DSS Professional

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V8.1.1

Foreword

General

This user's manual introduces the functions and operations of DSS Professional (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.

- 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

Dahua Security System (DSS) Professional is designed for centralized security management. It enhances hardware performance and provides centralized video monitoring, access control, video intercom, alarm controller, POS, radar and AI features, such as face recognition, automatic number plate recognition, and video metadata.

Whether you are a small business with a few cameras, or a global business spread across the globe with over 20,000 cameras, DSS Professional is the right solution for you. Even if your needs change in the future, you can easily scale, upgrade or add functionalities to DSS Professional so that your needs are met. Build your security management system on a solid foundation with DSS Professional.

1.2 Highlights

- Scalable design, easy to grow
  With distributed deployment, you can easily expand the supported channels to 20,000 and central storage capacity to 4 PB. The multi-site function allows you to incorporate multiple DSS platforms into one, and conveniently show their information on one PC client. You can access live and recorded videos, real-time and historical events, and more.
- AI-powered applications, proactive security
  DSS Professional integrates various AI capabilities that devices have, such as face recognition, automatic number plate recognition, and video metadata. You will be notified immediately when the target you are interested in appears, allowing you or security personnel to take necessary security measures.
- Highly available technology, more stable
  With hot standby and N+M redundancy, DSS Professional ensures that your business will not be interrupted by failed servers.
- Customized services, enhanced competitiveness
  We offer services for you to build DSS Professional into your own platform, allowing it to fully suit your needs and give you a competitive edge in the market.

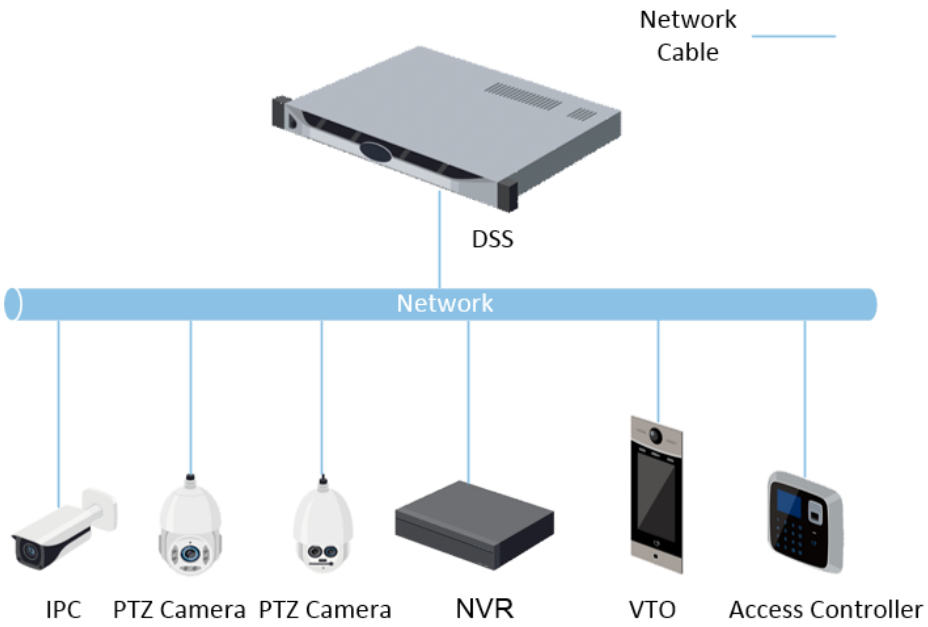
2 Installation and Deployment

DSS platform supports standalone deployment, distributed deployment, hot standby, and N+M deployment, and LAN to WAN mapping.

Standalone Deployment

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

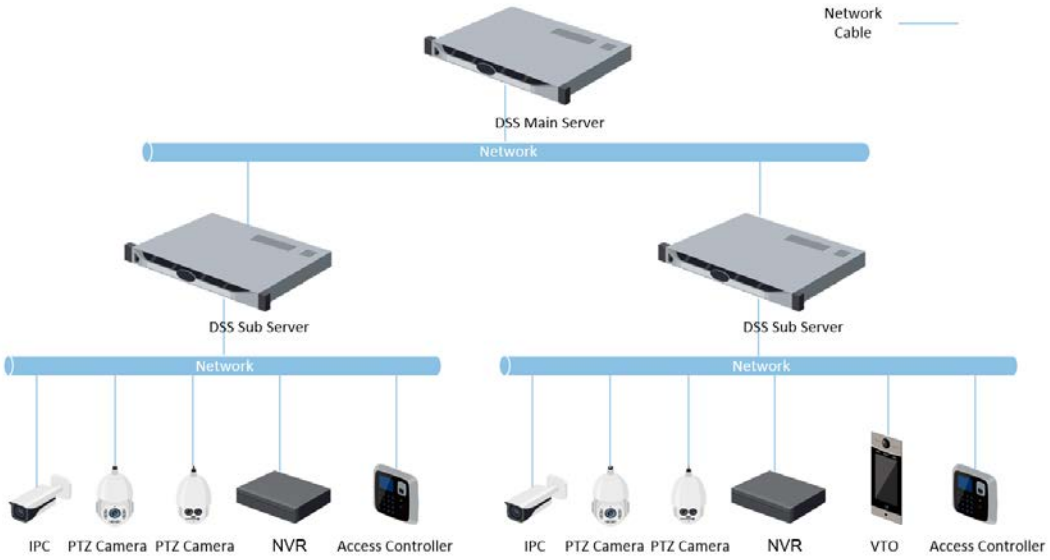
Figure 2-1 Standalone deployment



Distributed Deployment

Suitable for medium to larger projects. Sub servers are used to share system load, so that more devices can be accessed. The sub servers register to the main server, and the main server centrally manages the sub servers.

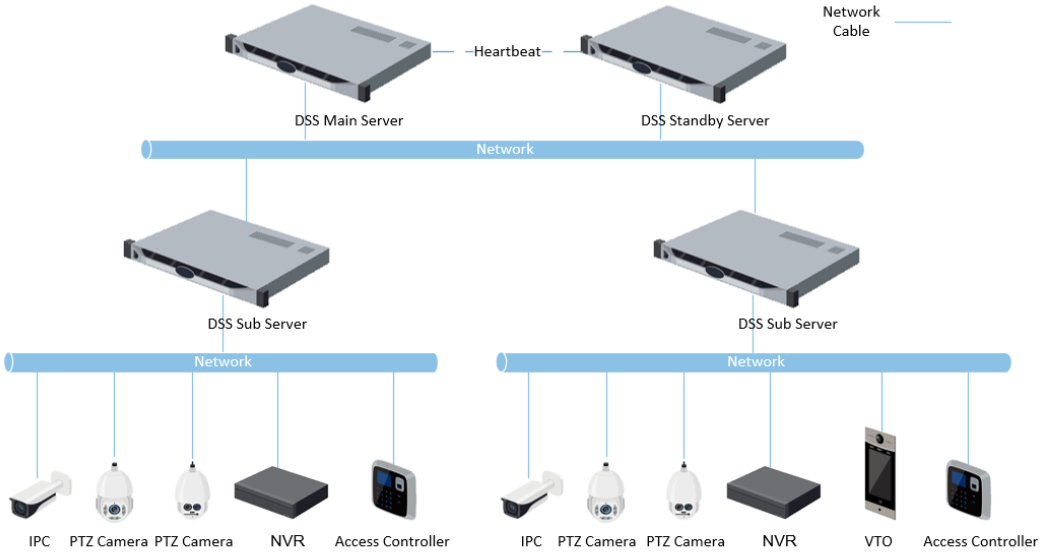
Figure 2-2 Distributed deployment



Hot Standby

Used with systems that require high stability. The standby server takes over the system when the active server malfunctions (such as with power-off and network disconnection). You can switch back to the original active server after it recovers.

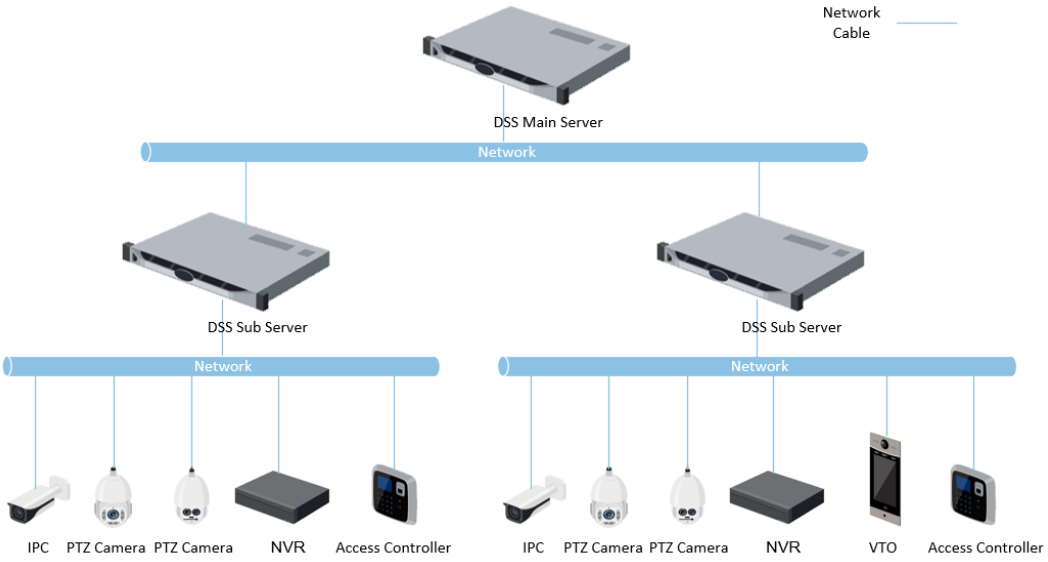
Figure 2-3 Hot standby



N+M

Each sub server has a standby server to maintain stability. When a sub server malfunctions, the system replaces it with an idle standby server. When the malfunctioning server normalizes, you can manually switch back to it. If you do not manually switch them, the system will automatically make the switch if the standby server malfunctions.

Figure 2-4 N+M



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 DSS Server 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 Standalone Deployment

2.1.1 Server Requirements

Table 2-1 DSS Pro hardware requirements

Parameter	Hardware Requirement	Operating System
Recommended configuration	• CPU: Intel Xeon Silver 4214 2.2GHz • RAM: 16 GB • Network card: 4 × Ethernet port @ 1000 Mbps • Hard drive type: 7200 RPM Enterprise Class HDD 1 TB • DSS installation directory space: 500 GB	• Win10-64 bit • Windows server 2012 • Windows server 2016 • Windows server 2019
Minimum configuration	• CPU: Intel Xeon E-2224 3.4GHz/4core • RAM: 8 GB • Network card: 2 × Ethernet port @ 1000 Mbps • Hard drive type: 7200 RPM Enterprise Class HDD 1 TB • DSS installation directory space: 500 GB	Win10-64 bit

- Face recognition images, videos, and files cannot be stored on the system disk and DSS installation disk. We recommend you store these files on network disks.
- For best performance, we recommend adding additional hard drives to store pictures.

2.1.2 Installing DSS

Prerequisites

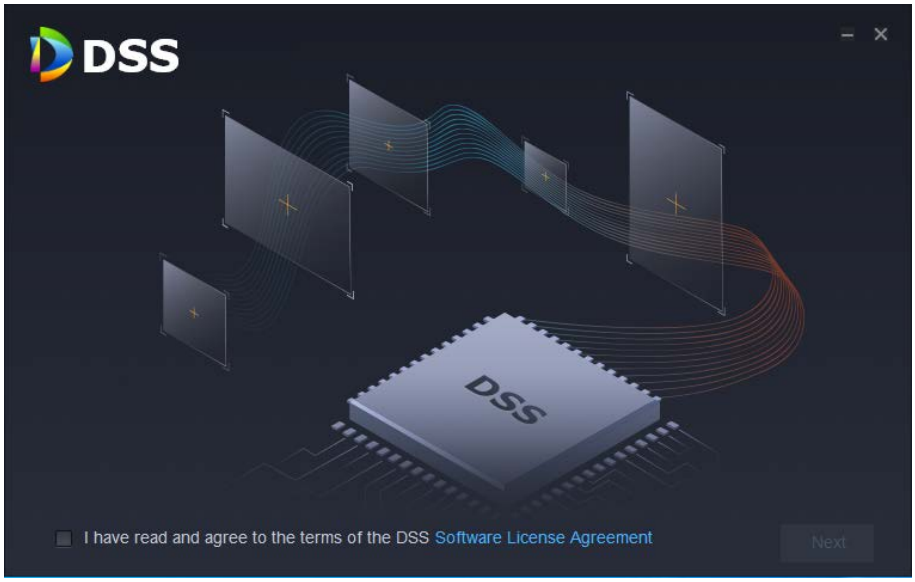
- You have downloaded the DSS installer from the official website or received it from our sales or technical support.
- You have prepared a server that meets the hardware requirements mentioned in "2.1.1 Server Requirements", and the server IP address is configured.

Procedure

Step 1 Double-click the DSS installer .

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

Figure 2-5 Install DSS server



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

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

Figure 2-6 Select a server type

Step 4 Select **Main** from the server type, and then click **Next**.

Step 5 Click **Browse**, and then select the installation path.

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

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

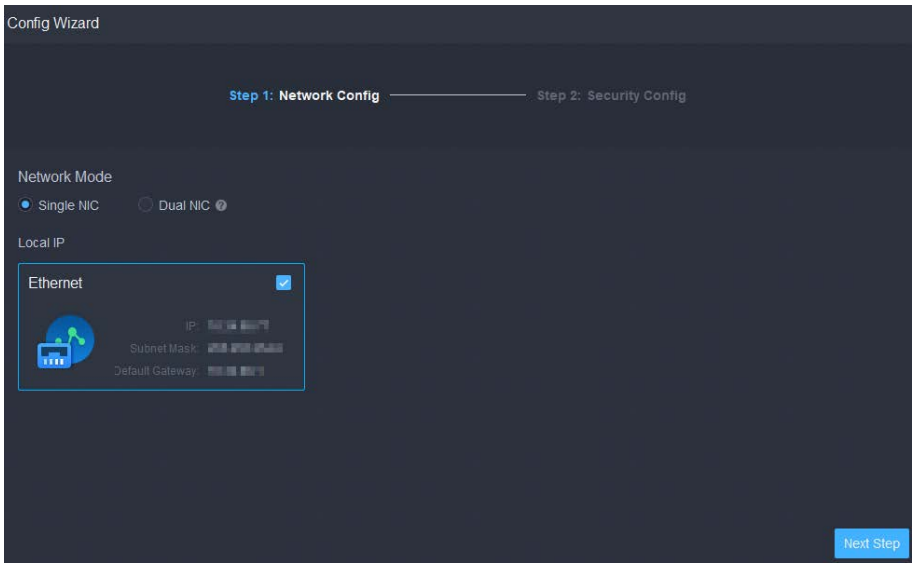
Step 6 Click **Install**.

The installation process takes about 4 to 8 minutes. Do not cut off the power or close the program.

Figure 2-7 Run the DSS server

Step 7 Click **Run** when the installation finishes.

Figure 2-8 Select the network mode and network card



Step 8 Select a network mode and the network card, and then click **Next Step**.

Dual NIC will be available if the server has two network cards. This is useful when you need to access devices on two different network segments.

Step 9 Enable or disable TLS1.0 as needed.

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

Step 10 Click **Finish**.

If the available RAM of the server is less than 4 GB, you can only use basic functions related to video. If it is less than 2.5 GB, you cannot use any function.

Related Operations

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

2.1.3 Configuring Server IP Address

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

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

2.1.4 Managing System Services

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

On the server, double-click  .

Figure 2-9 Service management page

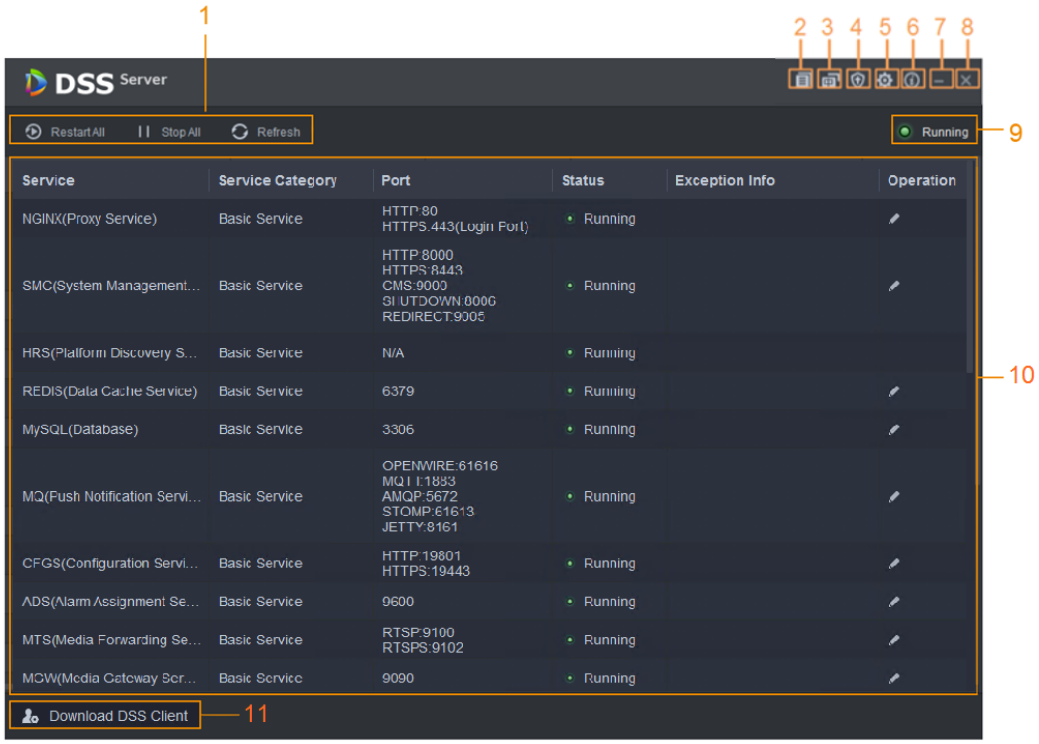


Table 2-2 Interface description

No.	Function	Description
1	Service Management	• Click Restart All to restart all services. When starting the platform, if the available memory of the server does not reach 4 GB, only the basic video services can be enabled. If the server has less than 2.5 GB of available memory, no services are available. • Click Stop All to stop all services. • Click Refresh to refresh services.
2	User's manual	User manual.
3	Language	Switch language.
4	Security Setting	TLS 1.0 has known security vulnerabilities. We strongly recommend you disable it to avoid security risks. If it is disabled, the web page of DSS platform cannot be accessed through the browser. You need to enable TLS 1.1 and TLS 1.2 in the browser settings to gain access to the web page. 1. Open Internet Explorer. 2. Click the **Tools** button at the upper-right corner, and then select **Internet Options**. 3. Select the **Advanced** tab. 4. Go to the **Settings** > **Security**, and then select **Use TLS 1.1** and **Use TLS 1.2**. 5. Click **OK**.

No.	Function	Description
5	Setting	Configure the IP address of the server and IP mapping. • Set up an IP address for the server so that the platform can access the network and the devices in it. If the server has two network cards, you can select **Dual NIC** mode, configure two IP addresses, and then the platform will be able to connect to two networks and access the devices on each one. • If the platform is in a local network and the devices are on the internet, or you need to access the platform that is in a local network from the Internet, you need to map the IP address of the platform to a WAN IP address or a domain name. For details, see "2.5.2 Mapping IP or Domain Name".
6	About	Software version information.
7	Minimize	Minimize the page.
8	Close	—
9	Service Status	• Starting: Services are starting. • Unavailable: Service is running abnormally • Stopping: Services are stopping. • Running: Service is running normally • Stopped: Services have stopped.
10	Services	Displays each service and service status. Click to modify service port number, and then the services will restart automatically after modification.
11	Download DSS Client	Go to client download page of the DSS client.

2.1.5 Installing and Logging into DSS Client

Install the DSS client before licensing it.

2.1.5.1 Installing DSS Client

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

2.1.5.1.1 DSS Client Requirements

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

Table 2-3 Hardware requirements

Parameters	Description
Recommended system requirements	• CPU: Intel Core i5, 64 bits 4 Core Processor • Memory: 8 GB and above • Graphics: NVIDIA® GeForce®GT 730 • Network Card: 1000 Mbps • HDD: Make sure that at least 200GB is reserved for the client.

2.1.5.1.2 Downloading and Installing DSS Client

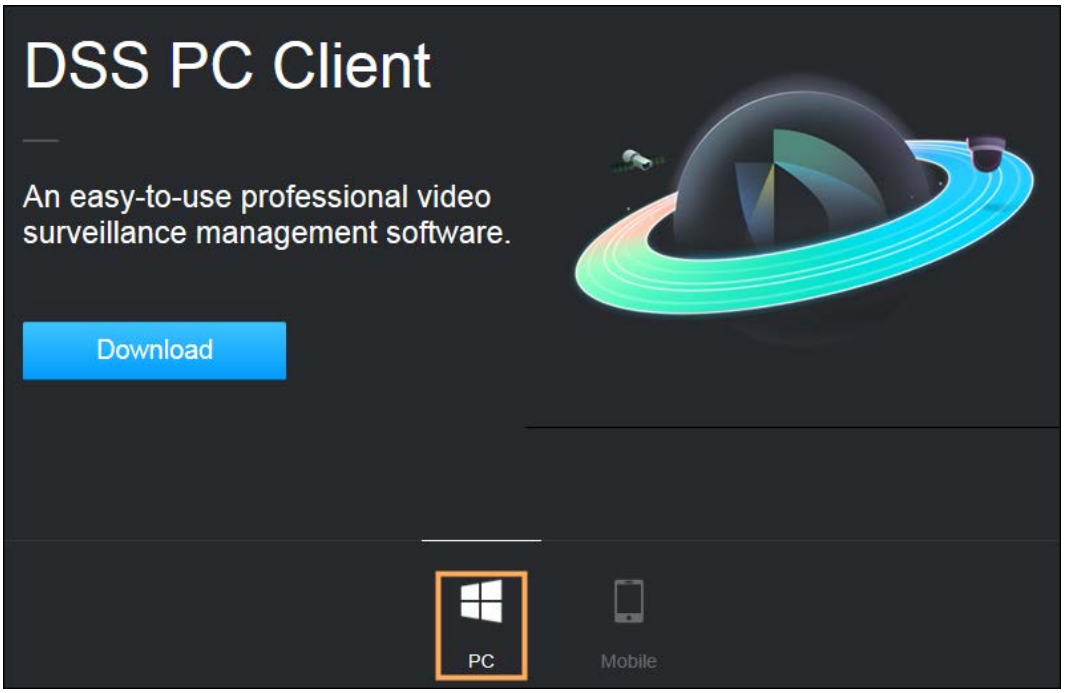
Step 1 Go to https://*IP address of the platform* in the browser

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

If you save the program, go to Step3.

If you run the program, go to Step4.

Figure 2-10 Download DSS Client



Step 3 Double-click the DSS Client program.

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

Step 5 Select installation path.

Step 6 Click **Install**.

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

2.1.5.2 Logging in to DSS Client

Step 1 Double-click  on the desktop.

Step 2 Select a language and user type.

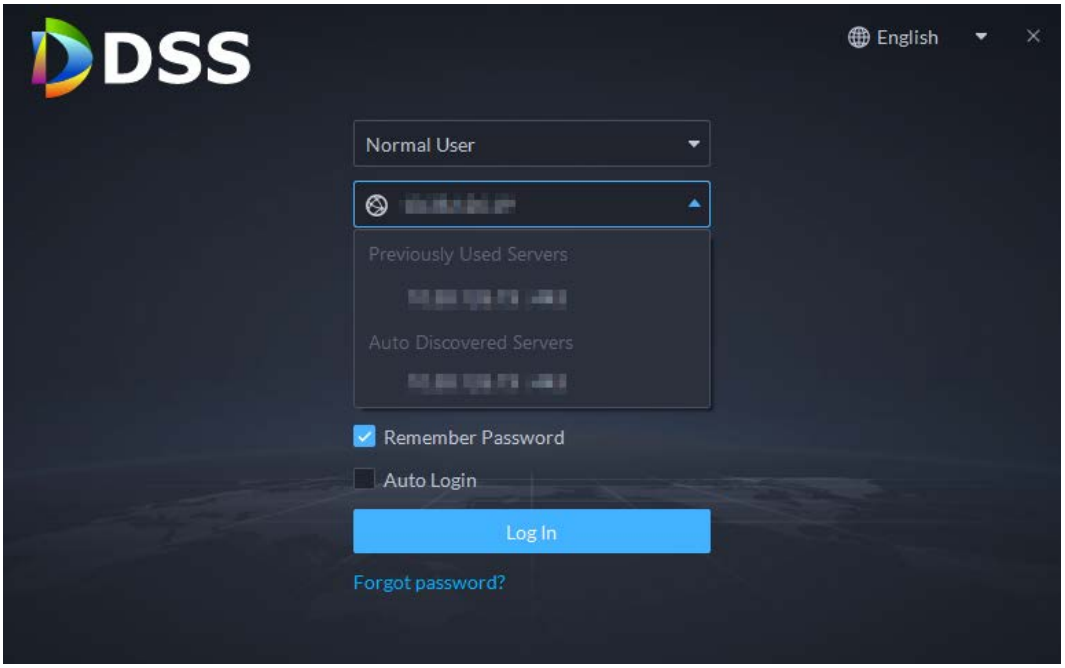
If you want to log in using a domain user account, you must import domain users first. For details, see the user's manualsee "3.3.3 Importing Domain User".

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. For details, see the user's manualsee "2.5.2 Mapping IP or Domain Name".

Figure 2-11 Automatically discovered platform



Step 4 Click anywhere else on the page to start initializing the platform.

For first-time login, you will be automatically directed to the initialization process.

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) The default user is system. Enter and confirm the password, and then click **Next**.

   The password must consist of 8 to 32 non-blank characters and contain at least two types of characters: Uppercase, lowercase, number, and special character (excluding ' " ; : &).

2) Select your security 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.

2.1.5.3 Homepage of DSS Client

Figure 2-12 Homepage

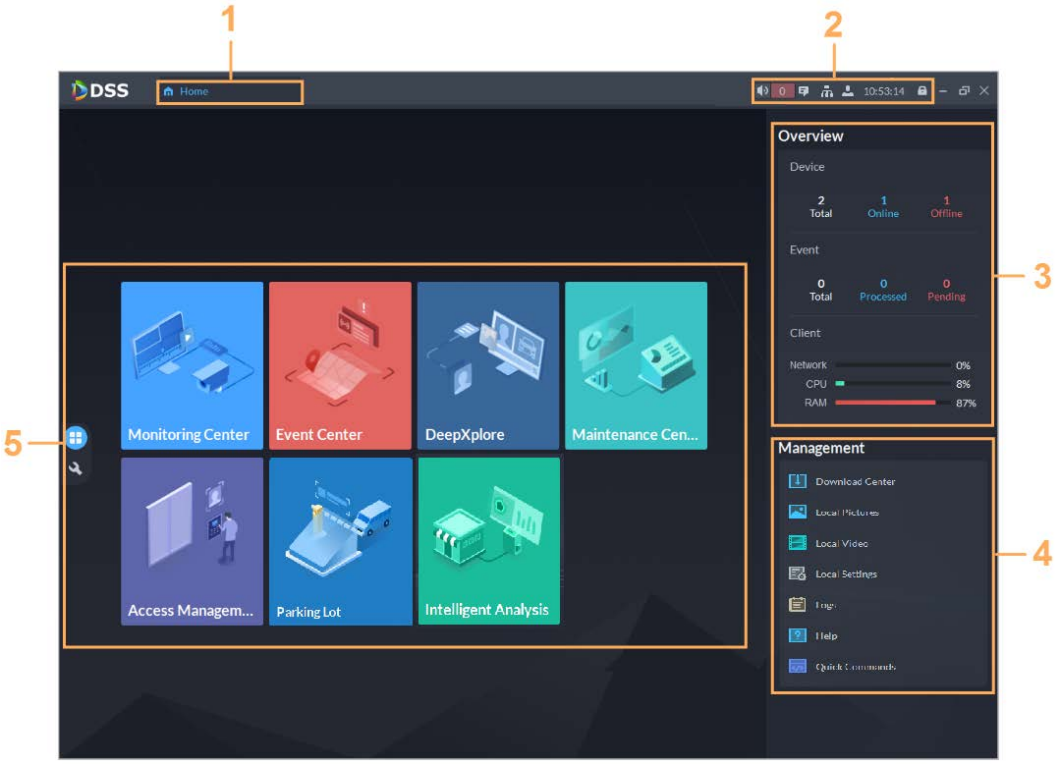


Table 2-4 Parameter description

No.	Name	Function
1	Tab	Displays the names of all tabs that are opened.

No.	Name	Function
2	System settings	• : Enable or disable alarm audio. • 0 : Displays number of alarms. Click the icon to go to **Event Center**. • Click to view system messages, such as the information of a device was edited or deleted. The permissions of a user will determine what messages can be seen. For example, if user A does not have the permission of device A, then user A will not get the message when device A is deleted. • Click to connect to other platforms as sites to your current platform. You can view certain resources from the sites. For details, see the user's manualsee "3.5 Connecting to Multiple Sites". • : User information: Click the icon, and then you can log in to the web page by clicking system IP address, change password, lock client and log out. ◇ Click platform IP address to go to the Web page. ◇ Click **Change Password** to change user password. ◇ Click **About** to view version information. ◇ Click **Sign Out** to exit client. • Click to lock client.
3	Overview	• The number of devices in total, offline and online. • The number of total, processed and pending events. • The client network, CPU and RAM usage.
4	Management	• Download videos. • Check local pictures and videos. • Settings for video, snapshot, video wall, alarm, security and shortcut keys. • View and manage logs. • View user manual. • Customize quick HTTP commands. For details, see the user's manualsee "8.5 Quick Commands".
5	Applications	• : Application options including monitoring center, access management, intelligent analysis and vehicle entrance control. • : Configuration options.

2.1.6 Licensing

Activate the platform with a trial or paid license the first time you log in to it. Otherwise you cannot use it. You can upgrade your license for more features and increased capacity.

This section introduces license capacity, how to apply for a license, how to use the license to activate the platform, and how to renew your license.

2.1.6.1 Applying for a License

A license is used to confirm the features and number of channels you purchased. To get a formal license, contact our sales personnel. To apply for a trial license, visit our website and find DSS Pro, scroll to the bottom, click **Apply**, and then follow the instructions.

2.1.6.2 Activating License

The following images of the page might slightly differ from the actual pages.

2.1.6.2.1 Online Activation

Prerequisites

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

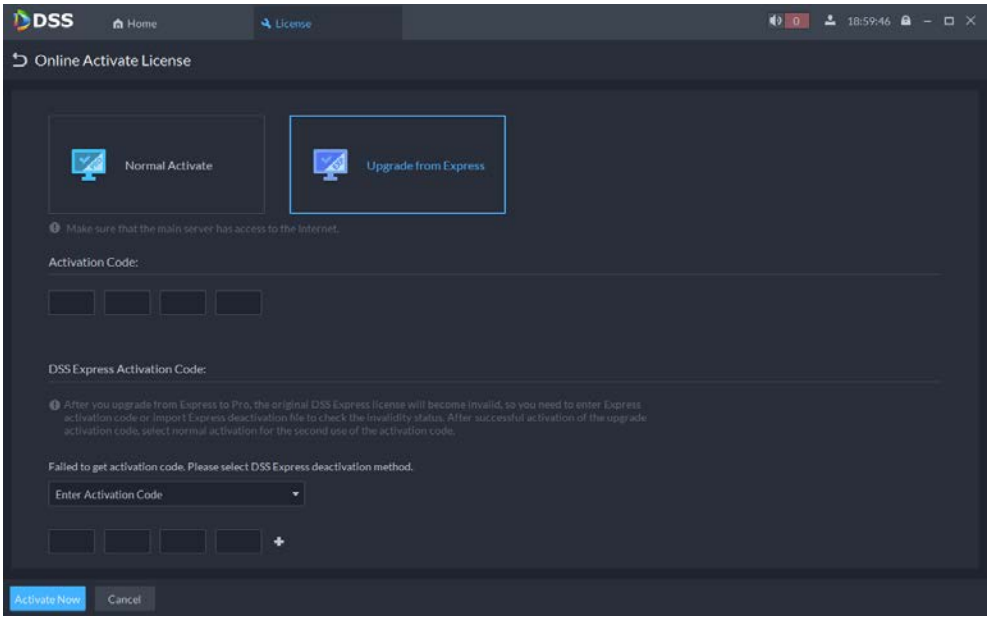
Procedure

Step 1 On the **Home** page, click and then in **System Config**, select **License**.

Step 2 Click **Online Activate License**.

Step 3 Select an activation method. Select **Normal Active** to complete the process. If you upgraded the system from Express to DSS Pro, and DSS Express has a paid license, then select **Upgrade from Express** instead.

Figure 2-13 Select a method



Step 4 Enter your new **Activation Code**.

1. Enter the DSS Pro activation code that you received.
2. If you select **Upgrade from Express**, enter the original Express activation code or

import the deactivation file.

- Enter the original activation code: Select **Enter Activation Code**, and then enter the original activation code.
- Import the deactivation file: Select **Import DSS Express Deactivation Code**, click , and then select the deactivation file.

Step 5 Click **Activate Now**.

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

2.1.6.2.2 Offline Activation

Prerequisites

You have received your license. If not, see "2.1.6.1 Applying for a License".

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

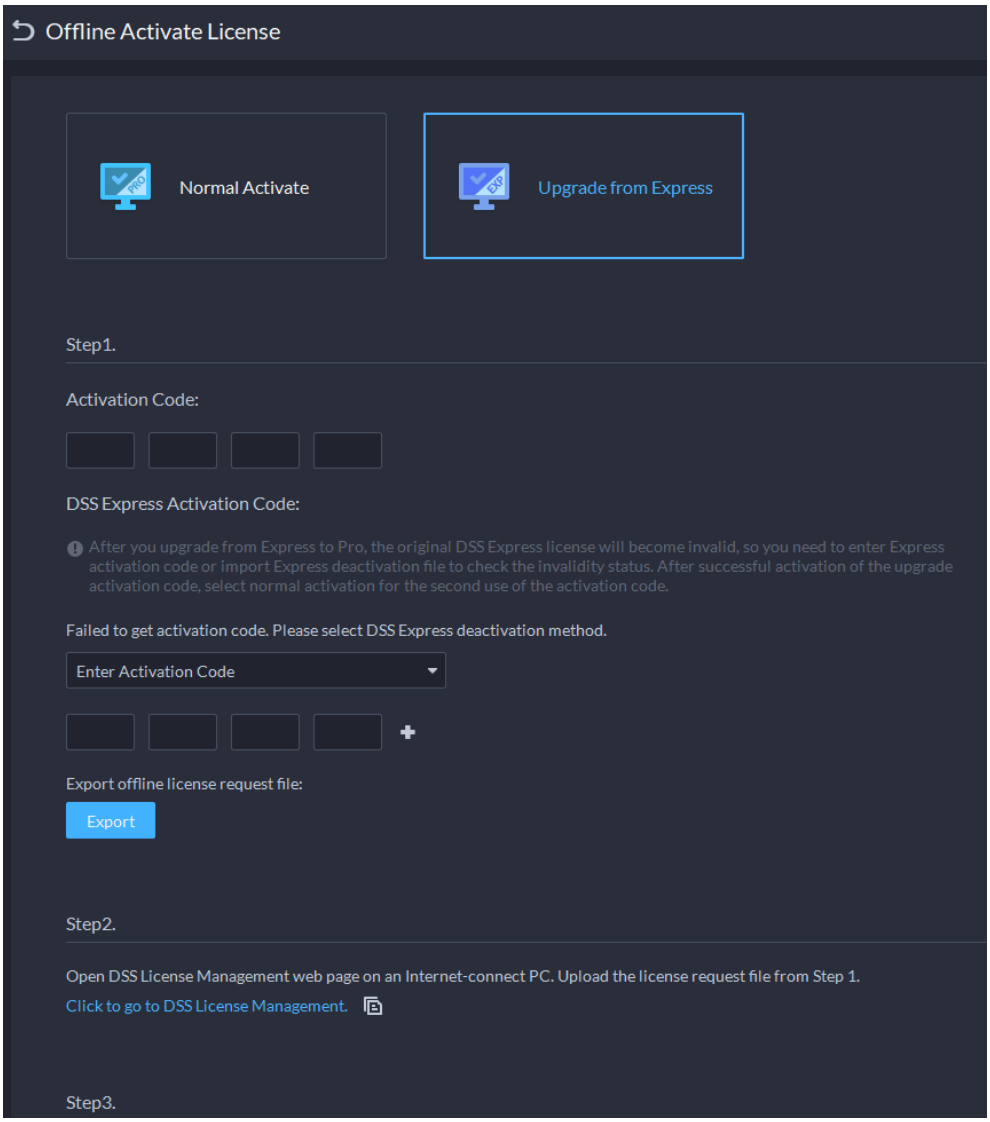
Procedure

Step 1 On the **Home** page, click , and then in **System Config**, select **License**.

Step 2 Click **Offline Activate License**.

Step 3 Select an activation method. Select **Normal Active** to complete the process. If you upgraded the system from Express to DSS Pro, and Express has a paid license, then select **Upgrade from Express** instead.

Figure 2-14 Select a method



Step 4 Enter your new **Activation Code**.

1. Enter the DSS Pro activation code that you received.
2. If you select **Upgrade from Express**, enter the original Express activation code or import the deactivation file.
   - Enter the original activation code: Select **Enter Activation Code**, and then enter the original activation code.
   - Import the deactivation file: Select **Import DSS Express Deactivation Code**, click , and then select the deactivation file.

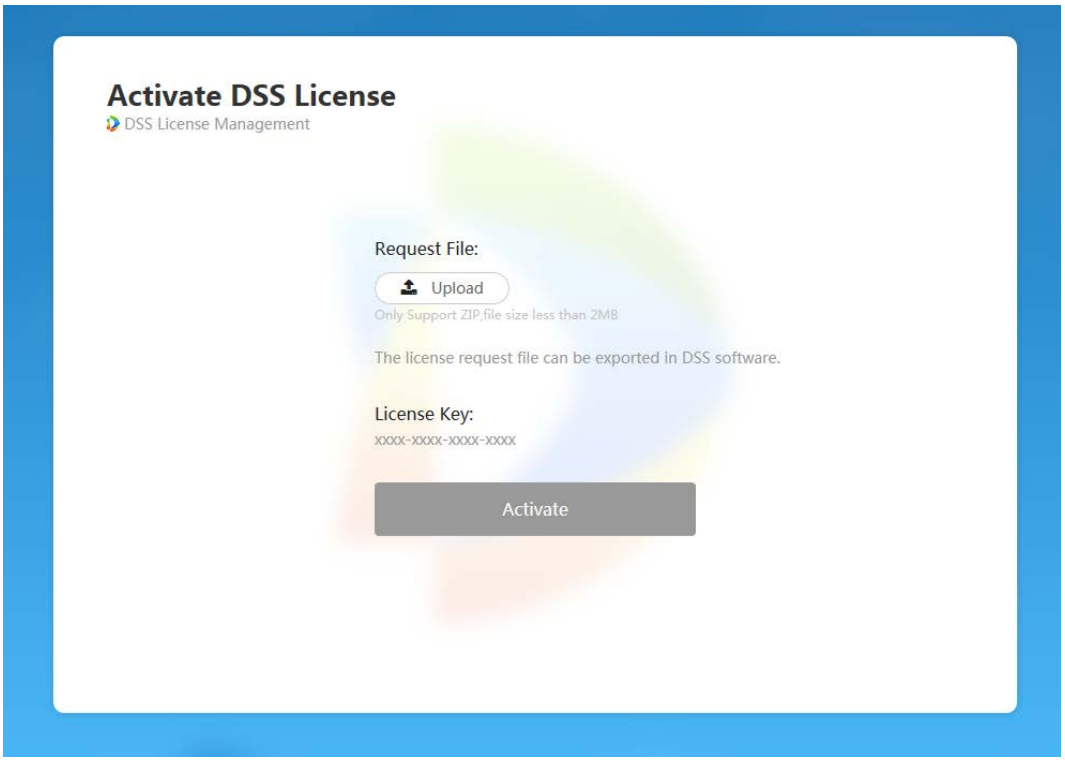
Step 5 Click **Export** to export the license request file.

Step 6 Generate license file.

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

The success page is displayed, where a download prompt is displayed asking you to save the license activation file.

Figure 2-15 Upload license request file



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

Step 7 On the **License** page, view your license details.

2.2 Distributed Deployment

2.2.1 Installing Main Server

For details about how to install the main server, see "2.1 Standalone Deployment".
After sub server are deployed, log in to the main server, and then you can view the status of the sub servers.

2.2.2 Installing Sub Server

This section introduces how to install sub servers and register them to the main server.

Prerequisites

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

Procedure

Step 1 Double-click the DSS installer .

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

Step 2 Click **agreement**, read through the agreement, and then accept it.

Step 3 Select the agreement check box, and then click **Next**.

Step 4 Select **Sub** for server type, and then click **Next**.

Step 5 Click **Browse**, and then select the installation path.

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

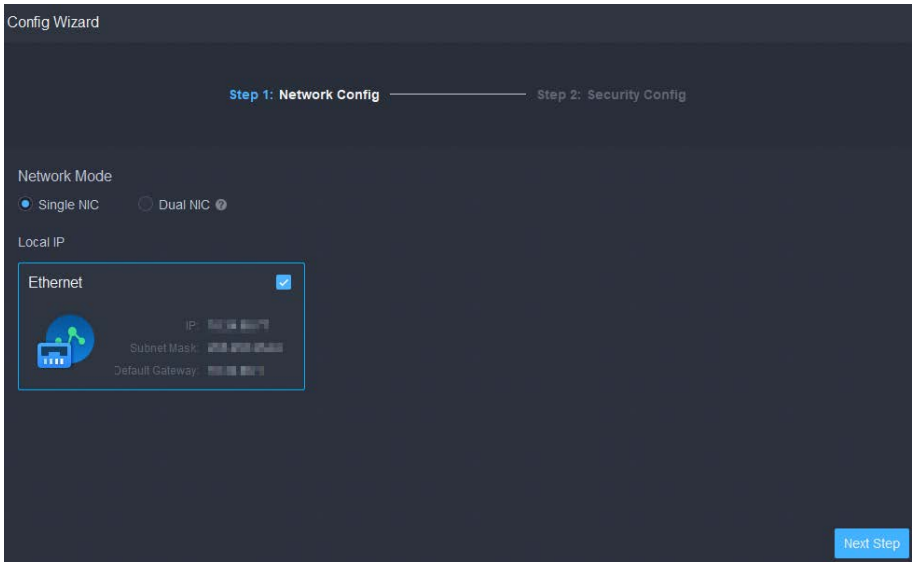
We recommend you do not install the platform into drive C because features such as face recognition require higher disk performance.

Step 6 Click **Install**.

The installation process takes about 5 to 10 minutes. Do not cut off the power or close the program.

Step 7 Click **Run** when the installation finishes.

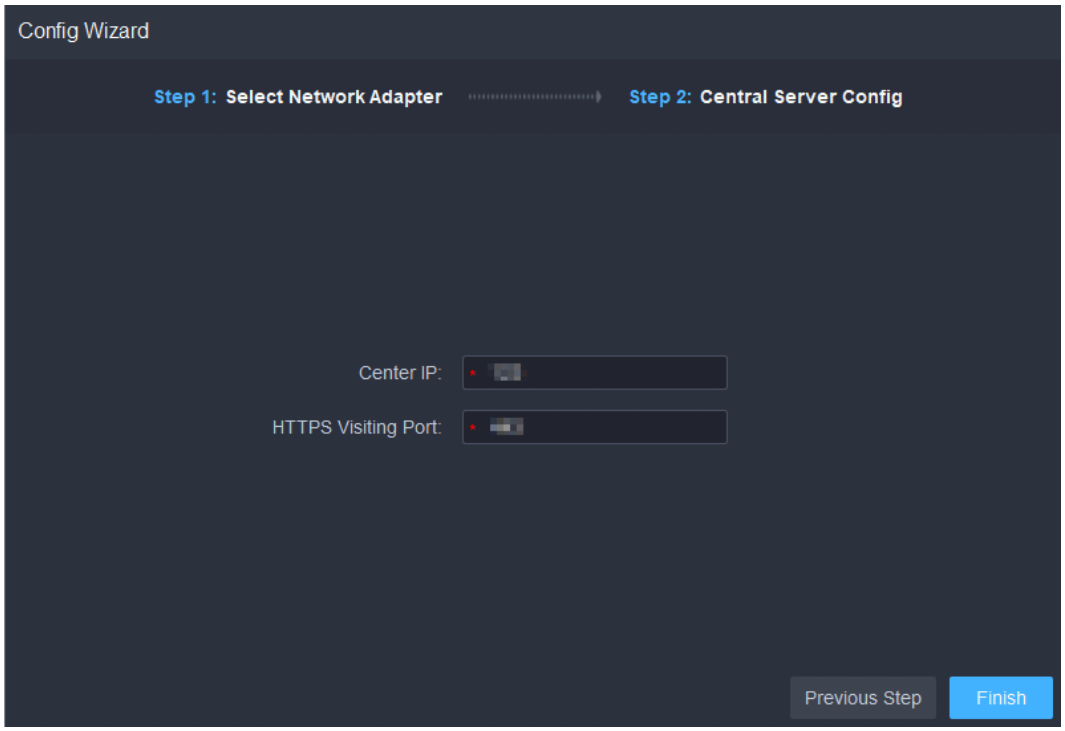
Figure 2-16 Select network mode and network card



Step 8 Select a network mode and the network card, and then click **Next Step**.

Dual NIC will be available if the server has two network cards. This is useful when you need to access devices on two different network segments.

Figure 2-17 Configure the information of the main server



Step 9 Configure the IP address and port of the main server.

Step 10 Click **Finish**.

After successfully installing a sub server, you need log in to the platform of main server to enable it so that it can work properly. For details, see the user's manualsee "7.1.1 Distributed Deployment".

Related Operations

- To edit service ports, start or stop services, refresh services, view service status or more, see "2.1.4 Managing System Services".
- To uninstall the platform, go to **Control Panel** > **Programs and Features**, and then locate DSS Server. Double-click it, and then uninstall it according to the on-screen instructions.

2.3 Hot Standby

For detailed steps, see *DSSReplicatorPlus2.0 Configuration Guide V8.1.1.docx*. If you have any problems, contact technical support.

2.4 N+M

On the main server, enable the sub server, and then create the sub-standby relationship.

Prerequisites

See "2.1 Standalone Deployment" and "2.2 Distributed Deployment" to deploy the servers you need.

The relevant servers have been well deployed.

Procedure

Step 1 Log in to the parent DSS client. On the **Home** page, click > **System Deployment**.

Step 2 Click .

Step 3 Click to enable the sub servers.

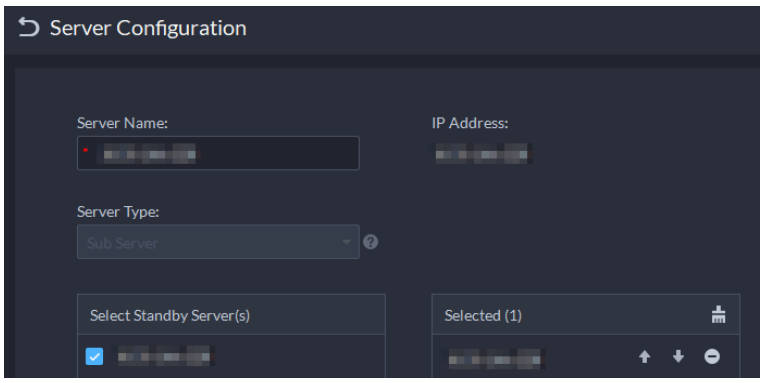
Step 4 Configure a standby server.

1) Click of a sub server.
2) Select **Standby Server** for **Server Type**, and then click **OK**.

Step 5 Configure the sub-standby relationship in either of the following ways.

- Go to the **Server Configuration** page of the sub server to select a standby server.
  1. Click of a sub server.
  2. On the **Select Standby Server(s)** section, select one or more standby servers.

Figure 2-18 Select a standby server



  3. Click **OK**.

- Go to the **Server Configuration** page of the standby server to select a sub server.
  1. Click of a standby server.
  2. On the **Select Sub Server(s)** section, select one or more sub servers.
     You can click to adjust the priority.
  3. Click **OK**.

2.5 Configuring LAN or WAN

2.5.1 Configuring Router

For the list of the ports that need to be mapped, see "Appendix 1 Service Module Introduction".

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

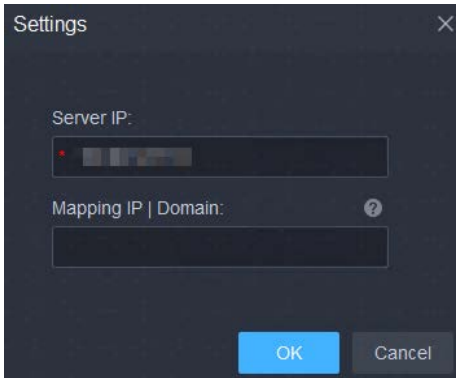
2.5.2 Mapping IP or Domain Name

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

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

Step 2 Click the on the upper-right corner.

Figure 2-19 Setting



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 Basic Configurations

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

3.1 Preparations

3.1.1 Installing DSS Client

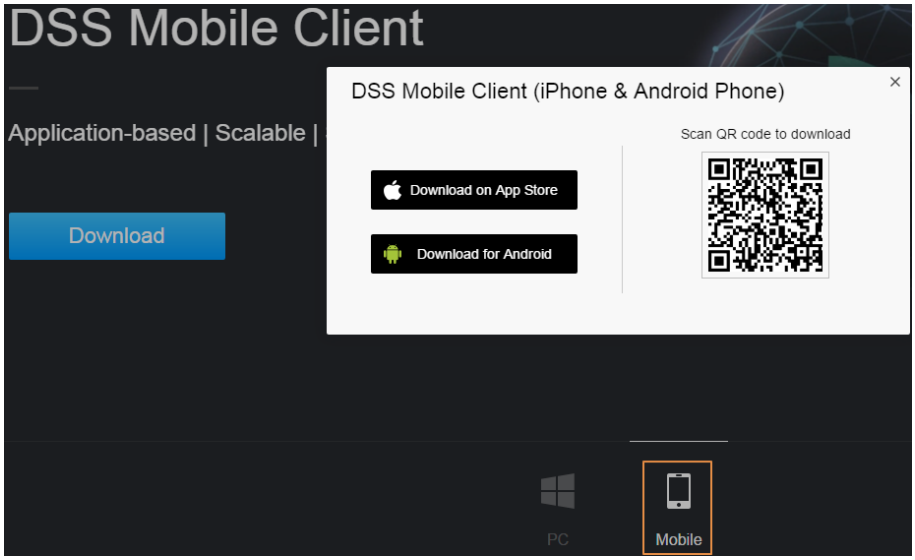
See "2.1.5 Installing and Logging into DSS Client".

3.1.2 Installing Mobile Client

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

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

Figure 3-1 Download App by scanning QR code



3.2 Managing Resources

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

3.2.1 Adding Organization

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

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

Procedure

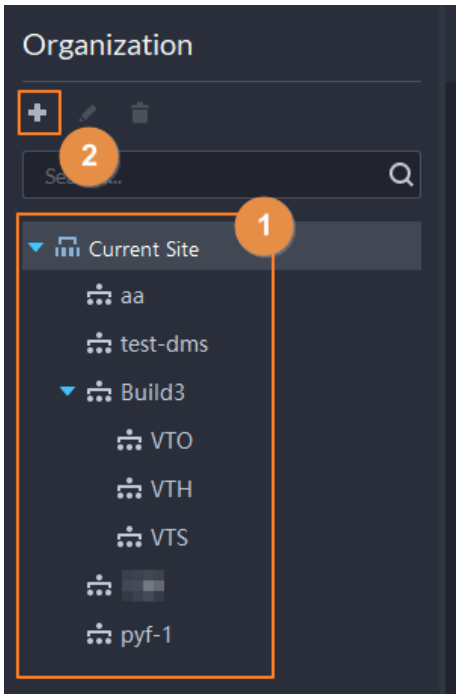
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

Step 2 Click .

Step 3 Add an organization.

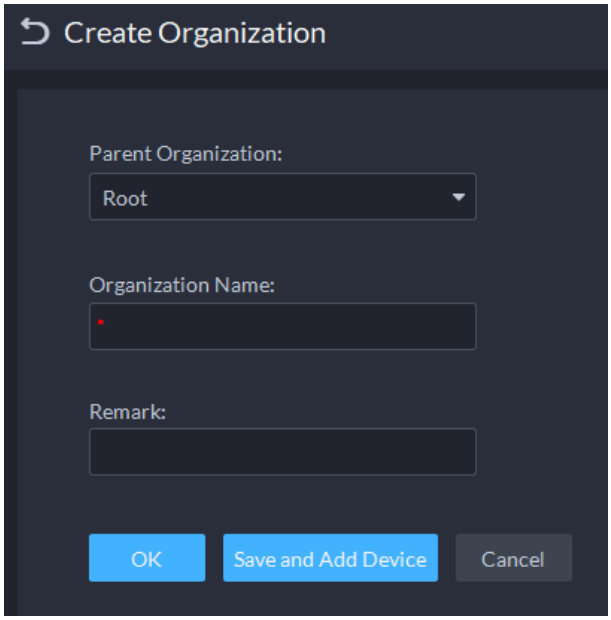
1) Select a parent organization.
2) Click .

Figure 3-2 Add an organization



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

Figure 3-3 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.

3.2.2 Managing Device

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

3.2.2.1 Searching for Online Devices

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

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

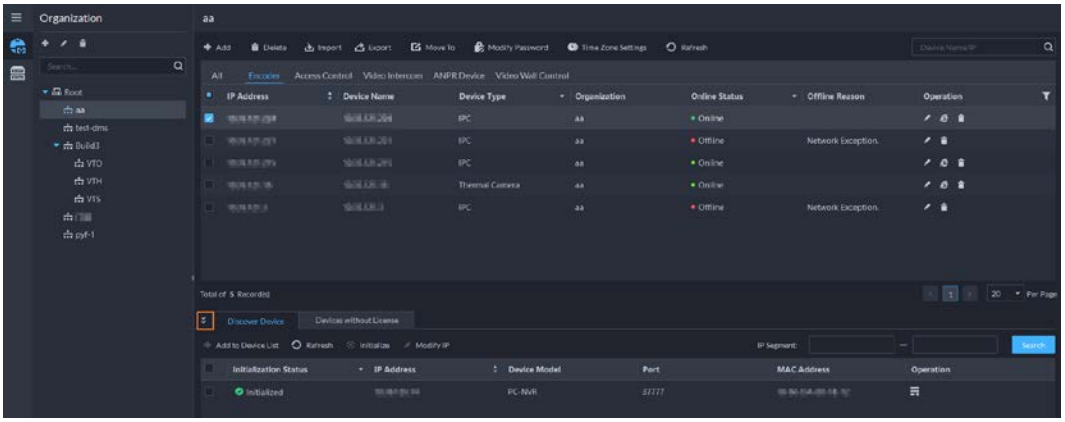
Step 2 Click .

Step 3 Click .

The icon changes to when devices are searched.

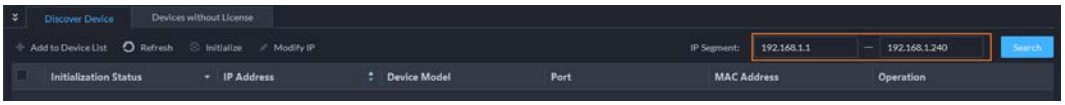
- When using the platform for the first time, the platform automatically searches for devices on the same network segment.
- If not the first time, the platform automatically searches for the devices in the network segment you configured last time.

Figure 3-4 Search for devices



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

Figure 3-5 IP segment search



3.2.2.2 Initializing Devices

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

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

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

- You can select multiple devices to initialize them in batches. Make sure that the selected devices have the same username, password and email information. 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.

3.2.2.3 Changing Device IP Address

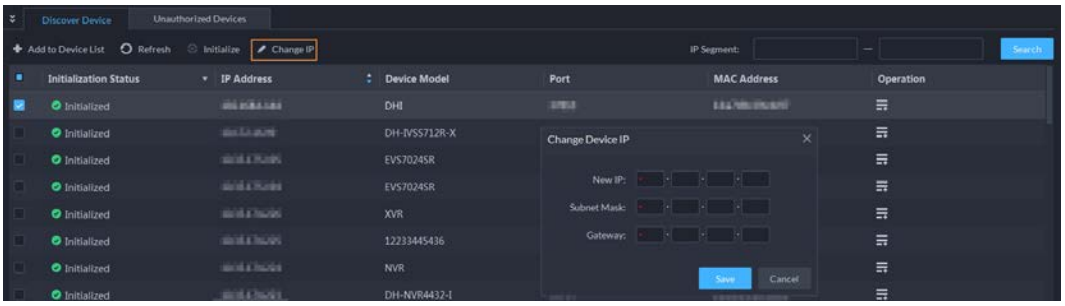
You can change IP addresses of the devices that have not been added to the platform.

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

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

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

Figure 3-6 Change IP address



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

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

Step 4 Enter the username and password used to log in to the devices, and then click **OK**.

3.2.2.4 Adding Devices

You can add different types of devices, such as encoder, decoder, ANPR device, access control, displays, emergency assistance device, alarm box, radar device, 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**.

3.2.2.4.1 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. Contact technical support for help.

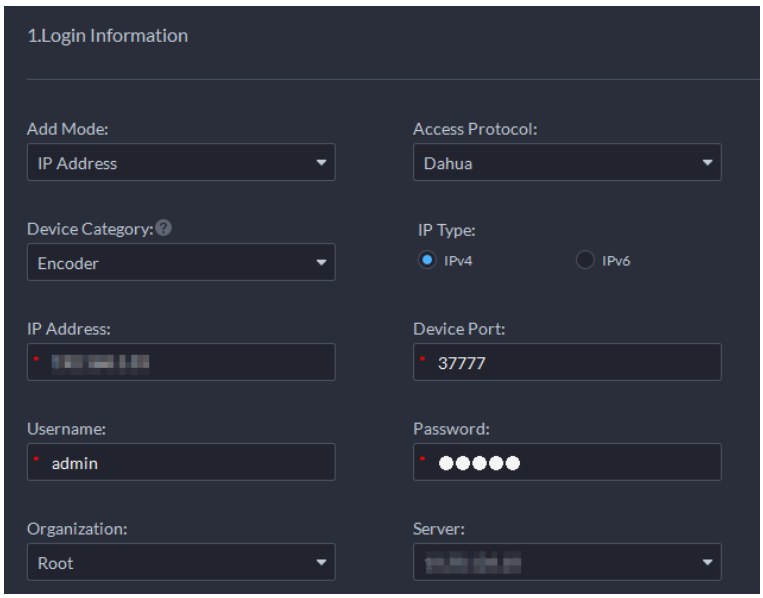
- **IP segment**: Add multiple devices in the same segment. We recommend selecting this option when the login username and password of the multiple devices in the same segment are the same.
- **Domain Name**: We recommend selecting this option when the IP address of the device changes frequently and 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, open the configuration tool to change the port number of DSS_ARS service.

Sleep function is supported for IPCs that use 4G mobile network to communicate and are solar-powered only when they are added to the platform through automatic registration.

- **P2P**: Add devices under the a P2P account to the platform. The platform must be able to access the P2P server. 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 3-7 Add an encoder



Step 5 Enter the information.

Step 6 Click **OK**.

- To add more devices, click **Continue to add**.
- To go to the web manager of a device, click .

3.2.2.4.2 Adding Devices through Searching

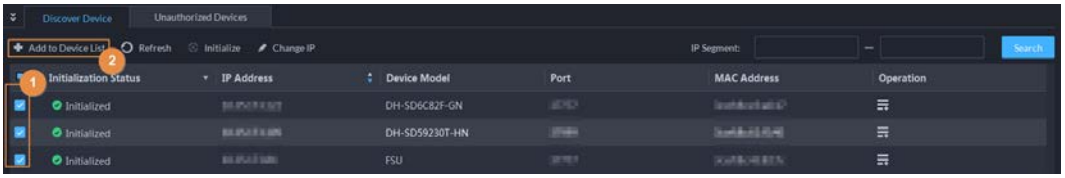
Devices on the same network with the platform server can be added using the automatic search function.

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

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

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

Figure 3-8 Add in batches



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

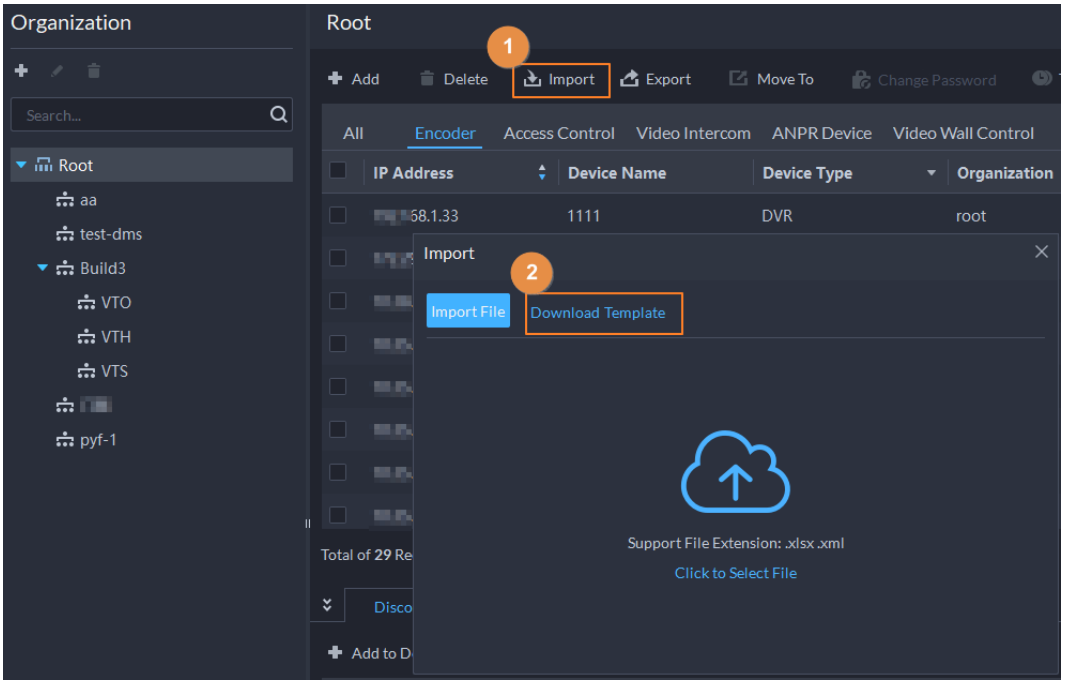
3.2.2.4.3 Importing Devices

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

Prerequisites

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

Figure 3-9 Download template



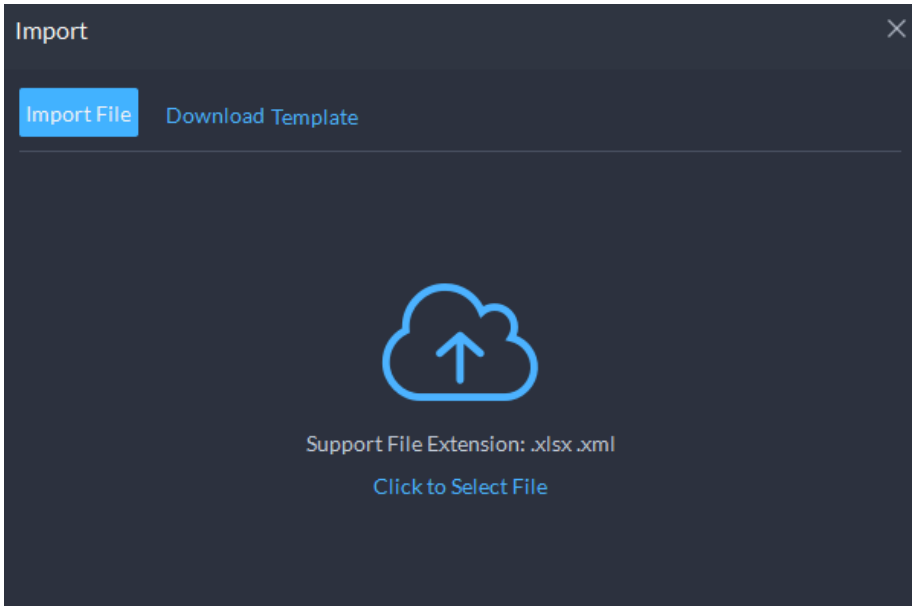
Procedure

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

Step 2 Click .

Step 3 Click **Import**.

Figure 3-10 Import devices



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

Step 5 Click **OK**.

3.2.2.5 Editing Devices

Edit the information of devices.

3.2.2.5.1 Changing IP Address

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

Step 2 Click **Device Config**.

Step 3 Click of a device.

Step 4 Edit the IP address, and then click **OK**.

3.2.2.5.2 Modifying Device Information

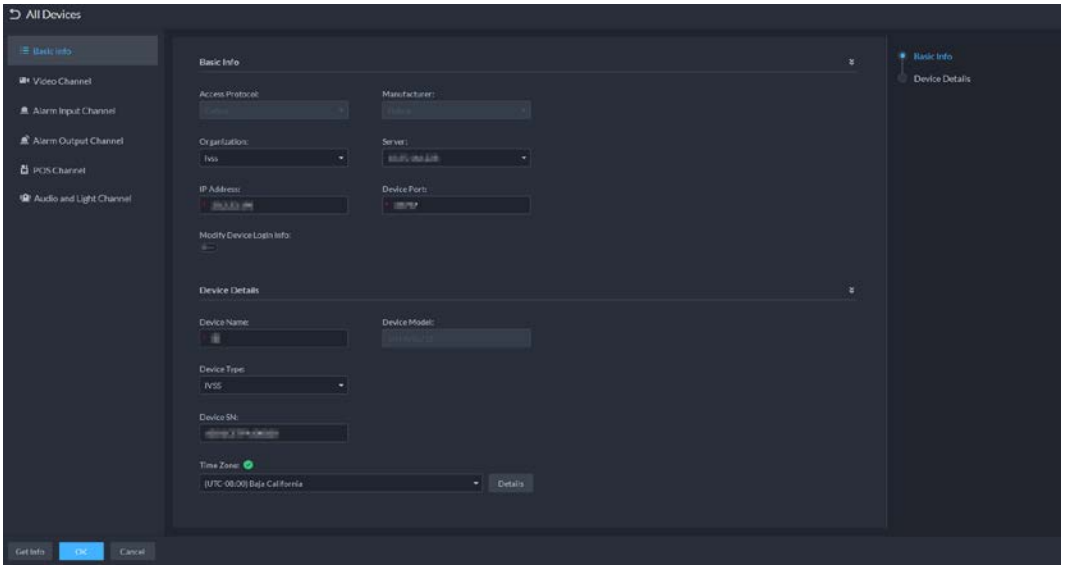
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

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 3-11 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 number, names, and alarm types of the alarm input channels.

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 number and names of alarm output channels.

Step 7 Click the **POS Channel**, and then edit the number and names of the POS channels.

This tab will only appear if the device has POS channels.

Step 8 Click the **Audio and Light Channel** tab, and then edit the number and names of the audio and light channels.

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

Step 9 Click **OK**.

3.2.2.5.3 Modifying Device Organization

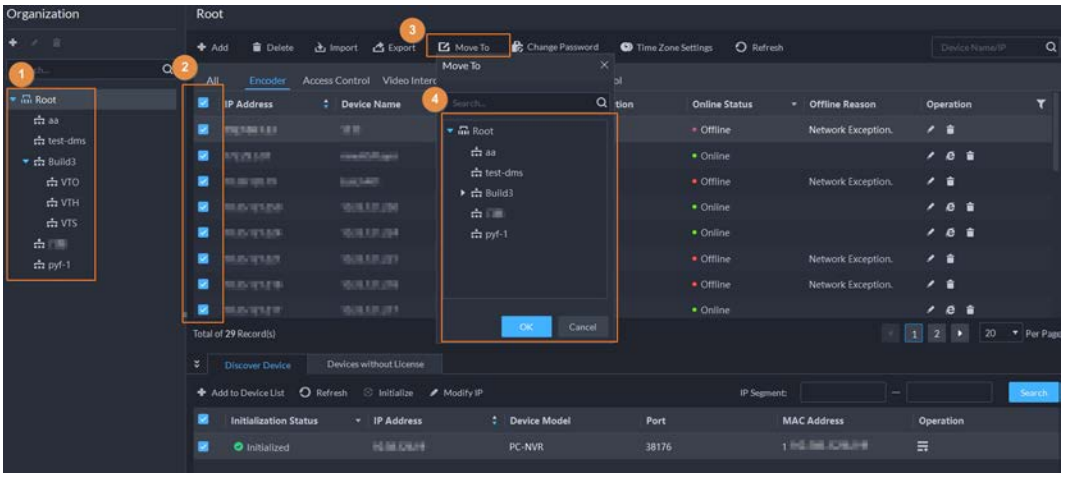
You can move a device from an organization node to another one.

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 3-12 Move a device



3.2.2.5.4 Changing Device Password

You can change device usernames and passwords in batches.

