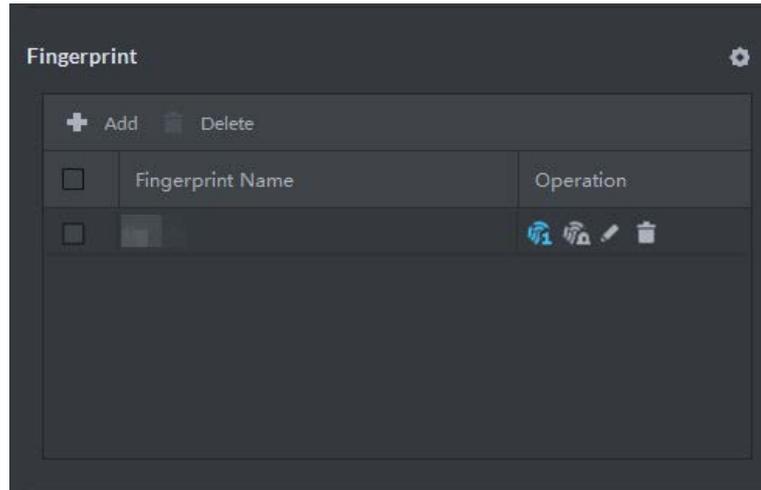
Table 5-3 Fingerprint operations

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 5-25 Add vehicle information

Step 11   If the person needs 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 page 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 "5.4.1.1 Creating Face Comparison Group".

Figure 5-26 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.

User's Manual

Figure 5-27 Face comparison
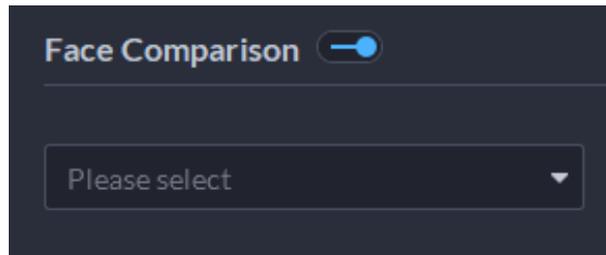
You need to create a face comparison group first.

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

1) Click [icon] next to **Vehicle Group**.

2) Enable **Parking Space Available** and configure the number of the parking space for the vehicle owner.

3) Click **Add** to select a vehicle of the person, and then select which vehicle group it belongs to, and for how long it has permission to park in the parking lot.

Figure 5-28 Vehicle group
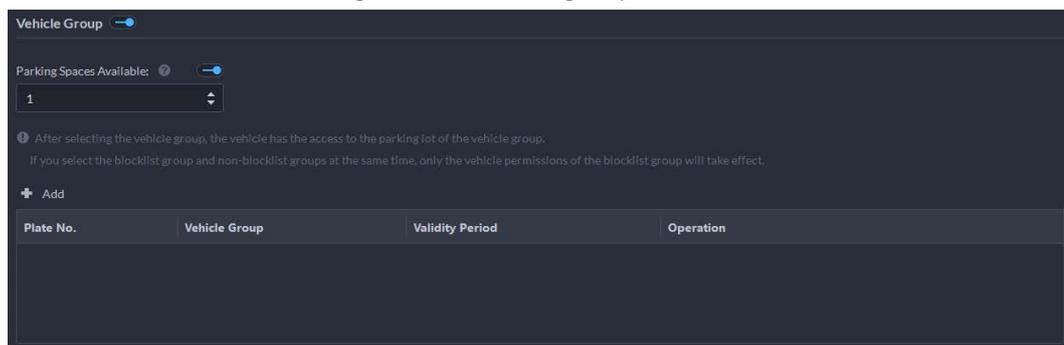
Step 14 Click **OK**.

To delete a person, you can select the person, and then click [icon] ; 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 [icon] .
- To delete a person:
  ◇ Click [icon] to delete a person and associated permissions.
  ◇ Select multiple people, and then click **Delete** to delete them and their permissions.
  ◇ Click **Delete All** to delete all the people and their permissions in the group.
- To view authorization exception, click [icon] .
- To search for a person, enter key words in the [icon] .

5.3.1.2.2 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.

Prerequisites

Prepare an .xlsx file that includes the information of the people you want to import, their face images (optional), and then compress them into a zip file. The .xlsx file can include information of up to 5,000 people. The zip file cannot be larger than 1 GB.

Procedure

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

Step 2   Click 👤≡.

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

Figure 5-29 Import personnel information
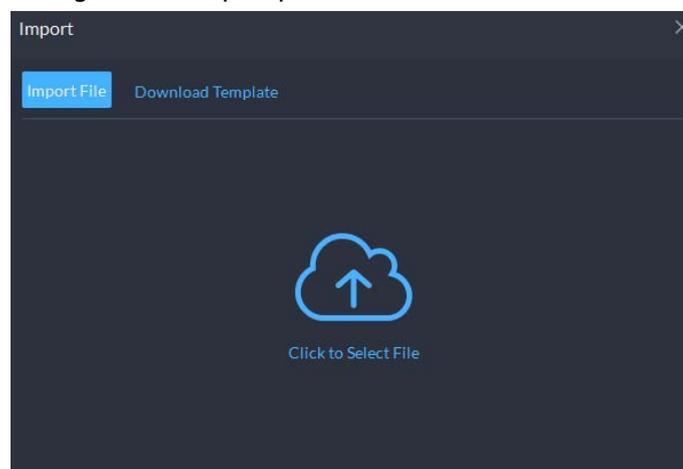
Step 4   Import the personnel information file.

📖

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

Related Operations

- Export personnel information.

  Select an organization, click **Export**, and then follow the instructions on the page 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.

5.3.1.2.3 Extracting Personnel Information

When personnel information has been configured on access control devices or door stations, you can directly synchronize the information to the platform.

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **App Config** section, select **Personal and Vehicle Info**.

Step 2   Click ![icon].

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

Figure 5-30 Import from device
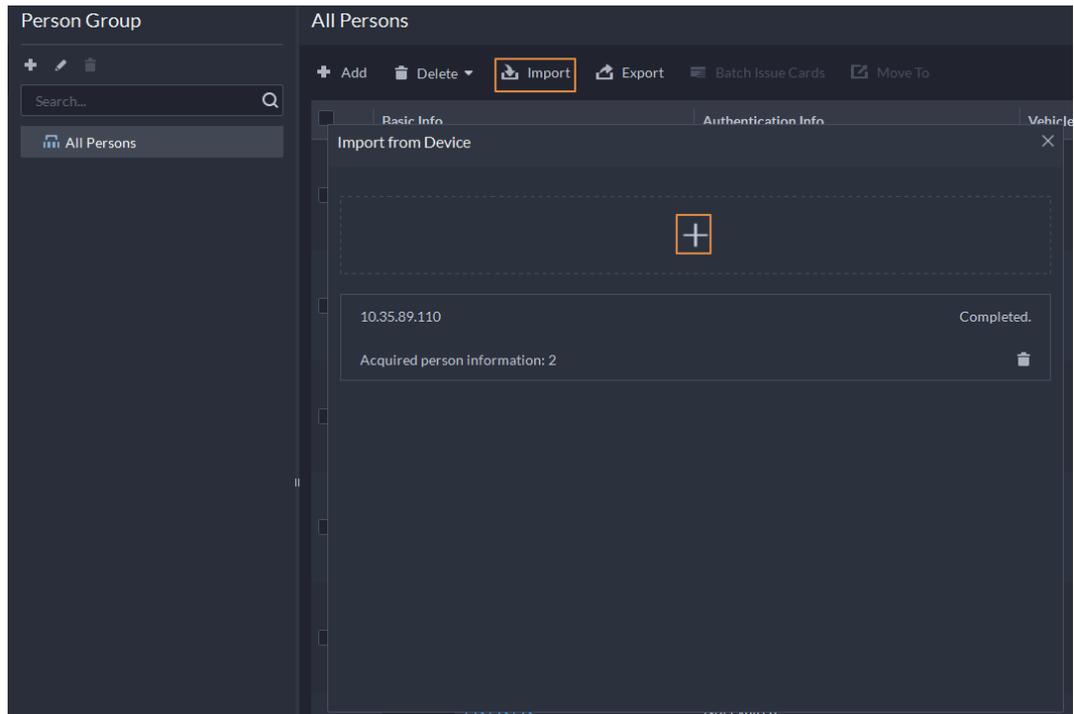
Step 4   Click ![+], select a channel from an access control device or door station, and then click **OK**.

Figure 5-31 Extract task list
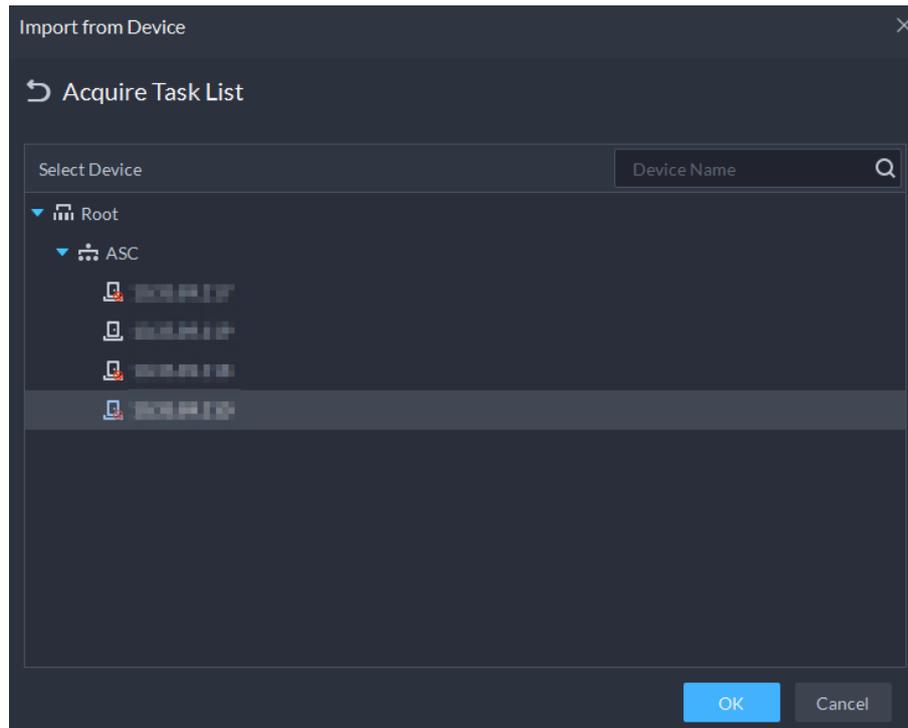
Step 5   Double-click a result to view the detailed information.

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

Figure 5-32 Personnel extraction results
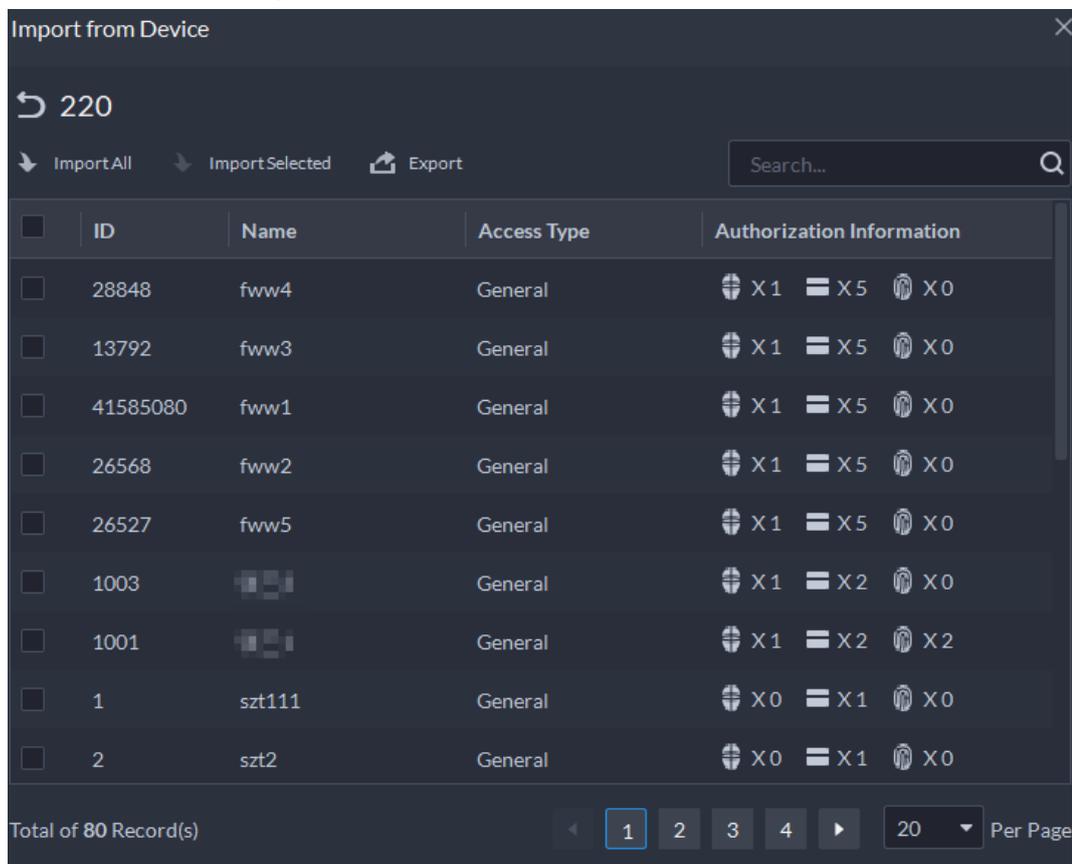
- To add all the personnel information to the platform, click **Import All**.
- To add part of the information, select the people of interest, and then click **Import**

selected.

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

5.3.1.3 Issuing Cards in Batches

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **App Config** section, select **Personal and Vehicle Info**.

Step 2   Click ![icon].

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

Figure 5-33 Issue card in batches
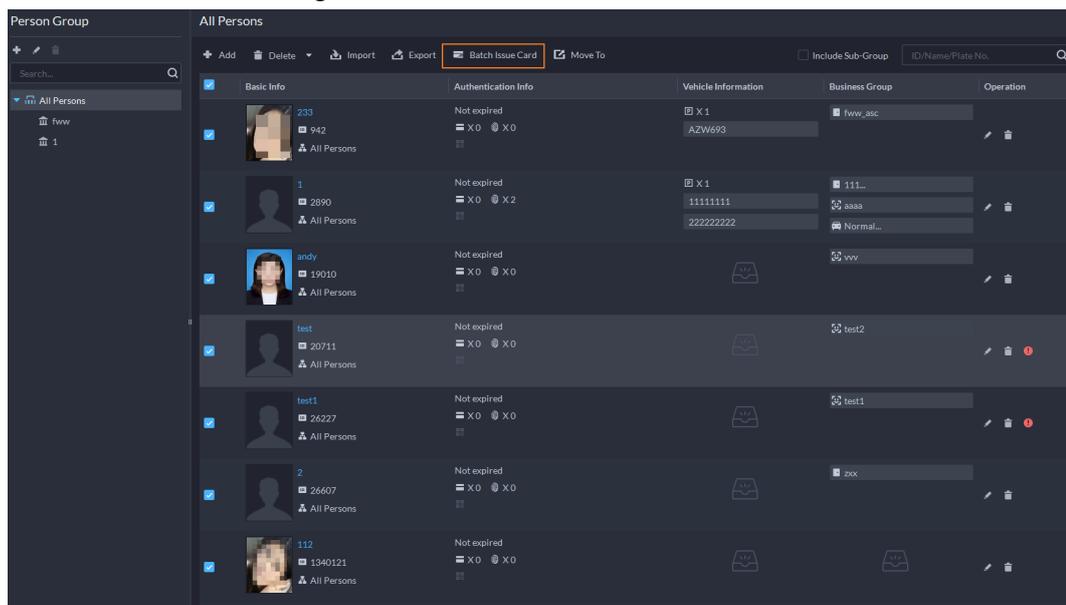
Step 4   Set term of validity.

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 5-34 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 5-35 Reader manager
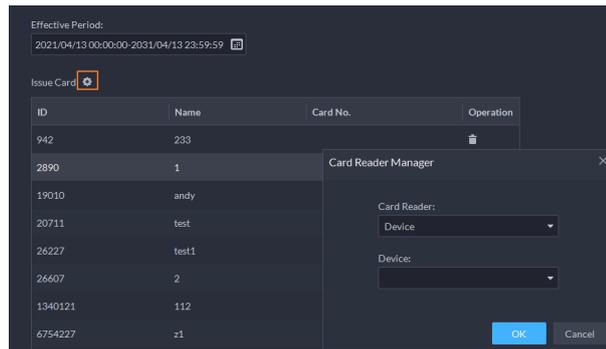
3) Select people one by one and swipe cards respectively until everyone has a card number.
4) Click **OK**.

5.3.1.4 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** page, click 🔍, and then in the **App Config** section, select **Personal and Vehicle Info**.

Step 2   Click 👤.

Step 3   Click 🖊 to edit information. For details, see "5.3.1.2.1 Adding a Person".

5.3.2 Vehicle Management

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

Procedure

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

Step 2   Click 🚗.

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

Figure 5-36 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 "5.4.2.1 Creating Vehicle Arming Group".
- Add vehicles in batches
    1. Click **Import** at the top, and then click **Template Download**.

Figure 5-37 Download template
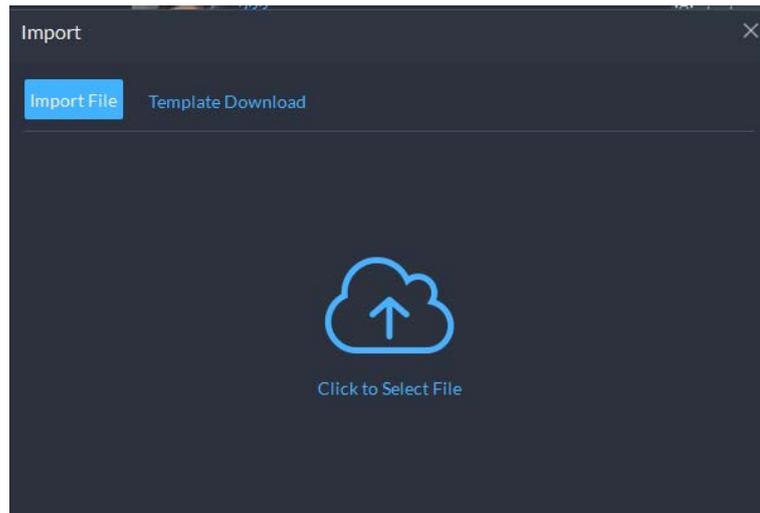
2. Fill in the template, and then select **Import** > **Import File**. Click to select the file and import.

📖

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 5-38 Export vehicle information
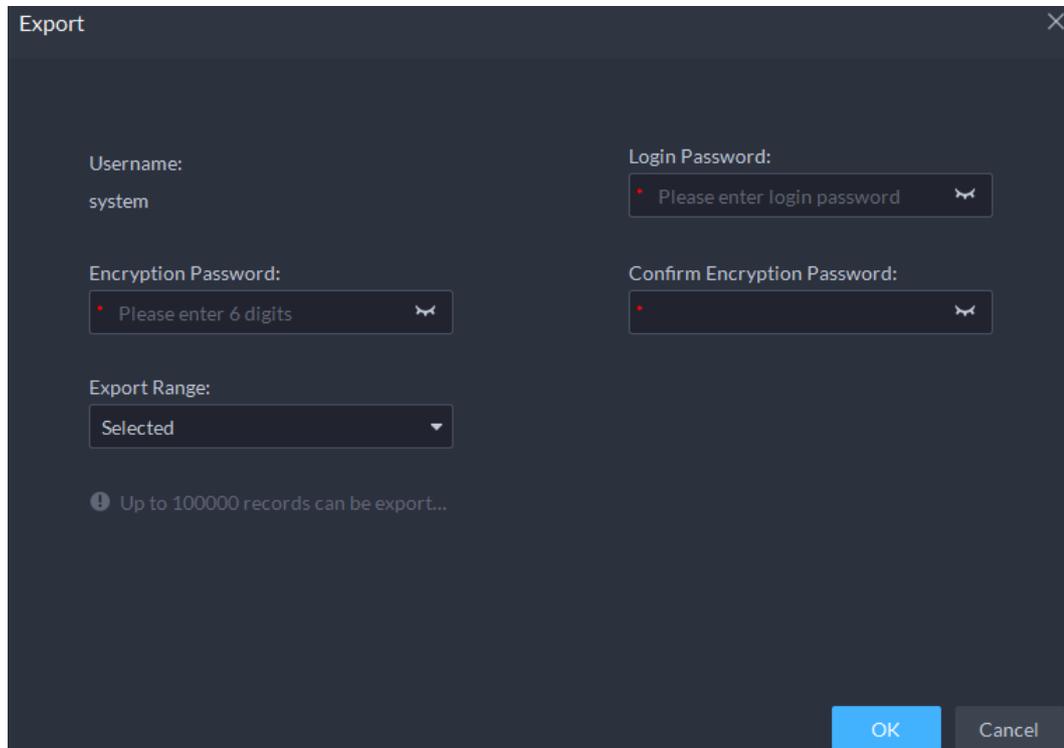
- Click **Export** and then enter required information, such as passwords for login and encryption, to export all the items.
- Select vehicles, and then click **Export** to export only the selected information.

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.

5.4 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.

5.4.1 Face Watch List

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

5.4.1.1 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 "4 Basic Configurations". During the configuration, you need to pay attention to following parts.
  - ◇ When adding devices on the **Device** page, set the **Device Category** to **Encoder**.

Figure 5-39 Device category

◇ When adding devices like NVR or IVSS which support face recognition, set the device feature to **Face Recognition**. For details, see "4.2.2.5 Editing Devices".

Figure 5-40 Feature configuration

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

Procedure

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then click **Watch List**.

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

Figure 5-41 Add face comparison 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 the group.

5.4.1.2 Adding Face

Add person in the created comparison group.

Procedure

Step 1   Log in to the DSS Client. On the **Home** page, 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** page, 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.

<p style="text-align:center">Figure 5-42 Add a person</p>

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

Step 5   Click **OK**.

- Click ![icon] at the bottom of the created group to add people one by one.
- Click ![icon] at the bottom of the created group to add multiple people at the same time.

Related Operations

- You can search faces by entering key words in the search box at the upper-right corner.
- Click ![edit icon] to edit the person information.
- Click ![delete icon] to delete person from the group and face library one by one.
- Click ![remove icon] 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.

5.4.1.3 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** page, click ![icon], and then click **Watch List**.

Step 2   Click ![icon], and then click ![icon] of the face comparison group you want to arm.

Step 3   Click **Add**, select one or more devices or channels, and then click **OK**.

The platform will send the information of the face watch list to the devices and channels you selected, and display the progress. If exceptions occur, you can click ![icon] to see the reason.

Figure 5-43 Send face comparison group
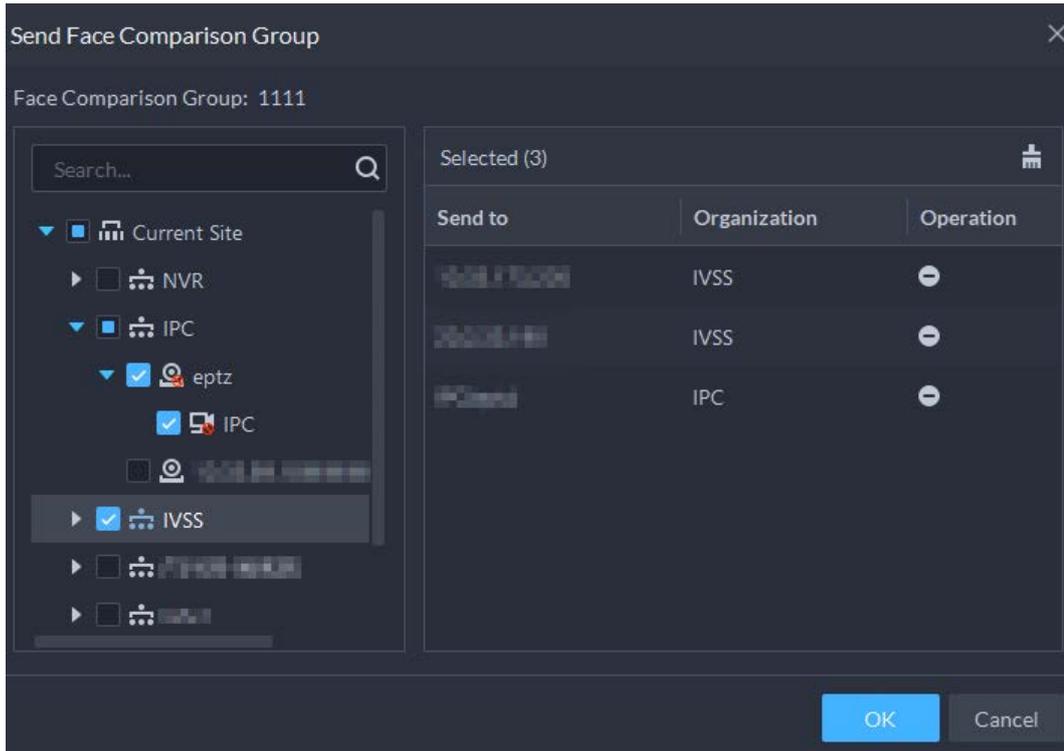
Step 4   After the face watch list is successfully sent, click **Next Step**.

Step 5   Click **Add**, select the channels you want to arm, and then configure the similarity for each channel.

When the similarity between the face captured by the channel and a face in the face watch list reaches or is greater than the defined value, it is considered a match.

Figure 5-44 Arm face comparison group
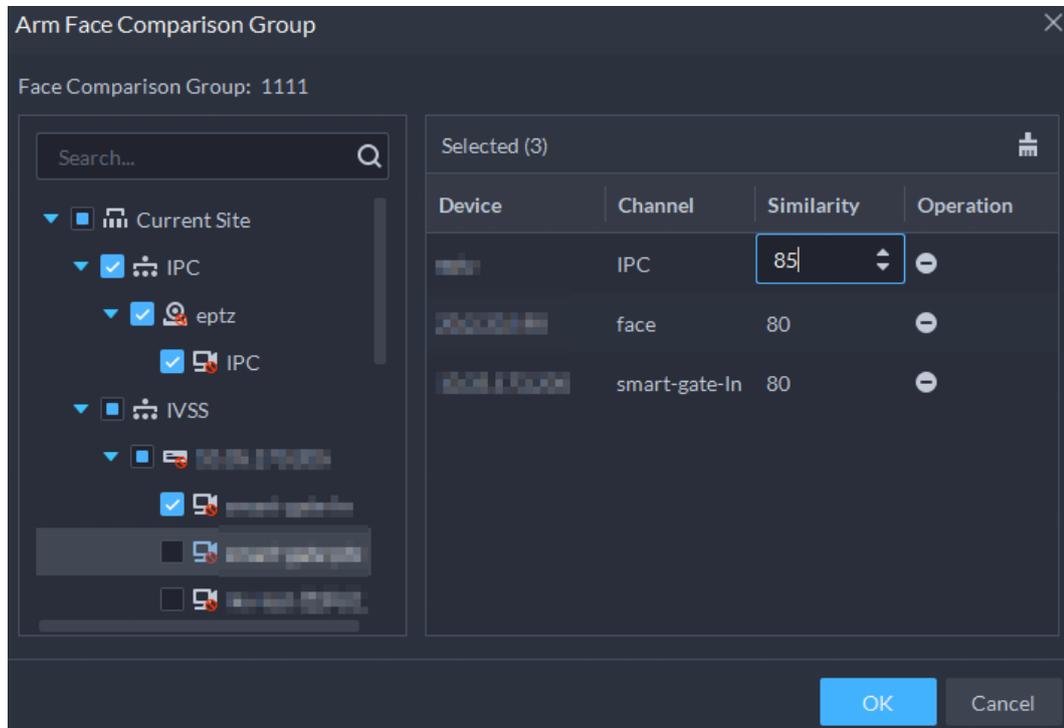
Step 6   Click **OK**.

Step 7   (Optional) View exceptions and arm the face comparison group again.

1) Click [icon] to view why arming failed and address the issue.

2) Click **Send Again** to arm the face comparison group again.

5.4.2 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.

5.4.2.1 Creating Vehicle Arming Group

Step 1   Log in to the DSS Client. On the **Home** page, click [icon], and then click **Watch List**.

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

Figure 5-45 Add a vehicle arming group
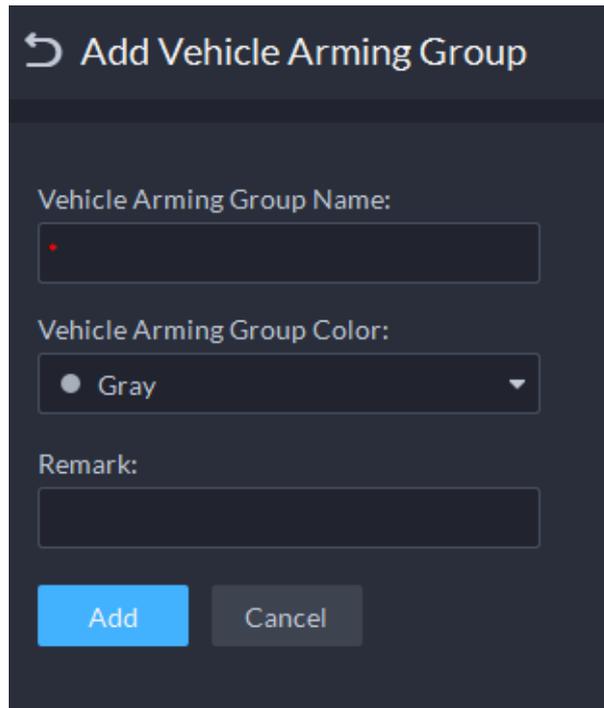
Step 3 Enter the required information, and then click **Add**.

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.

5.4.2.2 Adding Vehicles

Vehicles in the watch list that has been armed will be recognized and you will receive alarms.

Procedure

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

Step 2 Click 🚗.

Step 3 Click 🖼 of a group, or double-click a group, an then click **Select from Vehicle List**.

Step 4 Select the vehicles you want to add, and then click **OK**.

Related Operations

- You can search vehicles inside a group by setting search conditions on the left.
- Click ✎ to edit the information of a vehicle.
- Click ⊖ to remove vehicles from the group but keep it in the vehicle list. You can also select multiple vehicles, and then click **Remove** to remove them in batches.
- Click **Operation** at the upper-right corner to select what vehicle information to be displayed.

5.4.2.3 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** page, click ![icon], and then arm the vehicle on the **Event** page. Click **Add**. For how to configure events, see "5.1 Configuring Events".

Figure 5-46 Arm vehicle event
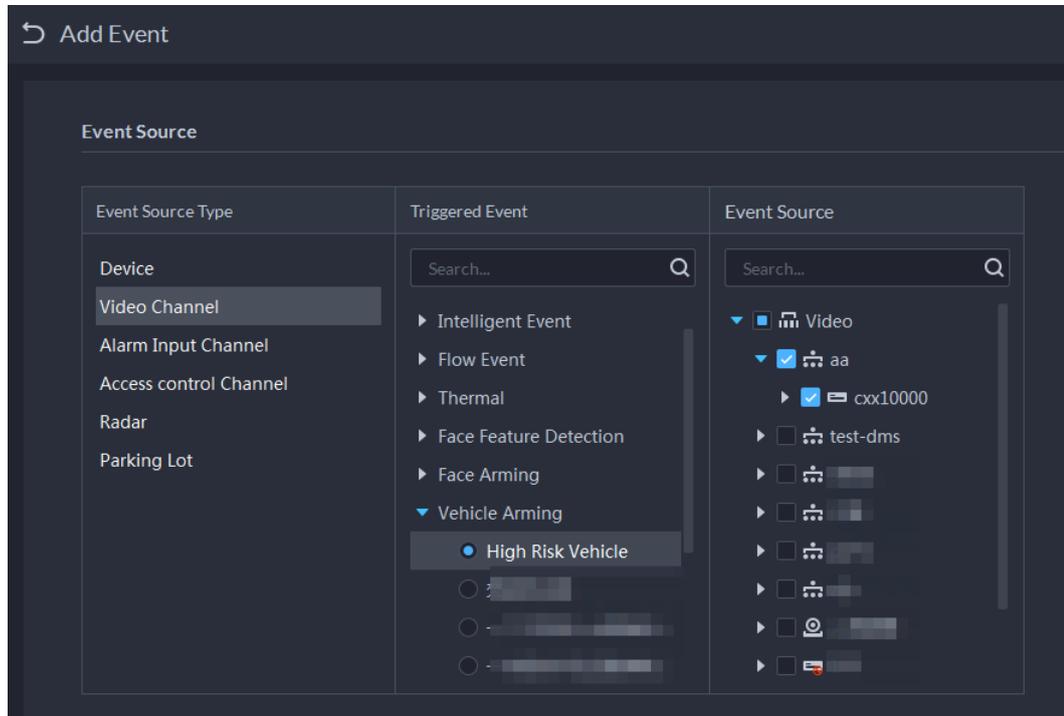
5.5 Access Control

Issue cards, collect fingerprints and face data, and apply permissions, so that the authorized people can open door by using card, face or fingerprint.

5.5.1 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 "4 Basic Configurations" for details.
  ◇ When adding access control devices, select **Access Control** for device category.
  ◇ (Optional) On the **Bind Resource** page, bind video channels for access control channels.
  ◇ Personnel information is added correctly. For details, see "5.3 Personnel and Vehicle Information Management".

5.5.2 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** page, click ![icon], and then in the **App 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 5-47 Add a door group
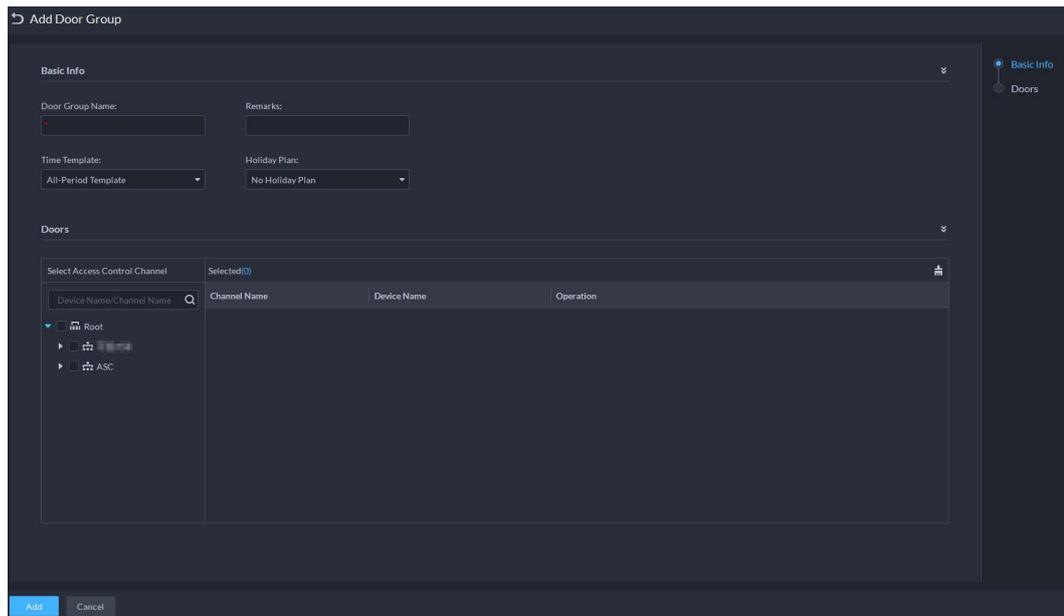
Step 4　Authorize.

    1)　On the **Access Permission Group** page, select a door group, and then click the corresponding ⊞ icon.

    2)　Select personnel, and then click **OK**.

5.5.3 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** page, click 🔧, and then in the **App Config** section, select **Access Control**.

Step 2　Click 🔲.

Step 3　Create an access permission group.

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

Figure 5-48 Add an access permission group
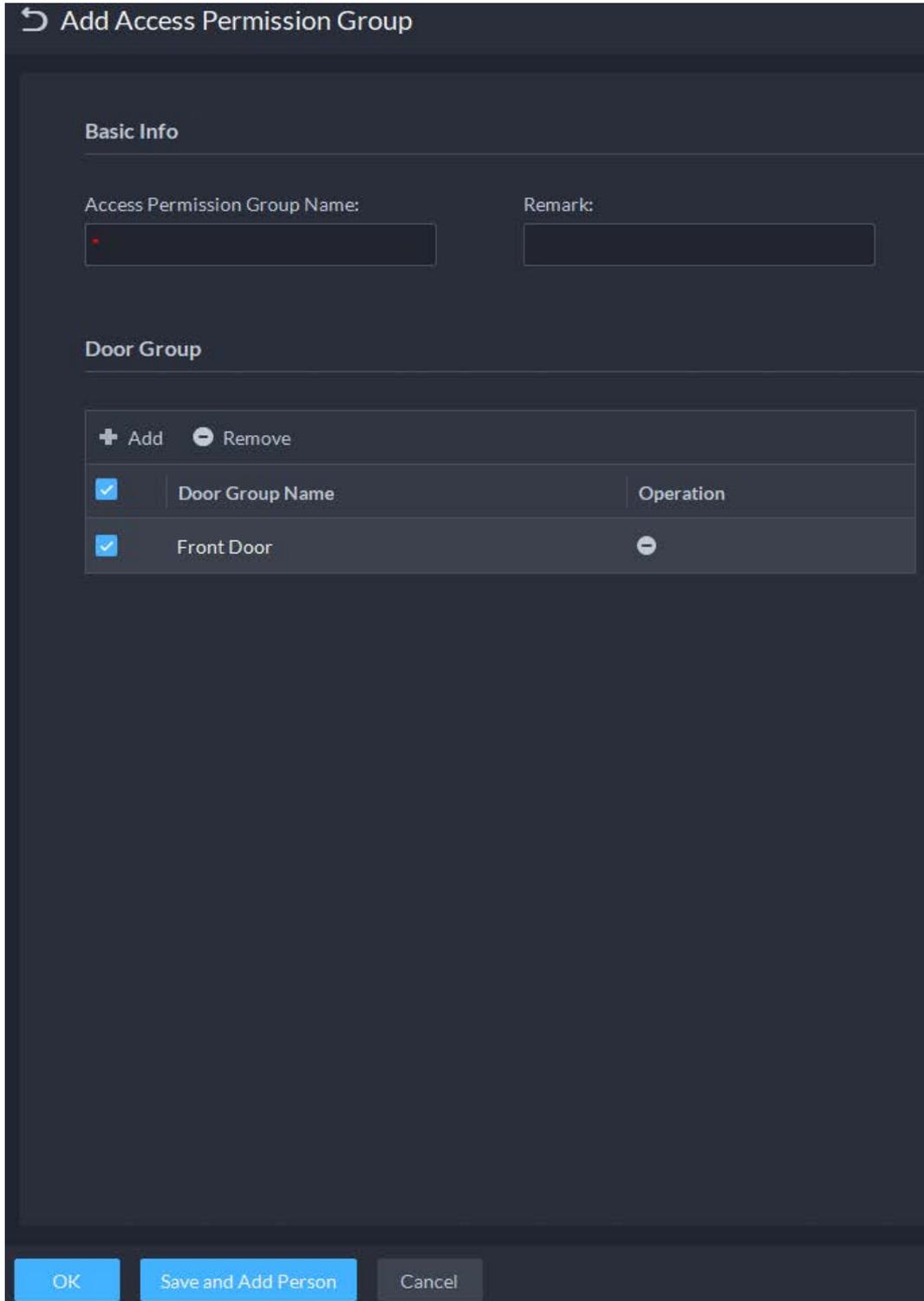
2) Enter the group name, and then select the door groups as needed.