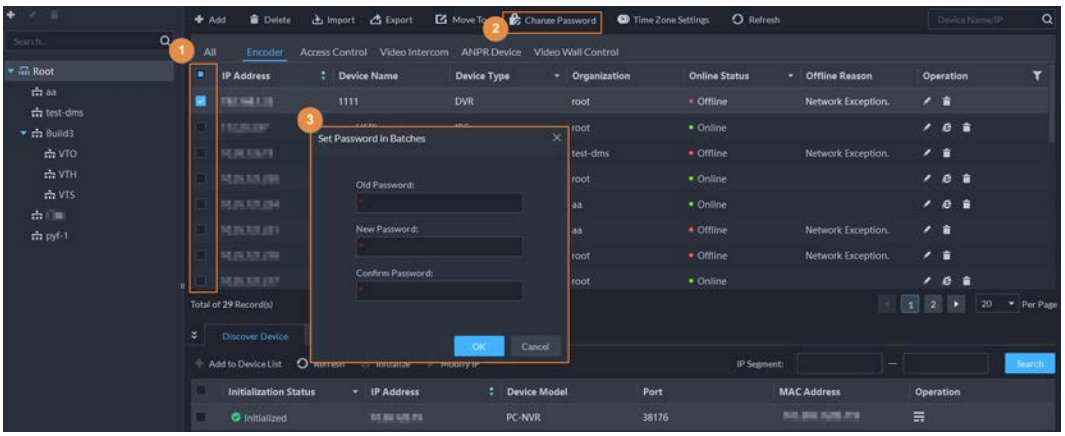
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **Device**.

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 3-13 Change device password



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

3.2.2.6 Modifying Device Time Zone

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

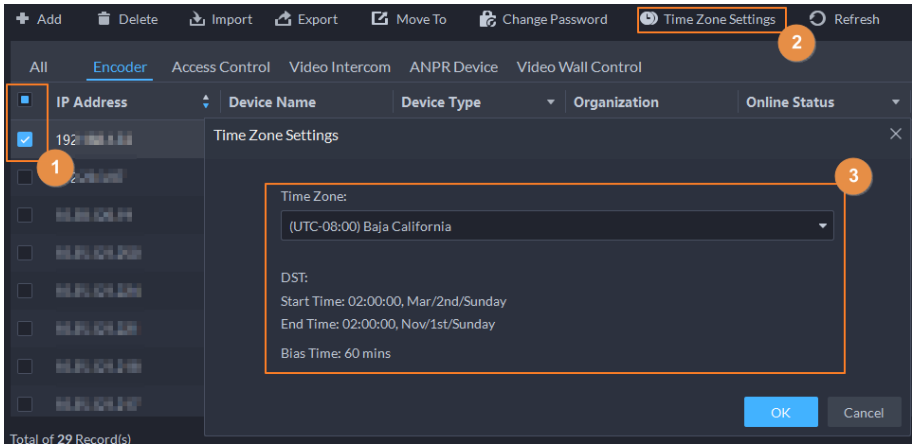
If a device is accessed through ONVIF and the ONVIF version is earlier than 18.12, the device DST cannot be edited on the platform. You can only edit manually.

Step 1 Log in to the DSS Client. On the **Home** 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 3-14 Modify device time zone



Step 4 Select a time zone.

Step 5 Click **OK**.

3.2.2.7 Exporting Devices

You can export the information (except username and password for login) of all the devices on the DSS client. When you need to switch or configure a new platform, you can quickly add them all by importing them, but you need to enter the username and password for login again.

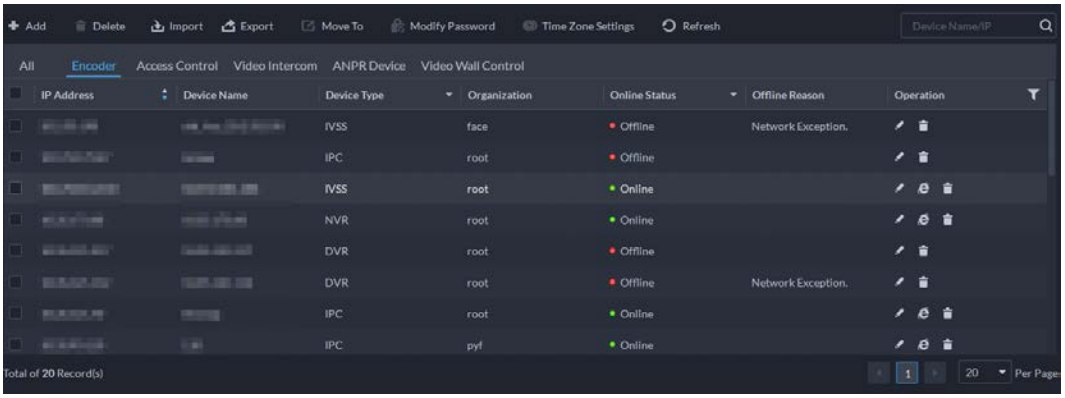
You can export up to 100,000 devices at a time.

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 3-15 Select a device type



Step 4 Click **Export**.

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

You can configure whether to verify the password. For details, see "7.3.1 Configuring Security Parameters".

- The encryption password is used to protect the export file. It consists of 6 uppercase or lower case letters, numbers, or their combination. You need to enter it when using the export file.
- You can select **All** to export all the devices, or **Selected** to export the devices you selected.

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

3.2.3 Binding Resources

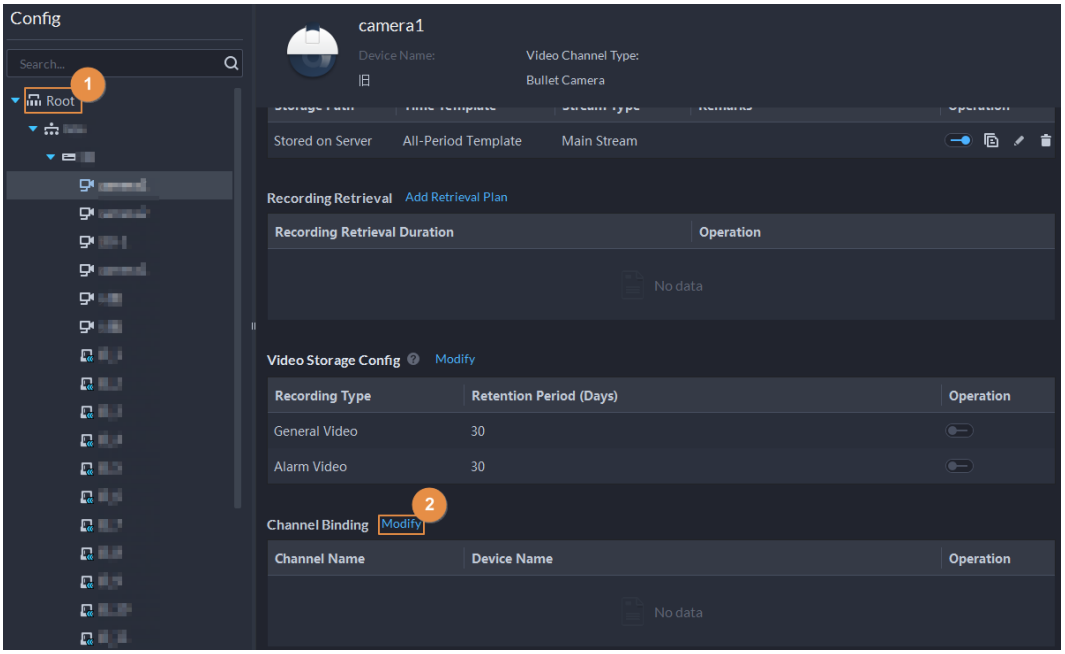
The platform supports binding resources for linked actions. You can link a video channel with an alarm input channel, ANPR channel, POS channel, access control channel, lift control channel or another video channel, so that you can view the associated video for alarm, face and other businesses.

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**.

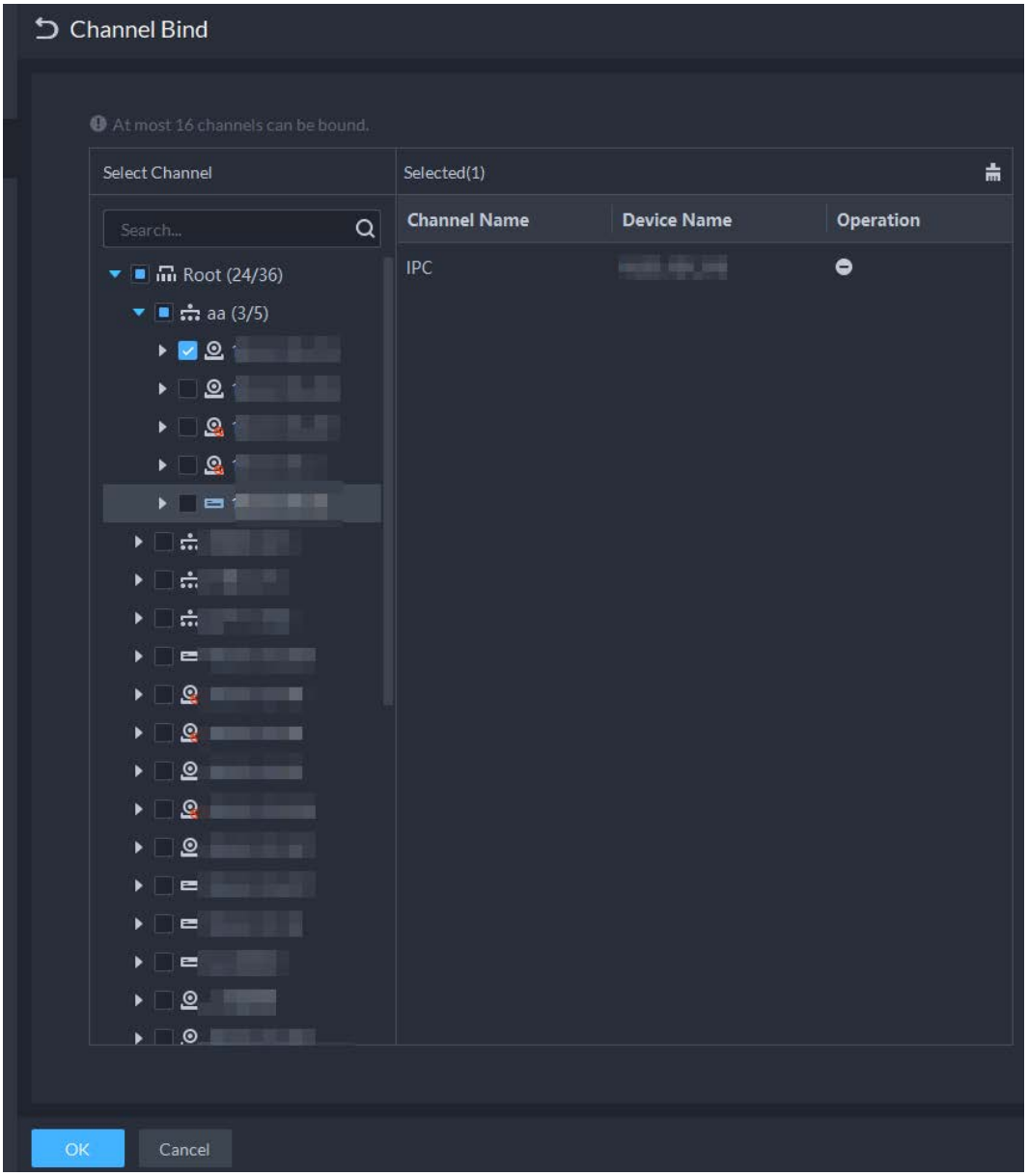
Figure 3-16 Bind channel



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

Multiple channels can be selected.

Figure 3-17 Select the channels you want to bind to the camera



Step 5 Click **OK**.

3.2.4 Adding Recording Plan

Configure recording plans for video channels so that they can record videos accordingly.
You can configure 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 continuously record videos when motion is detected.

3.2.4.1 Adding Recording Plan One by One

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

motion detection videos within the defined period.

Procedure

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

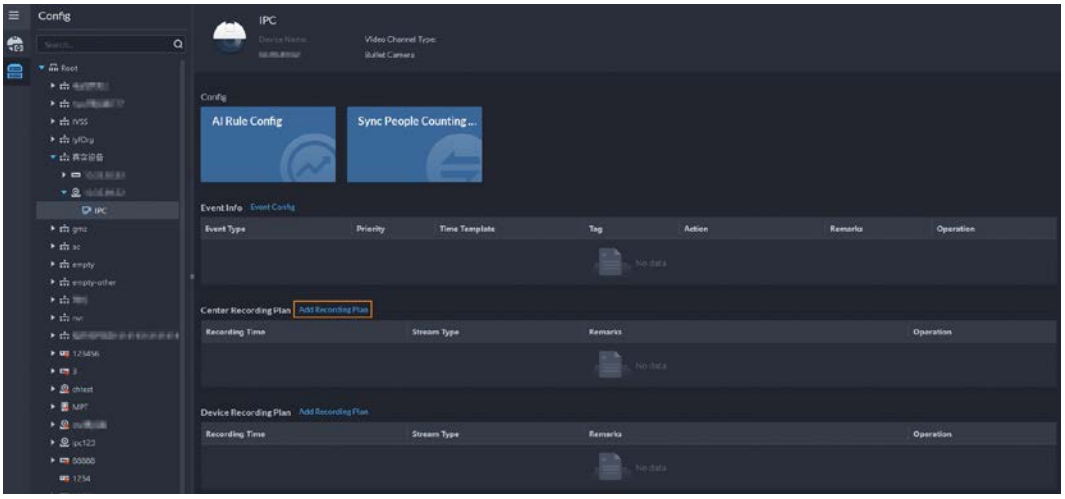
Step 2 Click .

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

- Configure a center recording plan.

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

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



2) Configure the parameters, and then click **OK**.

Table 3-1 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the server by default. It cannot be changed.
Recording Type	• General recording: The device will continuously record videos within the defined periods. • Motion detection recording: The device will continuously record videos within the defined periods on motion detections.
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 "3.2.6 Adding Time Template".

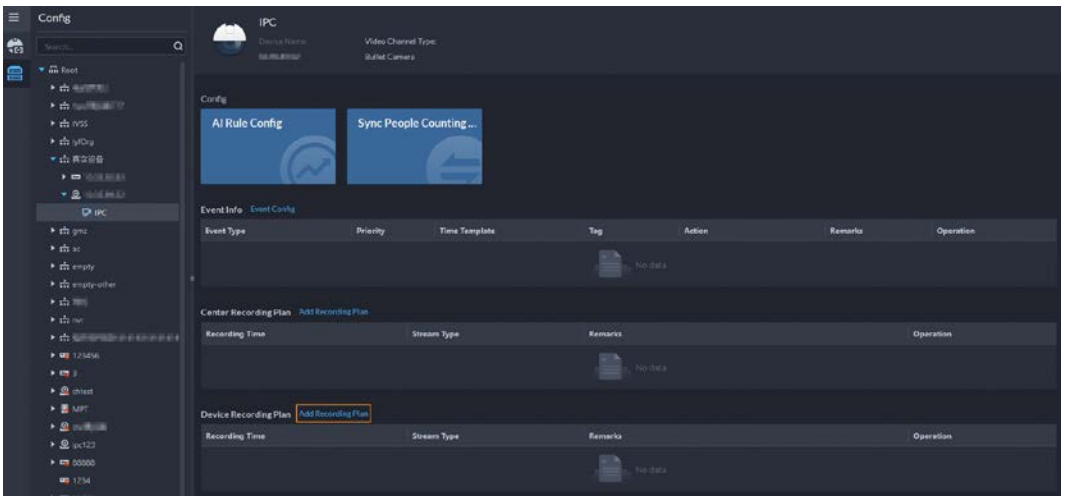
3) Click **OK**.

- Configure a device recording plan.

The platform can obtain and display the recording plan that has been configured on EVS of the latest versions. You can check if recording plan are obtained and displayed on the page to know if your EVS is of the latest version.

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

Figure 3-19 Add a device recording plan (1)



2) Configure the parameters, and then click **OK**.

Table 3-2 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the device by default. It cannot be changed.
Stream Type	The device will make recordings using the main stream by default. It cannot be changed.
Remarks	Customizable description for the recording plan.
Recording Time	Select a default time template or click **Create Time Template** to add a new time template. See "3.2.6 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.

3.2.4.2 Adding Center Recording Plans in Batches

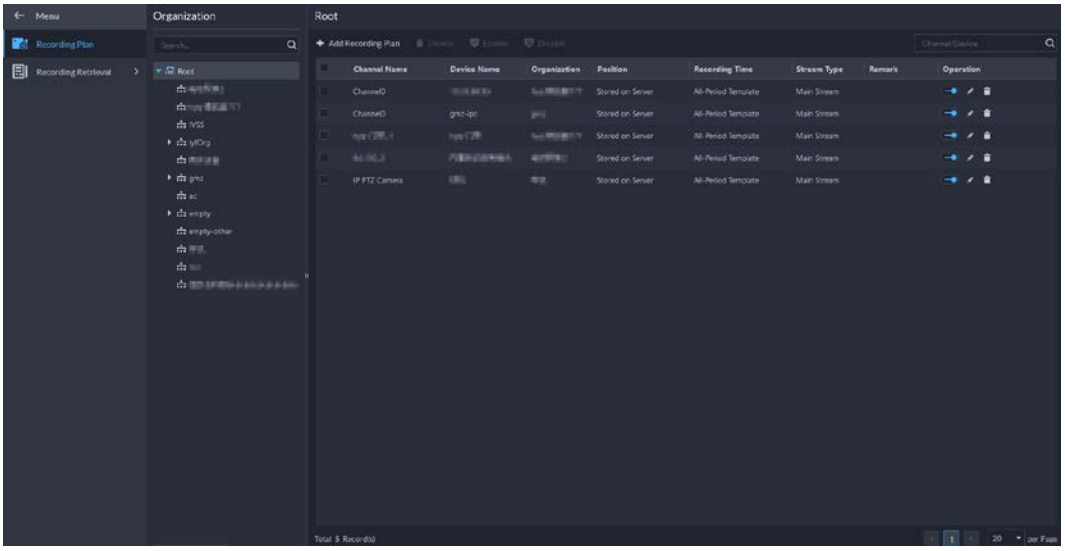
Add a center recording plan of general or motion detection videos for multiple channels at the same

time.

3.2.4.2.1 General Recording Plan

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

Figure 3-20 Center recording plan



Step 2 Select **General Recording Plan** > **Add General Recording Plan**.

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

Table 3-3 Parameter description

Parameter	Description
Enable	Turn on or off the recording plan.
Position	Videos will be stored on the server by default. It cannot be changed.
Stream Type	Select **Main Stream**, **Sub Stream 1** or **Sub Stream 2**. 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 "3.2.6 Adding Time Template".
Recording Channel	Select the channels you want to add the recording plan for.

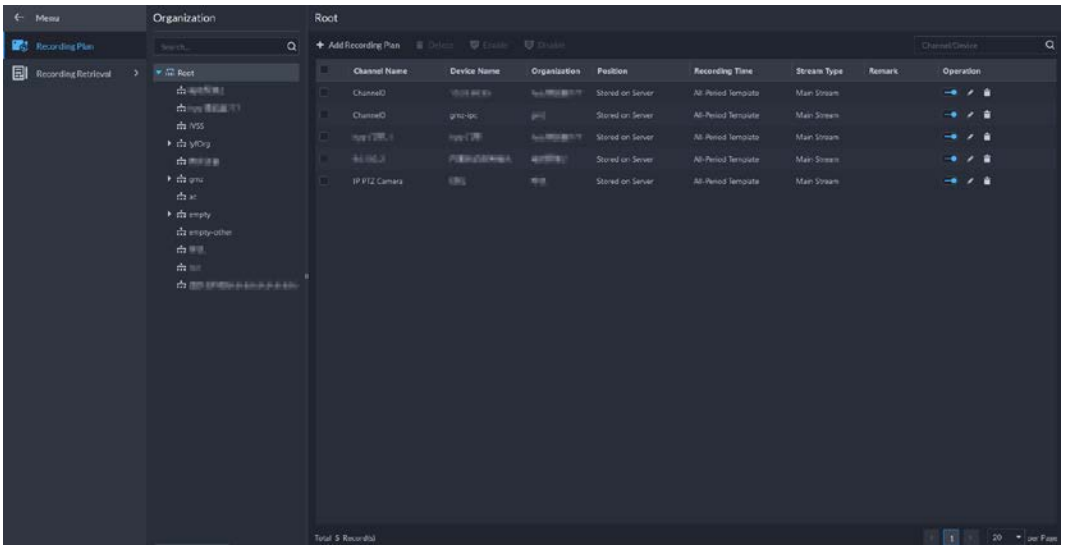
Related Operations

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

3.2.4.2.2 Motion Detection Recording Plan

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

Figure 3-21 Center recording plan



Step 2 Select **Motion Detection Recording Plan** > **Add Motion Detection Recording Plan**.

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

Table 3-4 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.
Recording Type	• General recording: The device will continuously record videos within the defined periods. • Motion detection recording: The device will continuously record videos within the defined periods on motion detections.
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 "3.2.6 Adding Time Template".
Recording Channel	Select the channels you want to add the recording plan for.

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

- Delete: Select multiple channels, and then delete them at the same time.
- Enable and Disable: Select multiple channels, and then enable or disable them at the same time.

3.2.5 Adding Video Retrieval Plan

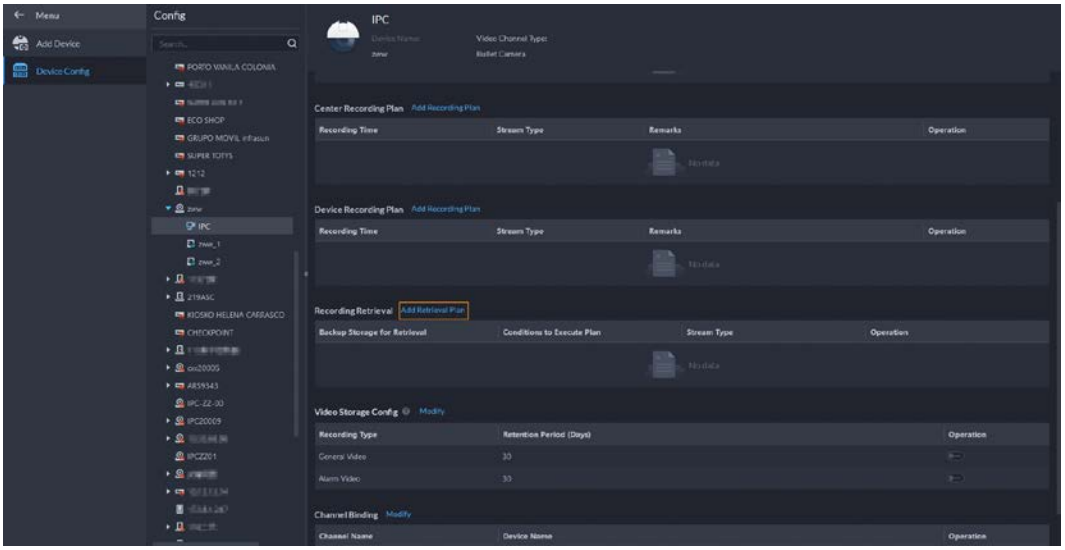
Configure a video retrieval plan to upload the videos that devices record when they are disconnected from the platform. During the defined period, videos will be automatically uploaded to the platform. The platform supports uploading videos within the past 7 days.
You can add a retrieval plan for each channel one by one, or add one for multiple channels in batches.

3.2.5.1 Adding Retrieval Plan One by One

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

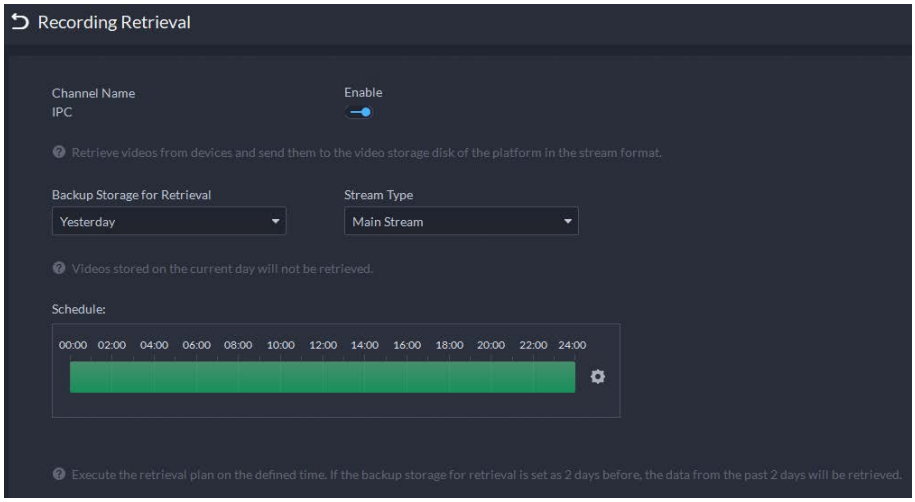
Step 2 Click .

Figure 3-22 Add a retrieval plan for a channel



Step 3 Select a device and then click **Add Retrieval Plan**.

Figure 3-23 Add a retrieval plan



Step 4 Configure the parameters.

Table 3-5 Parameter description

Parameter	Description
Enable	Turn on or off the retrieval plan.
Backup Storage for Retrieval	Select a period, and then the videos within the defined period will be uploaded. The platform supports uploading videos from devices within the past 7 days at most. Videos from the current day will not be included.
Stream Type	Select the stream type of the videos that you want up upload. If the videos are recorded on sub stream 1 and **Main Stream** is configured in this retrieval plan, uploading will fail.
Schedule	Configure when to upload videos every day. Click to configure specific periods. You can configure up to 6 periods.

Step 5 Click **OK**.

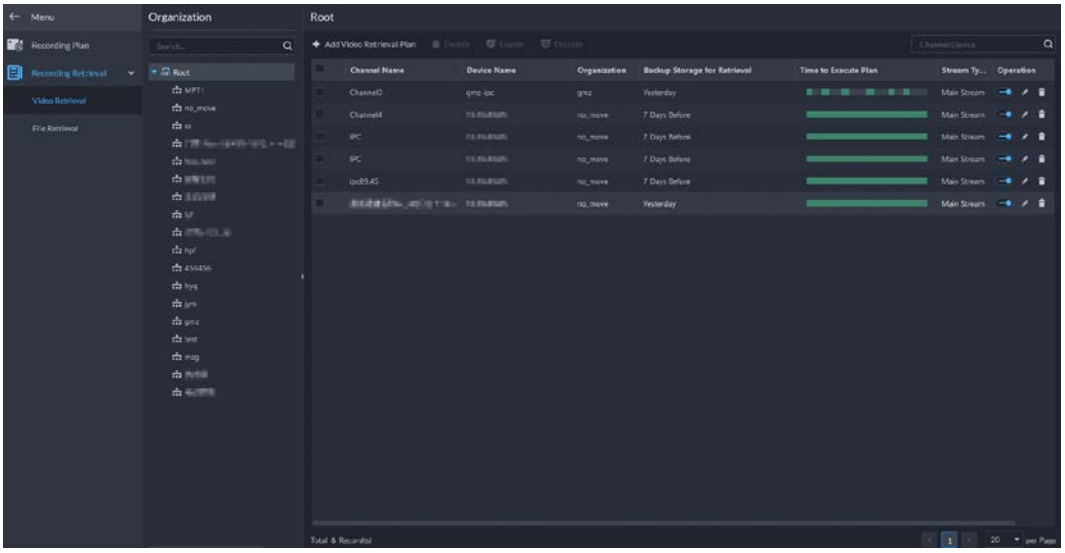
Related Operations

- Enable/disable retrieval plan
  means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.
- Edit retrieval plan
  Click of corresponding plan to edit the plan.
- Click to delete recording plans one by one.

3.2.5.2 Adding Retrieval Plans in Batches

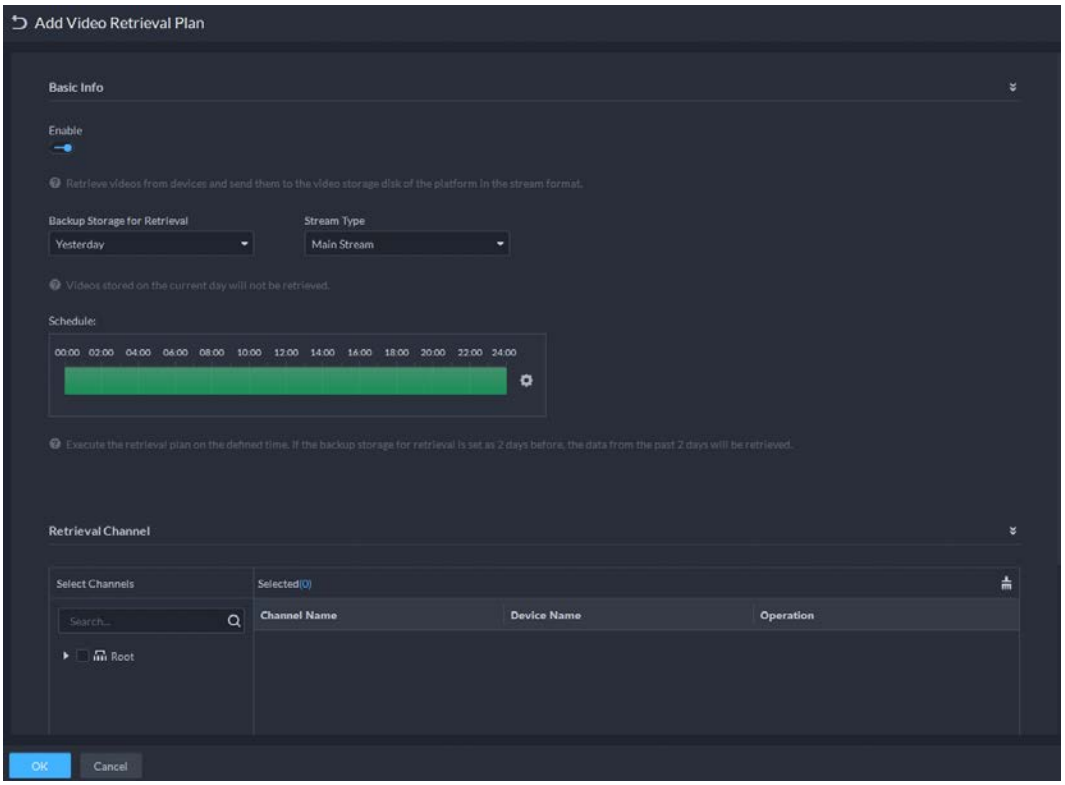
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Storage Plan** > **Recording Retrieval** > **Video Retrieval**.

Figure 3-24 Video retrieval



Step 2 Click **Add Video Retrieval Plan**.

Figure 3-25 Configure a video retrieval plan



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

Table 3-6 Parameter description

Parameter	Description
Enable	Turn on or off the retrieval plan.
Backup Storage for Retrieval	Select a period, and then the videos within the defined period will be uploaded. The platform supports uploading videos from devices within the past 7 days at most. Videos from the current day will not be included.

Parameter	Description
Stream Type	Select the stream type of the videos that you want up upload. If the videos are recorded on sub stream 1 and **Main Stream** is configured in this retrieval plan, uploading will fail.
Schedule	Configure when to upload videos every day. Click to configure specific periods. You can configure up to 6 periods.

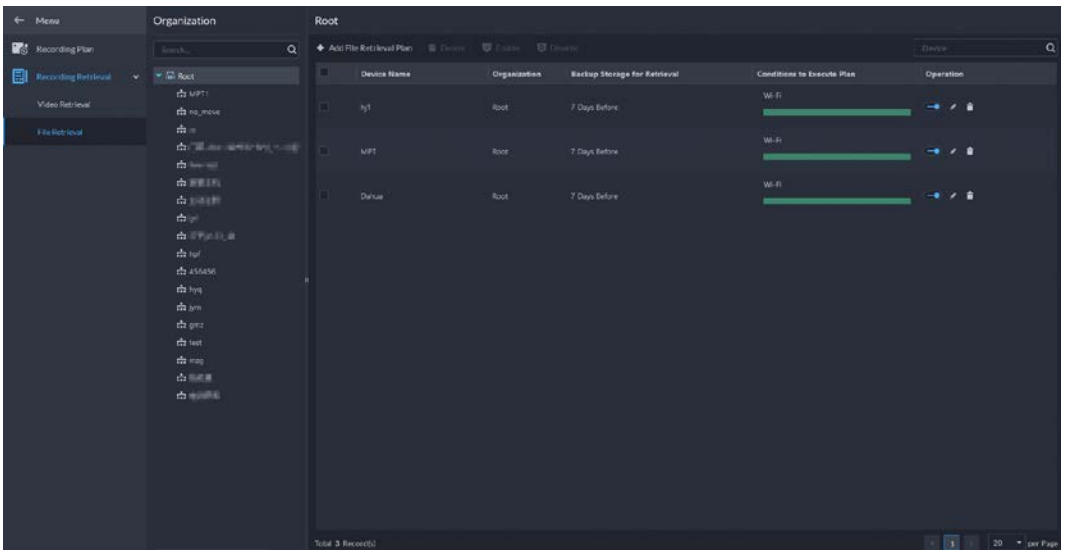
Step 4 Click **OK**.

- Enable/disable retrieval plan
  means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.
- Edit retrieval plan
  Click of corresponding plan to edit the plan.
- Click to delete recording plans one by one.
- Delete: Select multiple plans and delete them in batches.
- Enable and Disable: Select multiple plans and enable or disable them in batches.

3.2.5.3 Adding Retrieval Plan for MPT Devices

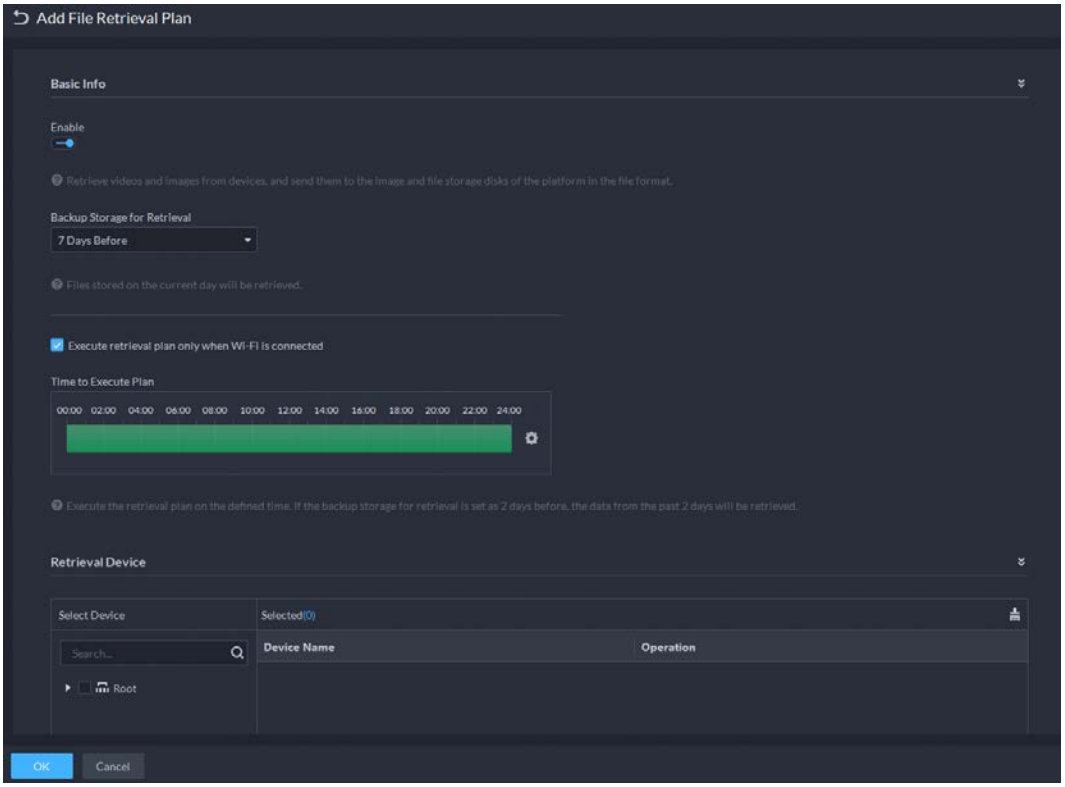
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Storage Plan** > **Recording Retrieval** > **File Retrieval**.

Figure 3-26 File retrieval



Step 2 Click **Add File Retrieval Plan**.

Figure 3-27 Configure a file retrieval plan



Step 3 Configure the parameters, and then select MPT devices in the **Retrieval Device** section.

Table 3-7 Parameter description

Parameter	Description
Enable	Turn on or off the retrieval plan.
Backup Storage for Retrieval	Select a period, and then the videos within the defined period will be uploaded. The platform supports uploading videos from devices within the past 7 days at most. Videos from the current day will also be uploaded.
Execute retrieval plan only when Wi-Fi is connected	When selected, videos on MPT devices will be uploaded only when they are connected to a Wi-Fi network. If it is not selected and MPT devices are connected to the mobile network, uploading videos might result in additional charges.
Time to Execute Plan	Configure when to upload videos every day. Click to configure specific periods. You can configure up to 6 periods.

Step 4 Click **OK**.

Related Operations

- Enable/disable retrieval plan
  means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.
- Edit retrieval plan
  Click of corresponding plan to edit the plan.
- Click to delete recording plans one by one.

- Delete: Select multiple plans and delete them in batches.
- Enable and Disable: Select multiple plans and enable or disable them in batches.

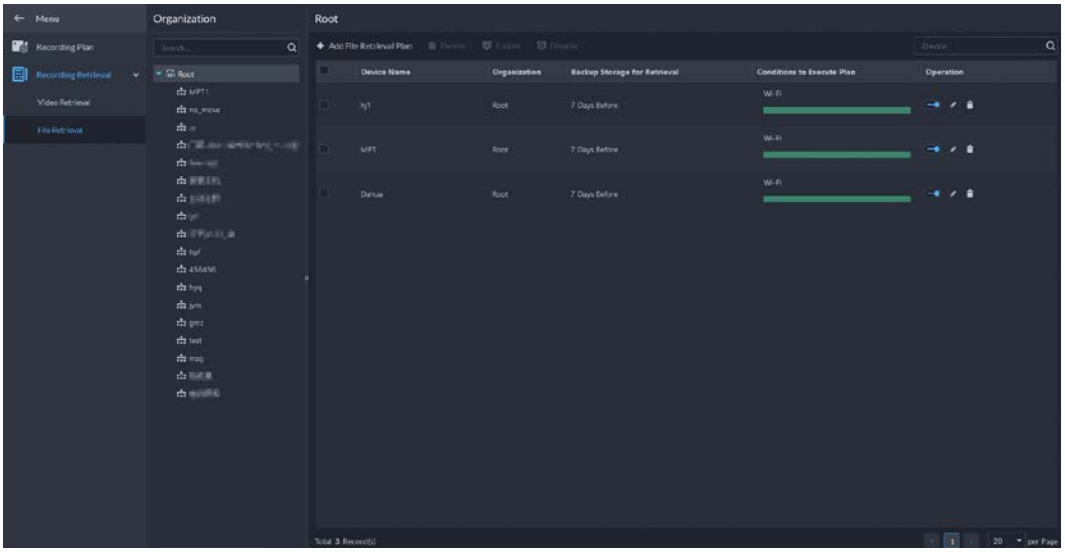
3.2.5.3.1 Adding Retrieval Plans One by One

The procedures are the same as other devices. For details, see "3.2.5.1 Adding Retrieval Plan One by One".

3.2.5.3.2 Adding Retrieval Plans in Batches

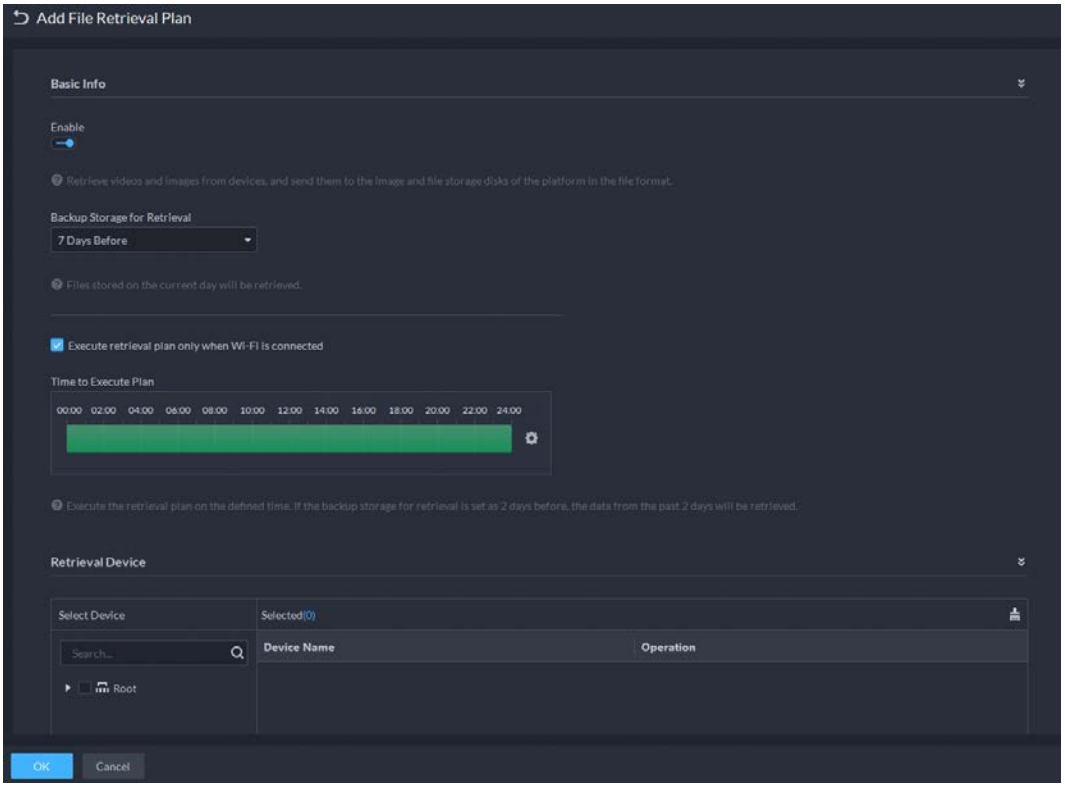
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Storage Plan** > **Recording Retrieval** > **File Retrieval**.

Figure 3-28 File retrieval



Step 2 Click **Add File Retrieval Plan**.

Figure 3-29 Configure a file retrieval plan



Step 3 Configure the parameters, and then select MPT devices in the **Retrieval Device** section.

Table 3-8 Parameter description

Parameter	Description
Enable	Turn on or off the retrieval plan.
Backup Storage for Retrieval	Select a period, and then the videos within the defined period will be uploaded. The platform supports uploading videos from devices within the past 7 days at most. Videos from the current day will also be uploaded.
Execute retrieval plan only when Wi-Fi is connected	When selected, videos on MPT devices will be uploaded only when they are connected to a Wi-Fi network. If it is not selected and MPT devices are connected to the mobile network, uploading videos might result in additional charges.
Time to Execute Plan	Configure when to upload videos every day. Click to configure specific periods. You can configure up to 6 periods.

Step 4 Click **OK**.

Related Operations

- Enable/disable retrieval plan
  means that the plan has been enabled. Click the icon and it becomes , and it means that the plan has been disabled.
- Edit retrieval plan
  Click of corresponding plan to edit the plan.
- Click to delete recording plans one by one.

- Delete: Select multiple plans and delete them in batches.
- Enable and Disable: Select multiple plans and enable or disable them in batches.

3.2.6 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**.

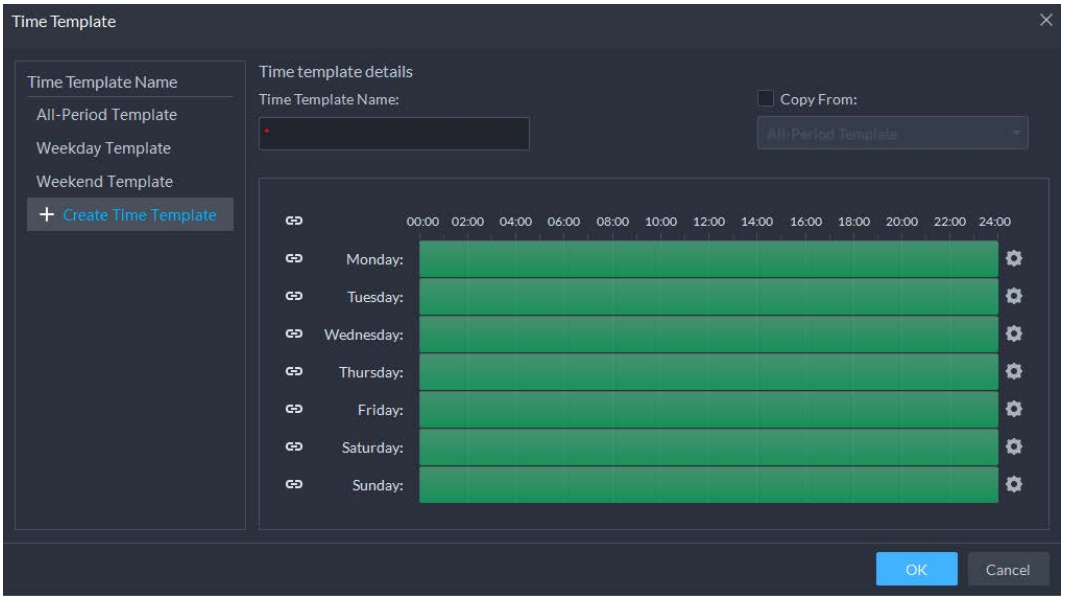
Step 2 Click .

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 3-30 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**.

3.2.7 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.

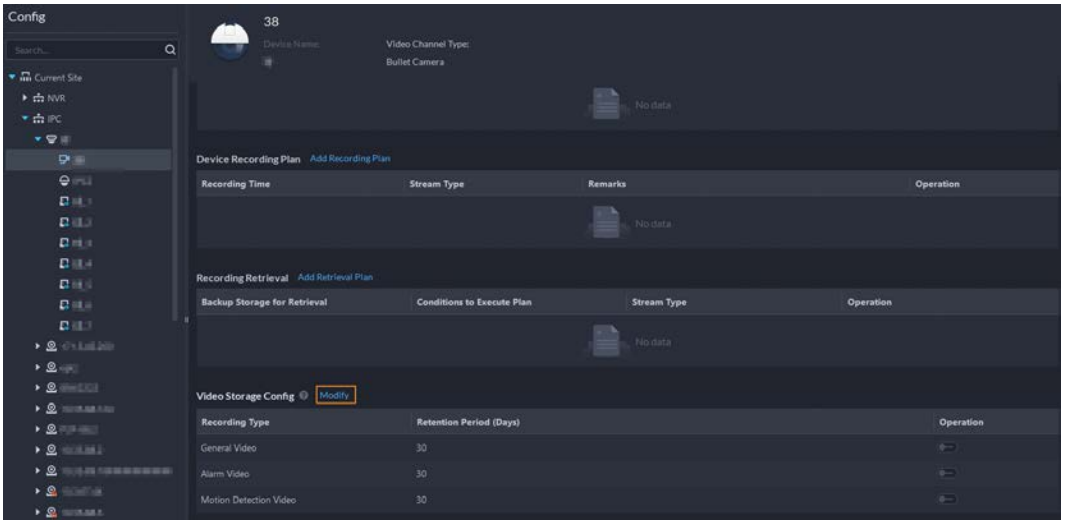
Procedure

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 3-31 Go to recording storage configuration page



Step 4 Click  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,  means that the recoding storage configuration has been enabled. Click the icon and it becomes  , meaning that the configuration has been disabled.

3.2.8 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  , and then in the **Basic Config** section, select **Device**.

Step 2 Click 

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

Events that can be configured are different for different types of devices. If you select **Device**, you can only configure general events. If you select **Channels**, various events supported by different types of channels will be displayed.

Figure 3-32 Go to the event configuration (device)

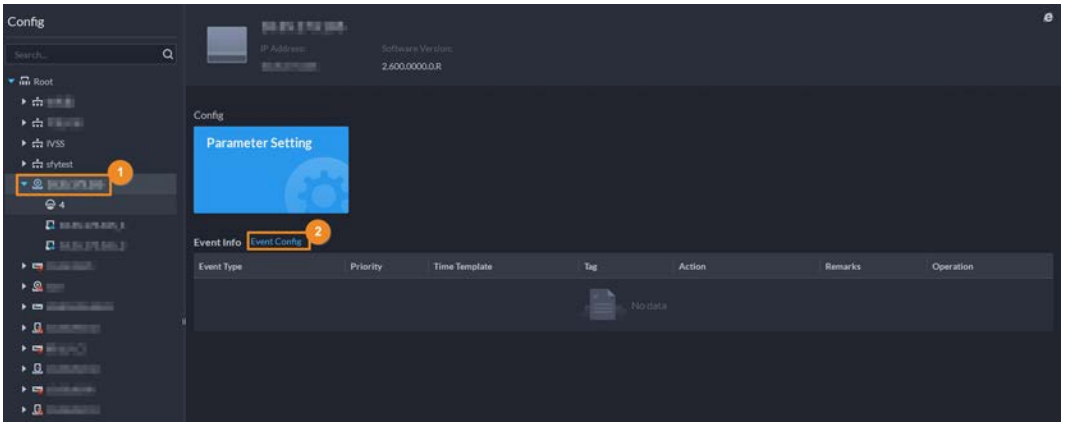
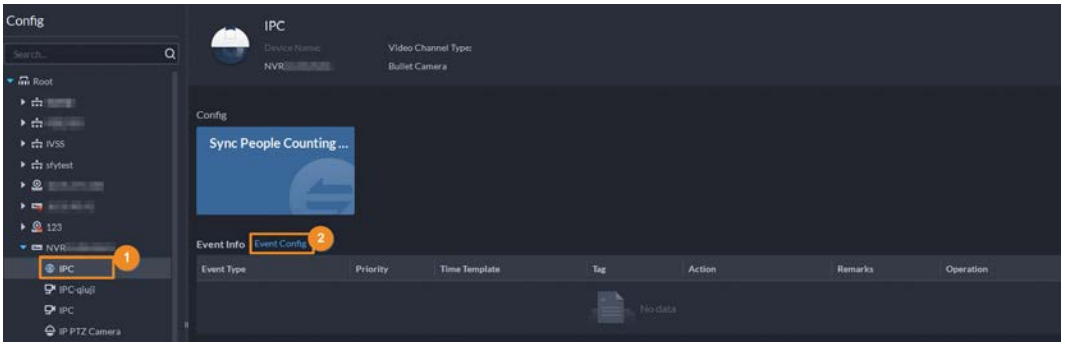


Figure 3-33 Go to the event configuration (channel)



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

3.2.9 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.

3.2.9.1 Configuring Camera Properties

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

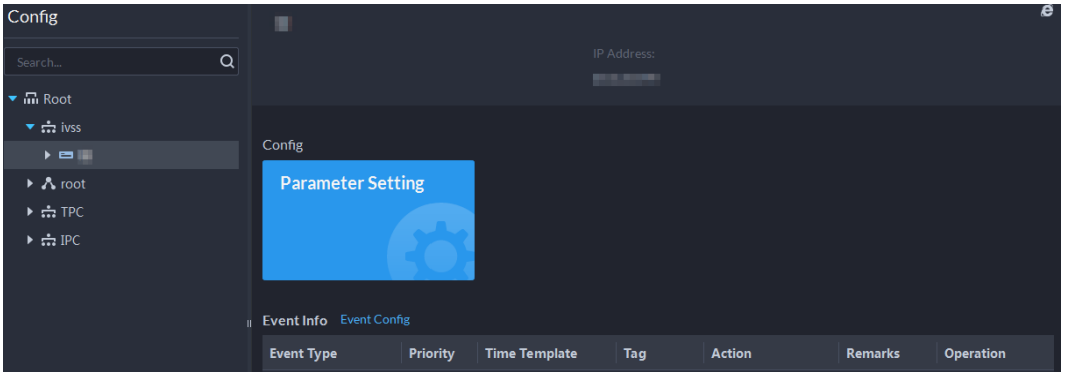
3.2.9.1.1 Configuring Property Files

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 .

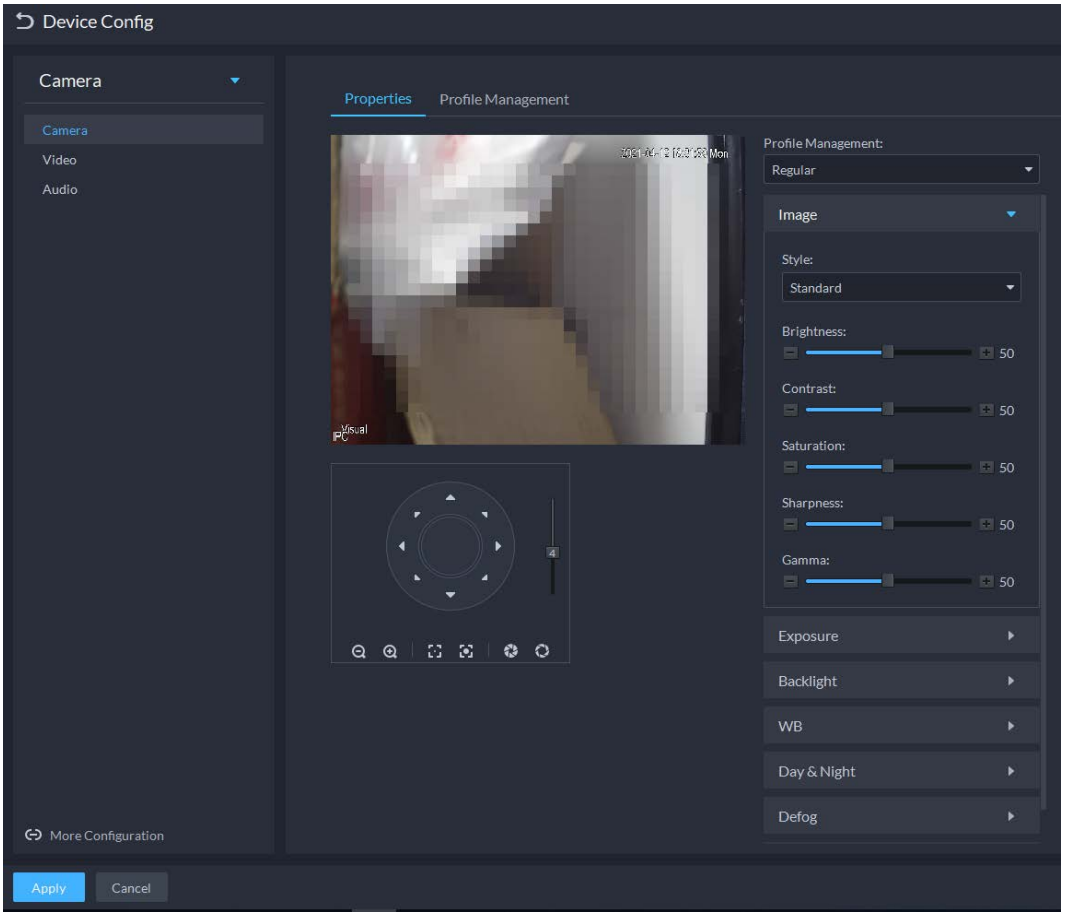
Step 3 Select a device, and then click **Parameter Setting**.

Figure 3-34 Device configuration



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

Figure 3-35 Image



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

Table 3-9 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 3-10 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 3-36 Exposure

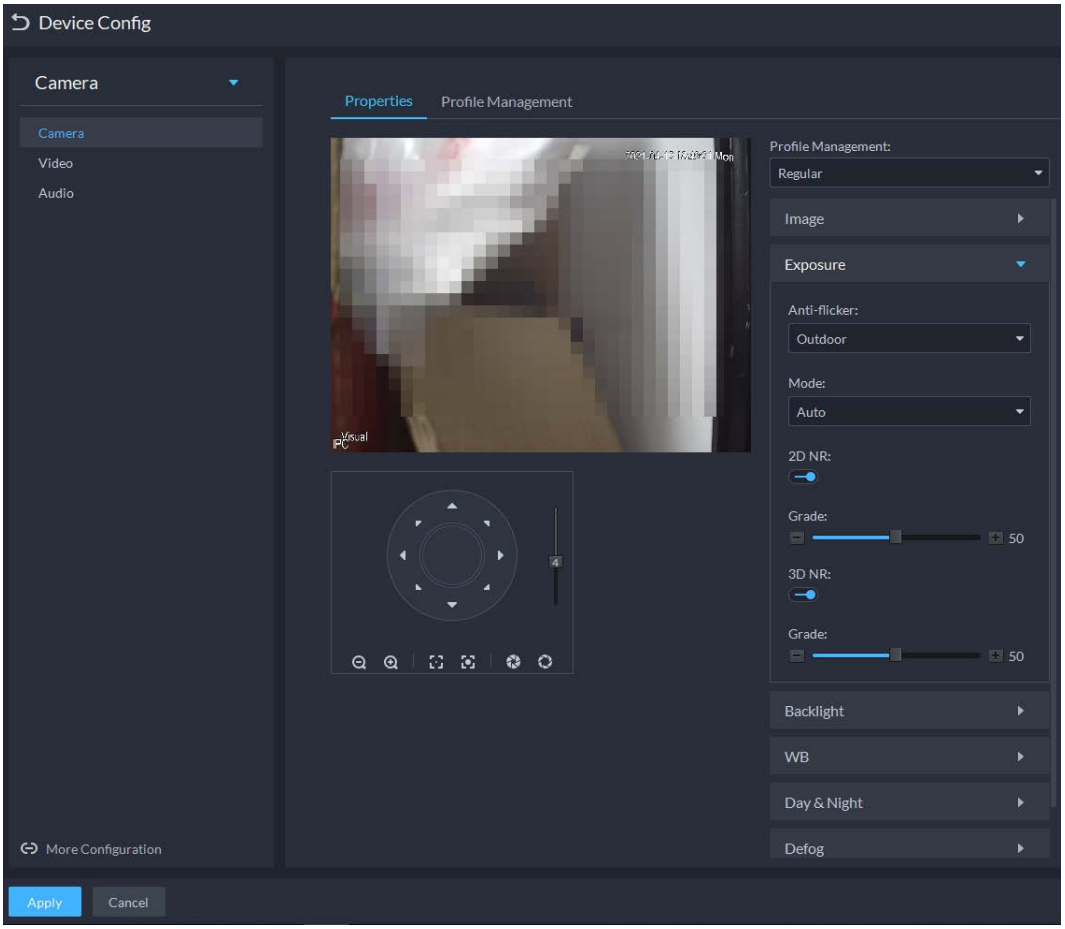


Table 3-11 Exposure parameters

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.
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.

Parameter	Description
	• **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 3-37 Backlight

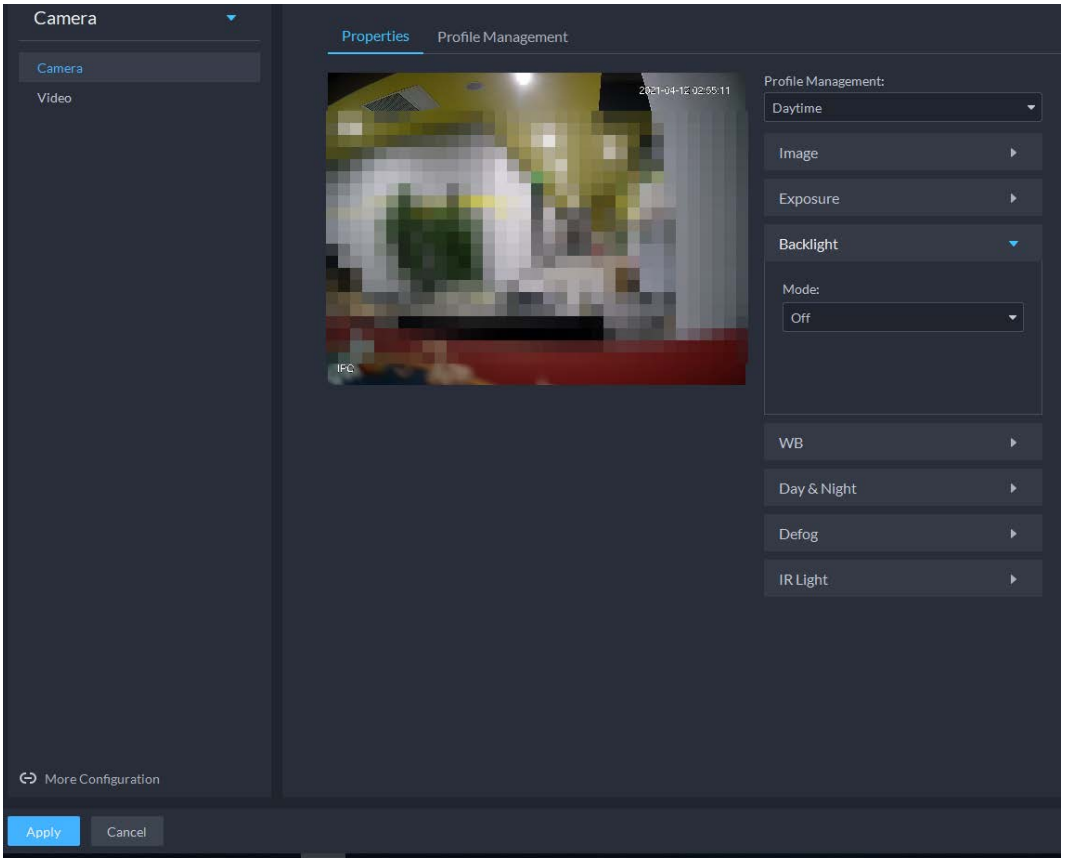


Table 3-12 Backlight parameters

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

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

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

Figure 3-38 WB

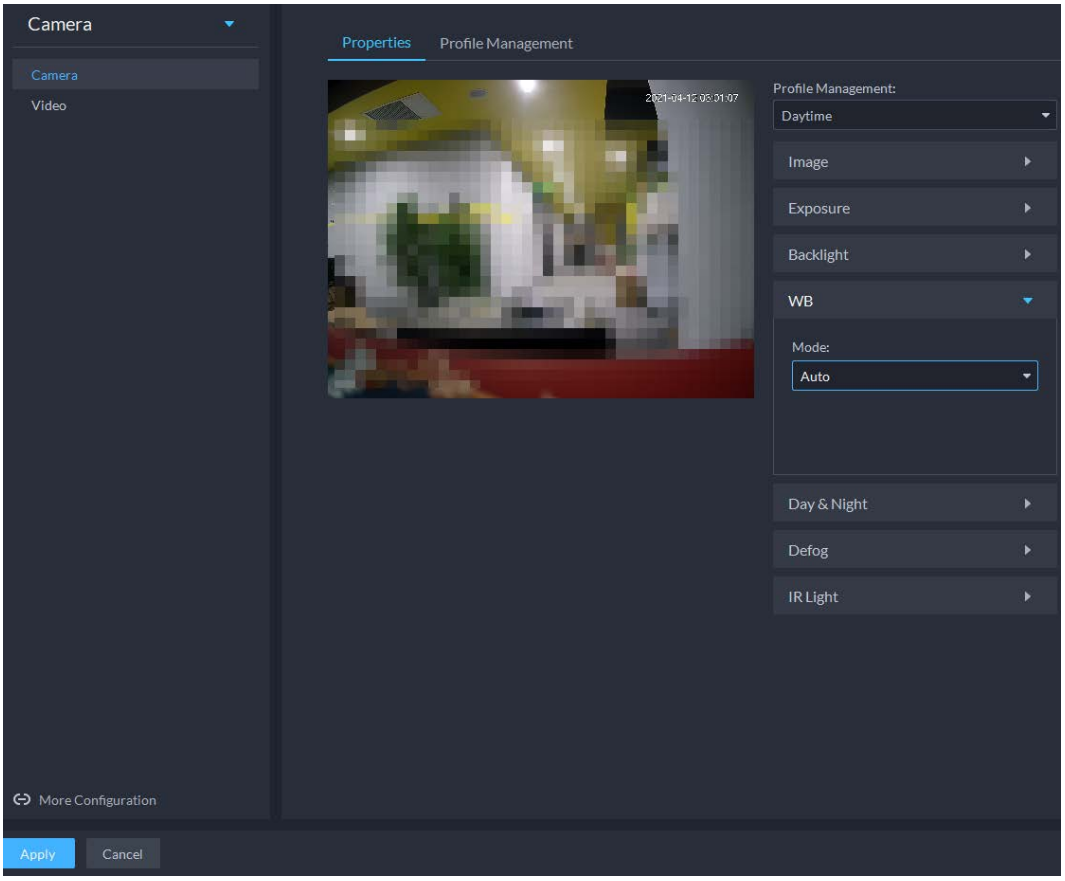


Table 3-13 WB parameters

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

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

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

Figure 3-39 Day & night

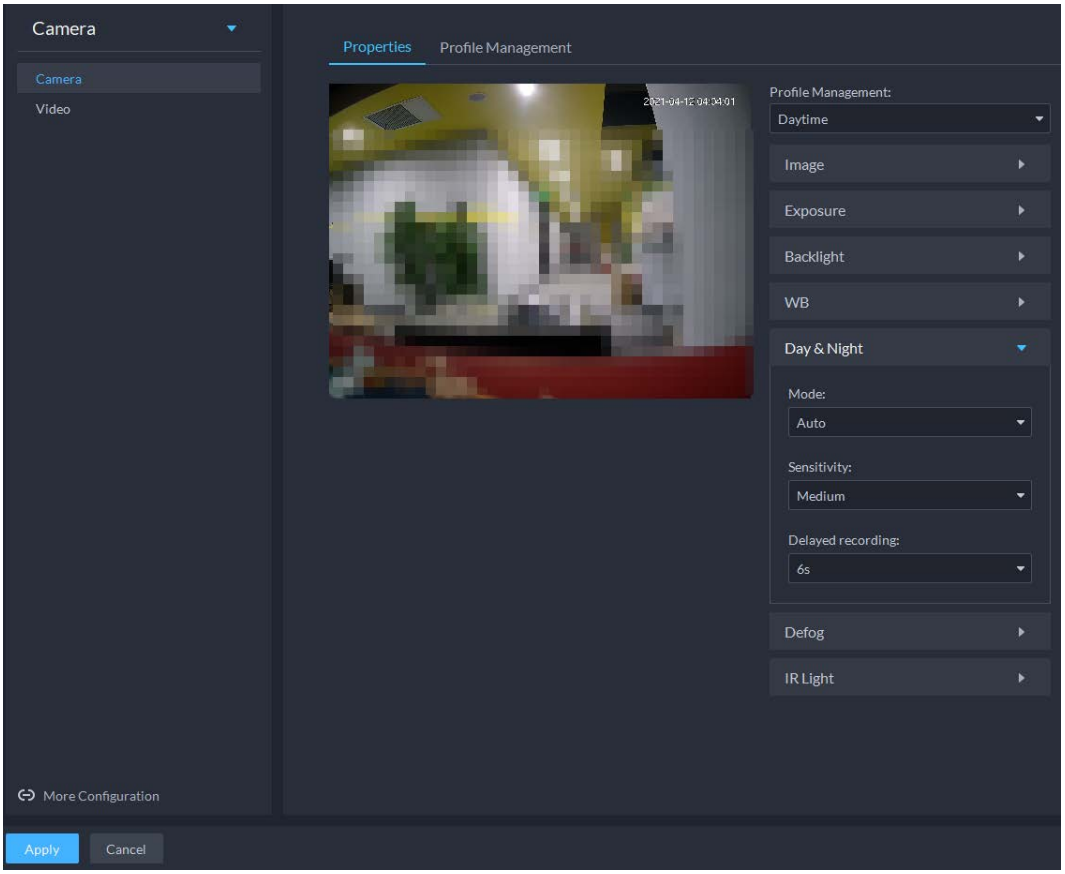


Table 3-14 Day & night parameters

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 3-40. For details of the parameters, see Table 3-15.

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

Figure 3-40 Defog

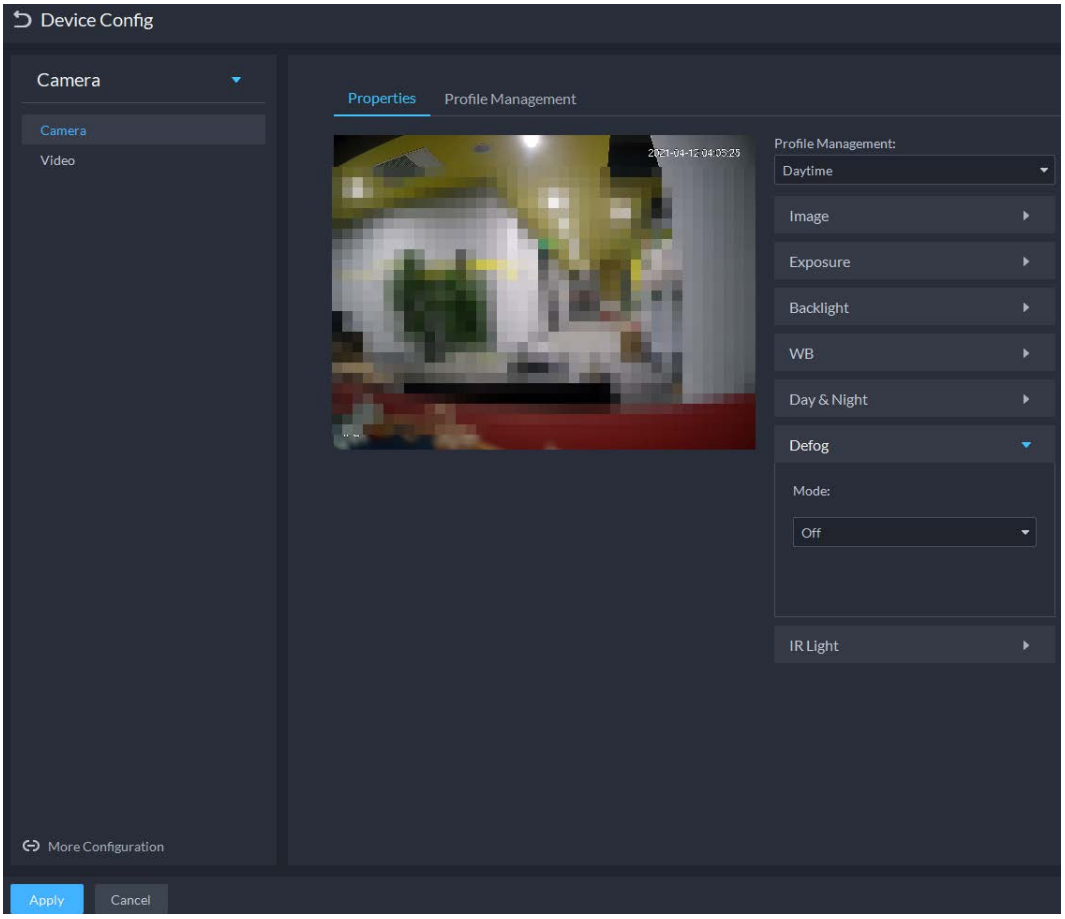


Table 3-15 Defog parameters

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

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

Figure 3-41 IR light

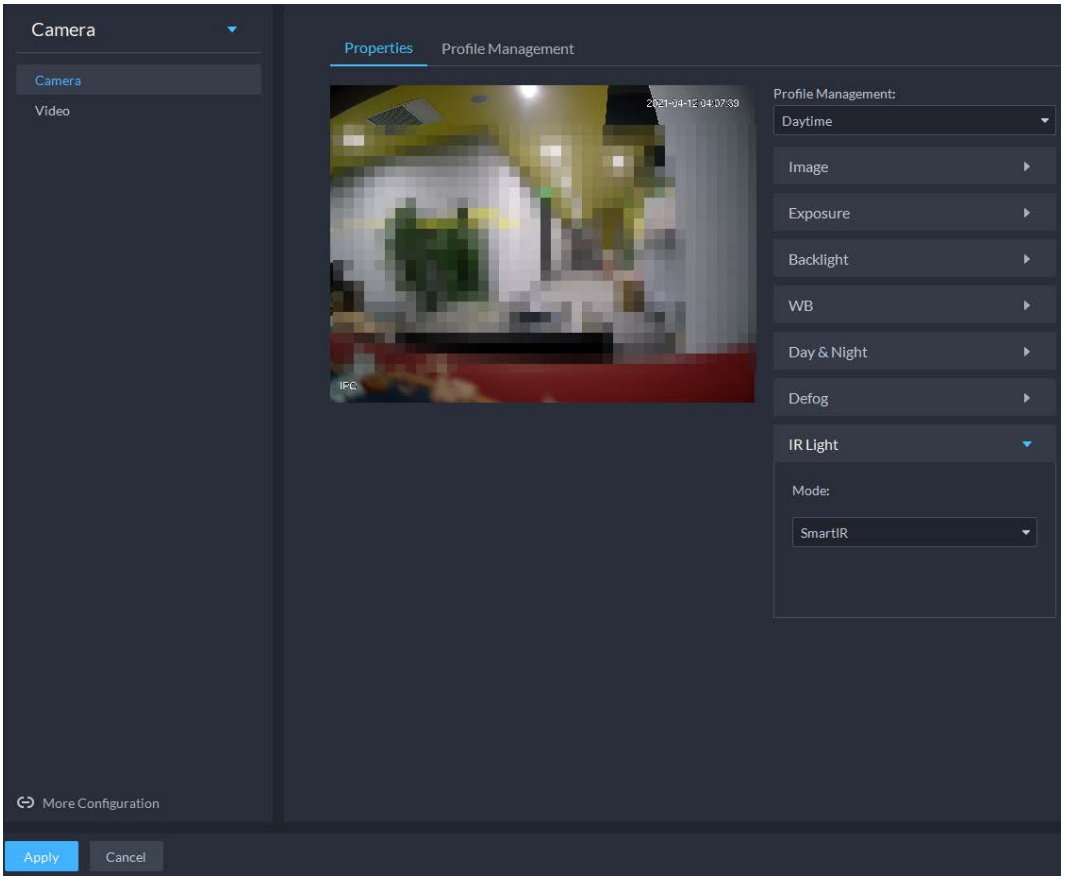


Table 3-16 IR light parameters

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.

3.2.9.1.2 Applying Configuration Files

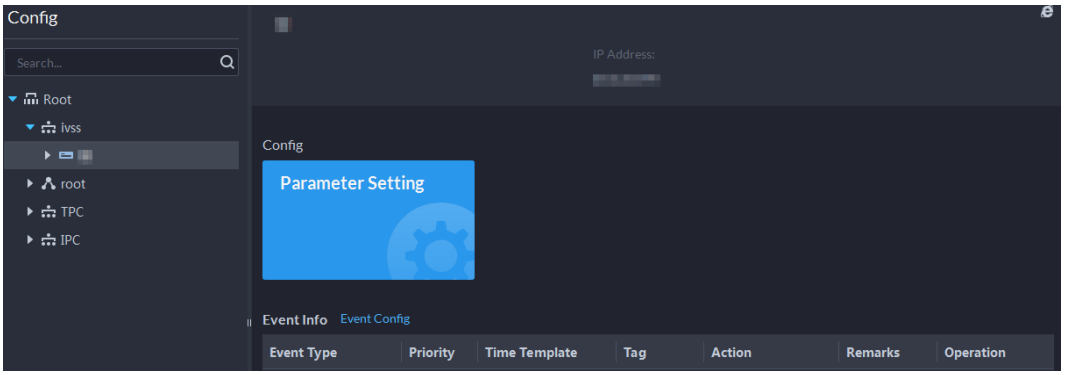
Apply the image parameters as configured in the pre-defined periods.

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

Step 2 Click .

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

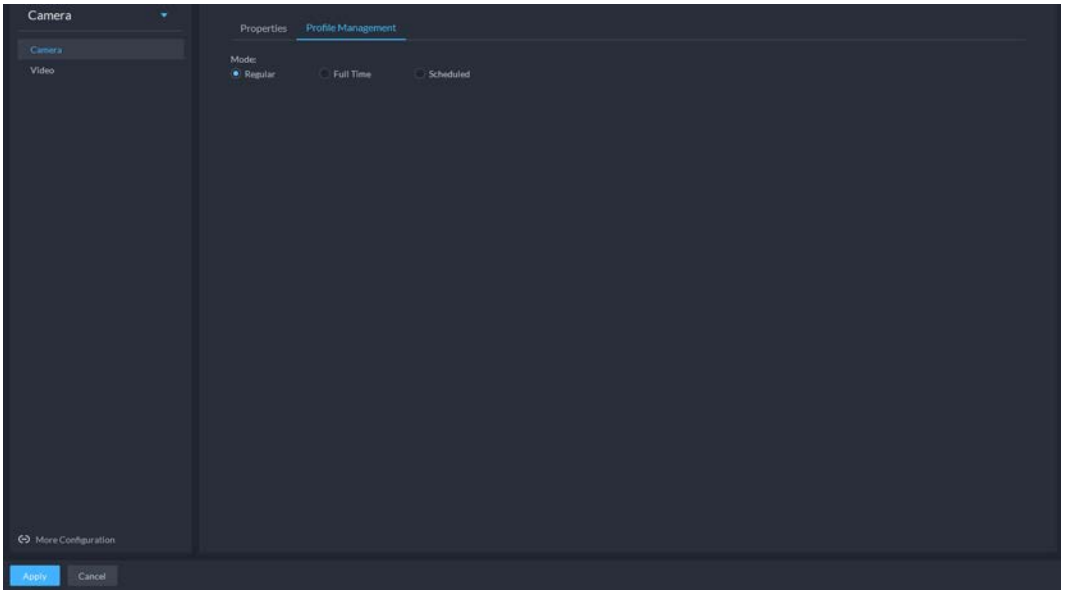
Figure 3-42 Device configuration



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

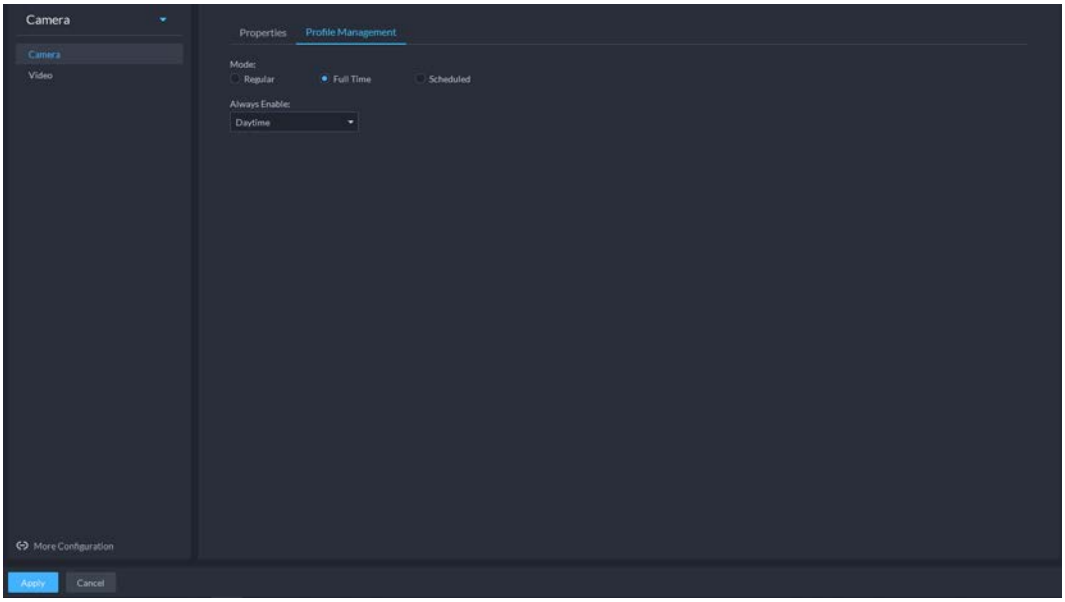
- When the mode is set to **Regular**, the system monitors the objects as per regular configurations.

Figure 3-43 Set configuration files as regular



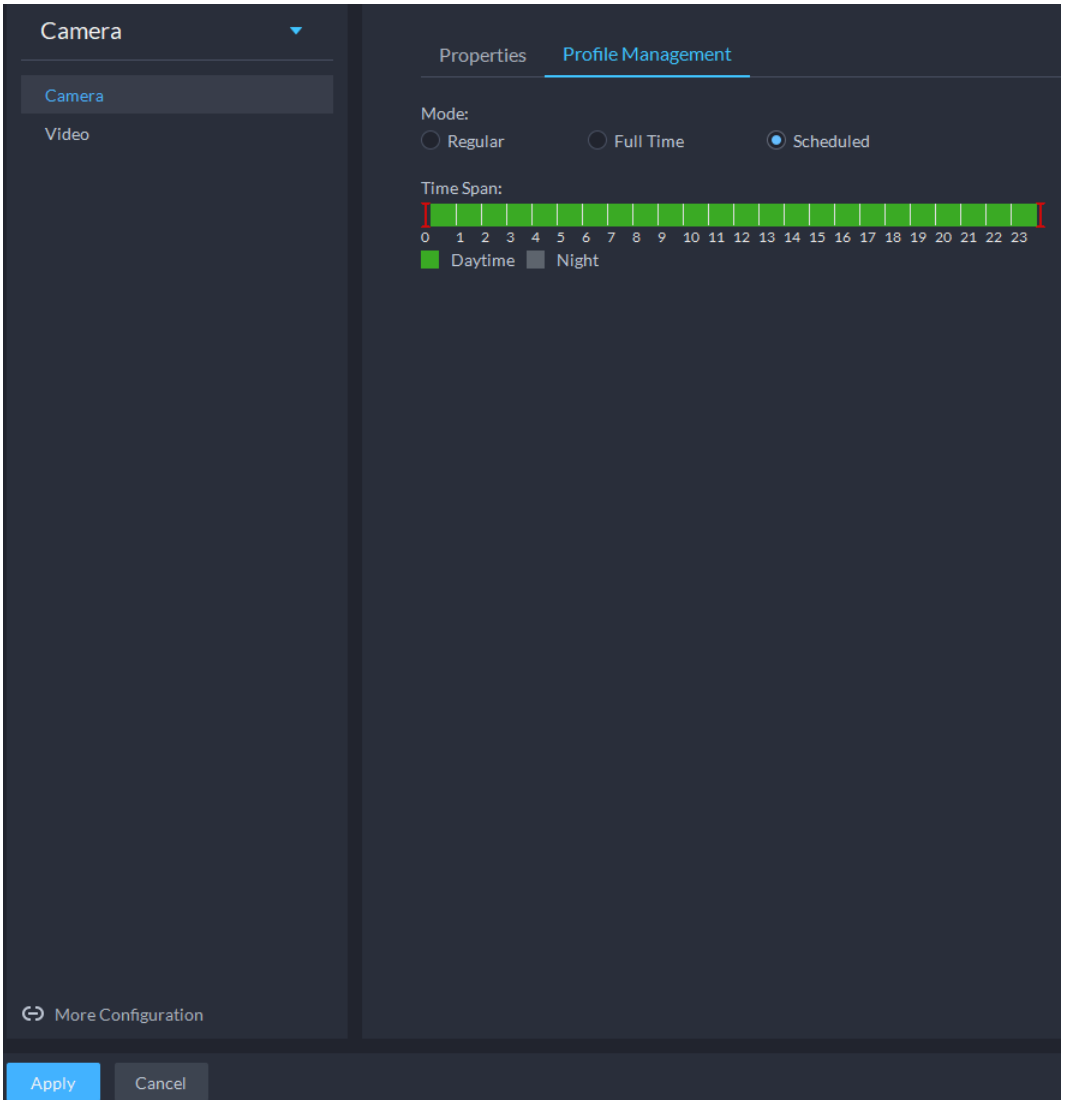
- When the mode is set to **Full Time**, you can set **Always Enable** to **Daytime** or **Night**. The system monitors the objects as per the **Always Enable** configurations.

Figure 3-44 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 3-45 Set configuration files as shift by time



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

3.2.9.2 Video

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

3.2.9.2.1 Video Stream

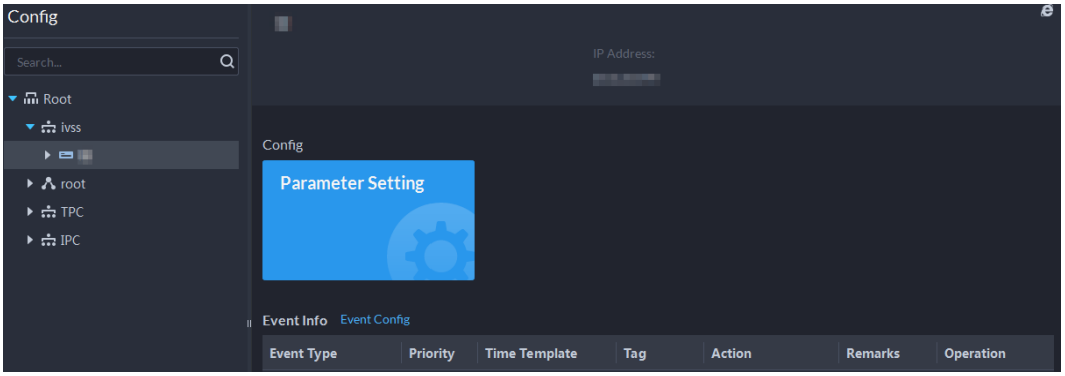
Set the video stream parameters such as stream type, encoding mode, resolution, frame rate, stream control, stream, I frame interval, SVC, and watermark.

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**.

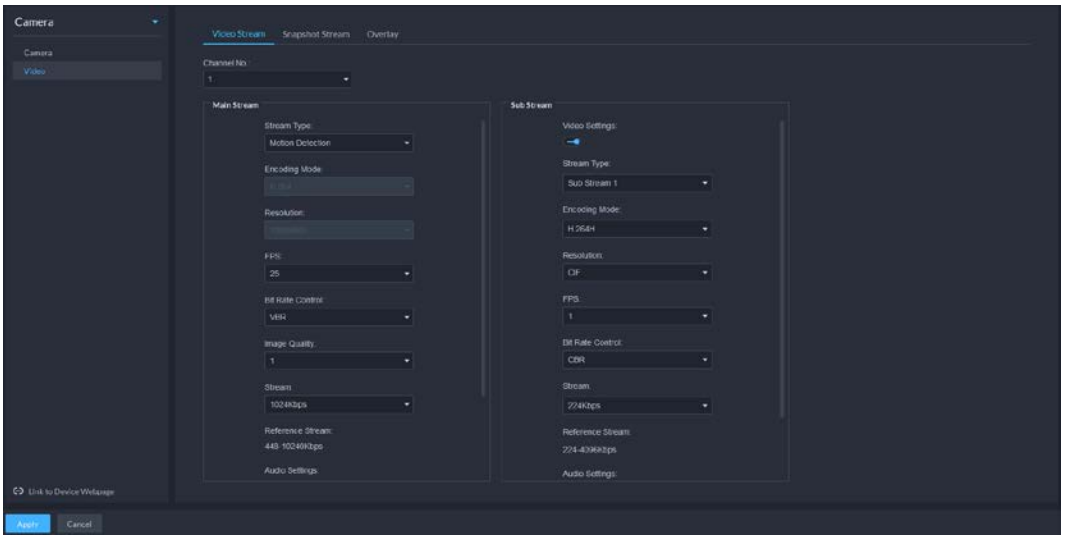
Figure 3-46 Device configuration



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

Step 5 Set **Video Stream**.

Figure 3-47 Configure video stream settings



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

Table 3-17 Video stream parameters

Parameter	Description
Video Settings	Enable or disable **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**.

3.2.9.2.2 Snapshot Stream

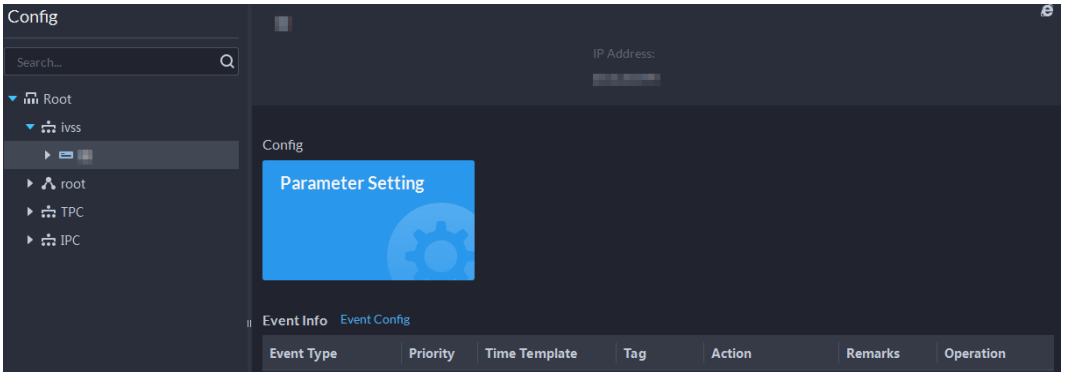
Set snapshot parameters, including snapshot type, picture size, picture quality, and snapshot speed.

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 .

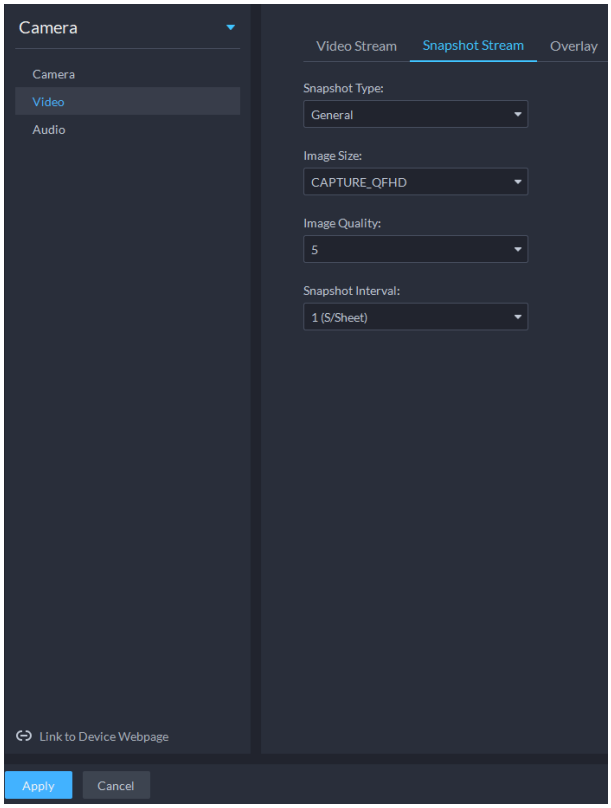
Step 3 Select a device, and then click **Device Config**.

Figure 3-48 Device configuration



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

Figure 3-49 Configure snapshot stream settings



Step 5 Set **Snapshot Stream**.

Table 3-18 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**.

3.2.9.2.3 Overlay

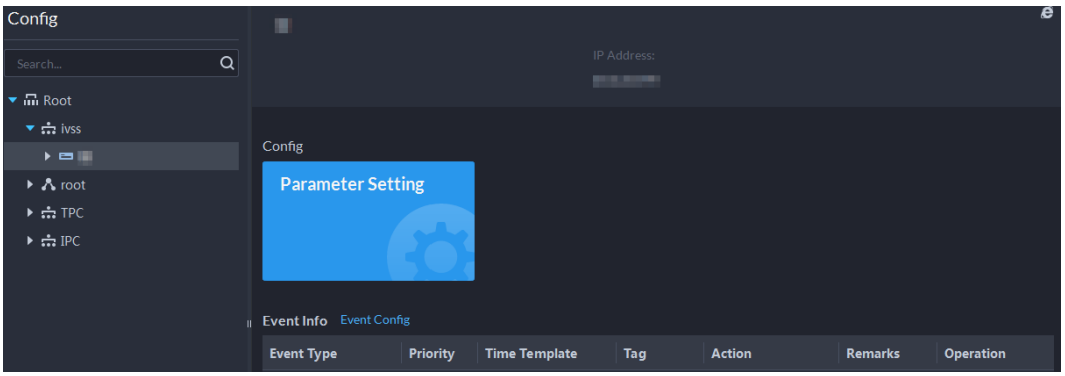
Set video overlay parameters, including tampering, privacy mask, channel title, period title, geographic position, OSD, font, and picture overlay.

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

Step 2 Click .

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

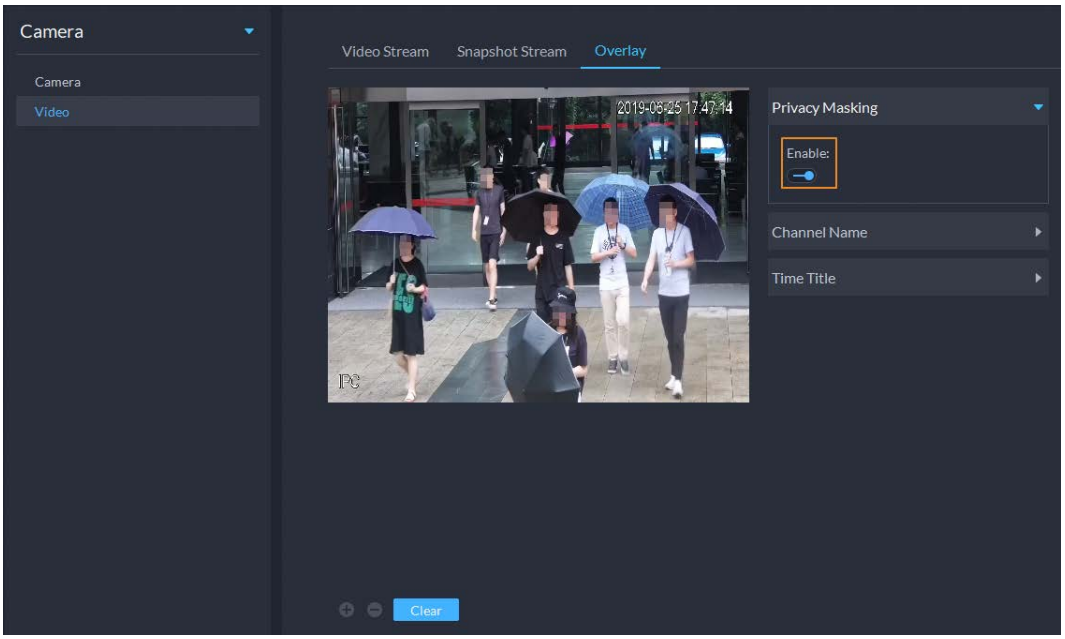
Figure 3-50 Device configuration



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

Step 5 Set privacy mask.

Figure 3-51 Overlay



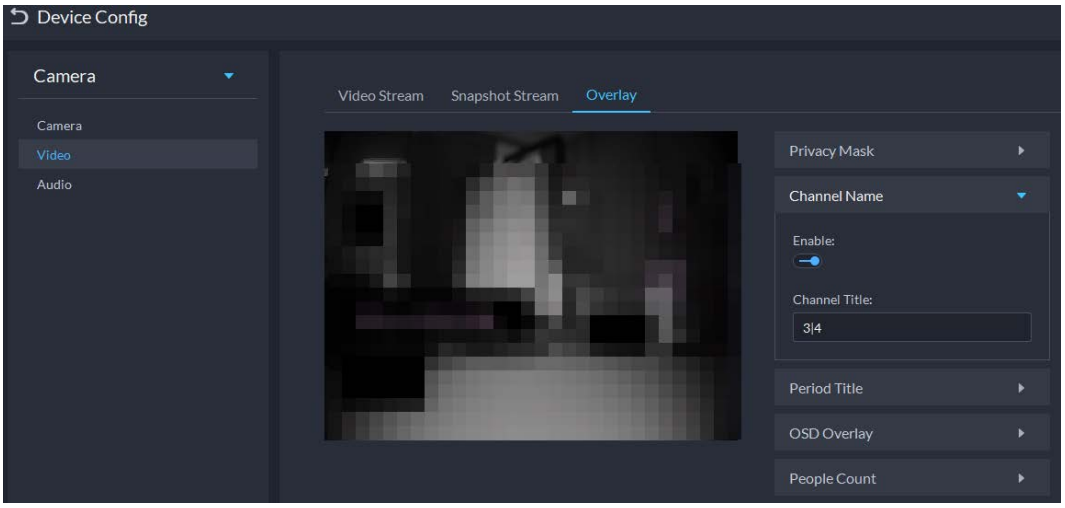
1) Click the **Privacy Mask** tab.

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

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

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

Figure 3-52 Set channel name

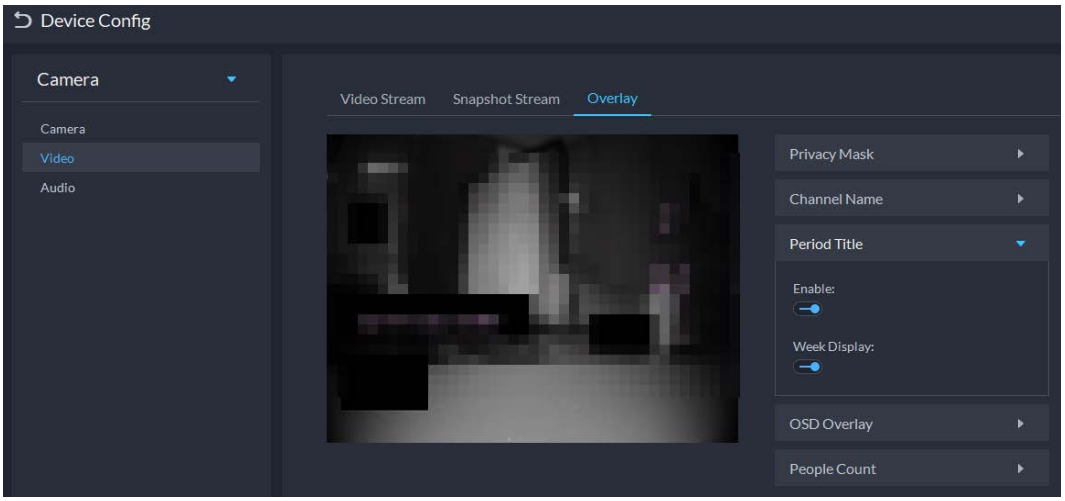


2) Click to enable the function.
3) Adjust the size and position of the name frame.

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

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

Figure 3-53 Set period title

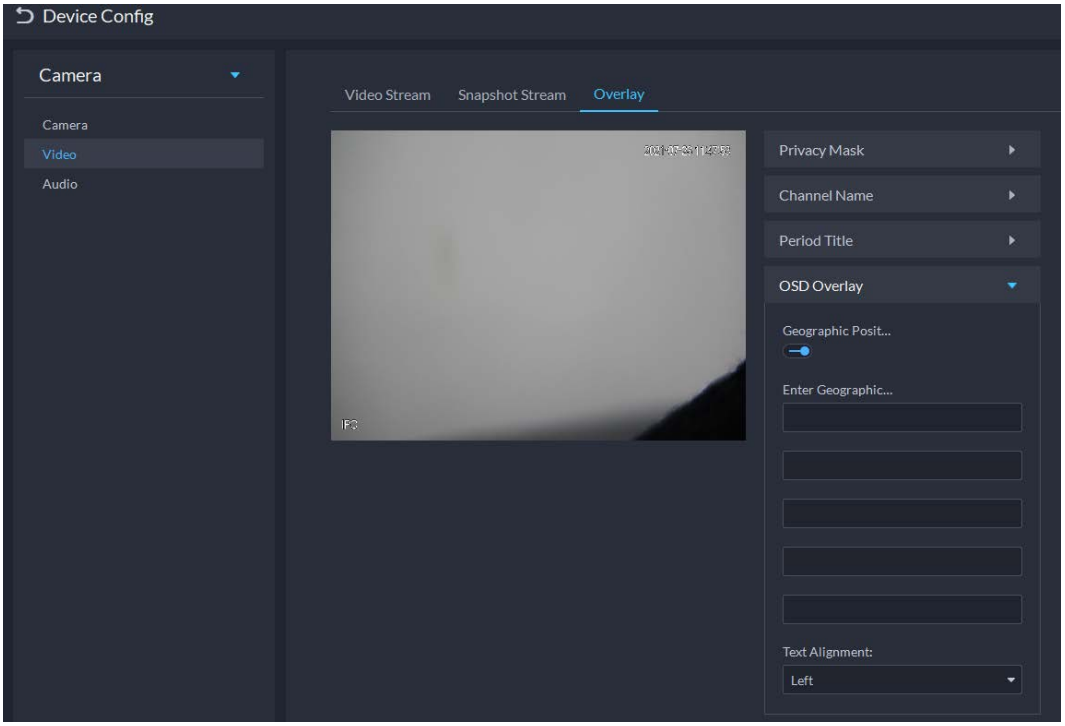


2) Click to enable the function.
3) (Optional) Select **Week Display** so that the week information displays in video images.
4) Adjust the size and position of the frame.

Step 8 OSD overlay.

1) Enable **Geographic Position**, and then enter the geographic information of the camera.
2) Select a text alignment method.

Figure 3-54 OSD overlay



Step 9 Click **OK**.

3.2.9.3 Audio

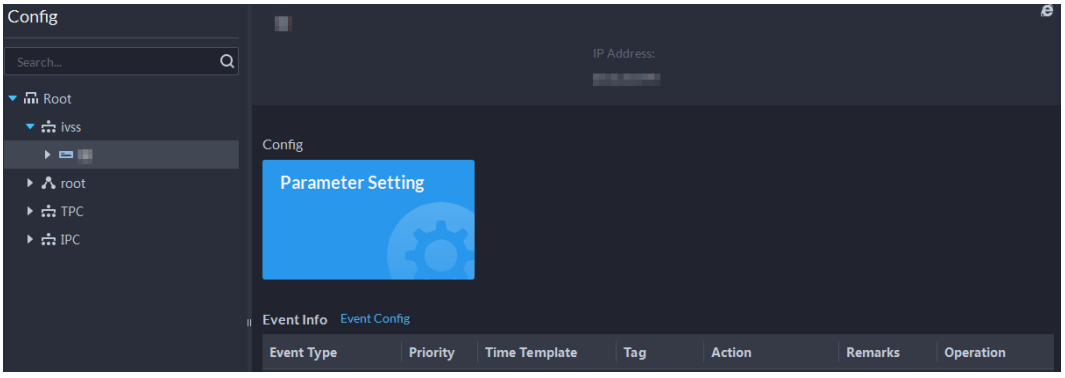
Set audio parameters such as encoding mode, sampling frequency, audio input type, and noise filtering.

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

Step 2 Click .

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

Figure 3-55 Device configuration



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

Step 5 Set parameters.

Figure 3-56 Configure audio settings

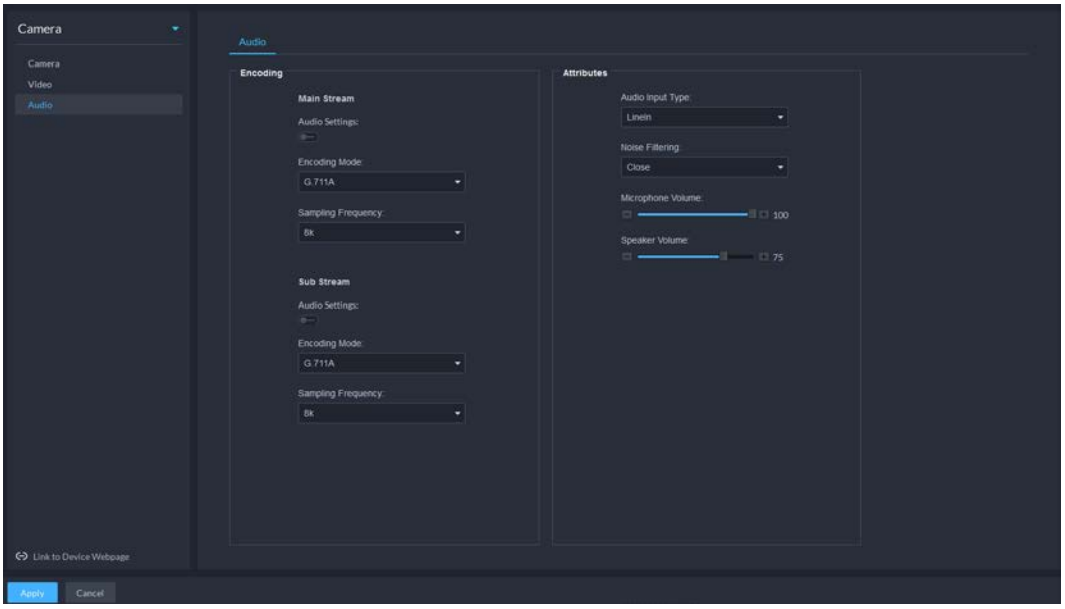


Table 3-19 Audio parameters

Parameter	Description
Audio Settings	Audio settings can be enabled when video has been enabled. After disabling **Audio Settings** in **Main Stream** or **Sub Stream** sections, the network transmits a mixed flow of videos and audios. Otherwise, the transmitted flow only contains video images.
Encoding Mode	The encoding modes of audios include G.711A, G.711Mu, AAC, PCM, and G.726. The preset audio encode mode applies to audio talks.
Sampling Frequency	Available audio sampling frequencies include 8K, 16K, 32K, 48K, and 64K.
Audio Input Type	The following types of audios connected to devices are available: • LineIn: The device must connect to external audio devices. • Mic: The device does not need external audio devices.
Noise Filtering	After enabling noise filtering, the system automatically filters out the noises in the environment.
Microphone Volume	Adjusts the microphone volume. Only some devices support adjusting microphone volume.
Speaker volume	Adjusts the speaker volume. Only some devices support adjusting speaker volume.

Step 6 Click **Apply**.

3.2.10 Synchronizing People Counting Rules

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

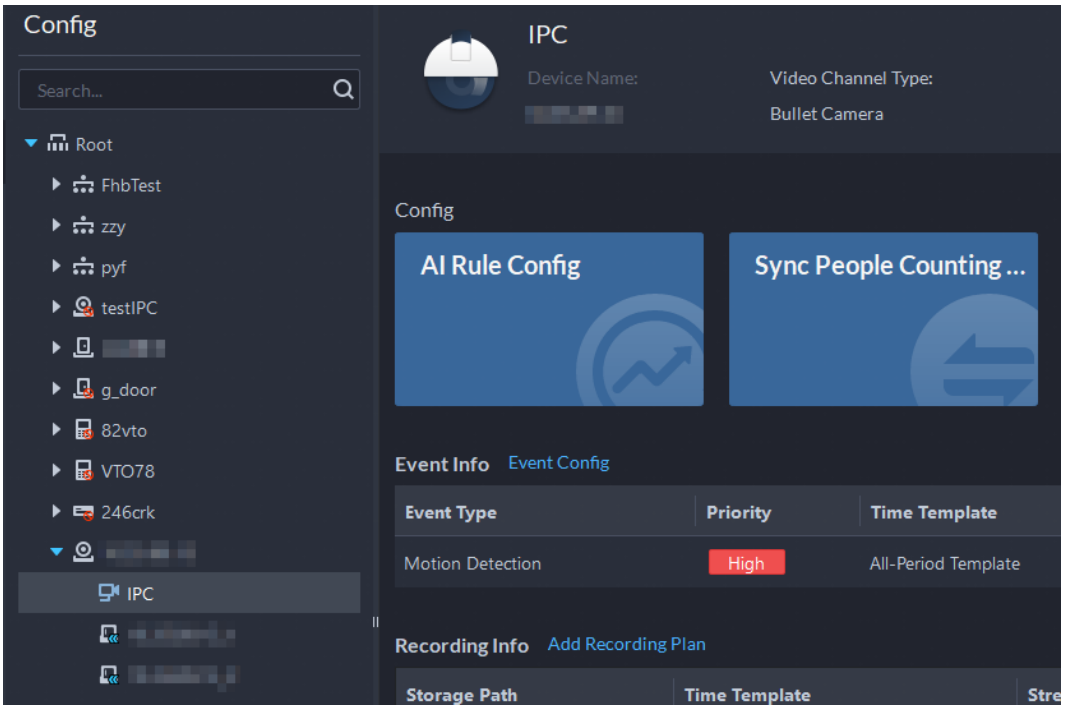
them to the platform.

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

Step 2 Click .

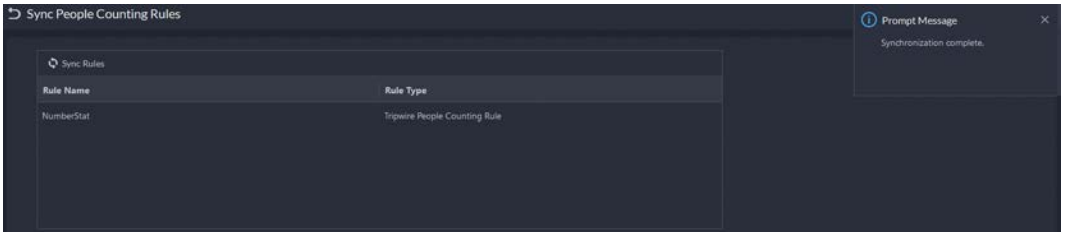
Step 3 Select a channel, and then click **Sync People Counting Rules**.

Figure 3-57 Synchronize people counting rules from the device



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

Figure 3-58 Synchronize people counting rules from the device



3.3 Adding Role and User

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

3.3.1 Adding User Role

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

- Super administrator: A default rule that has the highest priority and all the permissions. This role cannot be modified. A super administrator can create administrator roles and common roles. The system supports 3 super administrators at most.

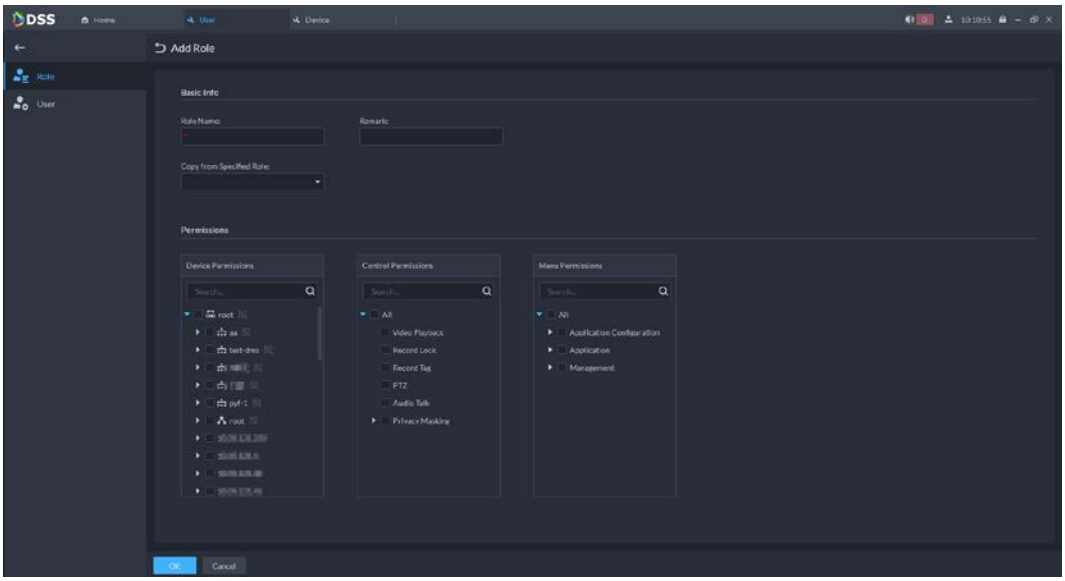
- Administrator: A default rule that cannot be modified and has no permission of configuring cascade, authorization, backup and restoring. An administrator can create other administrators.
- Common role: A common role that has no permission of configuring cascade, authorization, backup and restoring,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

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 .

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

Figure 3-59 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**.

3.3.2 Adding User

Create a user account for logging in to the platform.

Procedure

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

Step 2 Click .

Step 3 Click **Add**, and then configure the user information.

Table 3-20 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 Confirm Password	Used to log in to the client.
MPT User	Enable and enter a name, and then this user will be set as an MPT user. This is used in the group talk function in the map. For details, see "5.1.4 Map Applications". If you enable this function, you cannot enable **Multi-client Login**.
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.
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, which is locked, 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 4 Click **OK**.

Related Operations

- Click to lock user. The locked 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.

3.3.3 Importing Domain User

You can import domain users from the domain system of your current organization to create platform users.

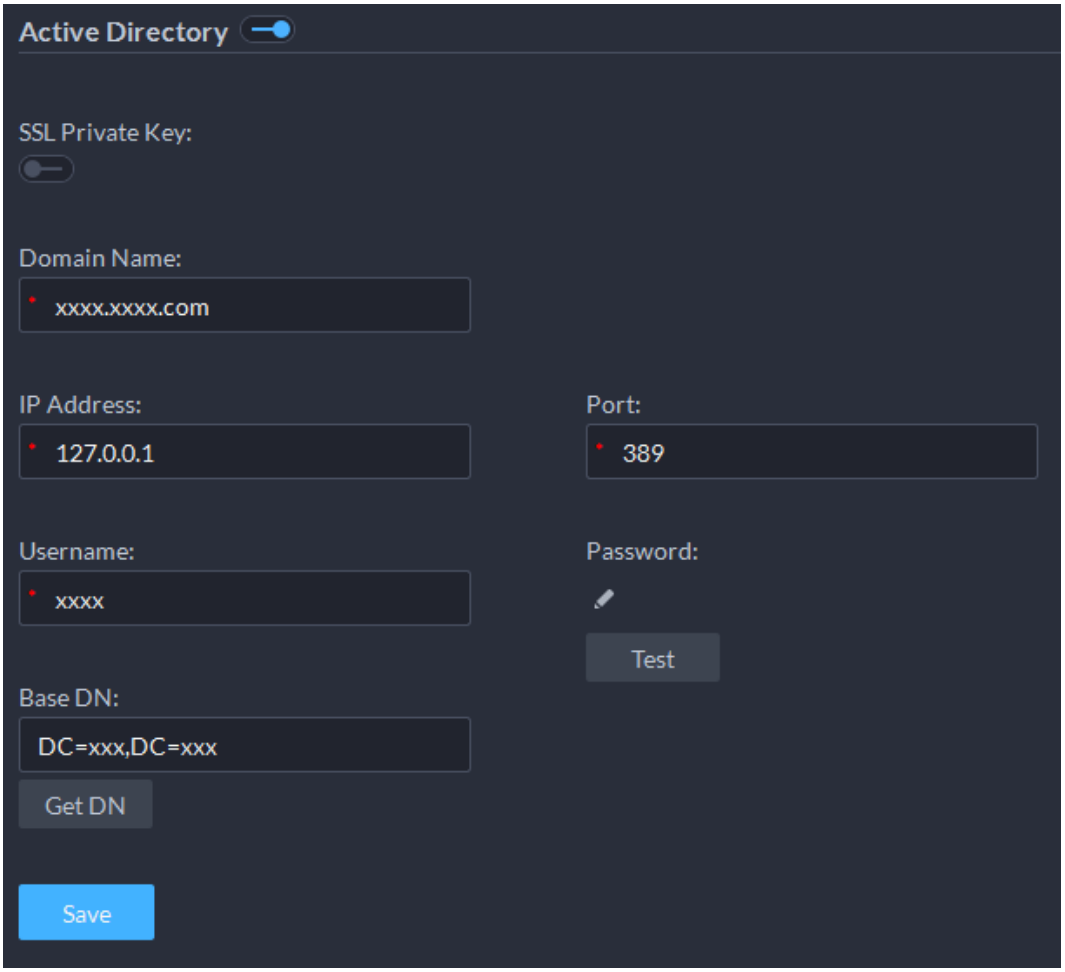
Step 1 Configuring domain information

1) Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameters**.
2) Click **Active Directory** and configure domain information.
3) Enable active directory to set domain information. indicates active directory is

enabled.

- Click to enter the password.
- After setting domain information, click **Get DN** and it will acquire basic DN information automatically.
- After getting DN information, click **Test** to test if domain information is available.

Figure 3-60 Set active directory



4) Click **Save**.

Step 2 Import domain users.

1) Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.
2) Click tab, and then click **Import Domain Users**.
3) Select the users to be imported, and then click **Next**.
   You can also search for a user by entering keywords in the search box.
4) Select the roles, and then click **OK**.

Related Operations

To log in using a domain user account, start the DSS Client, and then select **Domain User** for user type.

3.3.4 Syncing Domain User

When there are users that have expired, you can use sync domain user to delete the expired users.

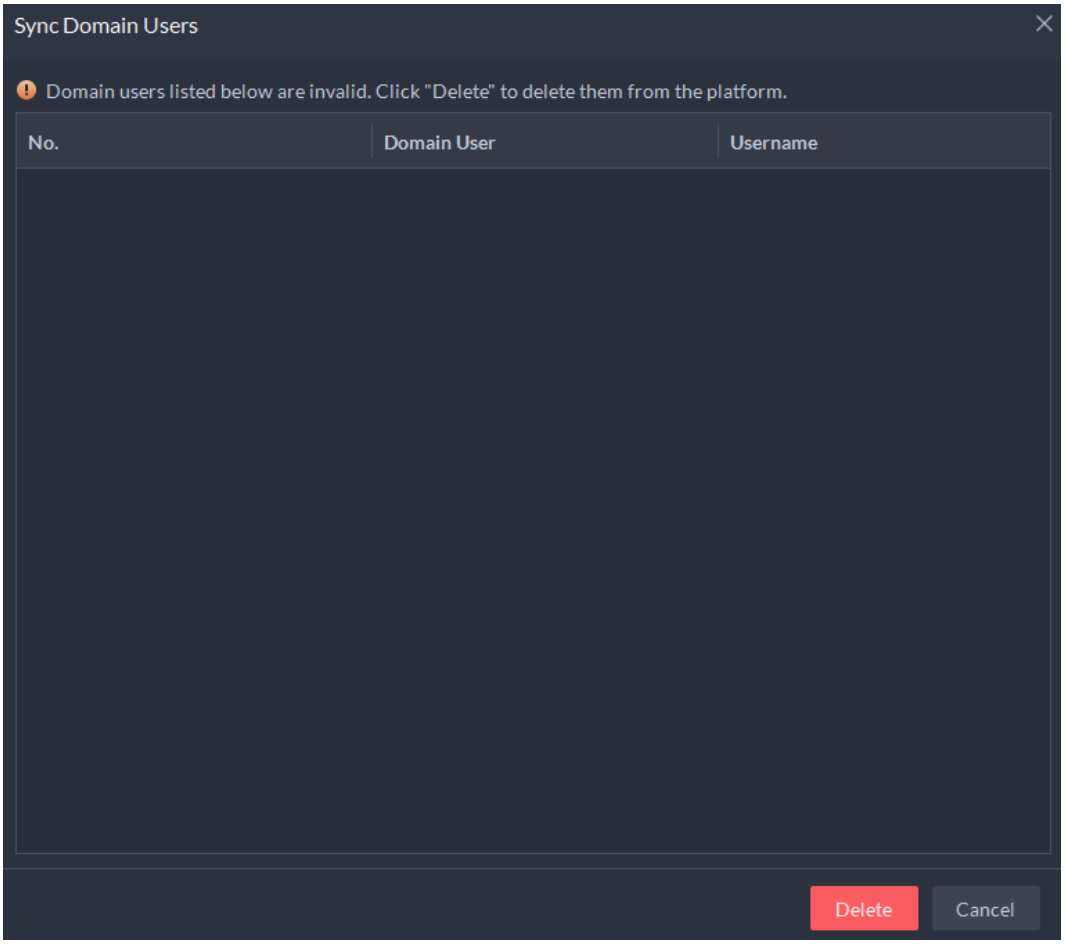
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.

Step 2 Click .

Step 3 Click **Sync Domain Users**.

Step 4 Select the users to be deleted, and the click **Delete**.

Figure 3-61 Sync domain user



3.3.5 Password Maintenance

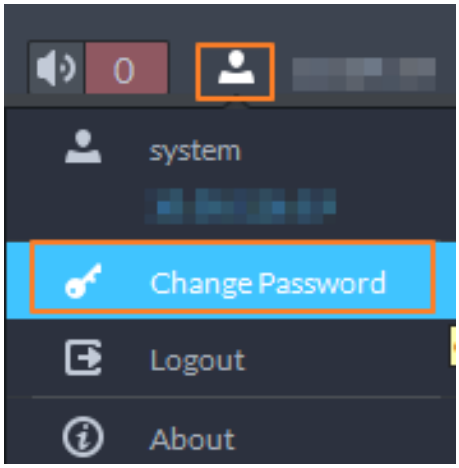
The platform supports modifying user password, and resetting system user password when it is forgotten. Only the system user can reset password. Other users, when their passwords are forgotten, can ask the system user to modify the passwords.

3.3.5.1 Changing Password for the Current User

We recommend changing your password regularly for account safety.

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

Figure 3-62 Change password



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

3.3.5.2 Changing Password for Other Users

The system user can change the password for other users without the need to verify the old password.

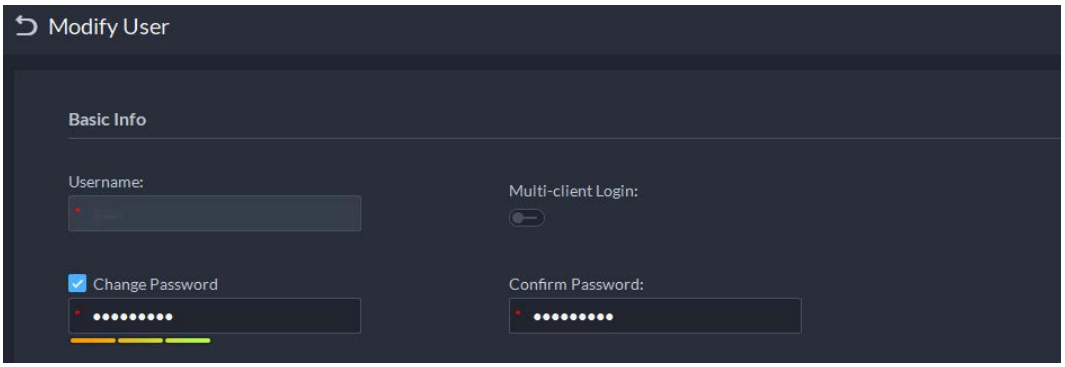
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.

Step 2 Click .

Step 3 Select a user, and then click .

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

Figure 3-63 Change user info



3.3.5.3 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 "3.3.2 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.

3.4 Configuring Storage

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

3.4.1 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 3-64 Add network disk (normal mode)

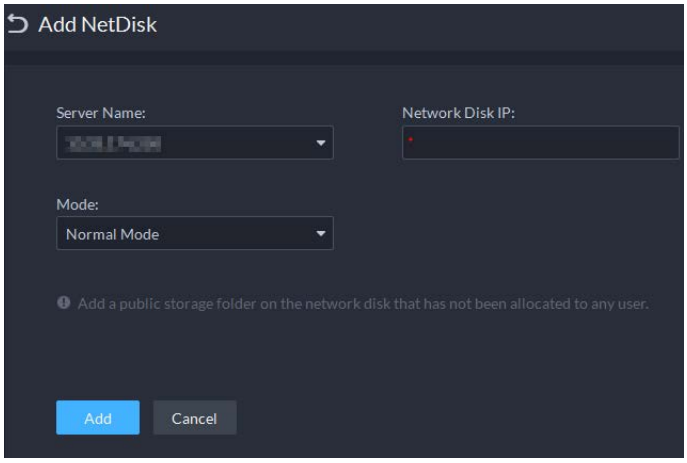
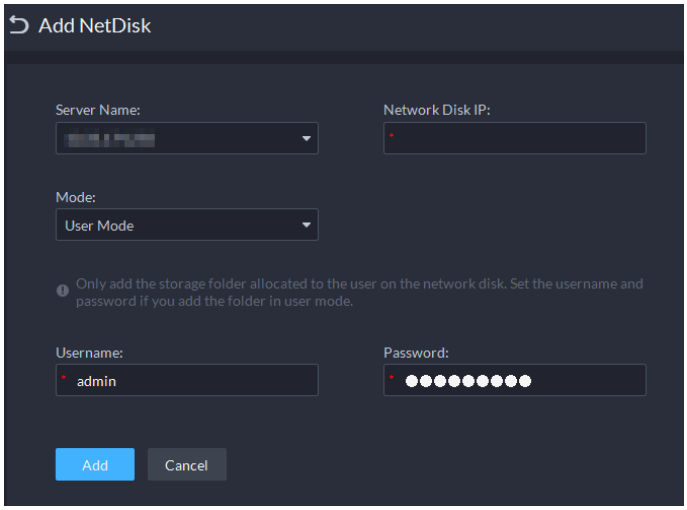


Figure 3-65 Add network disk (user mode)

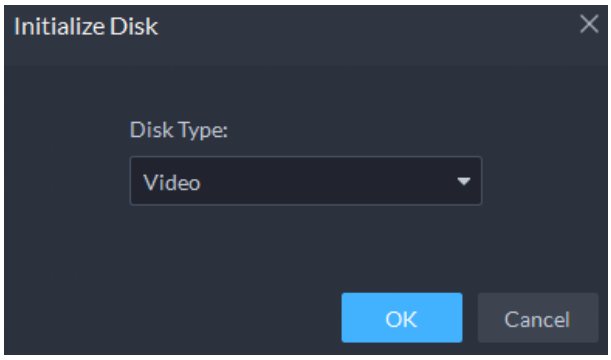


Step 5 Select disk, and then click to format the corresponding disk.

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

- **Video**: Stores videos.
- **Image and File**: Stores video files from MPT devices, and all types of images.

Figure 3-66 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.

3.4.2 Configuring Server Disk

Configure local disk to store different types of files, including videos, ANPR snapshots, incident files, 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 or the DSS server. See "2.1.2 Installing DSS".

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 video files from MPT devices, and all types of images.
   - **Incident File**: Stores videos and images in the case bank. This disk cannot be overwritten.

   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

3.4.3 Configuring Disk Group

Allocate disk groups for video storage.

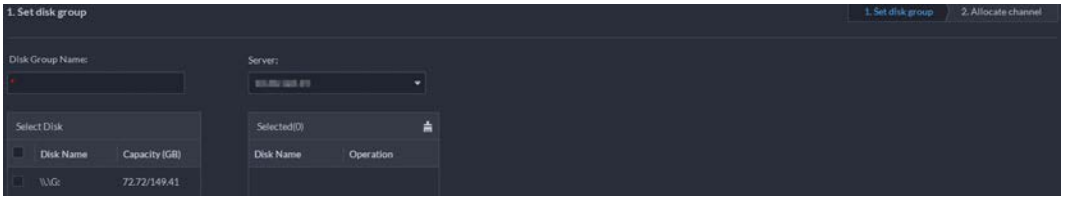
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config**

section, select **Storage**.

Step 2 Click .

Step 3 Click **Add Disk Group**, enter disk group name, and then select a server and disks.

Figure 3-67 Configure disk group



Step 4 Click **Next Step**.

Step 5 Select devices or channels on the left.

Step 6 Click **OK**.

3.4.4 Configuring Device Storage

When there are a large number of devices on the platform, it will put too much pressure on the network disks or 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 3-21 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 network disks or 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.
Event Video Storage Location	• **Save to Central Storage**: All alarm videos produced by the channels connected to this device will be stored on the network disks or 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.

Parameter	Description
	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.

3.5 Connecting to Multiple Sites

If you have multiple platforms, you can connect to others as sites to your current platform, so that you can view the resources from them directly on your platform, including viewing real-time videos from video channels, searching for viewing real-time and historical events, and downloading recorded videos.

The versions of different platform must be the same.

Step 1 Log in the DSS Client.

Step 2 Click on the upper-right corner, and then click **Add Site**.

Step 3 Enter a name for the site, and the login information, and then click **OK**.

You can now view real-time videos of the devices, and real-time and historical events from the site.

Figure 3-68 Resources from the site shown on the Monitoring Center

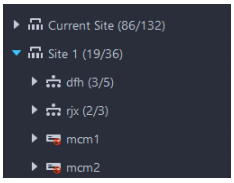


Figure 3-69 Search for historical events from the site in Event Center

4 Businesses Configuration

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

4.1 Configuring Events

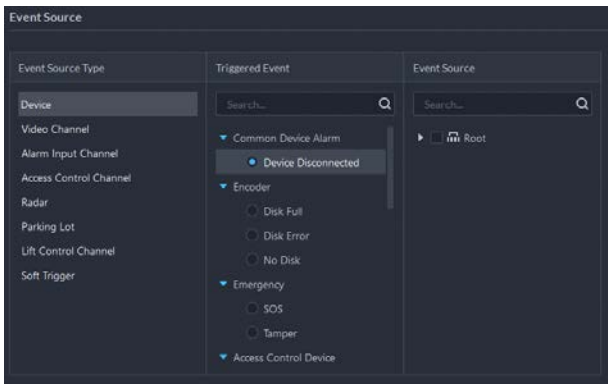
Configure events first if you want to display alarm event notifications on the platform.

Procedure

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

Step 2 Click **Add**.

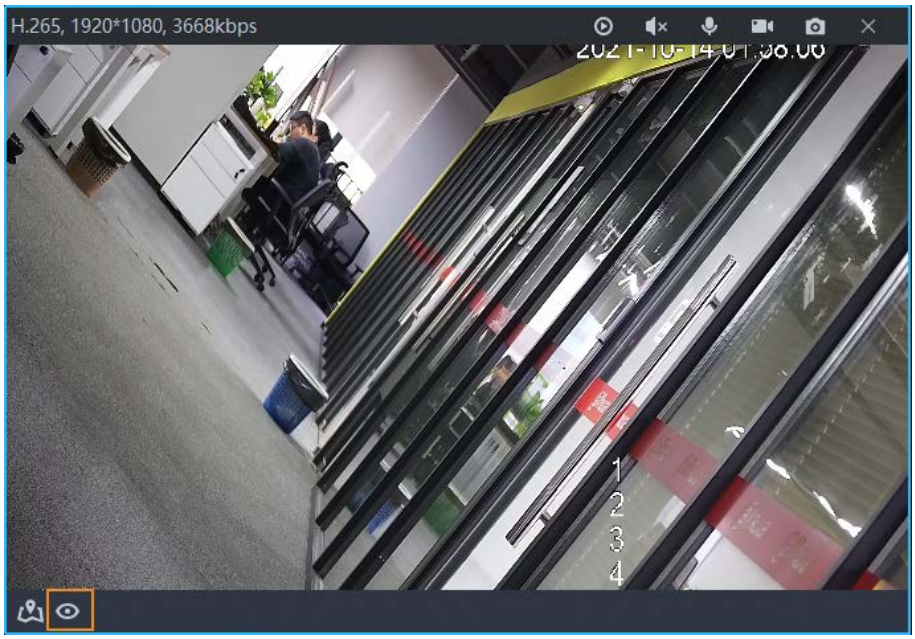
Figure 4-1 Configure the event source



Step 3 Configure the event source.

- Before configuring the event, check whether the channel features match the event type; otherwise the event type cannot be selected as the alarm source. To configure channel features, see "3.2.2.5.2 Modifying Device Information".
- If **Alarm Input Channel** is selected, check whether the **Triggered Event** that you select matches the alarm input channel you select; otherwise, the event will not be triggered.
- **Soft Trigger** is a type of event that is manually triggered. You can customize its name and button type. When viewing the live video image of the configured channel in the **Monitoring Center**, you can click its button to trigger an alarm manually.

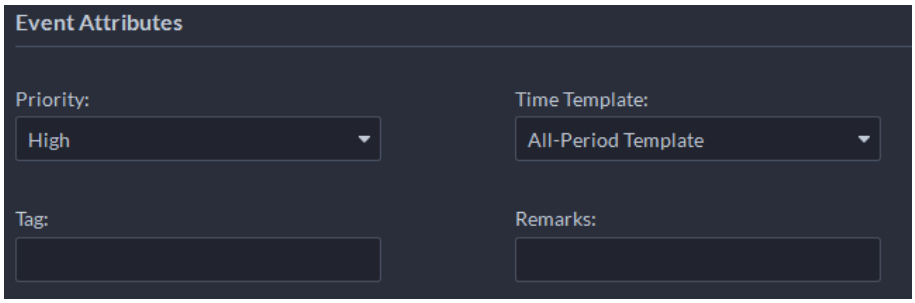
Figure 4-2 Manually trigger an alarm by clicking the button



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

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

Figure 4-3 Event attributes



Step 5 Configure alarm linkage actions.

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

Figure 4-4 Link video

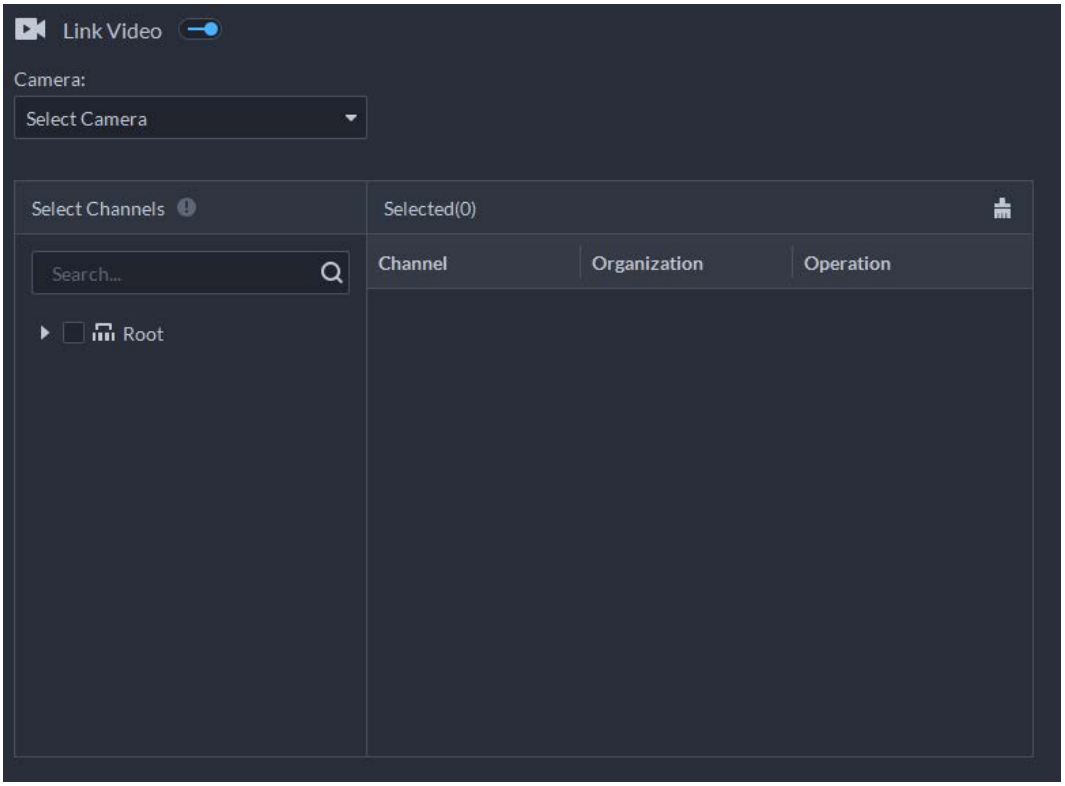


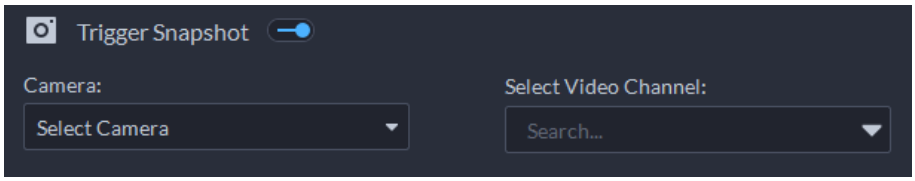
Table 4-1 Parameter description

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 "3.2.3 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 "8.3.4 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.

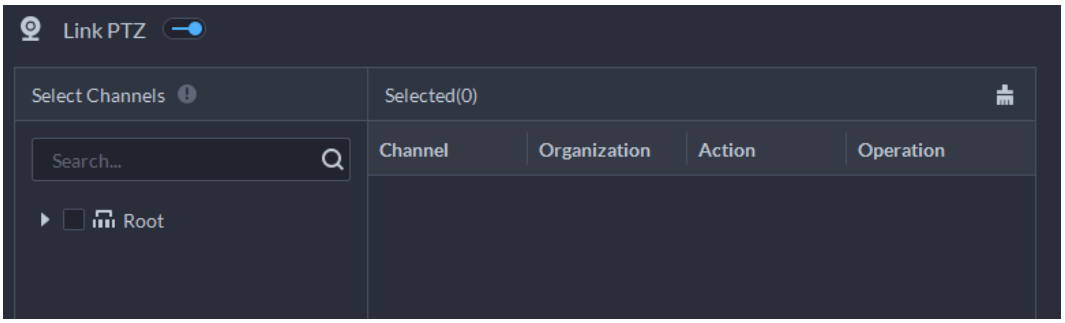
- To trigger a snapshot, enable **Trigger Snapshot**.
  Select a video channel, and then it will take a snapshot when an alarm is triggered.

Figure 4-5 Trigger a snapshot



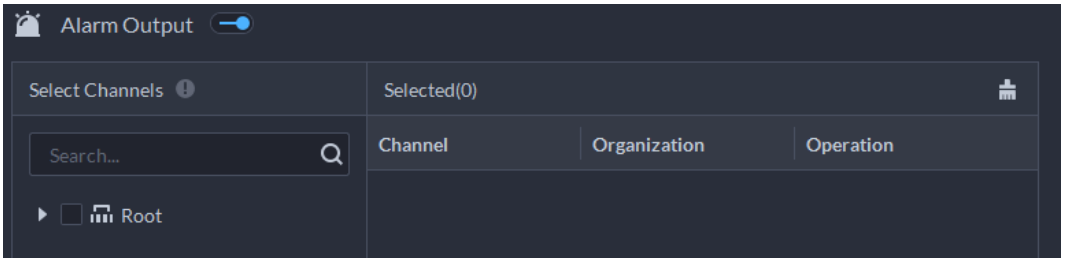
- To link a PTZ action, click **Link PTZ**, and then select the PTZ channels and presets to be linked.

Figure 4-6 Link PTZ



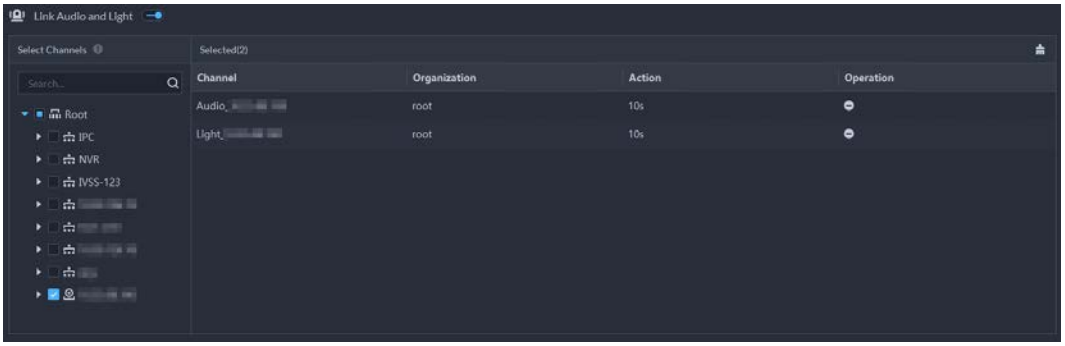
- Click **Alarm Output**, select an alarm output channel, and then set duration.

Figure 4-7 Alarm output



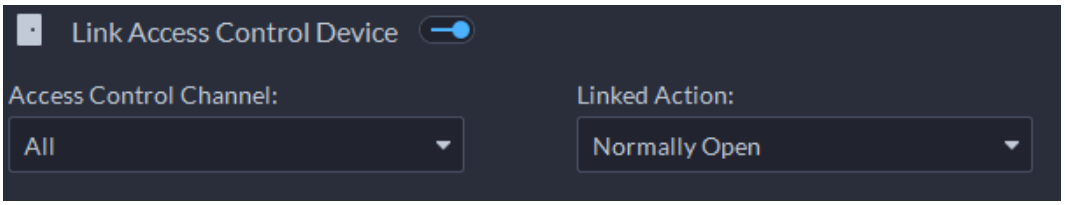
- To link audio and light, click **Link Audio and Light**, select the audio and light channels, and then select the action duration.