3) Click **Save and Add Person**.

Figure 5-49 Add a person
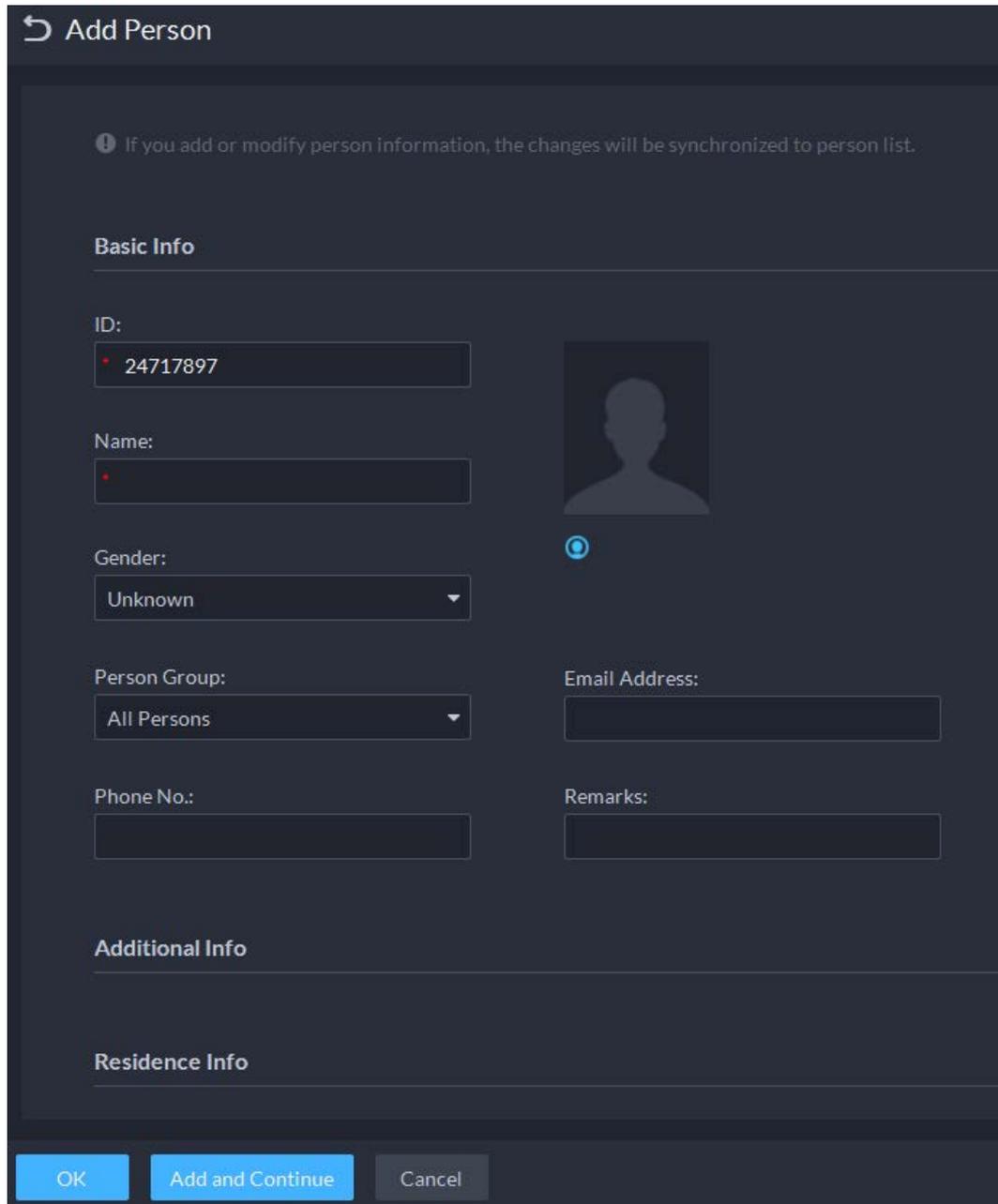
4) Enter the information from different sections. See "5.3.1.2.1 Adding a Person" for details.

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 ![icon] or ![icon] to add people to a group.
- Click ![icon] to edit the name, door groups, and remarks of a group.
- Click ![icon] to delete a group; select the groups as needed, and then click **Delete** to delete them all.

5.5.4 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** page, click 🔧, and then in the **App Config** section, select **Access Control**.

Step 2   Click 📝.

Step 3   Click **Add**, enter a name and a password, and then select the access control channels and video intercom devices as needed.

Figure 5-50 Add a public password
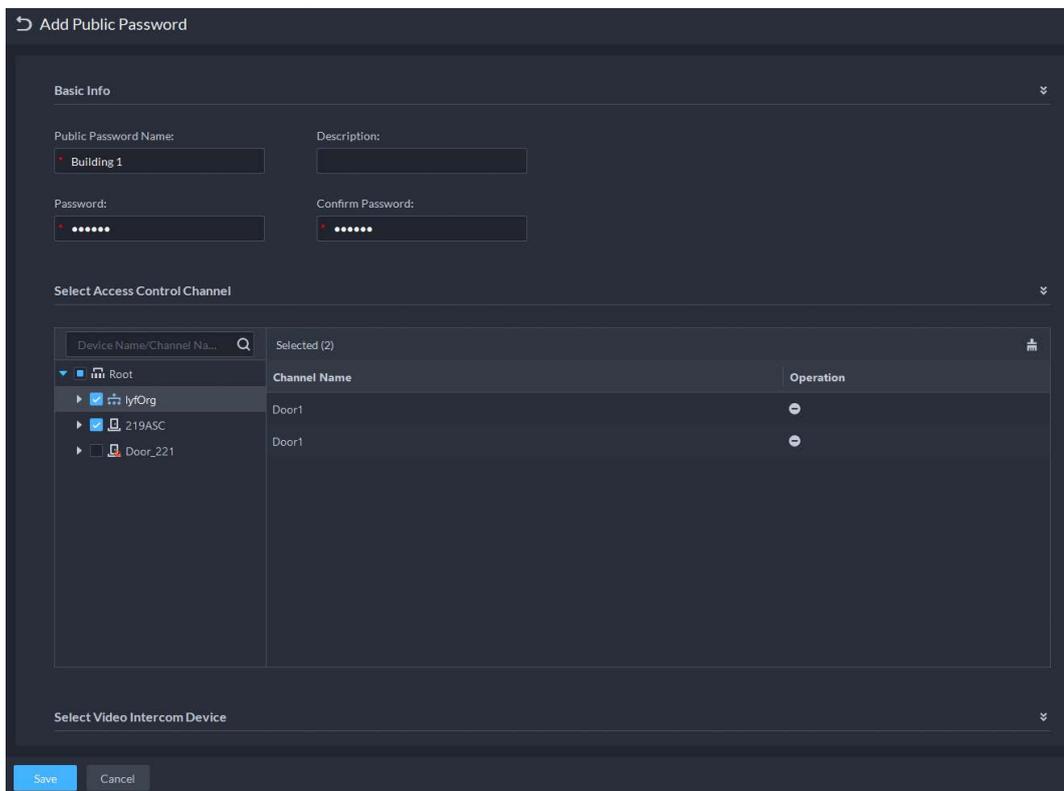
Step 4   Click **Save**.

5.5.5 Anti-passback

The anti-passback feature requires a person to enter and exit from the specific doors. For the same person, an entry record must pair with an exit record. If someone has entered by tailing someone else, which means there is no entry record, this person cannot unlock the door to exit.

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

Step 2   On the **Access Control** page, click 📇.

Step 3   Click the **Anti-passback** tab.

Step 4   Click **Add**.

Step 5   Configure the parameters, and then click **OK**.

Figure 5-51 Anti-passback parameters
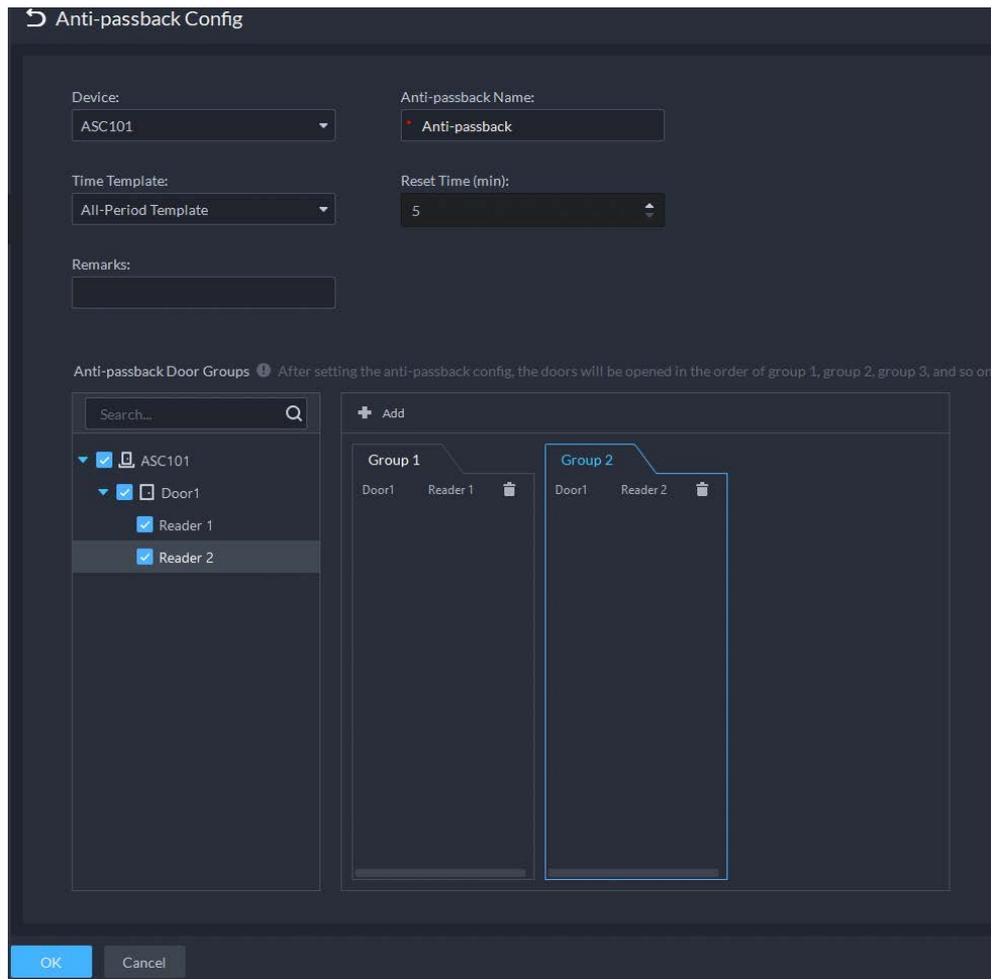
Table 5-4 User selection information description

Parameter	Description	
Device	You can select the device to configure the anti-passback rules.	
Anti-passback name	You can customize the name of an anti-passback rule.	
Reset Time(min)	The access card becomes invalid if an anti-passback rule is violated. The reset time is the invalidity duration.	When the selected device is a multi-door controller, you must set up these parameters.
Time Template	You can select the time periods to implement the anti-passback rules.	
Remark	Description information.	
Group X (X is a number)	The group sequence here is the sequence for swiping cards. You can add up to 16 readers for each group. Each group can swipe cards on any of the readers.	

Step 6   Click [ ], and then it changes to [ ]. The function is enabled.

5.5.6 Configuring Time Templates

Configure time templates for different access control strategies. For example, employees can only gain access to their offices during work time.

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **App Config** section, select **Access Control**.

Step 2   Click ![icon].

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

Figure 5-52 Time template
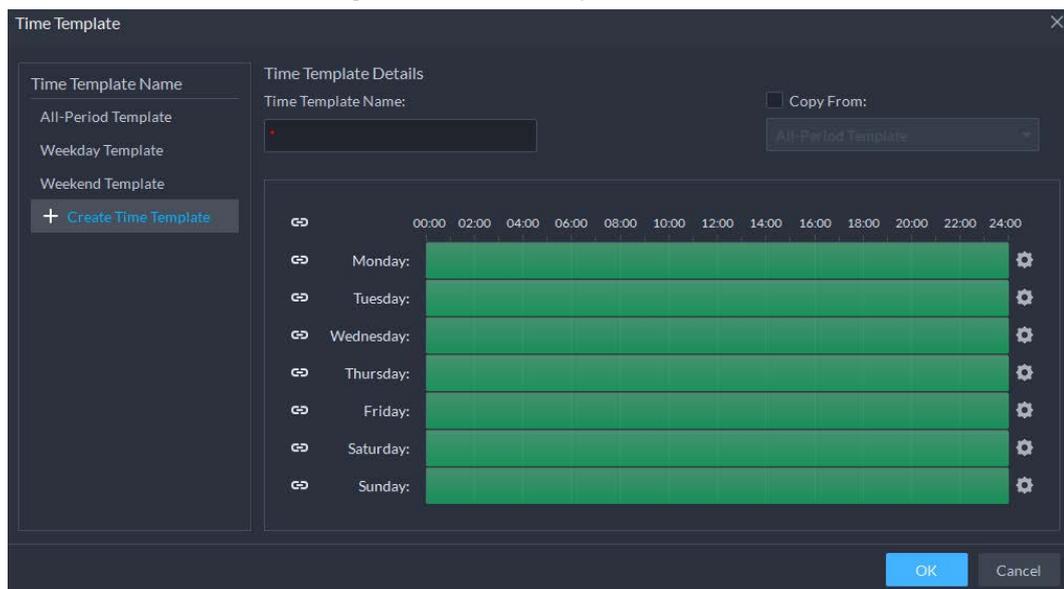
Step 4   Enter the template name, set time periods, and then click **OK**.

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 ![icon], and then set time periods in the **Period Setup** dialog box.

📖

- You can add up to 6 periods for each day.
- To use an existing template, select the **Copy From** check box and then select a template in the drop-down list.

5.5.7 Configuring Holidays

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **App 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 5-53 Add a holiday schedule
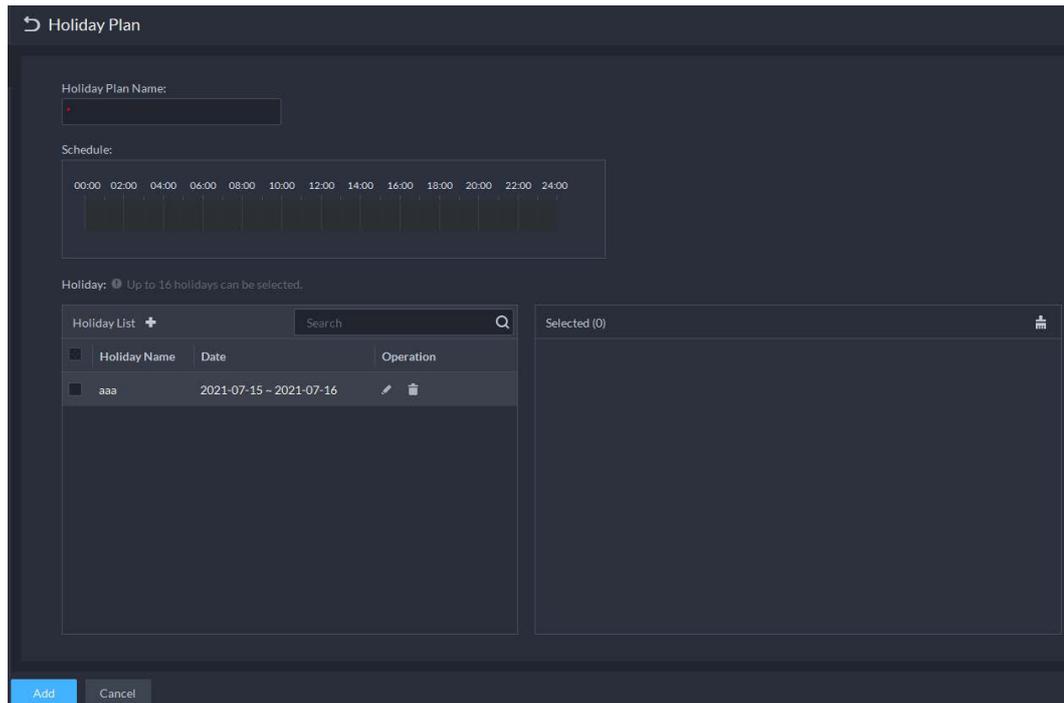
Step 3 Configure the parameters.
1. Enter a holiday schedule name.
2. Configure the periods in the **Schedule** section.
3. Click ![plus] to add a holiday: Enter the holiday name, set a start date, and how many days this holiday lasts, and then this holiday will be effective within the periods you set from the previous step.

Step 4 Click **Add**.

5.5.8 Configuring Access Control Devices

After an access control device is added, and if it is online, you can restart it, and synchronize its time with the platform.

Step 1 Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **Basic Config** section, select **Device**.

Step 2 Click ![icon].

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

Figure 5-54 Select an access control device
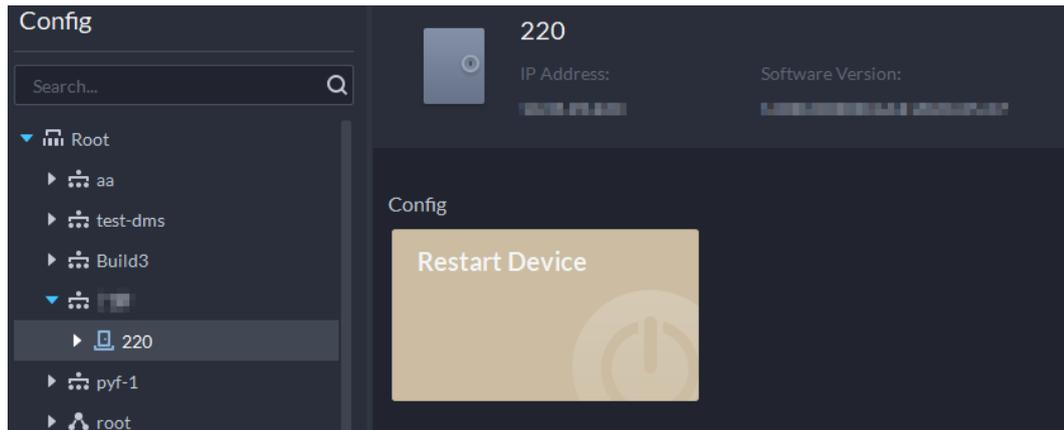
Step 4   Configure the access control device.
- Click **Restart Device** to restart the device.
- Click [icon] at the upper-right corner to go to the web page of the device.

5.5.9 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** page, click [icon], 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 5-55 Door configuration

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

Table 5-5 Parameters description

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 "5.5.4 Configuring Public Passwords".

Parameter	Description
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.
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.

5.6 Video Intercom

5.6.1 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 "4 Basic Configurations".
  ◇ When adding video intercom devices on the **Device** page, 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.

5.6.2 Call Management

Create call group, management group and relation group respectively and define restricted call relations. This function is only available for administrators.

⚠️

Click 🔄 on the page of call group, management group or relation group, the system will restore management group and relation group to their original status.

5.6.2.1 Configuring Call Group

VTOs and VTHs can only call each other when they are added into the same call group. DSS will automatically generate corresponding call 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 call 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 call 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 call group, and realize mutual call among unit VTOs, second confirmation stations and fence stations.

VTHs from different call groups can call each other only when there is a fence station is each group.

5.6.2.2 Adding Management Group

Management group is to make groups for administrators, and realize relation binding of one to one, one to many or many to many. Administrators include 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.

Step 1 Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **App Config** section, select **Video Intercom**.

Step 2 Click ![icon].

Step 3 Click **Manager 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 ![icon] and move the member to other groups.
- To manage group members, click ![icon] to add or delete group members.

Figure 5-56 Edit manager group
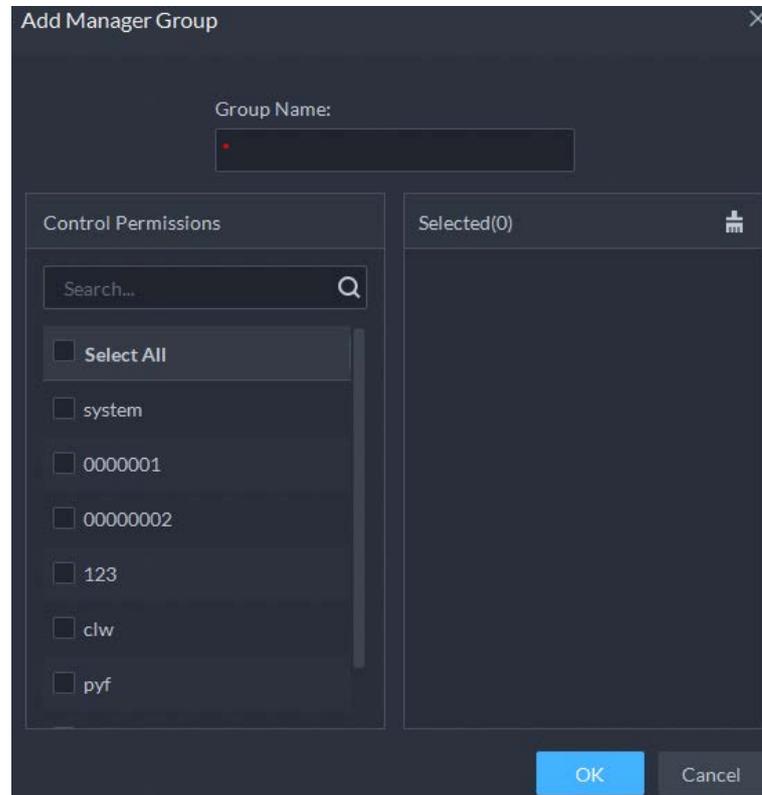
5.6.2.3 Configuring Group Relation

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

- A call 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 call 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** page, click ![icon], and then in the **App Config** section, select **Video Intercom**.

Step 2 Click ![icon].

Step 3 Click **Relation Group Config**.

Step 4   Click **Add**.

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

Figure 5-57 Add a group relation
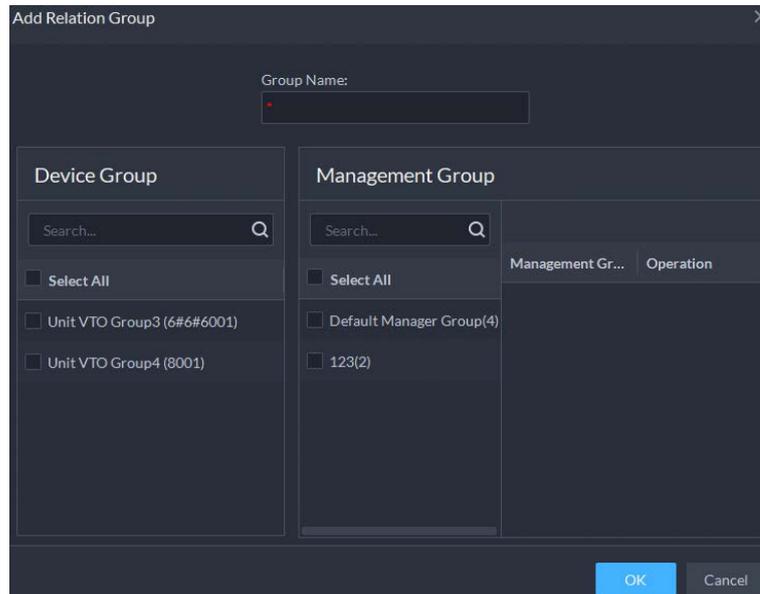
Added relation group is displayed in the list. If there are several relation groups, you can click ⬆ or ⬇ to adjust priority level. When there is a call, the online administrators with the highest priority will generate ring bell first.

5.6.3 Configuring Building/Unit and Call Mode

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:

- 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** page, click 🔧, and then in the **App Config** section, select **Video Intercom**.

Step 2   Click 🔳.

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

⚠️

This configuration must be the same as the device configurations. Otherwise, information of the devices might be incorrect. For example, if only **Building** is enabled on a VTO, you must only enable **Building** on the platform.

Step 4   Click **Save**.

5.6.4 Synchronizing Contacts

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

User's Manual

page.

Step 1   Log in to the DSS Client. On the **Home** page, click 🔧, and then in the **App 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 page.

5.6.5 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** page, click 🔧, and then in the **App 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.

📖

The format should be **room number + private password**, and the room number consists of 6 digits. For example, a person who lives in 1001 with the private password of the VTO in the building being 123456, can enter **001001123456** to unlock the door.

5.6.6 App User

You can view information of App users, freeze user, modify login password and delete user.
App users have registered by scanning the QR code on the platform or the VTH. For details, see the user manual of the App.

📖

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

Step 2   Click 👤.

Table 5-6 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.

Operation	Description
Change APP user login password	Click ⬚ and enter a new password on the **Reset Password** page, 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.

5.7 Visitor Management

After visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves.

5.7.1 Preparations

● Access control devices have been added into the platform.
● Basic configurations of the platform have been finished. To configure, see "4 Basic Configurations".

5.7.2 Configuring Visit Settings

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

Step 2   Configure the parameters.
● 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 5-58 Customize visitor pass remarks
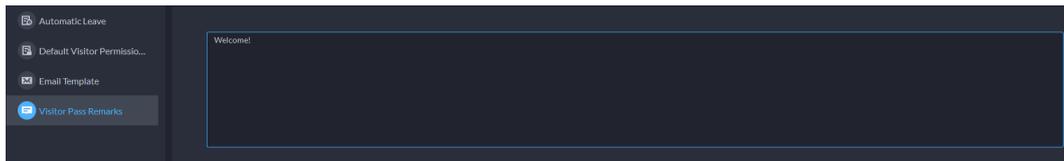
Figure 5-59 Visitor pass remarks
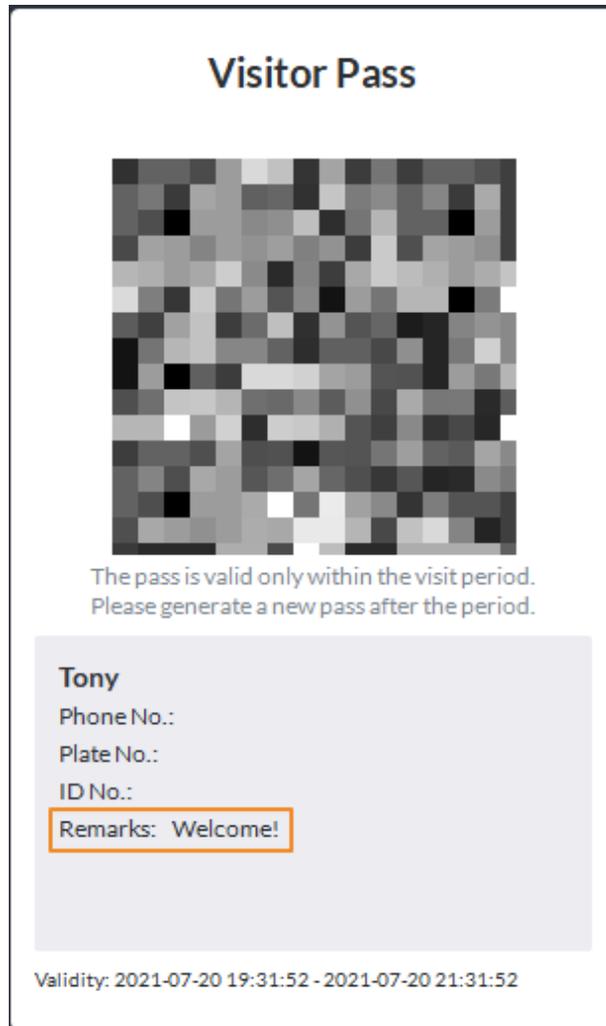
Step 3   Click **Save**.

5.8 Parking Lot

Control 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, and then the management center can remotely open the barriers after verifying the identity of the visitor.

5.8.1 Preparations

Make sure that the following preparations have been made:
- Devices, such as ANPR cameras, VTOs, barriers, are added to the platform.

- Basic configurations of the platform have been finished. To configure, see "4 Basic Configurations".
    - ◇ When adding an ANPR camera, select **Access ANPR Device** as the device category.
      After you have added ANPR cameras, you can bind video channels to their channels. This is useful when you have installed other cameras at the entrance to view and record videos of the entire scene, not just the vehicle. You can view video from the bound camera when checking the alarm details. For how to bind channels, see "4.2.3 Binding Resources".
    - ◇ When adding an NVR, select **Encoder** as the device category.
    - ◇ Select **Entrance ANPR** from **Features** for the corresponding NVR channels.
    - ◇ When adding VTO, select **Video Intercom** as the device category.
      Also, you need to add the information of people and assign them permissions so that they can use the VTO normally. For details, see "5.3 Personnel and Vehicle Information Management".

      📖

      Make sure that the configuration of building and unit on 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 "5.6.3 Configuring Building/Unit and Call Mode".
    - ◇ Snapshots taken by ANPR cameras are stored in the **Images and Files** disks. You must configure at least one **Images and Files** disk so that snapshots of vehicles can be normally dispalyed. For details, see "4.4 Configuring Storage".

5.8.2 Configuring Parking Lot

A parking lot includes parking spaces, entrances and exits, barrier control rules and other information. Link an ANPR camera for recognizing license plates, and a VTO for verifying identities.

5.8.2.1 Basic Information

Procedure

Step 1   Log in to the DSS Client. On the **Home** page, click 🔧, and then in the **App Config** section, select **Parking Lot** > **Parking Lot Configuration** > **Parking Lot Basic Config**.

Step 2   Click the root node named **Current Site**, and then click **Add**.

Step 3   Configure the basic information of the parking lot, and then click **Next Step**.

Table 5-7 Parameter description

Parameter	Description
Parking Lot Name	To differentiate from other parking lots.
Enable Parking Space Counting	Configure the total parking spaces and available ones. ● Total Parking Spaces: The total number of parking spaces in the parking lot. ● Available Parking Spaces: The number of parking spaces in the parking lot that are not in use.

Parameter	Description
Fuzzy Match of Entrance & Exit Plate No. Snapshot	- First Character Rule 1 character added to the front of the plate number: It will still be considered as a match when an additional character is added to the plate number. For example, AB12345 is recognized as AAB12345. - Missing the first character of the plate number: It will still be considered as a match when the first character is missing from the plate number. For example, AB12345 is recognized as B12345. - Last Character Rule 1 character added to the end of the plate number: It will still be considered as a match when an additional character is added to the end of the plate number. For example, AB12345 is recognized as AB123455. - Missing the last character of the plate number: It will still be considered as a match when the last character is missing from the plate number. For example, AB12345 is recognized as AB1234. - Misread Character Rule: It will still be considered as a match if a character is recognized incorrectly, but the number of characters are correct. For example, AB12345 is recognized as AB12B45. When you enable multiple rules, the platform will check if each rule is satisfied. Only when one or more rules are satisfied will platform consider it to be a match. For example, 1 character added to the front of the plate number, and missing the first character of the plate number are both enabled. When the plate number AB12345 is recognized as AAB12345, it satisfied 1 character added to the front of the plate number, but not missing the first character of the plate number. This will be considered as a match. If the plate number AB12345 is recognized as AB112345, it does not satisfy both rules. This will not be considered as a match.
Auto overwrite when captured vehicle has not existed	If a vehicle entered the parking lot but has not exited, a new entry record will be generated when the vehicle is recognized to have entered again.

Step 4   Configure the entrance and exit points, and then click **Next Step**.

The platform supports up to 6 entrances and exits.

1) Click ➕ or **Add Entrance and Exit Point**.
2) Enter a name, and then click **OK**.

3) If there is an entrance point, click ![icon] next to **Entrance**.

4) Enter a name for the point, select a capture mode, and then add a camera, video intercom device (optional), or information display (optional).

   If limited by the surroundings, you can install two cameras for this point, and then set **Capture Mode** to **Dual Camera** to improve the successful rate of recognition number plates.

   In **Dual Camera** mode, the vehicles captured by the two cameras within the defined **Dual Camera Coordination Time** will be considered as the same one. You must configure the time properly according to the installation positions of the cameras and the distance between them.

Figure 5-60 Entrance point configuration
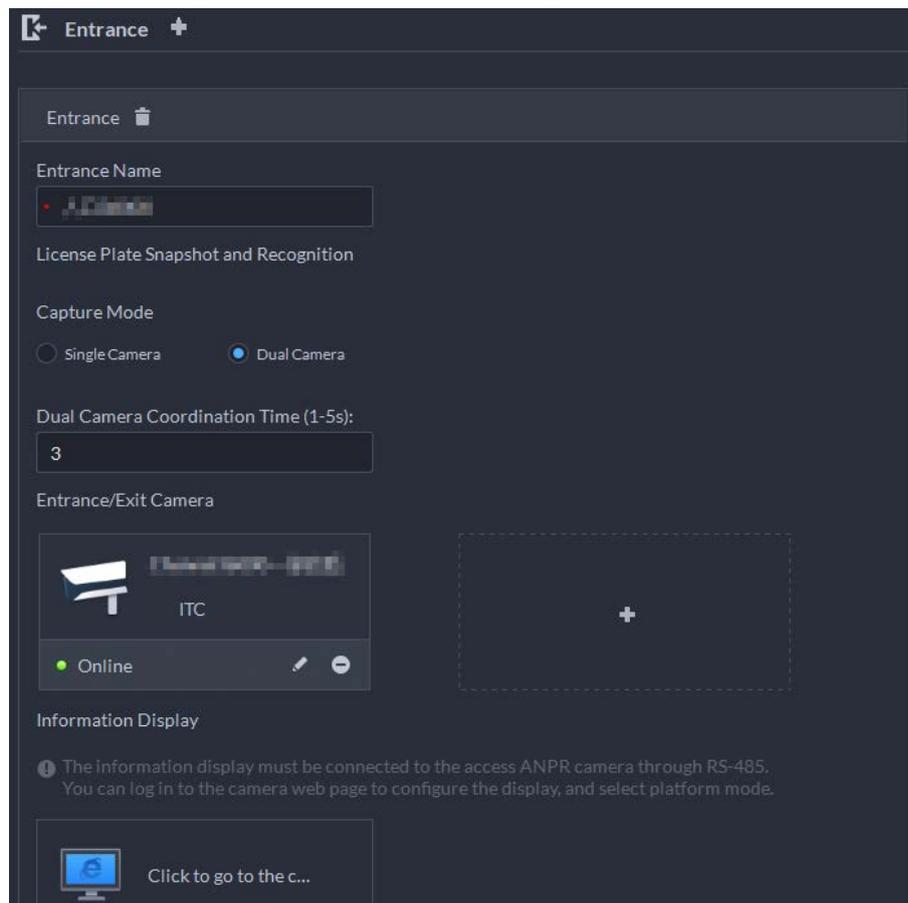
5) If there is an exit point, click ![icon] next to **Exit**, and then configure the parameters.

   The parameters are similar to the ones in **Entrance**. For details, see the steps above.

Step 5   Configure the passing rules, and then click **Save and Exit**.

1) Select a vehicle entrance rule, and then configure the parameters.

Table 5-8 Parameter description

Parameter	Description
Registered Vehicles	• **Registered Vehicles Access Rule** Click **Add**, and then select **By Parking Lot** or **By Point**. By parking lot: The vehicle groups will be added to all entrance and exit points of the parking lot, and the vehicles in these group can enter and exit through any entrance or exit. By point: You can add different vehicle groups to different entrance or exit points. For example, vehicle group is added to East entrance but not South entrance, then the vehicles in the group can only enter the parking lot through East entrance. • **Allow Passage When Available Space is 0**: After enabled, vehicles are allowed to enter the parking lot even if there are no available parking space. Click ⬤ to enable this function for an entrance point.
All Vehicles	All vehicles can enter the parking lot. • **Vehicles on the Blocklist**: After enabled, vehicles on the blocklist are also allowed to enter the parking lot. • **Registered Vehicles Access Rule** Click **Add**, and then select **By Parking Lot** or **By Point**. By parking lot: The vehicle groups will be added to all entrance and exit points of the parking lot, and the vehicles in these group can enter and exit through any entrance or exit. By point: You can add different vehicle groups to different entrance or exit points. For example, vehicle group is added to East entrance but not South entrance, then the vehicles in the group can only enter the parking lot through East entrance.

Parameter	Description
Custom	You can customize the passing rule for the entrance. ● For how to configure **Registered Vehicles Access Rule** and **Allow Passage When Available Space is 0**, see the content above. ● **All Vehicles**: Select a default time template or create a new one, and then any vehicle can enter the parking lot within the specified duration. For how to create a new time template, see "4.2.5 Adding Time Template". ● **Open Barrier by Verification**: After enabled, the access permission of a vehicle must be verified, and then an administrator can manually open the barrier for it. If **Open Barrier by Card Swiping After Verification** is also enabled, the driver can swipe a card, and then the barrier will automatically open if the can verify the driver to be the owner of the vehicle. ● **Open Barrier by Card Swiping Without Verification**: The barrier will automatically open if the card has access permission. 📖 You can enable **Open Barrier by Verification** or **Open Barrier by Card Swiping Without Verification** at the same time. ● **Available Parking Space Counting**: ◇ **Count each vehicle as an occupied parking space**: The number of parking spaces decreases after a vehicle enters. ◇ **Count each unregistered vehicle as an occupied parking space**: The number of parking spaces decreases only after a vehicle that is not registered to the platform enters. ◇ **Custom**: Configure which vehicles in the vehicle groups will be used to calculate parking spaces.

⊙⚿

For how to configure vehicle groups, see "5.8.3 Managing Vehicle Group".

2) Select a vehicle exit rule, and then configure the parameters.

The parameters are similar to the ones in the entrance. See the previous step.

3) Enable **Send Plate No. to Devices**, and then add vehicle groups to the allowlist and blocklist.

Devices can use this information to determine which vehicles to let in when the platform is offline.

Related Operations

● 🗒: 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.

5.8.2.2 Event Parameter

Configure events for a parking lot so that you can receive notifications when alarms are triggered.

Step 1 Configure an event, and you need to select **Parking Lot** as the type of event source. For how to configure an event, see "5.1 Configuring Events".

Step 2 Log in to the DSS Client. On the **Home** page, click 📷, and then in the **App Config** section, select **Parking Lot** > **Parking Lot Configuration** > **Event Parameter Config**.

Step 3 Select a parking lot, the events that were configured will be displayed on the right.

📖

Blocklist alarm will not be displayed because there are no additional parameters to be configured.