Figure 4-8 Link audio and light



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

Figure 4-9 Link access control device

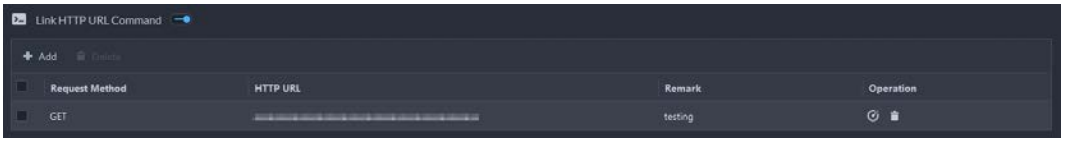


- To play alarm video on the video wall, click **Link Video Wall**, select a camera on the left of the page, and then select a video wall window on the right of the page.

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

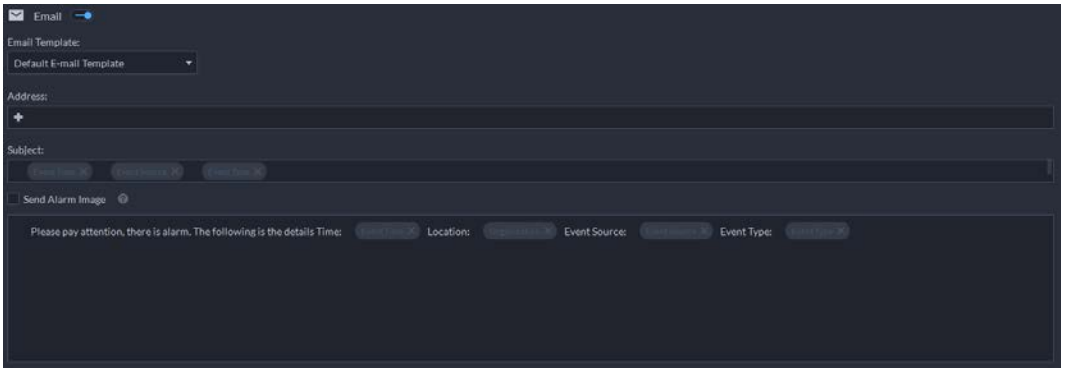
- To execute an HTTP URL; command, click **Link HTTP URL Command**. Click **Add**, and then configure its request method, HTTP URL, and remarks. You can click to test if the command is valid.

Figure 4-10 Link HTTP URL command



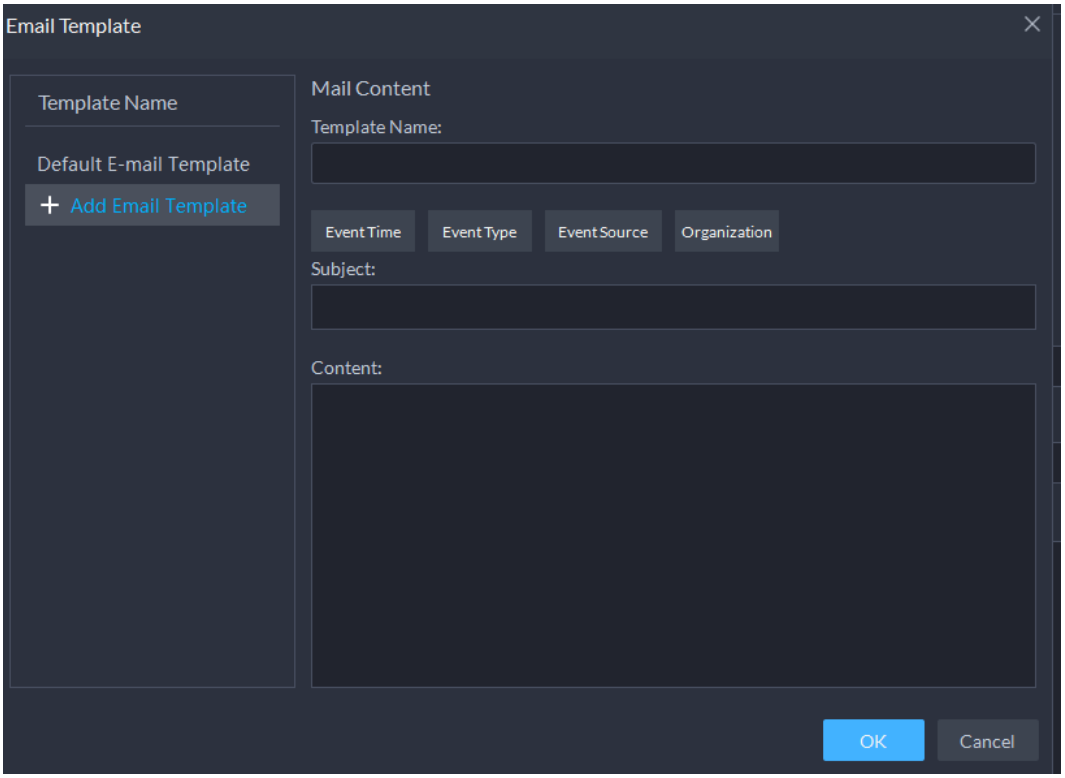
- To link emails, enable **Email**, and click to add the email address, and then an email will be sent to the selected email address when an alarm is triggered.

Figure 4-11 Link email



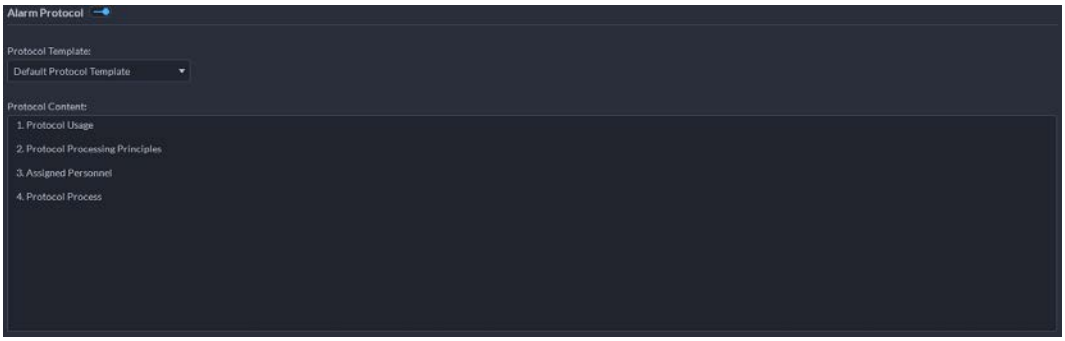
To configure the email template, select **Add Email Template** from the **Email Template** drop-down list.

Figure 4-12 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.

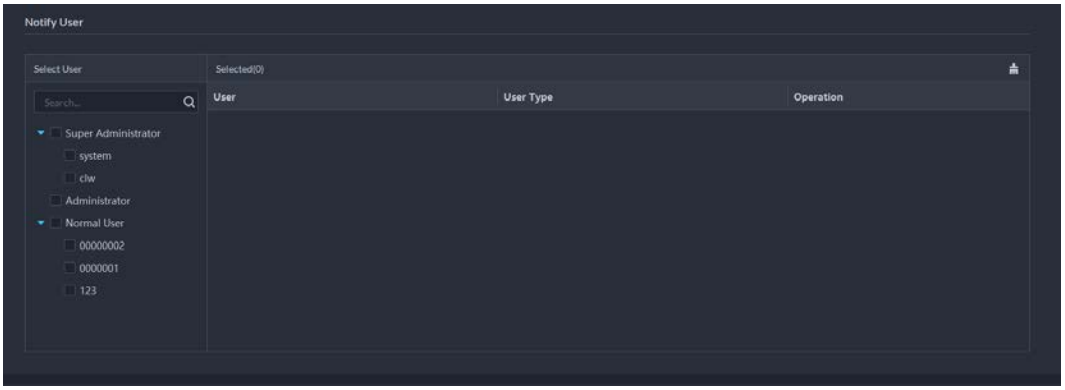
Figure 4-13 Alarm protocol



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 4-14 Notify user



Related Operations

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

4.2 Configuring Map

4.2.1 Preparations

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

4.2.2 Adding Map

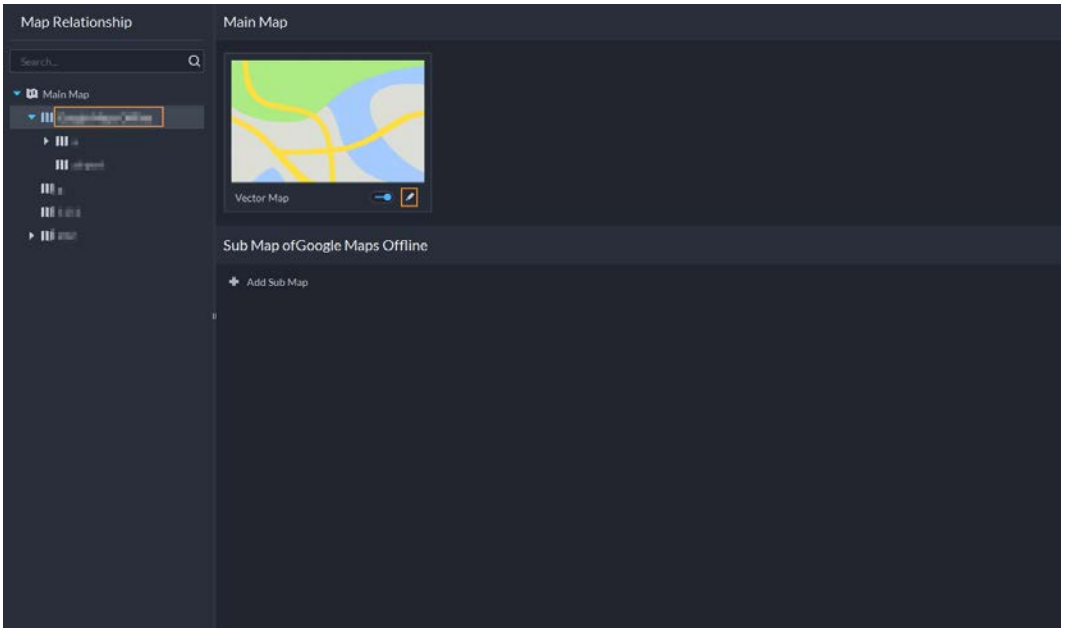
4.2.2.1 Adding Vector Map

Procedure

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

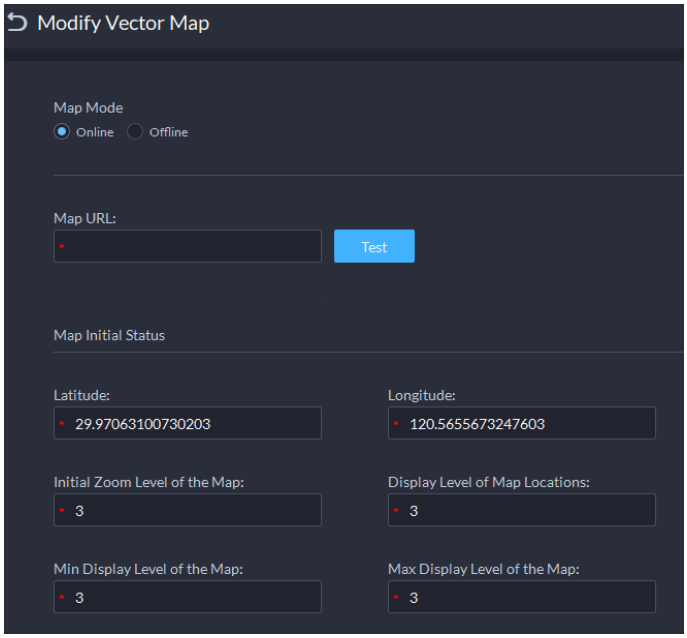
Step 2 In the map list, select the vector map, and then click .

Figure 4-15 Map



Step 3 Configure the parameters.

Figure 4-16 Map information



- Online map
  1. Select **Online**.
  2. Configure the information of the map, and then click **OK**.
- Offline map
  1. Select **Offline**.
  2. Click **Import** and import offline map.
  3. Configure map information, and then click **OK**.

Step 4 Add a sub map.

If there is a specific area on the map that you want to view its detailed information, you can add an image of it on the map as a sub map. For example, you can add a plane image of a parking lot on the map.

1) On the map resource tree on the left, click the name of the map that you have just added, or open the GIS map and click **Add Sub Map**.
2) Name the sub map, upload a map picture, and then click **OK**.
3) Drag the map to adjust its position, and then click **OK.**
   The sub map is added.

Related Operations

- Hide Device Name
  Only display the icons of devices.
- Satellite Map
  View the satellite map.
- Delete Devices
  To delete a device from the map, click it and then click **Delete Resource**.
- 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 on 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.

4.2.2.2 Adding Raster Map

A raster map is suitable for places where you want to view their detailed information, such as a parking lot. You can add multiple ones.

Procedure

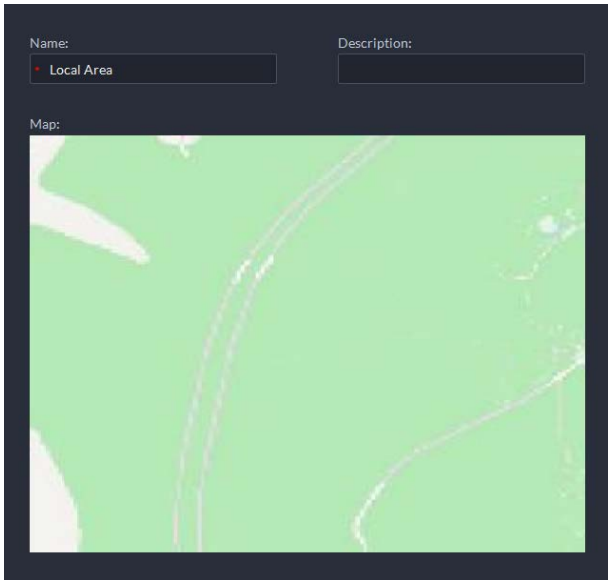
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section,

select **Map**.

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

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

Figure 4-17 Add main map



Step 4 Add a child 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 Devices
  To delete a device from the map, click it and then click **Delete Resource**.
- 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 on 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.

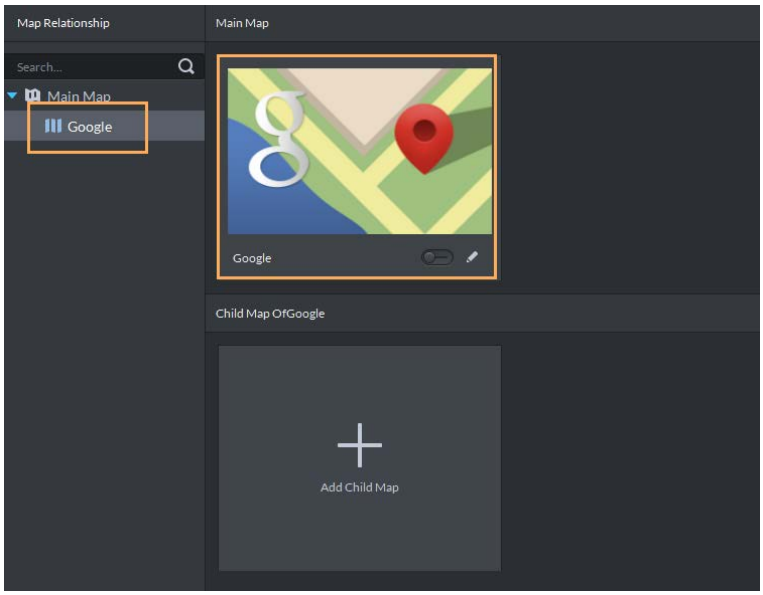
4.2.3 Marking Devices

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

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

Step 2 Click the map.

Figure 4-18 Map



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

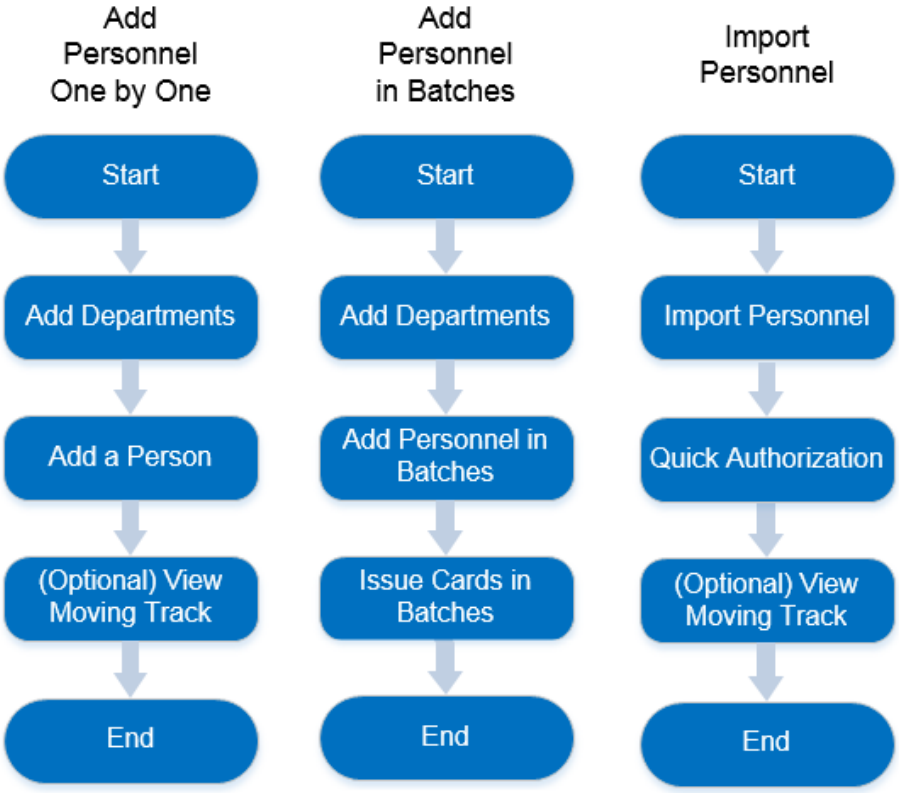
4.3 Personnel and Vehicle Information Management

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

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

4.3.1 Configuring Personnel Information

Figure 4-19 Personnel management



4.3.1.1 Adding Person Group

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

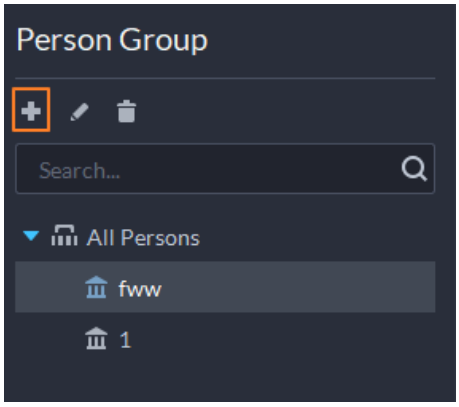
Procedure

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 .

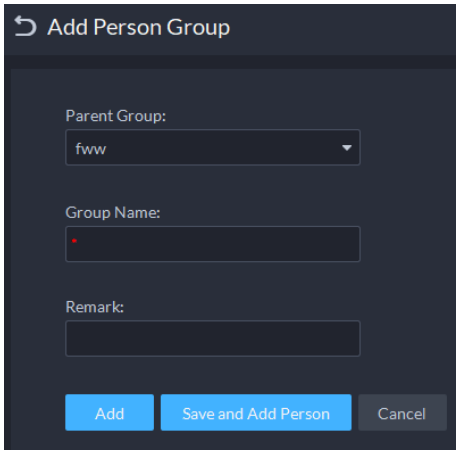
Step 3 Click .

Figure 4-20 Added person group (1)



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

Figure 4-21 Added person group (2)



Related Operations

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

4.3.1.2 Adding Personnel

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

- The information of a person must be the same on the platform and access control devices, such as the person ID and card number. Otherwise the attendance data of this person cannot be synchronized between the platform and access control devices.
- To collect fingerprints or card number, connect a fingerprint collector or card reader first.

4.3.1.2.1 Adding a Person

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**.

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

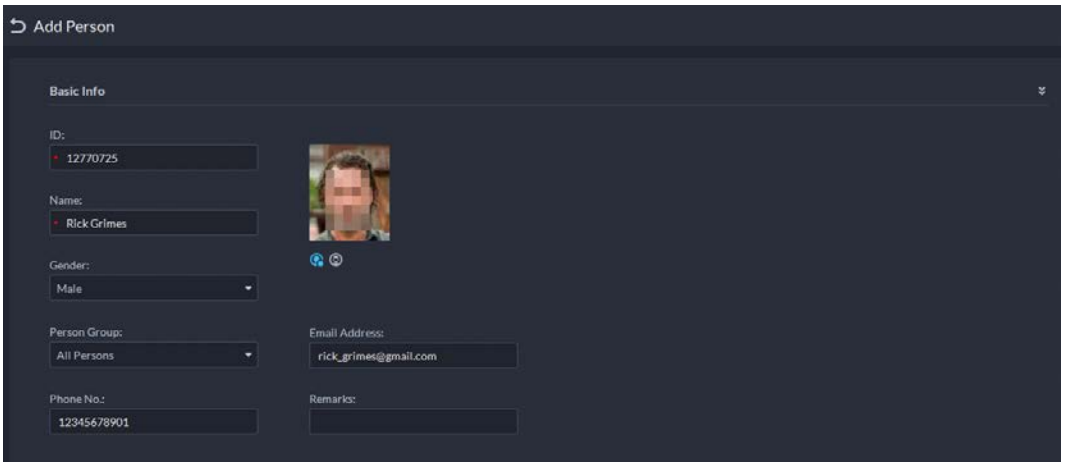
1) Hover over the profile, and then click **Upload** to select a picture or click **Snapshot** to take a photo.

   - You can upload 2 pictures or take 2 snapshots.
   - Click 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 4-22 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.

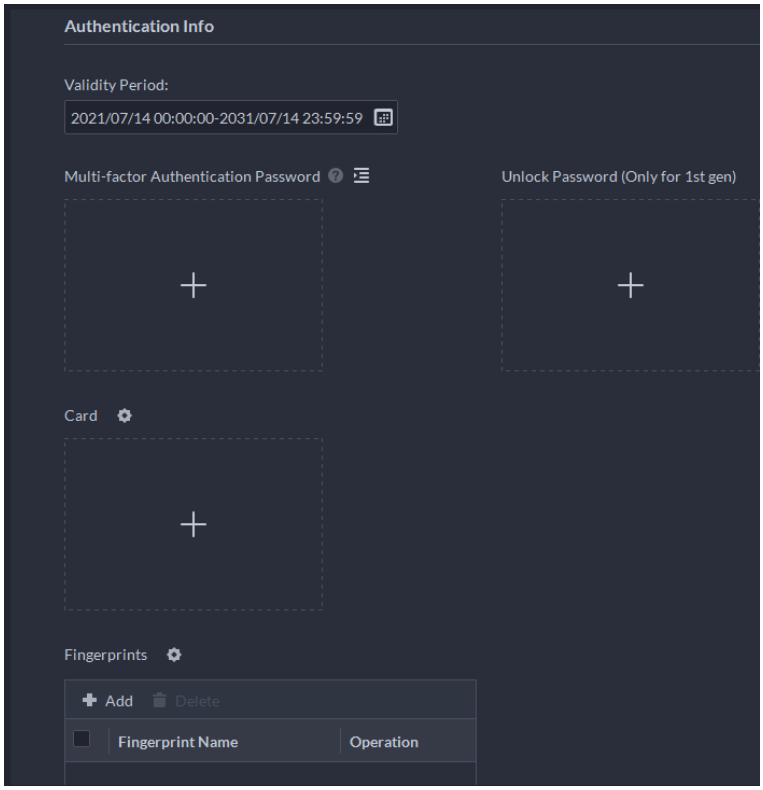
Step 5 Click », and then set person details as required, including nickname, ID, address, birthday, region, company, job title, and more.

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 4-23 Authentication Info



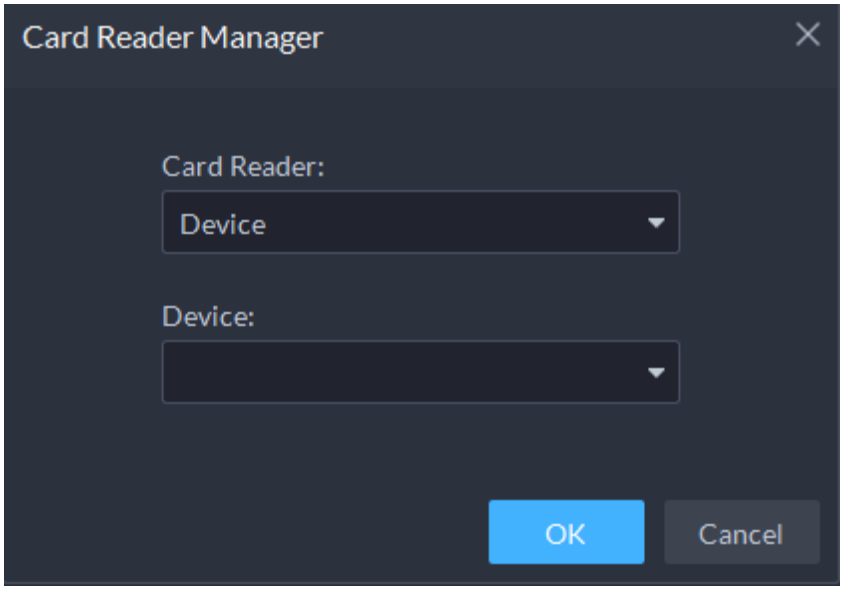
1) Configure effective periods, within which the face, card, password, and fingerprint are effective.
2) When access controllers are added and passwords are required to unlock the door, configure the password first.
   - A multi-factor authentication password must be used with a card, person ID, or fingerprint 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 4-24 Card reader manager



2. Click , swipe a card on the device you select, the card number will be recognized and displayed.
3. Click .

- Manually enter the card number.
  Click , enter card number, and then click .

Figure 4-25 Reader manager

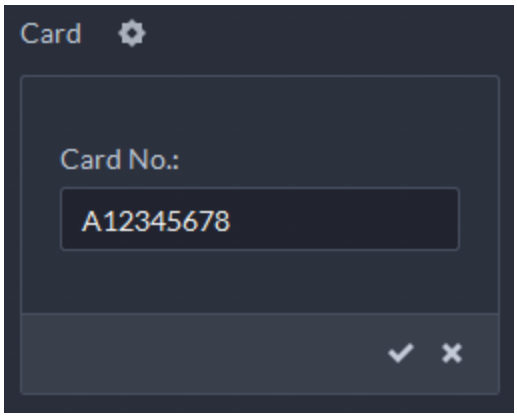


Table 4-2 Card operations

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

Step 9 Collect fingerprint.

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

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

Figure 4-26 A collected fingerprint

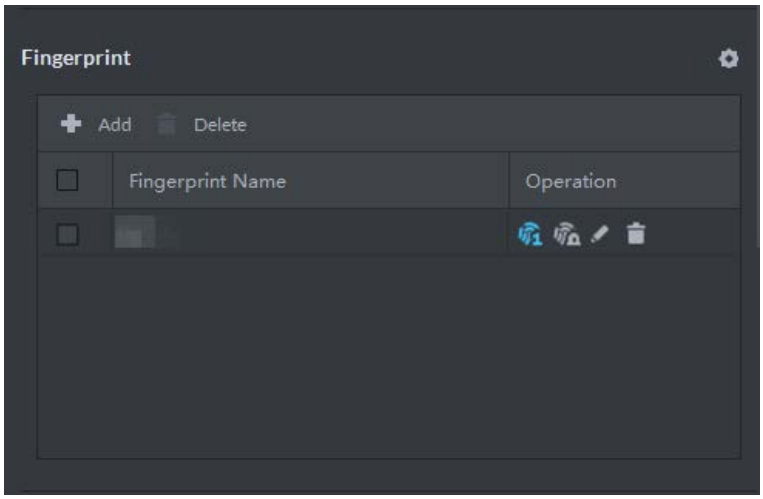


Table 4-3 Fingerprint operations

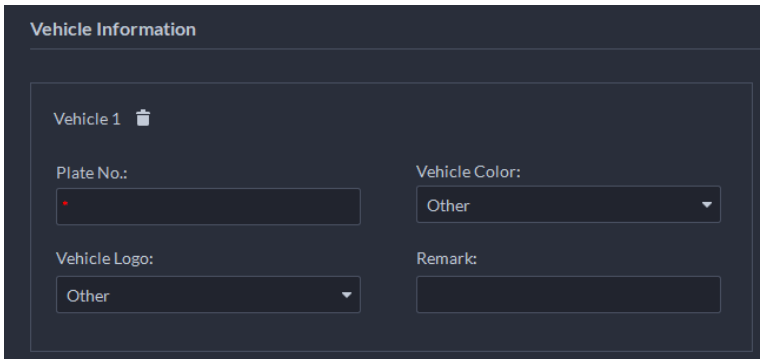
Icon	Description
	One can have 3 fingerprints, but only these fingerprints can be issued to devices. Click this icon, and then it turns into , which indicates that this fingerprint has been set as a main one. To cancel the main fingerprint setting, click .
	Set a fingerprint as duress fingerprint. When 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.

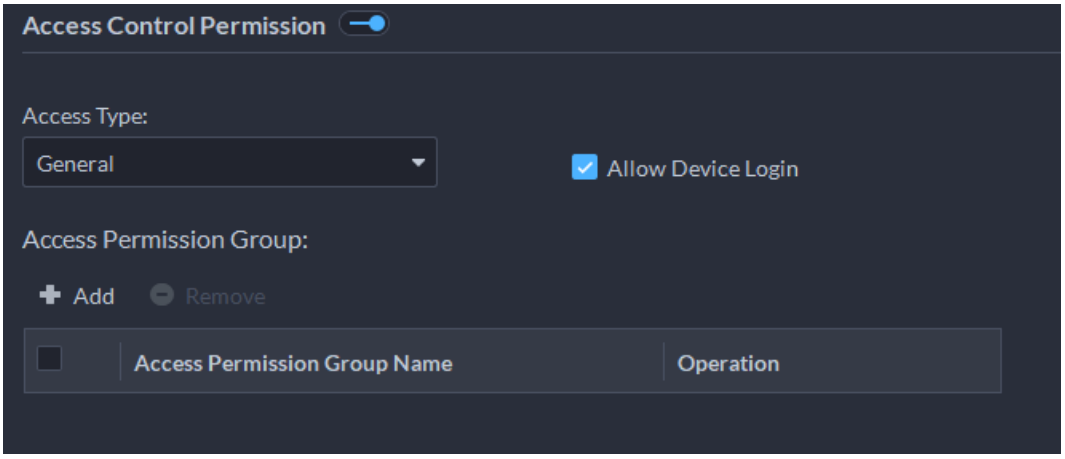
Figure 4-27 Add vehicle information



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 "4.4.1.1 Creating Face Comparison Group".

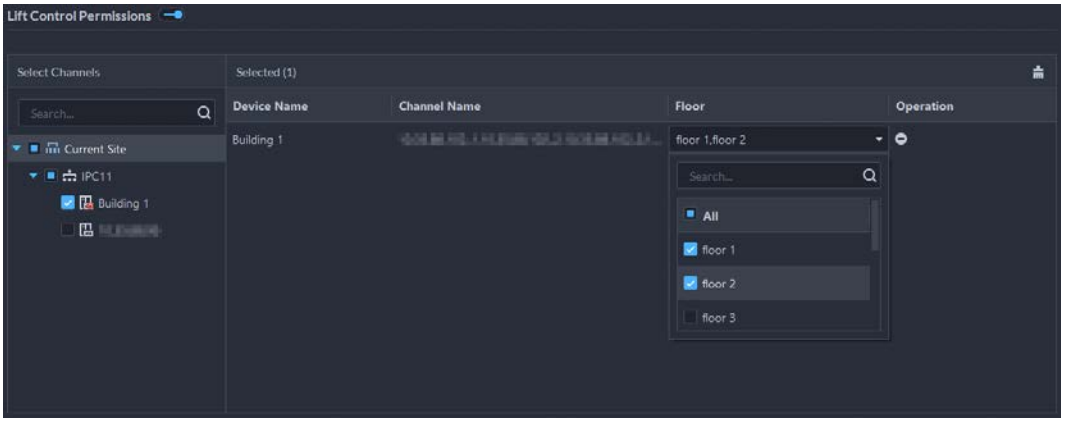
Figure 4-28 Add to access control permission group



Step 12 Enable **Lift Control Permissions** so that the person can use certain lifts.

1) Click next to **Lift Control Permissions**.
2) Select one or more lift control devices, and then select the floors this person can go to.

Figure 4-29 Lift control devices and floors

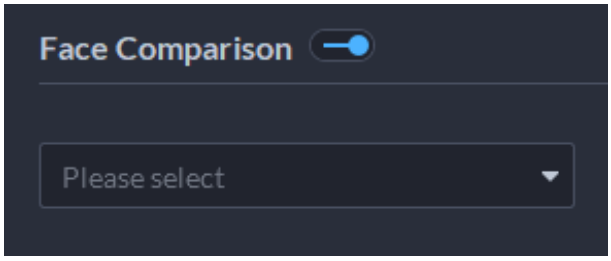


You need to create a face comparison group first.

Step 13 Enable **Face Comparison** to recognize the person by images.

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

Figure 4-30 Face comparison

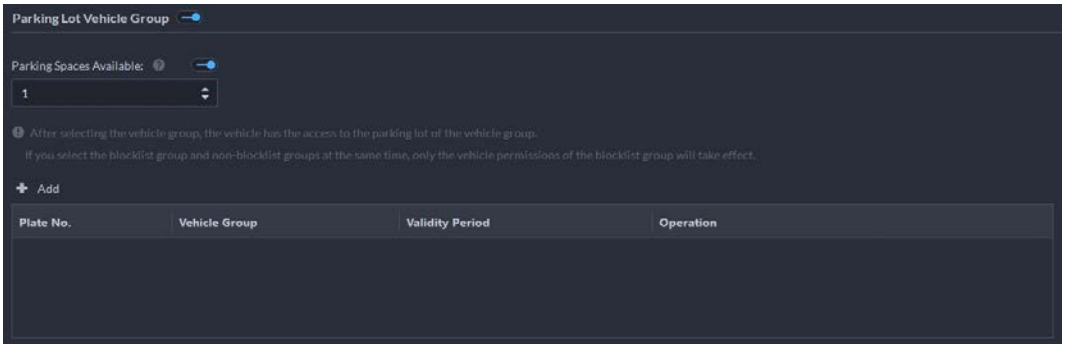


You need to create a face comparison group first.

Step 14 If the vehicle needs access to the parking lot, enable and configure **Vehicle Group** first.

1) Click next to **Parking Lot 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 4-31 Parking lot vehicle group



Step 15 Click **OK**.

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

Related Operations

- To edit basic information of a person, select the person, and then click .
- To delete a person:
  - Click 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 .
- To search for a person, enter key words in the .

4.3.1.2.2 Importing Personnel

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

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 10,000 people. The zip file cannot be larger than 1 GB.

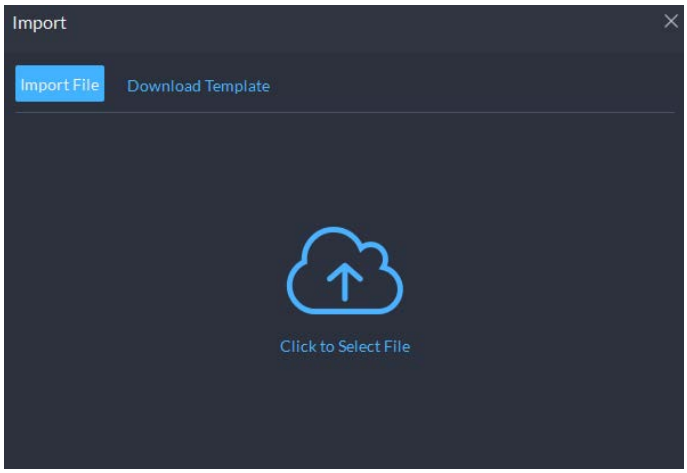
Procedure

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 4-32 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.

4.3.1.2.3 Extracting Personnel Information

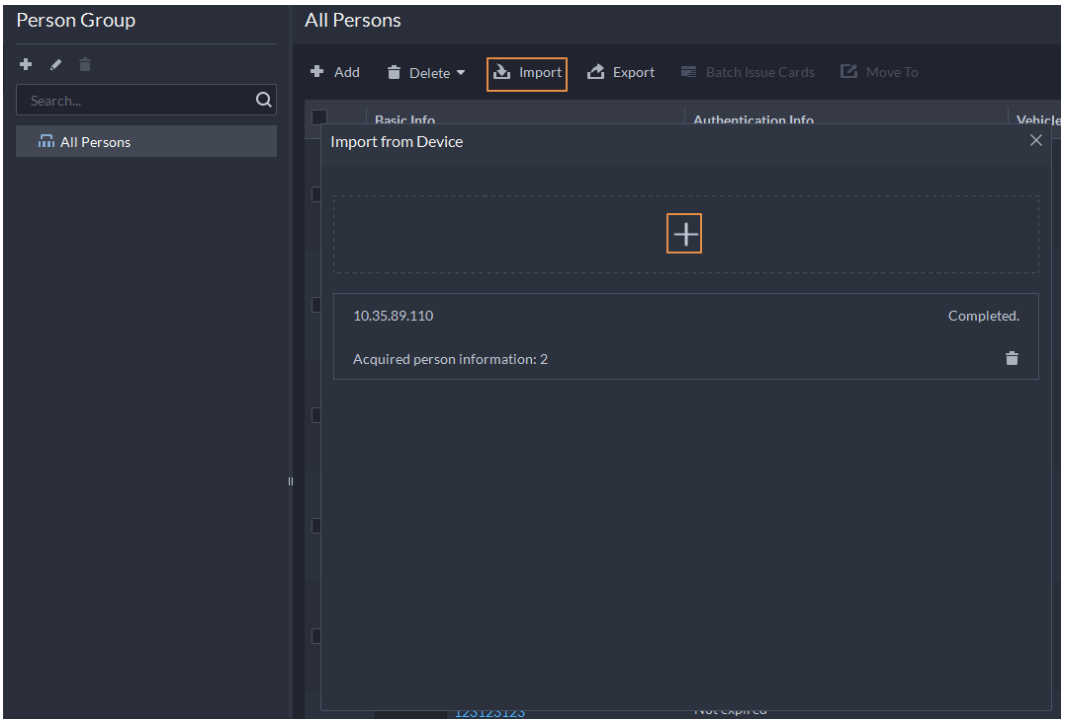
When personnel information has been configured on access control devices or door stations, you can directly synchronize the information to the platform.

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

Step 2 Click .

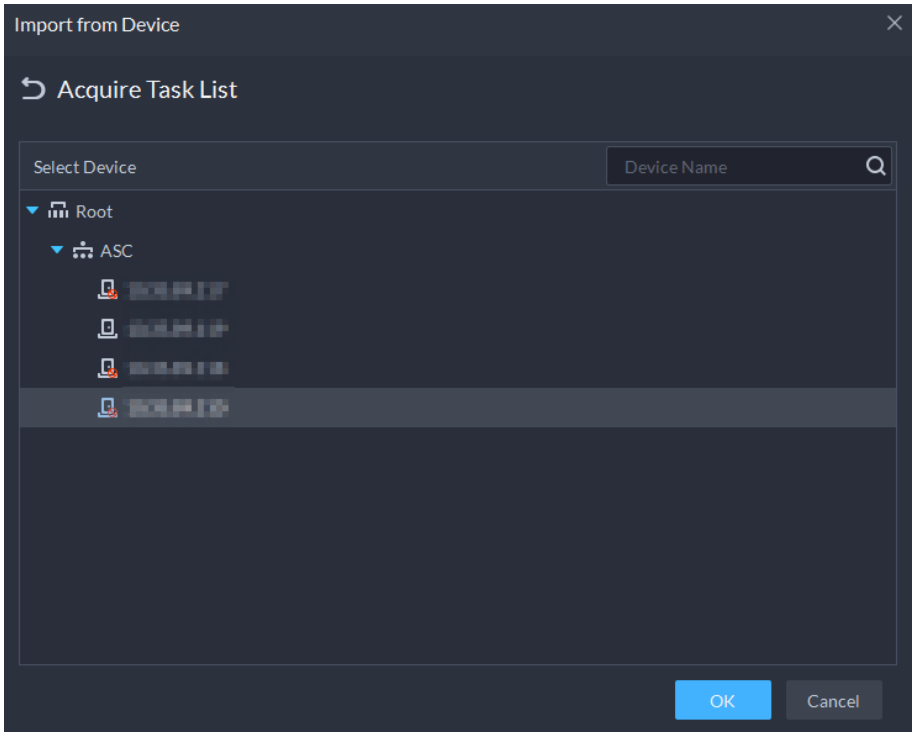
Step 3 Click **Import**, and then select **Import from Device**.

Figure 4-33 Import from device



Step 4 Click , select a channel from an access control device or door station, and then click **OK**.

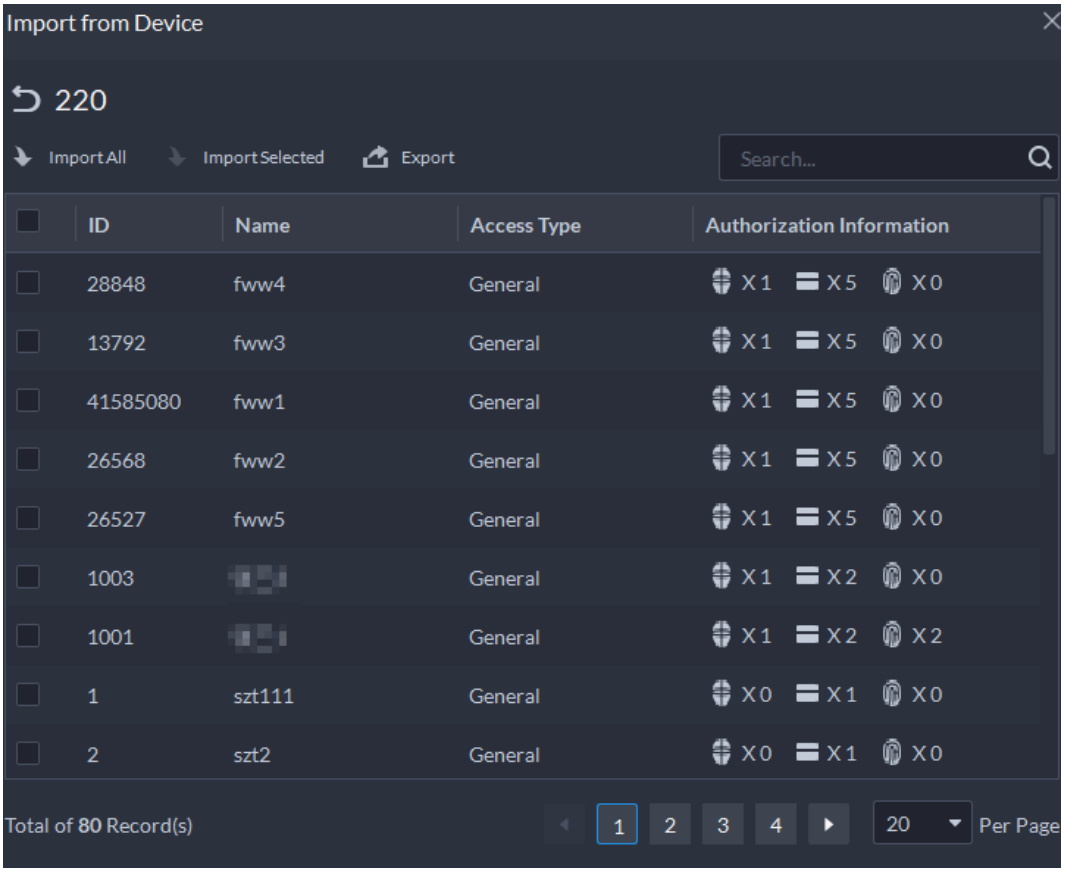
Figure 4-34 Extract task list



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

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

Figure 4-35 Personnel extraction results



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

selected.

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

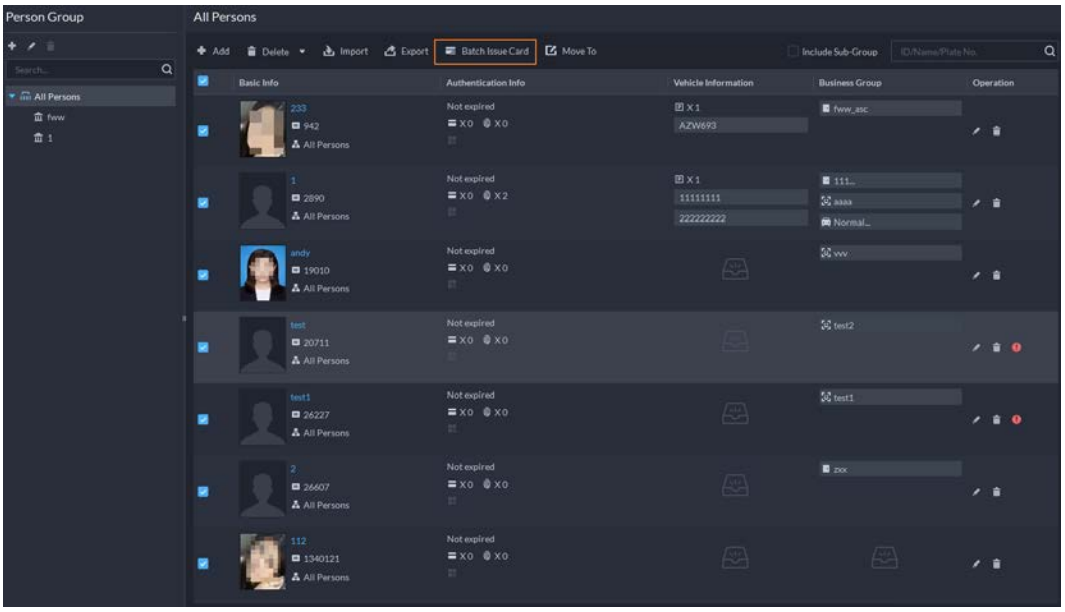
4.3.1.3 Issuing Cards in Batches

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

Step 2 Click .

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

Figure 4-36 Issue card in batches



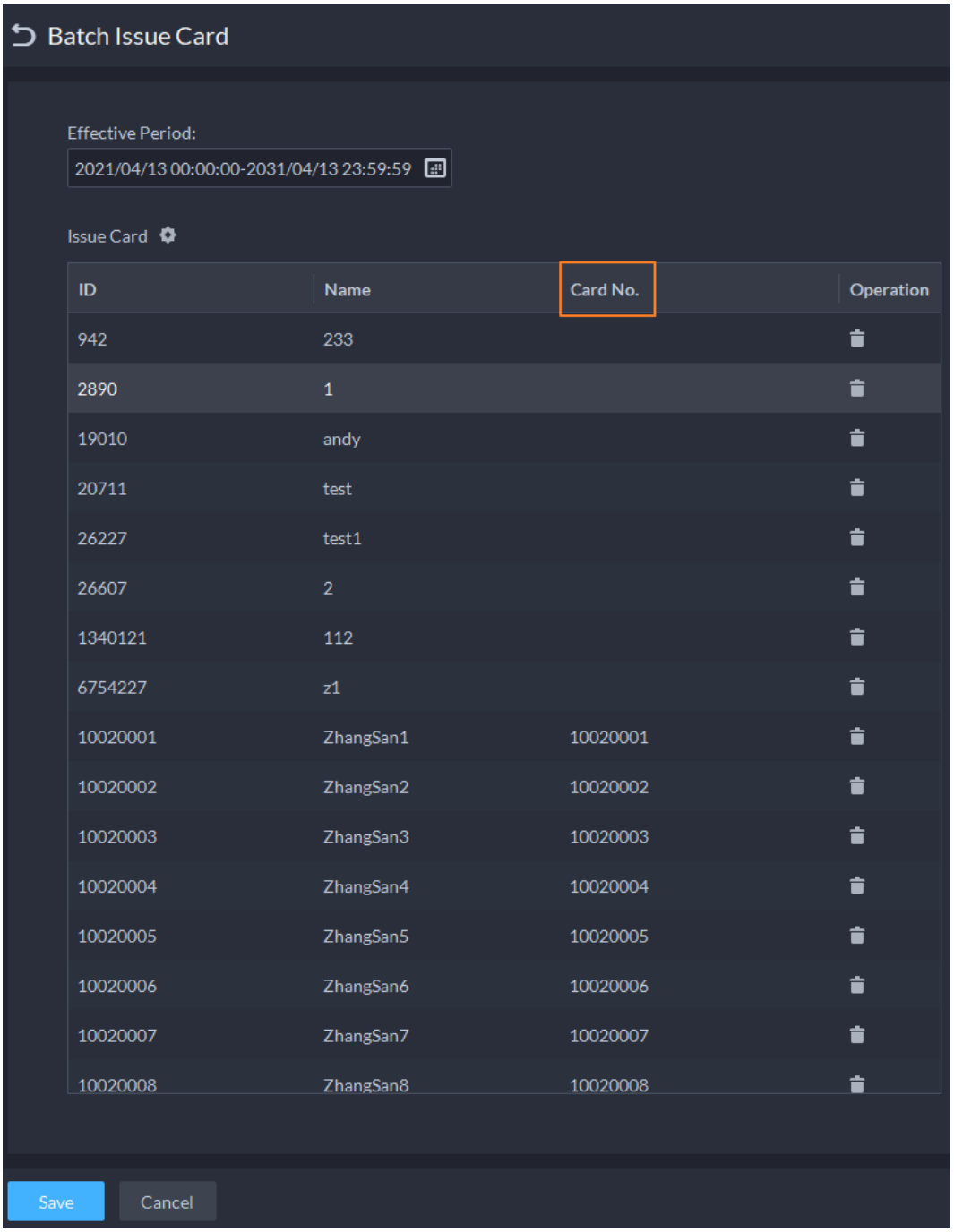
Step 4 Set term of validity.

Step 5 Issue cards to personnel.

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

- By entering card number

Figure 4-37 Enter card number

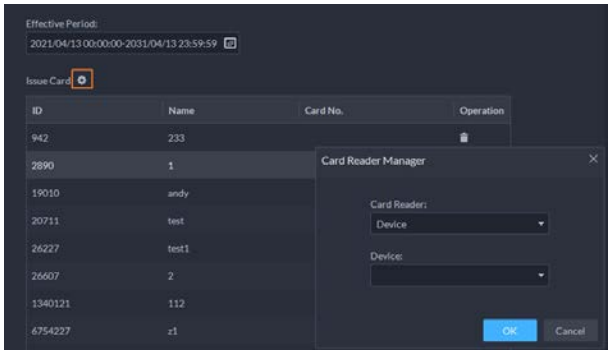


1) Double-click the **Card No.** input boxes to enter card numbers one by one.
2) Click **OK**.

- By using a card reader

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

Figure 4-38 Reader manager



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

4.3.1.4 Editing Personnel Information

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

Step 1 Log in to the DSS Client. On the **Home** 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 "4.3.1.2.1 Adding a Person".

4.3.2 Vehicle Management

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

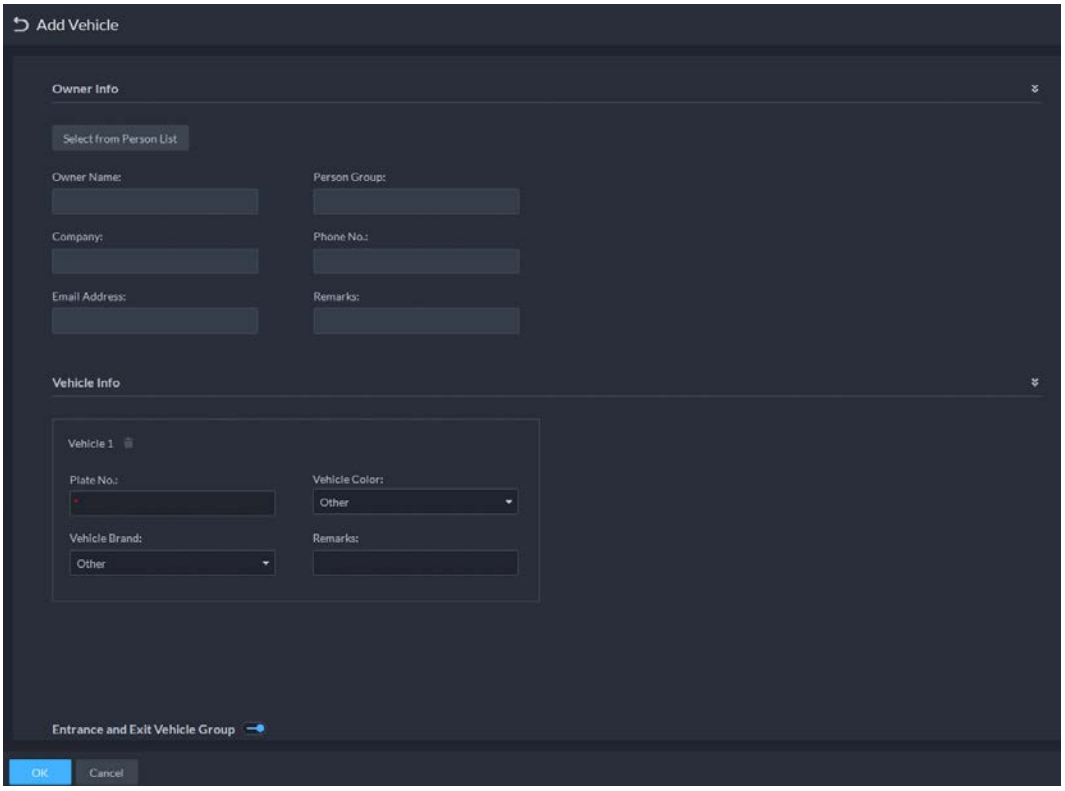
Procedure

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 4-39 Add vehicle information

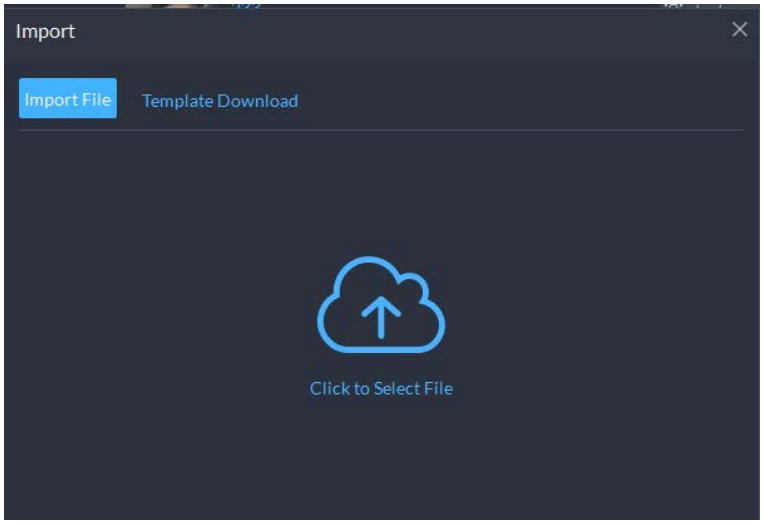


- Add vehicles one by one
  1. Enter **Owner Info** of the vehicle by clicking **Select from Person List**.
  2. Enter **Vehicle Info** such as plate number (required and unique), vehicle color, brand and more. After selecting owner, you can add multiple vehicles.
  3. Click  to enable **Parking Lot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

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

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

Figure 4-40 Download template



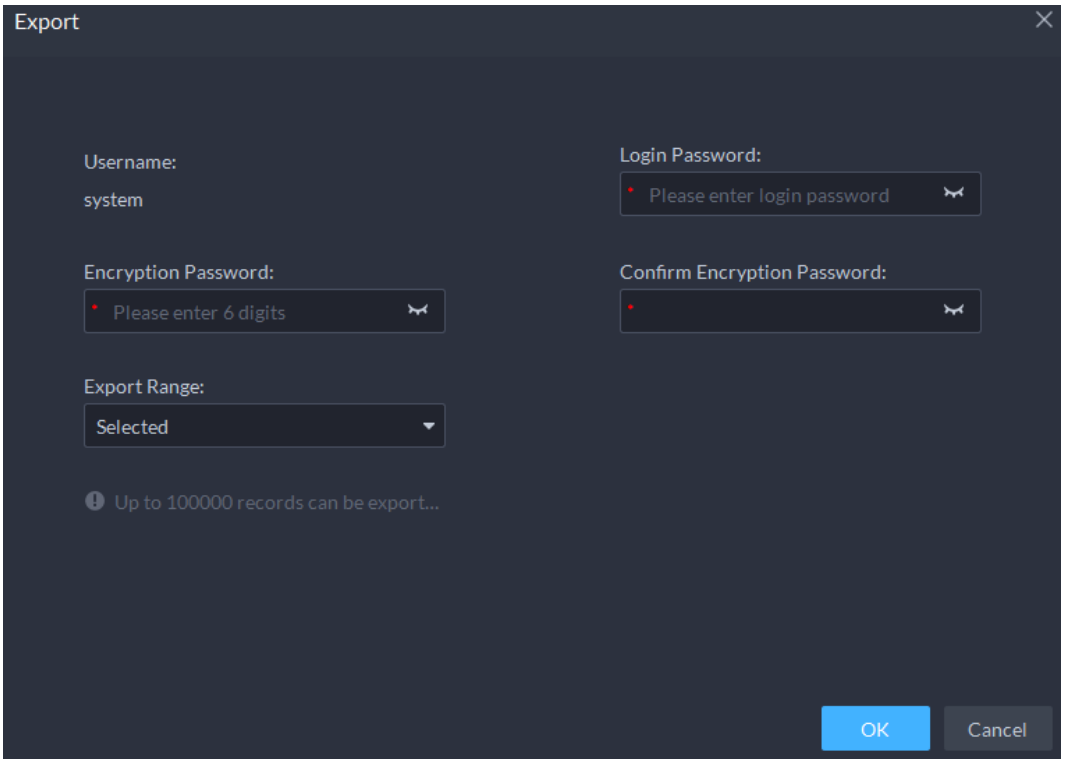
2. Fill in the template, and then select **Import** > **Import File**. Click to select the file and import.

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

Step 4 Click **OK**.

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

Figure 4-41 Export vehicle information



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

Related Operations

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

4.4 Watch List Configuration

Configure face and vehicle watch list for future investigation.

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

4.4.1 Face Watch List

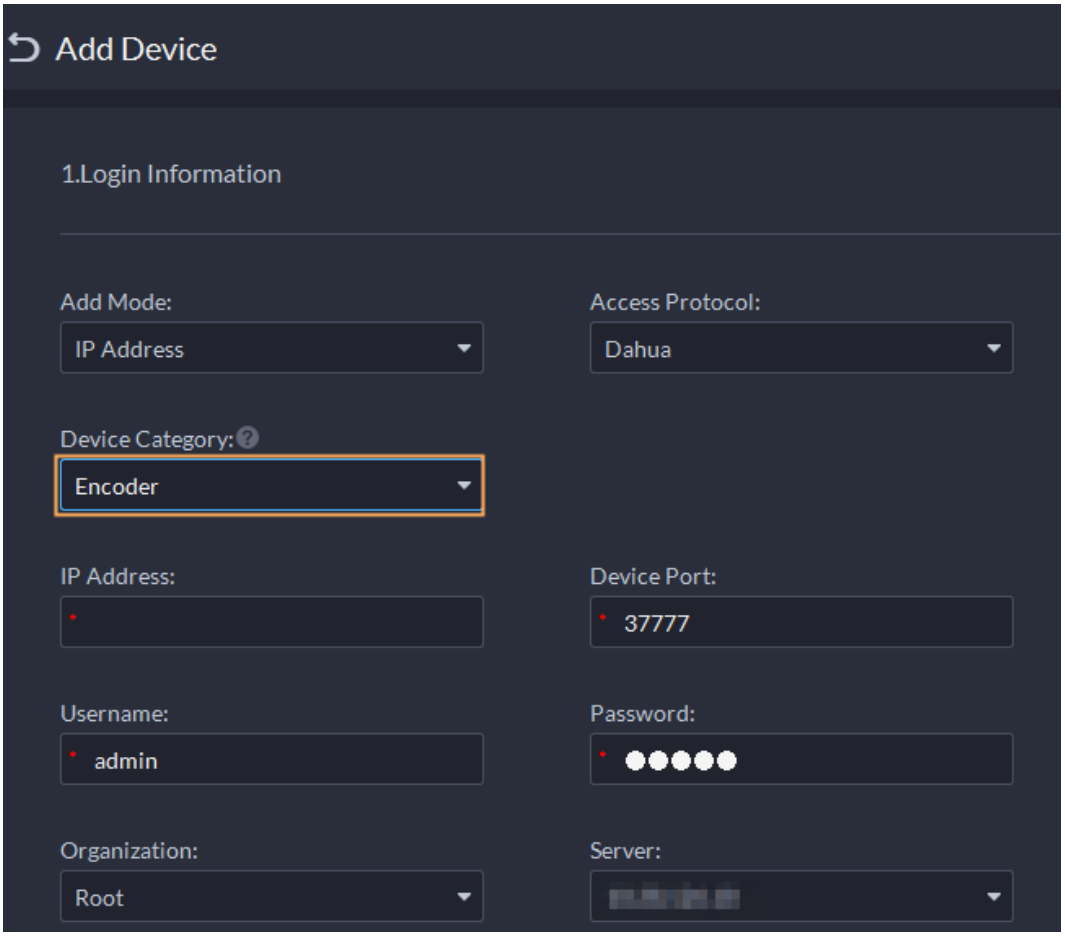
Configure face watch list and issue the list to devices for recognition and alarm.

4.4.1.1 Creating Face Comparison Group

Prerequisites

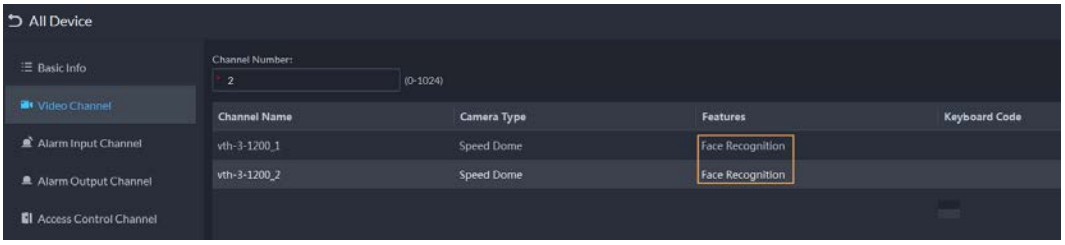
- Make sure that the devices for face recognition have been successfully configured onto the Platform.
- Make sure that the basic configuration of the Platform has completed. For details, see "3 Basic Configurations". During the configuration, you need to pay attention to following parts.
  - When adding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

Figure 4-42 Device category



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

Figure 4-43 Feature configuration



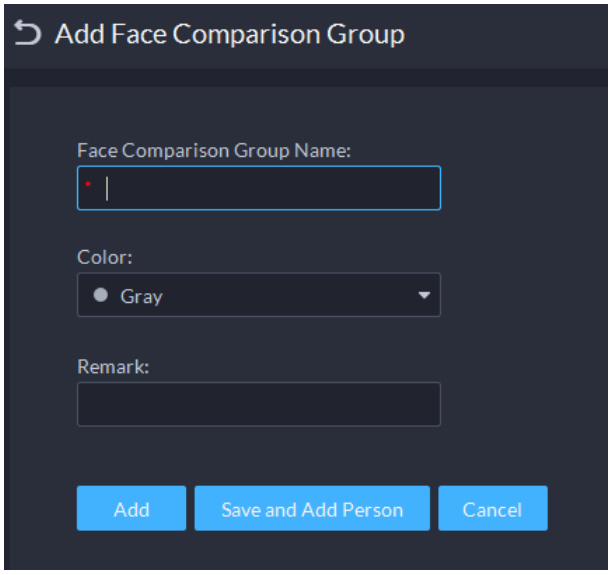
- Make sure that you have configured at least one disk with the type of **Images and Files** to store face images. Otherwise, the snapshots cannot be displayed.

Procedure

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

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

Figure 4-44 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.

4.4.1.2 Adding Face

Add person in the created comparison group.

Procedure

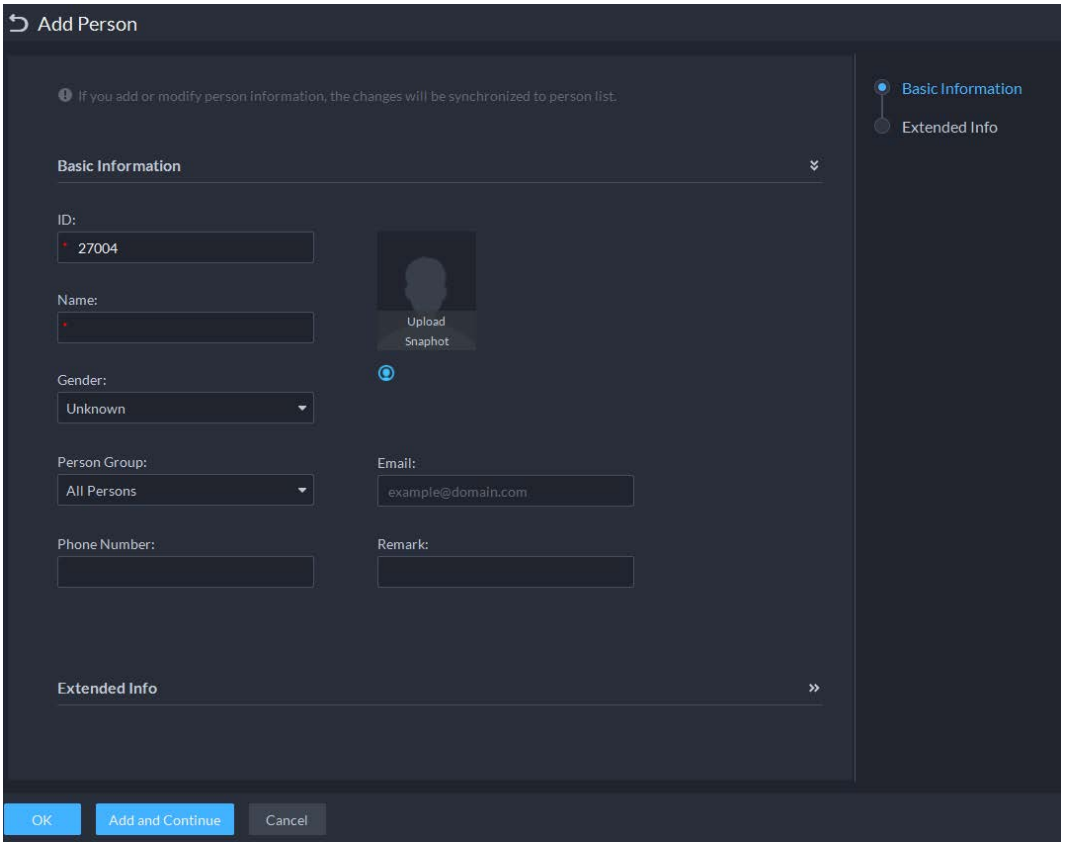
Step 1 Log in to the DSS Client. On the **Home** page, click , and then click **Watch List**.

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.

Figure 4-45 Add a person



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

Step 5 Click **OK**.

- Click at the bottom of the created group to add people one by one.
- Click 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 to edit the person information.
- Click to delete person from the group and face library one by one.
- Click to remove person from the group but keep it in the face library. You can also select multiple people and then click **Remove** at the top to remove in batches.

4.4.1.3 Arming Face

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

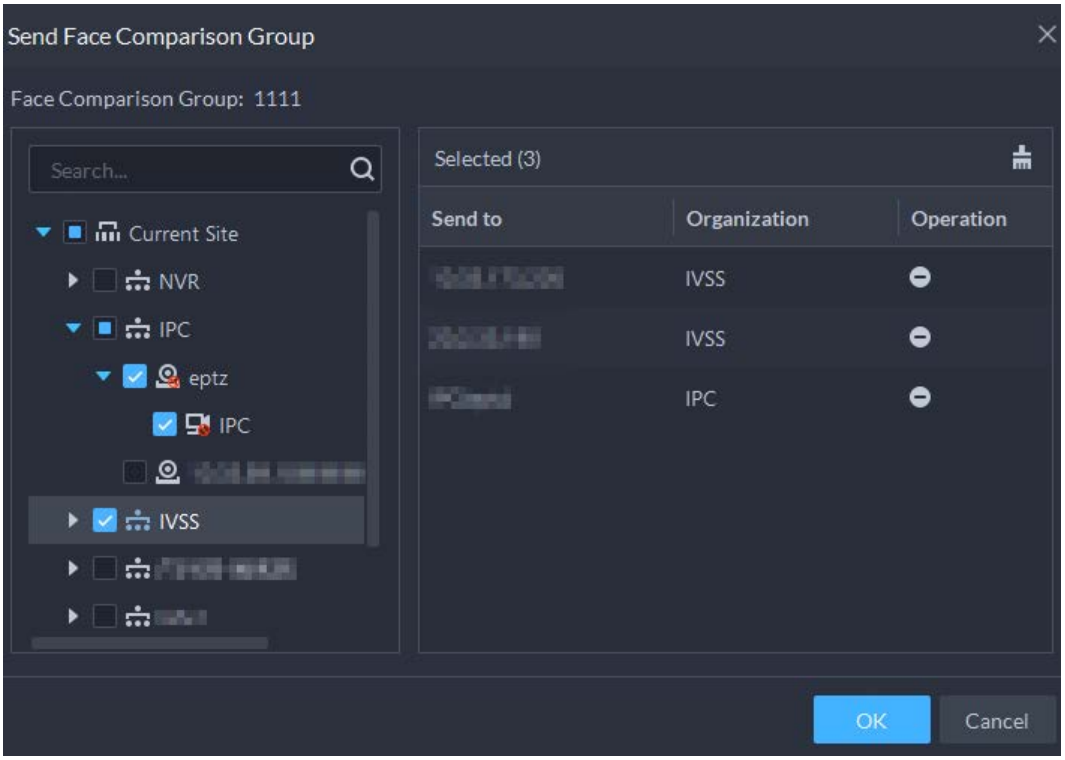
Step 1 Log in to the DSS Client. On the **Home** page, click , and then click **Watch List**.

Step 2 Click , and then click 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 to see the reason.

Figure 4-46 Send face comparison group

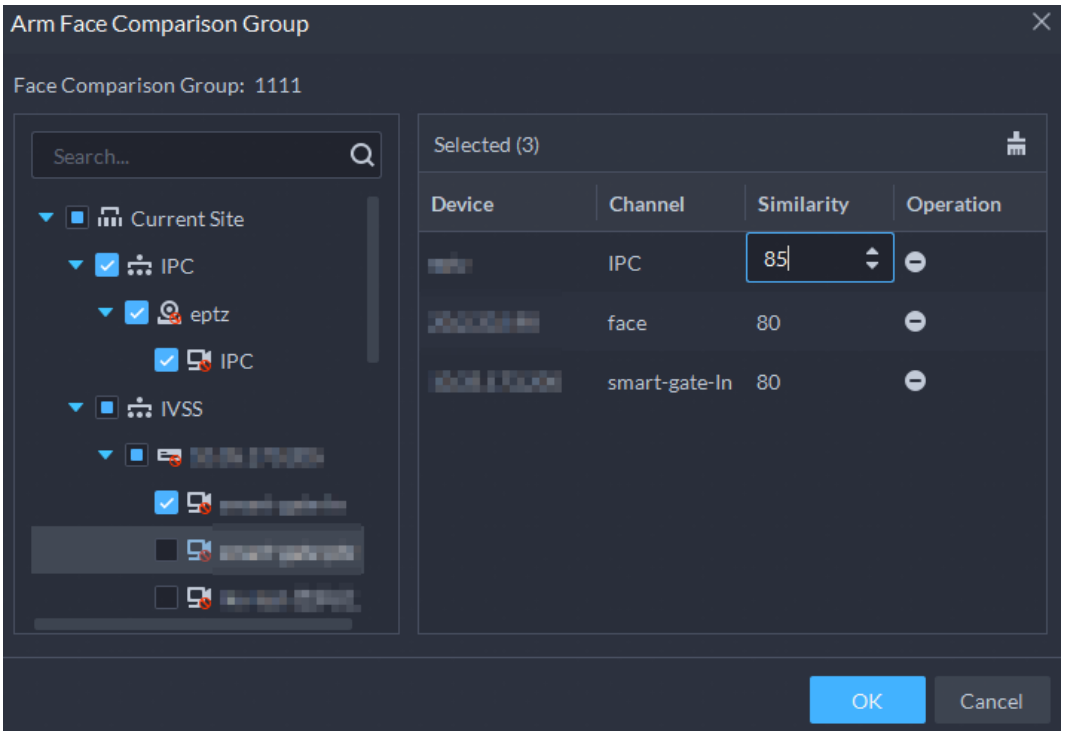


Step 4 After the face watch list is successfully sent, click **Next Step**.

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 4-47 Arm face comparison group



Step 6 Click **OK**.

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

1) Click to view why arming failed and address the issue.
2) Click **Send Again** to arm the face comparison group again.

4.4.2 Vehicle Watch List

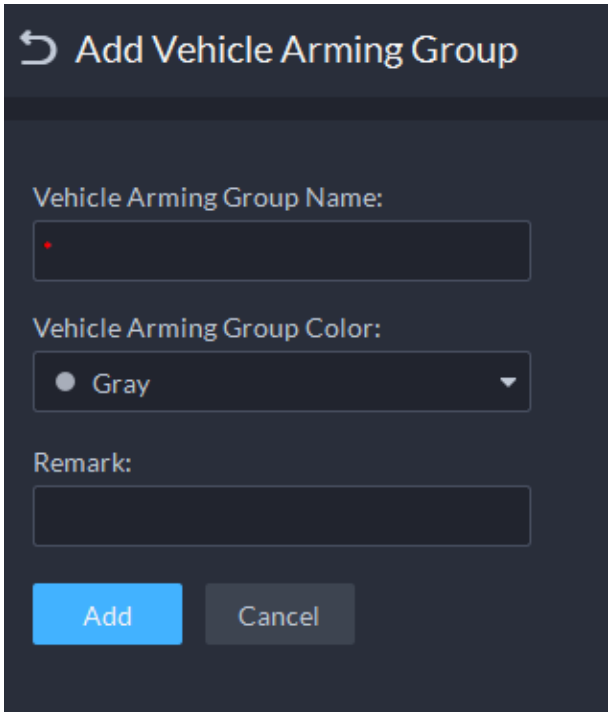
Create vehicle comparison group and add vehicles in, together with **Event** configuration, you can link devices like ANPR camera to recognize and reports to the Platform.

4.4.2.1 Creating Vehicle Arming Group

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

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

Figure 4-48 Add a vehicle arming group



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

Related Operations

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

4.4.2.2 Adding Vehicles

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.

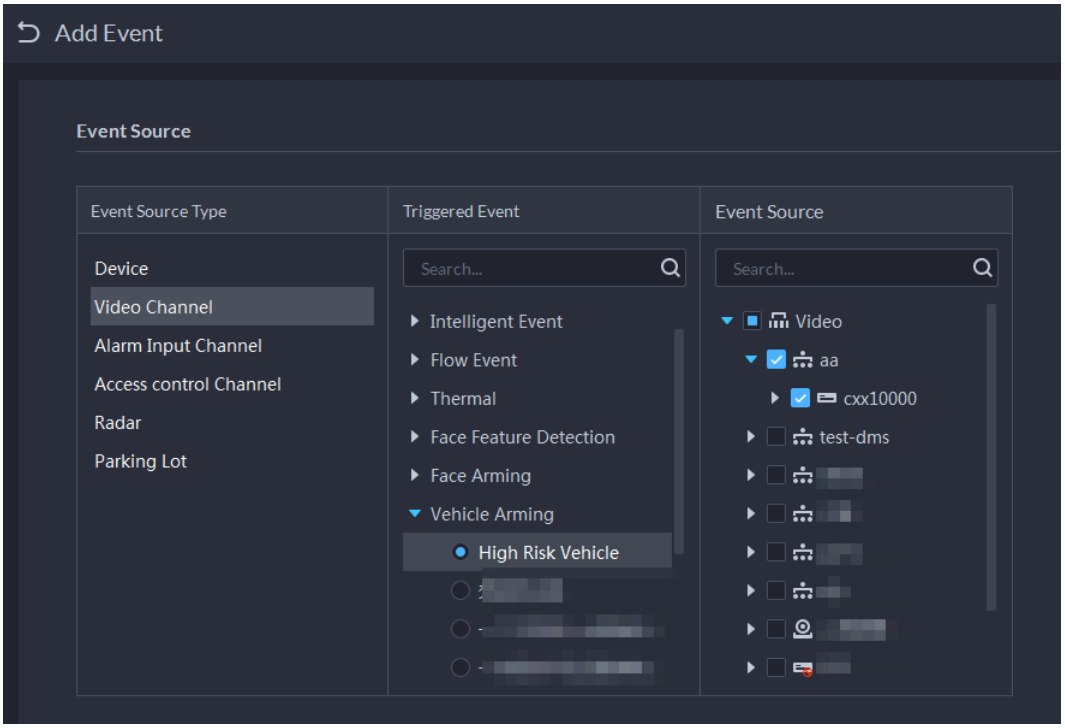
4.4.2.3 Arming Vehicles

Link ANPR camera or other devices which support plate recognition to arm watched vehicles in real

time. Once matched vehicles are detected, an alarm is triggered and reported to the Platform.

Log in to the DSS Client. On the **Home** page, click , and then arm the vehicle on the **Event** page. Click **Add**. For how to configure events, see "4.1 Configuring Events".

Figure 4-49 Arm vehicle event



4.5 Access Control

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

4.5.1 Preparations

Make sure that the following preparations have been made:

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

4.5.2 Configuring Door Groups

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

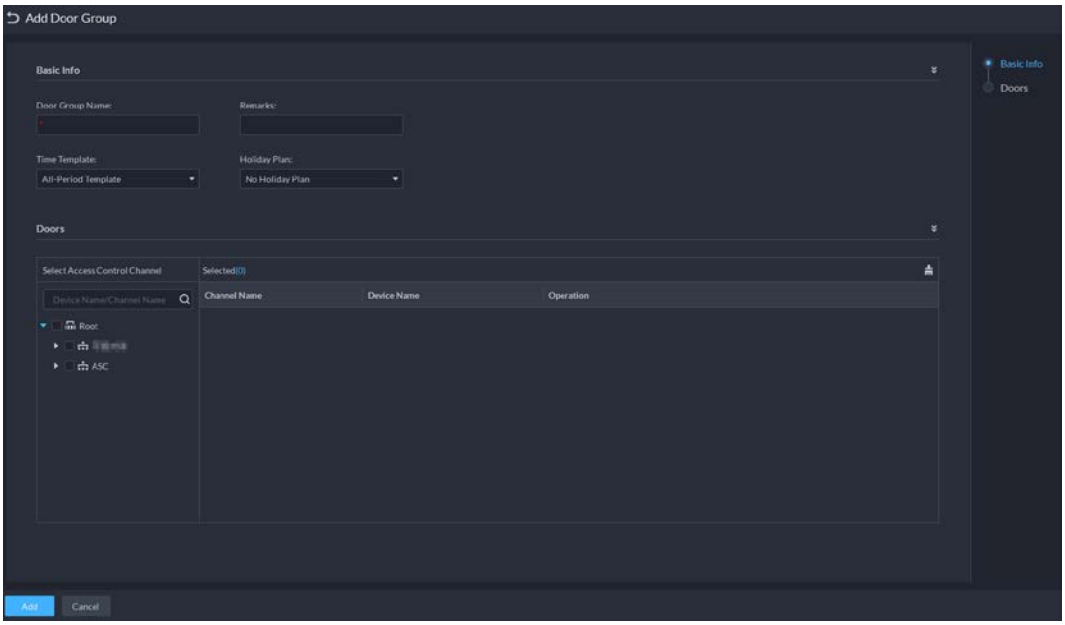
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control**.

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 4-50 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**.

4.5.3 Configuring Access Permission Groups

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

Procedure

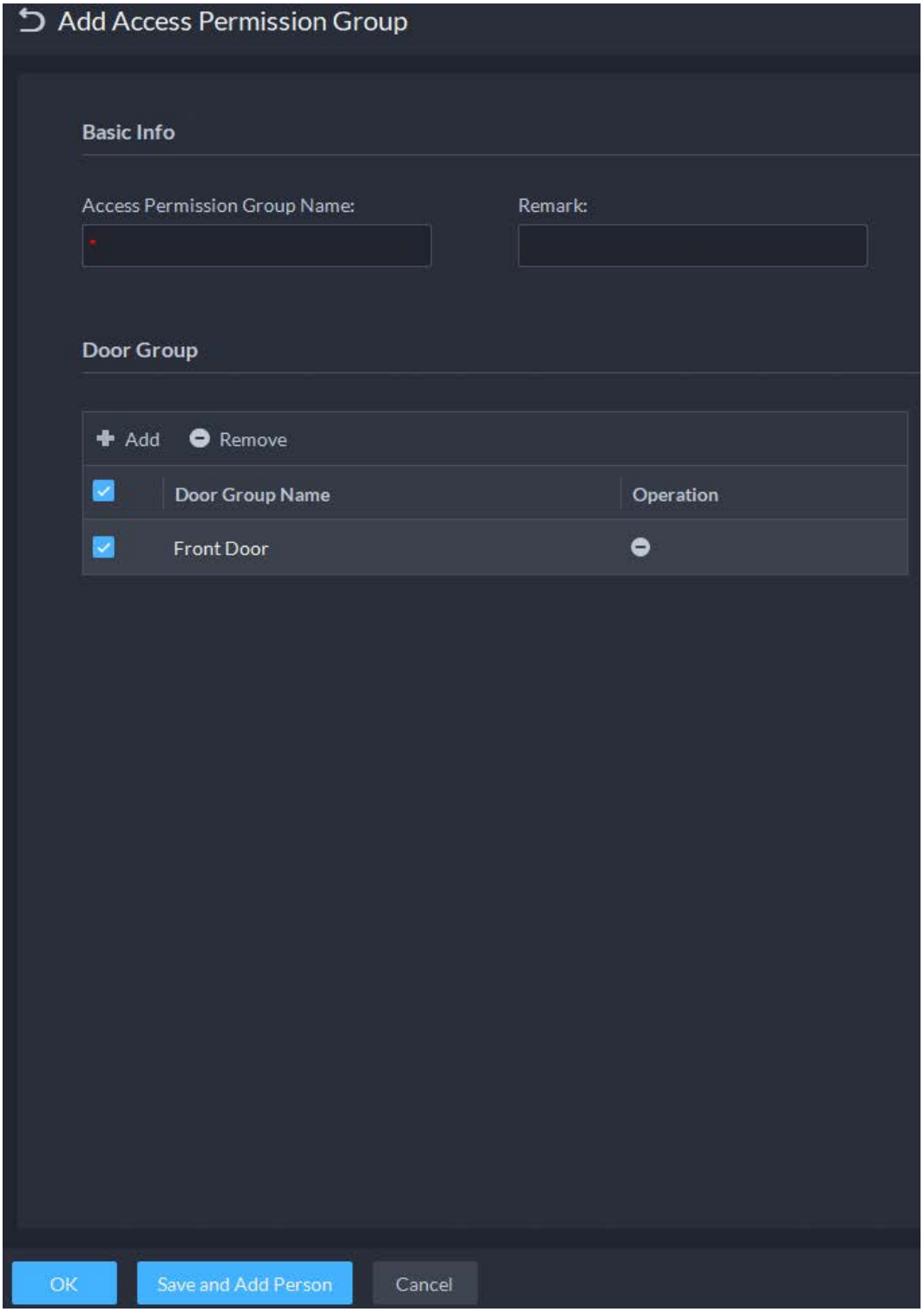
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control**.

Step 2 Click .

Step 3 Create an access permission group.

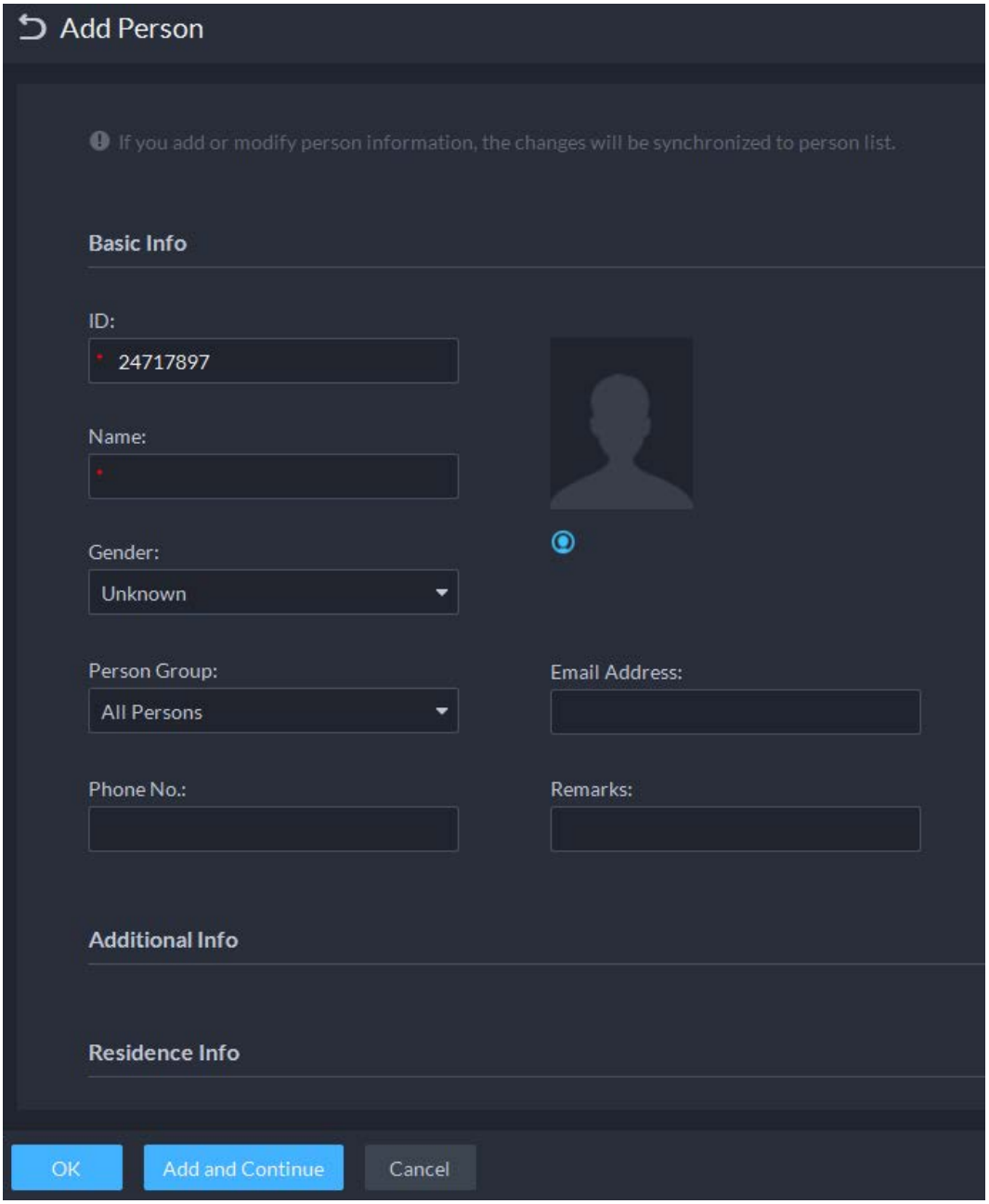
1) Click **Add** at the upper-left corner.

Figure 4-51 Add an access permission group



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

Figure 4-52 Add a person



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

Related Operations

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

4.5.4 Configuring Public Passwords

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

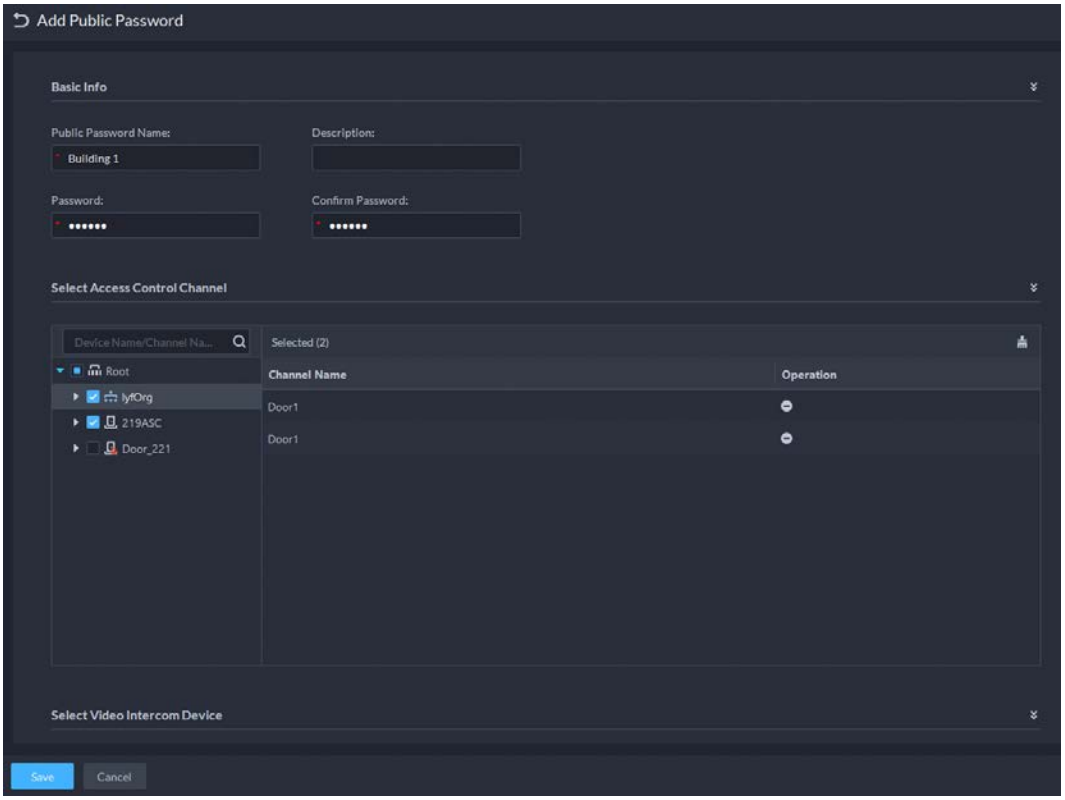
Only second-generation access control devices and video intercom devices support this function.

Step 1 Log in to the DSS Client. On the **Home** 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 4-53 Add a public password



Step 4 Click **Save**.

4.5.5 Configuring Advanced Functions

4.5.5.1 First Card Unlock

Only after the specified first-card user swipes the card every day can other users unlock the door with their cards. You can set up multiple first-card users.

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 **First Card Unlock** tab.

Step 4 Click **Add**.

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

Figure 4-54 First card unlock configuration

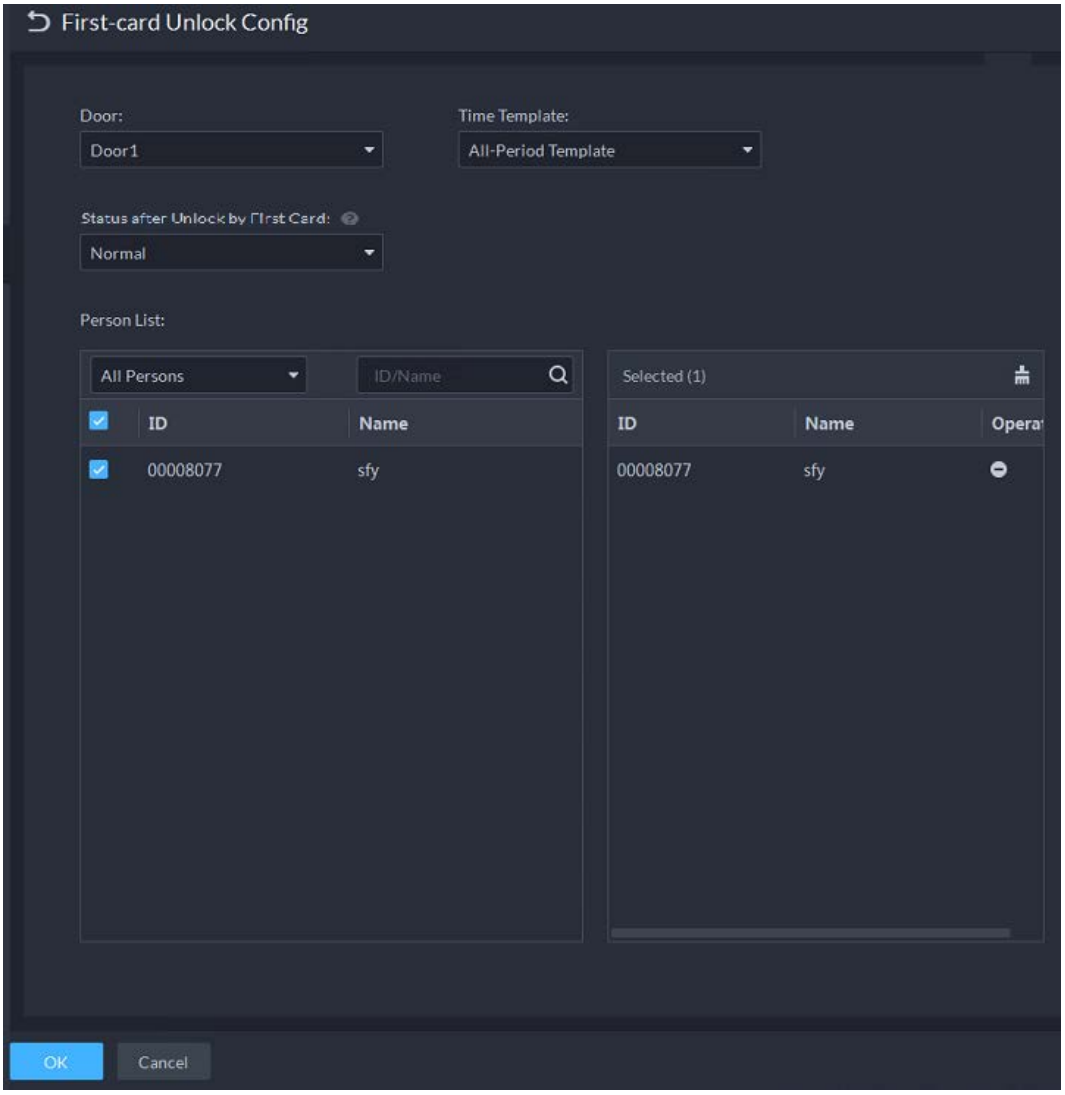


Table 4-4 Parameters

Parameter	Description
Door	You can select which access control channel to use the first-card unlock function.
Time Template	First-card unlock is valid in the time period of the selected time template.
Status	After first-card unlock is enabled, the door is in either the Normal mode or Always Open mode.
User	You can select one or more users to be first-card unlock users. Any one of them swipes the card, and then other users can unlock the door.

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

4.5.5.2 Multi-Card Unlock

You can configure a door to be opened by a number of people in a defined order.

- You can add up to 50 people in a group. Each person can only be added to one group at the same time.

- If you enable the multi-card unlock function for a door channel, you can select up to 4 multi-card unlock groups of people to the door, but the number of people who need to verify their identifications cannot exceed 5.

- If the first-card unlock and multi-card unlock functions are enabled on a door channel at the same time, the platform will execute first-card unlock first.
- We do not recommend adding the people related to the first-card unlock function to a multi-card unlock group. If a person related to the first-card unlock function and also in a multi-card unlock function swipes a card, the platform will consider that the first-card unlock function is used.
- The access type of the people in a multi-card unlock group cannot be **VIP** or **Patrol**. This parameter is configured when adding people to the platform. See "4.3.1.2 Adding Personnel".

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

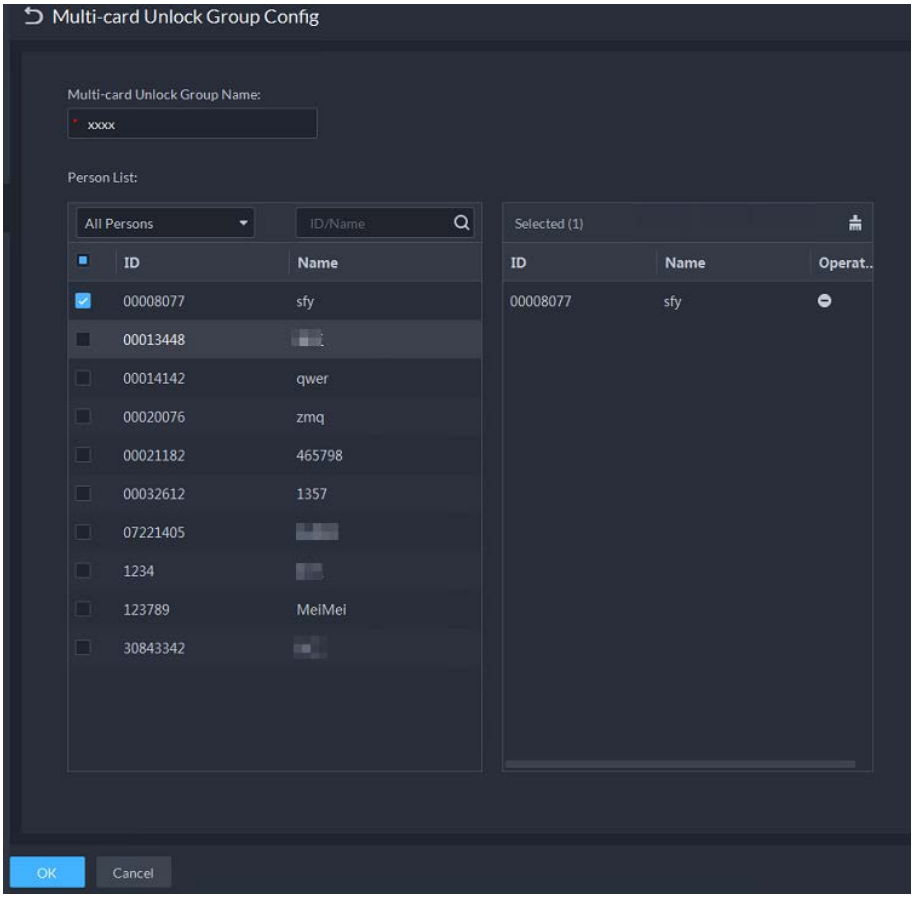
Step 2 On the **Access Control** page, click .

Step 3 Click the **Multi-card Unlock** tab.

Step 4 Add a user group.

1) Click **Add Multi-card Unlock Group**.
2) Click **Add**.
3) Enter the group name, select users from **User List** and then click **OK**.
   You can select up to 50 users.

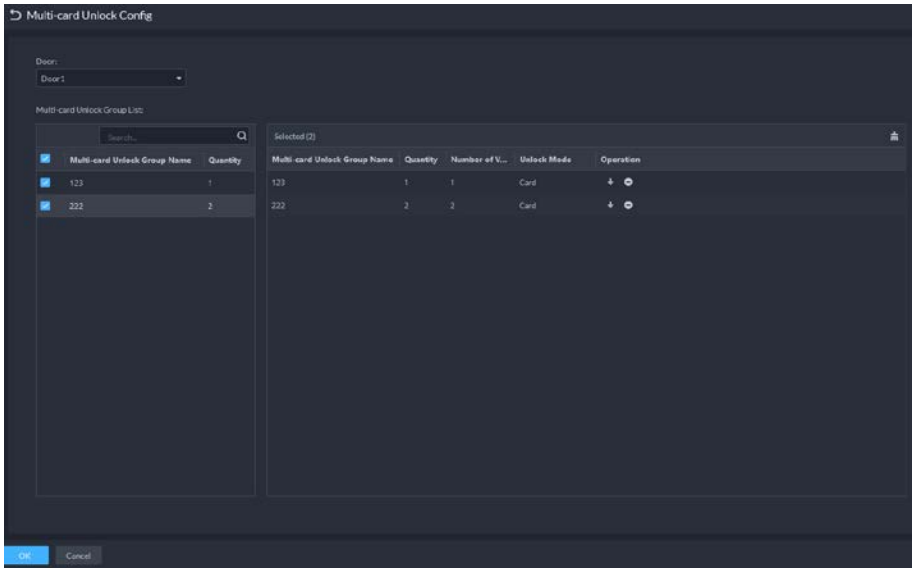
Figure 4-55 Multi-card unlock group configuration



Step 5 Configure the multi-card unlock function.

1) Go back to the **Multi-card Unlock** page, and click **Add**.
2) Select the door to use the multi-card unlock function.
3) Select the user group. You can select up to four groups.

Figure 4-56 User group information



4) Fill in the **Valid Quantity** for each group to be on site and the **Open Door Mode**. Click or to adjust the group order.
5) The valid quantity refers to the number of users in each group that must be on site to swipe their cards, user their passwords, or press their fingerprints.

   Up to five valid users are allowed.
6) Click **OK**.

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

4.5.5.3 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 4-57 Anti-passback parameters

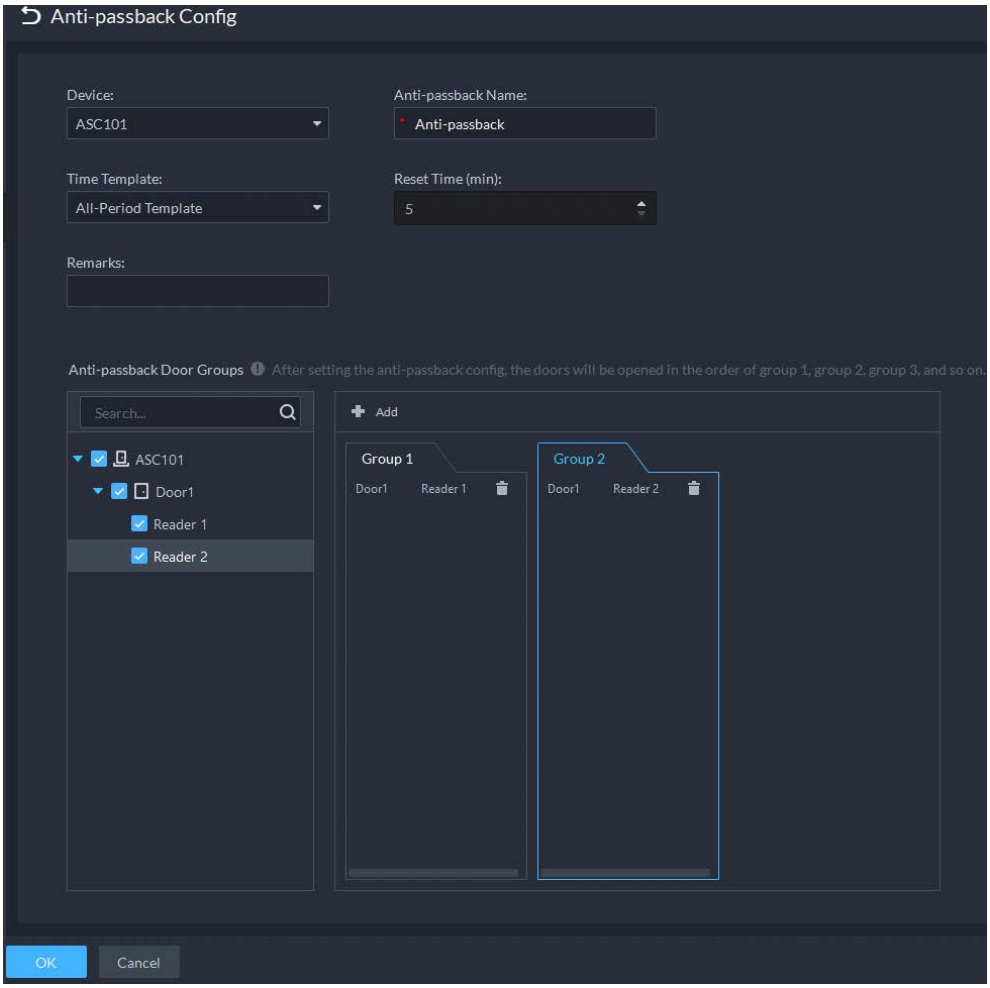


Table 4-5 User selection information description

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.

4.5.5.4 Multi-door Interlock

A regular access controller employs interlock within a group. To open one of the access control channels (under normal access control), other access control channels must be closed; otherwise the door cannot be unlocked. The A&C Central Controller employs interlock across groups, where the access control channels within the same group are not interlocked, and can all be opened. However, whenever an access control channel in a group is opened, no channels of other groups can be opened. The configuration steps in this chapter are for an A&C Central Controller.

Step 1 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 **Multi-door Interlock Config** tab.

Step 4 Click **Add**.

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

Figure 4-58 Multi-door interlock

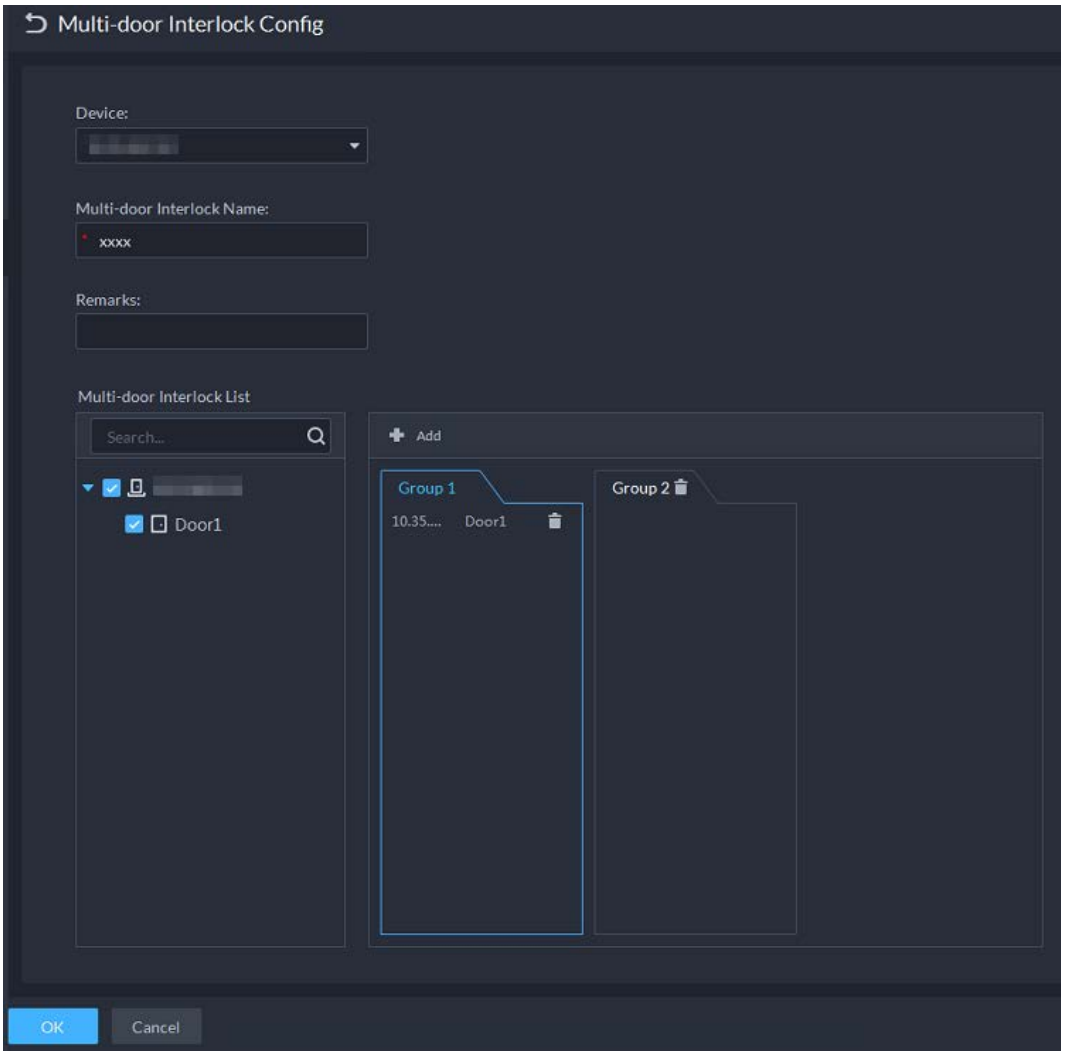


Table 4-6 Parameters

Parameter	Description
Device	You can select the device to set up inter-lock.

Parameter	Description	
Multi-door Interlock Name	You can customize the name of the inter-lock rule.	
Remark	Description information.	When the selected device is a multi-door controller, you must set up these parameters.
Multi-door Interlock List	You can set up inter-lock across different door groups. If a door in Group 1 is opened, no doors can be opened in Group 2 until all doors in Group 1 are closed. Supports up to 16 door groups, with up to 16 doors in each group.	

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

4.5.5.5 Remote Verification

For devices with remote verification, when users unlock the doors with card, fingerprint, or password in the specified time period, it must be confirmed on the platform client before the access controller can be opened.

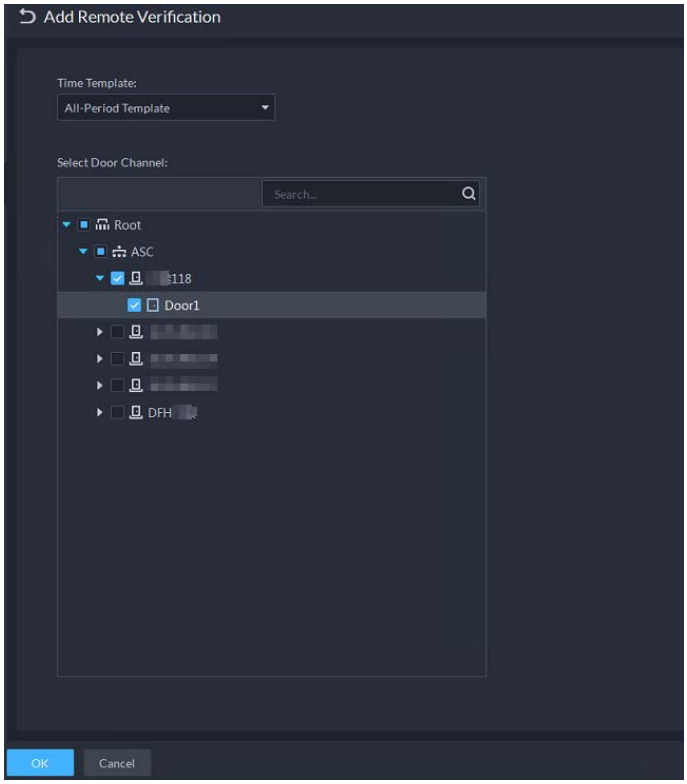
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Access Control**.

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

Step 3 Click the **Remote Verification** tab.

Step 4 Click **Add**.

Figure 4-59 Add remote verification



Step 5 Select **Time Template** and access control channel, and click **OK**.

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

After the setup, door unlocking by card, fingerprint, or password that takes place in the corresponding access control channel triggers a pop-up on the client.
You can choose to unlock the door or ignore it by clicking the corresponding button, and the pop-up automatically disappears.

4.5.6 Configuring Time Templates

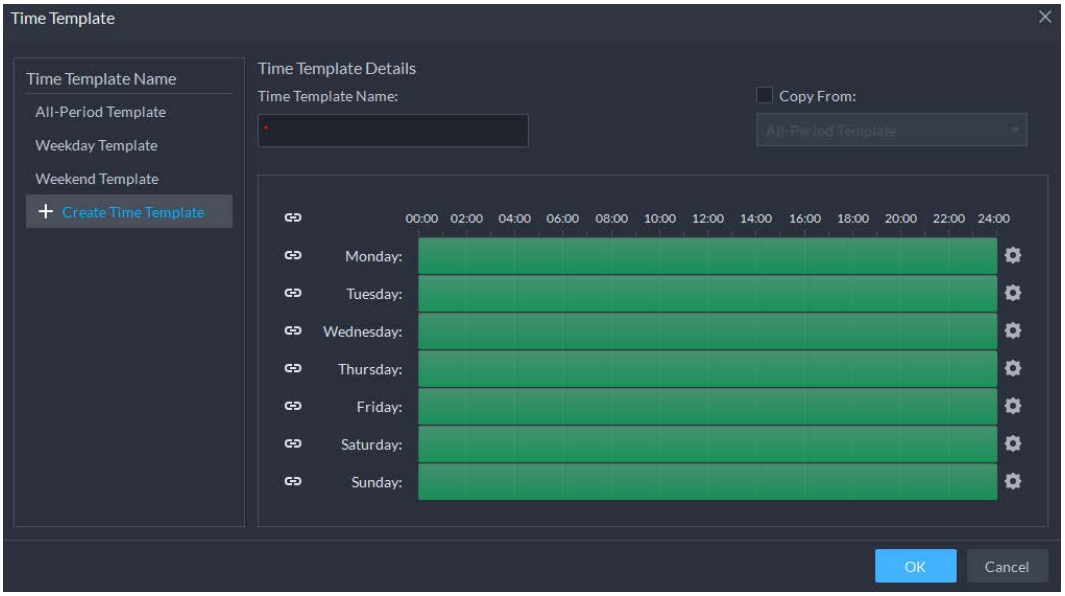
Configure time templates for different access control strategies. For example, employees can only gain access to their offices during work time.

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

Step 2 Click .

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

Figure 4-60 Time template



Step 4 Enter the template name, set time periods, and then click **OK**.
There are two ways to set time periods:

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

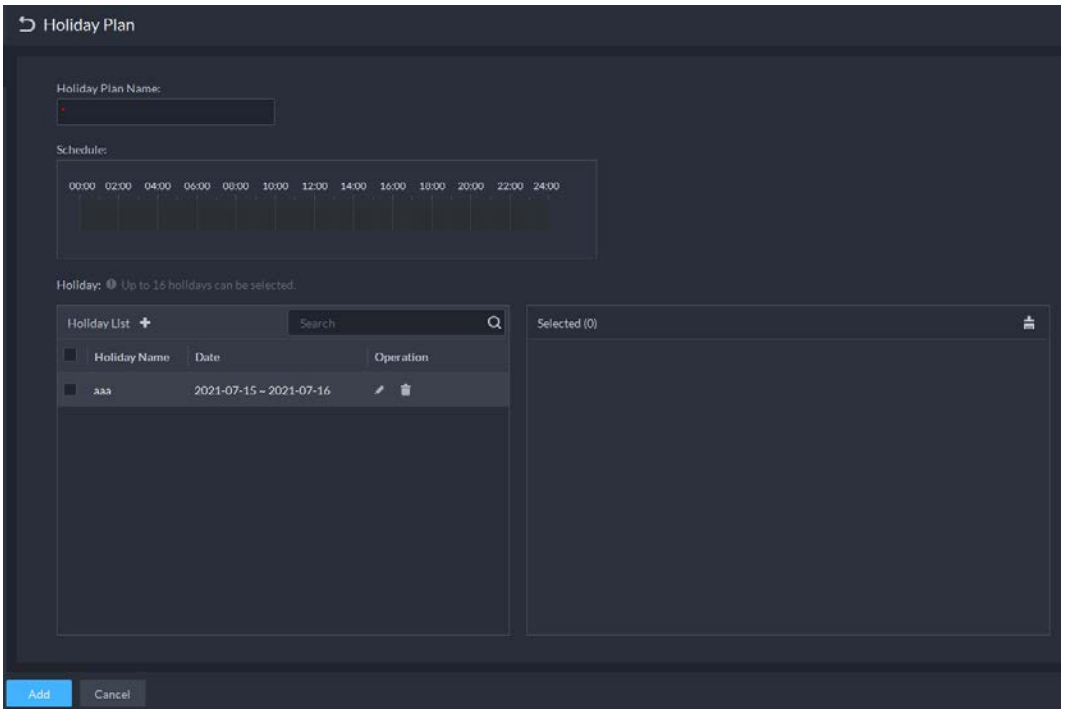
- You can add up to 6 periods for each day.
- To use an existing template, select the **Copy From** check box and then select a template in the drop-down list.

4.5.7 Configuring Holidays

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

Figure 4-61 Add a holiday schedule



Step 3 Configure the parameters.

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

Step 4 Click **Add**.

4.5.8 Configuring Access Control Devices

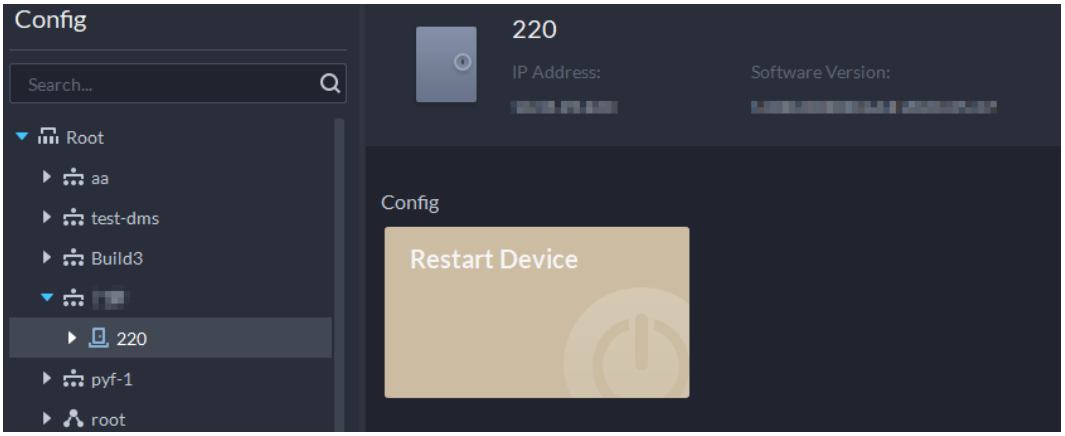
After an access control device is added, and if it is online, you can restart it, and synchronize its time with the platform.

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

Step 2 Click .

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

Figure 4-62 Select an access control device



Step 4 Configure the access control device.

- Click **Restart Device** to restart the device.
- Click at the upper-right corner to go to the web page of the device.

4.5.9 Configuring Door Information

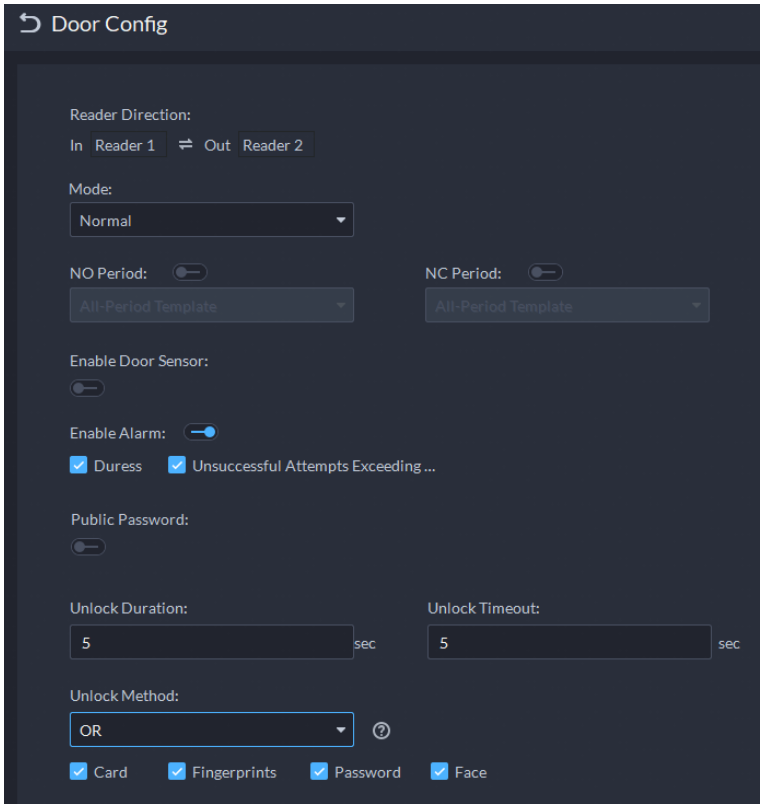
You can configure door status, Always-Open or Always-Close period, alarm and more.

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

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

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

Figure 4-63 Door configuration



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

Table 4-7 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 "4.5.4 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.
Multi-door interlock	Select whether to enable your multi-door interlock configuration. See "4.5.5.4 Multi-door Interlock".
Unlock Method	You can use any one of the methods, card, fingerprint, face, and password, or their combinations to unlock the door. • Select **And**, and select unlock methods. You can only open the door using all the selected unlock methods. • Select **Or** and select unlock methods. You can open the door in one of the ways that you configured. • Select **Unlock by period** and select unlock mode for each time period. The door can only be opened by the selected method(s) within the defined period.

4.6 Video Intercom

4.6.1 Preparations

Make sure that the following preparations have been made:

- Access control devices are correctly deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
  - ◇ When adding video intercom devices on the **Device** 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.

- The platform automatically creates a room after you add a VTH. For details, see "4.6.4 Configuring Room".
- Any configuration modification on the device will not be reported to the platform. You need to go to the device modification page of Web Manager to manually synchronize the modification.

4.6.2 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.

4.6.2.1 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.

4.6.2.2 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 , and then in the **App Config** section, select **Video Intercom**.

Step 2 Click .

Step 3 Click **Manager Group Config**.

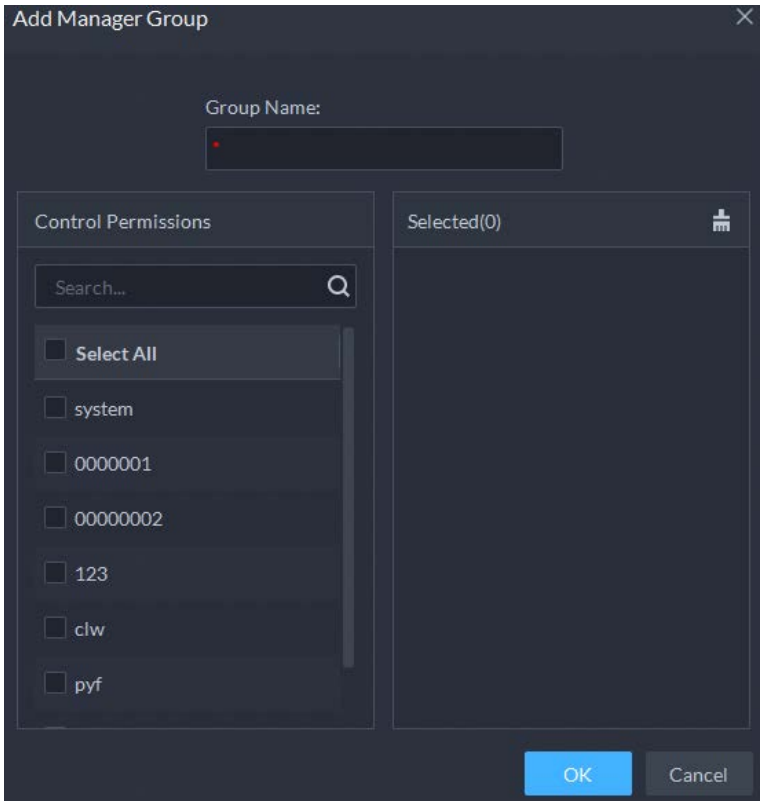
Step 4 Click **Add Group**.

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

Figure 4-64 Edit manager group



4.6.2.3 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 , and then in the **App Config** section, select **Video Intercom**.

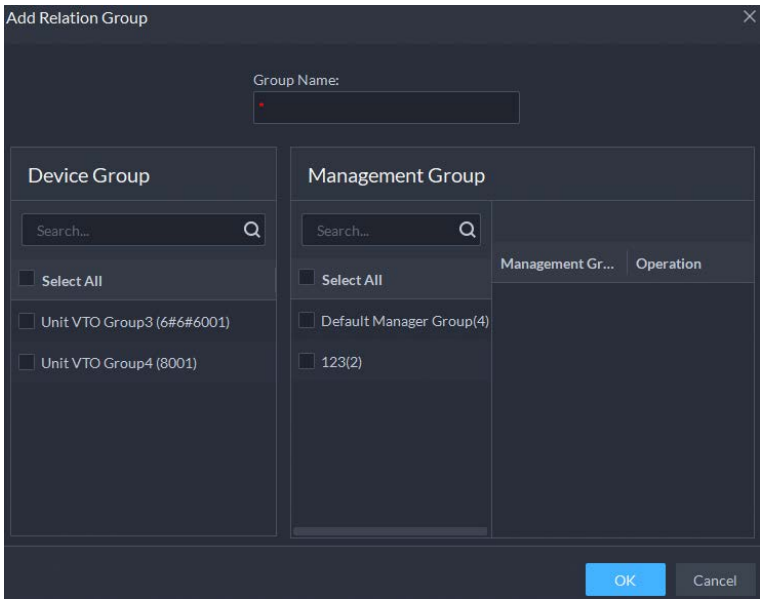
Step 2 Click .

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 4-65 Add a group relation



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

4.6.3 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 Configure the call mode.

- **Simultaneous Call**: When a room is being called, all the VTHs and App users in it will receive the call. If there are only App users in the room, then all App users will receive the call.
- **Group Call**: When calling a room, only the VTHs in it will receive the call. If call

forwarding is enabled on the VTHs, then all App users will receive the call.

Step 5 Click **Save**.

4.6.4 Configuring Room

Add a room to include the VTHs and App users in it.

When you add a VTH to the platform, the platform will automatically create a room. You can also create a room and add the VTH later. The VTH will automatically join the corresponding room. The rooms that are automatically created cannot be deleted. You can only delete those that are manually created.

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

Step 2 Click **Add**.

Step 3 Select an organization, enter a name for the room and the room number, and then click **Add**.

If the VTH with the same room number has been added to the platform, or the homeowner with the same room number has registered, the VTH or the App user will join the room automatically.

Related Operations

Operations on the App users:

- : Set an App user to be the homeowner after it is linked with a person.
- : Reset the password of an App user. The App user will need to log in to the App with the new password.
- : Link an App user to a person.
- : Delete an App user.

4.6.5 Synchronizing Contacts

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

4.6.6 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.

4.6.7 QR Codes

Configure the information of the QR codes that are used by homeowners to download the App and register an account.

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

Step 2 Enter a name and some notes for your community, and then click **Save**.

Homeowners can scan the **QR Code for App Download** to download and install the App on the phone, and then scan the **QR Code for App Registration** to register. For how to register, see the user manual of the App.

4.6.8 App User

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

Prerequisites

App users have registered by scanning the QR code on the platform or the VTH. For details, see the user manual of the App.

Procedure

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 4-8 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.

4.7 Attendance Management

Configure attendance devices, attendance shifts and periods, so as to manage attendance records and reports.

4.7.1 Preparations

Make sure that the following preparations have been made:

- Attendance devices are correctly deployed. For details, see the corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
  - When adding attendance devices on the **Device** page, select **Access Control** as the device category.
  - Personnel information is added correctly. For details, see "4.3.1 Configuring Personnel Information".

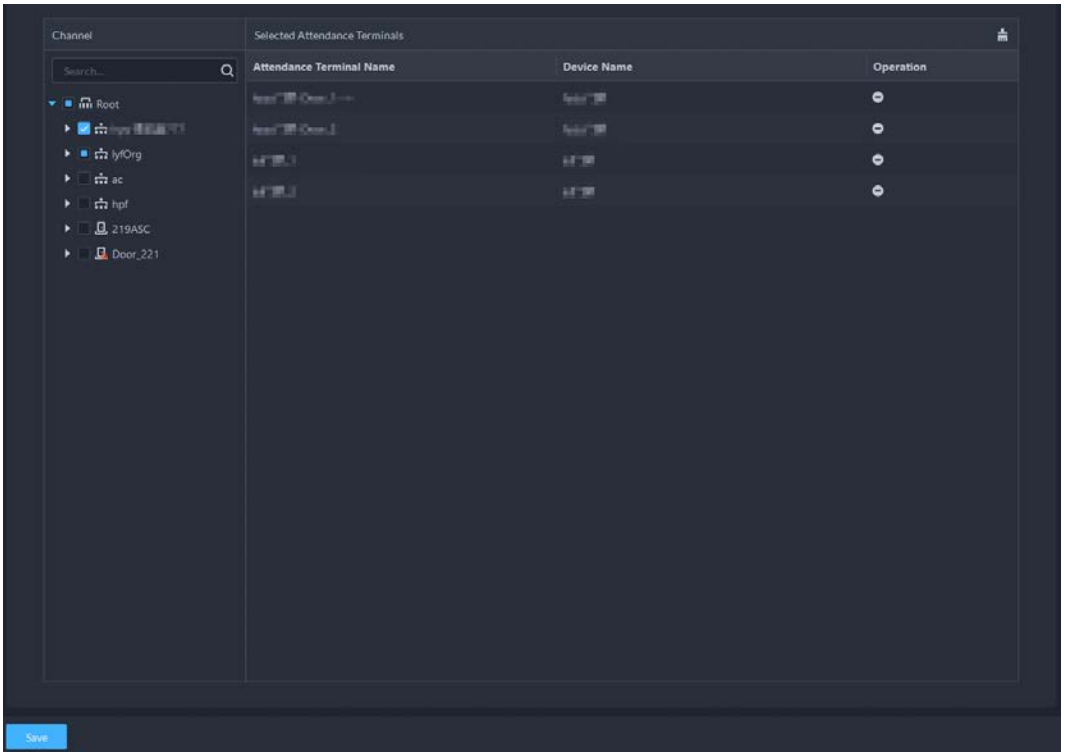
4.7.2 Configuring Attendance Terminal

Make sure that access controller is used as the attendance device for check-in and check-out, recording attendance information, and uploading attendance data.

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

Step 2 Select **Attendance Config** > **Attendance Terminals**.

Figure 4-66 Attendance terminal



Step 3 Select access control channels, and then click **Save**.

You can enter keyword and search for devices.

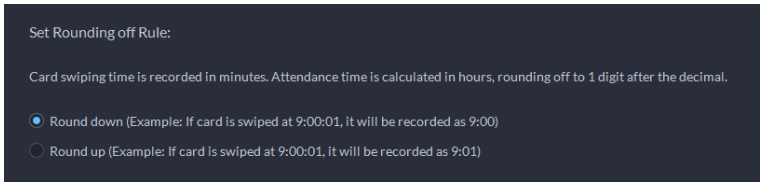
4.7.3 Configuring Statistics Rule

The smallest timing unit of swiping card is minute. Seconds will be rounded up or down. For example, if you swipe your card at 09:00:01 and the rule is set to round down, then the time of you swiping the card is 09:00; if the rule is set to round up, then the time of you swiping the card it is 09:01.

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

Step 2 Click on the left, and then select **Statistics Rule**.

Figure 4-67 Statistical rule



Step 3 Select a rule, and then click **Save**.

4.7.4 Synchronizing Attendance Records

The platform will synchronize attendance records from selected devices at the defined time. The

attendance report will be updated if new records are synchronized to the platform.

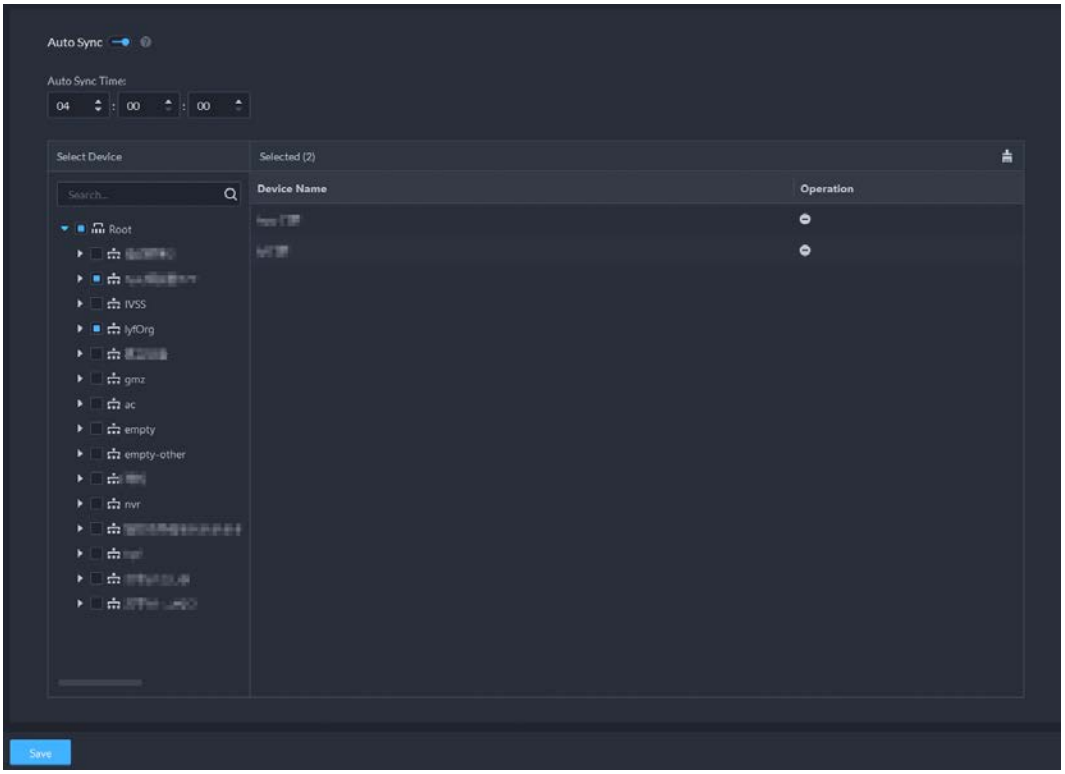
The platform also supports synchronizing attendance records manually. For details, see "5.4.4 Viewing Attendance Data".

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

Step 2 Select **Auto Sync Record**.

Step 3 Click to enable this function.

Figure 4-68 Automatically synchronize attendance records



Step 4 Configure the time, and then select access control devices.

Step 5 Click **Save**.

4.7.5 Configuring Attendance Period

Set attendance period, which can be used as time evidence to judge if a person is late, on time, or leaves early.

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

Step 2 Click .

Step 3 Click **Add** on upper-left corner of the page.

Step 4 Set parameters of attendance period.

- Fixed attendance requires you to sign in and sign out during the fixed hours.
  Click to add another working period. You can set up two working periods at most.

Table 4-9 Fixed attendance parameters

Parameter	Description
Period Name	Custom period name, used to recognize period, such as early shift and night shift.
Color	Set corresponding color of period, and corresponding color will be directly displayed on calendar when making shift for personnel, and quickly identify shift information.
Attendance Mode	Set as **Fixed Attendance**.
Working Time	Set corresponding working hour of period. Attendance time supports cross-day, but not exceeds 24 hours. One attendance period supports max two types of attendance time.
Working Hour	Fill in according to actual situation.
Valid Check-in Time	If working time is set from 09:00 to 18:00, then valid sign-in time can be set as 08:00-10:00, valid sign-out time can be set as 16:00-18:00. Configuration rules are as follows: • The start time of valid sign-in time is earlier than or equal to start working time (09:00), the end time of valid sign-in time should be later than start working time (09:00), earlier than start time of valid sign-out time. If there are several sign-in records within valid sign-in time, then the earliest record is considered as sign-in time. • The start time of valid sign-out time is later than the end time of valid sign-in time, earlier than end working time (18:00), the end sing-in time of valid sign-out time is later than or equal to end working time (18:00). If there are several sign-out records within valid sign-out time, then the earliest record is considered as sign-out time.
Valid Check-out Time	If working time is set from 09:00-18:00, then valid sign-in time can be set as 08:00-10:00, valid sign-out time can be set as 16:00-18:00. Configuration rules are as follows: • The start time of valid sign-in time is earlier than or equal to start working time (09:00), the end time of valid sign-in time should be later than start working time (09:00), earlier than start time of valid sign-out time. If there are several sign-in records within valid sign-in time, then the earliest record is considered as sign-in time. • The start time of valid sign-out time is later than the end time of valid sign-in time, earlier than end working time (18:00), the end sing-in time of valid sign-out time is later than or equal to end working time (18:00). If there are several sign-out records within valid sign-out time, then the earliest record is considered as sign-out time.
Shall check in	If you set two working time, then the second working time can cancel sign in, you don't have to sign in when you work at the second working time, and the start time of working time can be used as sign-in time.
Shall check out	If you set two working time, then the first working time can cancel sign in, you don't have to sign out when you finish work at the second working time, and the end time of working time can be used as sign-out time.

Parameter	Description
Allow Late Time (Minutes)	Define the rules for being late, absence and early leave. Take the values in the snapshot as an example. • Check in on time: Check in no later than 5 minutes. • Later: Check in 5 minutes later, but no later than 30 minutes. • Absence: Check in 30 minutes later or check out 120 minutes earlier. • Leave on time: Check out no earlier than 5 minutes. • Leave earlier: Check out 5 minutes earlier, but no earlier than 120 minutes. • Overtime: Check out 60 minutes later.
Allow Early Time (Minutes)	
Absence TimeOn duty _ minute later.	
Absence TimeOn duty _ minute earlier.	
OvertimeOff duty _ minte later.	Define overtime rule. If it is set to 120 minutes, off duty check-out time is later than end time of working time, and period >120 minutes, then it is recorded as overtime, overtime period is **Period– 120 minutes**.

- Flexible attendance just calculates whether the daily working hours of a person meets the rule according to the sign-in/out time.

Table 4-10 Free attendance parameters

Parameter	Description
Period name	Custom period name, used to recognize period, such as flexible attendance.
Attendance mode	Set as **Flexible Attendance**.
Color	Set corresponding color of period, corresponding color will be directly displayed on calendar when making shift for personnel, and quickly recognize shift information.
Work Time	Set the period you must work in a day.
Working Hours	Set how many hours you have to work a day. For example, if you set 8, then it means you are required to work 8 hours.
Valid Check-in Time	Sign in after restricted time is recorded as late.
Valid Check-out Time	You are required to sign out before the designated time, otherwise no sign out is recorded.
Must Check In/Out	You must check in or check out within the defined period. If you have configured 2 or mo re attendance periods, you can select which within period people must check in or out.
Minimum OverTime Work (Hours)	For example, working hour is 8 hours a day, and if you work overtime for 2.5 hours, then it is recorded as overtime, then you can set 10.5 here.
Cumulate Time For Every Two Punches.Minimum Time Interval Between Every Two Punches (Minutes)	Swipe card at odd number is recorded as check-in. For example, the first card-swiping is check-in. Swipe card at even number is recorded as check-out. For example, the second card-swiping is check-out. It is recorded swiping the card twice when the interval of two continuous card swiping is larger than the defined value.

Step 5 Click **Save**.

If attendance period is already applied to attendance shift, then before deleting attendance period, go to **Attendance Shift**, disable the attendance period in the attendance shift, and then delete the attendance period you want.

4.7.6 Configuring Holiday Plans

Set holiday time to determine overtime type.

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

Step 2 Click .

Step 3 Click **Add** on the upper-left corner.

Step 4 Configure the information.

Figure 4-69 Add a holiday

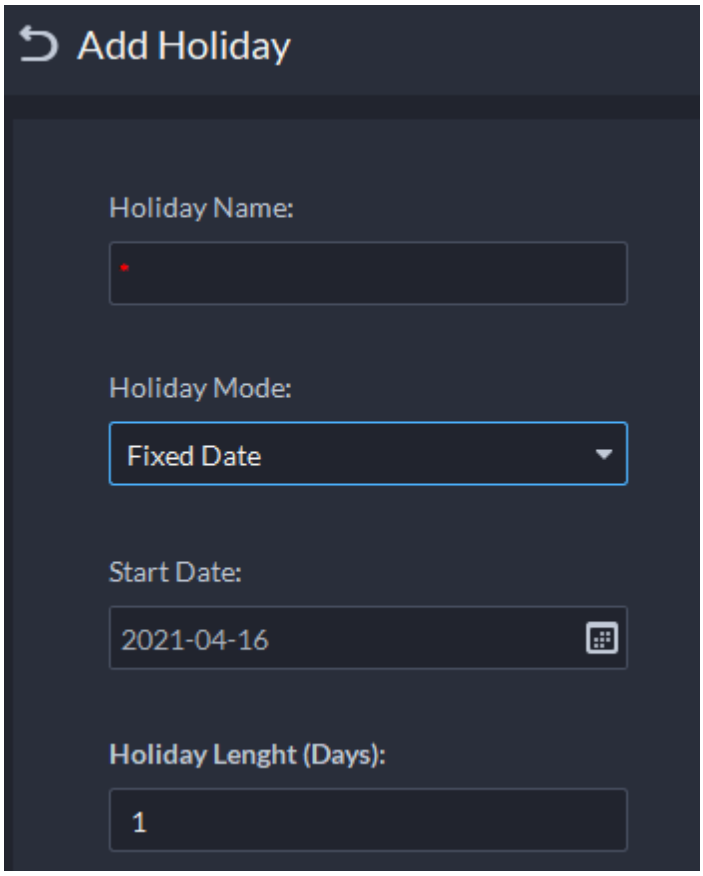


Table 4-11 Holiday parameters

Holiday mode	Description
Fixed Date	Set some specific date as holiday. For example, set May 1, 2019 (Labor's day) as holiday, and lasts for 1 day, then set **Start Date** as May 1, 2019 and **Holiday Days** as 1.