Step 4 Click ⚙ to configure an event.

Table 5-9 Parameter description

Parameter	Description

Parking Overtime	- **Overtime Parking Threshold**: The unit is minute. Alarm will be triggered if a vehicle has parked for longer than the defined value.
	- **Detection Interval**: How long the platform will check which vehicles have parked overtime. For example, select 5 minutes, then the platform will check whether there are vehicles that have parked overtime in the parking lot. If yes, then an alarm will be triggered.
	- **Vehicles to Trigger Alarms**:
	  ◇ **All Vehicles**: All vehicles will trigger alarms if they park overtime, but VIP vehicles are not included. If you enable **Include VIP Vehicles**, VIP vehicles will also trigger alarms when they park overtime.
	  ◇ **Non-registered Vehicle**: The vehicles whose information is not registered to the platform will trigger alarms when they park overtime.
	  ◇ **Custom**: Enable **Non-registered Vehicle**, and then the vehicles whose information is not registered to the platform will trigger alarms when they park overtime; enable **Registered Vehicle** and add vehicle groups, and then the vehicles in these groups will trigger alarms when they park overtime.
	  🔑
	  You can enable **Non-registered Vehicle** and **Registered Vehicle** at the same time.

Parameter	Description
No Entry and Exit Record	• **No Entrance/Exit Record Duration**: The unit is day. If a vehicle has not entered or exited the parking lot for longer than the defined duration, then an alarm will be triggered. • **Statistical Time Point**: The platform will start calculating the duration of a vehicle that has not entered or exited the parking lot on the defined time. • **Entrance and Exit Vehicle Group of Interest**: Only calculate the duration for the vehicles in the vehicle groups that are added.

5.8.3 Managing Vehicle Group

Add vehicles to different groups, so that you can quickly apply different parking lot functions to multiple vehicles at the same time.

General, VIP, and blocklist are the default groups. If you need to use them, you can directly add vehicles to them.

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **App Config** section, select **Parking Lot** > **Vehicle Groups**.

Step 2   Click **Add**.

Step 3   Enter a name and select a color for the group, and then click **Add**.

Step 4   Click ![icon] of a group, or double-click a group and click **Select from Vehicle List**, select the vehicles that you want to add to the group, and then click **OK**.

5.9 Intelligent Analysis

Before using the people counting and scheduled report functions, you must configure them first.

● People counting: Create a people counting group and add multiple people counting rules from one or more devices to it. Then, you can view the real-time and historical number of people of the group.

● Scheduled report: Configure the when to send a report with historical people counting data, the email address to send the report to, and the content of the email.

5.9.1 People Counting Group

Create a people counting group, and then add multiple people counting rules from one or more devices. In Intelligent Analysis, you can view the real-time and historical number of people of the group.

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then in the **App Config** section, select **Intelligent Analysis** > **People Counting Group Config**.

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

Figure 5-61 Add a people counting group

Step 3   Configure the parameters.

Table 5-10 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**.

5.9.2 Scheduled Report

Historical data will be sent on a regular basis to one or more email address that you set on the scheduled time.

Step 1   Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Intelligent Analysis** > **People Counting Group Config**.

Step 2   Configure one or more types of report.
   ● Daily report: Data from yesterday will be sent to your email at a defined time. If set to

03:00:00, the data from the day before (00:00:00–23:59:59) will be sent to your email at 03:00:00 every day.

- Weekly report: Data from last week will be sent to your email at a defined time. If set to 03:00:00 on Wednesday, the data from Wednesday to Tuesday of each week will be sent to your email at 03:00:00 every Wednesday.
- Monthly report: Data from last month will be sent to your email at a defined time. If set to 03:00:00 on 3rd, the data from 3rd of last month to 2nd of the current month will be sent to your email at 03:00:00 on 3rd of each month.

Step 3   Add one or more email addresses to send data to.

- Click ![icon] to select the users that have been configured email addresses.
- Enter an email address manually, and then press Enter.

Figure 5-62 Invalid email address, you must press Enter
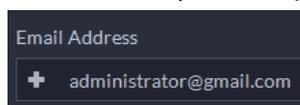
Figure 5-63 Valid email address
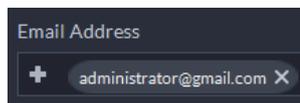
Step 4   Customize the body of the email.

Step 5   Click **Send Now** to send the reports that you configured immediately.

Step 6   Click **Save**.

6 Businesses Operation

6.1 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.

6.1.1 Main Page

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

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

Figure 6-1 Monitoring center
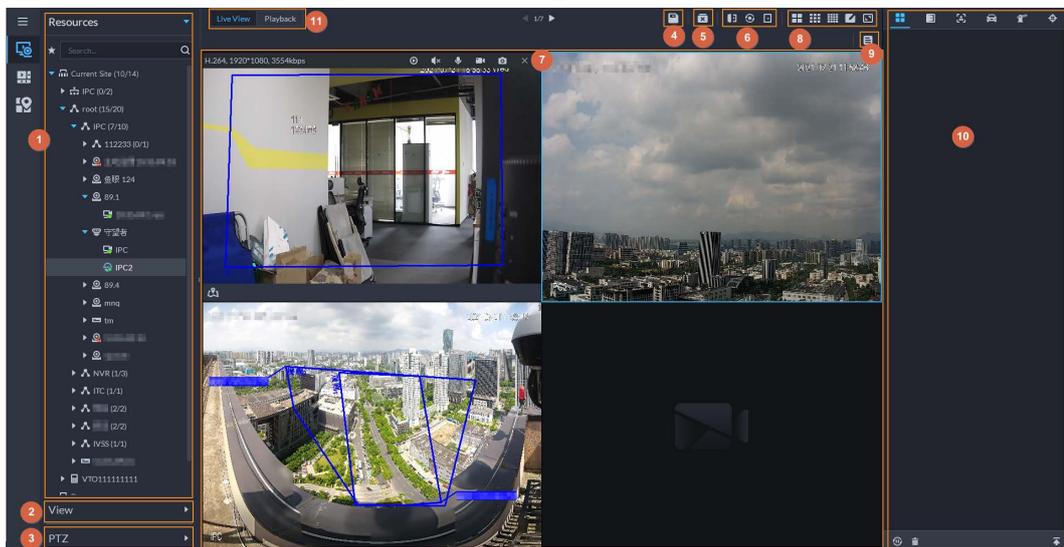
Table 6-1 Interface description

No.	Parameter	Description
1	Favorites and device tree	● List of resources including devices, browser, 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.

No.	Parameter	Description
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.
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 page. • 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 "6.1.3 Playback".

6.1.2 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.

6.1.2.1 Viewing Live Video

View the live video of connected devices.

📖

This section only introduces viewing live video. For map live view, see "5.2 Configuring Map".

Step 1   Log in to the DSS Client. On the **Home** page, 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.

    $\square$

    - ◇ 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 page to turn pages.
    - ◇ Close the on-going tour before starting live view.

Figure 6-2 Live view
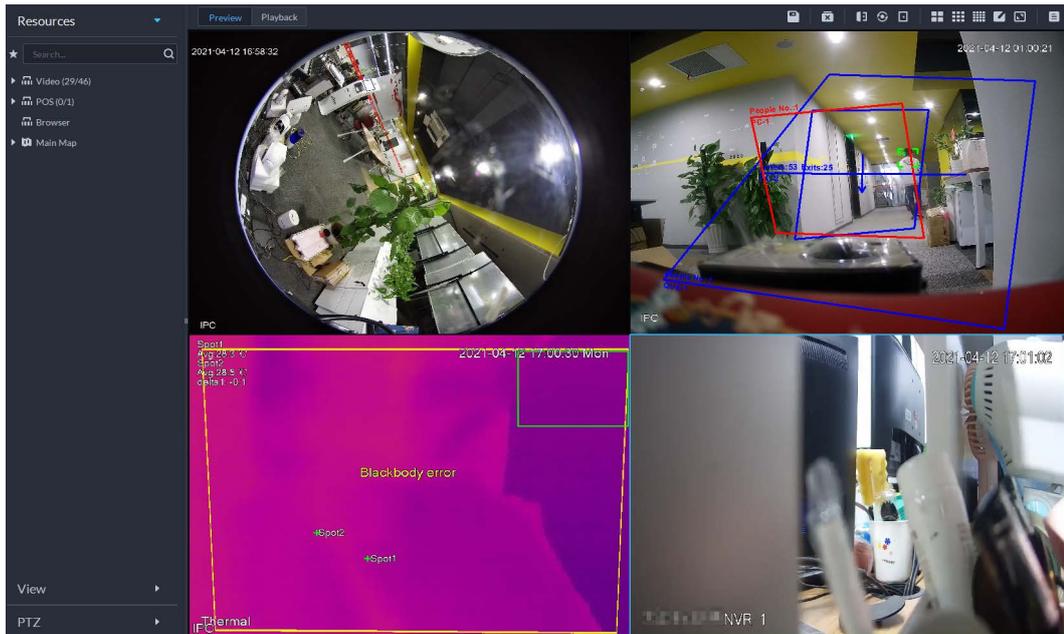
Step 4 You can perform the following operations during live view.

- 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 corner.

Figure 6-3 Live window
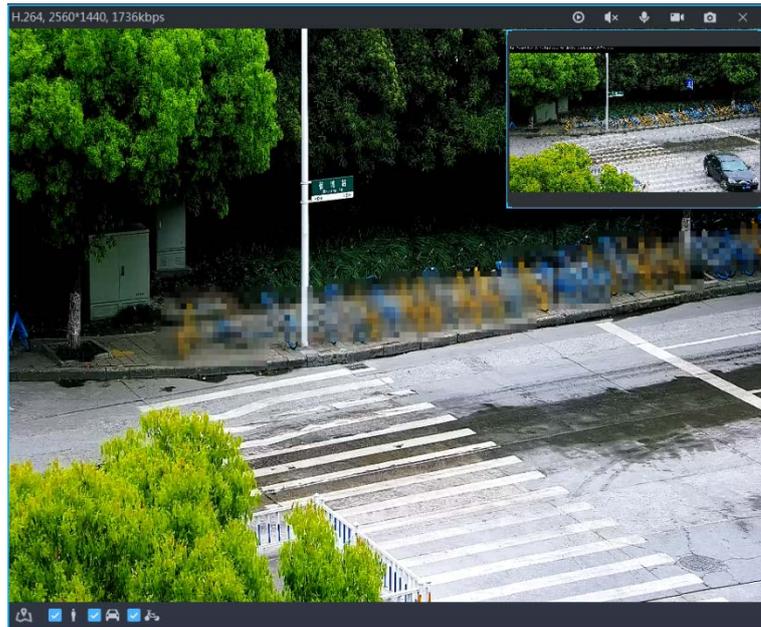
Table 6-2 Parameter description

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 "9.3.5 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 "9.3.5 Configure File Storage Settings".
	Close	Close the video.

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

$\Box$

The menu varies depending on device functions.

Figure 6-4 Live video operation menu
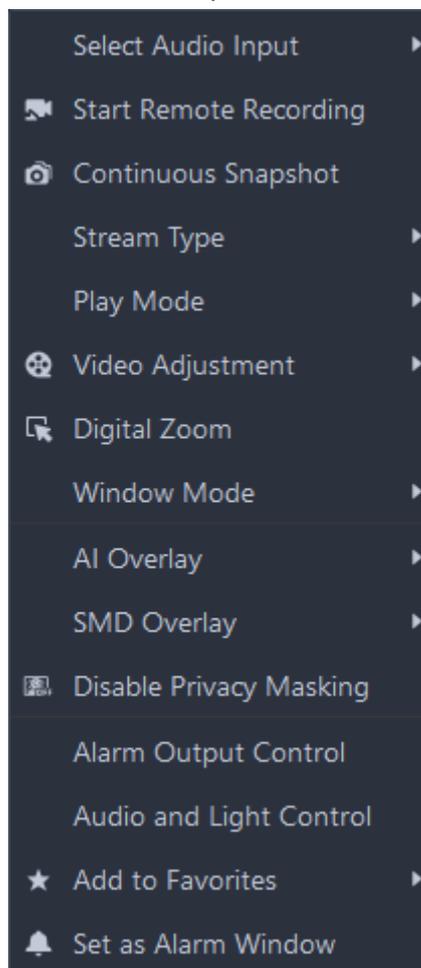
Table 6-3 Description

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 "9.3.5 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 2 (1+1 mode), 4 (1+3 mode), and 6 (1+5 mode). One window will play the real-time video, and the others play different defined areas of the real-time video. If a device supports target tracking, you can enable this function in any window mode, the windows that play defined areas of the real-time video will follow the target when detected, until it disappears.
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	Turn on or turn off alarm output channels.
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 6-5 View temperature
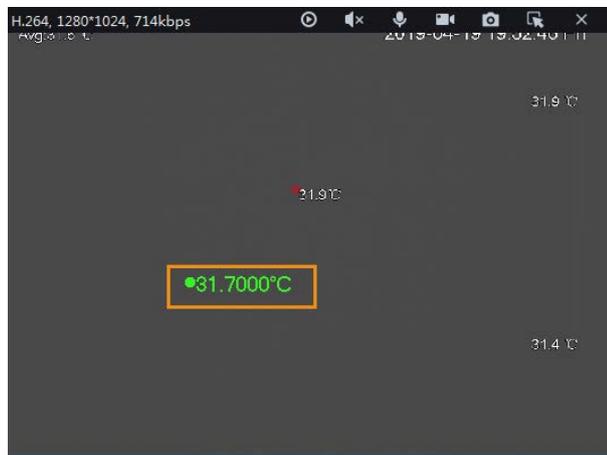
● If a channel supports electronic focus, you can enable electronic focus for it on the platform to adjust video definition and size.

The page 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 6-6 Live view
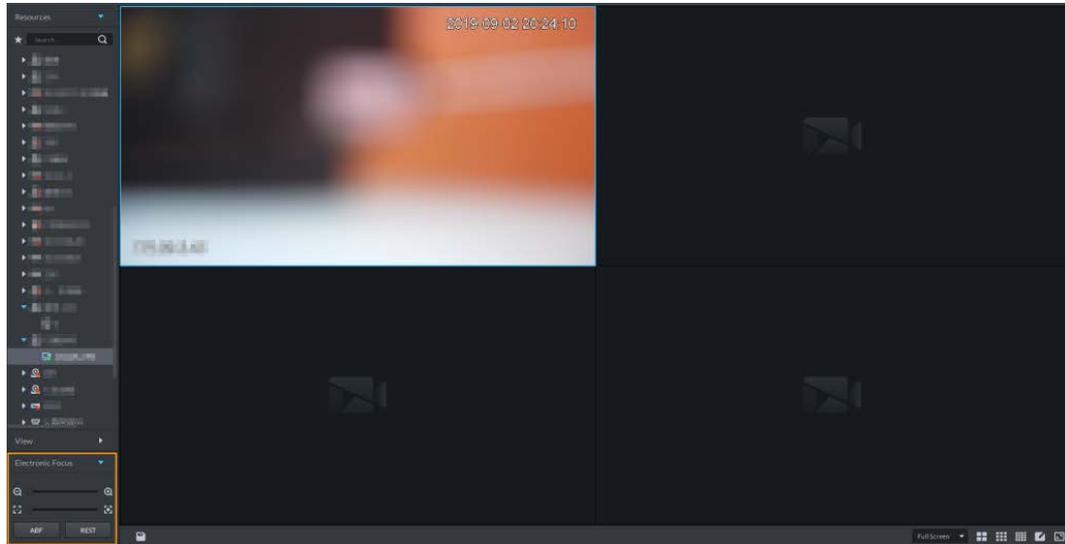
Table 6-4 Description

Parameters	Description
Zoom +/- (for embedded zoom lens)	Zoom in/out. Click or click and hold [icon] or [icon], or drag the slider [icon] to the left or right to zoom in/out.
Focus +/-	Adjust camera focus to achieve the best video definition. Click or click and hold [icon] or [icon], or drag the slider [icon] 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 page, 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 6-7 Start tour
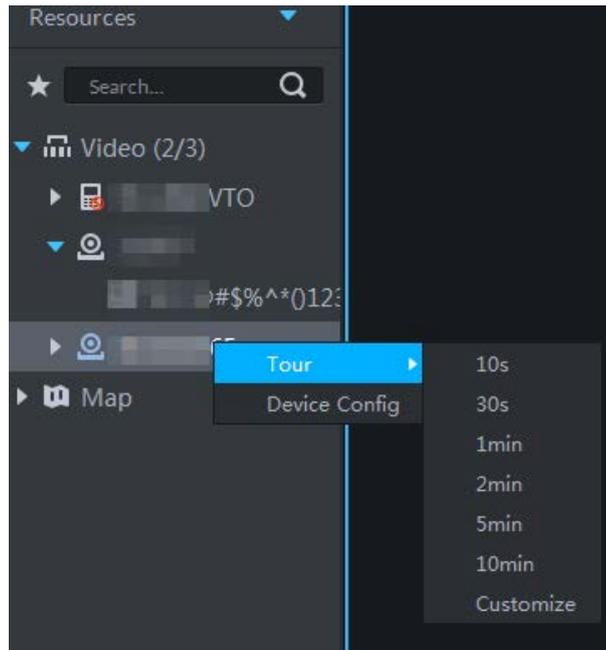
◇ To view remaining time of a channel during tour, check .

◇ 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 page, right-click the window, select **Window Mode**, and then select a mode. For example, select a 1+3 mode.

To exit the **Window Mode**, right-click the window and then select ⊠.

Figure 6-8 Split mode
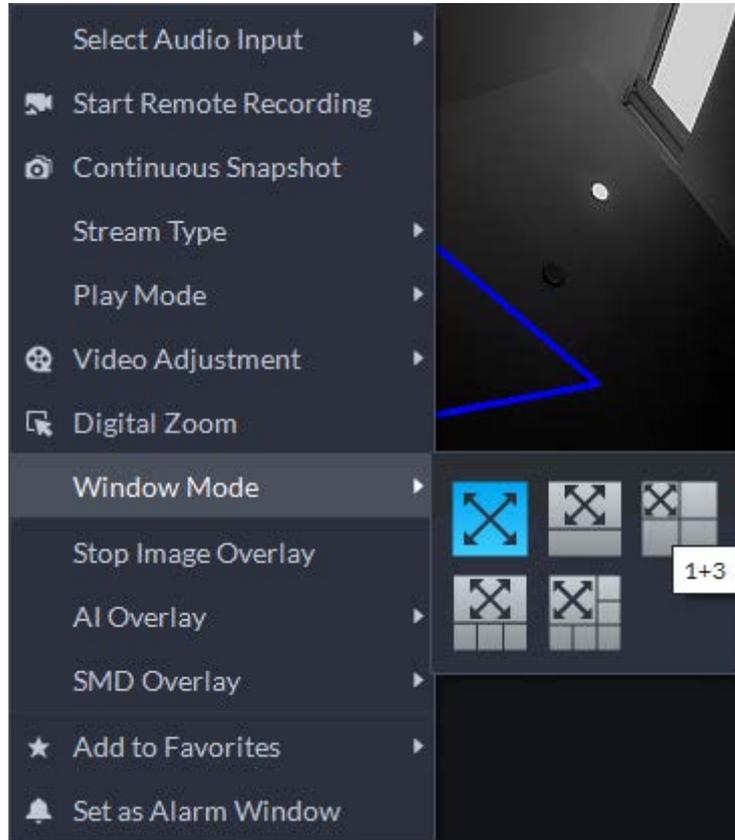
Figure 6-9 1+3 mode
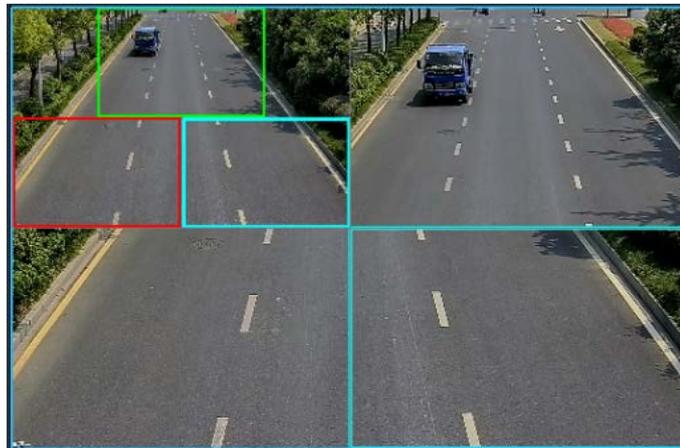
- View real-time events.

  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 corner: 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 6-10 Lock/unlock the door
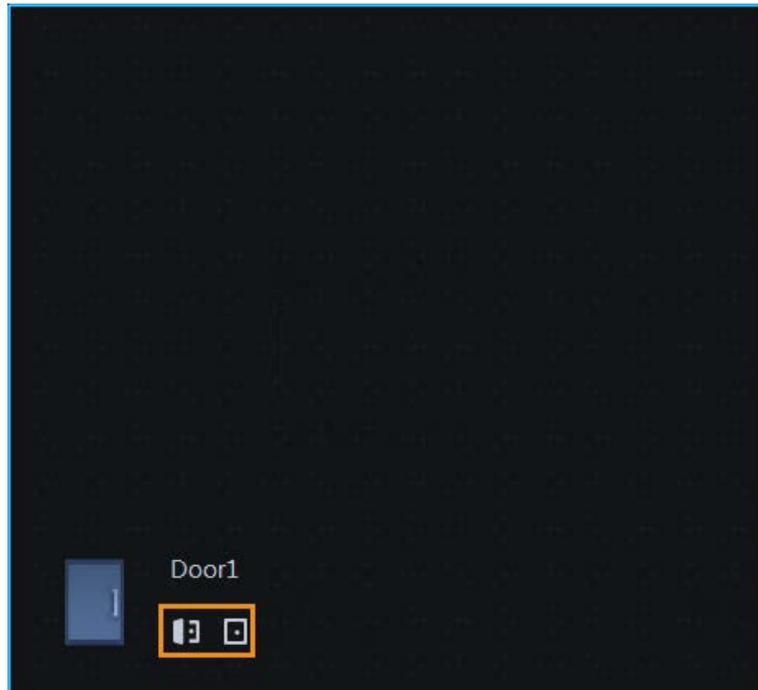
● Video intercom.

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

Figure 6-11 Video intercom
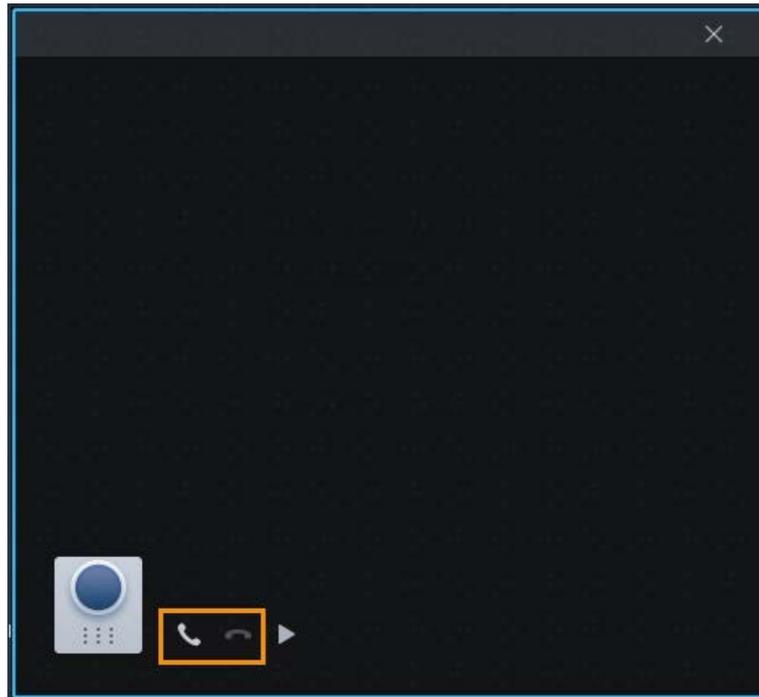
6.1.2.2 View

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.

6.1.2.2.1 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** page, 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 6-12 Create a new folder
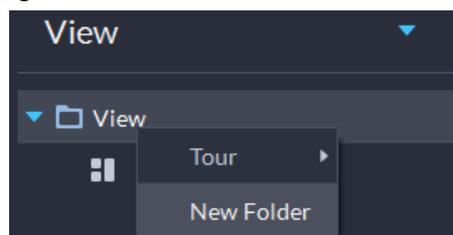
3) Enter a folder name, click **OK**.

Step 4   Create view.

1) Customize the window split mode, view real-time videos of channels in the windows,

and then click 📼 on the upper-right corner.

2) Enter a name for the view, select a view group it belongs to, and then click **OK**.

6.1.2.2.2 Viewing View

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

Figure 6-13 Go to video tour page
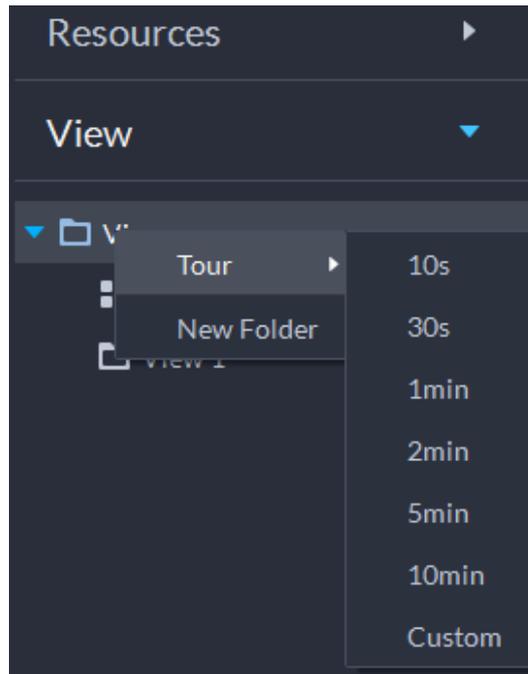
Figure 6-14 View tour
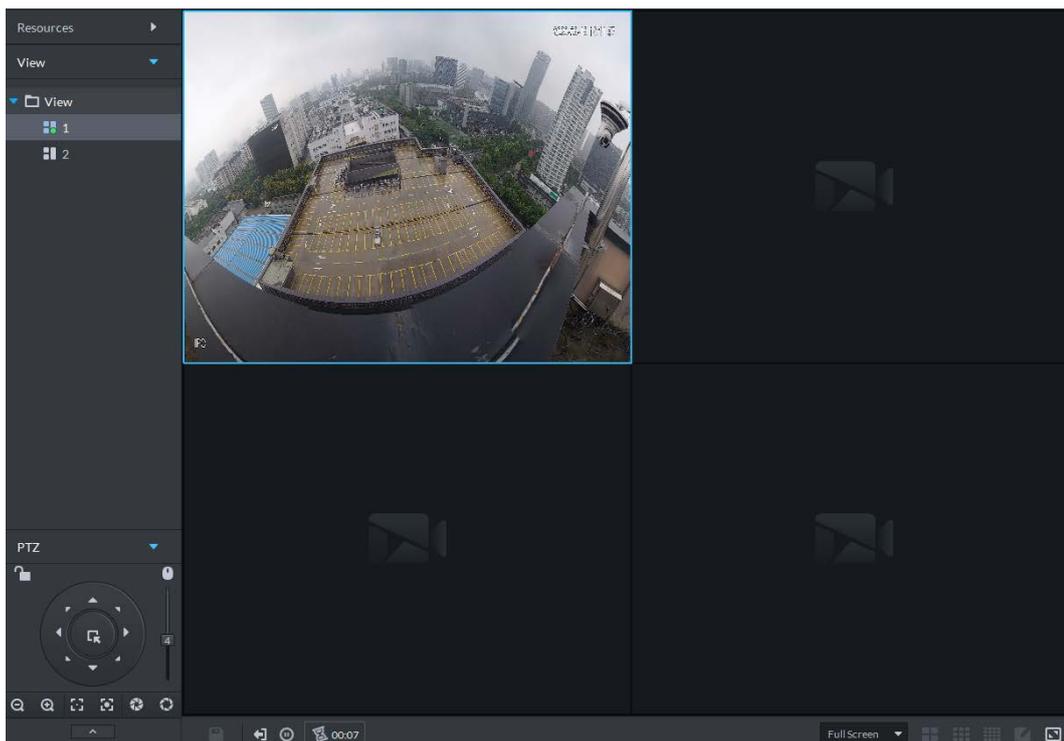
◇ To view remaining time of a channel during tour, check ⬦00:02.

◇ To pause, click ⬥.

◇ To exit tour play, click ⬥.

6.1.2.3 Favorites

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

6.1.2.3.1 Creating Favorites

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then select **Monitoring Center**.

Step 2   Click ![icon].

Step 3   Create favorites.

1) Click ![icon].

Figure 6-15 Favorites
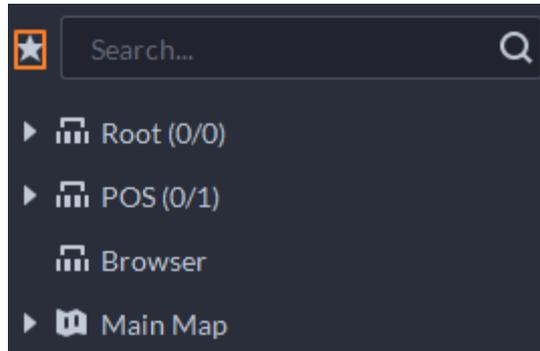
2) Right-click root node or created favorites, and then select **New Folder**.

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

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

4) Click ![icon].

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**.

6.1.2.3.2 Viewing Favorites

- Live view

On **Monitoring Center** page, click ![icon], 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** page, click ![icon], 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 ![icon].

◇ To pause, click ![icon].

◇ To exit tour play, click ![icon].

6.1.2.4 PTZ

Operate PTZ cameras during live view on the DSS Client.

6.1.2.4.1 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.

Procedure

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

Step 2   Click ▭.

Figure 6-16 Go to PTZ control panel
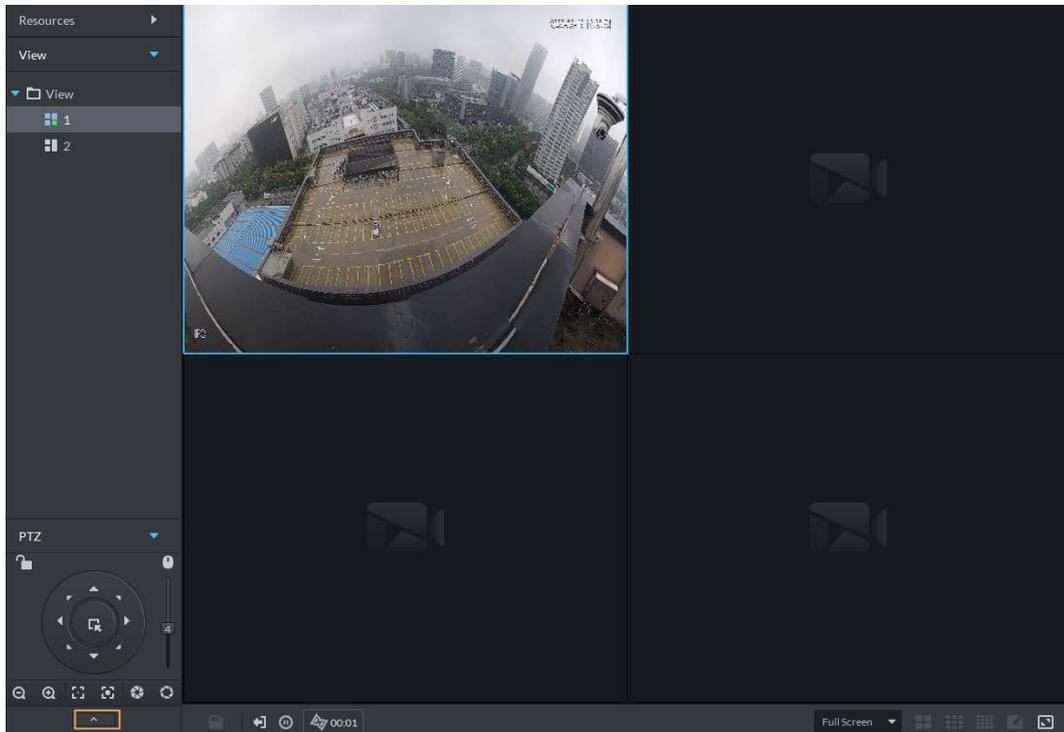
Step 3   Click ▭.

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.

6.1.2.4.2 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** page, open the video of a PTZ camera.

Step 2   Click ▭.

Figure 6-17 Go to PTZ control panel
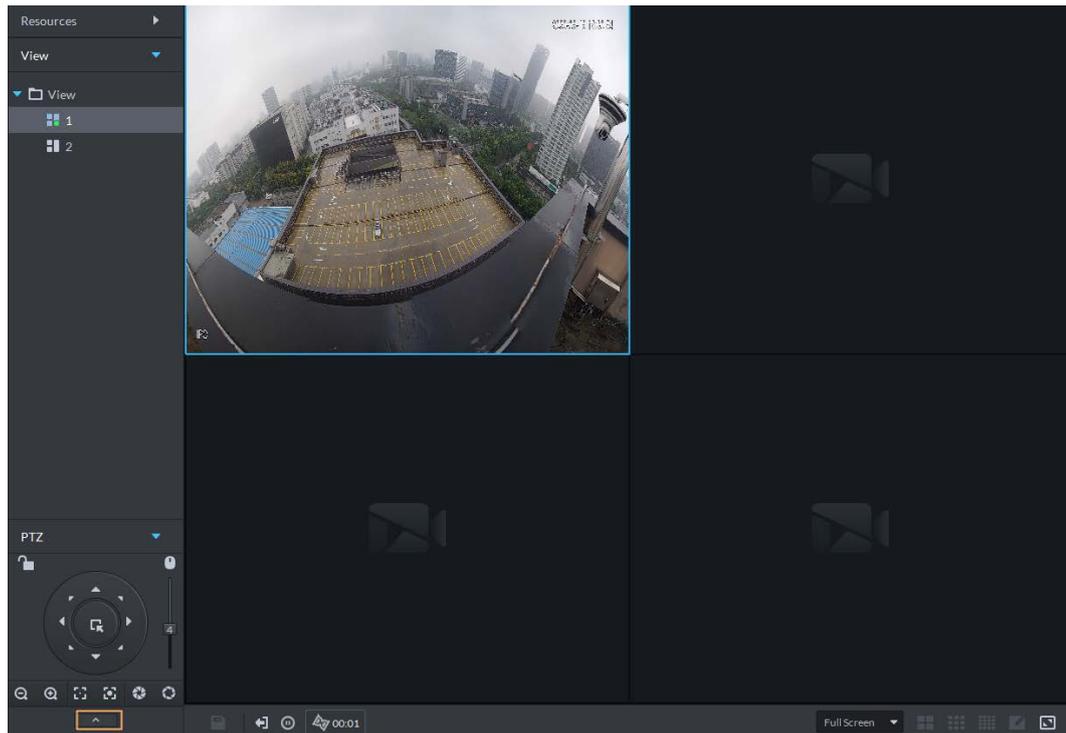
Step 3   Click ![icon].

Step 4   Click ![icon].

Step 5   Add tours.

1) Enter tour name, and click ![icon].

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 ![icon], then camera goes back and forth among the presets.

6.1.2.4.3 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** page, open the video of a PTZ camera.

Step 2   Click ![icon].

Figure 6-18 Go to PTZ control panel
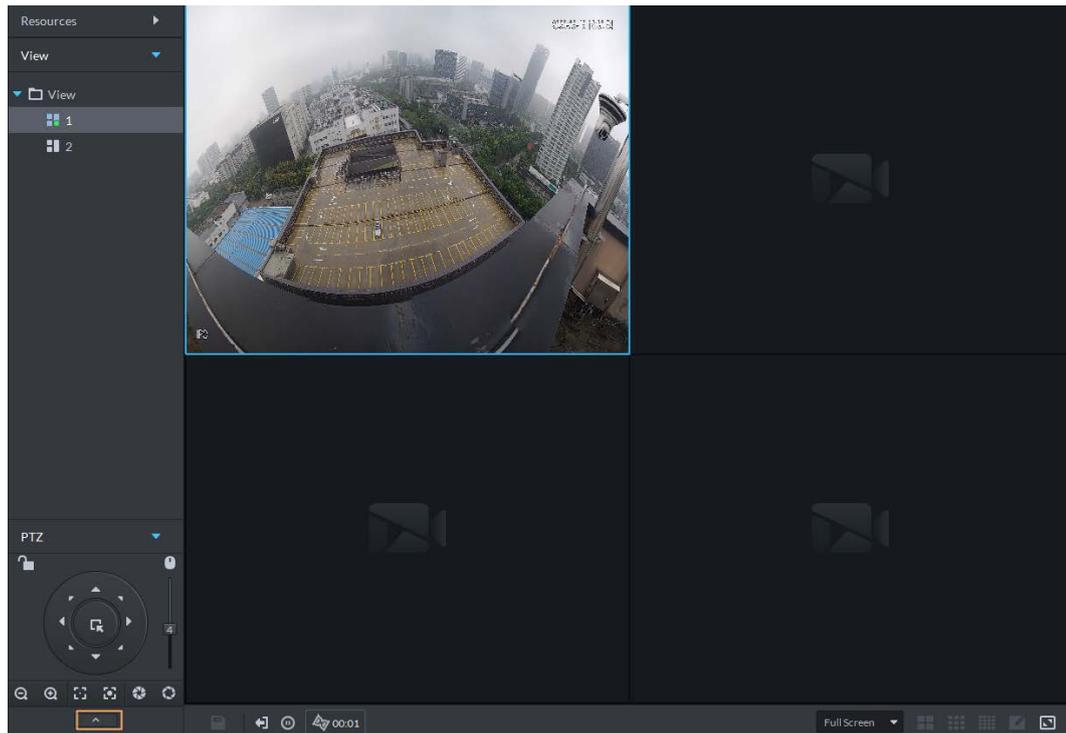
Step 3   Click .

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.

6.1.2.4.4 Enabling/Disabling Pan

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

6.1.2.4.5 Enabling/Disabling Wiper

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

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

6.1.2.4.6 Enabling/Disabling Light

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

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

6.1.2.4.7 Configuring Custom Command

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

Step 2   Click [⌃] .