Holiday mode	Description
Date Cycle	If the holiday is the fixed weekday of some week in some specific month, and it cycles according to year, which can be configured as date cycle. For example, if you want to set Mother's Day as holiday, and it lasts for 1 day, then you can set **Start Date** as the second Sunday in May, and **Holiday Days** as 1.
Year Cycle	If the holiday is fixed date and it cycles according to year, which can be configured as year cycle. For example, set New Year's Day as holiday, and it lasts for 1 day, then you can set **Start Date** as January 1 and **Holiday Days** as 1.

Step 5 Click **Save**.

4.7.7 Configuring Attendance Shift

Set attendance shift according to attendance period, used for department and personnel shift.

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

Step 2 Click .

Step 3 Click **Add** on the upper-left corner of the page.

Step 4 Set shift details, select a day, and then click **Apply** to arrange attendance period for the day.

Figure 4-70 Configure attendance shifts

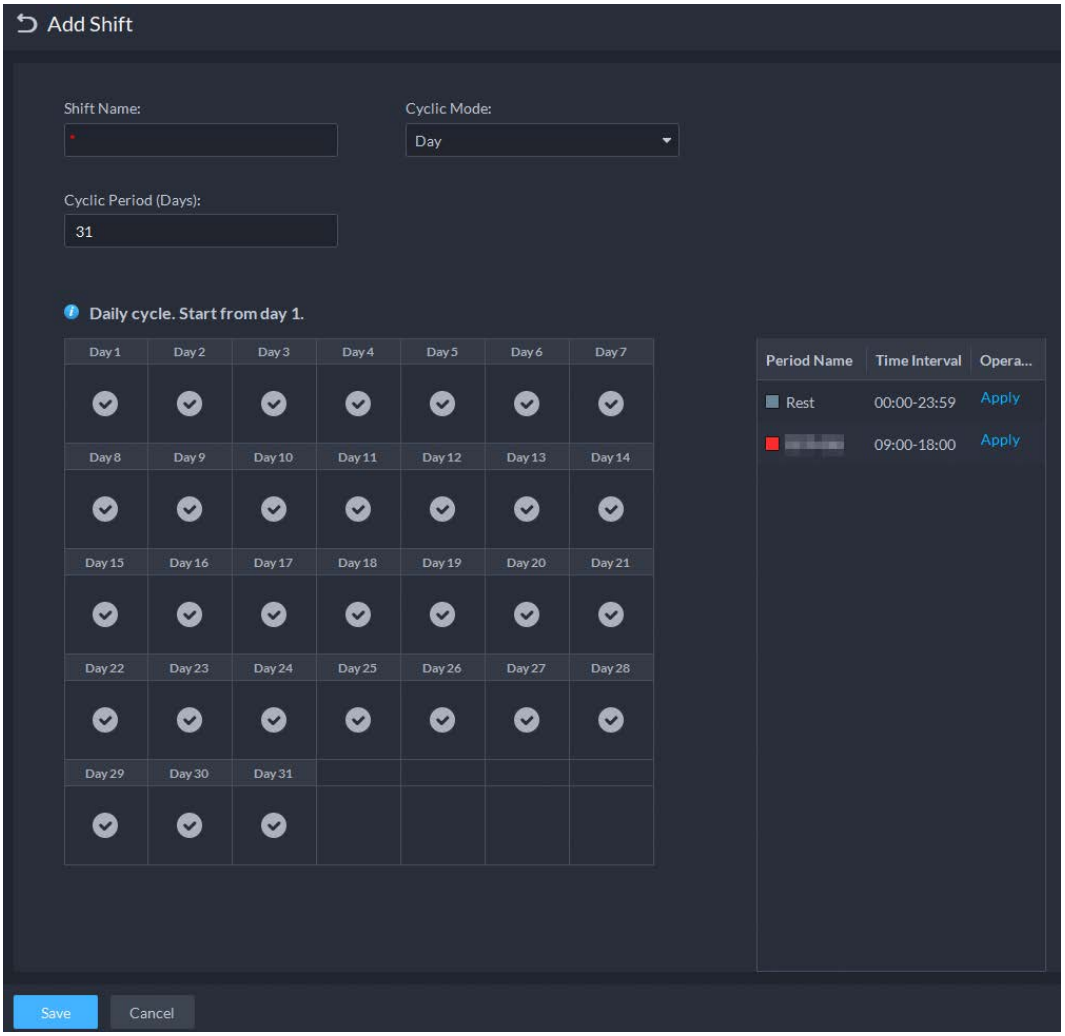


Table 4-12 Attendance shift parameters

Parameter	Description
Shift Name	Custom period name, used to recognize shift.
Cyclic Mode	Day: Start cycle from the first day, cycle period can be set as any number from 1 to 31 according to day. For example, if you set 2, then the cycle period is 2 days. Week: There are 7 days in a week by default, it starts cycle from Sunday, and so Sunday is required to be set as the first day. Cycle period can be set as any number from 1 to 4. For example, if you set 2, then 2 weeks can be a cycle period. Month: There are 31 days in a month by default, it starts cycle from the current day (If the date does not exist, then it will be deleted during shift arrangement), cycle period can be set as any number from 1 to 3 according to month. For example, if you set 2, then 2 months can be a cycle period.
Cyclic Period (Days)	

Step 5 Click **Save**.

Delete in-use attendance shift: Go to **Shift Management** > **Person Shift**, check if there are shifts to be deleted; if yes, remove the relation, and then delete.

4.7.8 Shift Management

Arrange shifts for personnel or department. You can also arrange temporary shift for personnel. The shift priority is temporary shift > holiday > personnel shift > department shift.

4.7.8.1 Personnel/Department Shift Arrangement

The operations for personnel shift and department shift are similar. This section takes personnel shift as an example.

- If you configure department shift, then all the personnel of the department need to conform to the shift.
- If both personnel and department are configured with shift, then the latest personnel shift shall prevail. For example, after configuring the personnel shift, and the corresponding department is configured as well, then personnel shift is based on the latest department shift.
- If the department where new personnel belong to is configured with shift, then the shift of new personnel should conform to department shift.

Step 1 Click on the **Attendance** page.

Step 2 Click on the upper-left corner of the page.

- If you need to configure shift for department, click on the upper-left corner and enter the page of department shift arrangement. The following operation is the same as personnel shift arrangement.
- Click next to the personnel and you can view the shift details.

Step 3 Select shift personnel, click to add shift information.

Figure 4-71 Select shifts

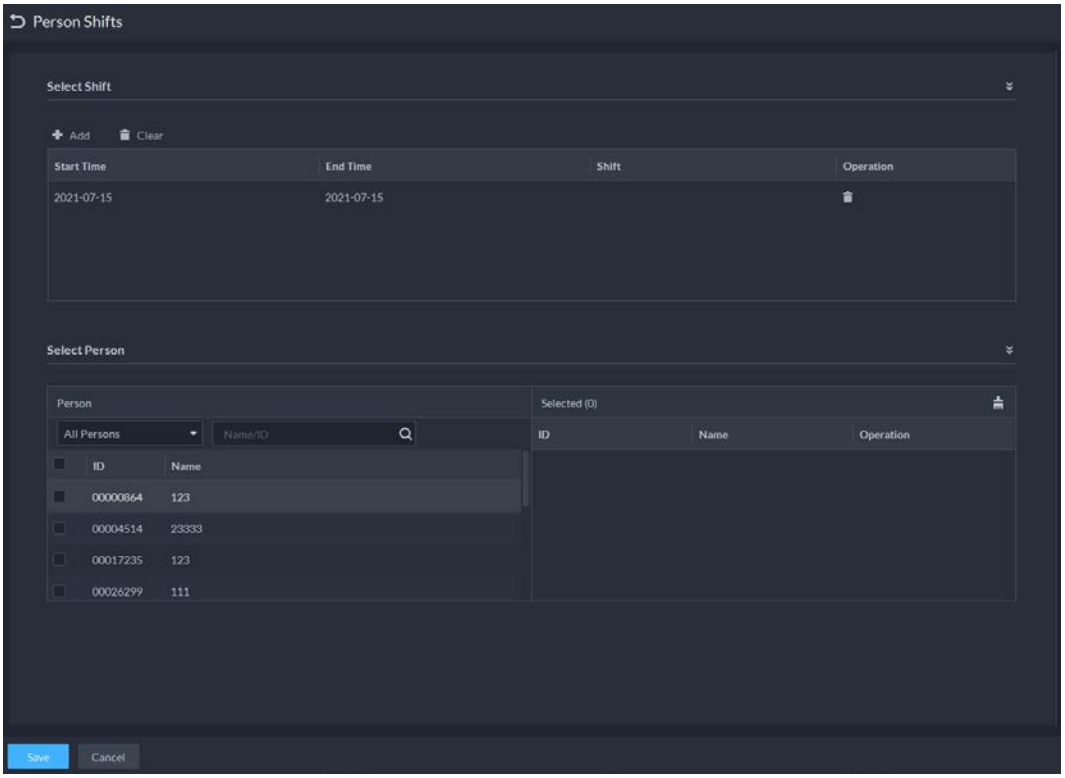


Table 4-13 Parameter description

Parameter	Description
Start Time	Set start date and end date of personnel shift. Click the column of **Start Time** and display calendar, select date and time, and then click **OK** to complete date setting
End Time	
Shift	Select the one you need. See "4.7.8.1 Personnel/Department Shift Arrangement".

Step 4 Click **Save**.

4.7.8.2 Temporary Shift

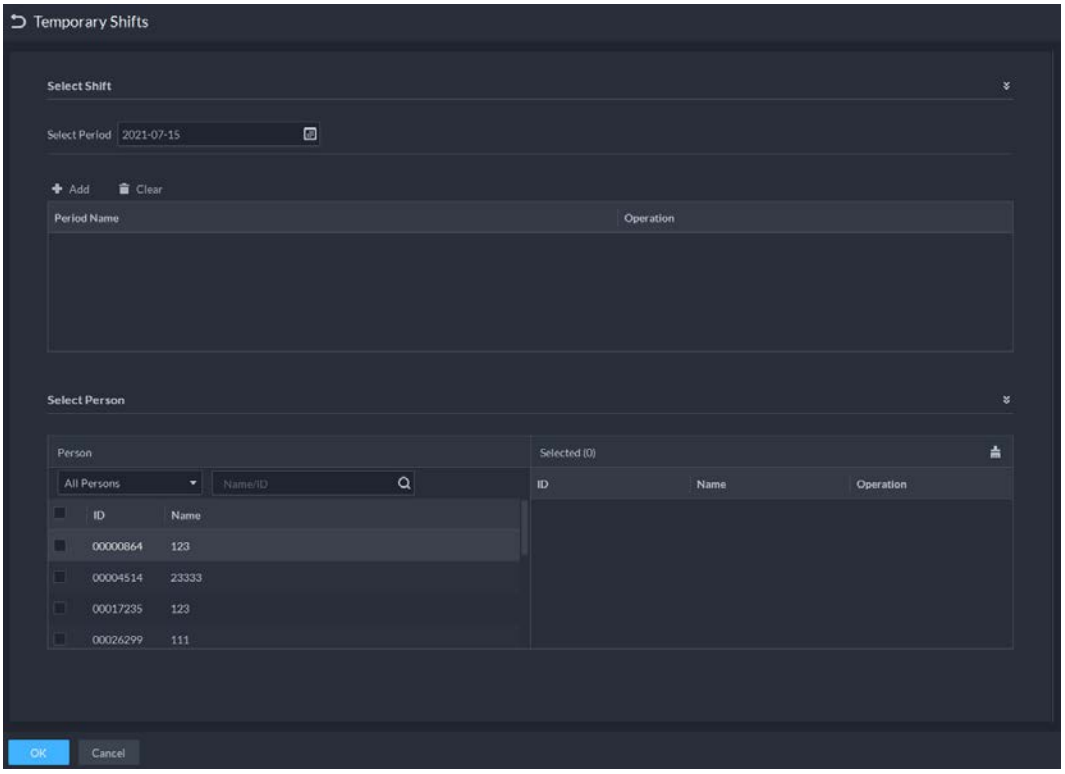
Arrange a temporary shift when needed.

Step 1 Click on the **Attendance** page.

Step 2 Select personnel and date.

Step 3 Click , and then click **Reset** to select an attendance shift as needed. You can add max. 2 attendance periods and 1 free attendance period.

Figure 4-72 Temporary shift



Step 4 Click **OK** and save shift information.

Temporary shift can be deleted, right-click the date which is configured with temporary shift, and delete temporary shift according to system prompt.

4.8 Visitor Management

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

4.8.1 Preparations

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

4.8.2 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**.

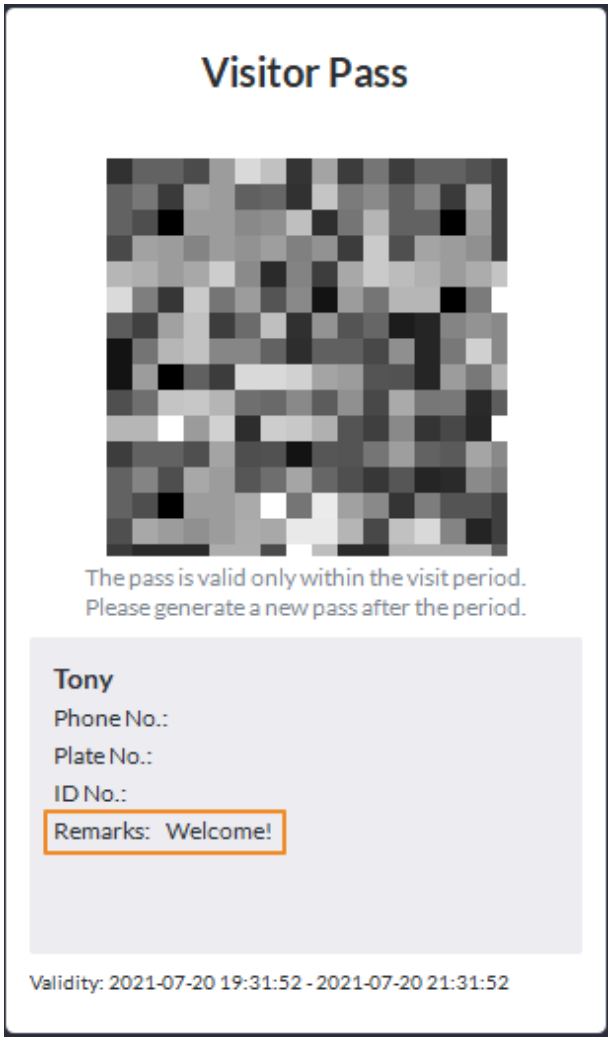
Step 2 Configure the parameters.

- Automatic visit
  Enable the function, and then select the channels as needed. Visitors with appointment can verify their identities on the selected channels without registering.

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

Figure 4-73 Customize visitor pass remarks

Figure 4-74 Visitor pass remarks



Step 3 Click **Save**.

4.9 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.

4.9.1 Preparations

Make sure that the following preparations have been made:

- Devices, such as ANPR cameras, parking space detectors, VTOs, barriers, and displays for available

parking spaces, are added to the platform.

- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
  - When adding an ANPR camera, select **Access ANPR Device** as the device category.
    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 "3.2.3 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 "4.3 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 "4.6.3 Configuring Building/Unit and Call Mode".
  - Add a screen.
    Add a display for available parking space. Select **Display Device** as the device category. Dahua screen and Jiuzhou screen are supported as the display for available parking space.
  - 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 displayed. For details, see "3.4 Configuring Storage".

4.9.2 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.

4.9.2.1 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 4-14 Parameter description

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

Parameter	Description
Enable Parking Space Counting	• **Count parking spaces by entering and exiting vehicles**: Set up the total and available parking spaces in the parking lot, and then the parking spaces will be automatically counted based on each vehicle that enters or exits the parking lot. • **Count parking spaces using parking space detectors**: After parking space detectors are added to the platform and configured, parking spaces will be automatically counted.
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.

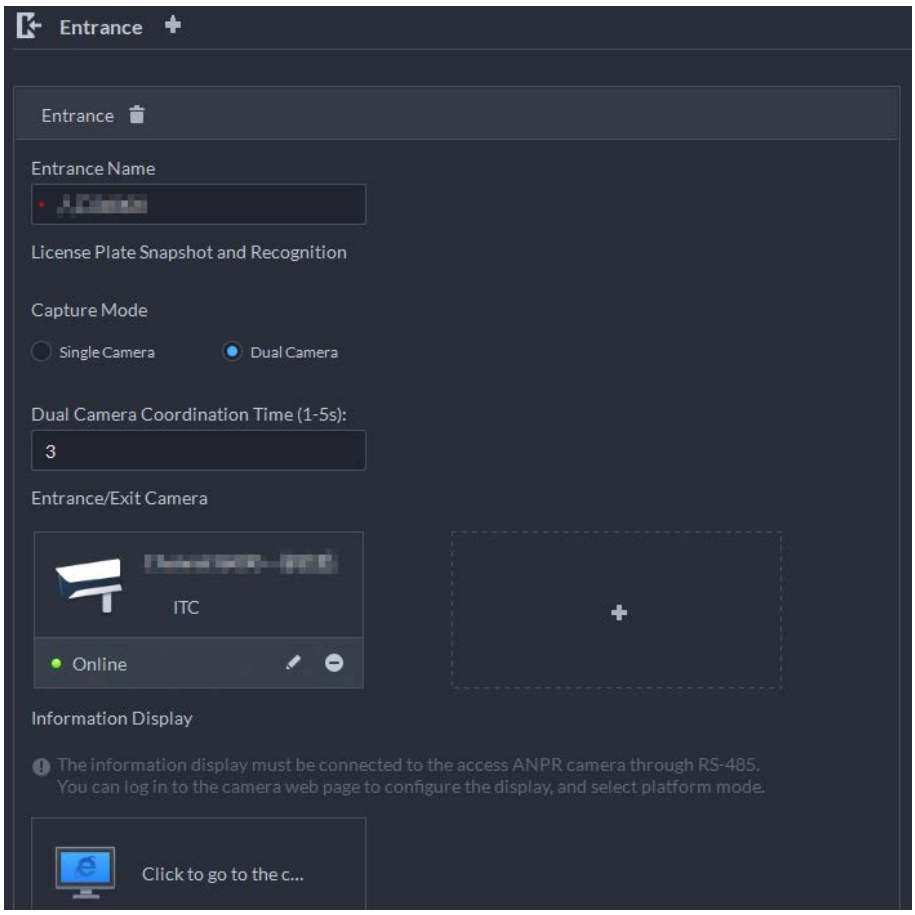
Parameter	Description
Auto overwrite when captured vehicle has not existed	If a vehicle entered the parking lot but has not exited, a new entry record will be generated when the vehicle is recognized to have entered again.

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

The platform supports up to 60 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 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 4-75 Entrance point configuration



5) If there is an exit point, click 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 **Next Step**.

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

Table 4-15 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 to Enter**: 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 "3.2.6 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**: You must enable parking space counting and select **Count parking spaces by entering and exiting vehicles**. ◇ **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 "4.9.3 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.

Step 6 (Optional) Configure parking space detectors, and then click **Next Step**.

If you do not need to calculate parking spaces by using parking space detectors, you can skip this step and click **Next Step**.

1) Click **Add** or **Add Parking Space Detector**.

You need to add parking space detectors to the platform first. For how to add parking space detectors, see "3.2.2 Managing Device".

2) Select the parking space detectors that belong to this parking lot, and then click **OK**.

Step 7 (Optional) Configure indoor and outdoor parking space available displays, and then click **Save and Exit**.

1) Click **Add**, and then select the displays that belong to this parking lot, and then click **OK**.
2) Click of an outdoor parking space available display, select the color and what to display when available parking space is 0, and then click **OK**.
3) Click of an outdoor parking space available display, select a parking space counting mode, and then click **OK**.
   If you select **Count parking spaces using parking space detectors**, two options are available:
   - **Selected Parking Spaces**: Only count the parking spaces of the parking space detectors you select.
   - **Count parking spaces by parking space detectors**: Count the parking spaces from all parking space detectors in this parking lot.
4) Click of an indoor parking space available display, select the arrow position and the color, and then click **OK**.
5) Click of an indoor parking space available display, select a parking space counting mode, and then click **OK**.
6) Click of an indoor parking space available display, configure a parking space counting mode for each direction, and then click **OK**.
   If you select **Count parking spaces using parking space detectors**, two options are available:
   - **Selected Parking Spaces**: Only count the parking spaces of the parking space detectors you select.
   - **Count parking spaces by parking space detectors**: Count the parking spaces from all parking space detectors in this parking lot.

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.

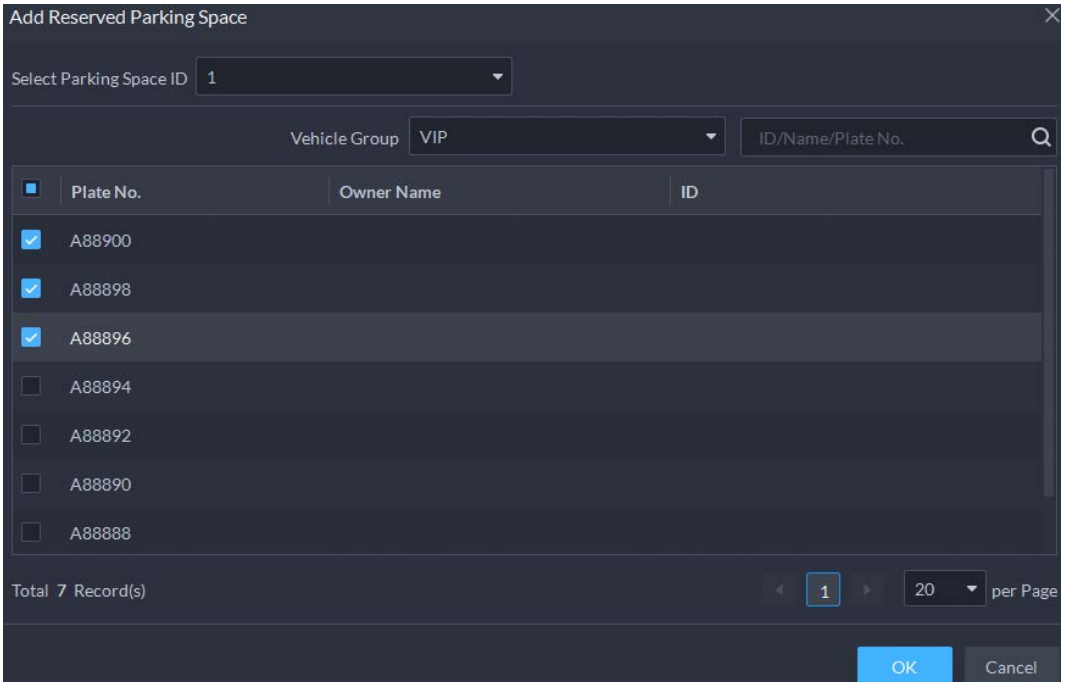
4.9.2.2 Reserved Parking Space

Link a parking space to one or more plate numbers. Alarms will be triggered if vehicles with other plate numbers park in this parking space.

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** > **Reserved Parking Space Config**.

Step 2 Select a parking lot, and then click **Add**.

Figure 4-76 Link a parking space to plate numbers



Step 3 Select a parking space you want to link plate numbers to, a vehicle group, and one or more plate numbers, and then click **OK**.

4.9.2.3 Parking Lot Layer

Add a plan view image to the parking lot, and then mark the entrance and exit points, parking spaces, parking space available displays, and monitoring devices on it, so that you can manage the parking lot in an intuitive way. If the parking lot has multiple floor, you can add an image for each floor.

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 Layer Config**.

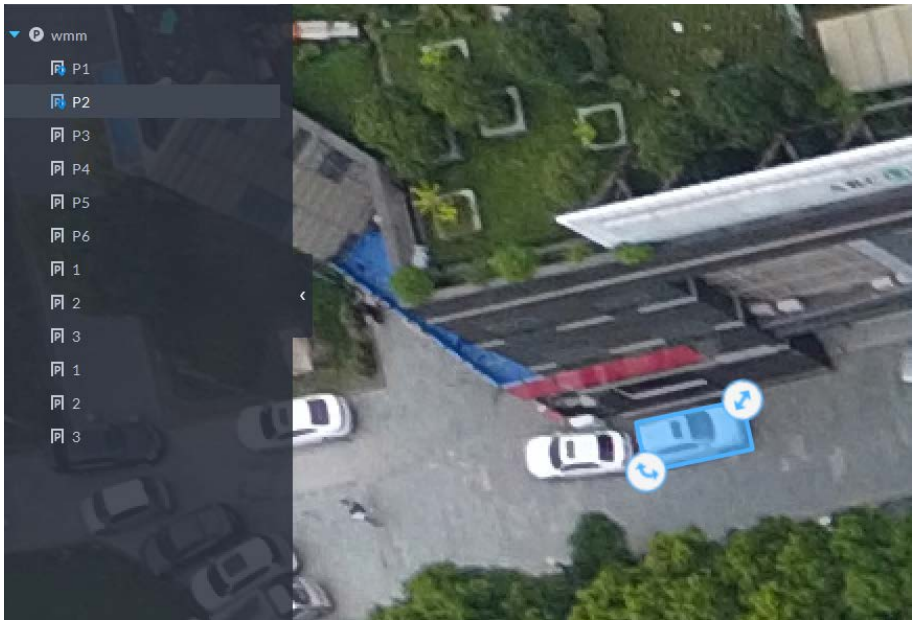
Step 2 Select a parking lot, and then click **Add**.

Step 3 Enter a name for the layer, upload an image, and then click **Save and Configure Layer**.

Step 4 Drag an entrance or exit point to the image, and then click **Next Step**.

Step 5 Drag a parking space to the image, adjust its size and direction, and then click **Next Step**.

Figure 4-77 Mark a parking space



Step 6 Drag a parking space available display to the image, and then click **Next Step**.

Step 7 Drag a channel of a monitoring device to the image, and then click **Next Step**.

Related Operations

- : Edit the marked information on the layer.
- : Edit the name and image of the layer.
- : Delete the layer.

4.9.2.4 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 "4.1 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.

The following events will not be displayed because there are no additional parameters to be configured.

- Blocklist alarm: An alarm will be triggered when a vehicle on the blocklist enters the parking lot.
- Reserved parking space alarm: An alarm will be triggered when a vehicle parks in a parking space, but its plate number is not linked to the parking space.
- Parking overline: An alarm will be triggered when a vehicle crosses a line after it is parked.

Step 4 Click to configure an event.

Table 4-16 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 and Vehicle in the Blocklist**: 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.
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.

4.9.3 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 , 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 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**.

4.10 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.

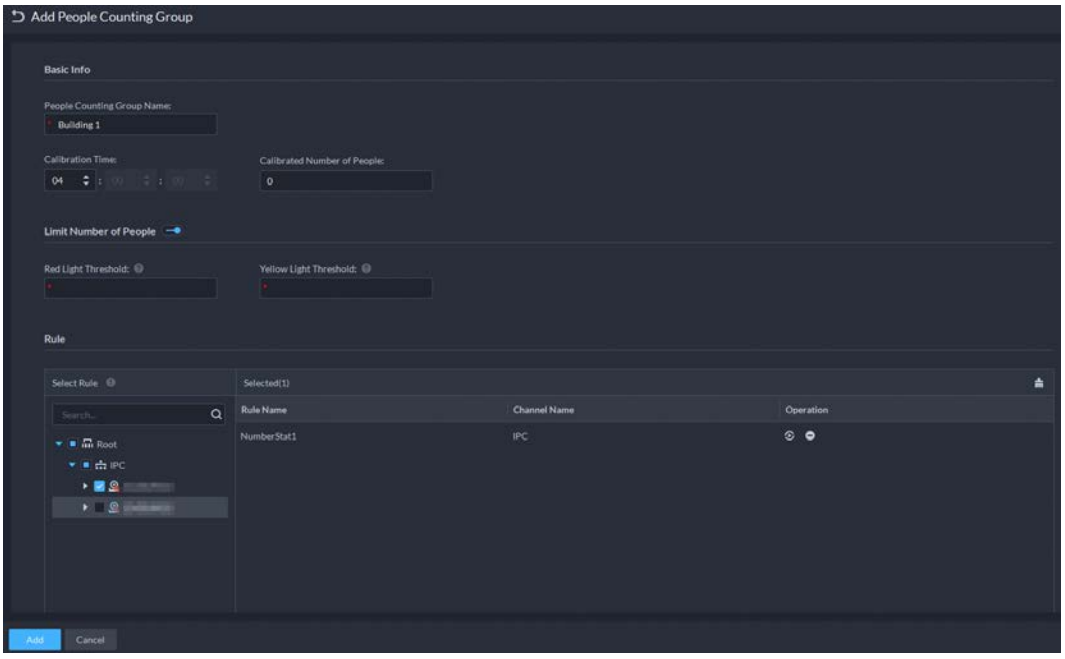
4.10.1 People Counting Group

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 , and then in the **App Config** section, select **Intelligent Analysis** > **People Counting Group Config**.

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

Figure 4-78 Add a people counting group



Step 3 Configure the parameters.

Table 4-17 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**.

4.10.2 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 Configure one or more email addresses to send the report to, and the content of the email.

1) Click to select the users that have been configured email addresses, or enter an email address, and then press Enter.

Figure 4-79 Invalid email address, you must press Enter

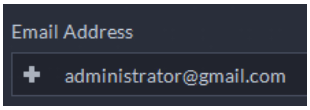
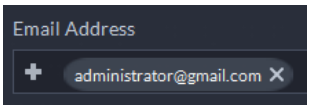


Figure 4-80 Valid email address



2) Configure the content of the email.

Step 4 Send the report.

- Click **Send Now** to immediately send the report that you configured.
- Click **Save**, and then the report will be sent at the defined time.

4.11 Synthesis

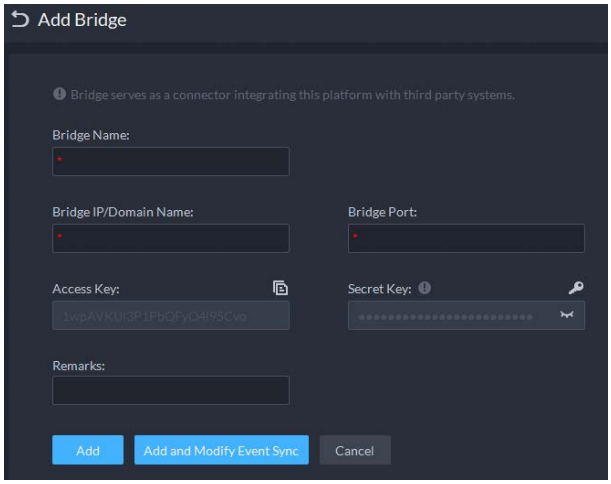
Use a bridge to import events to the platform from third-party systems, and then use these events to create alarms schemes and perform certain linkage actions. You can also share access control and attendance data with third-party databases, which can be used by third-party personnel to formulate their own reports.

4.11.1 Synchronizing Events

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Synthesis** > **Event Sync**.

Step 2 Click **Add**.

Figure 4-81 Add a bridge



- A bridge serves as a connector between the platform and third-party systems, and is responsible for importing events from a third-party system to the platform. It must comply with the connection protocol between the third-party system and the platform. For different systems, the protocol might vary and you might need to develop a new bridge. Before using this function, make sure the bridge has been deployed and is running.
- You can add up to 5 bridges.

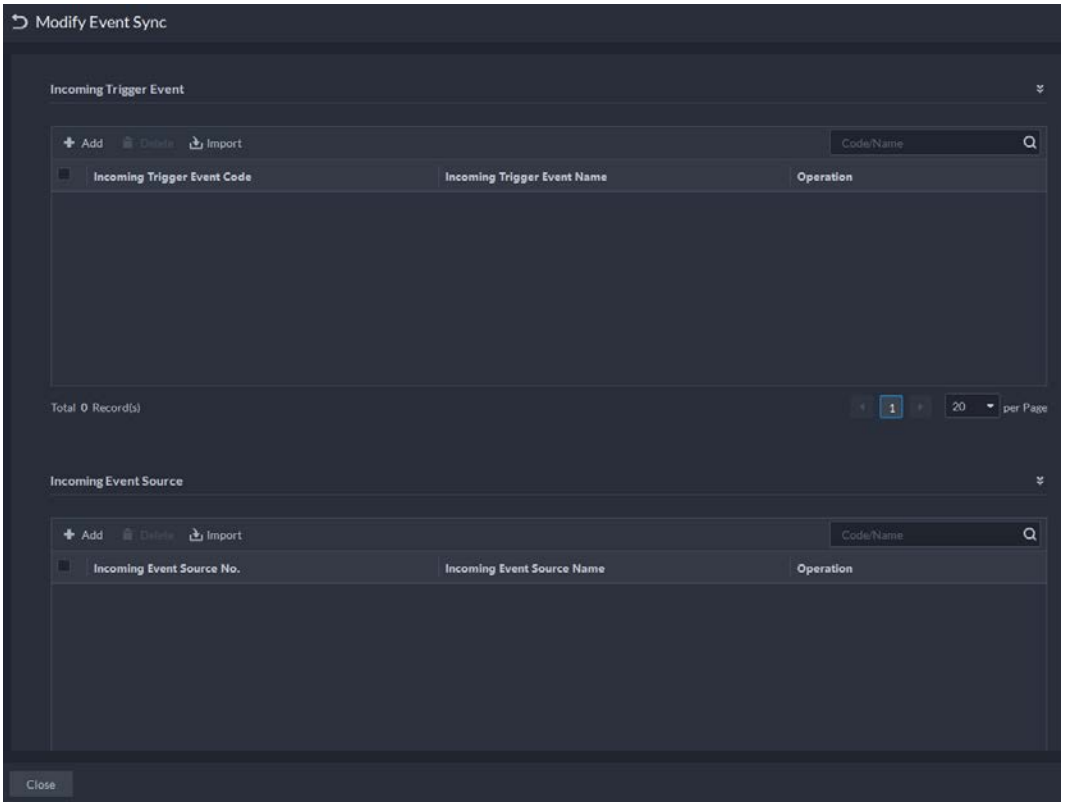
Step 3 Configure the parameters.

Table 4-18 Parameter description

Parameter	Description
Bridge Name	Name of the bridge.
Bridge IP/Domain Name	IP address or domain name, and port number of the bridge.
Bridge Port	
Access Key	Automatically generated. Click to copy it.
Secret Key	Automatically generated. • Click to verify your password, and then generate a new secret key. • Click to verify your password, and then you can click to copy it.

Step 4 Click **Add** or **Add and Modify Event Sync**.

Figure 4-82 Synchronize events

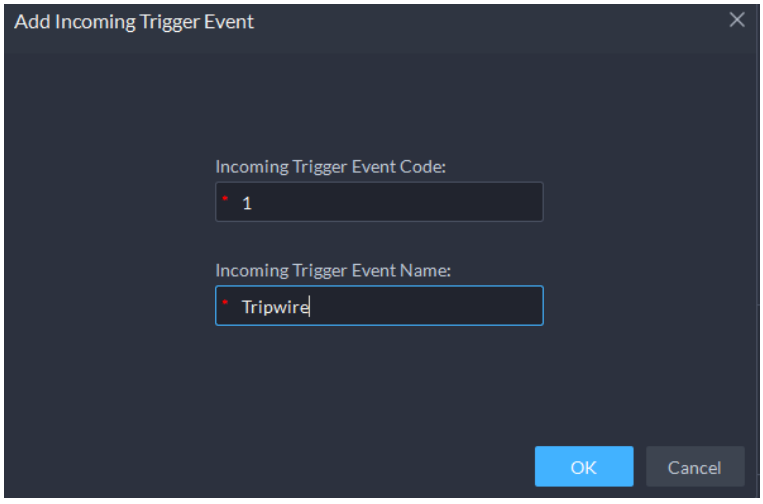


Step 5 Synchronize incoming trigger events.

- One by one

1) Click **Add**.
2) Enter the code and name of the incoming trigger event.
3) Click **OK**.

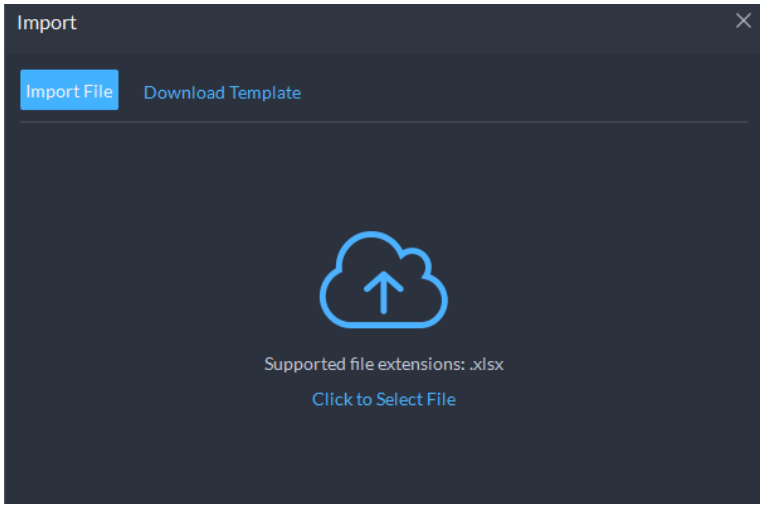
Figure 4-83 Enter the code and name of the incoming trigger event



- In batches

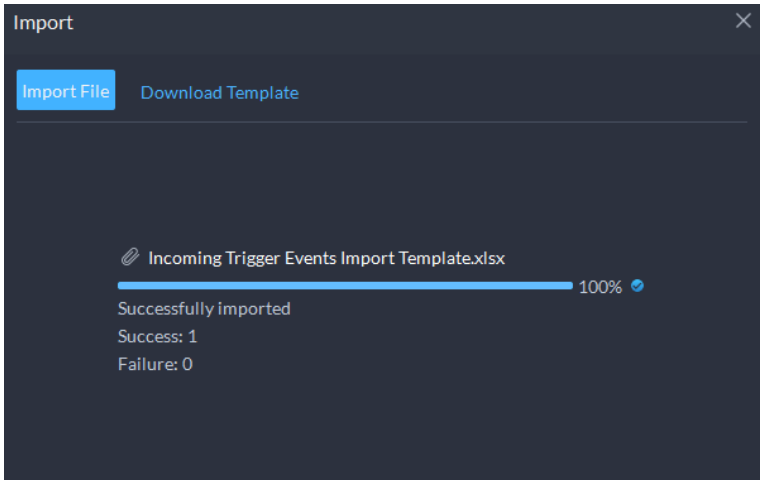
1) Click **Import**.

Figure 4-84 Download template



2) Click **Download Template**, save the template to your PC, and then enter the information in it.
3) Click **Import File**, select the file, and then click **Open**.

Figure 4-85 Synchronize events in batches

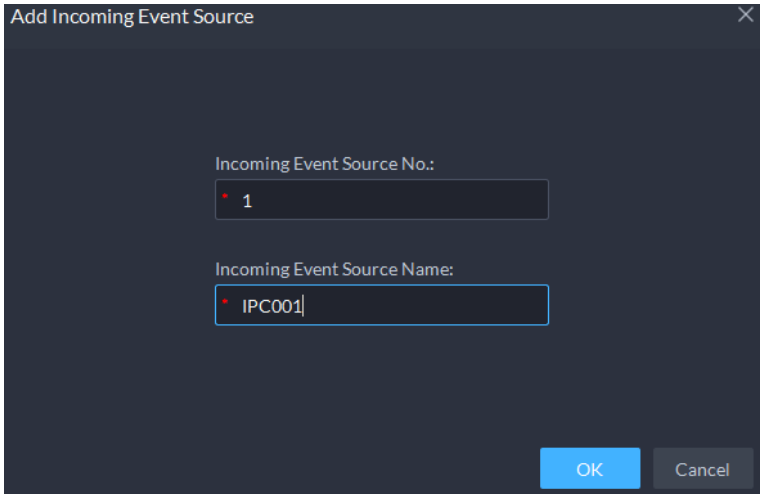


Step 6 Synchronize incoming event sources.

- One by one

1) Click **Add**.
2) Enter the number and name of the incoming event source.
3) Click **OK**.

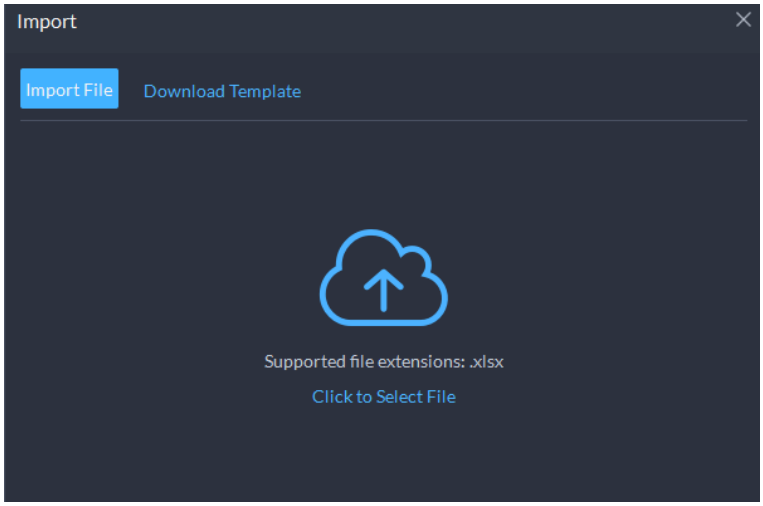
Figure 4-86 Enter the code and name of the incoming event source



- In batches

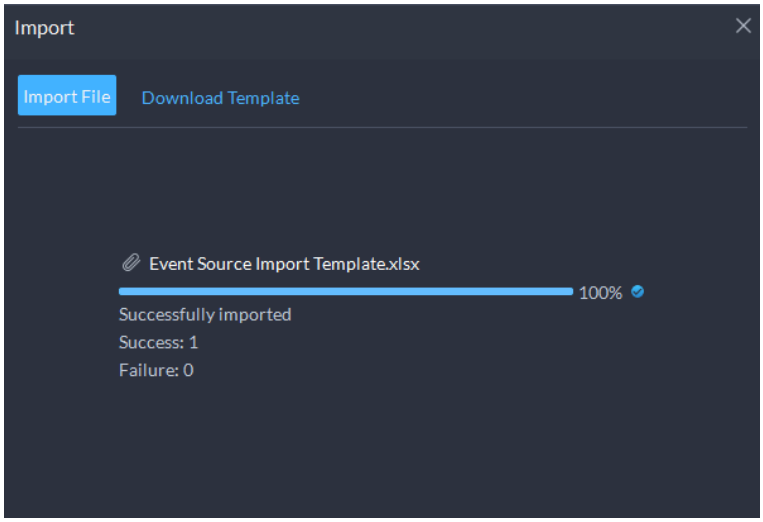
1) Click **Import**.

Figure 4-87 Download template



2) Click **Download Template**, save the template to your PC, and then enter the information in it.
3) Click **Import File**, select the file, and then click **Open**.

Figure 4-88 Synchronize incoming event sources in batches

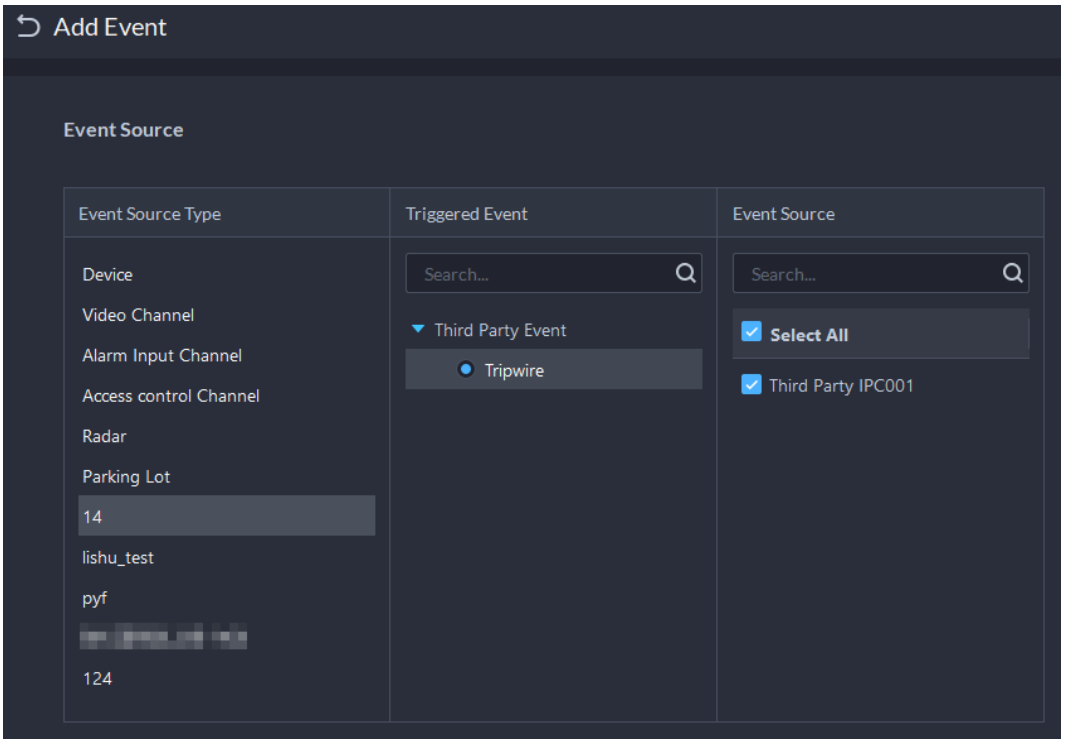


Step 7 Click **Close** at the lower-left corner.

Related Operations

- : Edit the information of the bridge.
- : Edit the incoming trigger events and event sources.
- : Delete the bridge.
- Add event
  1. Go to **Home** page, click , and then in the **Applications Configuration** section, select **Event**.
  2. Click **Add**.
  3. In the **Event Source section**, select the one you import from the third-party system.

Figure 4-89 Add an third-party event



4. For other parameters, see "4.1 Configuring Events".

4.11.2 Synchronizing Data

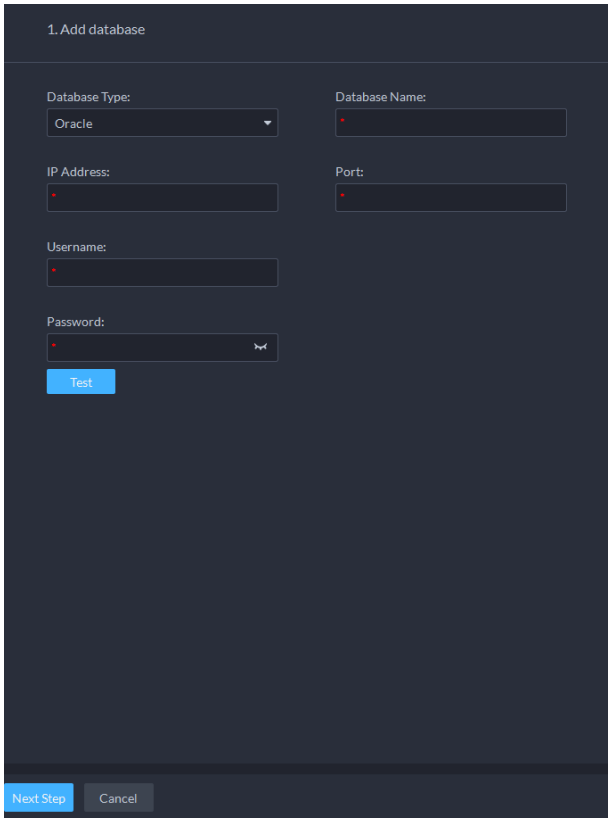
You can manually or regularly synchronize data in the platform to third-party databases.

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Synthesis** > **Data Sync**.

Step 2 Click **Add**.

You can only add one database.

Figure 4-90 Add a database

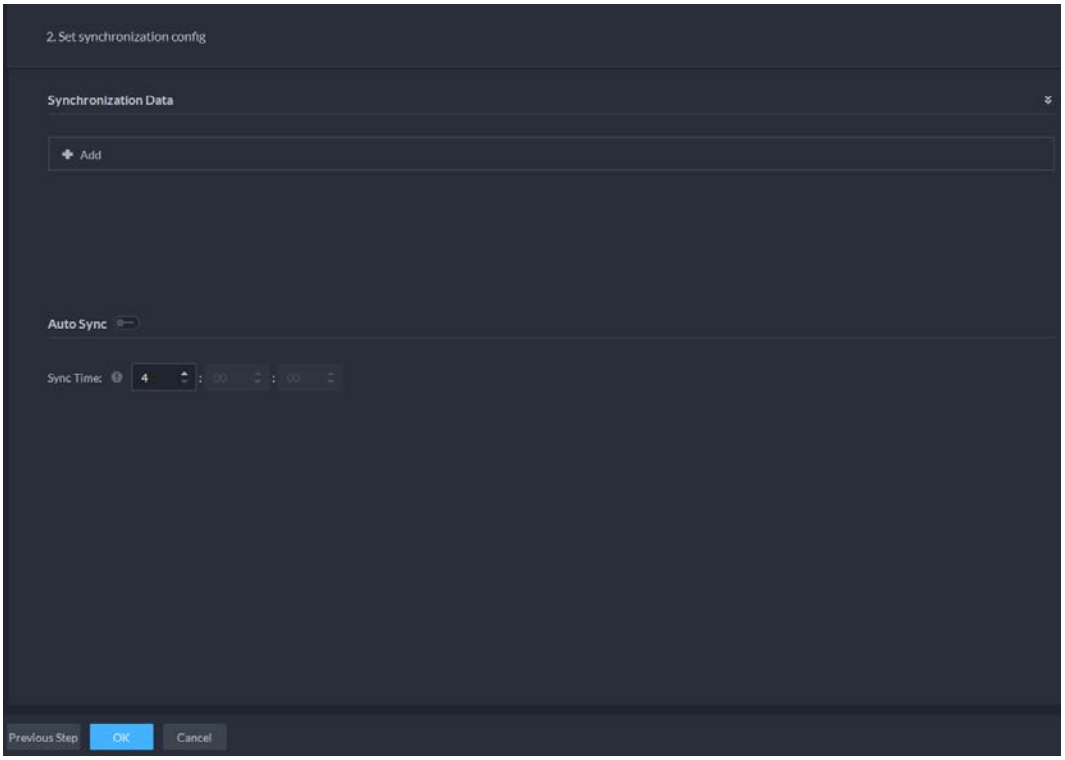


Step 3 Select the type of the database, and then enter its name, IP address, port, username and password.

Click **Test**. If the connection is through, the system will prompt that it connects to the database successfully.

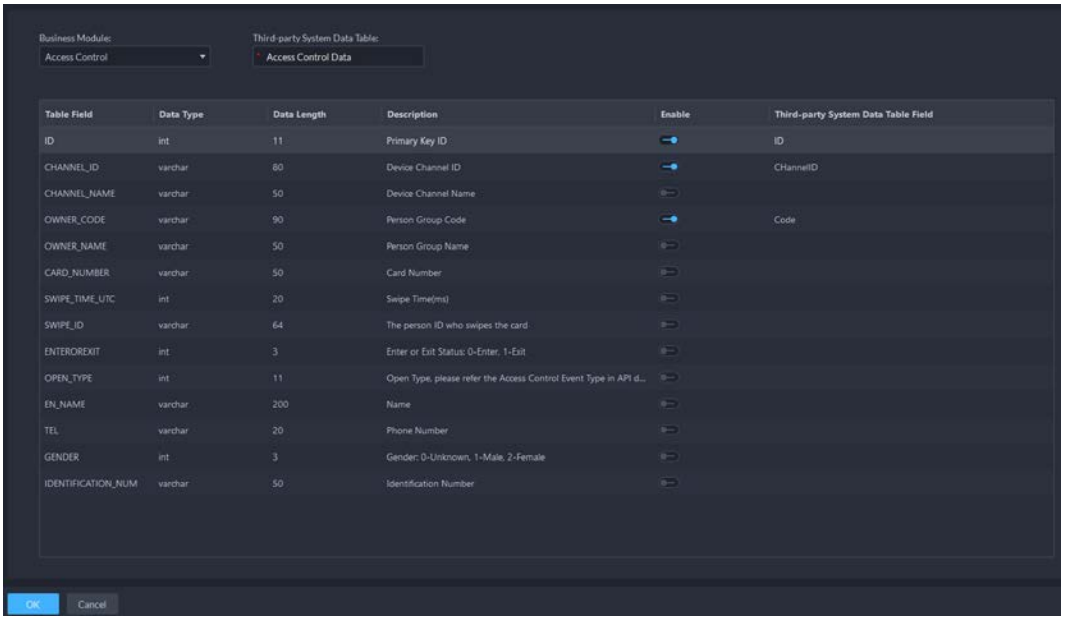
Step 4 Click **Next Step**.

Figure 4-91 Synchronize data



Step 5 Click **Add**.

Figure 4-92 Configure parameters



Step 6 Set **Business Module** to **Access Control** or **Attendance**, and then enter the name of the data table in the third-party system.

Each business module can only be added once.

Step 7 Click to select what data to be synchronized. You must disable the data you do not want to synchronize.

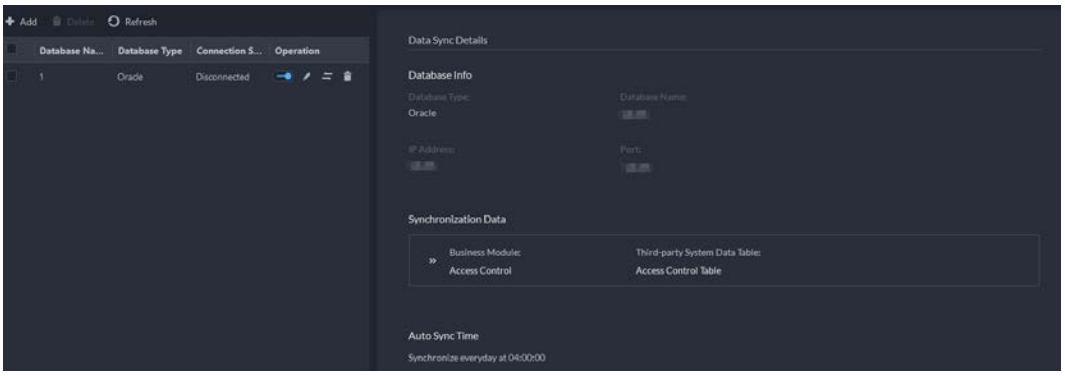
Step 8 Double-click the area under **Third-party System Data Table Field**, enter the corresponding name in the table in the third-party system.

Step 9 Click , and then configure the time to automatically synchronize the data everyday.

You can only configure 4:00–23:00.

Step 10 Click **OK**.

Figure 4-93 Database information



Related Operations

- : Turn on or off automatic synchronization.
  All the data will be synchronized on the first attempt, including after you delete and then add the database again. Only new data will be updated on subsequent synchronizations.
- : Edit the information of the database or the data that is being synchronized. You can view each synchronization result in the log. See "8.1.3 System Log".
- : Synchronize the data immediately.
- : Delete the database.

4.12 Maintenance Center

After configuring video storage detection, you will be prompted if the duration or integrity of recording is abnormal. Also, a scheduled report can be sent at the defined time to one or more email addresses to keep the persons updated of the status of the platform. The information in the report can include channel status, device status, server status, hard disk status, fault status, and abnormal videos.

4.12.1 Configuring Video Storage Detection

The platform will continue to check the duration and integrity of the videos. You will be prompted if the one of them is abnormal. For example, 30 days of duration and video integrity have been configured for channel A. If there are only 24 days of video, or the video does not last for 24 hours on any day, the platform will give corresponding prompts.

Prerequisites

Recording plans have been configured for channels and videos have been recorded.

Procedure

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

select **Maintenance Center** > **Video Storage Detection Config.**.

Step 2 In the **Video Storage Detection Config** section, select channels, and then configure the number of days of video.

You can also enter a number in the **Days to Record Videos in Batches Config** input box, and then click **Apply**. The number of days will be applied to all selected channels.

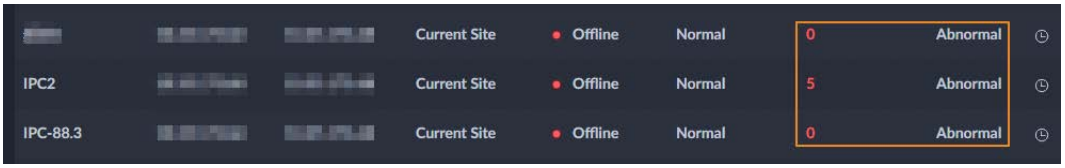
Step 3 In the **Detection of Video Completion Status**, select channels.

Step 4 Click **OK**.

Related Operations

You can view the detection results in **Maintenance Center**. If the duration of video is not enough, the number of days will be displayed in red. If video does not last for 24 hours on any day, the integrity status will be abnormal. For details, see "5.7.1 Viewing System Status".

Figure 4-94 Video duration and integrity status



4.12.2 Configuring Scheduled Report

Configure a period so that the platform will regularly send data on how the system is running to the defined email addresses, including channel status, device status, server status, disk status, faults, and abnormal videos.

Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **App Config** section, select **Maintenance Center** > **Scheduled Report 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 Select a format of the report, including Excel or PDF.

Step 4 Select the type of information to be included in the report.

It includes channel status, device status, server status, disk status, faults, and abnormal videos.

Step 5 Configure one or more email addresses to send the report to, and the content of the email.

1) Click to select the users that have been configured email addresses, or enter an email address, and then press Enter.

Figure 4-95 Invalid email address, you must press Enter

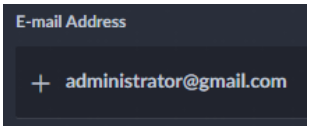
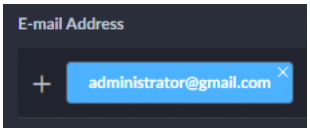


Figure 4-96 Valid email address



2) Configure the content of the email.

Step 6 Send the report.

- Click **Send Now** to immediately send the report that you configured.
- Click **Save**, and then the report will be sent at the defined time.

5 Businesses Operation

5.1 Monitoring Center

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

5.1.1 Main 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 5-1 Monitoring center

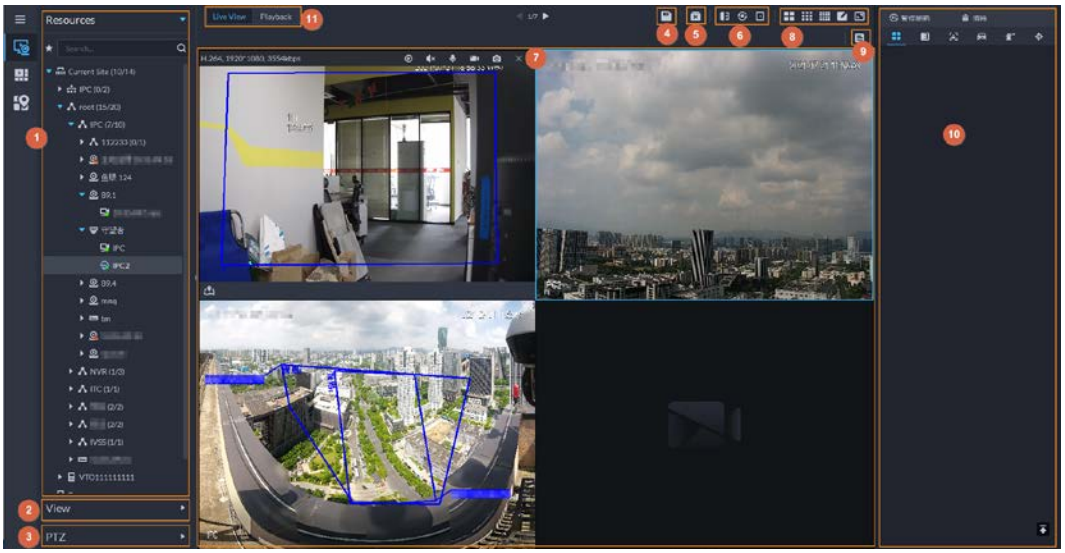


Table 5-1 Interface description

No.	Parameter	Description
1	Favorites and device tree	• List of resources including devices, POS channels, 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 "5.1.3 Playback".

5.1.2 Video Monitoring

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

5.1.2.1 Viewing Live Video

View the live video of connected devices.

This section only introduces viewing live video. For POS live view, see "6.4 POS". For map live view, see "4.2 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

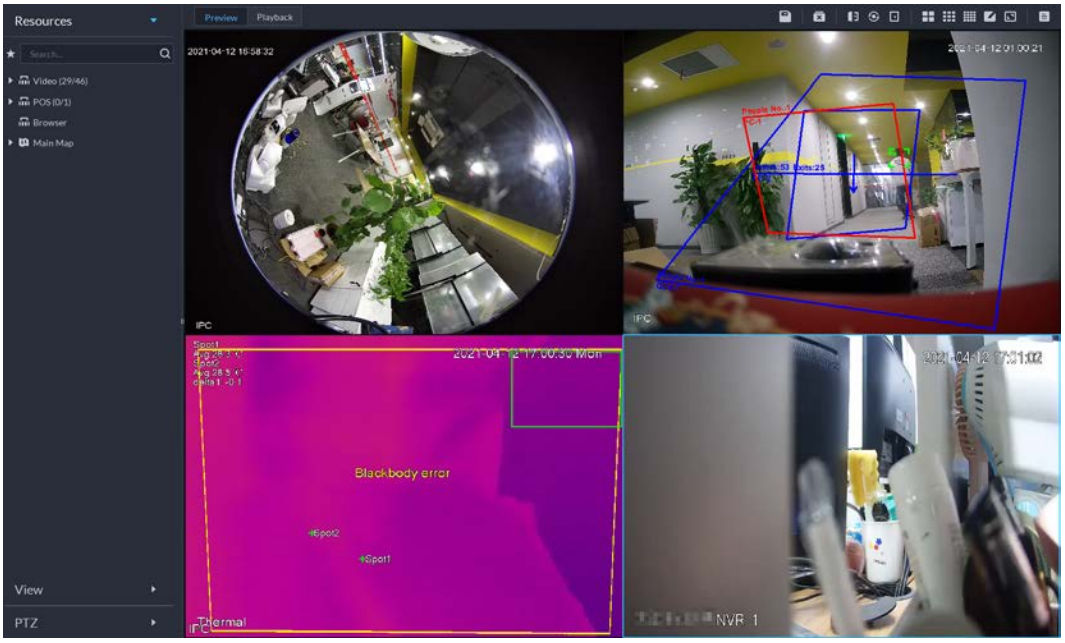
window on the right.

- 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.

  ◇ 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 5-2 Live view



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

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

Figure 5-3 Live window

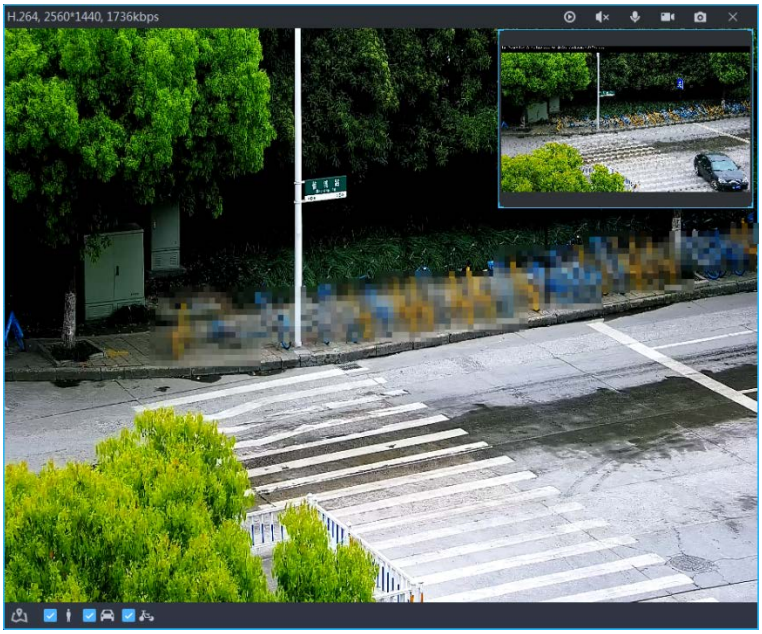
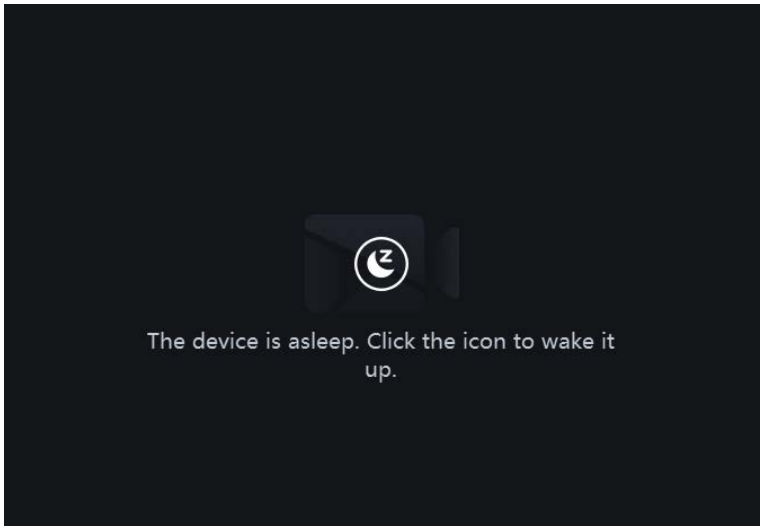


Table 5-2 Parameter description

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 "8.3.5 Configure File Storage Settings".
	Snapshot	Take a snapshot. The snapshots are saved to ..*DSS\DSS Client\Picture* by default. To change the snapshot storage path, see "8.3.5 Configure File Storage Settings".
	Close	Close the video.

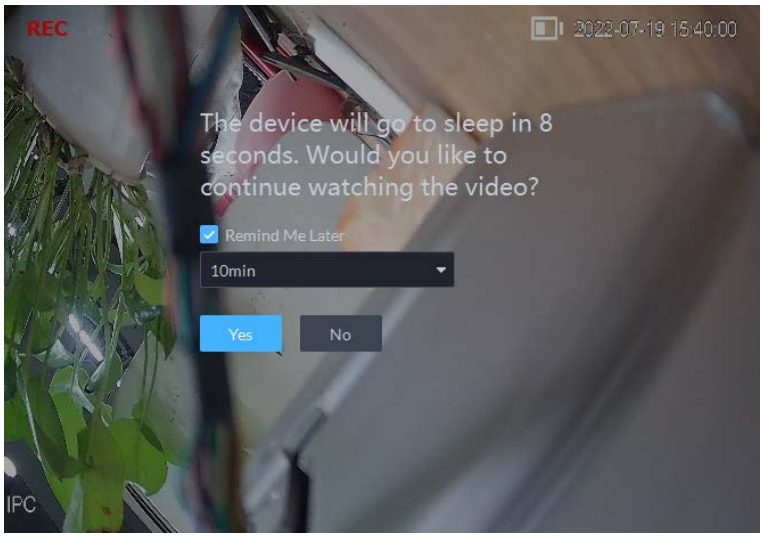
- Sleep function is supported for IPCs that use 4G mobile network to communicate and are solar-powered.
  - ◇ When the device is asleep, you can click to wake it up.

Figure 5-4 Wake up the device



- The device will regularly request to sleep to save battery. When you are viewing its live video, the device will request to sleep every 2 minutes. When you are not viewing its live video, the device will request to sleep every 1 minute. You can accept or reject so that you can continue to watch live video. When rejecting the request, you can choose whether to delay the next request from the device.

Figure 5-5 Request to sleep from the device



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

The menu varies depending on device functions.