Figure 6-19 Go to PTZ control panel
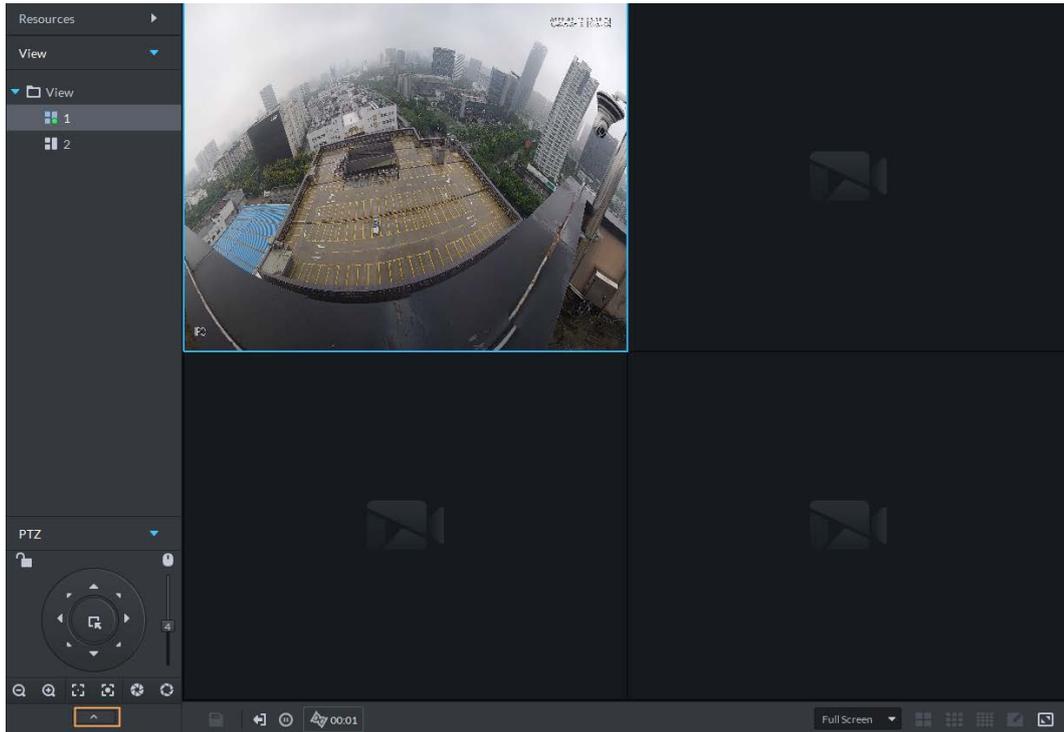
Step 3   Enter your command in the **Command** box.

Figure 6-20 Custom command
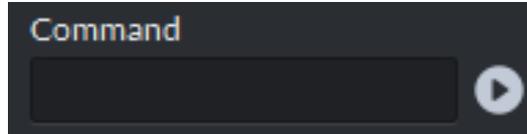
Step 4   Click [▶] to show the command functions.

6.1.2.4.8 PTZ Menu

Step 1   On the **Monitoring Center** page, open the video of a PTZ camera.
Step 2   Click [⌃] .

Figure 6-21 Go to PTZ control panel
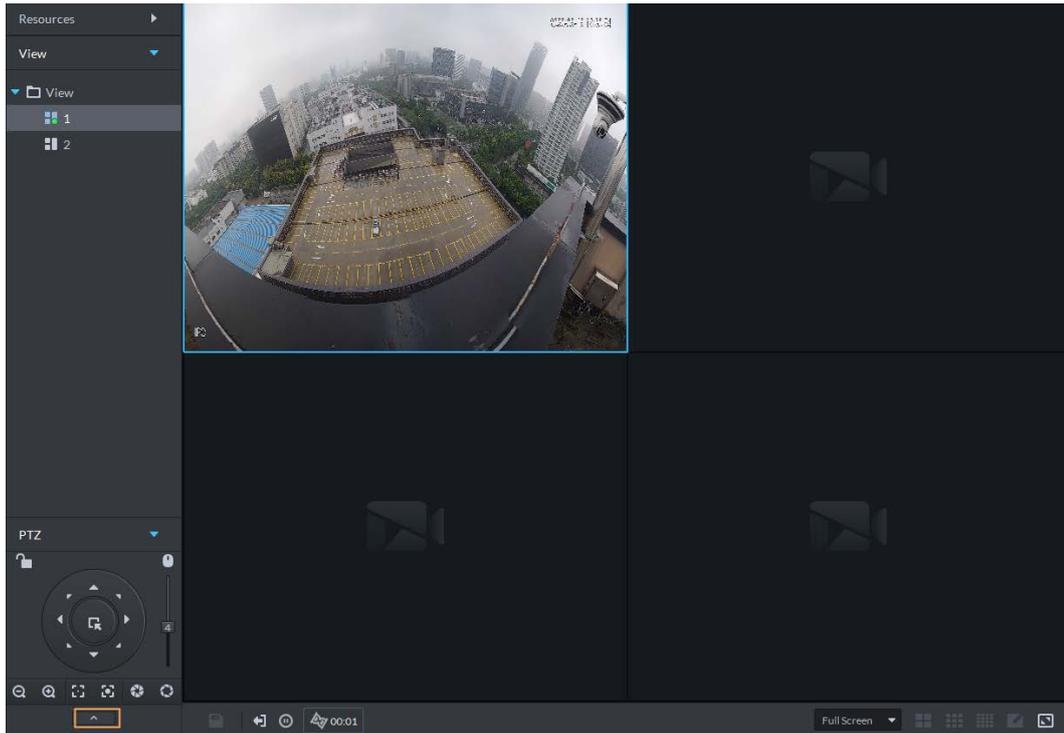
Step 3   Click [icon].

Step 4   Click [icon].

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

Figure 6-22 Go to PTZ menu configuration page
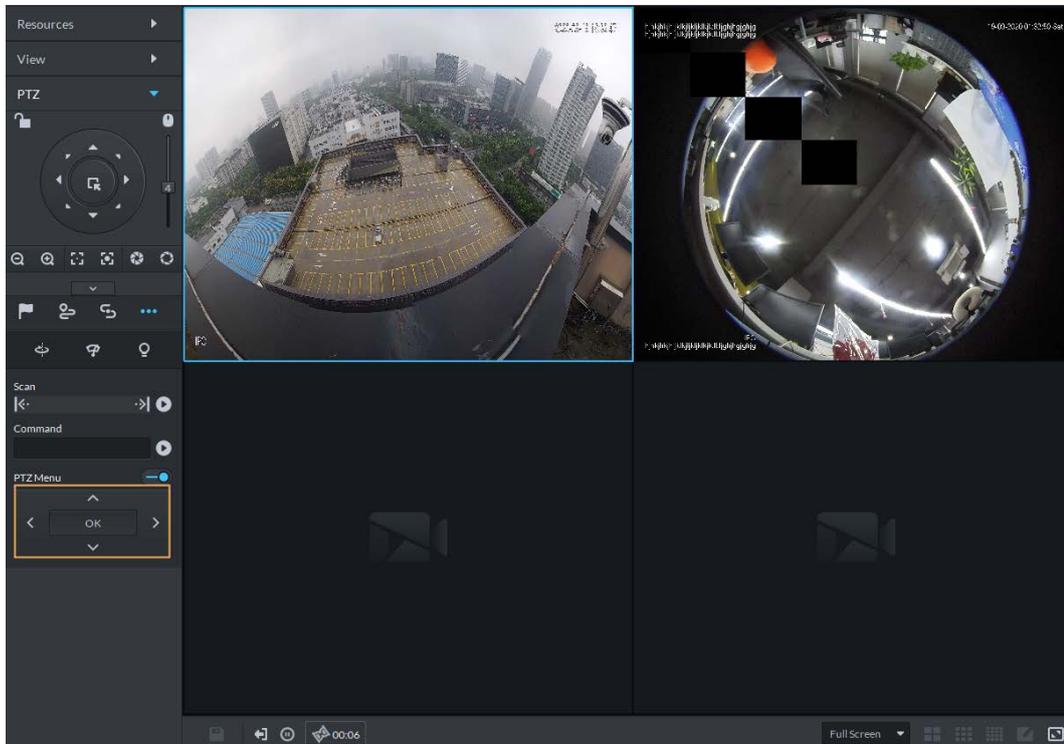
Table 6-5 PTZ menu description

Parameters	Description
[icon]/[icon]	Up/down.

Parameters	Description
◀/▶	Left/right. Point to set parameters.
◉▬	Click ◉▬ to enable PTZ menu function. System displays main menu on the monitor window.
▬◉	Click ▬◉ to close PTZ menu function.
OK	It is the confirm button. It has the following functions. ● If the main menu has the sub-menu, click **OK** to enter the sub-menu. ● 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 page. 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 page. 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 page. 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.

6.1.2.5 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.

6.1.2.5.1 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 "4 Basic Configurations".
  ◇ When adding cameras, select **Encoder** from **Device Category**.
  ◇ **Features** of fisheye camera is set to **Fisheye**. For details, see "4.2.2.5.1 Modifying Device Information".

Figure 6-23 Set fisheye camera features
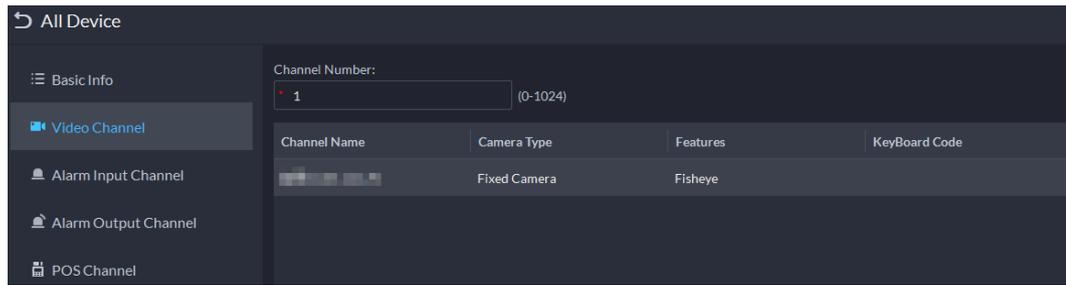
6.1.2.5.2 Configuring Fisheye-PTZ Smart Track

Step 1   Log in to the DSS Client. On the **Home** page, 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 6-24 Set smart track rules (1)
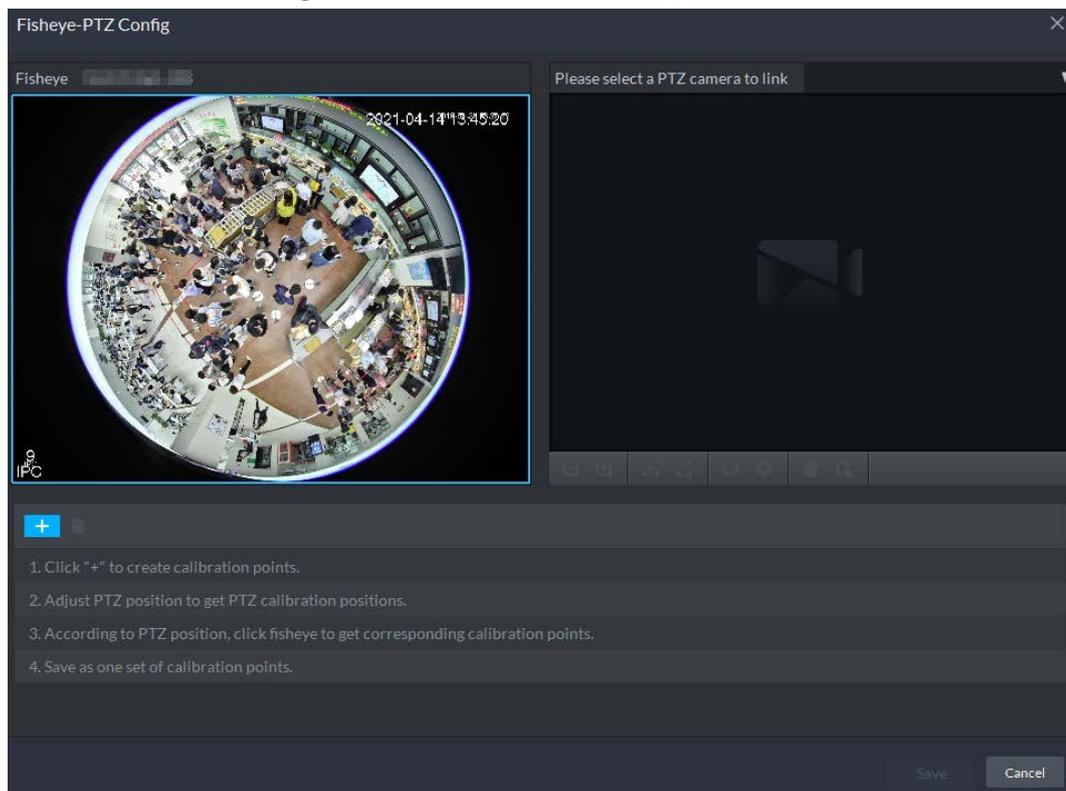
Step 5   Click ➕ and then move the ✛ of the fisheye on the left to select a position. Click 🔲 of the PTZ camera to find the position. Adjust the PTZ camera to find the position and move the PTZ to the center position (The green cross on the image).

Figure 6-25 Set smart track rules (2)
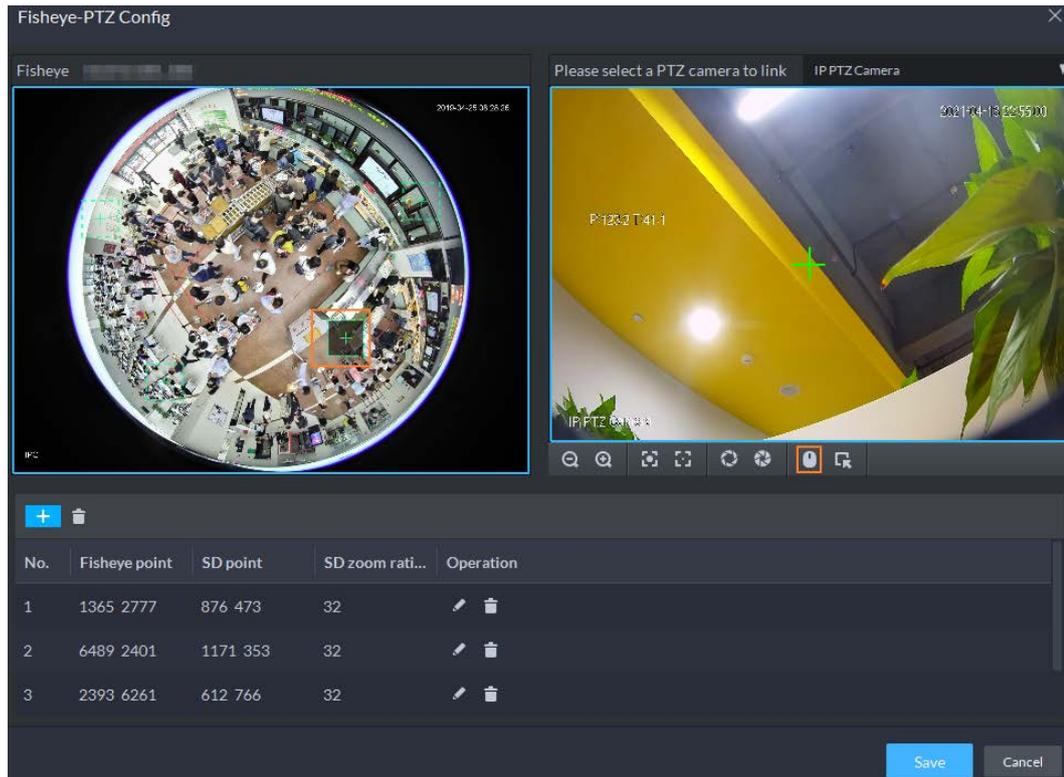
- Select 3-8 mark points on fisheye camera.
- When you find mark point on the right side of the PTZ camera, click ⊖ to zoom out PTZ.
- Click ⊡ to 3D position, and when you click a certain point on the left side of PTZ camera, it will automatically move to the center.

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**.

6.1.2.5.3 Applying Fisheye-PTZ Smart Track

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

Figure 6-26 Select a smart track channel
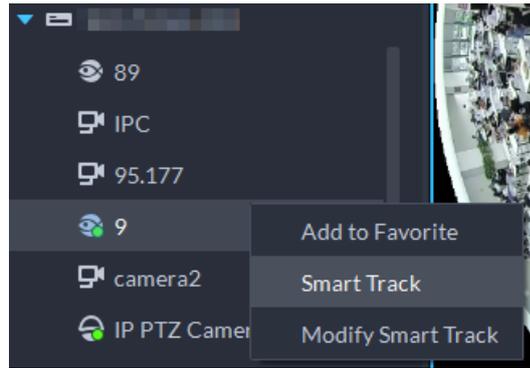
Step 2   Click any point on the left of fisheye, PTZ camera on the right will automatically rotate to corresponding position.

6.1.2.6 Bullet-PTZ Smart Track

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

6.1.2.6.1 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 "4 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 "4.2.2.5.1 Modifying Device Information".

Figure 6-27 Set camera features
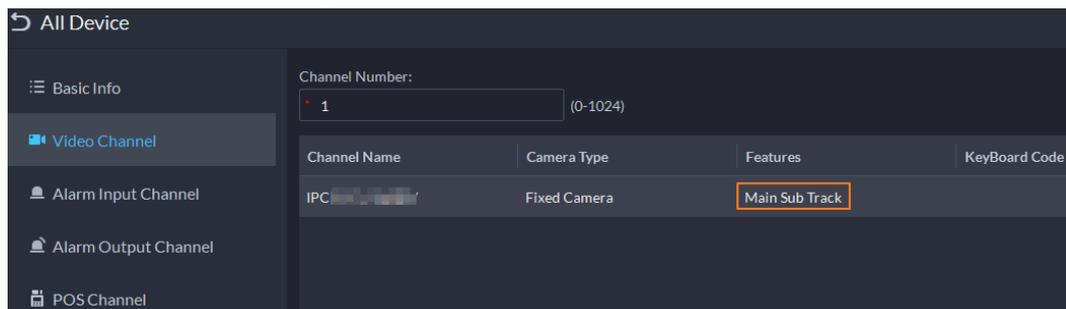
6.1.2.6.2 Configuring Bullet-PTZ Smart Track

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** page, 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 page.

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 page.

6) Click **Apply**.

6.1.2.6.3 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 6-28 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 6-29 3D positioning (1)

Before Positioning

After Positioning

Figure 6-30 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 6-31 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** page, 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 6-32 Select automatic track
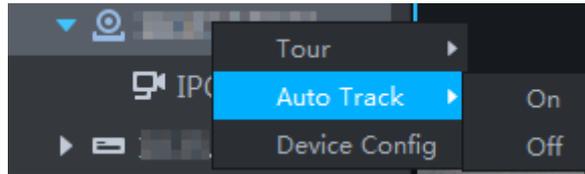
Figure 6-33 Automatic track

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.

6.1.3 Playback

Play back recorded videos.

6.1.3.1 Page Description

Log in to the DSS Client. On the **Home** page, click ![icon], and then click **Monitoring Center**. Click the **Playback** tab.

Figure 6-34 Playback page
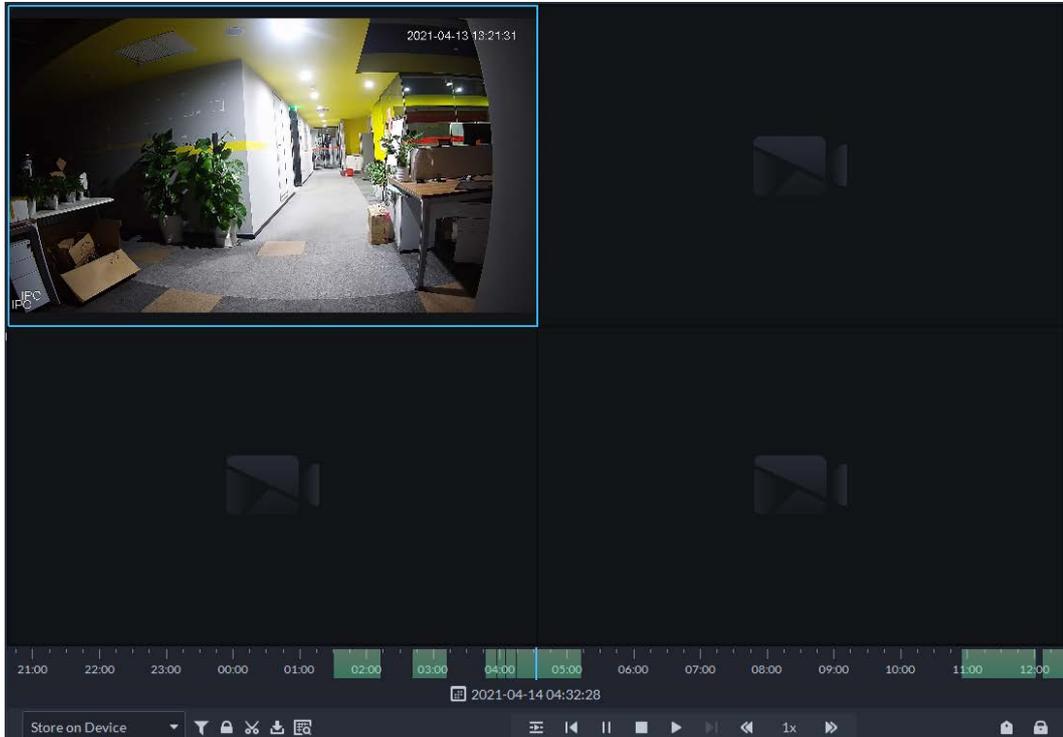
Table 6-6 Description

Icon	Description
![lock icon]	Lock the video stored to the server within some period of designated channel. Locked video will not be overwritten when disk is full.
![cut icon]	Cut video
![download icon]	Download video
![filter icon]	Filter video according to record type.
![dynamic detection icon]	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.
![playback icon]	Play back recording files of the same period from different channels on selected windows.
![stop/pause icon]	Stop/pause playback
![frame icon]	Frame by frame playback/frame by frame backward.
![fast/slow icon] 1x	Fast/slow playback. Max. supports 64X or 1/64X.
![time bar icon]	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.
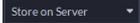
Icon	Description
	Tag records.
	Lock records.

6.1.3.2 Playing Back Recordings

Step 1   Log in to the DSS Client. On the **Home** page, 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.
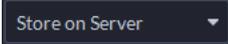
Step 4   Select the storage path of recorded video from   Store on Server   , and then click   to select the date.

Dates with blue dot means there are recordings.

Figure 6-35 Playback page
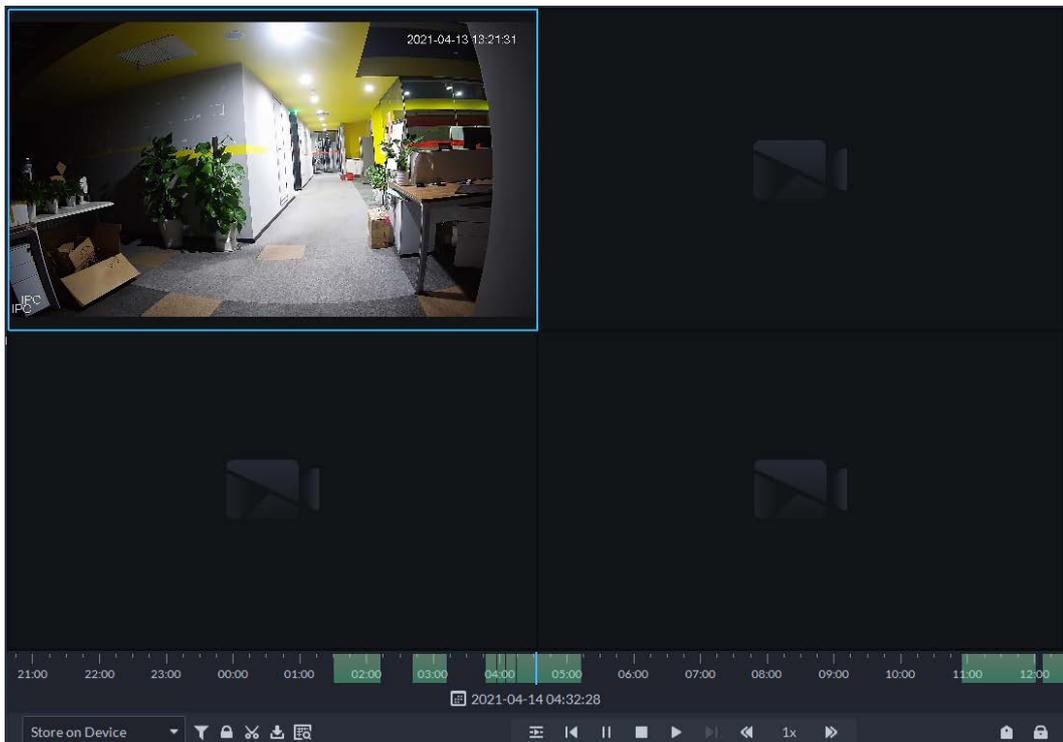
Step 5   Click   to play the video.

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

Figure 6-36 Video playback
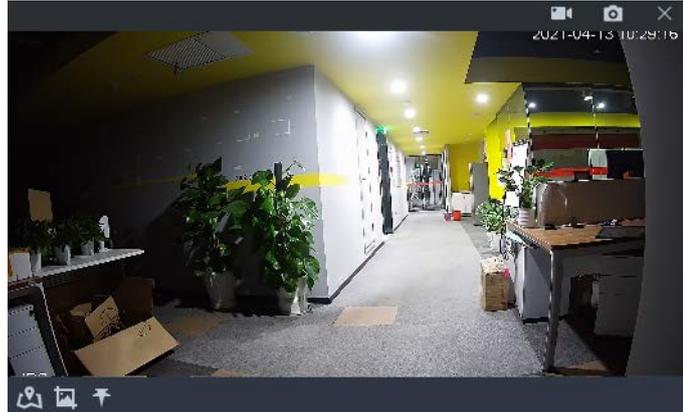
Table 6-7 Description

Icon	Name	Description
	Take a recording on the device	Click this icon to start recording. The recorded video is stored locally. The saving path is C:\DSS\DSS Client\Record\ by default.
	Take a snapshot on the device	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 page 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 6-37 Shortcut menu
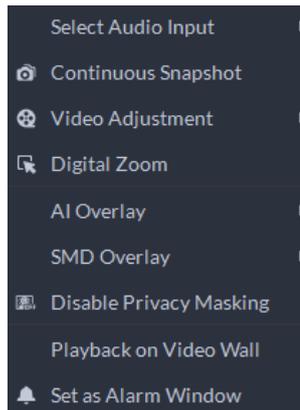
Table 6-8 Description

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 "9.3.5 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 "6.1.5 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.

6.1.3.3 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.

Procedure

Step 1   Log in to the DSS Client. On the **Home** page, 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.

📖
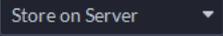
Dates with blue dot means there are video recordings.

Figure 6-38 Playback page
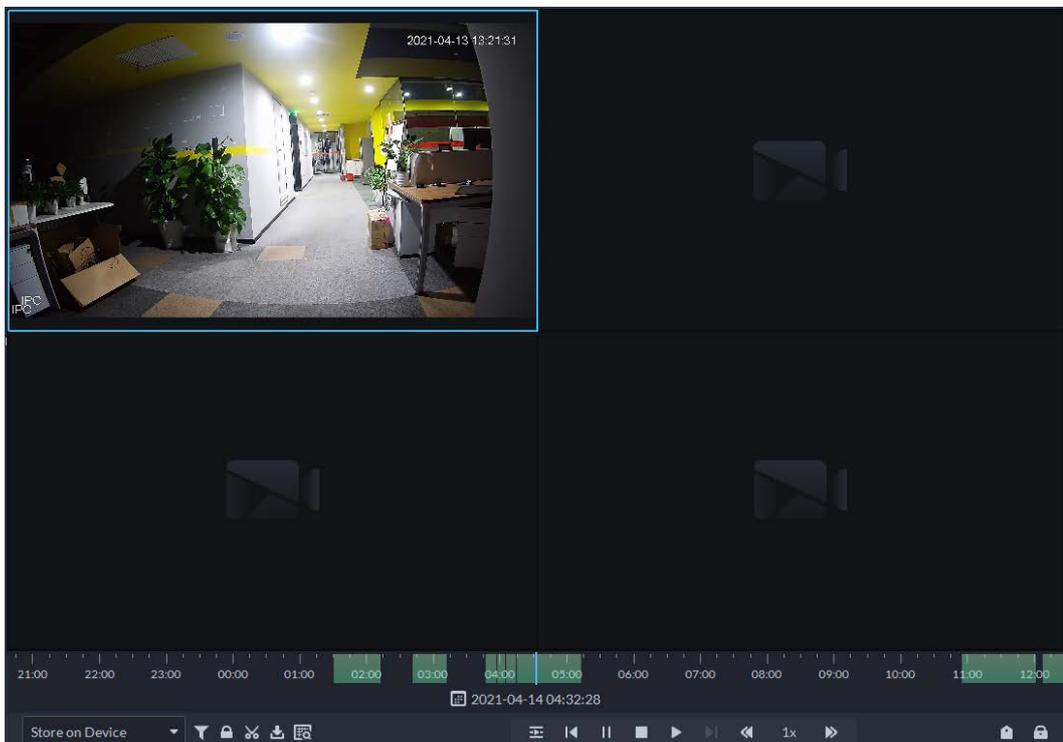
Step 5   Select a window that has recorded video, and then click 🔒 on the bottom of the page, and then click on the timeline to mark the start point and end point of the video clip you need.

Figure 6-39 Lock record
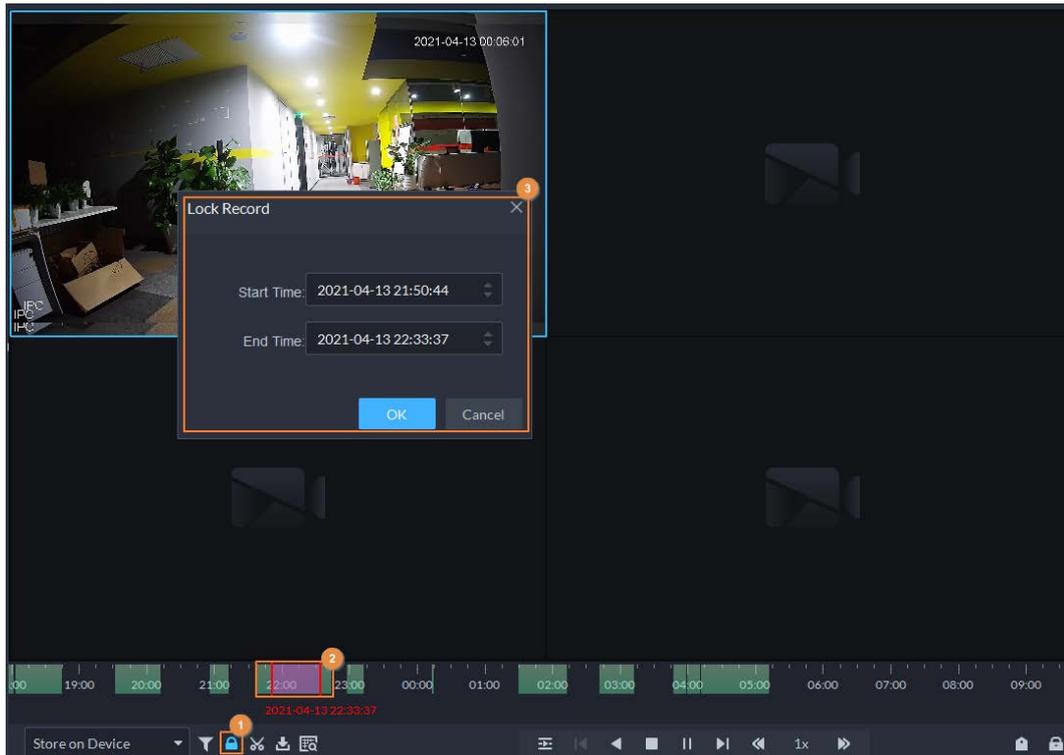
Step 6   Confirm the start and end time, and then click **OK**.

Related Operations

Click ![icon] on the lower-right corner, and then all the recordings locked by the user currently logged in to the client are displayed. Double-click one to quickly play the recording.

6.1.3.4 Tagging Videos

You can tag records of interest for quick search.

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], 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 ![icon] to select the date.

The search results are displayed.

Dates with blue dot means there are video recordings.

Figure 6-40 Playback page
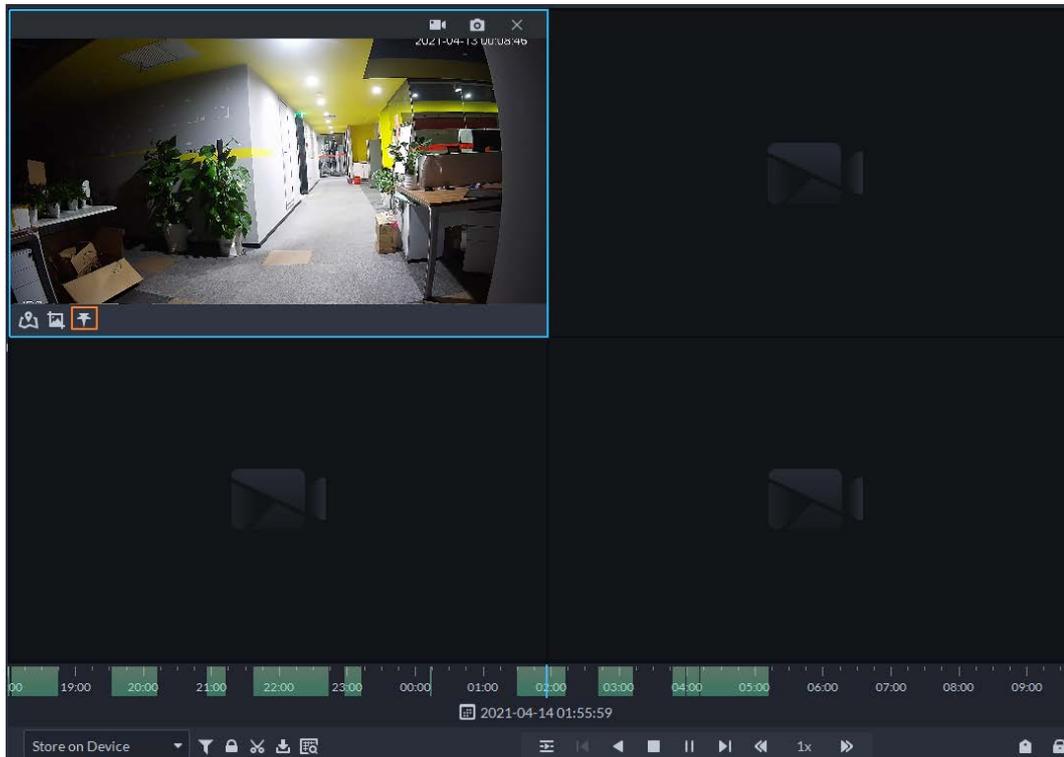
Step 5   Point to the window that is playing record, and then click   .

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

6.1.3.5 Filtering Recording 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** page, 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. Each section on the time bar in green indicates a recorded video of the type you selected.

Figure 6-41 Filter record type
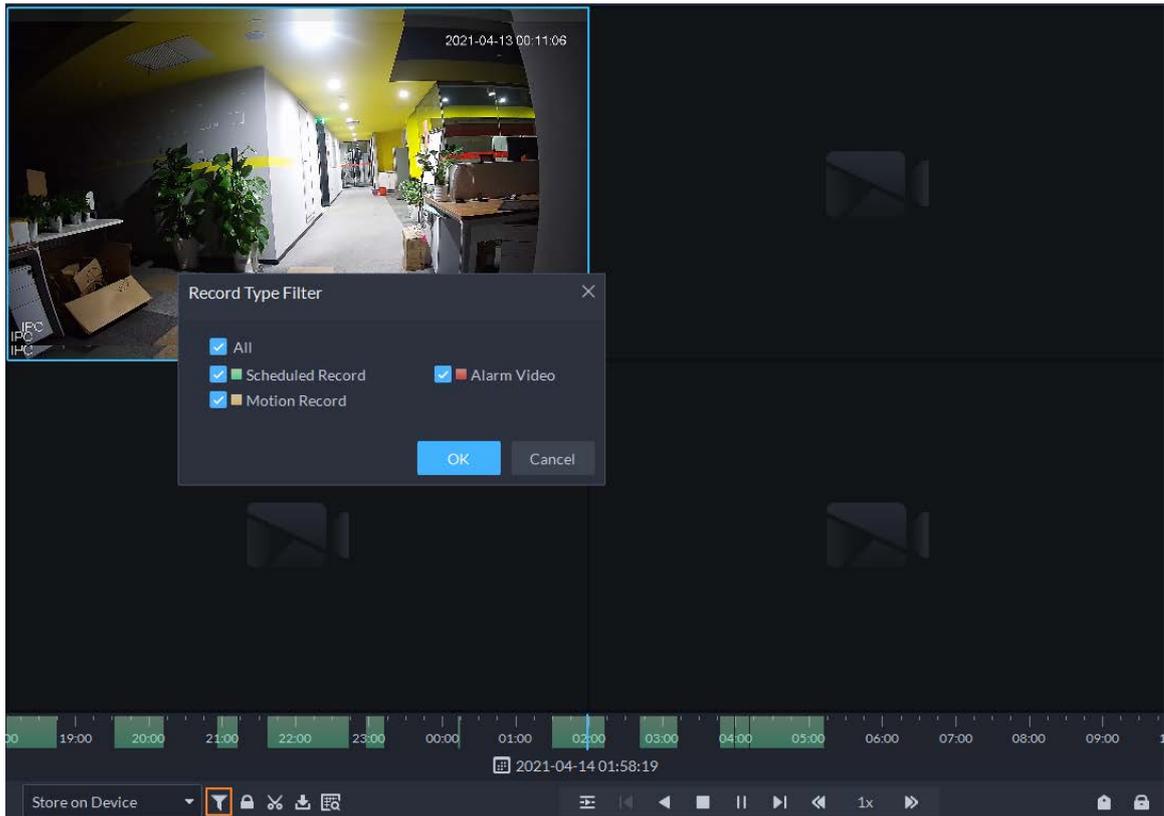
6.1.3.6 Clipping Videos

Step 1   Log in to the DSS Client. On the **Home** page, 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.
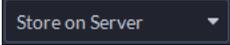
Dates with blue dot means there are video recordings.

Figure 6-42 Playback page
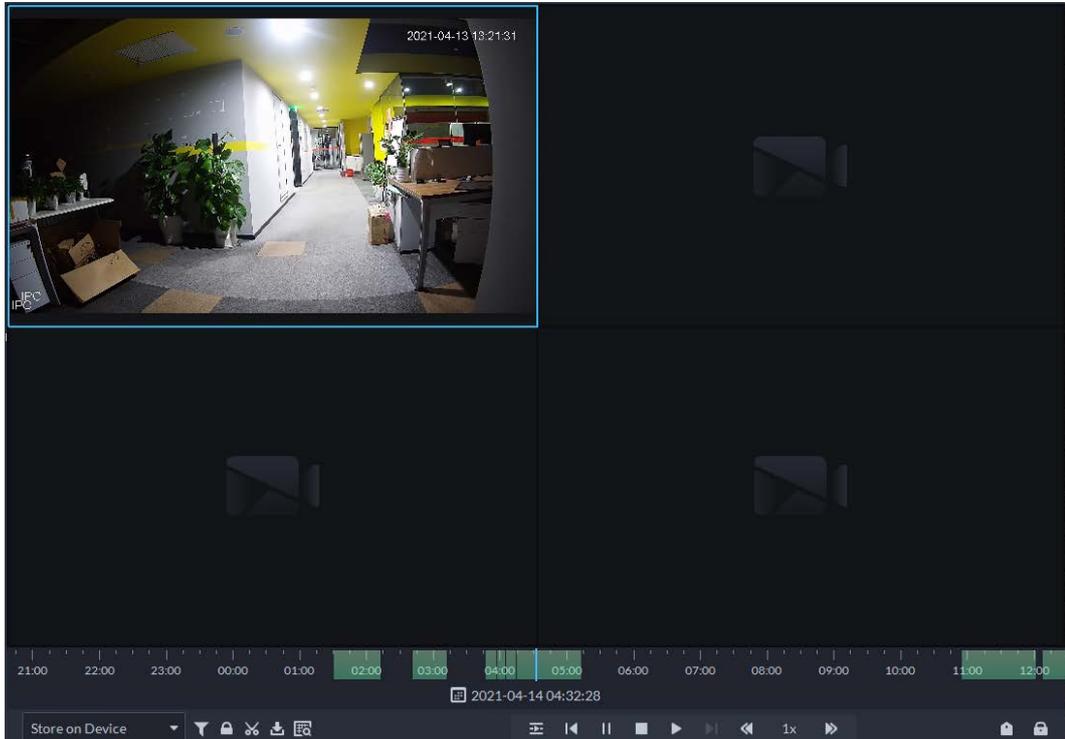
Step 5   Select a date with video recordings, and then click ![scissors icon].

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 6-43 Download recorded video
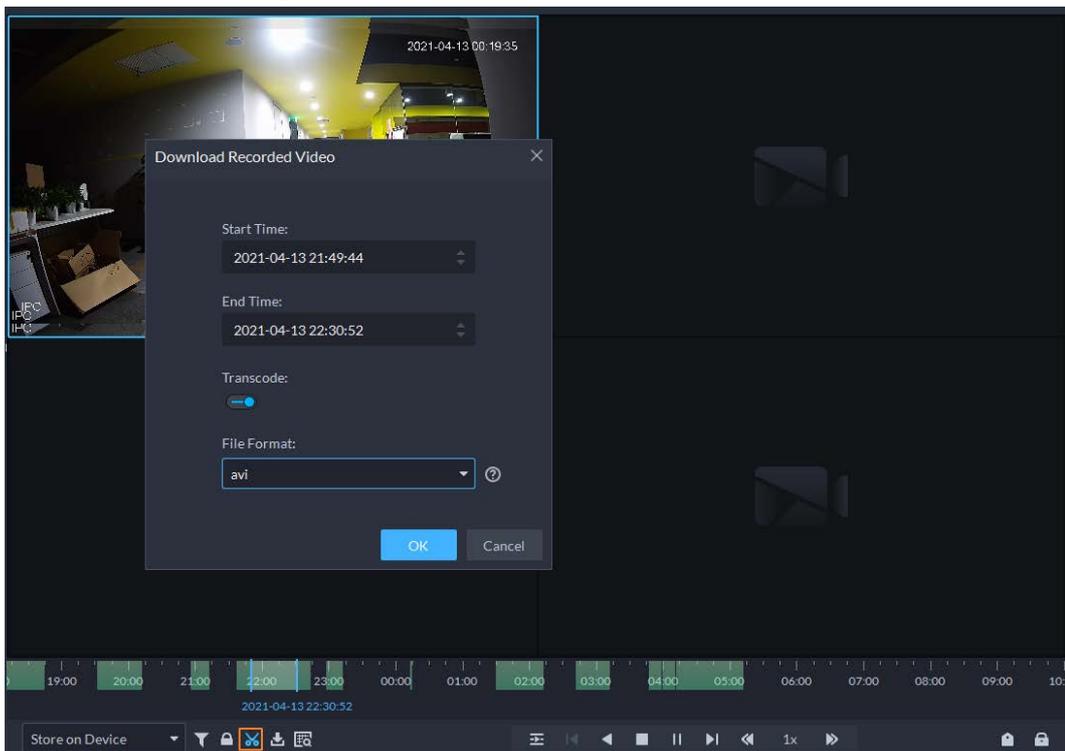
Step 7   Enter the password for logging in to the DSS client.

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

Step 9   Click **OK**.

6.1.3.7 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** page, 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 6-44 Playback page
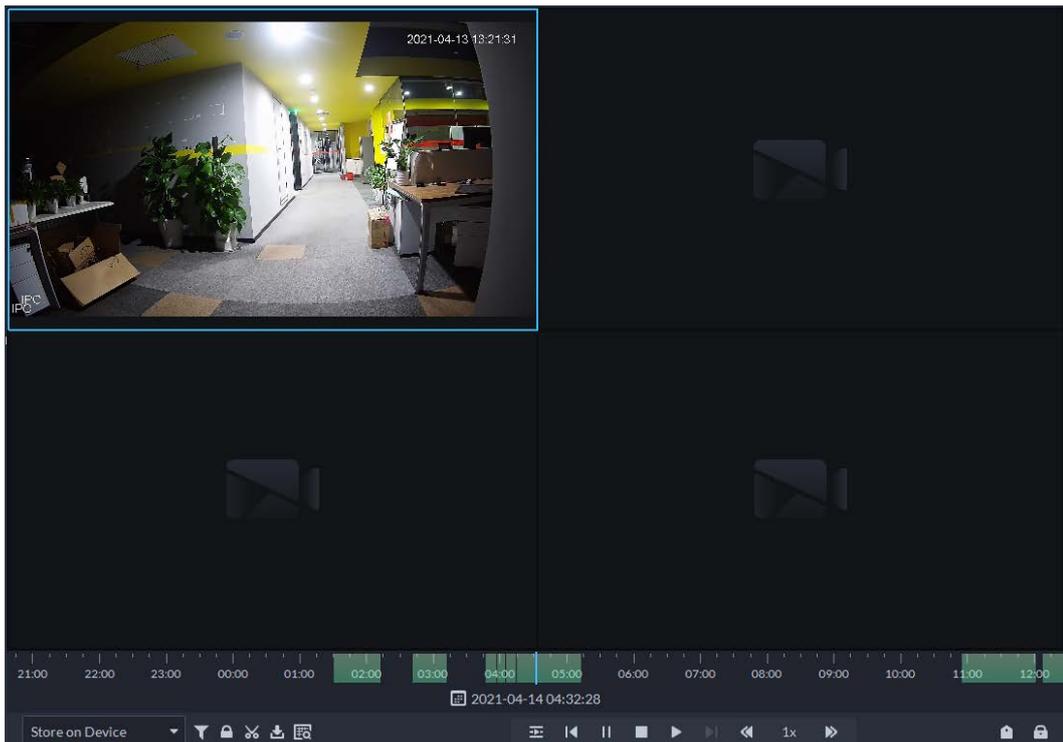
Step 5   Select a window that has videos, click [ ], and then select a type.
The smart search page is displayed, with 22 × 18 squares in the window.

Figure 6-45 Smart search
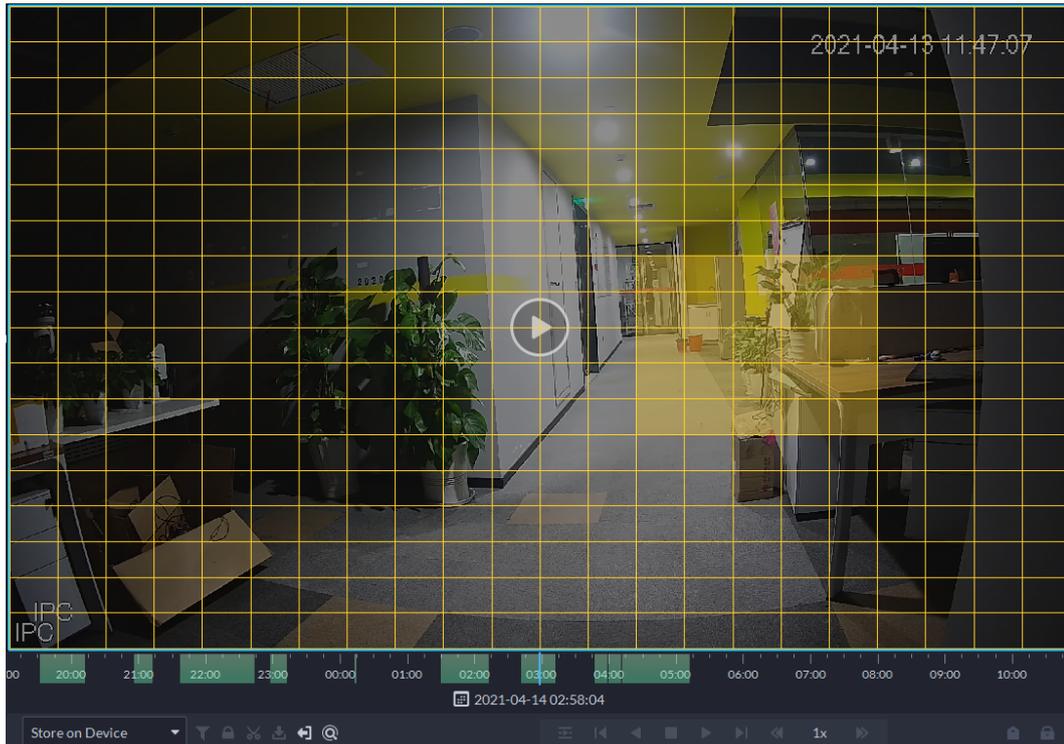
Step 6   Click the squares and select detection areas.

📖

- Select a detection area: Point to image, click and drag to select a 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.

6.1.4 Map Applications

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

Prerequisites

Make sure that you have configured a map. For details, see "5.2 Configuring Map".

Procedure

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

Step 2   Click 🔍.

Step 3   In the map list, click a map.

Figure 6-46 View map
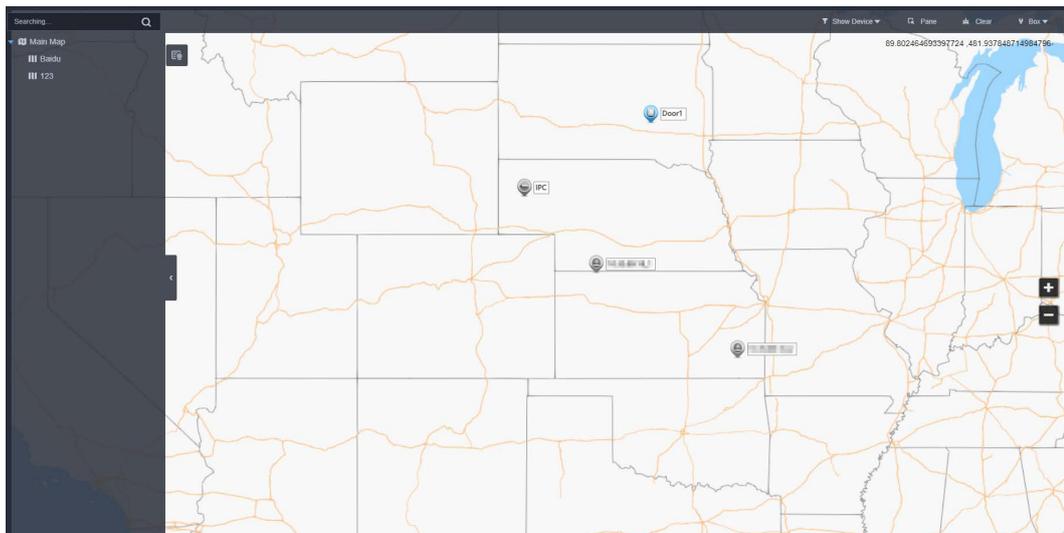
Step 4   Click a device on the map, and then you can view video, cancel alarms, view longitude and latitude, and more.

Related Operations

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

- Hide Device Name

  Only display the icons of devices.

- View live video

  Click **Pane**, select devices on the map, and then click ![icon] to view videos in batches; or click ![icon] on the map, and then select to view videos.

- Playback

  Click **Pane**, select devices on the map, and then click ![icon] to view videos in batches; or click ![icon] on the map, and then select to view videos.

- Cancel alarms

  Click a device on the map, and then select ![icon].

- 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 ![icon] to view the information of the sub map.

- Double-click ![icon], and then the platform will go to the sub map, where you can view the resources on it.

6.1.5 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.

6.1.5.1 Configuring Video Wall

6.1.5.1.1 Page Description

Before using the video wall function, you should get familiar with what you can do on the video wall page.

Figure 6-47 Video wall
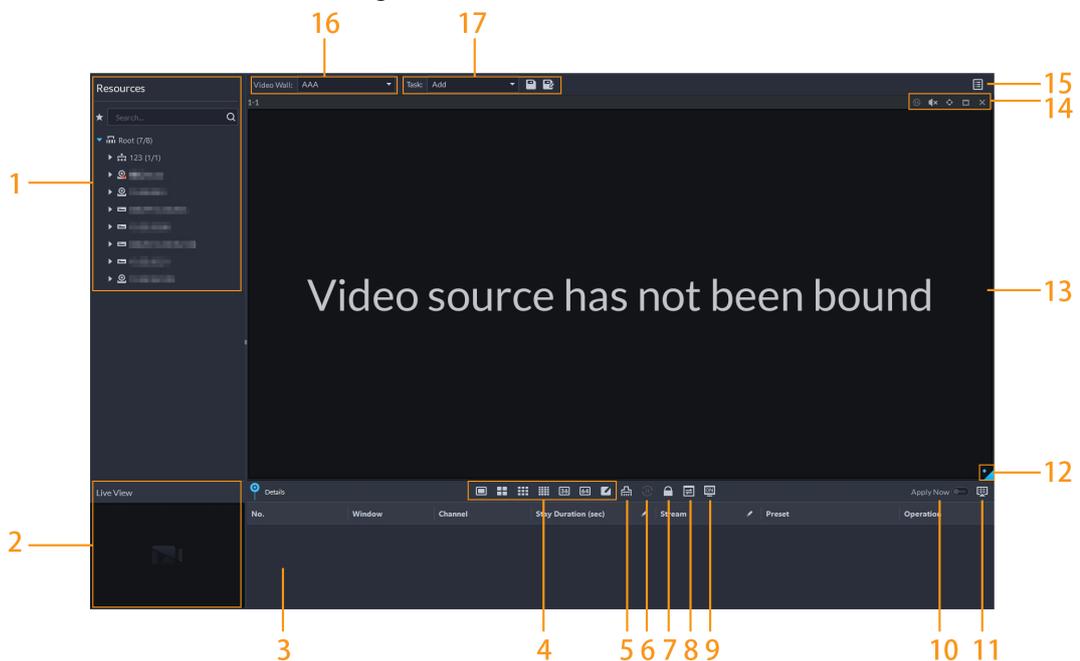
Table 6-9 Page description

No.	Function	Description
1	Device tree	If you have selected **Device and Channel** in **Local Settings** > **General**, the device tree will display all devices and their channels. Otherwise, it will only display all channels. Click ⭐ to view channels that you have saved to favorites. You can enter keywords in [Search...] to search for the channels you want.
2	Live view	View live videos from channels.

No.	Function	Description
3	Detailed information	View the channel information in a screen of the video wall. ● Click ⊙ and view the live video of the channel in **Live View** on the lower-left corner. This can be helpful when you need to make sure whether it is the channel you want. ● Click ⬆ ⬇ to adjust the order of channels. ● Click 🗑 to delete the channel from the screen. ● Click **Stay Duration (sec)** or ✎ to define the for how long the live video of the channel will be displayed during each tour. ● Click **Stream** or ✎ to change the video stream of the channel.
4	Window split	Select how you want the window to split.
5	Clear screen	Clear all the screens.
6	Stopping or starting all tours	Stop or start all tours.
7	Lock window	If multiple screens in a video wall are configured to be a combined screen, then you can perform video roaming on the window that has been locked.
8	Display mode	Display the real-time video, or a snapshot of the real-time video every 10 minutes of the bound channel in the screen. If nothing happens after operation, you can just click another screen, then click the screen you want, and then it should work properly.
9	Turning on or off screens	Turn on or off the screens configured for the currently selected video wall.
10	Decoding to wall immediately after configuration	When a task has been configured, the platform will immediately decode channels to the video wall.
11	Decoding to wall	Manually decode channels to the video wall.
12	Video wall layout	Click to view the layout of the current video wall.
13	Video wall display area	The display area for video walls.
14	Screen operations	Includes stopping tour for the screen, muting, pasting, maximizing or restoring the screen, and closing the screen,
15	Video wall plan	Configure a timed or tour plan for the video wall. For detailed procedures, see "6.1.5.1.5 Configuring Video Wall Plans".
16	Video wall selection	Select the video wall you want to configure.
17	Display task management	Add, save, and delete tasks.

6.1.5.1.2 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 "4 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**.

6.1.5.1.3 Adding Video Wall

Add a video wall layout on the platform.

Step 1 Log in to the DSS Client, and on the **Home** page, 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 ![icon].
- 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 ![icon]
- To create a combined screen, press and hold Ctrl, select multiple screens, and then click ![icon].
- To clear the created screen, click ![icon].

Figure 6-48 Add a video wall
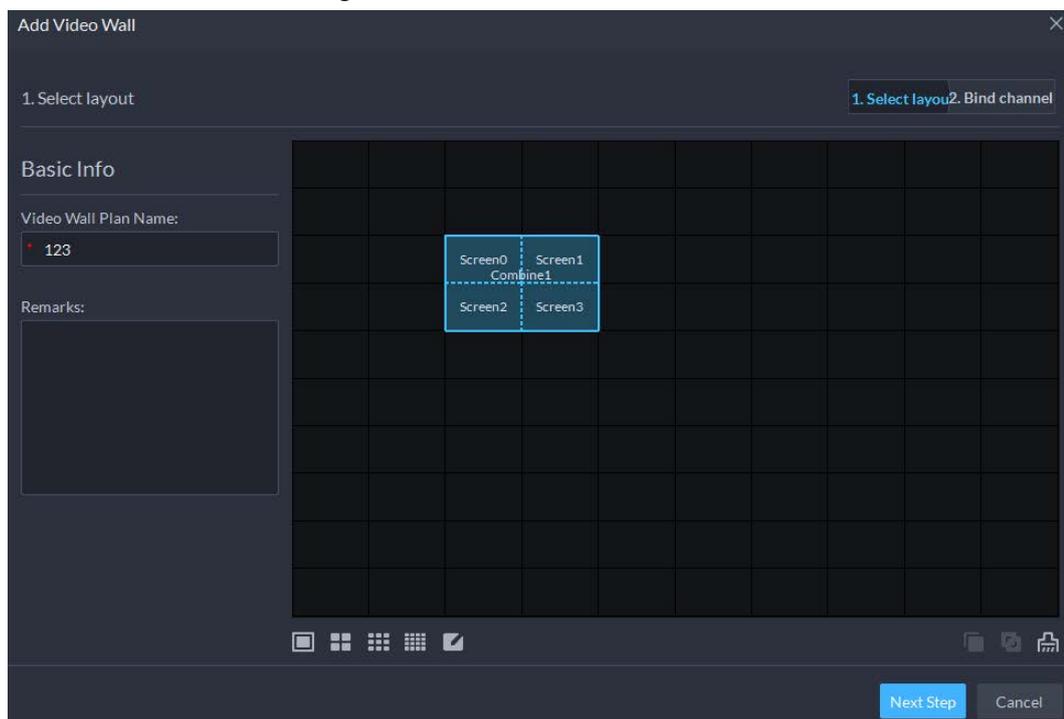
Step 4   Click **Next Step**.

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**.

6.1.5.1.4 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** page, select **Monitoring Center** > ![icon].

Step 2   In the **Task** drop-down list, select **Add**.

Figure 6-49 Add a video wall task
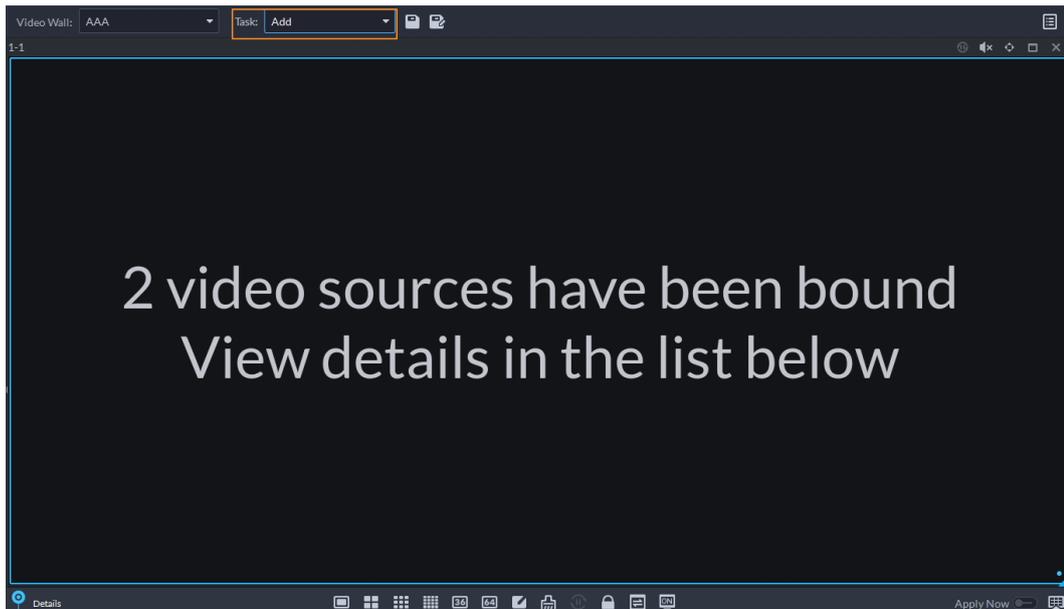
Step 3　From the device tree, select a camera, and then drag it to a screen, or select a window, drag the camera to the **Detail** section.

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 [icon].

If you have selected an existing task in the **Task** drop-down list, after dragging the video channel to the window, click [icon] 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 [icon] to start video wall display manual.
- During video wall display, click [icon] or [icon] to stop or start tour display.

Step 6　Click [icon] to start video wall display.

6.1.5.1.5 Configuring Video Wall Plans

Configuring Timed Plans

Step 1　Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > [icon].

Step 2　Click [icon] on the upper-right corner.

Step 3　Hover over [icon], and then select [icon].

Figure 6-50 Set timed plan
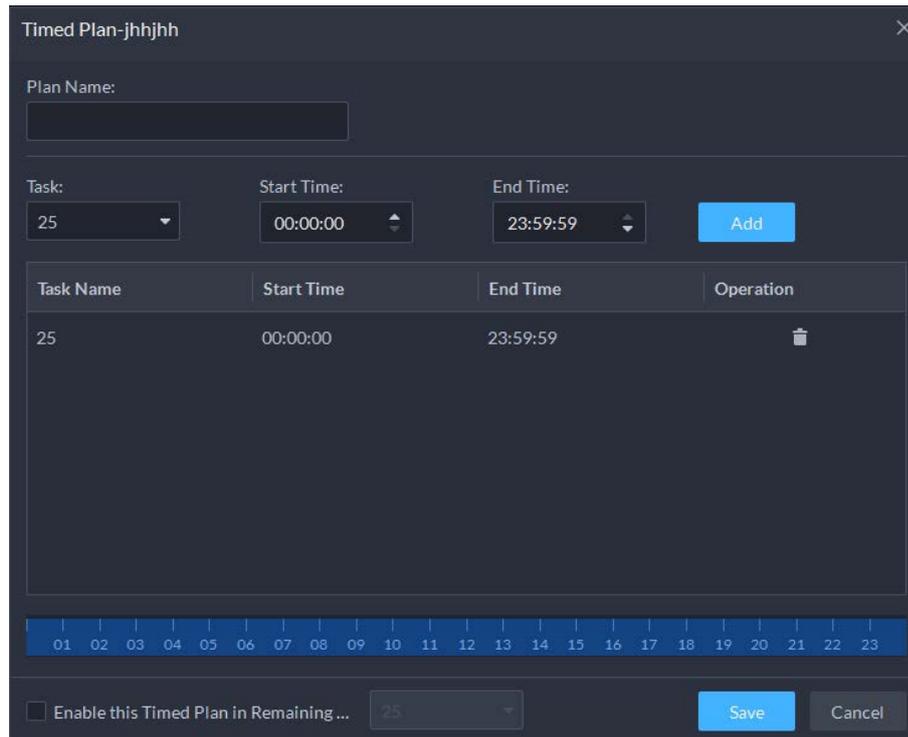
Step 4   Enter the plan name.

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 6-51 Enable timed plan
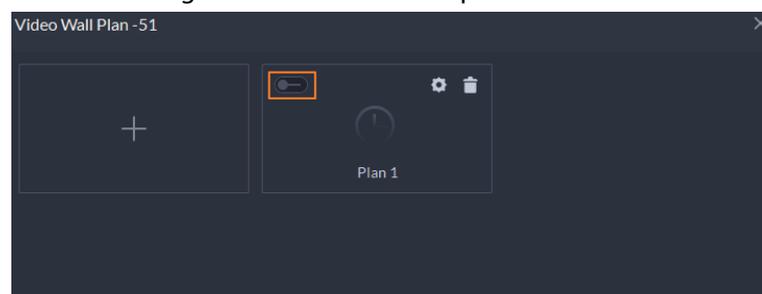
- Modify plan: ⚙.
- Delete plan: 🗑.

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** page, select **Monitoring Center** > ⊞.

Step 2   Click ▤ on the upper-right corner.

Step 3   Hover over ┼, and then select ⏱.

Figure 6-52 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 6-53 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 6-54 Enable tour plan
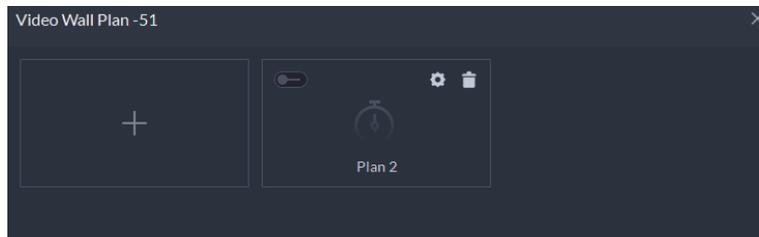
- Modify plan: Click ⚙.
- Delete plan: Click 🗑.

6.1.5.2 Video Wall Applications

Make sure that decoder video ports are connected to the video wall screens.

6.1.5.2.1 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 "6.1.5.1.4 Configuring Video Wall Display Tasks".

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

Step 2   In the **Video Wall** drop-down list, select a video wall.

Step 3   Click ▭ 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 "9.3.3 Configuring Video Wall Settings".
- For a fisheye camera, right-click it to select the installation mode for fisheye dewarping.

Figure 6-55 Bind video channel
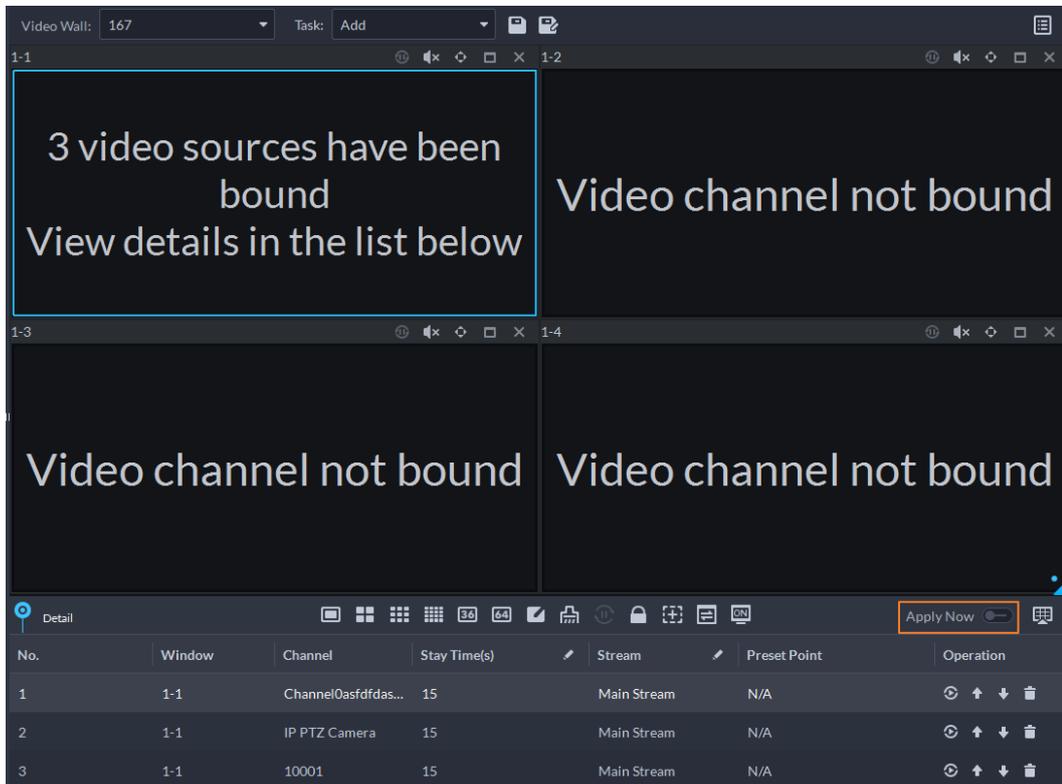
Step 5   Select a screen, and then click **Detail** to view detailed information about the screen and channel, including stream type, preset and display sequence.
- Click [icon] to view live video of the current channel on the lower left.
- Click [icon] to adjust sequence.
- Click [icon] to delete the video channel on the current window.

6.1.5.2.2 Video Wall Task Display

Display a pre-defined task on video wall.
Step 1   Log in to the DSS Client, and on the **Home** page, 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 [icon] at the lower-right corner before you can see the effect on video wall.
- Click [icon]/[icon] 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.

6.1.5.2.3 Video Wall Plan Display

Display a pre-defined plan on video wall.

📖

Make sure that there are pre-defined plans. For details, see "6.1.5.1.5 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** page, and then it changes to ⊡. Click ⊡ to start
displaying video on wall again.

Figure 6-56 Display video wall plan
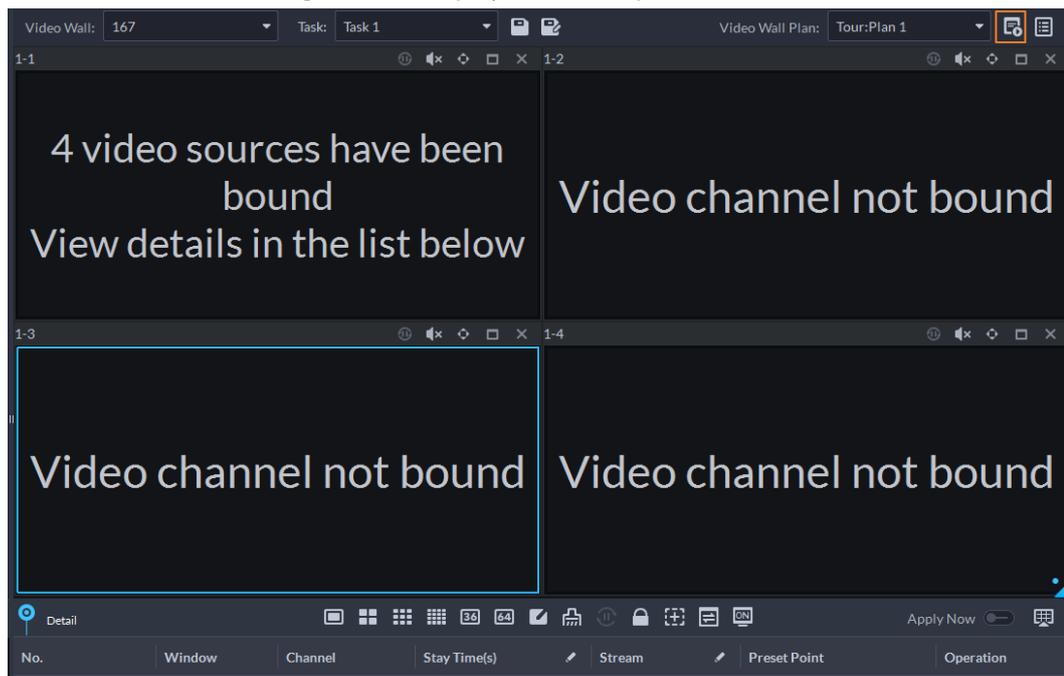
6.2 Event Center

When alarms are triggered, you will receive notifications on real-time alarms. You can view their
details, such as snapshots and recordings, and process them. If you miss alarms occurred during a
certain period, or want to check certain alarms, such as high priority alarms occurred in the past day
or all alarms that have not been processed in the past week, you can set the search conditions
accordingly and search for these alarms.
Make sure you have configured and enabled alarm events. To configure, see "5.1 Configuring
Events".

6.2.1 Real-time Alarms

View and process real-time alarms.

Step 1   Log in to the DSS Client. On the **Home** page, click ▦, and then select **Event Center**.

Step 2   Click ⚠.

Figure 6-57 Real-time alarms

Step 3 Click ![icon] to claim an alarm.

After an alarm has been claimed, the username of your account will be displayed under the **Processed by** column.

Step 4 Process alarms.

You can use the up and down arrow keys on the keyboard to quickly select other alarms.

1. Click ![icon] or double-click the alarm.

Figure 6-58 Alarm details
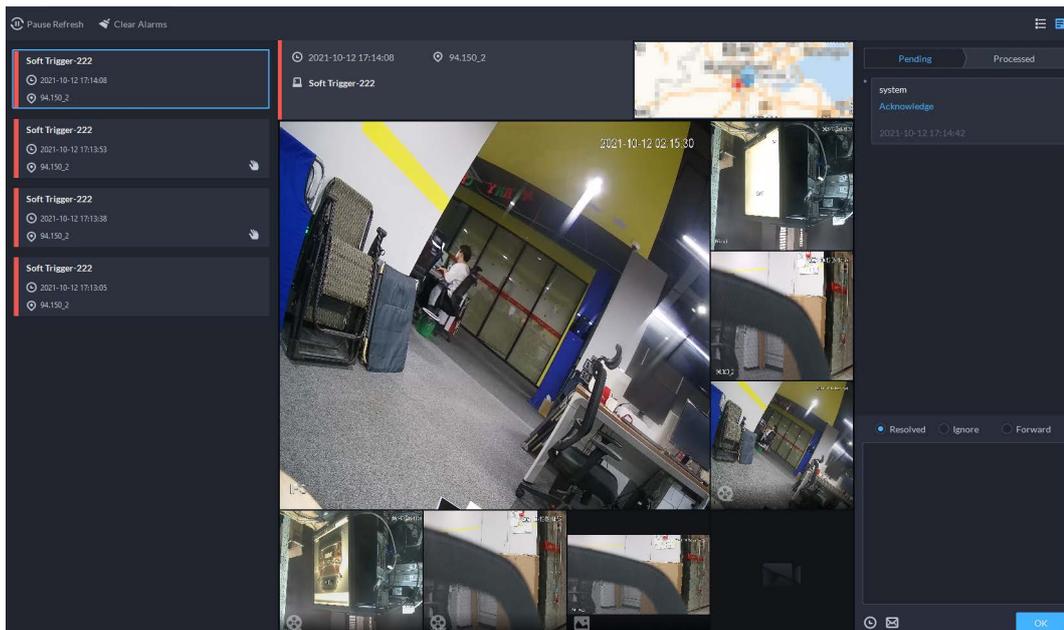
2. The middle area displays the time when the alarm was triggered, name and location of the alarm source, alarm type, and the live video images of linked channels, alarm videos, and alarm snapshots.

Double-click a window to view them in larger size. Click ![icon] to go back.

Figure 6-59 Alarm linkage media
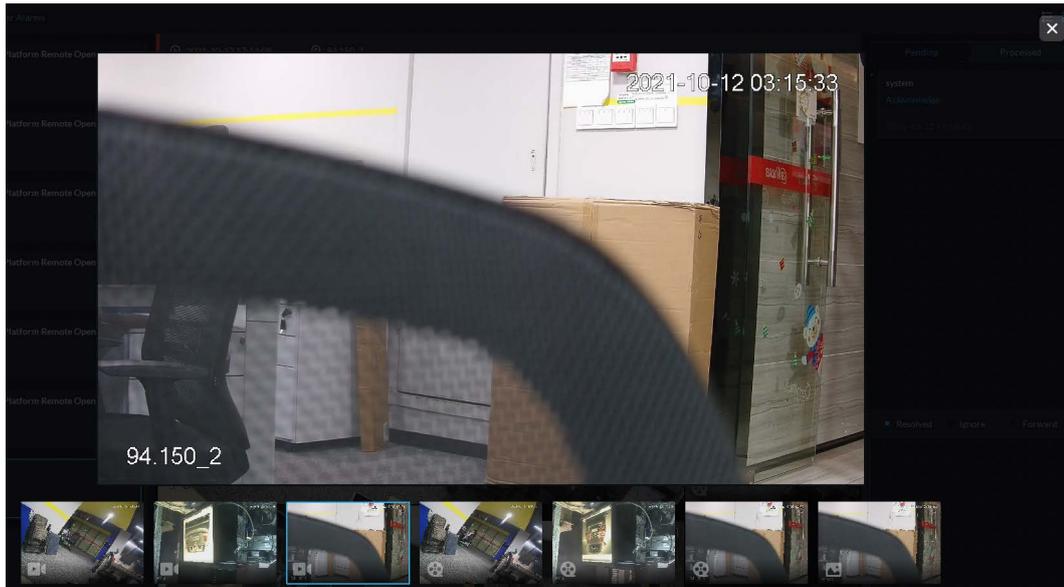
3. On the right side, select how to process the alarm from **Resolved**, **Ignore**, or **Forward**. Enter comments, and then click **OK**.

   Forward allows you to forward the alarm to another user who will process it.

4. (Optional) Click [icon] to disarm the alarm. This alarm will not be triggered within the defined period.

5. (Optional) Click [icon] to send the alarm information to other users as a prompt or an email.