Figure 5-6 Live video operation menu

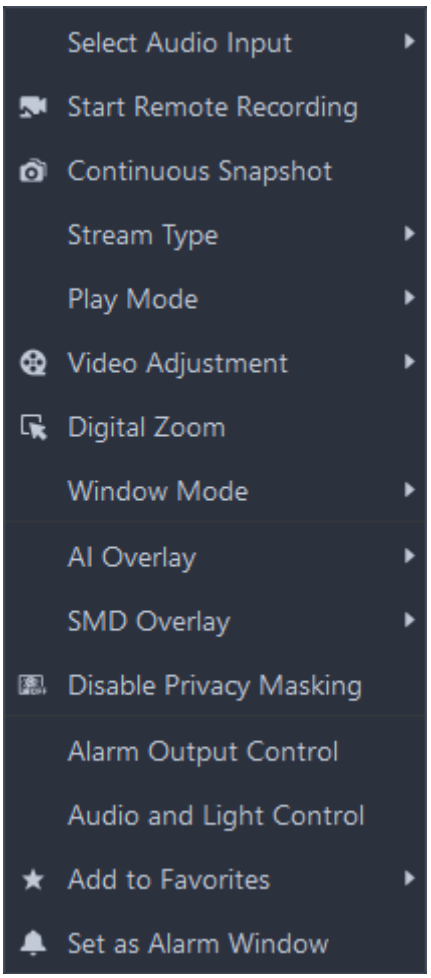


Table 5-3 Description

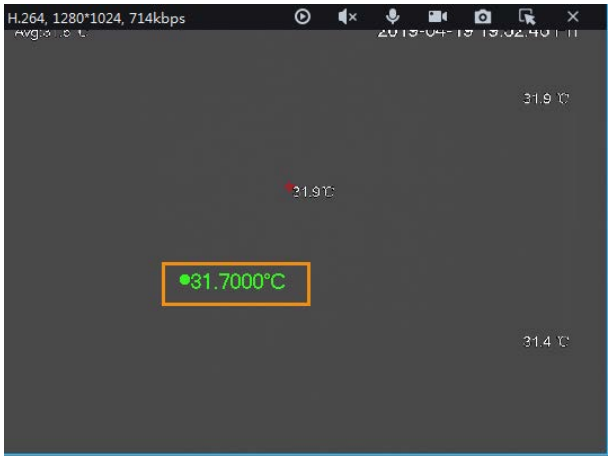
Parameters	Description
Audio Input Selection	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Start Remote Record	Record the audio and video in the current window, and save the recordings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

Parameters	Description
Play Mode	• Real-Time Priority: The video is in real-time, but video quality might be reduced. • Fluency Priority: The video is fluent, but video lagging might occur. • Balance Priority: Real-time priority or fluency priority, depending on actual conditions. • Custom: Configure the video buffer time from **Local Settings > Video**. The larger the value, the more stable the video quality.
Video Adjustment	Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement.
Digital Zoom	Click it, and then click and hold the video image to zoom in on the image. Right-click the image, and then select **Digital Zoom** again to exit zooming in.
Window Mode	Divide one window into 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 5-7 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 5-8 Live view

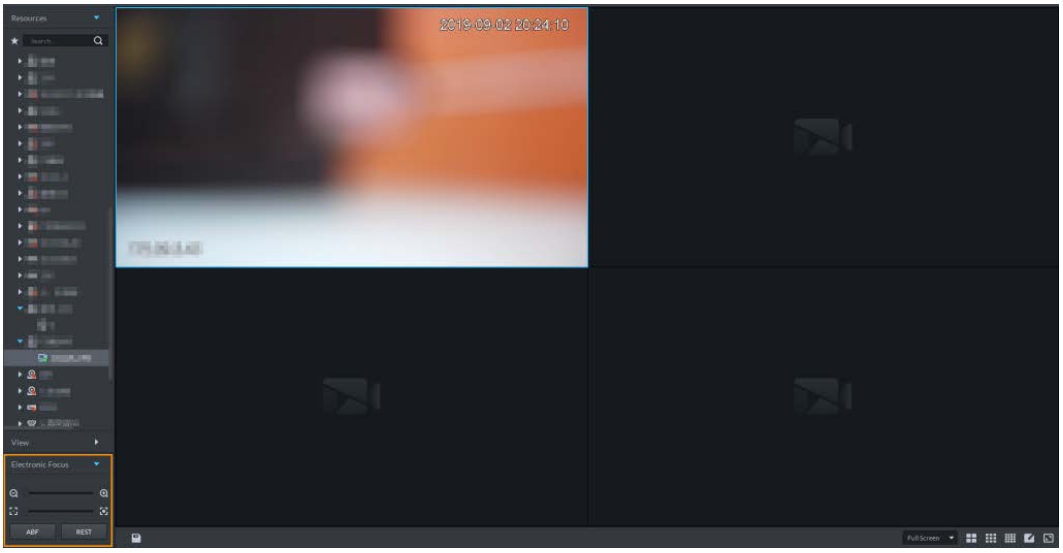


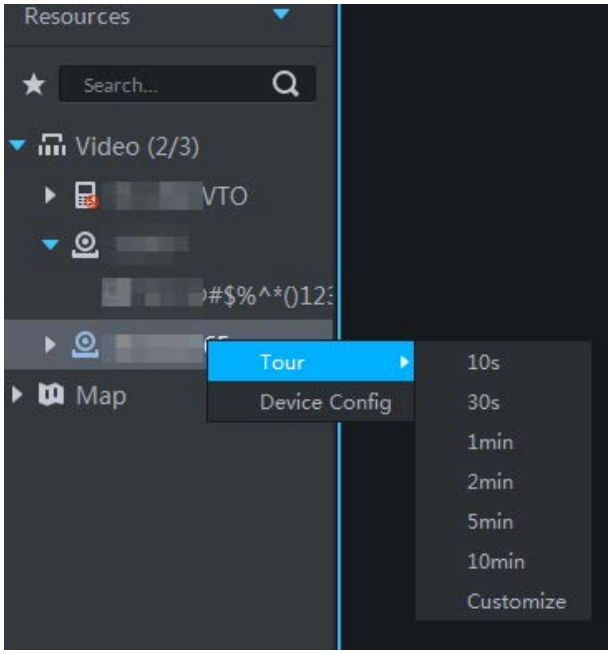
Table 5-4 Description

Parameters	Description
Zoom +/- (for embedded zoom lens)	Zoom in/out. Click or click and hold or , or drag the slider to the left or right to zoom in/out.
Focus +/-	Adjust camera focus to achieve the best video definition. Click or click and hold or , or drag the slider to the left or right to adjust focus.
Auto Focusing (for embedded zoom lens)	Adjust image definition automatically. Other focusing operations are unavailable during auto focusing.
ABF (auto back focusing, for external CS electronic lens)	
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 5-9 Start tour



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

- Region of interest (RoI)

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

  On the live view 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 5-10 Split mode

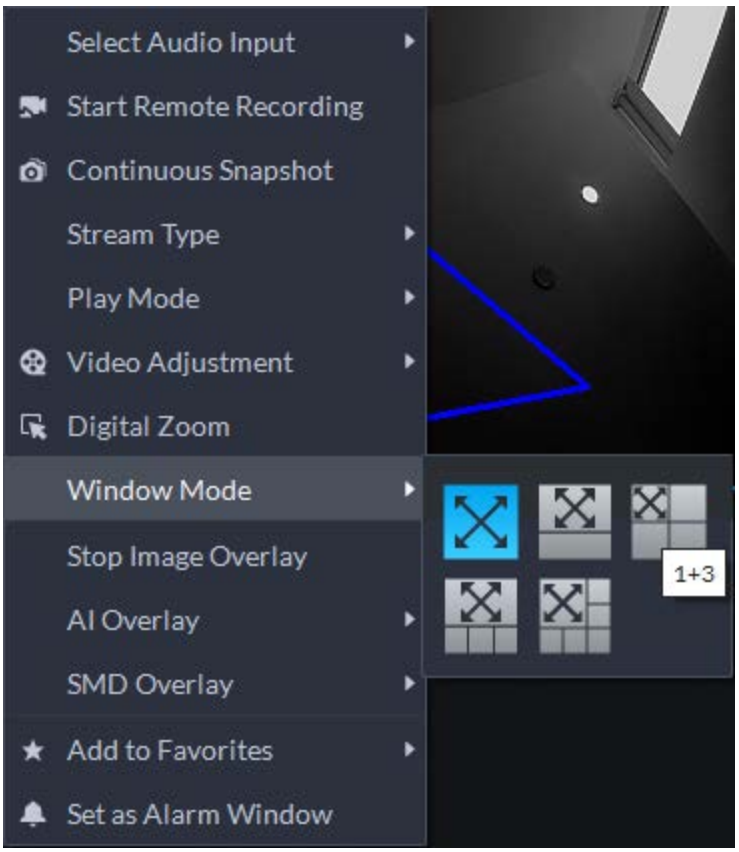
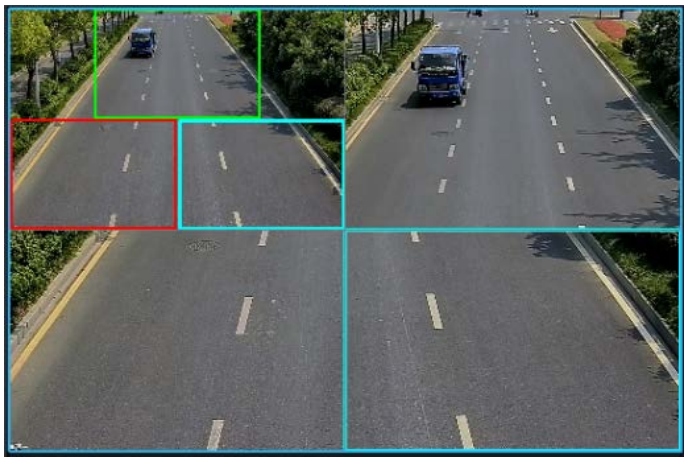


Figure 5-11 1+3 mode



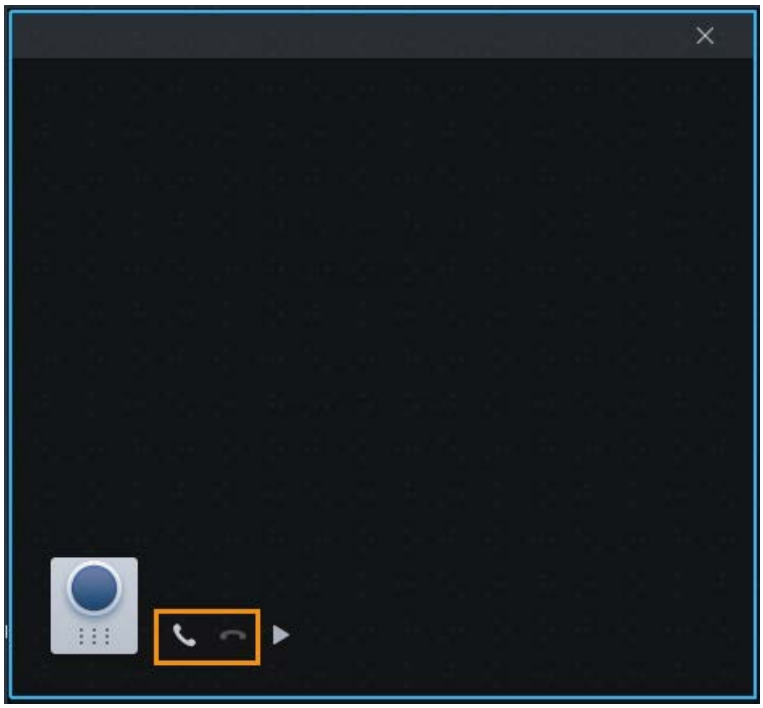
- View real-time events.
  Click to open the event panel, which displays the real-time alarm events of the channel.
  - Click the event type on the top of the event panel to view the corresponding event.
  - Click event record to view the snapshot. Video playback is also supported. Operations related 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 5-12 Lock/unlock the door

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

Figure 5-13 Video intercom



5.1.2.2 View

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

5.1.2.2.1 Creating View

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

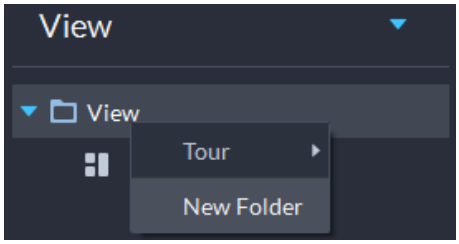
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center**.

Step 2 Click .

Step 3 Create a view group.

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

Figure 5-14 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**.

5.1.2.2.2 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 5-15 Go to video tour page

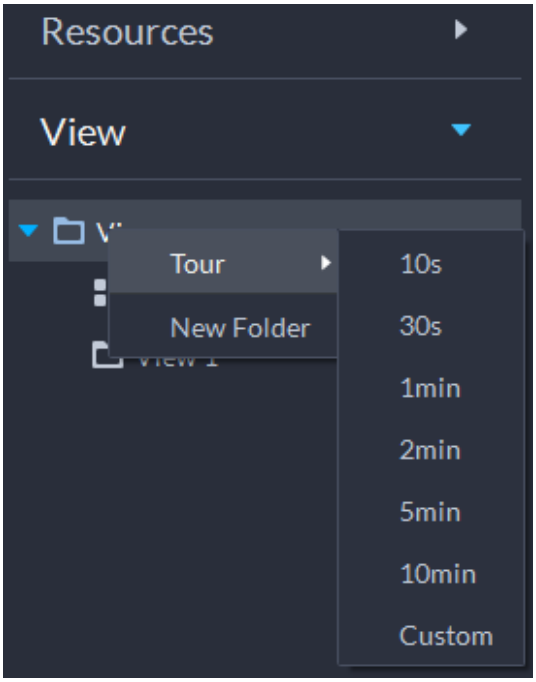
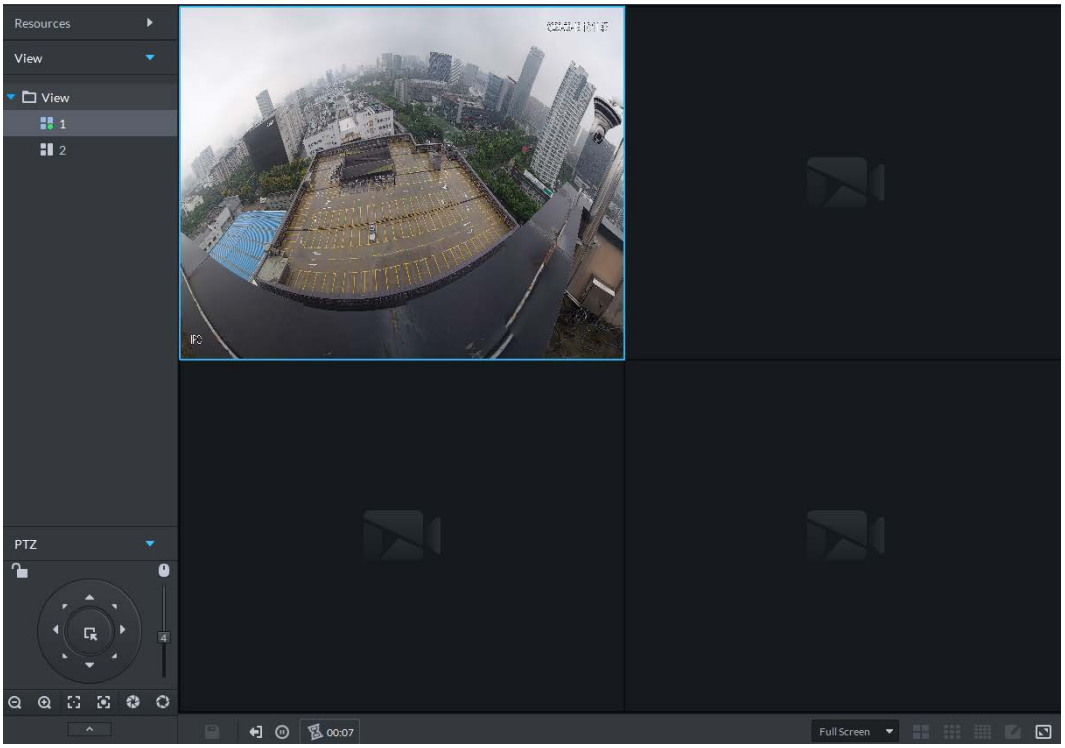


Figure 5-16 View tour



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

5.1.2.3 Favorites

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

5.1.2.3.1 Creating Favorites

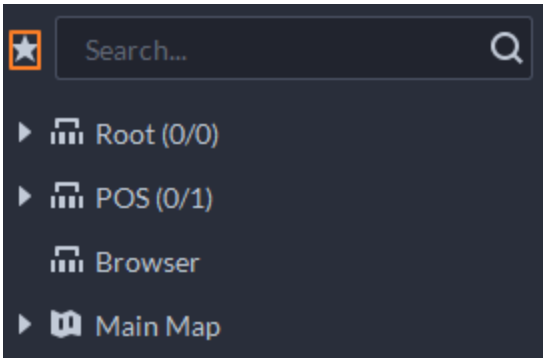
Step 1 Log in to the DSS Client. On the **Home** page, click , and then select **Monitoring Center**.

Step 2 Click .

Step 3 Create favorites.

1) Click .

Figure 5-17 Favorites



2) Right-click root node or created favorites, and then select **New Folder**.
3) Enter a folder name, click **OK**.
   Lower-level favorites are generated under the selected root node or favorites.
4) Click .
   The system goes back to the device list.

Step 4 Add channels to favorites.

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

5.1.2.3.2 Viewing Favorites

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

5.1.2.4 PTZ

Operate PTZ cameras during live view on the DSS Client.

5.1.2.4.1 Configuring Preset

A preset is a set of parameters involving PTZ direction and focus. By calling a preset, you can quickly

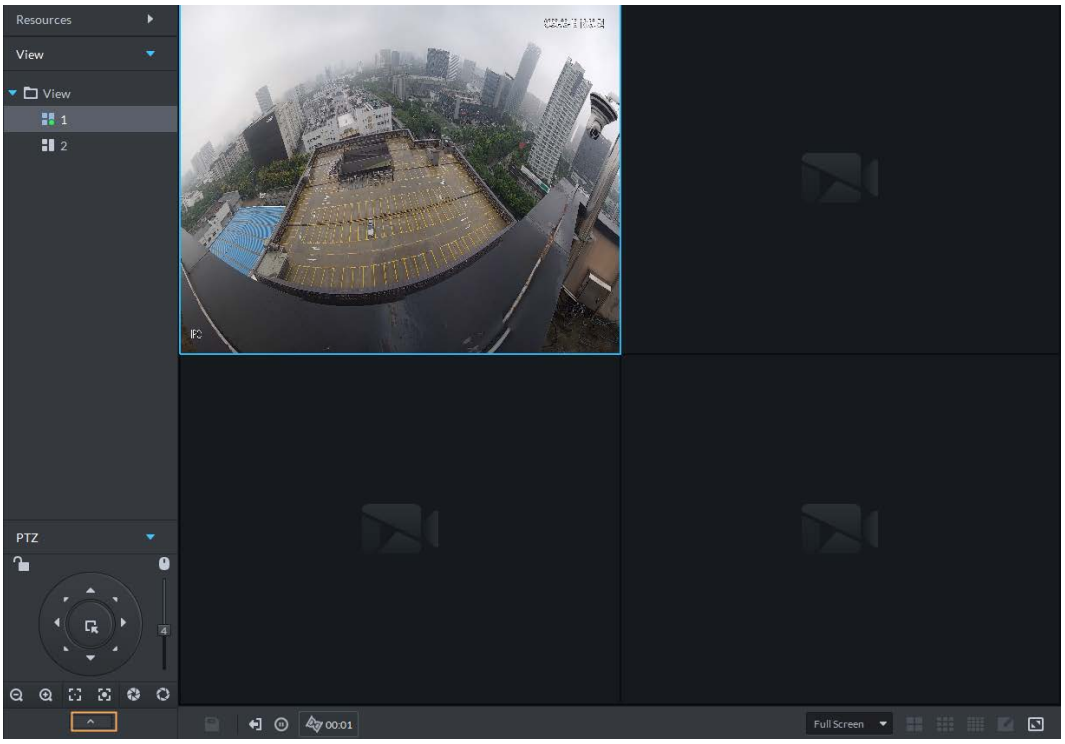
rotate the camera to the pre-defined position.

Procedure

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

Step 2 Click .

Figure 5-18 Go to PTZ control panel



Step 3 Click .

Step 4 Add a preset.

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

Related Operations

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

5.1.2.4.2 Configuring Tour

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

Prerequisites

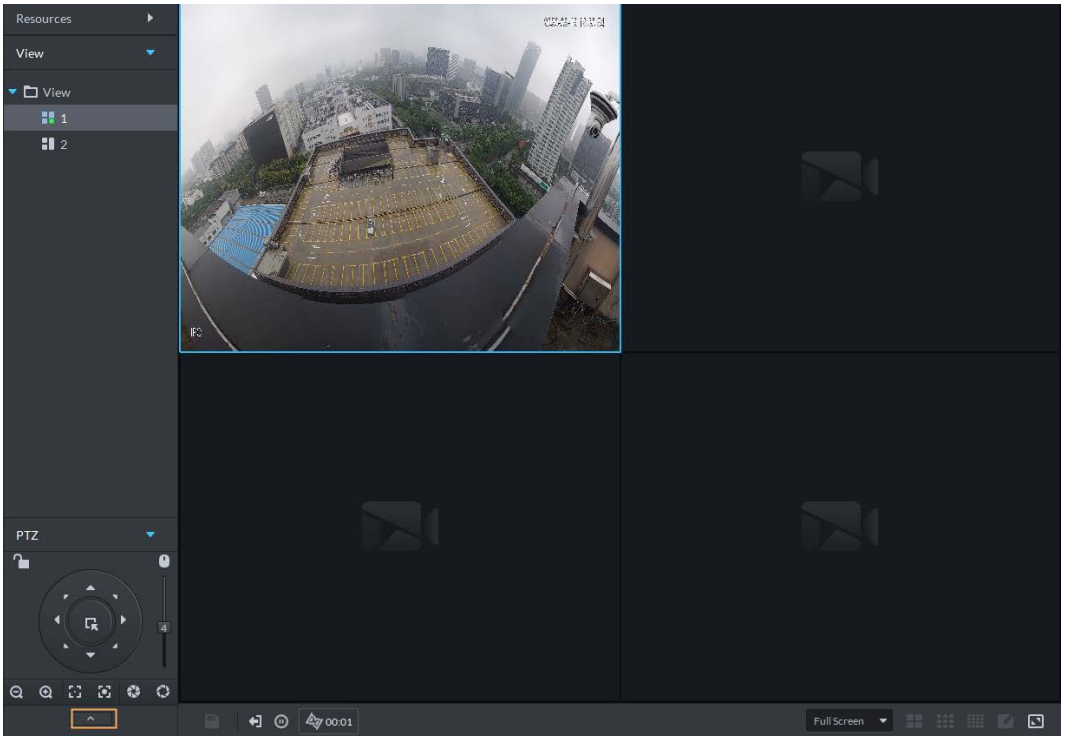
You have added at least 2 presets.

Procedure

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

Step 2 Click .

Figure 5-19 Go to PTZ control panel



Step 3 Click .

Step 4 Click .

Step 5 Add tours.

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

Related Operations

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

5.1.2.4.3 Configuring Pattern

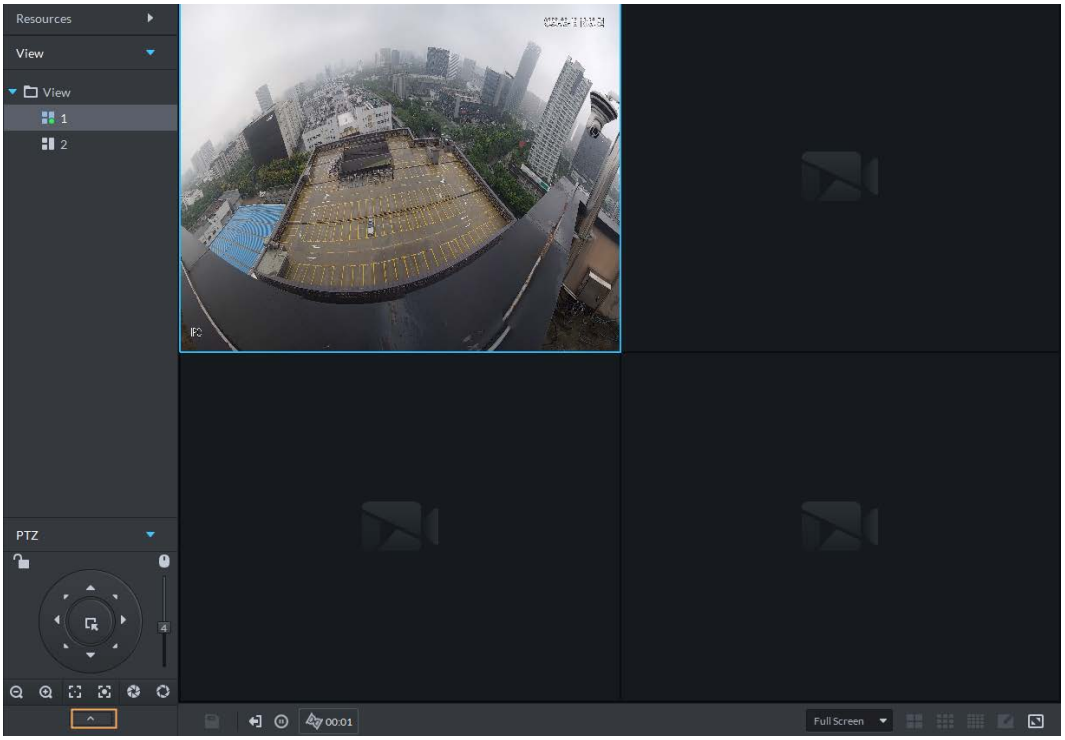
A pattern is a record of a consecutive series of PTZ operations. You can select a pattern to repeat the corresponding operations quickly. See pattern configuration instructions as follows.

Procedure

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

Step 2 Click .

Figure 5-20 Go to PTZ control panel



Step 3 Click .

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

Step 5 Click .

Related Operations

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

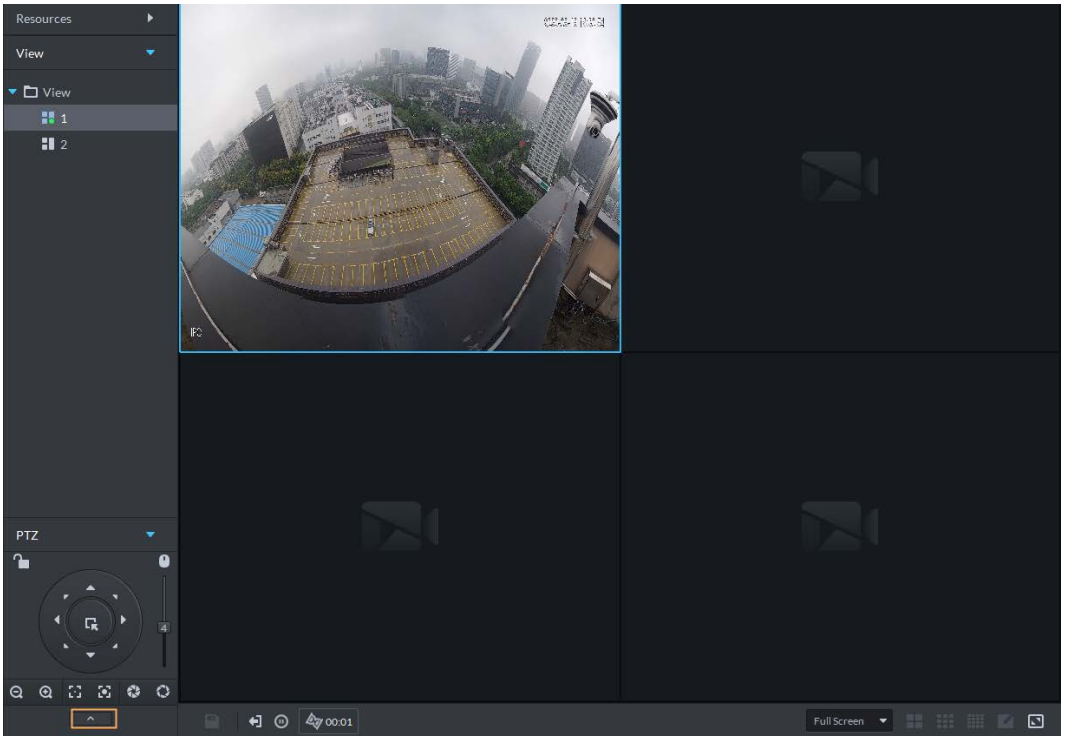
5.1.2.4.4 Configuring Scan

The camera automatically scans horizontally at a certain speed.

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

Step 2 Click .

Figure 5-21 Go to PTZ control panel



Step 3 Click .

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

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

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

5.1.2.4.5 Enabling/Disabling Pan

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

5.1.2.4.6 Enabling/Disabling Wiper

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

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

5.1.2.4.7 Enabling/Disabling Light

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

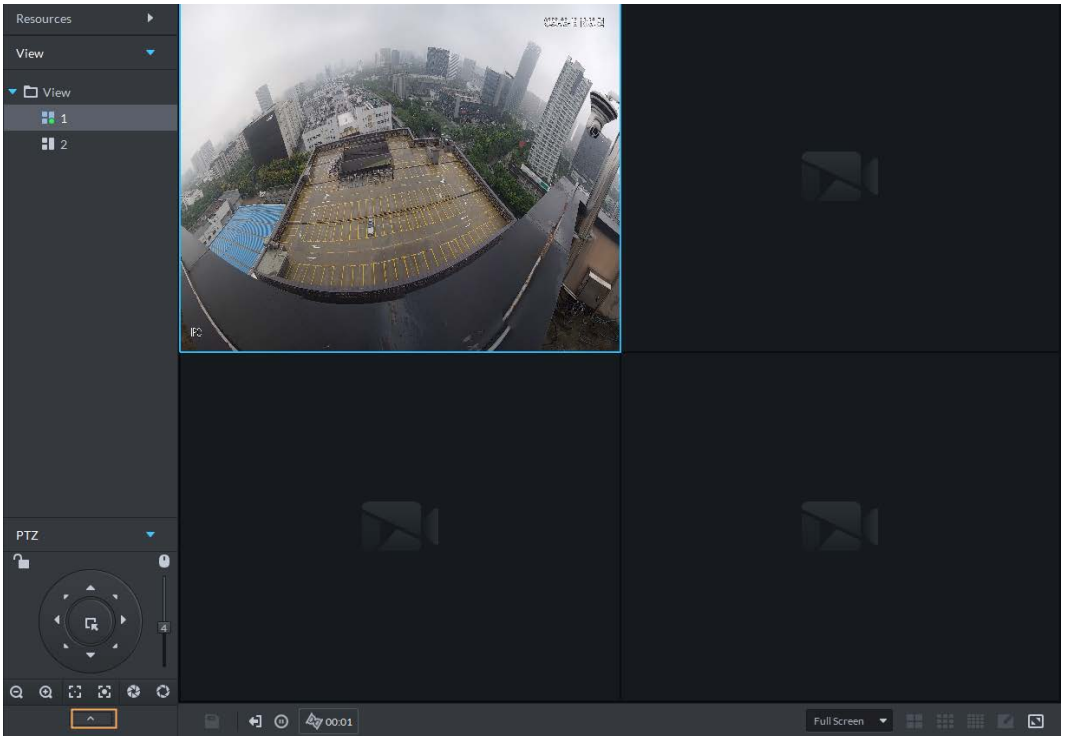
On the **Monitoring Center** page, open the video of a PTZ camera. Click , and then click to turn on light. After enabling light, click to turn off light.

5.1.2.4.8 Configuring Custom Command

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

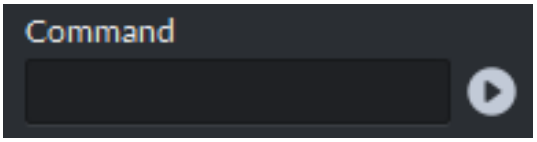
Step 2 Click .

Figure 5-22 Go to PTZ control panel



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

Figure 5-23 Custom command



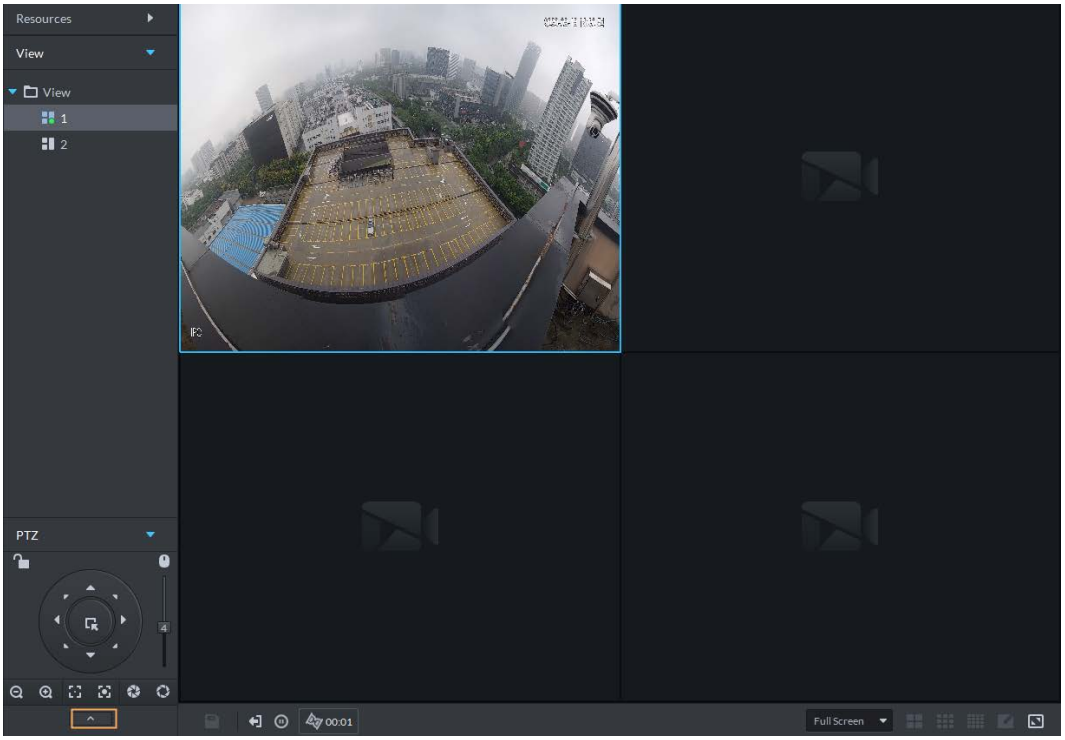
Step 4 Click to show the command functions.

5.1.2.4.9 PTZ Menu

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

Step 2 Click .

Figure 5-24 Go to PTZ control panel



Step 3 Click .

Step 4 Click .

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

Figure 5-25 Go to PTZ menu configuration page

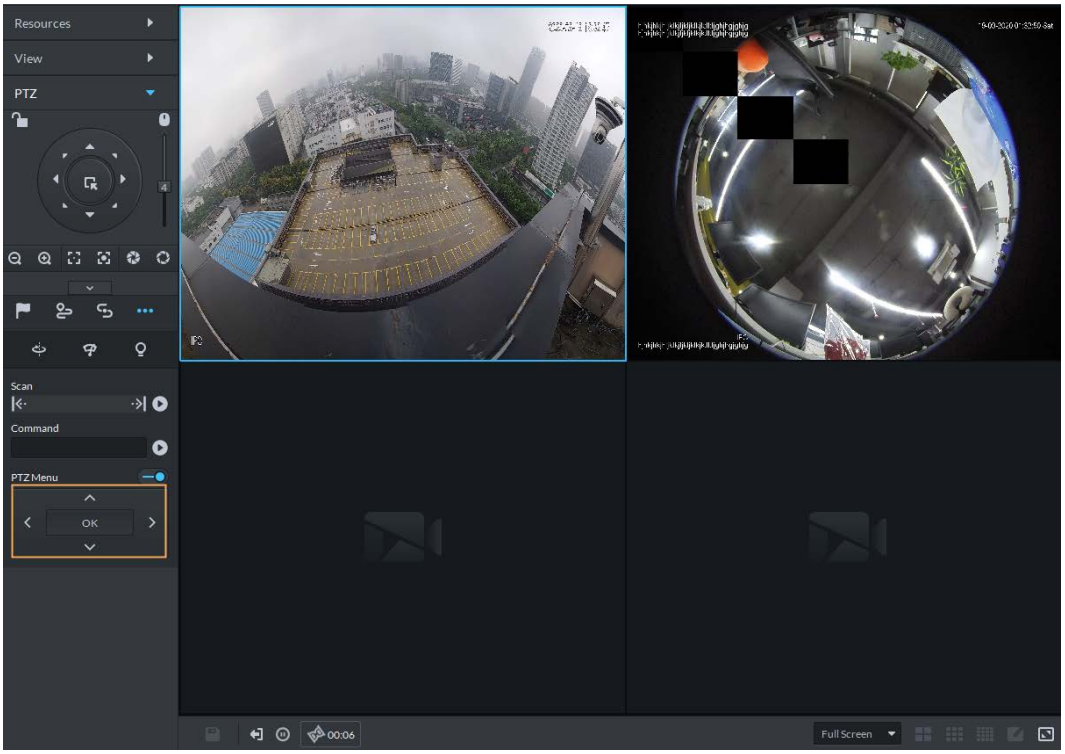


Table 5-5 PTZ menu description

Parameters	Description
/	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.

5.1.2.5 Fisheye-PTZ Smart Track

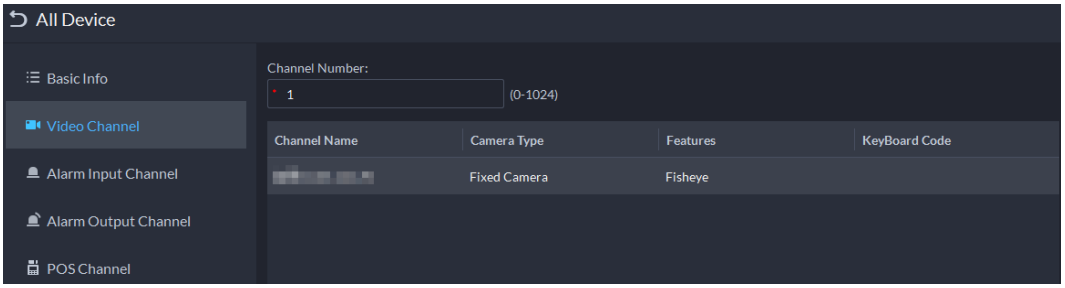
Link a PTZ camera to a fisheye camera so that when the fisheye camera detects a target, the PTZ camera automatically rotates to it and track.

5.1.2.5.1 Preparations

Make sure the following preparations have been completed:

- Fisheye camera and PTZ camera are well deployed. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. For details, see "3 Basic Configurations".
  - When adding cameras, select **Encoder** from **Device Category**.
  - **Features** of fisheye camera is set to **Fisheye**. For details, see "3.2.2.5.2 Modifying Device Information".

Figure 5-26 Set fisheye camera features



5.1.2.5.2 Configuring Fisheye-PTZ Smart Track

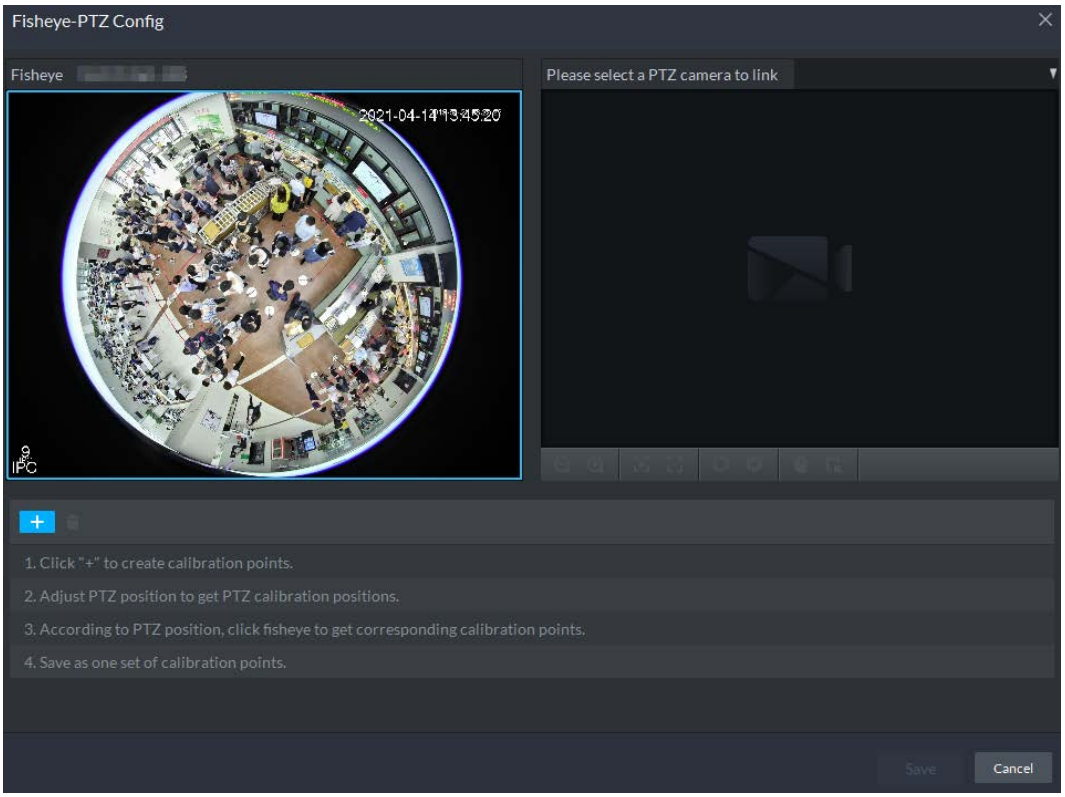
Step 1 Log in to the DSS Client. On the **Home** page, click , and then click **Monitoring Center**.

Step 2 Click .

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

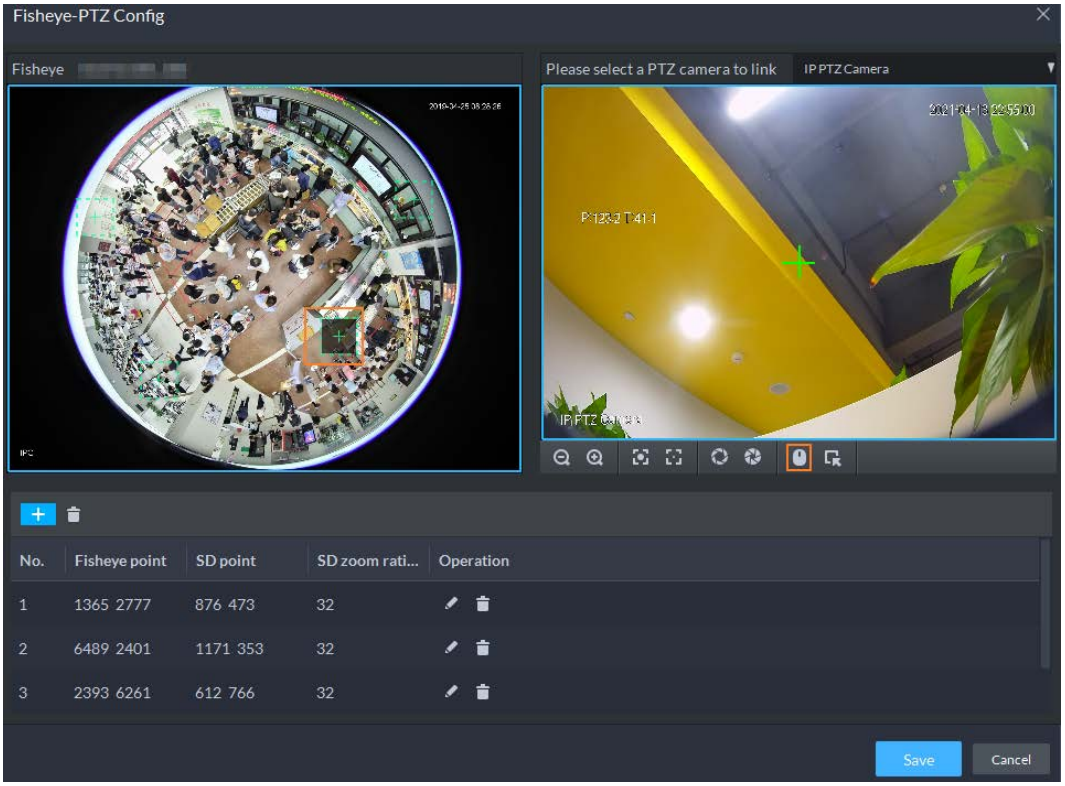
Step 4 Click next to **Please select a PTZ camera to link**, and then select a PTZ camera.

Figure 5-27 Set smart track rules (1)



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

Figure 5-28 Set smart track rules (2)



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

Step 6 Click to save the calibration point.

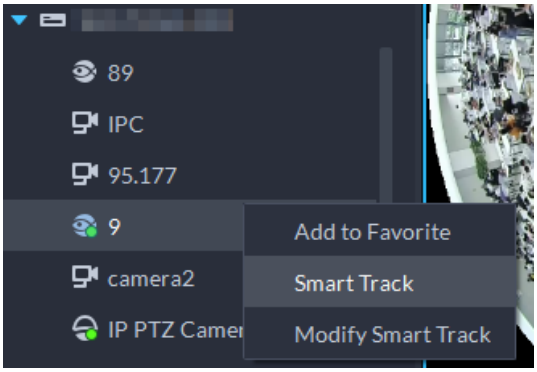
See above steps to add at least three calibration points. These three points shall not be on the same straight line.

Step 7 Click **Save**.

5.1.2.5.3 Applying Fisheye-PTZ Smart Track

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

Figure 5-29 Select a smart track channel



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

5.1.3 Playback

Play back recorded videos.

5.1.3.1 Page Description

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

Figure 5-30 Playback page

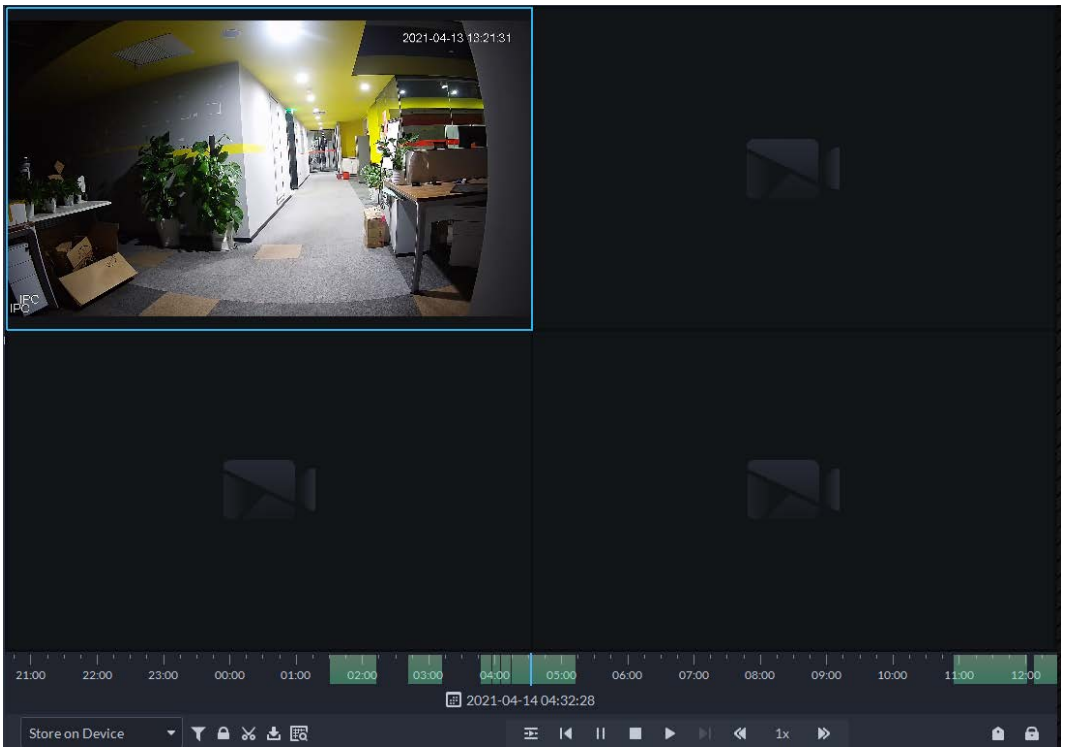
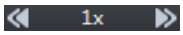
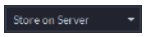


Table 5-6 Description

Icon	Description
	Lock the video stored to the server within some period of designated channel. Locked video will not be overwritten when disk is full.

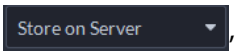
Icon	Description
	Cut video
	Download video
	Filter video according to record type.
	Make dynamic detection analysis over some area of the record image, and it only plays back the video with dynamic image in the detection area.
	Play multiple recorded videos from the same time. For example, you are playing recorded videos from 3 channels at the same time. Select channels, configure when you want to play the recorded video from, and then click this icon. All 3 channels will play recorded videos from the same time.
	Stop/pause playback
	Frame by frame playback/frame by frame backward.
	Fast/slow playback. Max. supports 64X or 1/64X.
	During playback, you can drag time progress bar to play back record at the specific time.
	Select the storage location of the video to be searched. Supports searching for the video on the platform server or storage device.
	Tag records.
	Lock records.

5.1.3.2 Playing Back Recordings

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

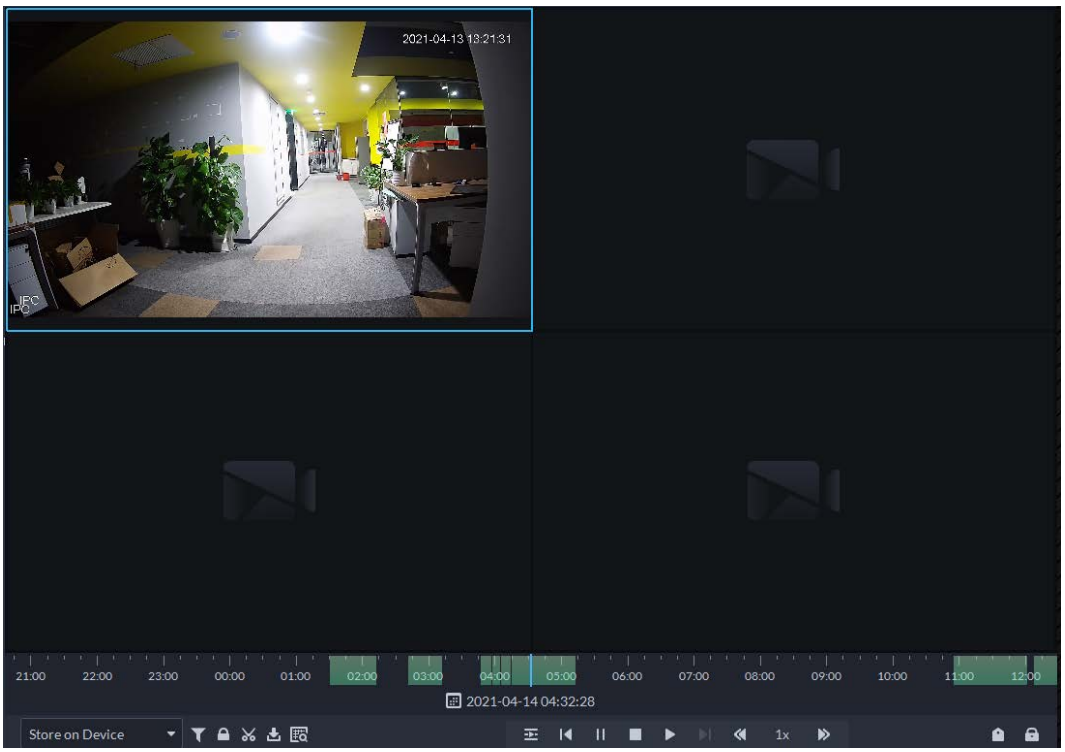
Step 2 Click the **Playback** tab.

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  , and then click  to select the date.

Dates with blue dot means there are recordings.

Figure 5-31 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 5-32 Video playback

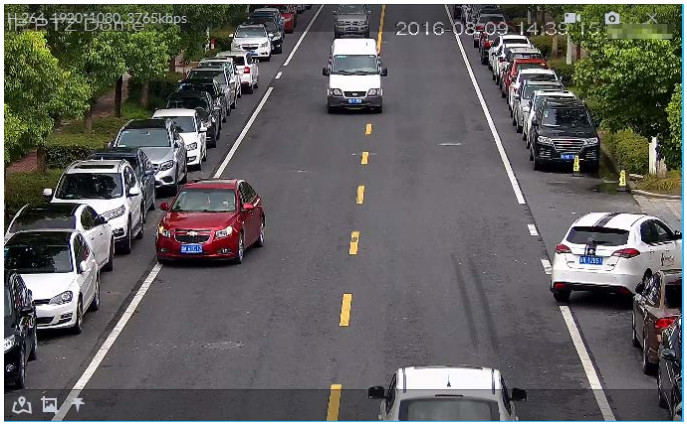


Table 5-7 Description

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.

Icon	Name	Description
	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 5-33 Shortcut menu

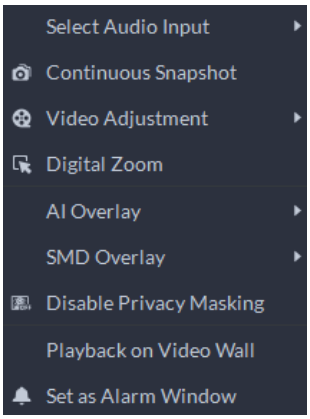


Table 5-8 Description

Parameters	Description
Select Audio Input	If the camera has more than one audio input channels, you can select one or select the mixed audio. This configuration is effective with both live view and playback.
Continuous Snapshot	Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to ..\DSS\DSS Client\Picture by default. To change the snapshot saving path, see "8.3.5 Configure File Storage Settings".
Video Adjustment	Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement.
Digital Zoom	Click it, and then double-click the video image to zoom in the image. Double-click the image again to exit zooming in.
AI Overlay	The client does not show rule lines over live video by default. When needed, you can click **AI Overlay** and enable **Rule Overlay** and **Bounding Box Overlay**, and then the live video shows rule lines if the AI detection rules are enabled on the device. This configuration is effective with the current selected channel both in live view and playback.

Parameters	Description
SMD Overlay	Enable **SMD Overlay** to show target bounding box over live video. When SMD is enabled on the device, you can enable **SMD Overlay** for the device channel, and then the live video will display dynamic target bounding boxes. This configuration is effective with the current selected channel both in live view and playback.
Disable Privacy Masking	For a camera that supports privacy masking of human face, you can disable the masking here to view the face image.
Playback on Video Wall	Play the video of the current channel on video wall. Make sure that video wall is configured (see "5.1.5 Video Wall").
Set as Alarm Window	When selecting open alarm linkage video **In Preview**(in live window) from **Local Settings > Alarm**, then the video will be displayed on the window which is set to alarm window. If multiple alarms are triggered, the video linked to the latest alarm will be opened. If the number of alarm windows is fewer than the number of linkage videos, the video linked to the earliest-triggered alarm will be opened. After enabling **Set as Alarm Window**, the window frame is displayed in red.

5.1.3.3 Locking Videos

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

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.

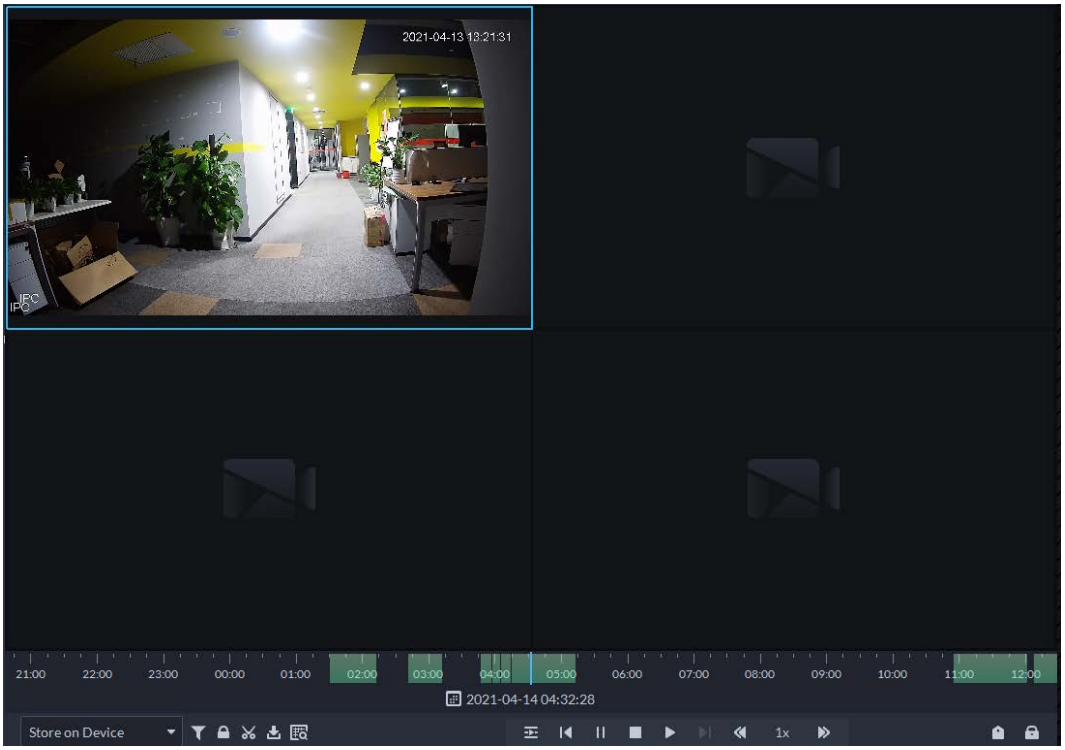
Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

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.

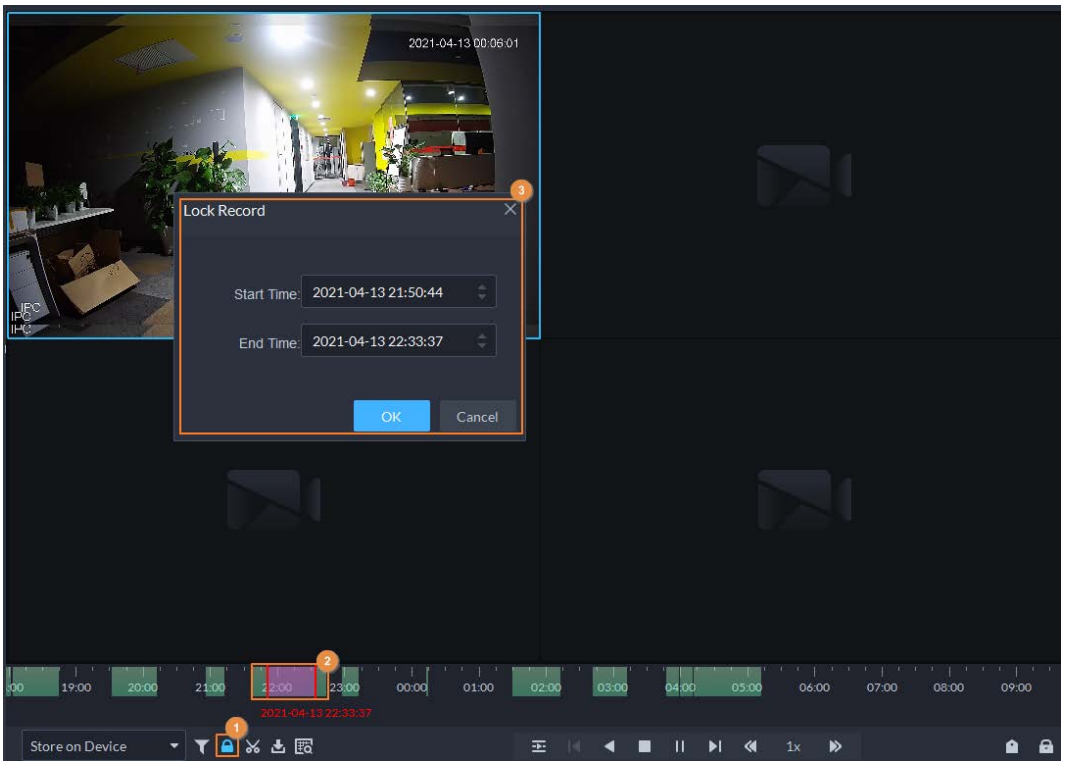
Dates with blue dot means there are video recordings.

Figure 5-34 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 5-35 Lock record



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

Related Operations

Click 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.

5.1.3.4 Tagging Videos

You can tag records of interest for quick search.

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

Step 2 Click the **Playback** tab.

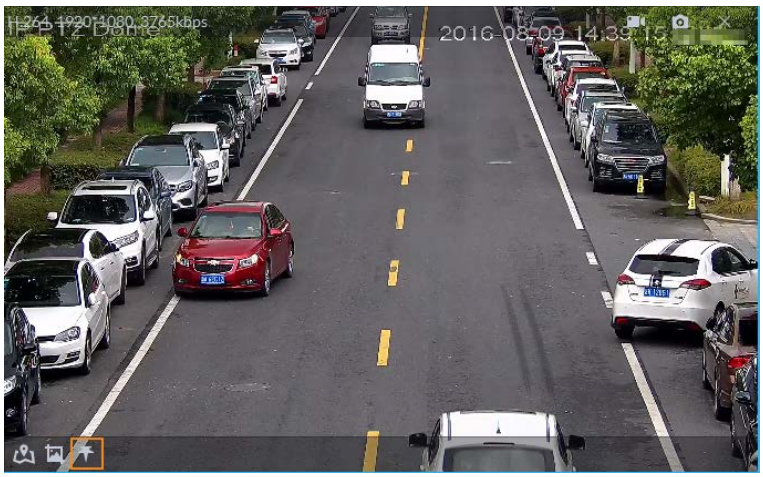
Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

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 5-36 Playback page



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

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

5.1.3.5 Filtering 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**.

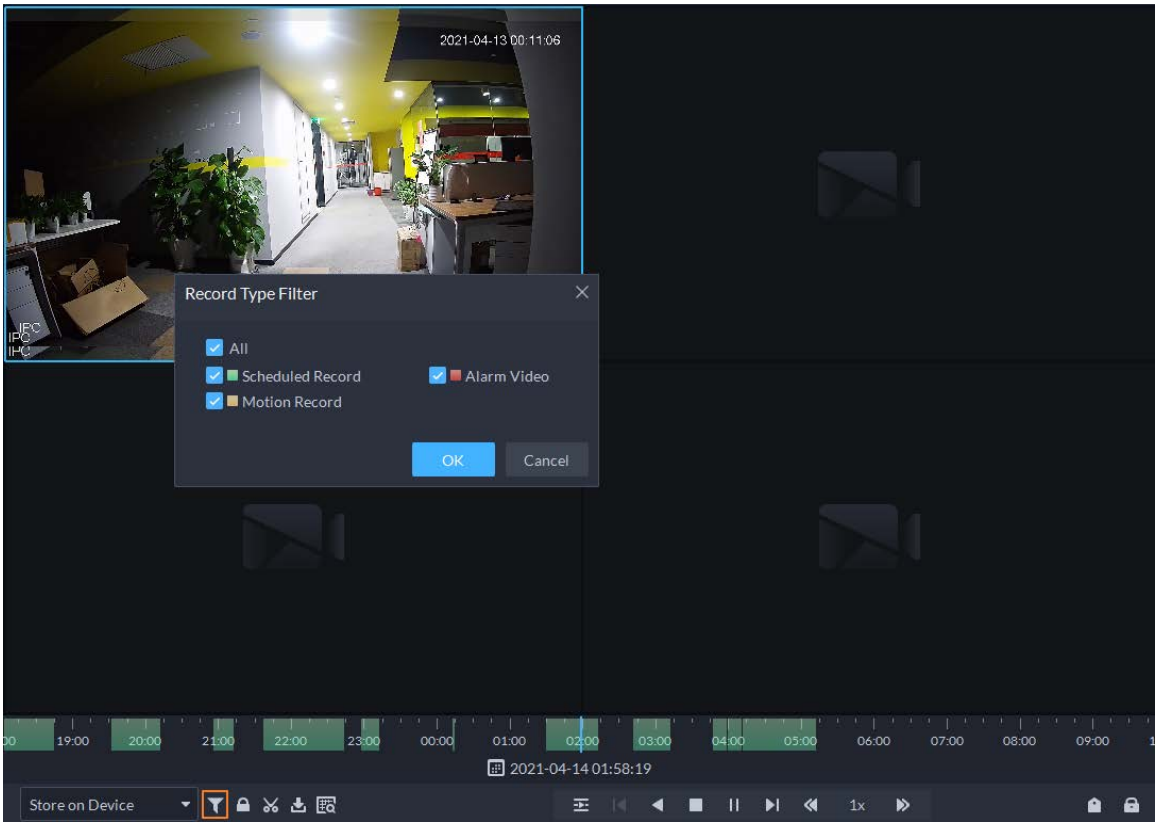
Step 2 Click the **Playback** tab.

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 5-37 Filter record type



5.1.3.6 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.

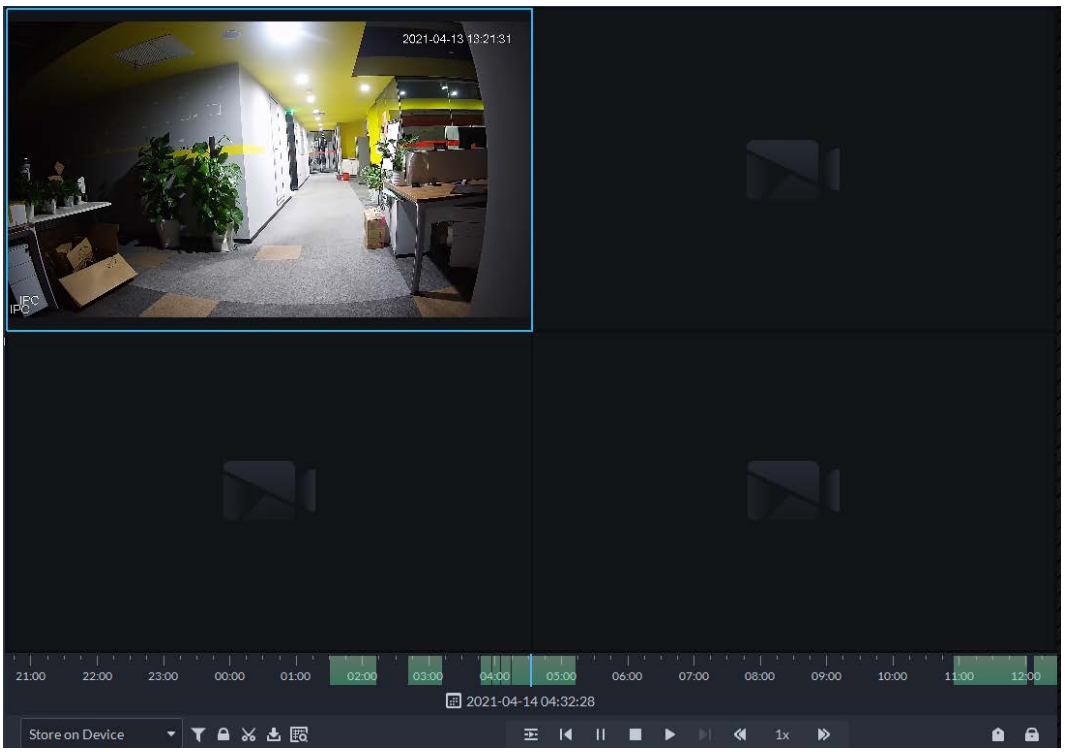
Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

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.

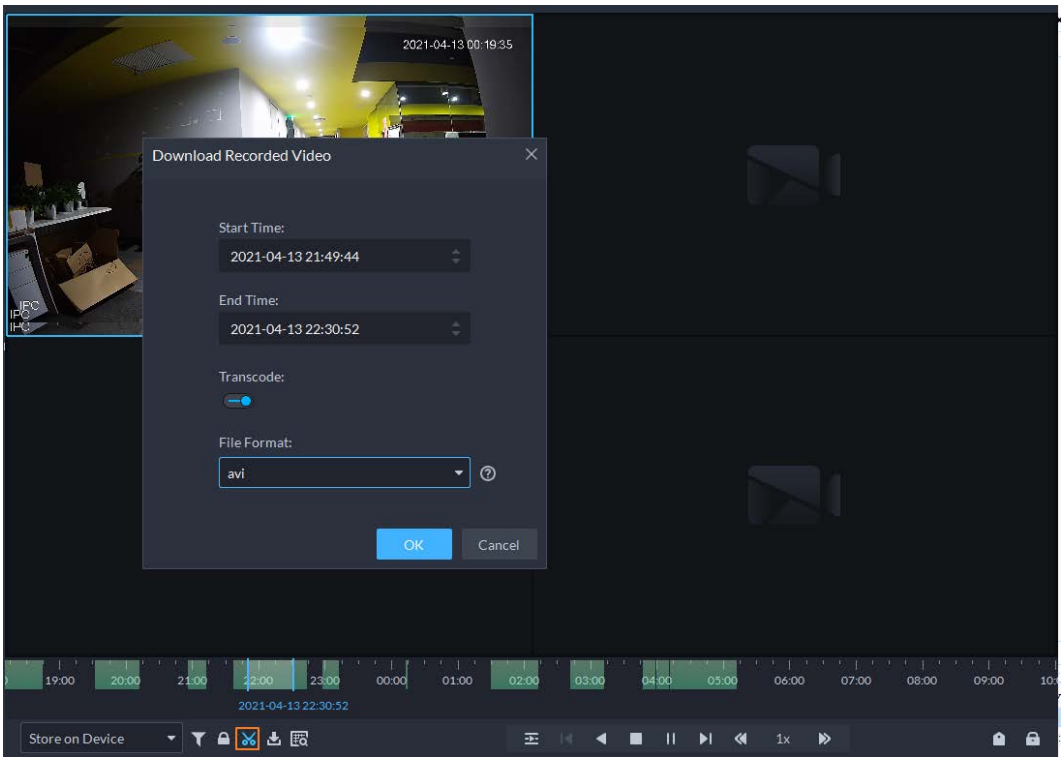
Figure 5-38 Playback page



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

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

Figure 5-39 Download recorded video



Step 7 Enter the password of the current user.

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

Step 9 Click **OK**.

5.1.3.7 Smart Search

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

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

Step 2 Click the **Playback** tab.