Figure 6-60 Send email
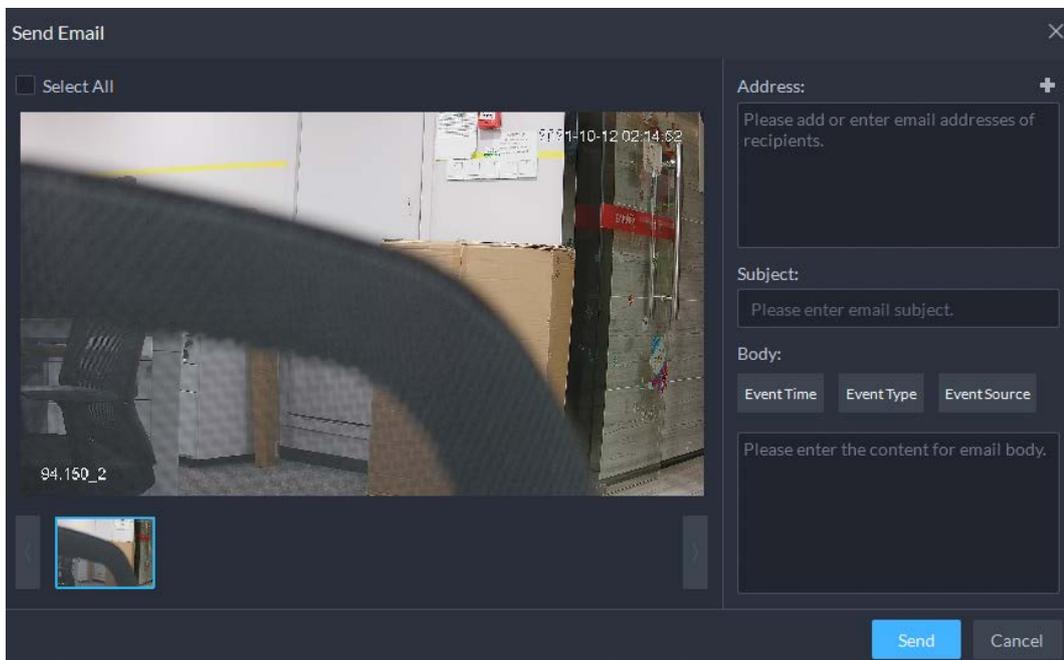
6.2.2 History Alarms

Search for and process history alarms.

Step 1   Log in to the DSS Client. On the **Home** page, click [icon], and then select **Event Center**.

Step 2　　Click .

Step 3　　Set search conditions, and then click **Search**.

Figure 6-61 history alarms

Step 4　　Claim and process alarms, see "6.2.1 Real-time Alarms".

You can use the up and down arrow keys on the keyboard to quickly select other alarms.

6.3 DeepXplore

You can set multiple search conditions to view records of people, vehicle snapshots and access that you are interested in.

6.3.1 Searching for Records

In this section, you can view integrated records of people, vehicle.

Step 1　　Log in to the DSS Client. On the **Home** page, click , and then select **DeepXplore**.

Step 2　　click , and then select **Record**.

Figure 6-62 Record search
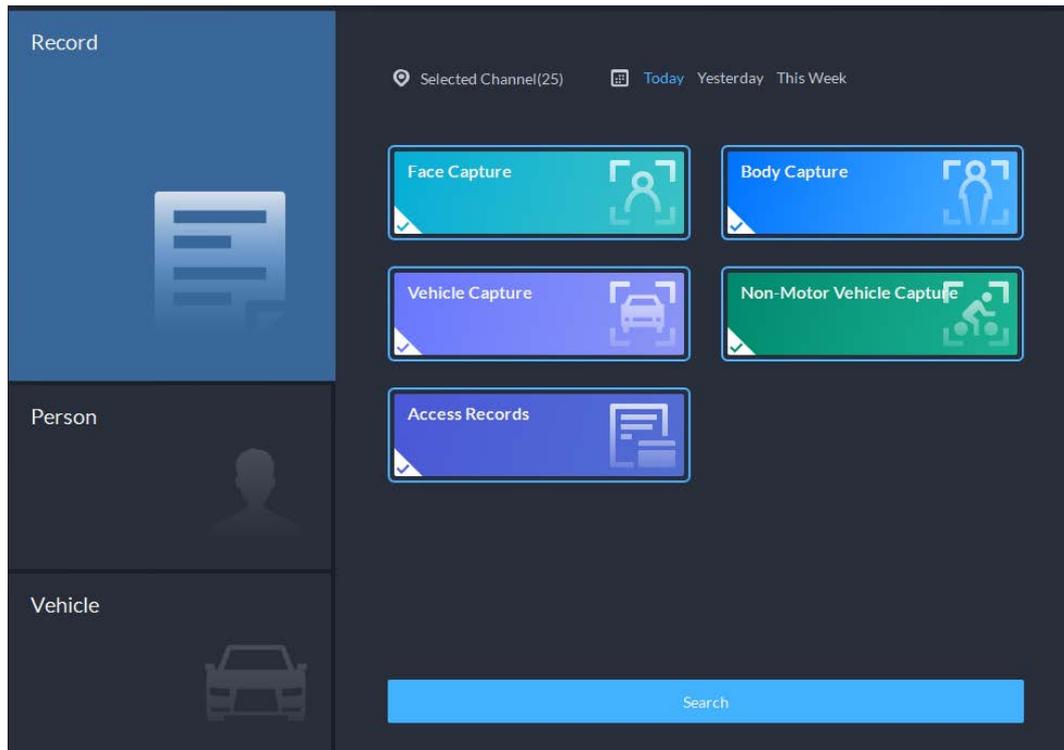
Step 3 Set the search object, channel and time, and then click **Search**.

Figure 6-63 Search result
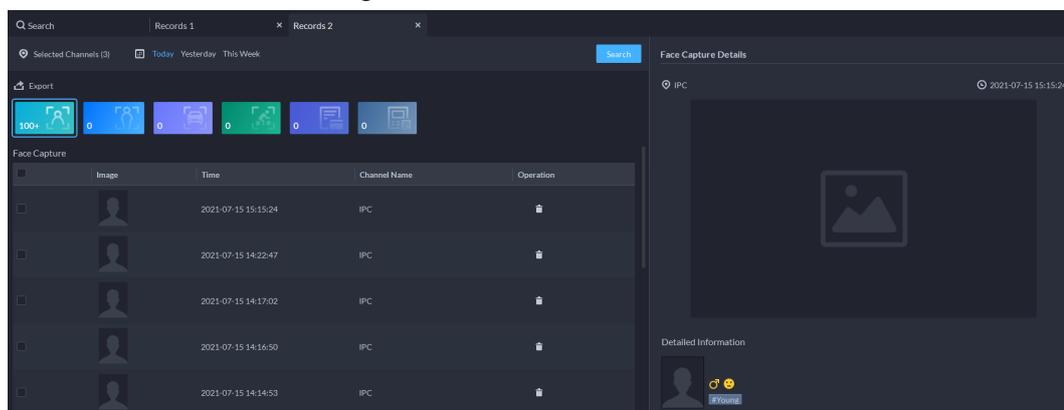
For the search result, you can perform following operations.

- 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 4 Select a record, and on the right side, you can see the details. Click on the video image to view the linked recording.

6.3.2 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** page, click ⊞, and then select **DeepXplore**.

Step 2   click , and then select **Person**.

Figure 6-64 Person search
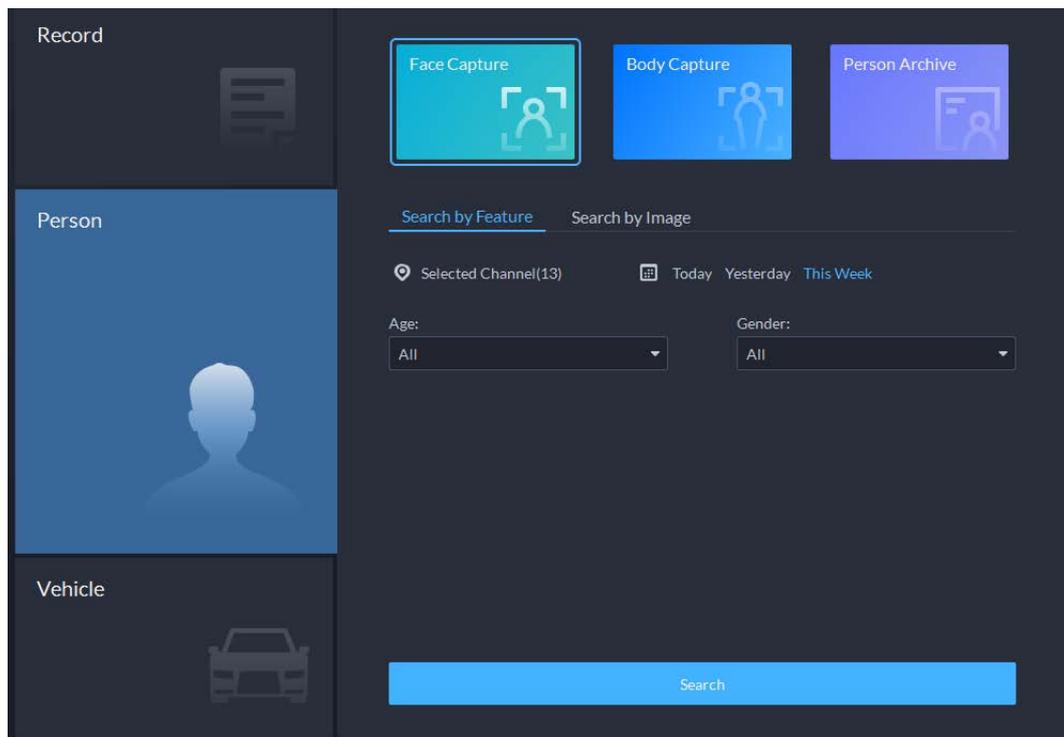
- Search object
  ◇ **Face Capture**: Search for records in face capture database.
  ◇ **Body Capture**: Search for records in body capture database.
  ◇ **Person Archive**: Search for records in person information database.
- Search type
  ◇ **Search by Feature**: Search for records by the defined features 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 records.
- 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 6-65 Search result

For the search result, you can perform following operations.

- Click ⌄ next to **Search** to change search conditions.
- Click Time 1↓ | ⊞ ☰ to change records arrangement.
- 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.

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 6-66 Person information
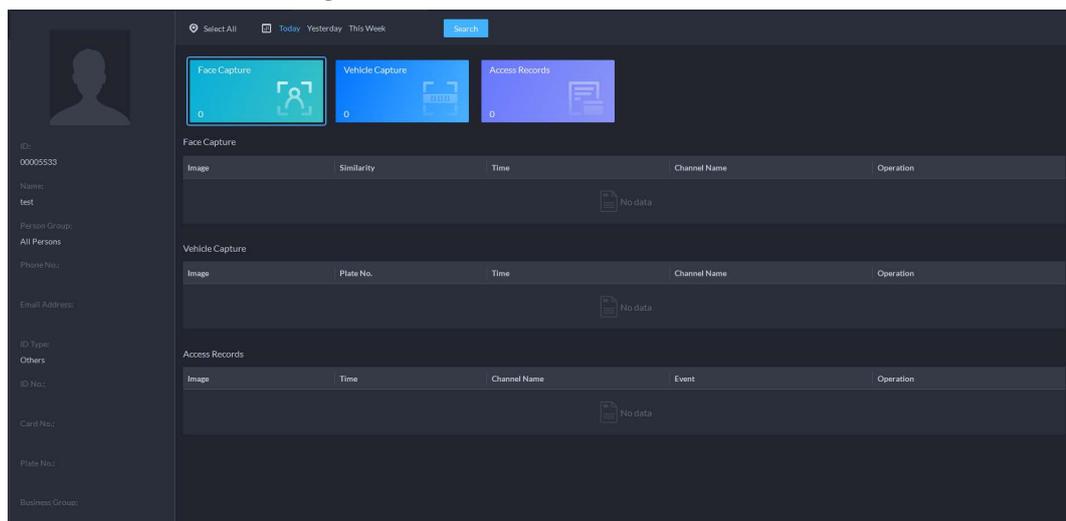
6.3.3 Searching for Vehicles

Step 1   Log in to the DSS Client. On the **Home** page, click ⊞, and then select **DeepXplore**.

Step 2   click 🔍, and then select **Vehicle**.

Figure 6-67 Vehicle search
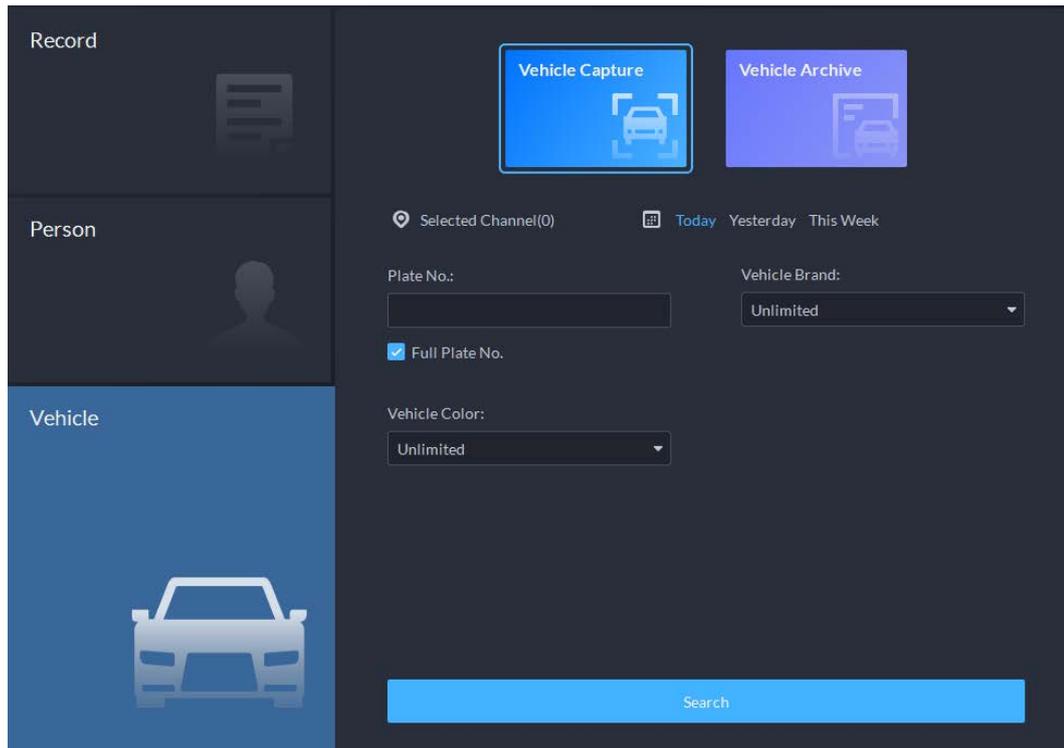
- Search object
  - ◇ **Vehicle Capture**: Search for records in vehicle capture database.
  - ◇ **Vehicle Archive**: Search for records in vehicle information database.
- Search type
  - ◇ Search channel: Select device channels of the records by clicking **Selected Channel**.
  - ◇ Search time: Select time period of the records from **Today**, **Yesterday** and **This Week**.

    📖

    Only available for vehicle capture records.
- 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 3   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 ⬚ to change records arrangement.
- 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 on the video image to view the linked recording.

click 🚗 at the upper-right corner to view all records added to temporary records. Inside it, you can click 🔗 to generate target track, and click 🗑 to remove the record form the bank.

6.4 Access Management

On the **Access Management** page, you can do operations on access control, video intercom, and visitor.

6.4.1 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 "5.5 Access Control". You can also click 🔧 Access Control Configur... to go to the access control configuration page.

6.4.1.1 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 "4.2.3 Binding Resources".
Log in to the DSS Client. On the **Home** page, select ⊞ > **Access Management** > ◫ > **Access Control Console**, and then view the linked real-time videos by the following two methods.
● On the right side of the console page, click 📷 in the access control channel list.

Figure 6-68 Viewing video (1)
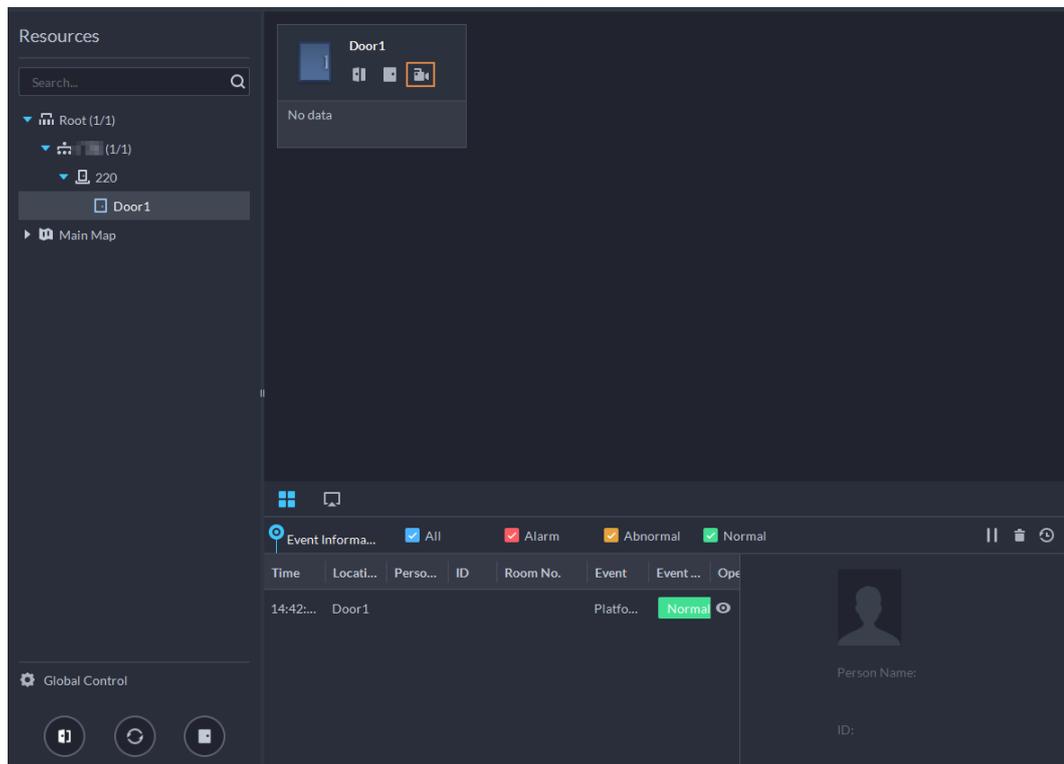
● Click 🖥 on the console page. The video page is displayed. Drag the access control channel on the left side of the screen to the live view page on the right side. The system displays videos in

real time.

Figure 6-69 Viewing video (2)
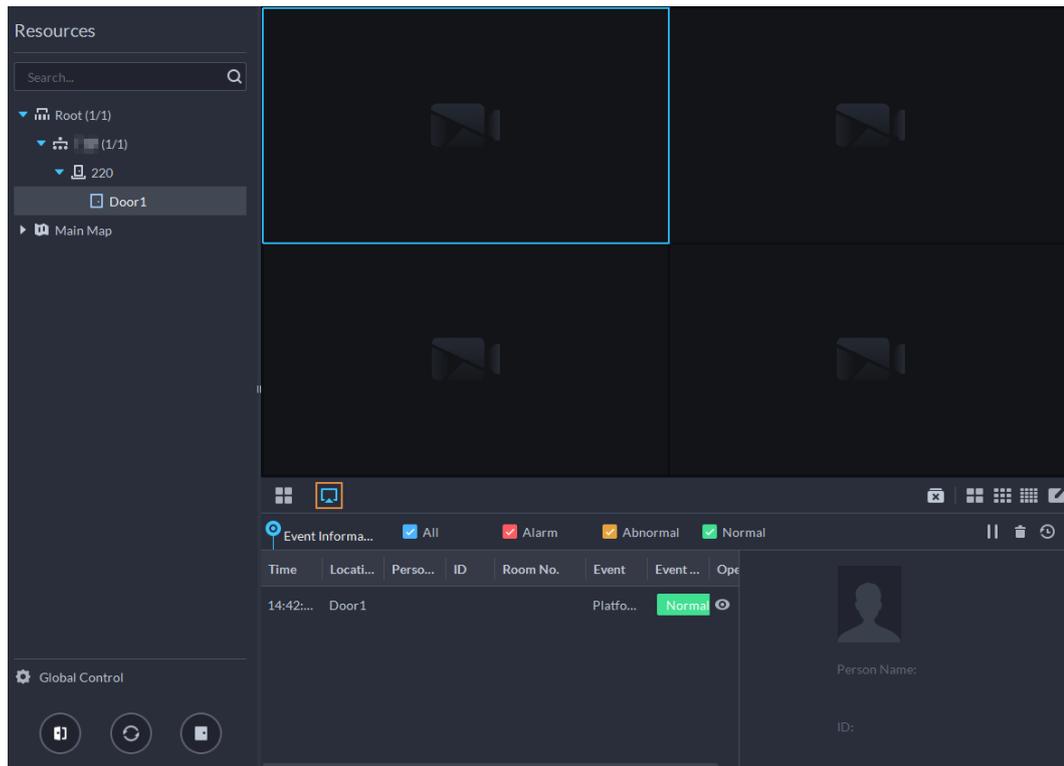
6.4.1.2 Unlocking Door

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 page, 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 page changes to open, as .
- Click of a door channel on the right to unlock the door.
- When viewing videos bound to the channel, click on the video page to unlock the door.

Figure 6-70 Unlock door
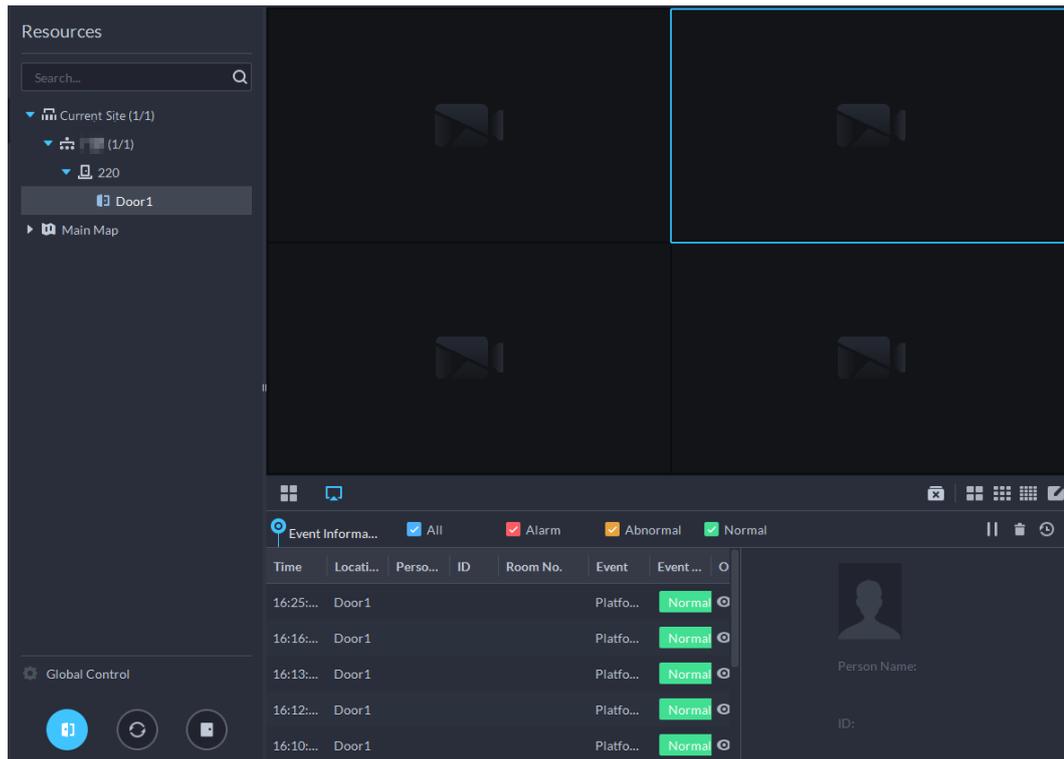
- Temporary Always Open of multiple doors
  Select door channels through global control, and then you can set the door to be Always Open.

Step 1   Click ⚙ on the lower left of the console page 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 page.

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.

6.4.1.3 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 page, 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 page changes to closed, as ▮.
- Click ▫ of a door channel on the right to unlock the door.
- When viewing videos bound to the channel, click ▣ on the video page to lock the door.
- 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 page 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 page, and then click **OK**.

📖

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.

6.4.1.4 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 "4.2.3 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 "5.1 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 page, 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 6-71 Event information
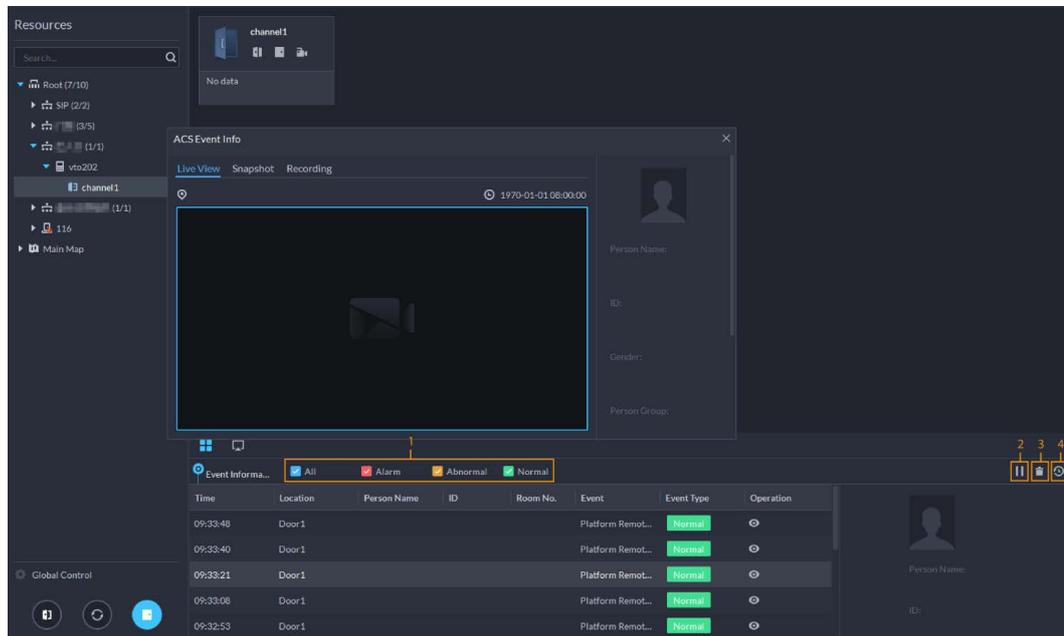
Table 6-10 More operations

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.
2	● Click ⏸ to stop displaying reported event information. In this case, the page no longer displays the reported new events. After clicking, the button changes to ▶. ● Click ▶ to start refreshing reported event information. The page 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.

6.4.1.5 Viewing Access Control Records

You can view access control records on the platform or directly on a device. For records on a device, see "9.1 Managing Logs".

6.4.1.5.1 Online Records

The access control records stored on the platform.

Step 1   Log in to the DSS Client. On the **Home** page, click ⊞ > **Access Management** > ◁〕 > **Access Control Record**.

Step 2 Set search conditions, and then click **Search**.

Figure 6-72 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 page, and then export records as the screen instructs.

6.4.1.5.2 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** page, click ![icon] > **Access Management** > ![icon] > **Access Control Record**.

Step 2 Click ![Acquire Records button] at the upper-left corner.

Figure 6-73 Extract records during disconnection
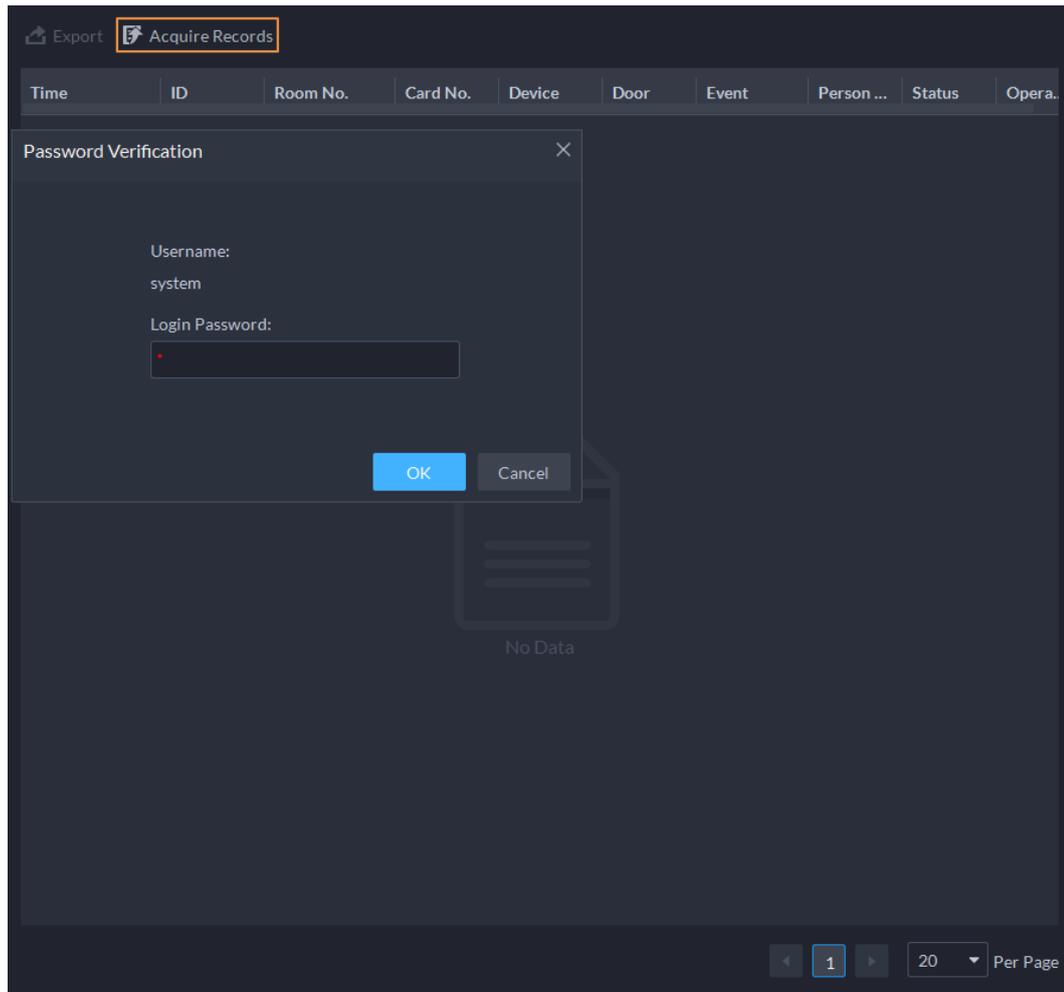
Step 3   Enter the login password for verification.

Step 4   Click [icon] to set period, select **Card-swiping Records** or **Alarm Log**, and then select device.

[book icon]

You can select up to one week.

Step 5   Click **OK**.

6.4.2 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 "5.6 Video Intercom". You can also click [Video Intercom Configur...] to go to the video intercom configuration page.

6.4.2.1 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** page, click [icon] > **Access Management** > [icon] >

Call Center.

Figure 6-74 Call center
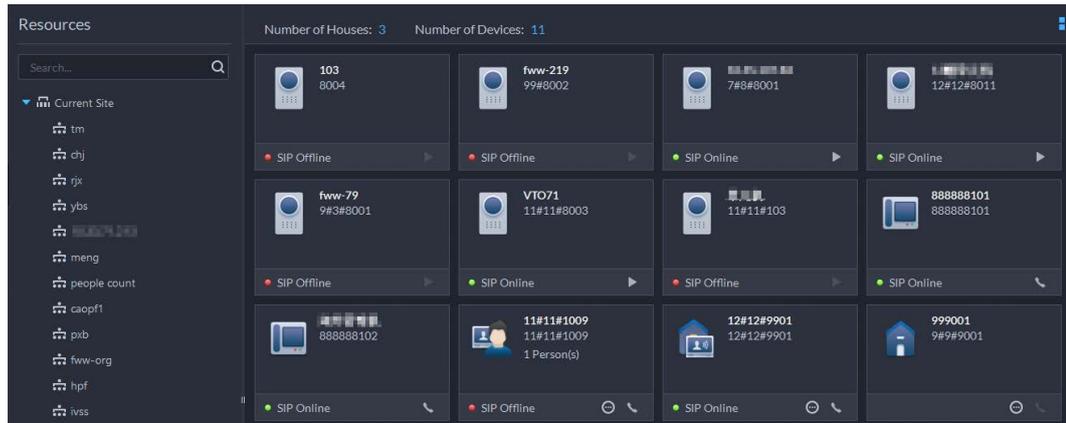
Step 2 You can call different devices.

● Call from the platform to VTO

Select VTO in the device list; click ▷ corresponding of VTO and call VTO. The system pops out call page. 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 "9.3.5 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 "9.3.5 Configure File Storage Settings".

◇ ☎: Click this icon to hang up.

Figure 6-75 Call
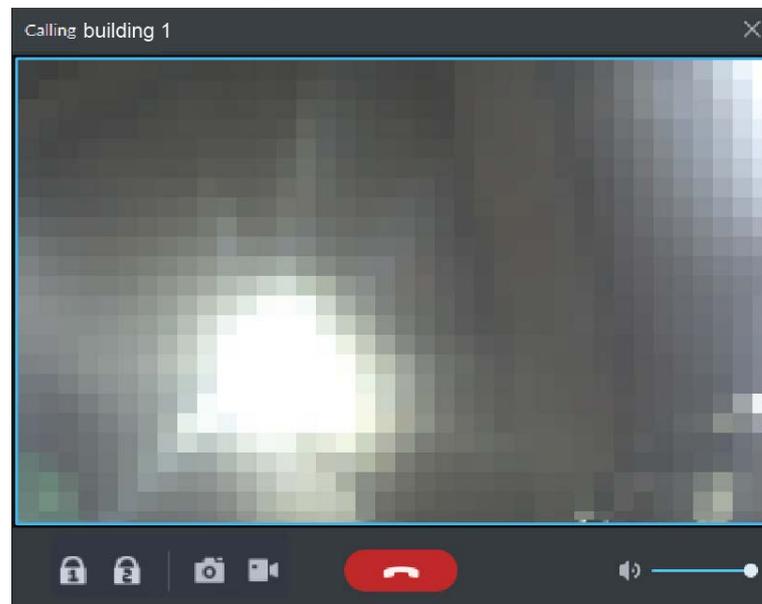
● Call from the platform to VTH

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 6-76 Calling
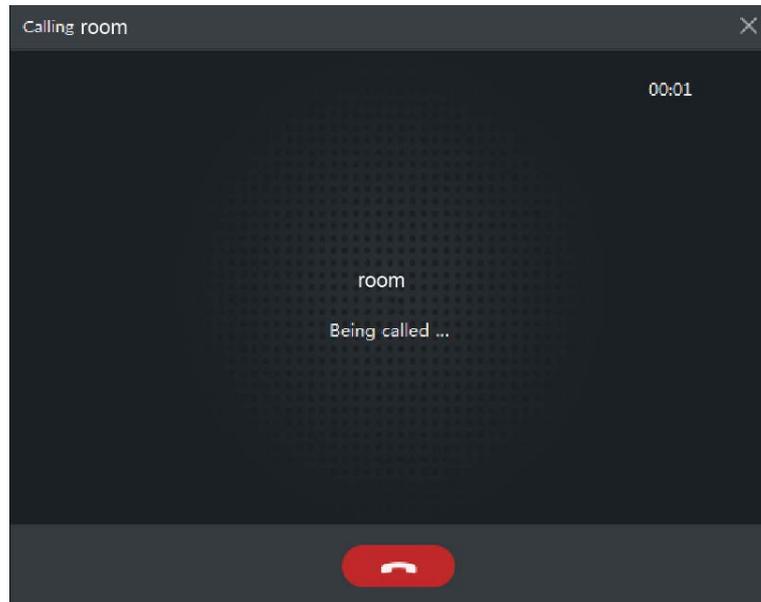
● Call from the platform to an access control device that supports video intercom

Select a device from the device list, click [icon] on 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 device, bidirectional talk between client and the device. Press [icon] 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 6-77 Calling
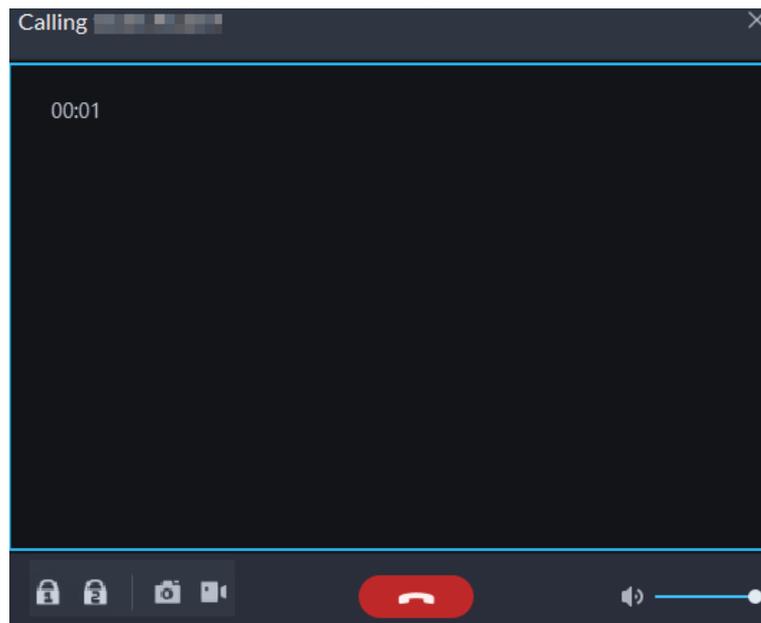
● Call from VTO to the platform

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 6-78 VTO Call
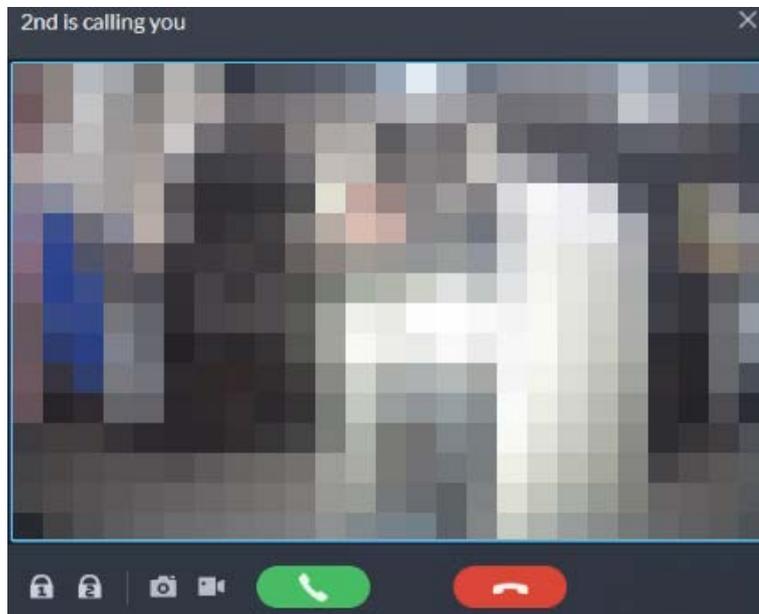
- When VTH is calling the platform

  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.

- When an access control device that supports video intercom is calling the platform

  The client pops out the dialog box. Click 📞 to talk with the device.

  Click ☎ to hang up.

Figure 6-79 Call from an access control device that supports video intercom
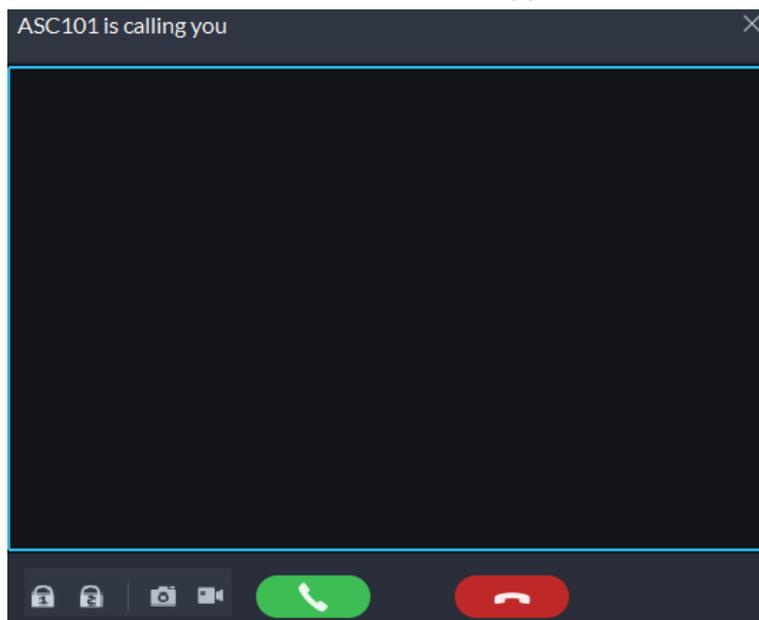
- Call through call records

  All the call records are displayed in the **Call Record** at the lower-right corner of the

page of **Video Intercom**. Click the record to call back.

Figure 6-80 Call records

6.4.2.2 Releasing Messages

Send message to VTHs.

Step 1 Log in to the DSS Client. On the **Home** page, click [icon] > **Access Management** > **Video Intercom** > **Information Release**.

Step 2 Click **Add New Message**, select one or more VTHs, and then configure the information you want to send.

Step 3 (Optional) Enable **Schedule Release**, and then configure the time.

Step 4 Send the message.

● If no scheduled release time is configured, click **Instant Release**, or click **Save**, and then click [icon] to send the message immediately.

● If a scheduled release time is configured, click **Save**, and then the message will be sent on the defined time.

6.4.2.3 Video Intercom Records

View log records and you can trace recorded calls.

Step 1 Log in to the DSS Client. On the **Home** page, click [icon] > **Access Management** > [icon] > **Video Intercom Record**.

Step 2 Set conditions, and then click **Search**.

Figure 6-81 Video intercom records

Step 3   Click **Export** and the records will be saved locally according to system prompt.

6.4.3 Visitor Application

After visitor information is registered, the visitor can have access permission. Access permission is disabled after the visitor leaves.

6.4.3.1 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 "4 Basic Configurations".
- Make sure that you have configured the visitor configuration before application. For details, see "5.7 Visitor Management". You can also click Visitor Configuration to go to the video intercom configuration page.

6.4.3.2 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.

Procedure

Step 1   Log in to the DSS Client. On the **Home** page, click > **Access Management** > > **Visitor Management**.

Step 2   Click **Visit Registration**, and then enter the information of the visitor.

Figure 6-82 Visitor information

Step 3   (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 6-83 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 6-84 Reader manager
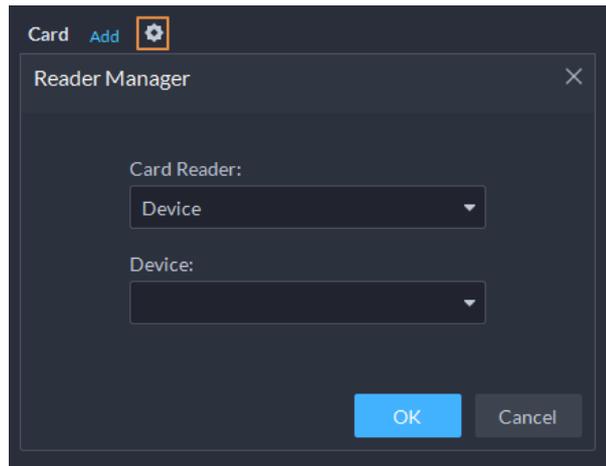
3) Set face picture. Position your face in the snapshot area, and click **Upload Picture** to select a picture or click **Snapshot** to take a photo.

Figure 6-85 Take a face photo
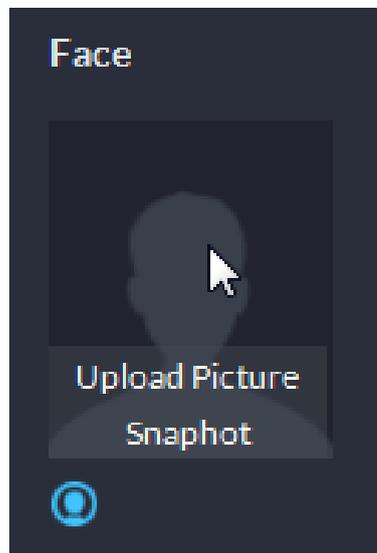
4) Click **Generate** to generate a QR code for the pass.
You can click ⬇ to download the QR code, and click ◁ to send it to the visitor by email.

Figure 6-86 Authentication
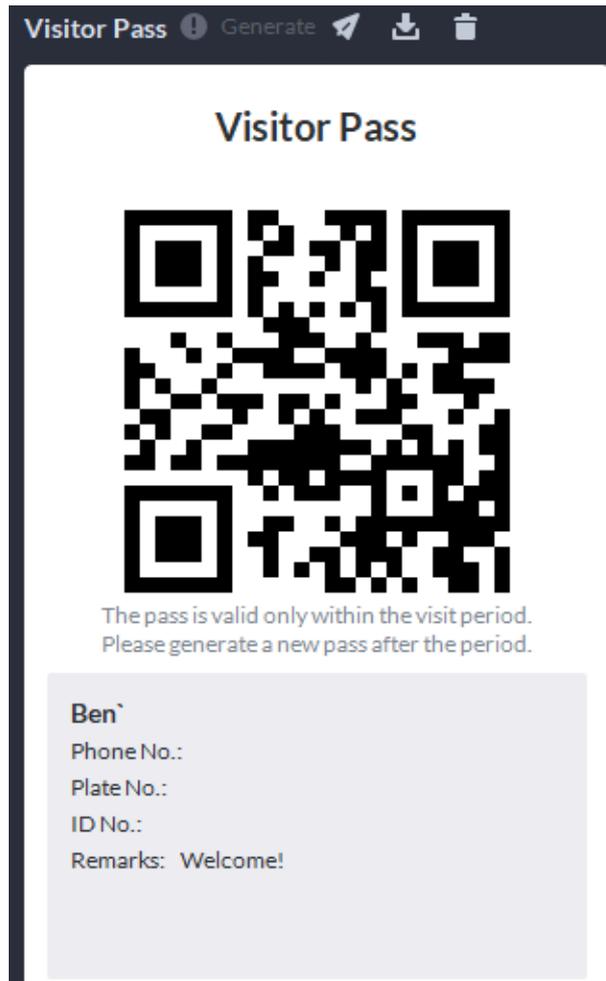
Step 4　Click the **Authorize** tab, and then select access permissions for the visitor.

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 6-87 Authorize
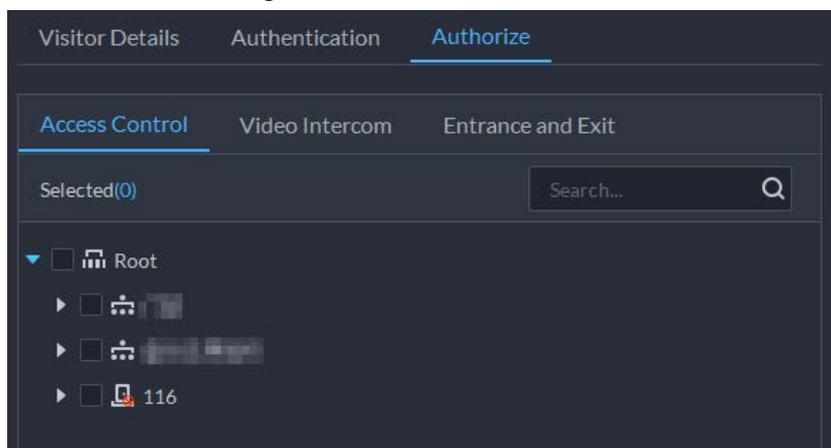
Step 5　Click **OK**.

Related Operations

● End visit.

Click ![icon] to end a visit.

● View card swiping records.

Click the **Card-swiping Record** tab, or click ![icon] in visitor record to view visitor card swiping records.

6.4.3.3 Checking Out

When visitors are leaving, remove their access permissions.

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon] > **Access Management** > ![icon] > **Visitor Management**.

Step 2   Find the appointment record of the visitor, and then click ![icon].

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.

6.4.3.4 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** page, click ![icon] > **Access Management** > ![icon] > **Visitor Record**.

Step 2   Set search conditions, and then click **Search**.

The results are displayed.

![icon]

In addition to entering the card number, you can also click ![icon], select a card reader and then get the card number by swiping card.

Step 3   Click ![icon] to view visitor details and card swiping records.

6.5 Parking Lot

You can monitor vehicles that enter and exit in real time, view vehicle information, and search for on-site vehicle, exit vehicle and snapshot records.

6.5.1 Entrance and Exit Monitoring

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon] > **Parking Lot** > **Entrance and Exit Monitoring**.

Step 2   Select the number of windows you want from ![icons].

Step 3   Click **Please click to select the entrance and exit.**, select an entrance or exit point, and then click **OK**.

The real-time video of that point will be opened in the window.

Figure 6-88 Monitor entrances and exits
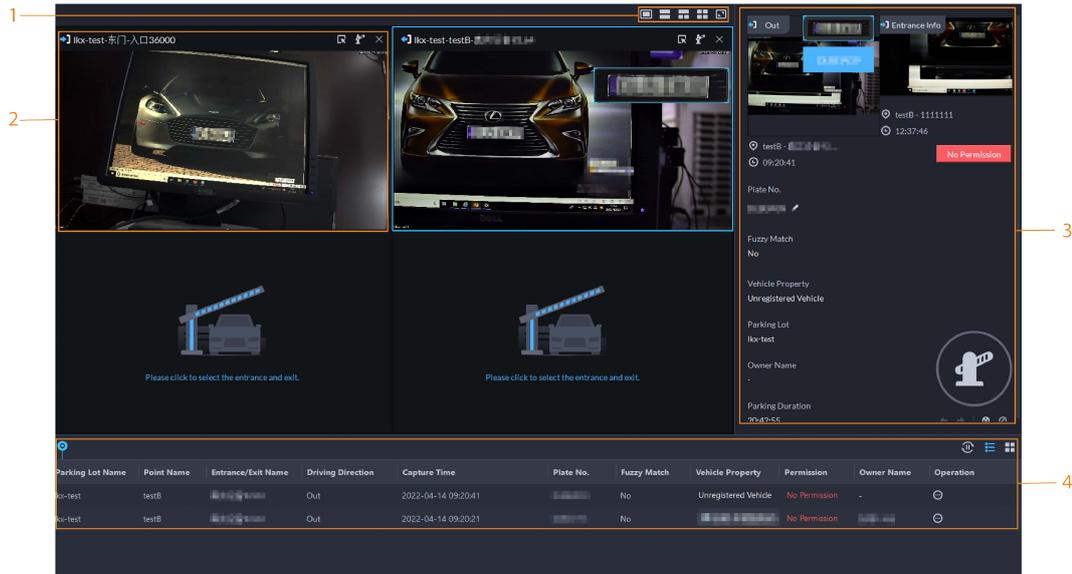
Table 6-11 Page description

No.	Description
1	Select the number of windows you want. Each window can display the real-time video of one entrance or exit point.
2	The real-time video of an entrance or exit point. ● Click ⬛ to open the real-time video of another entrance or exit point in the window. ● Click 🔧 to open the barrier for vehicles. 　◇ **Open without Recording Plate Info**: Open the barrier for vehicles without recording their plate numbers. If you select **Count Parking Spaces** at the same time, the number available parking spaces in the parking lot will decrease or increase depending on whether the vehicles are entering or leaving. 　◇ **Open and Record Plate Info**: This is applicable to when the ANPR cameras cannot recognize the number plates. You can manually enter the number plate, and a snapshot will be taken, and then the platform will generate an entrance or exit record.
3	Real-time entrance or exit information. ● Click 🔧 to open the barrier for the vehicle. ● If the plate number is incorrect, you can click ✏️ to manually edit it. ● Click ⊞ to view the recorded video from the corresponding channel.
4	All entrance and exit records. ● ▶/⏸: Pause or resume refreshing the entrance and exit records. ● ⊙: View the details and recorded video of a record.

6.5.2 Searching for Records

Search for entry and exit records, forced exit records, and snapshot records.

Log in to the DSS Client. On the **Home** page, click [icon], and then select **Vehicle Entrance and Exit**.

Click [⚙ Entrance and Exit Config...] to go to the entrance and exit configuration page.

6.5.2.1 Searching for Entrance Records

Step 1   Log in to the DSS Client. On the **Home** page, click [icon] > **Parking Lot** > **Info Search**.

Step 2   Click the **Entrance Records** tab.

Step 3   Configure the search conditions, and then click **Search**.

      [📖]

      Click **Show More** and you can search by vehicle owner, company, person group, and more.

Step 4   Manage the records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click [icon], and the detailed information is displayed on the right. Click the play icon to play the recorded video, and then click [icon] to download it.
  Click [icon] to modify the information of the vehicle, such as the plate number, brand and color.
  For the dual camera mode, click each channel to view the information it captured.
- Forced exit.
  If **No** is displayed under **Already Exited** when the vehicle has exited, click [icon] to change the status to **Yes**.
- Export records.
  Select the records to be exported, click **Export**, and then export them according to the on-screen instructions. You can also click **Export**, and the then export all records according to the on-screen instructions.
- Click [icon] and then select the items to be displayed.

6.5.2.2 Searching for Exit Records

Step 1   Log in to the DSS Client. On the **Home** page, click [icon] > **Parking Lot** > **Info Search**.

Step 2   Click the **Exit Records** tab.

Step 3   Configure the search conditions, and then click **Search**.

      [📖]

      Click **Show More** and you can search by vehicle owner, company, person group, and more.

Step 4   Manage the records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click [icon], and the detailed information is displayed on the right. Click the play icon to play the recorded video, and then click [icon] to download it.
  Click [icon] to modify the information of the vehicle, such as the plate number, brand and color.
  For the dual camera mode, click each channel to view the information it captured.

- Export records.

  Select the records to be exported, click **Export**, and then export them according to the on-screen instructions. You can also click **Export**, and the then export all records according to the on-screen instructions.
- Click ![icon] and then select the items to be displayed.

6.5.2.3 Searching for Forced Exit Records

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon] > **Parking Lot** > **Info Search**.

Step 2   Click the **Forced Exit Records** tab.

Step 3   Configure the search conditions, and then click **Search**.

📖

Click **Show More** and you can search by vehicle owner, company, person group, and more.

Step 4   Manage the records.

- Click the image, and then a bigger one will be displayed.
- Double-click a record or click ![icon], and the detailed information is displayed on the right. Click the play icon to play the recorded video, and then click ![icon] to download it. Click ![icon] to modify the information of the vehicle, such as the plate number, brand and color.

  For the dual camera mode, click each channel to view the information it captured.
- Export records.

  Select the records to be exported, click **Export**, and then export them according to the on-screen instructions. You can also click **Export**, and the then export all records according to the on-screen instructions.
- Click ![icon] and then select the items to be displayed.

6.5.2.4 Searching for Capture Records

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon] > **Parking Lot** > **Info Search**.

Step 2   Click the **Capture Records** tab.

Step 3   Configure the 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 image, and then a bigger one will be displayed.
- Double-click a record or click ![icon], and the detailed information is displayed on the right. Click the play icon to play the recorded video, and then click ![icon] to download it. Click ![icon] to modify the information of the vehicle, such as the plate number, brand and color.

  For the dual camera mode, click each channel to view the information it captured.
- Restore entry

  If **Yes** is displayed under **Exited** when the vehicle is still in the parking lot, click ![icon] to

change the status to **No**.
- Export records.
  Select the records to be exported, click **Export**, and then export them according to the on-screen instructions. You can also click **Export**, and the then export all records according to the on-screen instructions.
- Click ▼ and then select the items to be displayed.

6.6 Intelligent Analysis

View real-time and history people counting data, heat maps, and number of people in an area.

6.6.1 People Counting

6.6.1.1 Real-time Count

Step 1   Log in to the DSS Client. On the **Home** page, 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 6-89 Real-time count
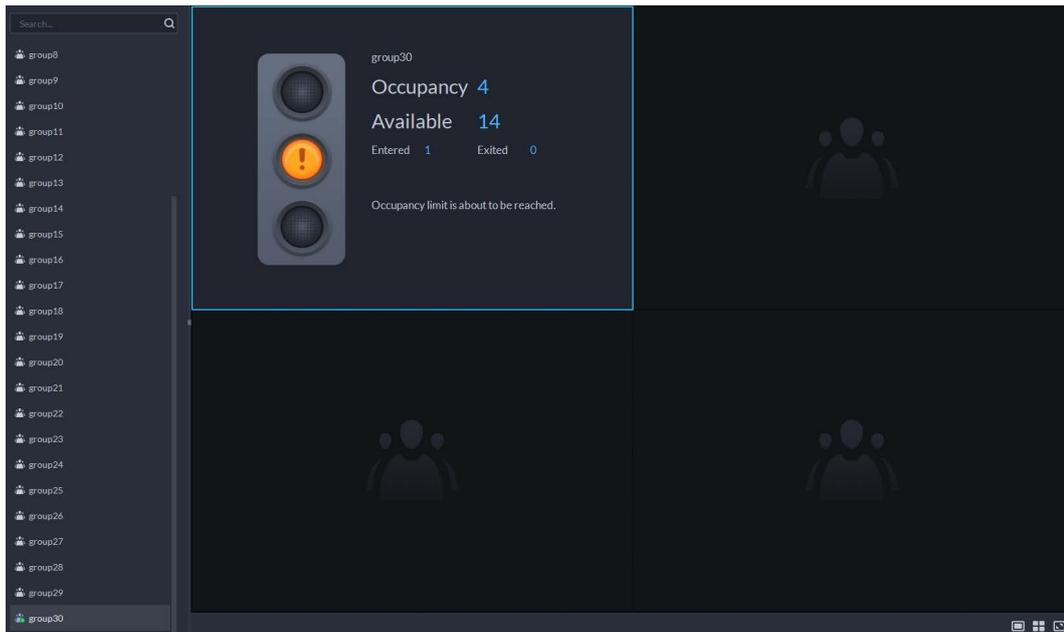
Step 3   Hover you mouse on the window displaying real-time data, and then click 🖉.

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 6-90 Edit the content and data
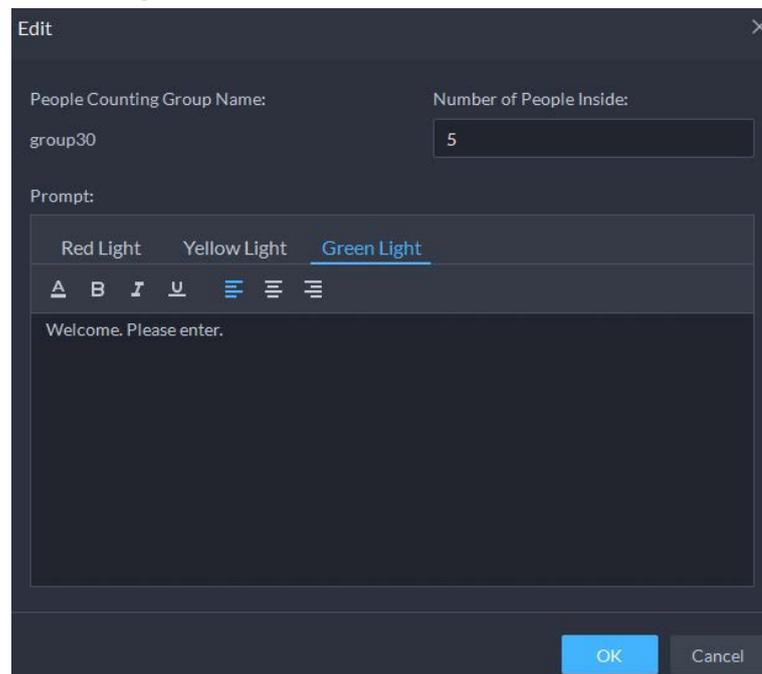
Step 5   Click **OK**.

6.6.1.2 Historical Count

Procedure

Step 1   Log in to the DSS Client. On the **Home** page, 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 6-91 Historical people counting data
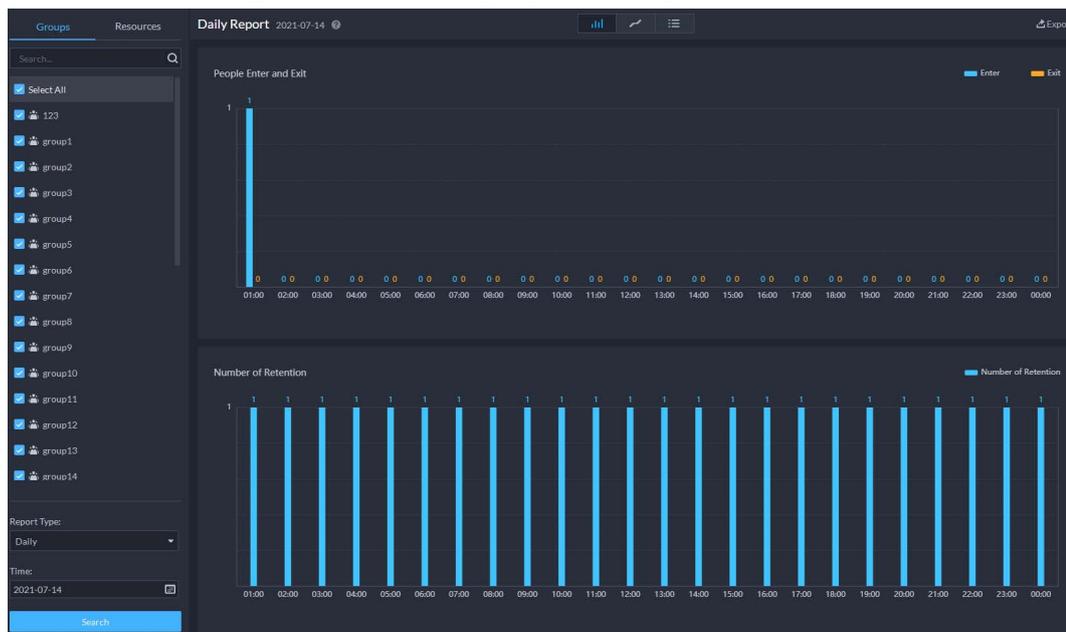
Related Operations

- ![icons]: 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 computer.

6.6.2 Heat Maps

View heat maps generated by devices. A heat map shows the distribution of people flow by different colors, such as red for many people have visited an area and blue for only a few people have visited an area. The platform supports generating general heat maps and advanced heat maps. Only fisheye cameras support advanced heat maps.

Configure the channel feature for either type of heat maps. For details, see "4.2.2.5.1 Modifying Device Information".

- General heat map: Select the **General Heat Map** from the channel features.
- Advanced heat map: Select the **Advanced Heat Map** from the channel features.

Step 1 Log in to the DSS Client. On the **Home** page, click ![icon] > **Intelligent Analysis** > ![icon].

Step 2 Select a channel, and then generate a heat map.

📖

You can generate a heat map with data from up to one week.

- Generate a general heat map.

  Configure the time, and then click **Search**.

- Generate an advanced heat map.

1) Select how you want to generate the heat map, **Number of People** or **Time**.

2) Configure the threshold.

   📖

   - When you select **Number of People**, the area with the closest number of people to the threshold will be in red.

   - When you select **Time**, the area where people stay for a duration closest to the threshold will be in red.

3) Set the time, and then click **Search**.

Step 3   Click **Export** on the upper-right corner to export the heat map to your PC.

6.6.3 In-area People Counting

View the in-area people number statistics of one or more channels.

Procedure

Step 1   Log in to the DSS Client. On the **Home** page, click ⊞ > **Intelligent Analysis** > 🗠.

Step 2   Select a channel and configure the search settings, and then click **Search**.

Figure 6-92 In-area people number statistics
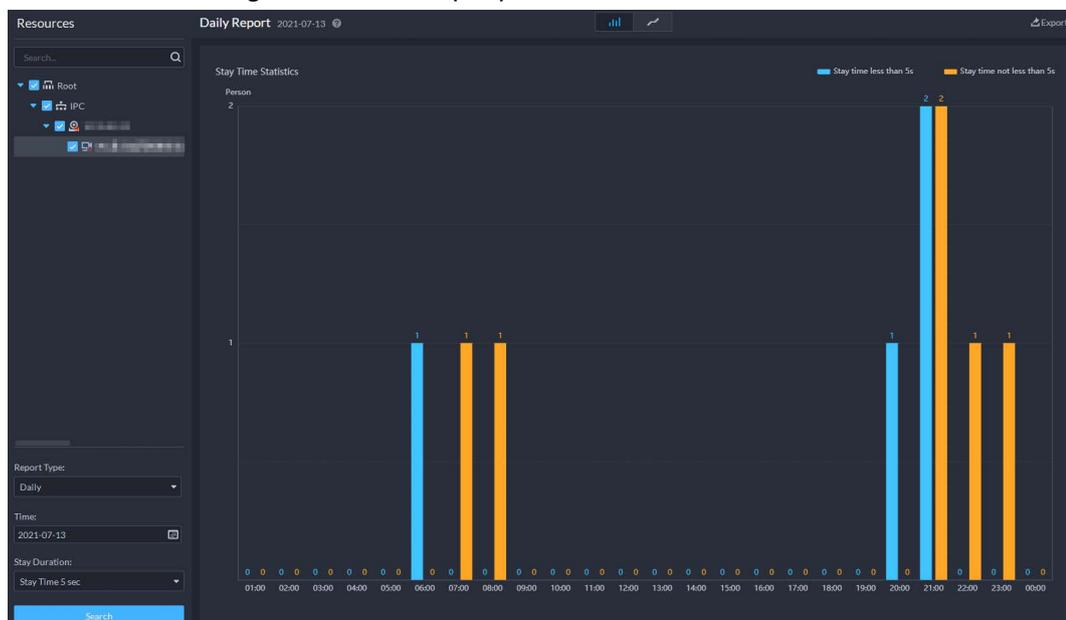
Related Operations

- 📊 📈 : Change the display format of the data.

- **Export**: Export the data to your PC.

7 General Application

This chapter introduces the general businesses, including target detection, face recognition, and ANPR.

7.1 Target Detection

View and search for the metadata of people, vehicle, and non-motor vehicle.

📖

Target detection can be done by video metadata cameras + a platform, or IPCs + IVSSs + platform.

7.1.1 Typical Topology

Figure 7-1 Typical topology
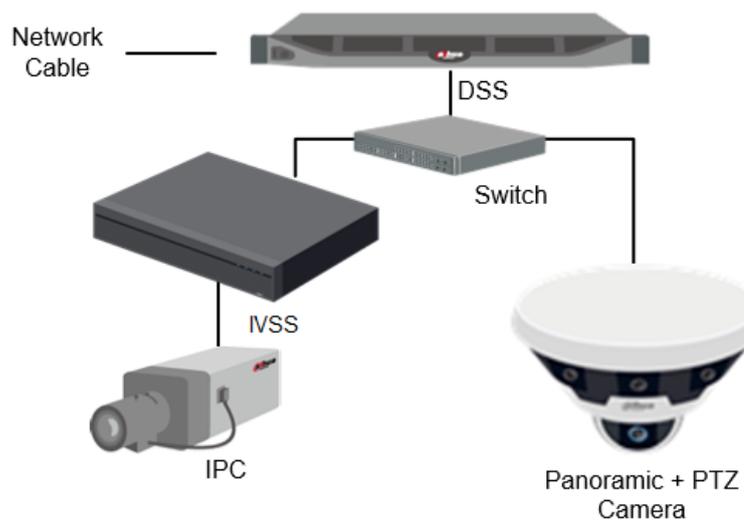
- General cameras record videos.
- Video metadata cameras such as panoramic + PTZ camera record videos and analyze people, and motor and non-motor vehicles.
- IVSS manages cameras and analyzes people, and motor and non-motor vehicles.
- The platform centrally manages IVSS and cameras, receives analysis results from cameras and displays the reports.

7.1.2 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 the parameters, see "4 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.

7.1.3 Live Target Detection

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

Step 2   Select a window, double-click the channel or drag the channel to the window.

Figure 7-2 Live view
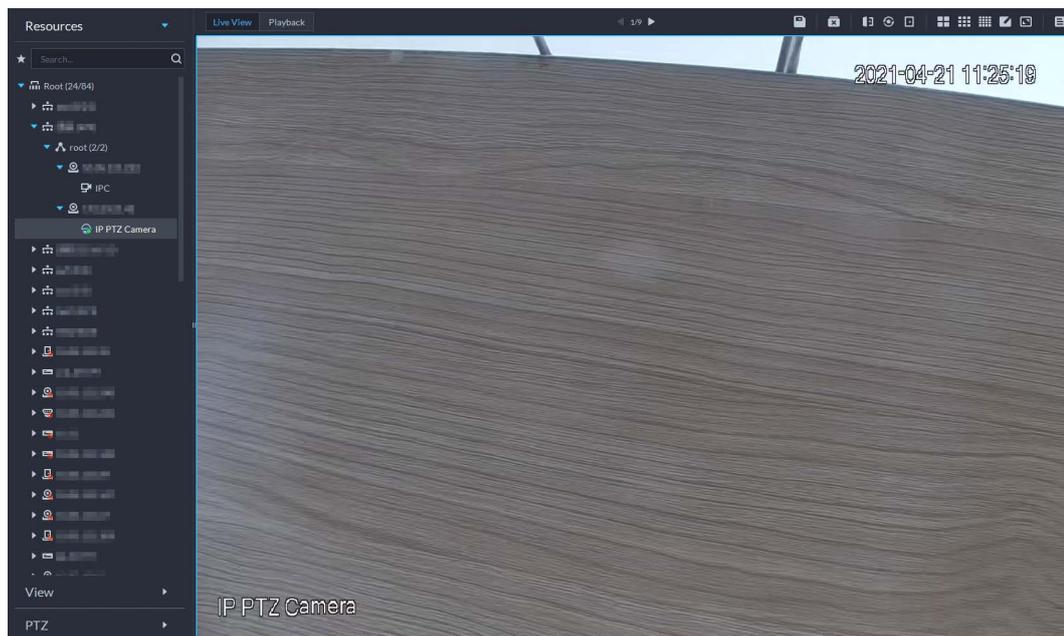
Step 3   Click   and then click   to view live metadata events.

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.

7.1.4 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** page, 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 "6.3 DeepXplore".

7.2 ANPR

View automatic number plate recognition in real time or search for records.
- Automatic number plate recognition

  The platform displays vehicle snapshots and ANPR results in real time.
- Vehicle records

  Search for vehicle records according to the filtering conditions you have set.

7.2.1 Typical Topology

Figure 7-3 Typical topology
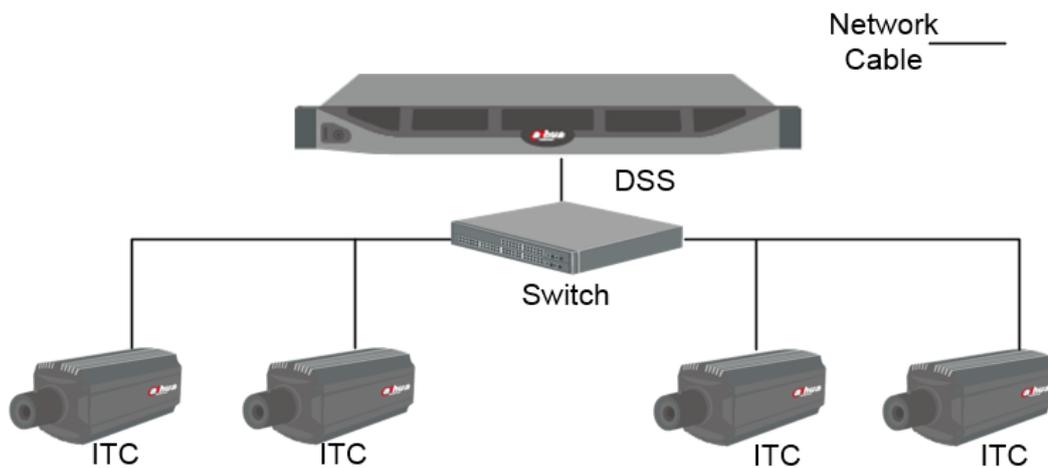
- ANPR cameras (ITC camera) capture and recognize vehicles.
- DSS centrally manages ANPR cameras, receives and displays vehicle snapshots and information uploaded from the cameras.

7.2.2 Preparations

Make sure that the following preparations have been made:
- ANPR cameras are added to the platform, and the ANPR function is configured. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "4 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** page, configure at

least one **ANPR Picture** disk. Otherwise vehicle pictures cannot be viewed.

7.2.3 Live ANPR

View ANPR live video and plate snapshots.

Step 1　Log in to the DSS Client. On the **Home** page, click ⊞, and then select **Monitor Center** > **Monitor**.

Step 2　Select a window, double-click the channel or drag the channel to the window.

Figure 7-4 Live view
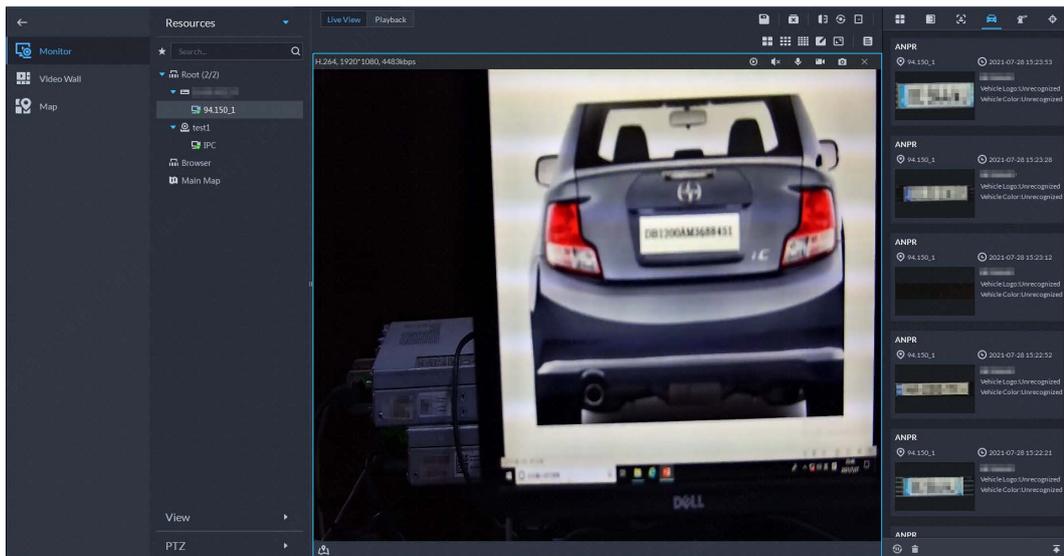
Step 3　Click 🗐 and then click 🚗.

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.

7.2.4 Searching for Vehicle Snapshot Records

Step 1　Log in to the DSS Client. On the **Home** page, click ⊞, and then select **DeepXplore**.

Step 2　Click 🔍.

Step 3　Configure the search conditions.

You can search for vehicle snapshots in the **Record** or **Vehicle** section. For details, see "6.3 DeepXplore".

7.3 Face Recognition

Configure face recognition settings on the device and the platform before you can view face recognition results on the platform.

7.3.1 Typical Topology

The face recognition feature is available on select models of NVR, IVSS and FR cameras.

● Face recognition by NVR/IVSS

Figure 7-5 Typical topology (NVR/IVSS)
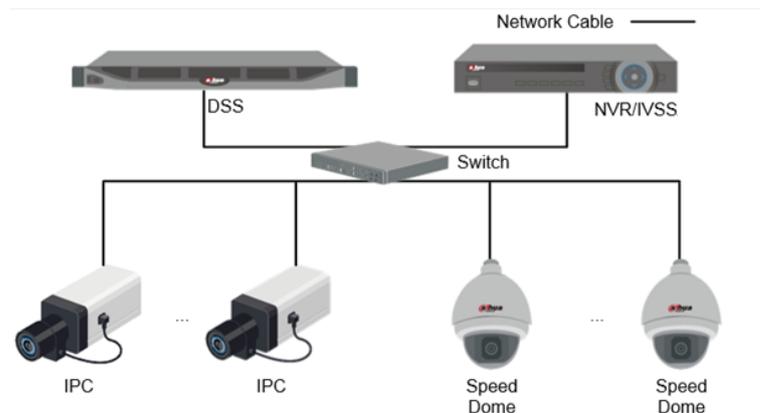
◇ Cameras record videos.
◇ NVR/IVSS is used for face recognition and storage.
◇ DSS centrally manages cameras, NVRs, and the face database, and provides live view and face search.

● Face recognition by camera

Figure 7-6 Typical topology (camera)
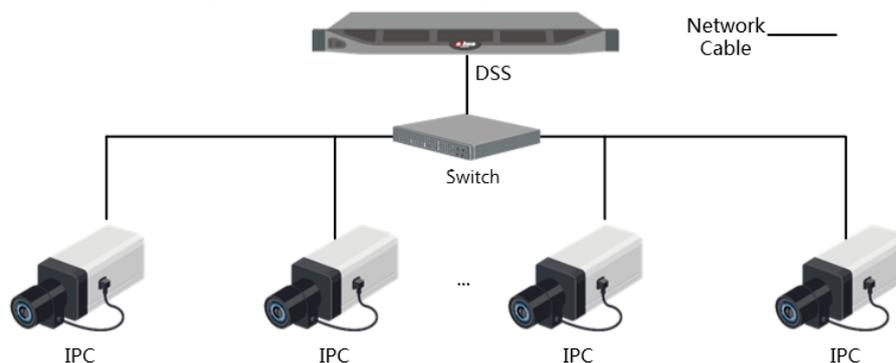
◇ Cameras record face videos, and detect and recognize faces.
◇ DSS centrally manages cameras, NVRs, and the face database, and provides live view and face search.

7.3.2 Preparations

Make sure that the following preparations have been made:

- Face recognition devices are correctly configured. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "4 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.

7.3.3 Arming Faces

Before arming faces, you need to add the persons to face recognition group. For details, see "5.4.1 Face Watch List".

7.3.4 Live Face Recognition

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], and then select **Monitor Center** > **Monitor**.

Step 2   Select a window, double-click the channel or drag the channel to the window.