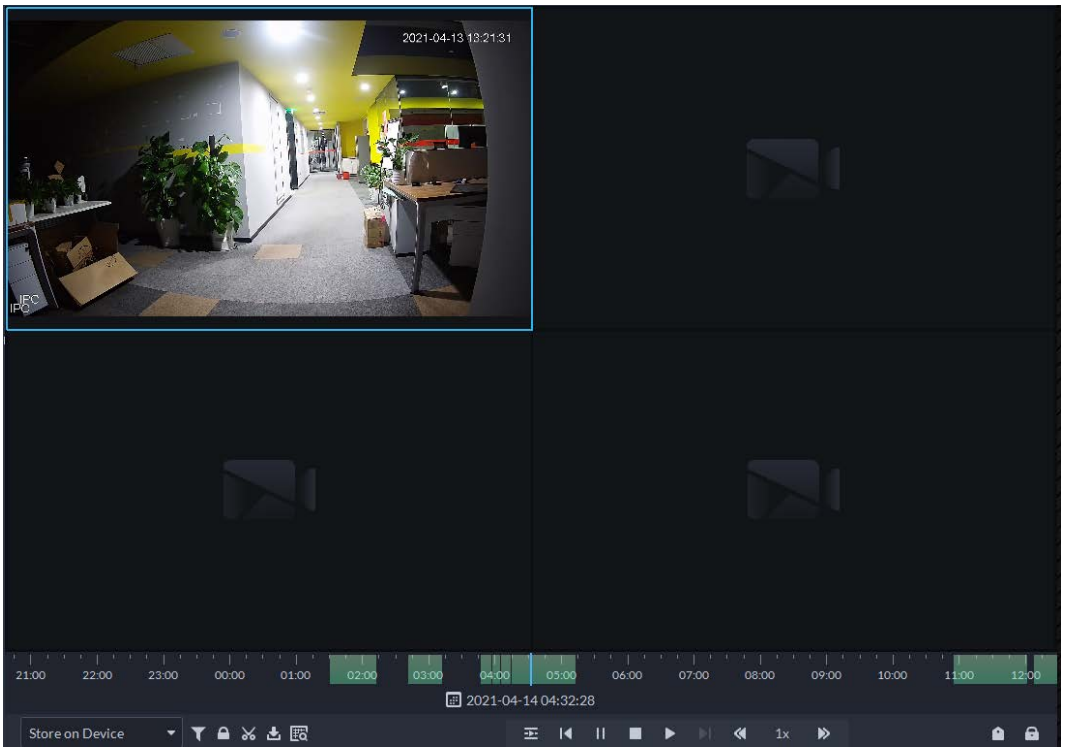
Step 3 Select a channel from the device tree, and then double-click it, or drag it to the window.

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.

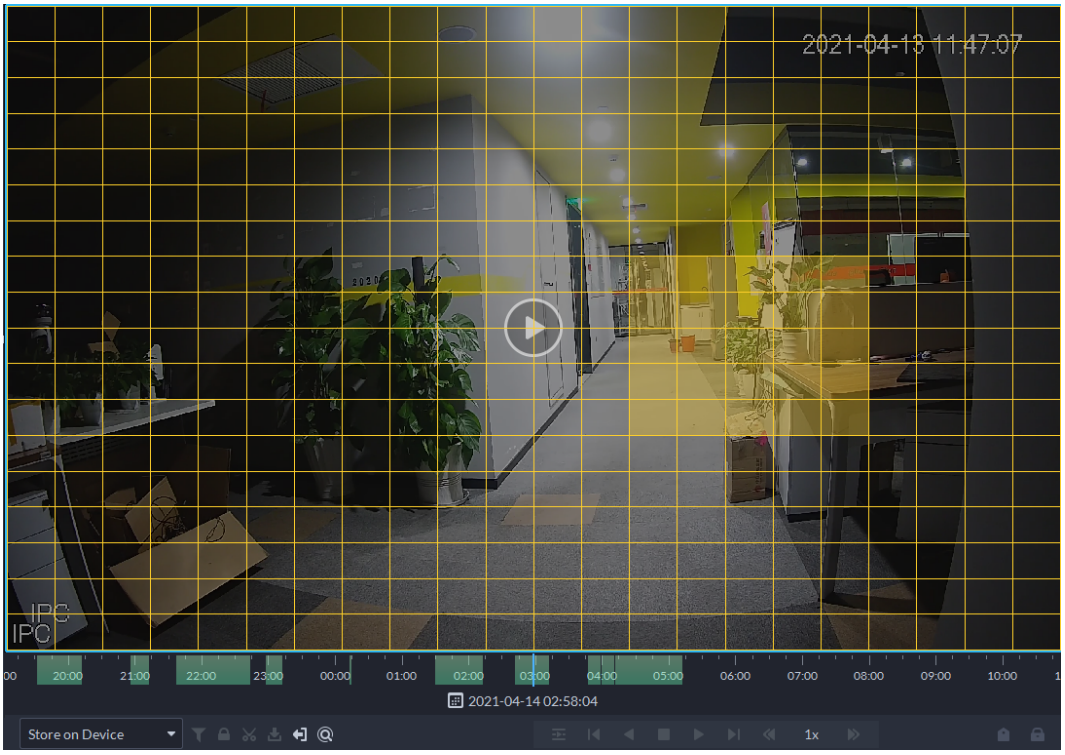
Figure 5-40 Playback page



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 5-41 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.

5.1.4 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 "4.2 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 5-42 View map (GIS map)

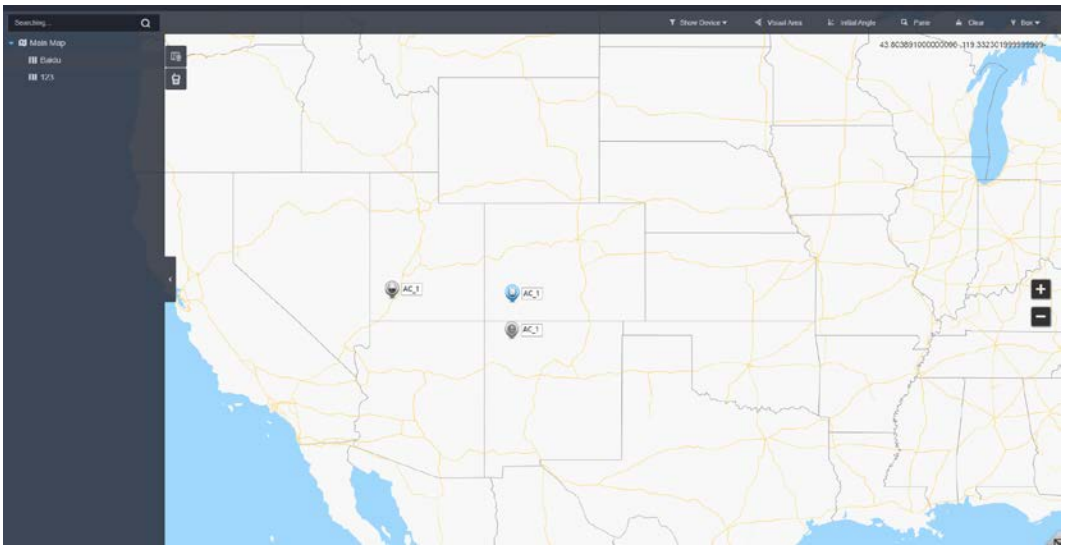
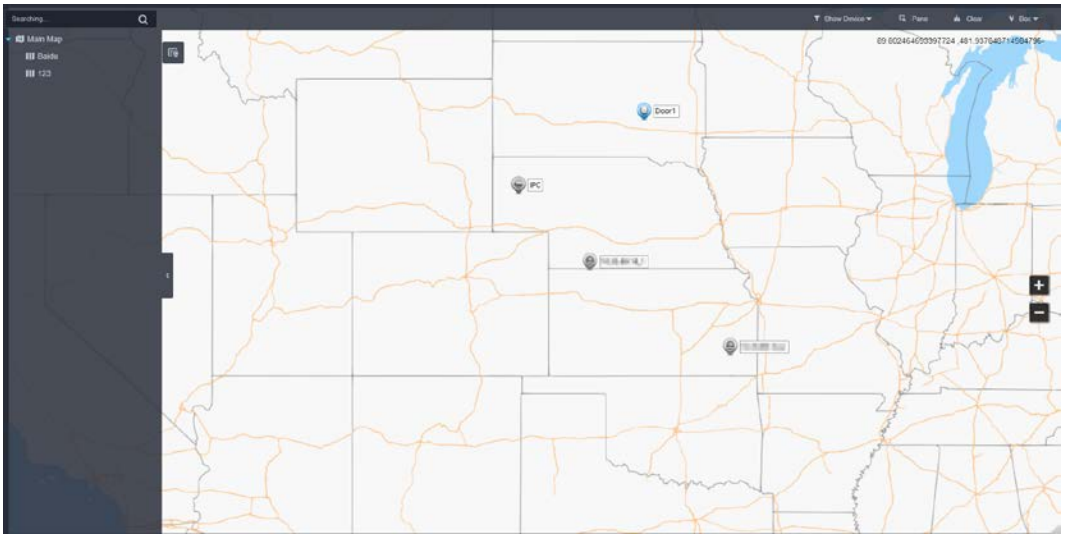


Figure 5-43 View map (raster map)



Step 4 Engage in group talk on the GIS map.

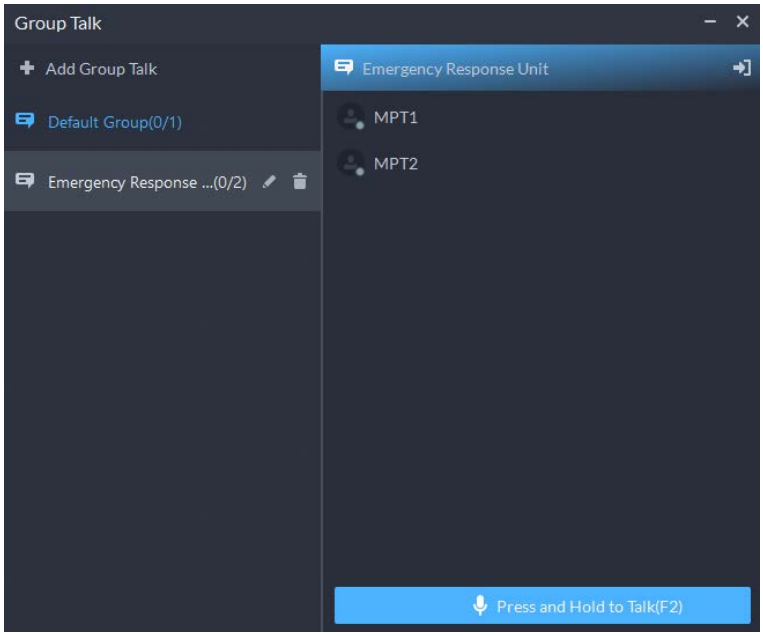
1) Click next to the list of maps.

   The default group includes all MPT users.

   For how to configure an MPT user, see "3.3.2 Adding User".

2) Click **Add Group Talk**.
3) Enter a name for the group, select MPT users, and then click **OK**.
4) Click the new group, and then click on the upper-right corner to join the group.

Figure 5-44 Join the new group



5) Press the F2 key to talk to the users in the group.
6) (Optional) Click and you can edit the users in the group.
The users removed from the group will return to **Default Group**.

Step 5 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.
- Satellite Map
  View the satellite map.
- View live video
  Click **Pane**, select devices on the map, and then click to view videos in batches; or click on the map, and then select to view videos.
- Playback
  Click **Pane**, select devices on the map, and then click to view videos in batches; or click on the map, and then select to view videos.
- Cancel alarms
  Click a device on the map, and then select .
- Show devices
  - On a raster map, you can select to display video channels, access control channels, alarm input channels, lift control channels, and defense zone alarms.
  - On a GIS map, you can select to display video channels, alarm input channels, radar channel, lift control channels, MPT channels, and defense zone alarms.
- Visual area (available on GIS maps)
  If a device supports visual area, click **Visual Area** and double-click a device on the map to show its monitoring area.
- Initial angle (available on GIS maps)

If a device supports initial angle, click **Initial Angle** and double-click a device on the map to show the initial angle.

- Clear
  To clear all markings on the map, click **Clear**.
- Measure distance (available on GIS maps)
  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.
- Measure area (available on GIS maps)
  Select **Box** > **Area**, select a region on the map (double-click to finish drawing), and then the area is measured.
- 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  to view the information of the sub map.
- Double-click  , and then the platform will go to the sub map, where you can view the resources on it.

5.1.5 Video Wall

A video wall, which consists of multiple video screens, is used for displaying videos on the wall, instead of small PC displays.
Complete video wall settings before you can view videos on the wall.

5.1.5.1 Configuring Video Wall

5.1.5.1.1 Page Description

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

page.

Figure 5-45 Video wall

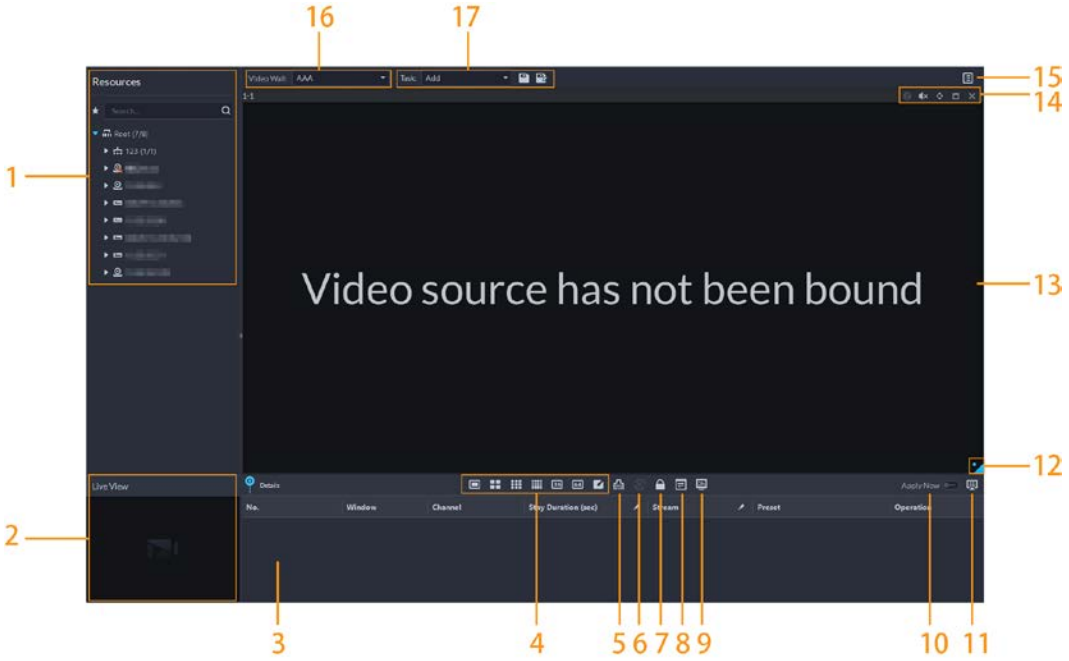


Table 5-9 Page description

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.
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.

No.	Function	Description
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 "5.1.5.1.5 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.

5.1.5.1.2 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 "3 Basic Configurations".
  During configuration, make sure that:
  - When adding a camera, select **Encoder** from **Device Category**.
  - When adding a decoder, select **Video Wall Control** from **Device Category**.

5.1.5.1.3 Adding Video Wall

Add a video wall layout on the platform.

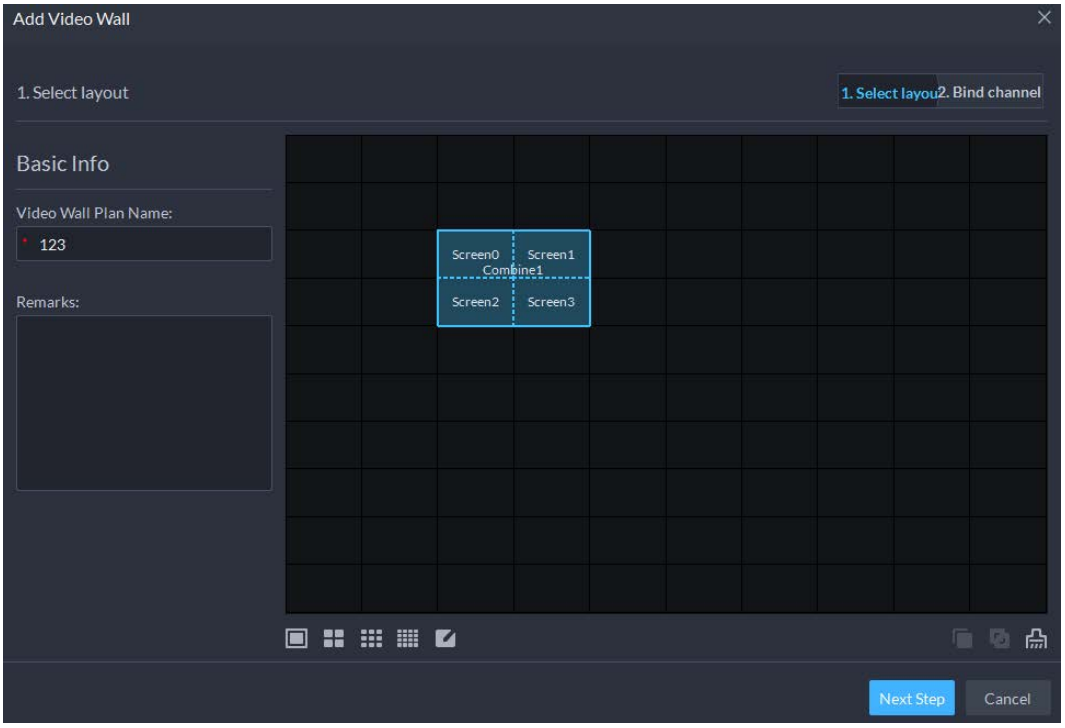
Step 1 Log in to the DSS Client, and on the **Home** page, select **Monitoring Center** > .

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

Figure 5-46 Add a video wall



Step 4 Click **Next Step**.

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

- You can set whether to show ID in the screen, Show Screen ID means that the screen ID is disabled; click the icon and it becomes Show Screen ID, which means that screen ID is enabled.
- Each screen in a combined screen must be bound with a decoding channel.

Step 6 Click **Finish**.

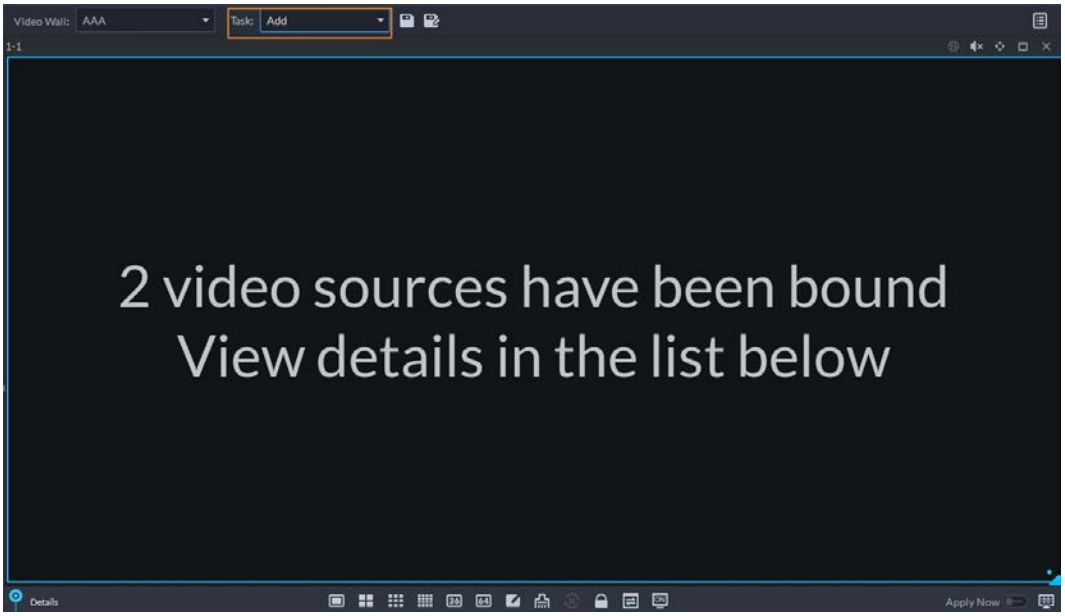
5.1.5.1.4 Configuring Video Wall Display Tasks

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** > .

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

Figure 5-47 Add a video wall task



Step 3 From the device tree, select a camera, and then drag it to a screen, or select a window, drag the camera to the **Detail** section.

If you do not close video wall display in advance, this action will delete the bound camera and play the selected camera on the wall.

Step 4 Click .

If you have selected an existing task in the **Task** drop-down list, after dragging the video channel to the window, click to save it as a new task, which will be played on the wall immediately.

Step 5 Name the task, and then click **OK**.

- During video wall display of a task, if you have rebound the video channel, click to start video wall display manual.
- During video wall display, click or to stop or start tour display.

Step 6 Click to start video wall display.

5.1.5.1.5 Configuring Video Wall Plans

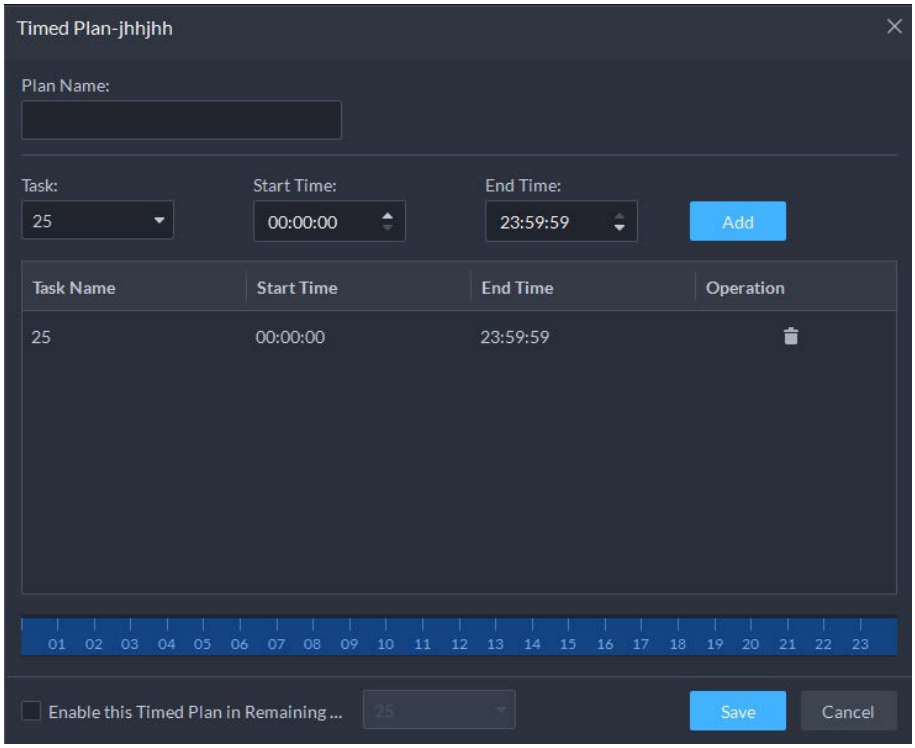
Configuring Timed Plans

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 5-48 Set timed plan



Step 4 Enter the plan name.

Step 5 Select a video task, set start time and end time, and then click **Add**.

Repeat this step to add more tasks. The start time and the end time of tasks cannot be repeated.

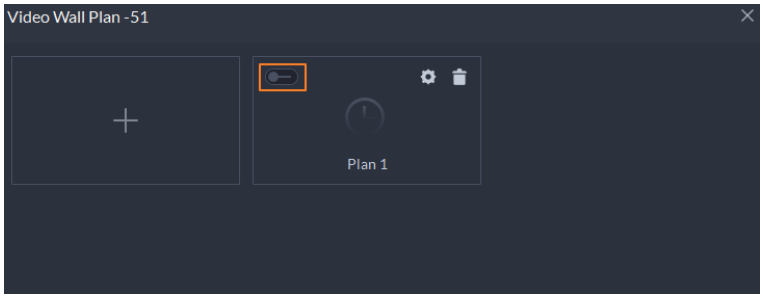
Select the **Enable This Timed Plan in Remaining Time** check box, and then set the task. The video wall displays the selected task during the remaining period.

Step 6 Click **Save**.

Step 7 Click  to start the plan.

You cannot display multiple plans on the wall at the same time. When a plan is enabled, the previous plan on the wall is automatically terminated.

Figure 5-49 Enable timed plan



- Modify plan:  .
- Delete plan:  .

Configuring Tour Plans

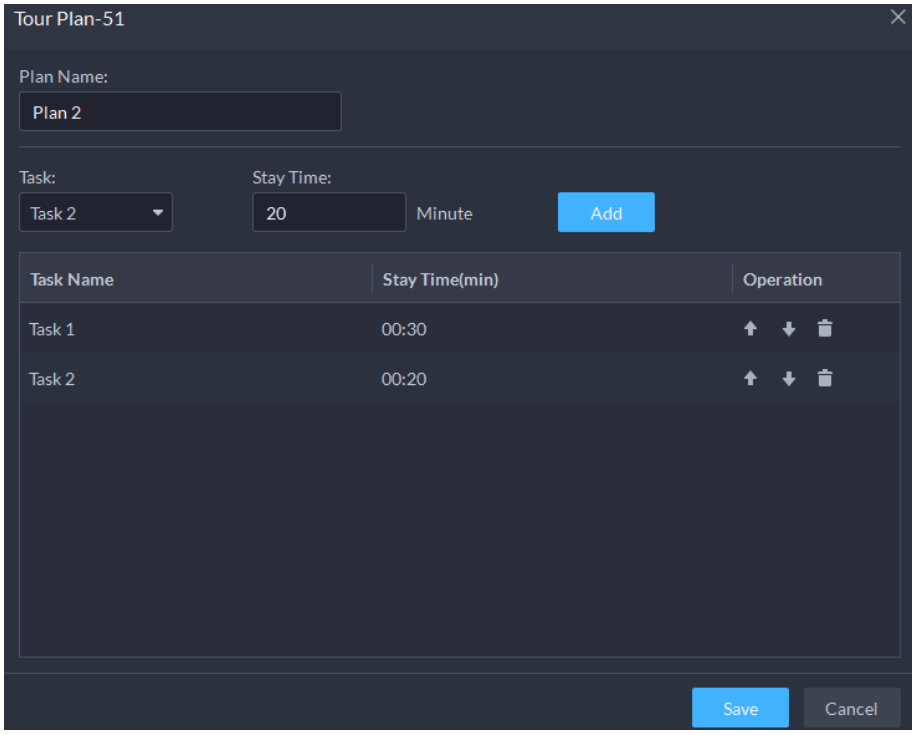
After setting video wall tasks, you can configure the sequence and interval of tasks so that they can automatically play in turn on the wall.

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 5-50 Tour plan

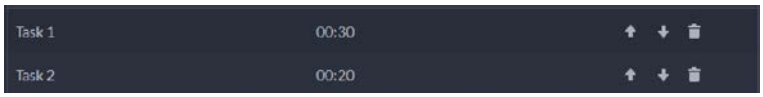


Step 4 Enter task name, select a video task and then set stay time. Click **Add**.

Repeat this step to add more tasks.

Click to adjust task sequence; click to delete a task.

Figure 5-51 Tour information

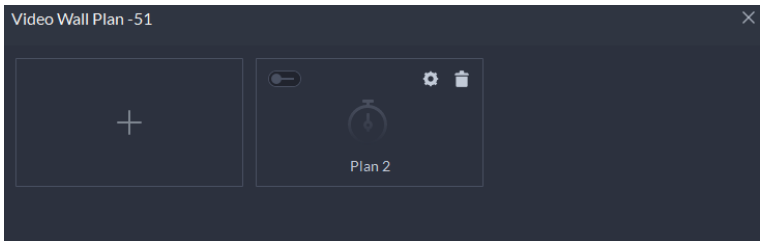


Step 5 Click **Save**.

Step 6 Click to start the tour plan.

You cannot display multiple plans on the wall at the same time. When a plan is enabled, the previous plan on the wall is automatically terminated.

Figure 5-52 Enable tour plan



- Modify plan: Click .
- Delete plan: Click .

5.1.5.2 Video Wall Applications

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

5.1.5.2.1 Instant Display

Drag a camera to the video wall screen for instant display on the wall.

The video wall display task is configured. For details, see "5.1.5.1.4 Configuring Video Wall Display Tasks".

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

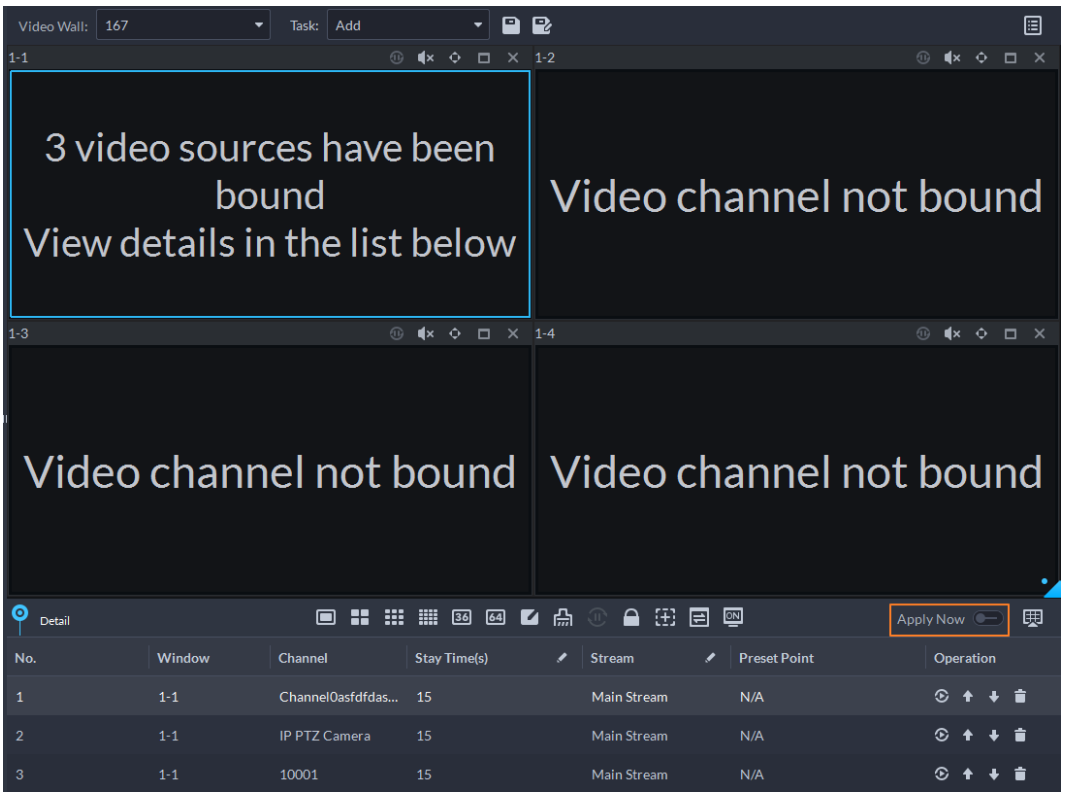
Step 2 In the **Video Wall** drop-down list, select a video wall.

Step 3 Click Apply Now to start video wall display.

Step 4 Drag a camera from the device tree to a screen, or select a window and drag the camera to the **Detail** section.

- A window can be bound to multiple video channels.
- The binding mode, which includes **Tour**, **Tile**, and **Inquiry**, can be set in **Local Settings** > **Video Wall**. For details, see "8.3.3 Configuring Video Wall Settings".
- For a fisheye camera, right-click it to select the installation mode for fisheye dewarping.

Figure 5-53 Bind video channel



Step 5 Select a screen, and then click **Detail** to view detailed information about the screen and channel, including stream type, preset and display sequence.

- Click to view live video of the current channel on the lower left.
- Click to adjust sequence.
- Click to delete the video channel on the current window.

5.1.5.2.2 Video Wall Task Display

Display a pre-defined task on video wall.

Step 1 Log in to the DSS Client, and on the **Home** 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 at the lower-right corner before you can see the effect on video wall.
- Click / to pause or stop.
- Select a screen, and then click **Detail** to view detailed information about the screen and channel, including stream type, preset and display sequence.

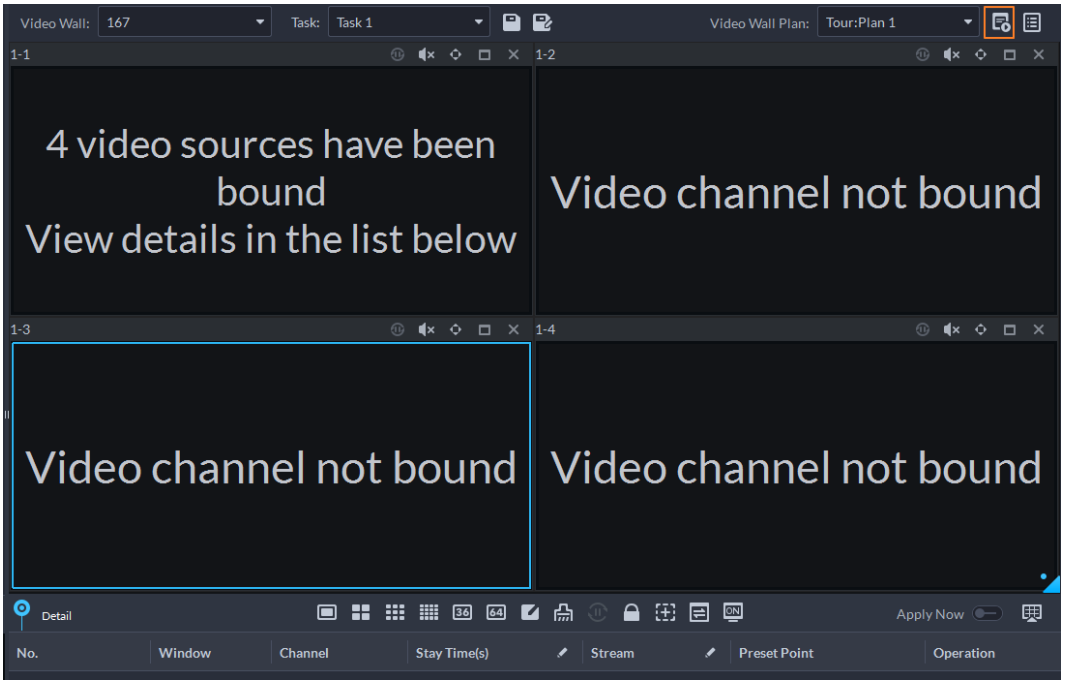
5.1.5.2.3 Video Wall Plan Display

Display a pre-defined plan on video wall.

Make sure that there are pre-defined plans. For details, see "5.1.5.1.5 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 5-54 Display video wall plan



5.2 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. Based on all the alarms that were triggered, the platform will generate statistics ready for your review. This can be helpful for how you can optimize your security measures.

Make sure you have configured and enabled alarm events. To configure, see "4.1 Configuring Events".

5.2.1 Real-time Alarms

View and process real-time alarms.

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

Step 2 Click .

The alarm list is refreshed in real time. To stop refreshing, click **Pause Refresh**. To continue receive alarms, click **Start Refresh**.

Figure 5-55 Real-time alarms

Step 3 Click to claim an alarm.

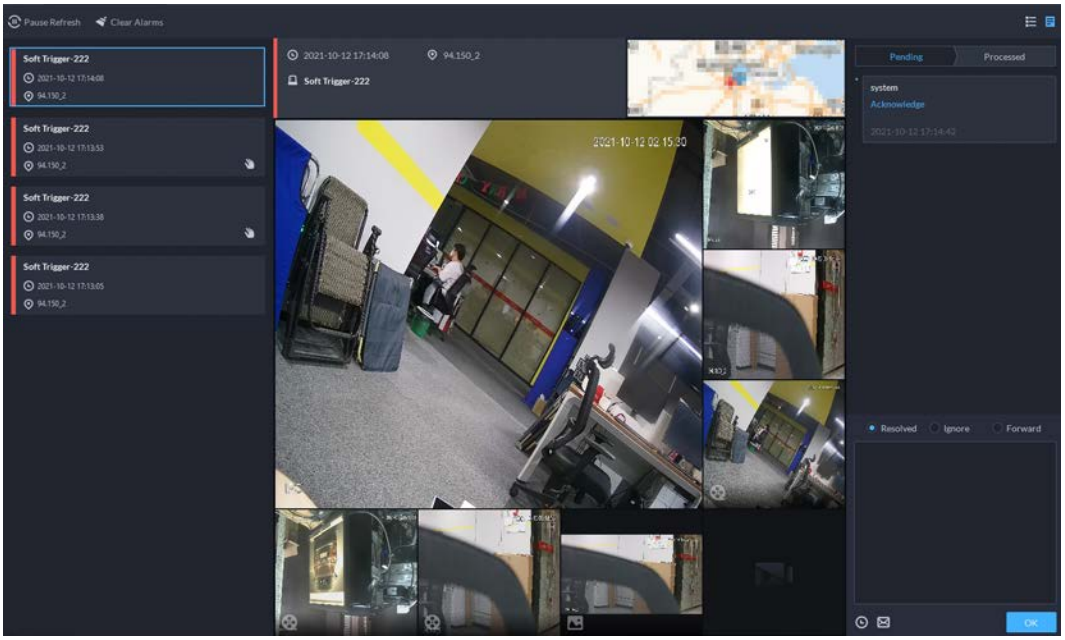
After an alarm has been claimed, the username of your account will be displayed under the **Processed by** column.

Step 4 Process alarms.

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

1. Click or double-click the alarm.

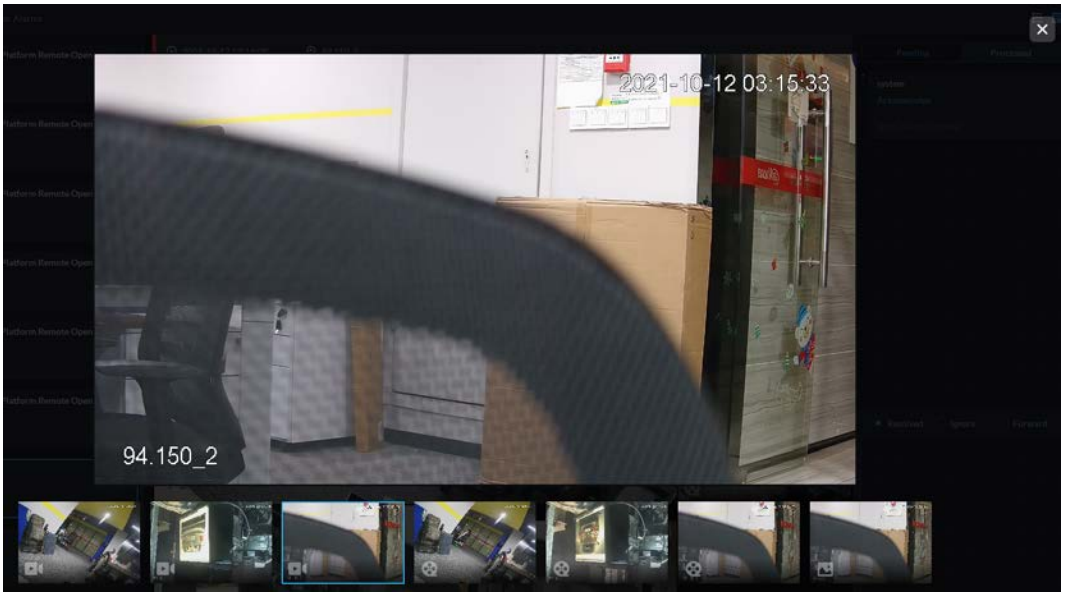
Figure 5-56 Alarm details



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

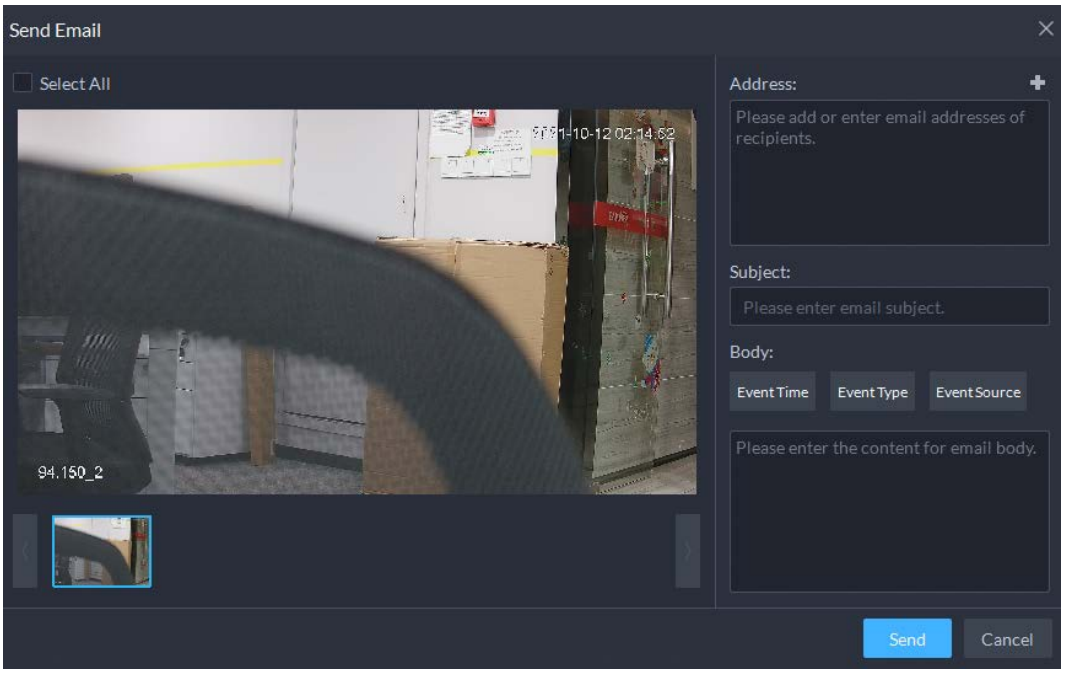
   Double-click a window to view them in larger size. Click to go back.

Figure 5-57 Alarm linkage media



3. On the right side, select how to process the alarm from **Resolved**, **Ignore**, or **Forward**. Enter comments, and then click **OK**.
   Forward allows you to forward the alarm to another user who will process it.
4. (Optional) Click to disarm the alarm. This alarm will not be triggered within the defined period.
5. (Optional) Click to send the alarm information to other users as a prompt or an email.

Figure 5-58 Send email



5.2.2 History Alarms

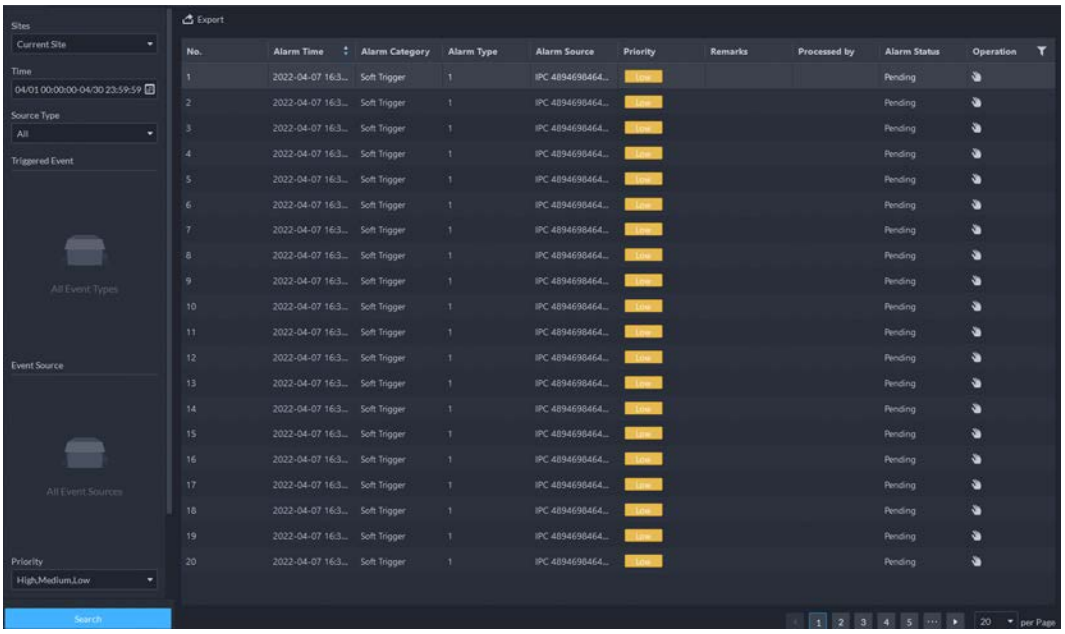
Search for and process history alarms.

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

Step 2 Click .

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

Figure 5-59 history alarms



Step 4 Claim and process alarms, see "5.2.1 Real-time Alarms".

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

5.2.3 Event Overview

With alarms being triggered and processed, statistics are generated to give you a clear picture of what is happening in your area, such as the number of alarms that were processed, and the type of alarms that are triggered most frequently.

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

- To view event overview, click .

Figure 5-60 Alarm overview

Table 5-10 Alarm overview description

No.	Parameter	Description
1	Search conditions	• To view real-time alarm overview, click **Real Time**, select a site (if any), an organization, and refresh frequency. • To view daily alarm overview, click **Daily**, configure the time, select a site, an organization, and then click **Search**. • To view weekly alarm overview, click **Weekly**, configure the time, select a site, an organization, and then click **Search**. • To view monthly alarm overview, click **Monthly**, configure the time, select a site, an organization, and then click **Search**. If the time zone of the server is not the same as the DSS client, statistics will be generated based on the time zone of the server. For example, daily statistics will be generated from 00:00 to 24:00 based on the time zone of the server.
2	Alarm Overview	Statistics is generated based on the alarms that the current user has access to. The number and proportion of alarm events that are pending, processed, or not processed are displayed. The data will only refresh in real-time when you are viewing daily statistics.

No.	Parameter	Description
3	Alarm Priority	Statistics is generated based on the events that the current user has access to. The number of alarms of all priorities are displayed. The data will only refresh in real-time when you are viewing daily statistics. You can click high, medium, or low to not include the number of certain alarms. For example, if you click **High**, the number of the alarms in this priority will not be counted.
4	Top 10 Alarm Sources	Top 10 alarm sources that the current user has access to are sorted by the number of alarms. The data will only refresh in real-time when you are viewing daily statistics. You can click high, medium, or low to not include the number of certain alarms. For example, if you click **High**, the number of the alarms in this priority will not be counted.
5	Top 10 Alarm Types	Top 10 alarm types that the current user has access to are sorted by the number of alarms. The data will only refresh in real-time when you are viewing daily statistics.
6	Alarm Trend	Displays trend of alarms of all priorities.

- To view and process alarms, click .
- To view and process alarms, click .

5.2.4 Alarm Controller

You can monitor and manage alarms controllers.

Prerequisites

Alarm controllers are added to the platform. See "3.2.2 Managing Device".

Procedure

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

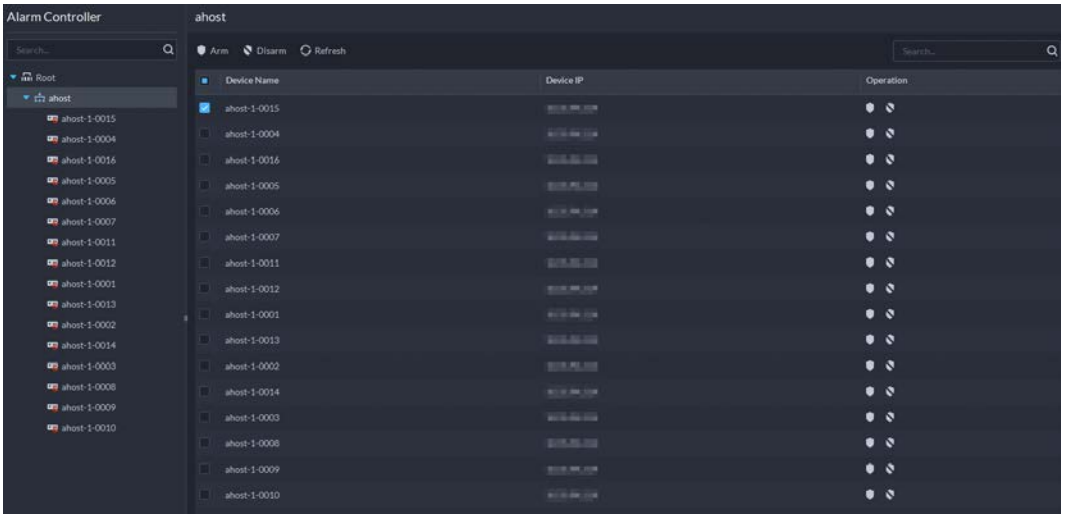
Step 2 Click .

Step 3 In the device tree, click an organization.

All alarm controllers under this organization will be displayed on the right. You can select one or more alarm controllers, and then click **Arm** or **Disarm** to arm or disarm the alarm controllers you selected.

If arming failed, you can click **Force Arm** on the prompt window to arm again.

Figure 5-61 Alarm controller organization

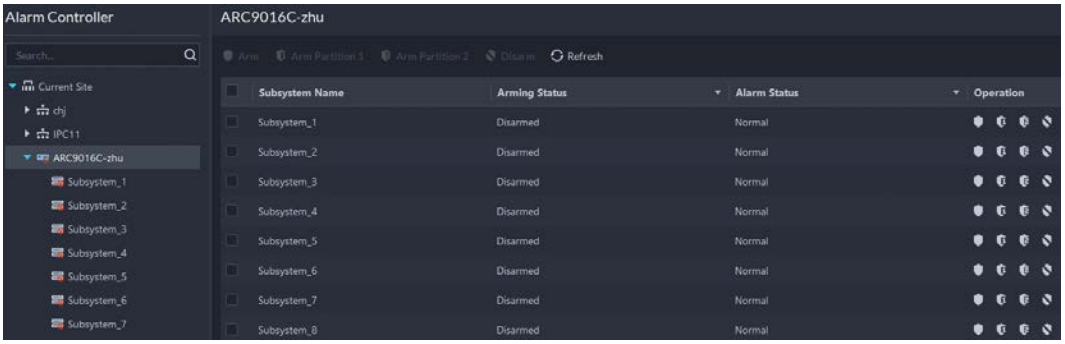


Step 4 In the device tree, click an alarm controller.

All subsystems under this alarm controller will be displayed on the right.

You can right-click an alarm controller, and then click **Update Alarm Controller** to update its information.

Figure 5-62 Subsystems



Step 5 Arm or disarm subsystems.

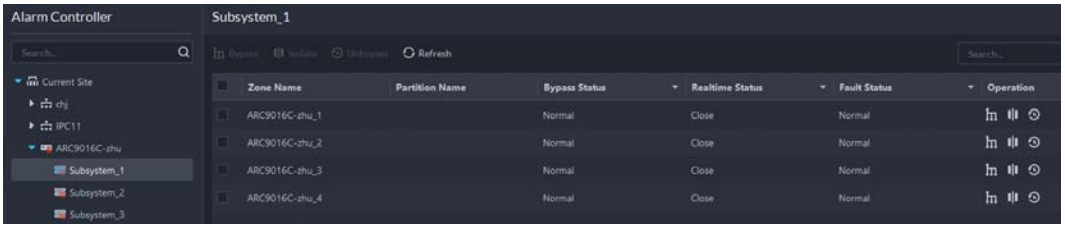
- Arm Arm Partition 1 Arm Partition 2 Disarm: Operate on multiple subsystems.
- : Operate on one systems.

- See the user manual of the alarm controller for detailed description on each function.
- If arming failed, you can click **Force Arm** on the prompt window to arm again.

Step 6 In the device tree, click a subsystem of the alarm controller.

All zones under this subsystem will be displayed on the right.

Figure 5-63 Zone



Step 7 Bypass, isolate, or unbypass zones.

- Bypass Isolate Unbypass: Operate on multiple zones.
- : Operate on one zone.

- See the user manual of the alarm controller for detailed description on each function.
- If arming failed, you can click **Force Arm** on the prompt window to arm again.

5.3 DeepXplore

You can set multiple search conditions to view records of people, vehicle snapshots, access, POS, and MPT.

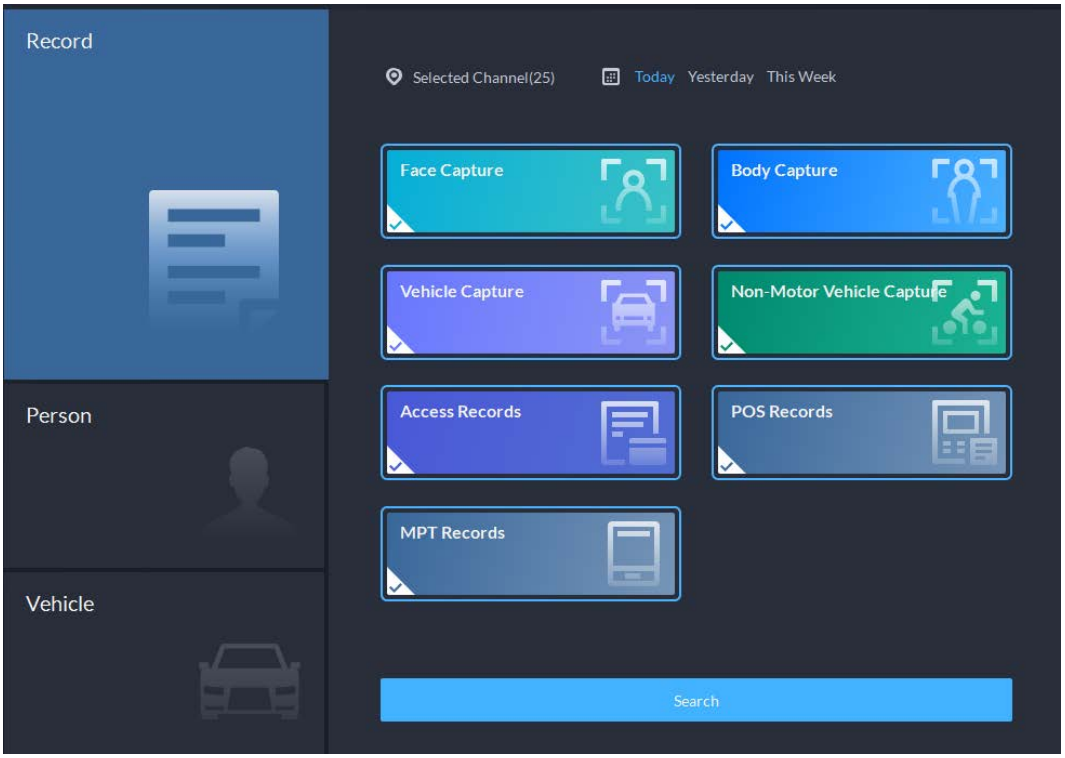
5.3.1 Searching for Records

In this section, you can view integrated records of people, vehicle, access, POS, and MPT.

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

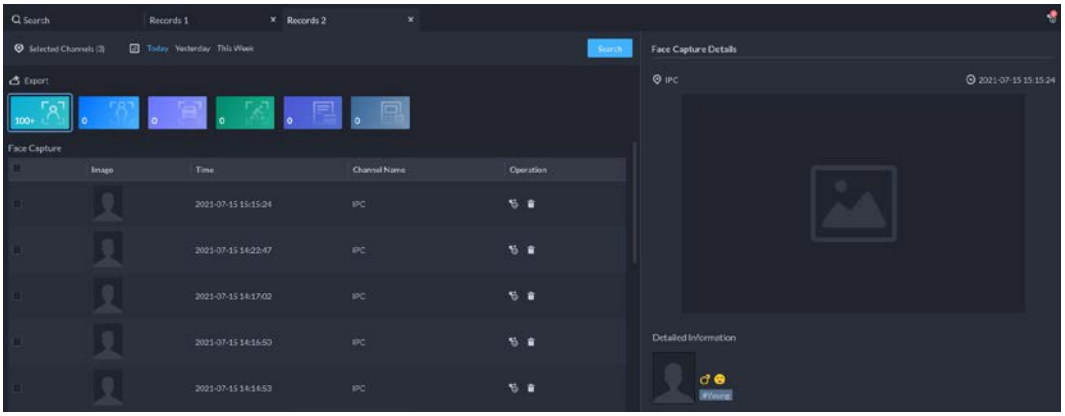
Step 2 click , and then select **Record**.

Figure 5-64 Record search



Step 3 Set the search object, channel and time, and then click **Search**.

Figure 5-65 Search result



For the search result, you can perform following operations.

- Click next to the record to add it to temporary records.
- For face capture records, you can hover the mouse over the small image on the right, and then click to search for images similar to this one. For details, see "5.3.2 Searching for People".
- Click next to the record to delete it one by one.

  Access records and POS 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.

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.

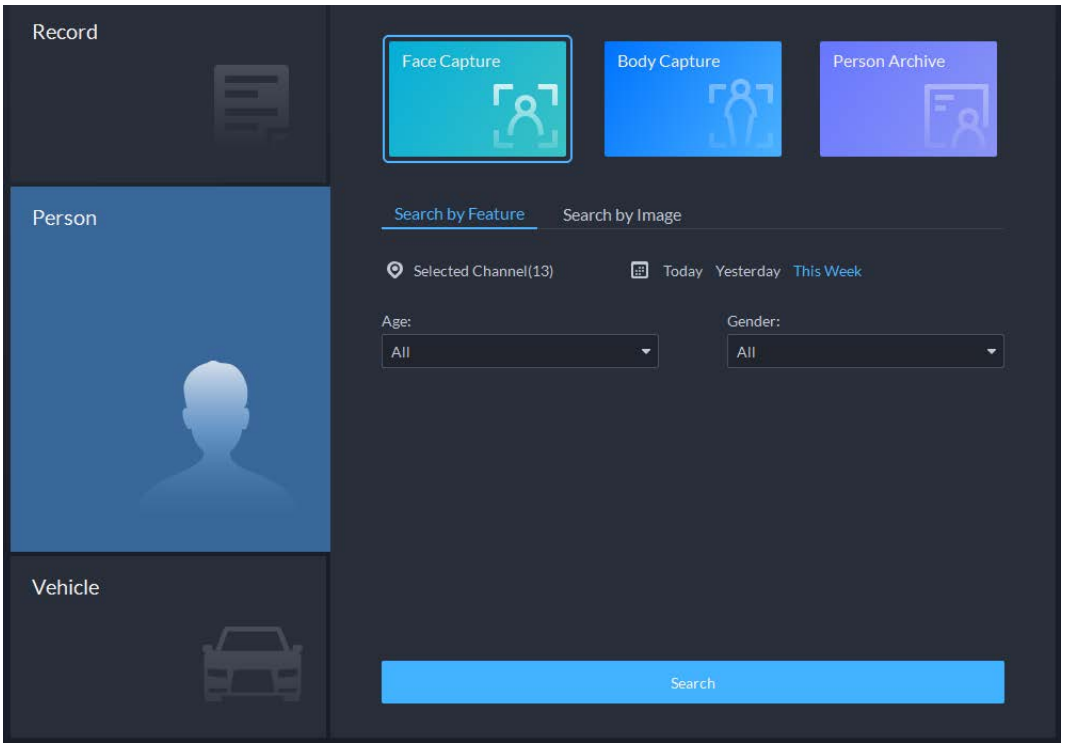
5.3.2 Searching for People

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 5-66 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.

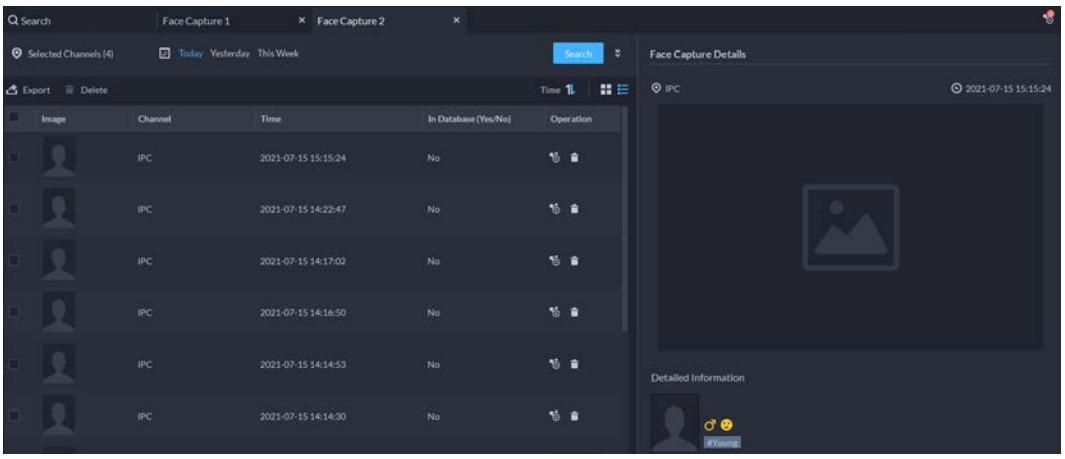
    Only new versions of IVSS devices support displaying similarity.
  - Search channel: Select device channels of the records by clicking **Selected Channel**.
  - Search time: Select time period of the records from **Today**, **Yesterday** and **This Week**.

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 5-67 Search result



For the search result, you can perform following operations.

- Click next to **Search** to change search conditions.
- Click Time to change records arrangement.
- Click next to the record to add it to temporary records.
- Click next to the record to delete it one by one, or you can select records, and then click **Delete** to delete them in batches.
- Click **Export** to export records to the local storage.

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

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

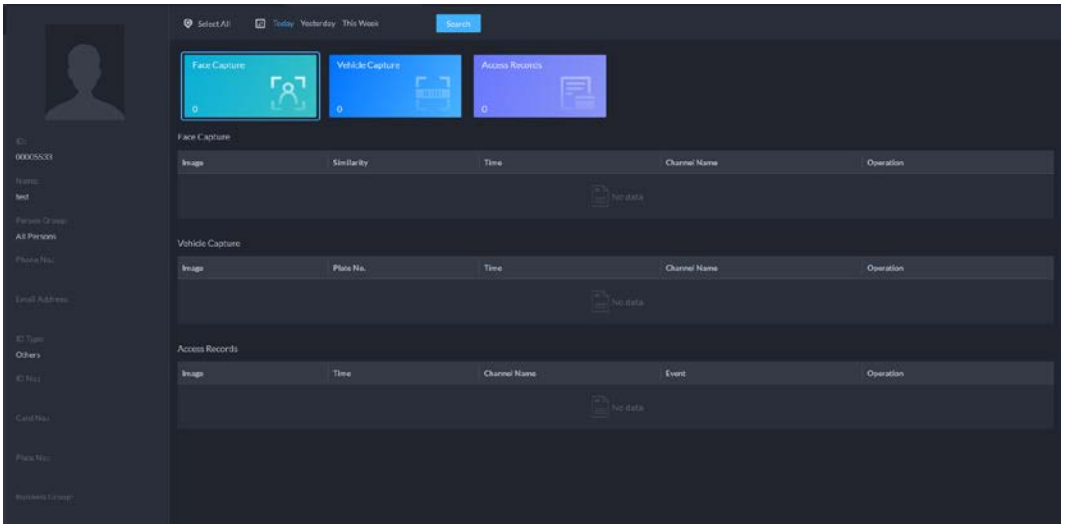
Step 5 Go back to Step2, and then click **Person Archive**.

Step 6 Enter the ID, name or card number of the person you want to search for.

Step 7 Double-click the record.

You can see the face capture, vehicle capture, access records and other information of the corresponding person.

Figure 5-68 Person information

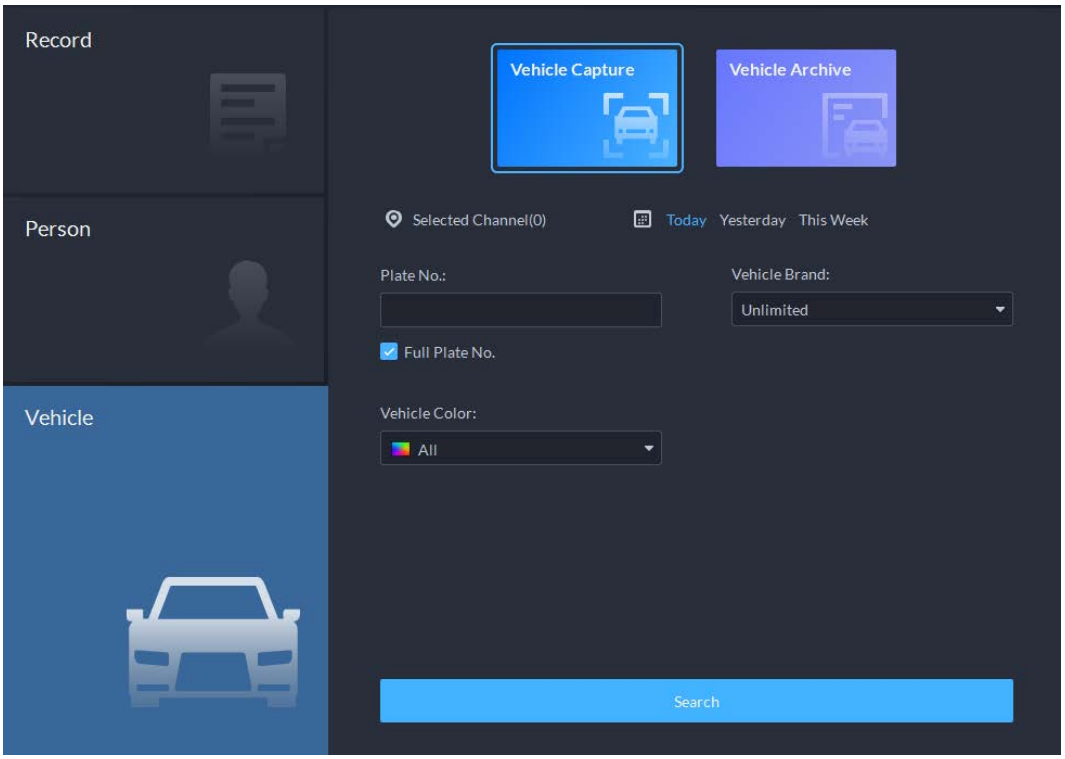


5.3.3 Searching for Vehicles

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 5-69 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 add it to temporary records.
- 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.

5.3.4 Searching for POS Transaction

You can search for POS transactions by keywords and POS fields.

Step 1 Log in to the DSS Client. On the **Home** page, select > **DeepXplore** > **DeepXplore** > **POS Transaction**.

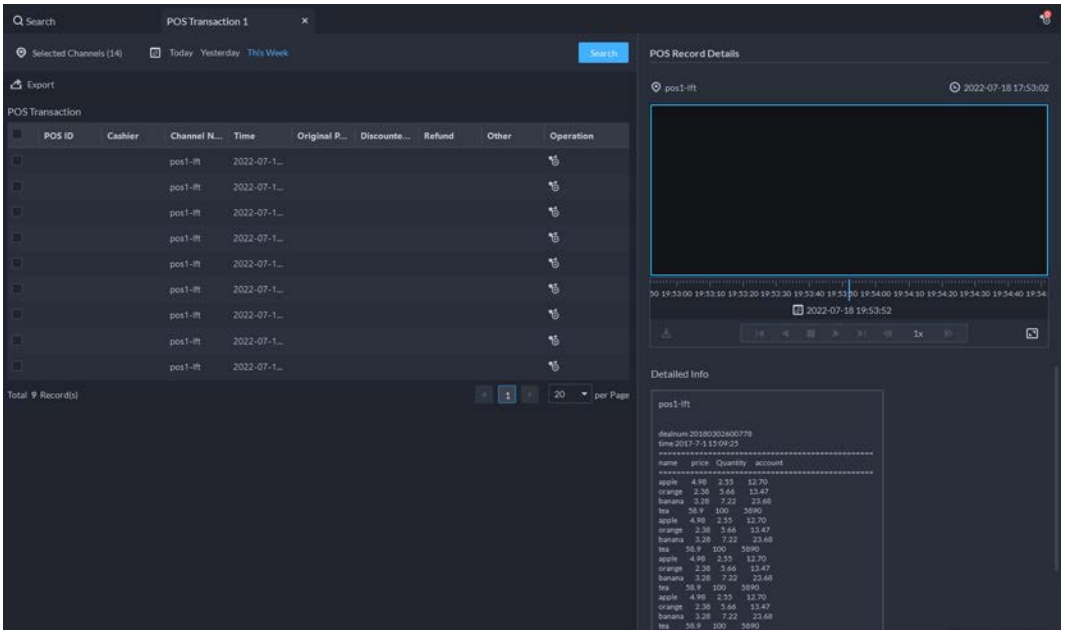
Step 2 Configure POS field.

1) Click **POS Field Config**.
2) Configure a POS field for its receipt field, and then click to enable it.
3) Click **OK**.

Step 3 Configure the search conditions.

1) Configure the information you want to search for.
   - **POS Info**: Keywords in the transaction information. This can be used with one or more POS fields at the same time.
   - POS fields: The POS fields you have configured in step 2 will be used to search for certain information in the transactions. For example, the POS field for total price is TTL, then the platform will obtain the number for TTL and return the results.
2) Select POS channels, configure the period, and then click **Search**.

Figure 5-70 Search results



Step 4 Manage the search results.

- View details.

  Select a transaction, and then you can view the detailed information and video at the time of transaction on the right.

  If you need video at the time of transaction, you must bind POS channels with video channels, and configure recording plans for the video channels. For details, see "3.2.3 Binding Resources" and "3.2.4 Adding Recording Plan".

- Add to a case.

  1. Click of a transaction to add it to the temporary library.
  2. Click on the upper-right corner.
  3. Select one or more transactions, and then click **Add to Case**.
  4. Select a case, and then click **OK**.

  In the temporary library, select one or more transactions, and then click to remove them. This operation will only remove them from the temporary library, but not delete them.

- View track.

  1. Click of a transaction to add it to the temporary library.
  2. Click on the upper-right corner.
  3. Select transactions, and then click . The platform will open a page and display the track based on the transactions you select.

If you need to view tracks, you must mark POS channels on the map first. For details, see "4.2.3 Marking Devices".

5.3.5 Adding Case Bank

Inside the case bank, you can integrate the records of face, plate, access and more into one complete case, and configure details of it for future investigation. The platform supports storing up to 10,000 cases.

Prerequisites

The case files can only be stored in **Incident File** disk. Make sure that you have configured such disk type in advance.

Users with access to **Case Bank**:

- Super administrator: View, edit and delete incident files.
- Administrator:
  - View incident files created by themselves and common users. No access to incident files of other administrators.
  - Edit and delete files opened.
  - Cannot edit or delete files closed.
- Common user:
  - Can only view files created by themselves.
  - Edit and delete files opened.
  - Cannot edit or delete files closed.

Procedure

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