Figure 7-7 Live view
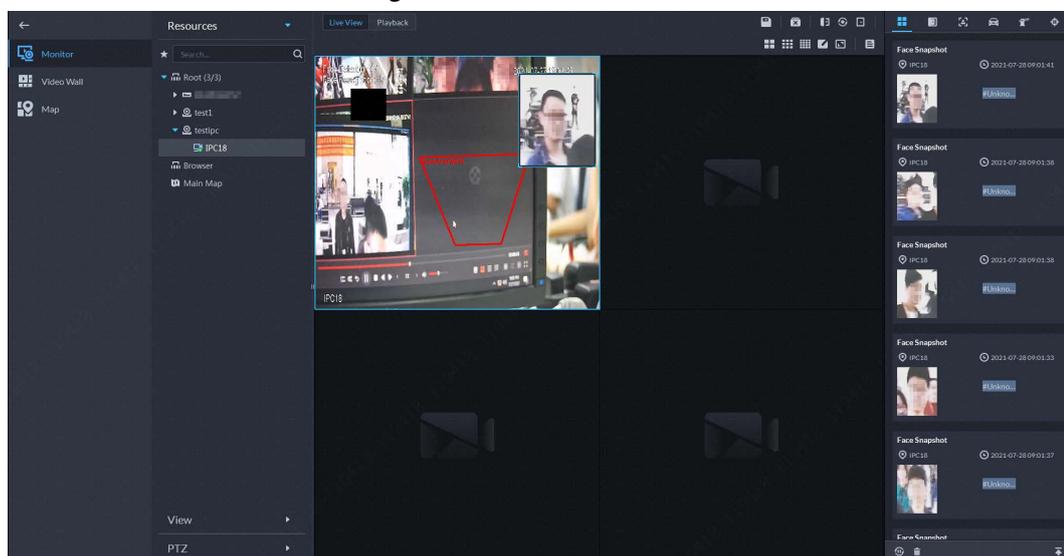
Step 3   Click ![icon] and then click ![icon] to view live face recognition information.

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 ![icon] to download the video to designated path.

- Click ![icon] to play back the video before and after the snapshot.

- Click ![icon] to refresh events; click ![icon] to pause refreshing.

- Click ![icon] to delete event information.

- Click ![icon] to view the most recent events.

7.3.5 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** page, click ![icon], and then select **DeepXplore**.

Step 2   Click ![icon].

Step 3   Configure the search conditions.

You can search for vehicle snapshots in the **Record** or **Person** section. For details, see "6.3 DeepXplore".

8 System Configurations

This chapter introduces system parameters configuration, license, service management and backup and, restore.

8.1 License Information

Log in to the DSS Client. On the **Home** page, click [icon], and then in the **System Config** section, select **License**.

On this page, you can view the types of devices and the number of channels that can be connected to the platform, and the number of App users that can be registered.

8.2 System Parameters

Configure security parameters, storage retention duration, email server, time sync, remote log, login method, and more.

8.2.1 Configuring Security Parameters

- 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.
- Protect your data by verifying login password when download or export information, and encrypting the export files.
- After the firewall of the server is enabled, you need to add the IP address of the computer where the DSS Client is installed to the HTTP allowlist so that it can access the server.
- After the firewall of the server is enabled, only the IP addresses in the RSTP allowlist can request video stream through the media gateway service. The IP addresses of decoders will be added automatically. If there are other IP addresses that need to request video stream through media gateway service, you need to manually add them to the RSTP allowlist.

Step 1   Log in to the DSS Client. On the **Home** page, click [icon], and then in the **System Config** section, select **System Parameter** > **Security Parameter**.

Step 2   Click [icon] to upload the SSL certificate and private key, and then click **Save**.

Step 3   Enable **File Export or Download Password Authentication** and **Encrypt Exported File**, and then click **Save**.

- **File Export or Download Password Authentication**: You need to enter the password of the current account to export or download files.
- **Encrypt Exported File**: When you use the exported file, you need to verify the password.

Step 4   Add IP addresses to the HTTP and RSTP allowlist.

8.2.2 Configuring Retention Period of System Data

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** page, click ![icon], and then in the **System Config** section, select **System Parameter**.

Step 2   Click **Message Retention Period**.

Step 3   Double-click a number to change its value.

Step 4   Click **Save**.

8.2.3 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 the time manually or automatically.

Step 1   Log in to the DSS Client. On the **Home** page, click ![icon], 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 8-1 Enable time synchronization
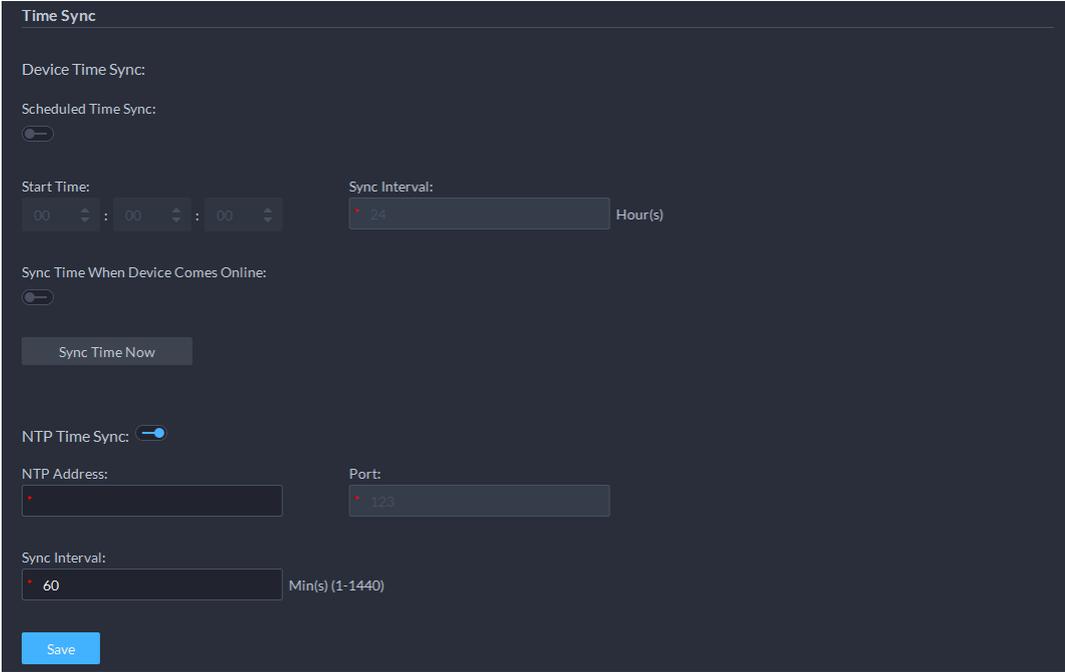
- Scheduled Time Sync: Enable the function, enter the start time in time sync for each day, and the interval.
- Sync Time When Device Comes Online: Syncs device time when the device goes online.
- NTP Time Sync: If there is an NTP server in the system, you can enable this function to let the system enable 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 **General** tab, select the check box next to **Time Sync**, and then click **Save**.

The system immediately synchronizes the time after you enable the function.

Figure 8-2 Enable time sync
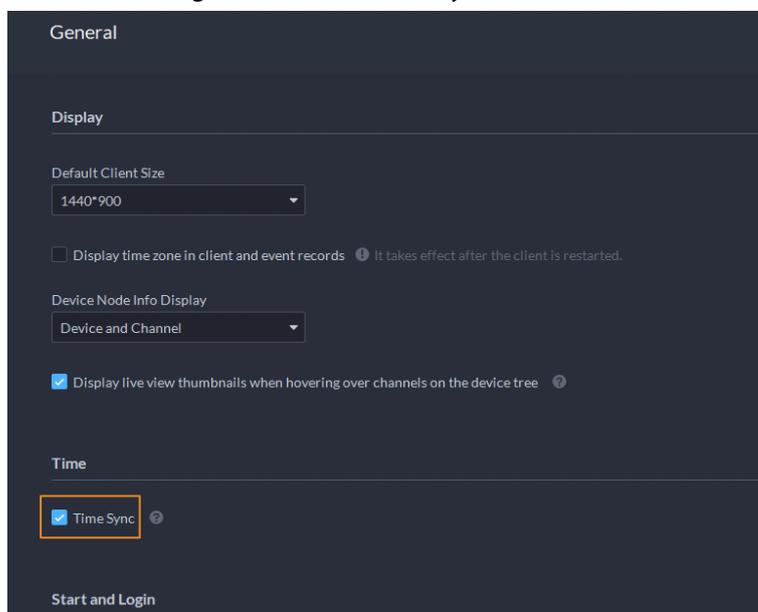
3) Restart the client for the configuration to take effect.

8.2.4 Configuring Email Server

Step 1   Log in to the DSS Client. On the **Home** page, 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 8-3 Set email server

Table 8-1 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**.

8.2.5 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** page, click , and then in the **System Config** section, select **System Parameter**.

Step 2   Click the **Login Mode** tab.

Step 3   Select a mode.

Figure 8-4 Select a login mode
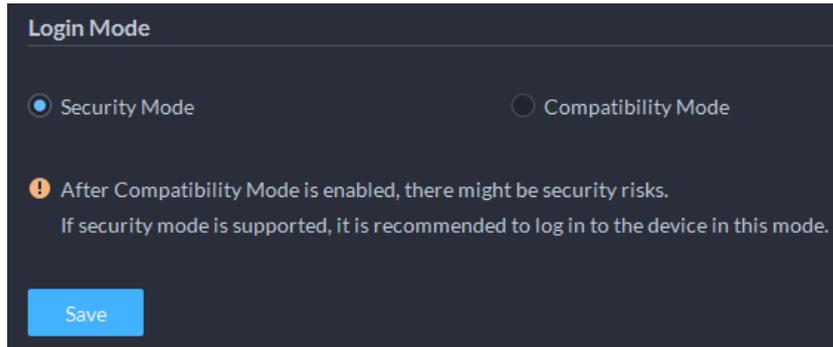
Step 4   Click **Save**.

8.2.6 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** page, 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 8-5 Enable remote log
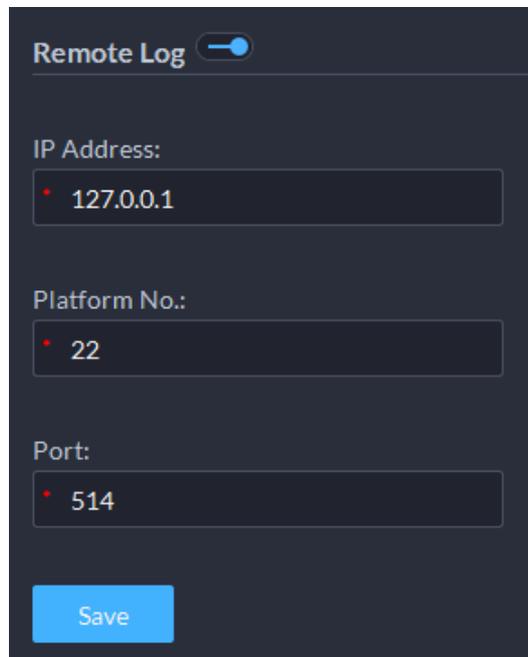
Step 4   Click **Save**.

8.3 Backup and Restore

The platform supports backing up configuration information and saving it to a computer or server, so that you can use the backup file for restoring settings.

8.3.1 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** page, 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 8-6 Manual backup
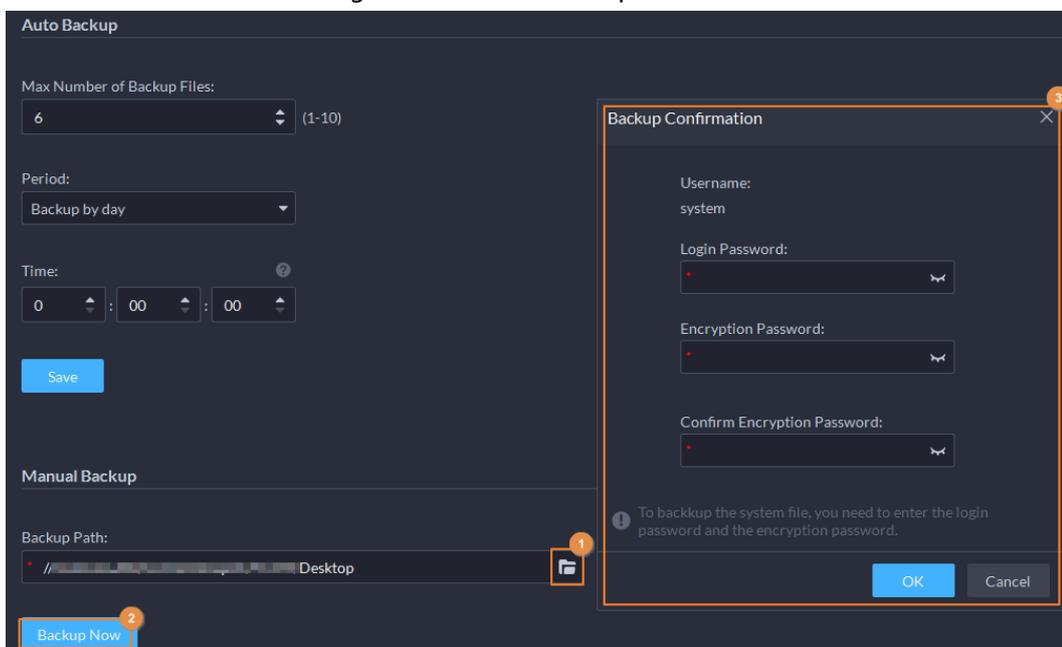
- Auto backup: In the **Auto Backup** section, configure backup parameters, and then click **OK**. The **Login Password** is the same as the system user's. Create an **Encryption Password** to protect the data. The platform automatically backs up data according to the defined time and period. The backup path is the installation path of the platform server by default.

📖

Max Number of Backup Files means you can only save defined number of backup files in the backup path.

Figure 8-7 Auto backup
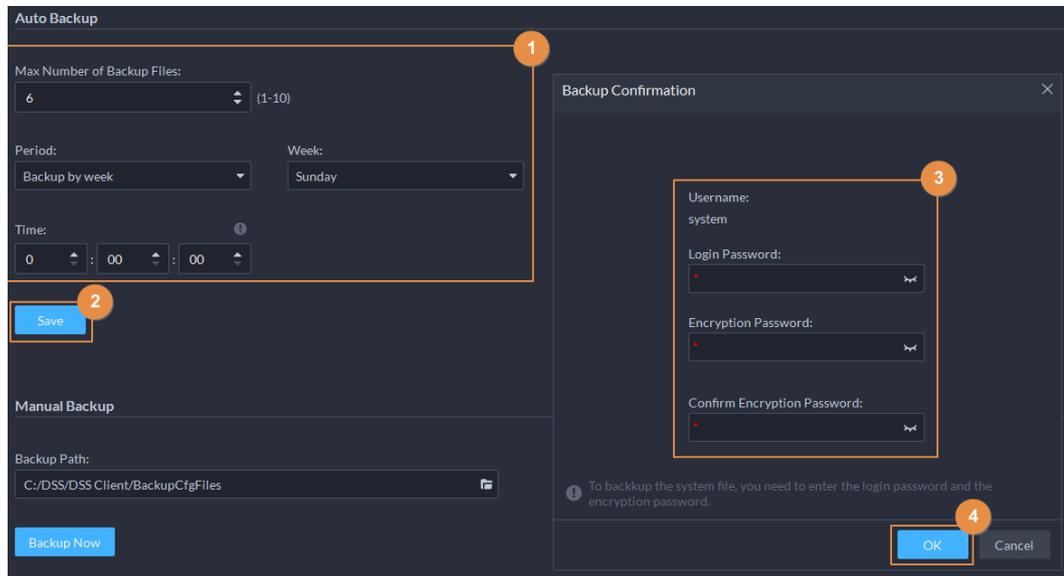
8.3.2 System Restore

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. Please be advised.

Step 1   Log in to the DSS Client. On the **Home** page, 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 8-8 Local restore
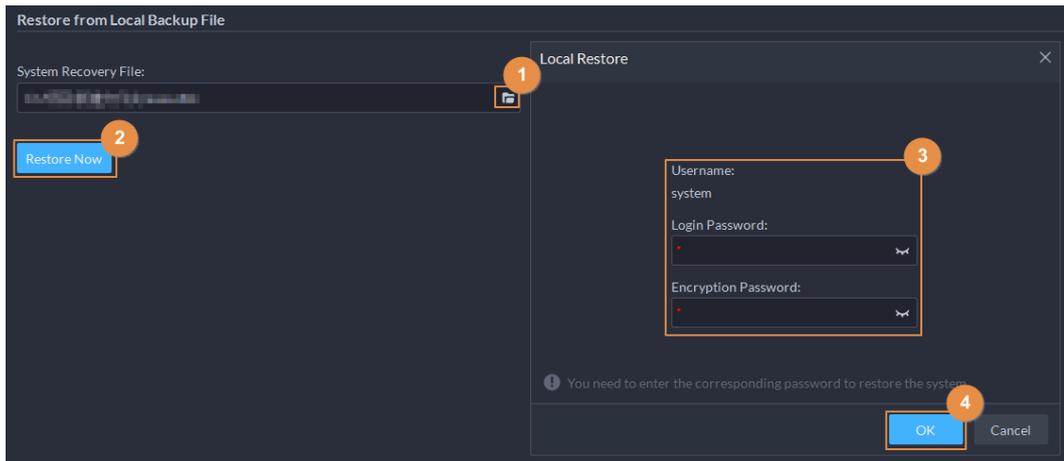
- Restore from backup file on the server: In the **Restore from Backup File on the Server** section, click ⟳, enter the passwords (the **Password** is the same as the system user's. The **Encryption Password** is the one created when the file was backed up), and then click **OK**. After restoration, the platform will automatically restart.

Figure 8-9 Restore from backup files on the server
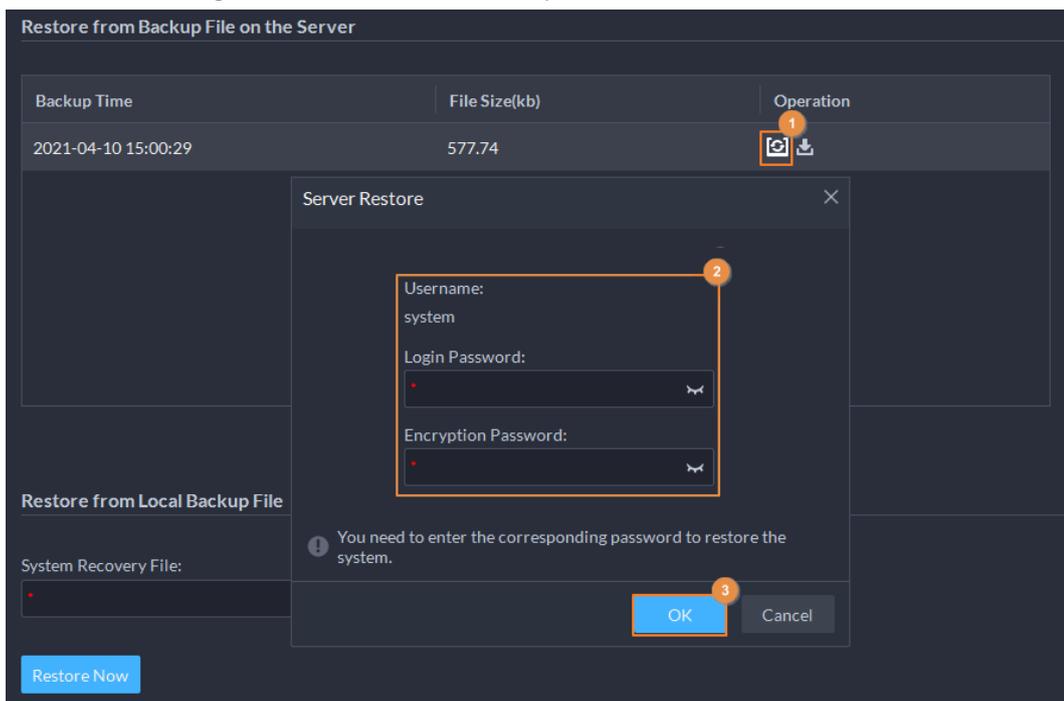
You can click 🔽 to download the backup file.

9 Management

9.1 Managing Logs

View and export operator logs, device logs and system logs, and enable the service log debug mode for troubleshooting.

9.1.1 Operator Log

Step 1   Log in to the DSS Client. On the **Home** page, select **Management** > **Logs**.

Step 2   Click ![icon].

Step 3   Click ![icon], select one or more types of log you want to search for, specify the time and keywords, and then click **Search**.

Step 4   To export the logs, click **Export**.

9.1.2 Device Log

Step 1   Log in to the DSS Client. On the **Home** page, select **Management** > **Logs**.

Step 2   Click ![icon].

Step 3   Select a device and time, and then click **Search**.

Step 4   To export the logs, click **Export**.

9.1.3 System Log

Step 1   Log in to the DSS Client. On the **Home** page, select **Management** > **Logs**.

Step 2   Click ![icon].

Step 3   Click ![icon], and then select one or more types of logs you want to search for.

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 computer.

9.1.4 Service Log Debug

Enable the debug mode of a service, and then it generates logs that are more detailed for troubleshooting.

Step 1   Log in to the DSS Client. On the **Home** page, select **Management** > **Logs**.

Step 2   Click ![icon].

Step 3   Enable the debug mode of one or more services.

📖

After the debug mode of a service is enabled, the service will generate a large amount of logs that occupy more disk space. We recommend you disable the debug mode after you have finish troubleshooting.

9.2 Downloading Videos

You can download videos of interest stored on the server or the device. The downloaded videos are in .avi, .mp4, or .asf formats. 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** page, select **Management** > **Download Center**.

Step 2   Set search conditions, and then click **Search**.

Figure 9-1 Download center
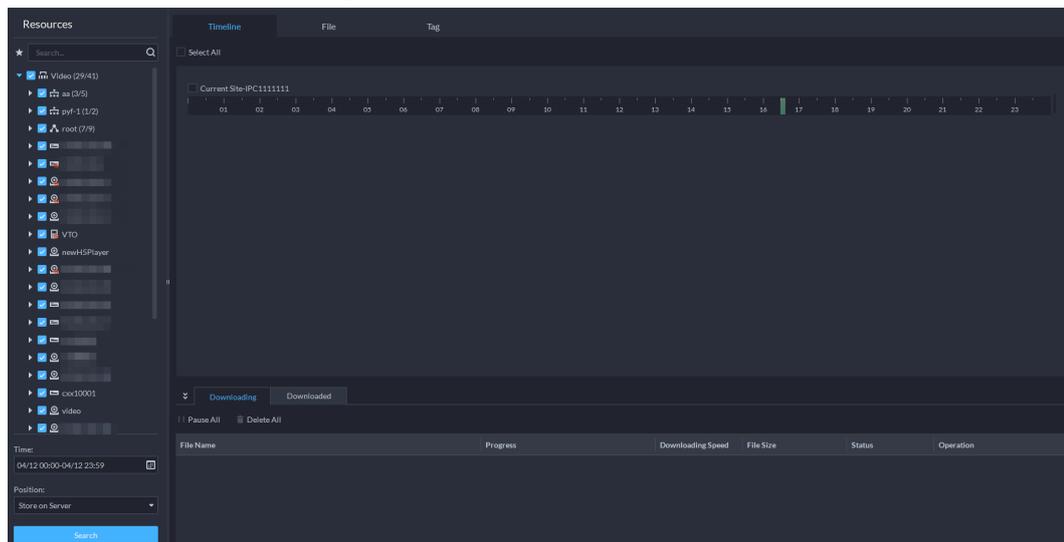
Step 3   Select videos to download.
● To download videos by clipping the timeline, click the **Timeline** tab, and then select the start and end time of the video clip by clicking on the timeline.
● To download videos by selecting searched video files, click the **File** tab, and then click 📥.
● To download 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 [toggle] 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 "9.4 Playing Local Videos".

9.3 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, video wall, security settings and shortcut keys.

9.3.1 Configuring General Settings

Configure client language, client size, time, and more.

Step 1   Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2   Click **General**, and then configure the parameters.

Figure 9-2 General parameters

Table 9-1 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.

Parameters	Description
Time Sync	If enabled, the client starts to synchronize network time with the server to complete time synchronization.
Auto run at startup	• If **Remember Password** has been selected on the **Login** page, select **Auto restart after reboot**, and the system will skip the login page and directly open the homepage after you restart the PC next time. • If **Remember Password** is not selected on the **Login** page, select **Auto restart after reboot**, the client login page will appear after you restart the PC.
Auto Login	Enable the system to skip the login page and directly open the homepage when logging in next time. • If **Remember Password** and **Auto Login** have been selected on the **Login** page, the function is already enabled. • If **Remember Password** has been selected while **Auto Login** is not selected on the **Login** page, select **Auto Login** on the **Basic** page to enable this function. • If neither **Remember Password** nor **Auto Login** has been selected on the **Login** page, select **Auto Login** on the **Basic** page 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**.

9.3.2 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** page, select **Management** > **Local Settings**.

Step 2   Click **Video**, and then configure the parameters.

Figure 9-3 Video parameters

Table 9-2 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 page 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.

Parameters	Description
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. 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.
Number of Continuous Snapshots	

Step 3　　Click **Save**.

9.3.3 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** page, select **Management** > **Local Settings**.

Step 2　　Click **Video Wall**, and then configure the parameters.

Figure 9-4 Configure video wall settings

Table 9-3 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 the video to maximize the window, and then its stream type will switch to main stream.

Parameter	Description
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.
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**.

9.3.4 Configuring Alarm Settings

Configure alarm sound and alarm display method on the client.

Step 1   Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2   Click **Alarm**, and then configure the parameters.

Figure 9-5 Configure alarm settings
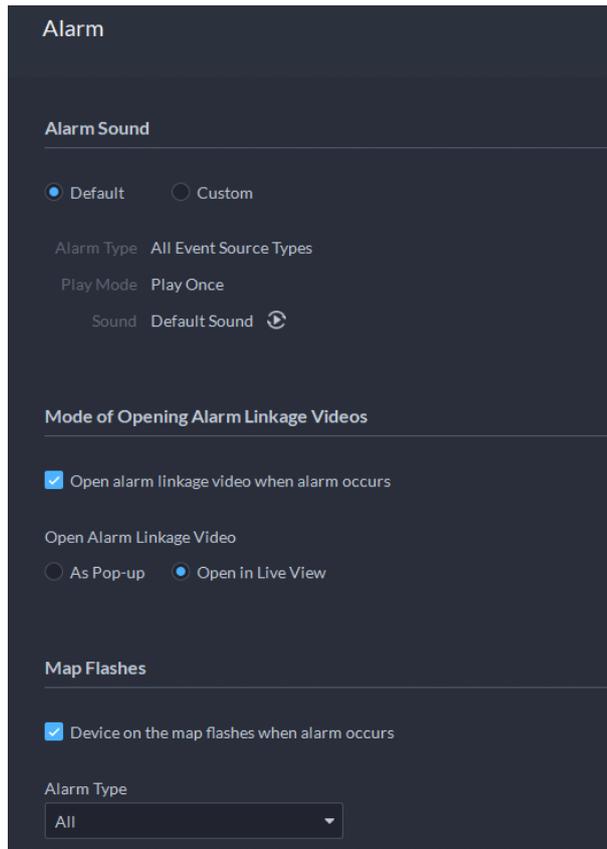
Table 9-4 Parameter description

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.

Parameters	Description
Open alarm linkage video when alarm occurs	If selected, the platform will automatically open linked video(s) when an alarm occurs. ● **As Pop Up**: The alarm video will be played in a pop-up window.
Open Alarm Linkage Video	● **Open in Live View**: The alarm video will be played in a window in **Monitoring Center**. For this function to work properly, you must enable **When an alarm is triggered, display camera live view on client** when configuring an event. For details, see "5.1 Configuring Events".
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**.

9.3.5 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** page, select **Management** > **Local Settings**.

Step 2   Click **File Storage**, and then configure the parameters.

Figure 9-6 Configure file storage settings

Table 9-5 Parameter description

Parameters	Description
Video Naming Rule	Select a naming rule for manual recordings.
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 for 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**.

9.3.6 Viewing Shortcut Keys

View shortcut keys for operating the client quickly.

Step 1　Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2   Click **Shortcut Key** to view shortcut keys of the PC keyboard and USB joystick.

Figure 9-7 View shortcut keys

Function	Shortcut Keys
Move Up	Up
Move Down	Down
Move Left	Left
Move Right	Right
Iris -	Insert
Iris +	Delete
Focus -	Home
Focus +	End
Zoom -	PgUp
Zoom +	PgDn
Open Single Window	Enter
Close Single Window	Enter
Open Full Screen	Ctrl+F
Exit Full Screen	Esc
Pause/Continue Tour	Ctrl+T
Lock Client	Ctrl+L

(Shortcut Keys — 262 — Keyboard Type: ⦿ PC Keyboard ◯ Joystick USB Keyboard)

9.4 Playing Local Videos

You can play local videos directly on the platform.

Step 1   Log in to the DSS Client. On the **Home** page, select **Management** > **Local Video**.

Figure 9-8 Local video

No video file. Click Add File to add video files.
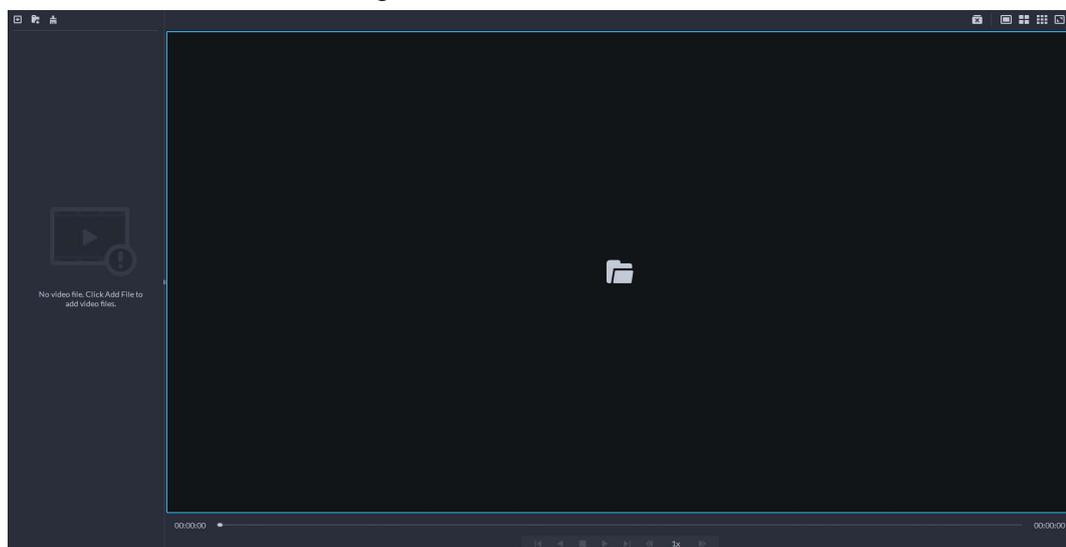
Step 2   Click [icon] to select one or more files, or [icon] to open all files in a folder.

Figure 9-9 Play list

Step 3   Drag a file to the window on the right or right click it to play.

Related Operations

Table 9-6 Interface operation

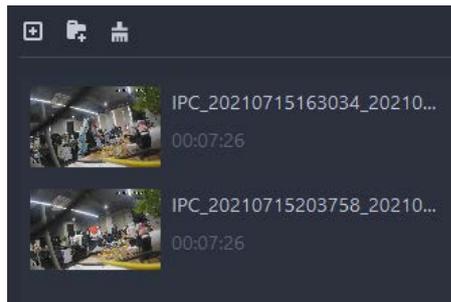| Icon/Function	Description
Right-click menu	• **Continuous Snapshot**: Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to ..*DSS\DSS Client\Picture* by default. To change the snapshot saving path, see "9.3.5 Configure File Storage Settings". • **Video 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.
	Fast/slow playback. Max. supports 64X or 1/64X.
	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 page with search results. More operations: • : Move the selection area. • : Adjust the size of the selection area. • Right-click to exit search by snapshot.

9.5 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** page, select **Management** > **Quick Commands**.
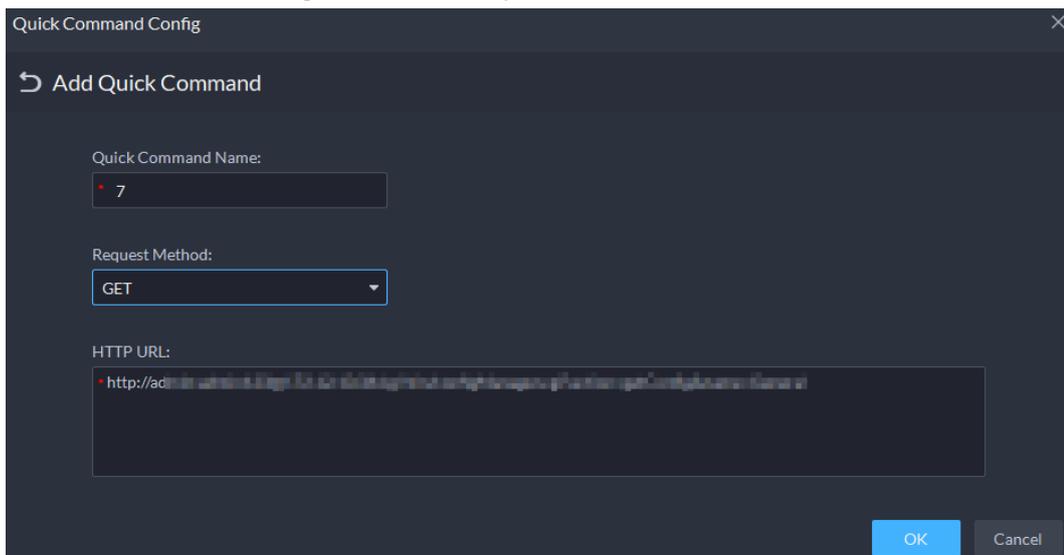
Figure 9-10 Quick commands
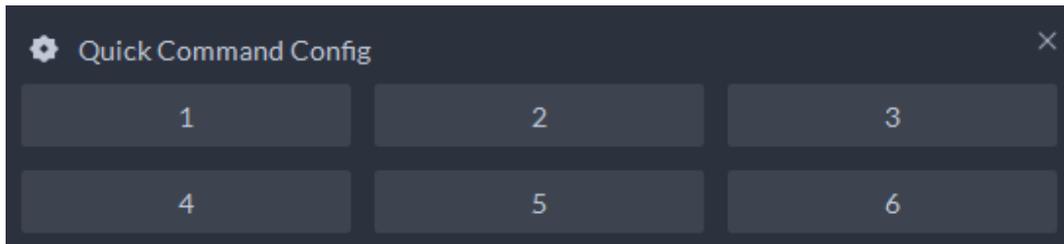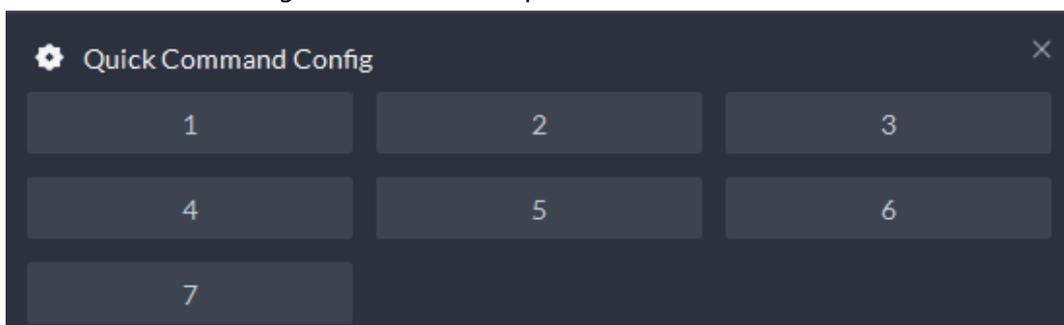

Step 2   Click ⚙.
Step 3   Click **Add**.

Figure 9-11 Add a quick command

Step 4   Configure the parameters, and then click **OK**.

Figure 9-12 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

Service Name		Function Description
Access Service	NGINX	Reverses user requests to distributed system management services.
System Management Service	SMC	Manages services and provides access to various pages.
Device Discovery Service	HRS	Broadcasts platform information to discover devices.
Data Cache Service	REDIS	Stored temporary business data from the platform.
Database	MySQL	Stores platform business data.
Message Queue Service	MQ	Transfers messages between platforms.
Device Management Service	DMS	Registers encoders, receives alarms, transfers alarms, and sends out the sync time command.
Media Transmission Service	MTS	Gets audio/video bit streams from front-end devices and then transfers the data to DSS, the client and decoders.
Storage Service	SS	Stores, searches for and plays back recordings.
File Resource Node Management Service	FNODE	Manages the file resource node management service.
File Resources Node Service	FILERESOURCE	Manages files from MPT devices and related operations.
Device Search Service	SOSO	Searches for device information.
Auto Register Service	ARS	Listens, logs in, or gets bit streams to send to MTS.
ProxyList Control Proxy Service	PCPS	Logs in to ONVIF device, and then gets the stream and transfers the data to MTS.
Alarm Dispatch Service	ADS	Sends alarm information to different objects according to defined plans.
Access Controller Access Service	MCDDOOR	Manages access controller access and related operations.
External LED Device Access Service	MCDLED	Manages LED access and other related operations.
External Alarm Controller Access Service	MCDALARM	Manages alarm controller access and other related operations.

Service Name		Function Description
Access Control Service	ACDG	Manages access control and other related operations.
Video Intercom Switch Center	SC	Manages PC client and App client login as SIP client, and also forwards audio-talk streams.
Object Storage Service	OSS	Manages storage of face snapshots and intelligent alarm pictures.
Picture Transfer Service	PTS	Manages picture transmission.
Video Matrix Service	VMS	Logs in to the decoder and sends tasks to the decoder to output on the TV wall.
Media Gateway	MGW	Sends MTS address to decoders.
Power Environment Server	PES	Manages access of dynamic environment monitoring devices.

Appendix 2 Cybersecurity Recommendations

Security Statement

- If you connect the product to the Internet, you need to bear the risks, including but not limited to the possibility of network attacks, hacker attacks, virus infections, etc., please strengthen the protection of the network, platform data and personal information, and take the necessary measures to ensure the cyber security of platform, including but not limited to use complex passwords, regularly change passwords, and timely update platform products to the latest version, etc. Dahua does not assume any responsibility for the product abnormality, information leakage and other problems caused by this, but will provide product-related security maintenance.
- Where applicable laws are not expressly prohibited, for any profit, income, sales loss, data loss caused by the use or inability to use this product or service, or the cost, property damage, personal injury, service interruption, business information loss of purchasing alternative goods or services, or any special, direct, indirect, incidental, economic, covering, punitive, special or ancillary damage, regardless of the theory of liability (contract, tort, negligence, or other) , Dahua and its employees, licensors or affiliates are not liable for compensation, even if they have been notified of the possibility of such damage. Some jurisdictions do not allow limitation of liability for personal injury, incidental or consequential damages, etc., so this limitation may not apply to you.
- Dahua's total liability for all your damages (except for the case of personal injury or death due to the company's negligence, subject to applicable laws and regulations) shall not exceed the price you paid for the products.

Security 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 an allowlist 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.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING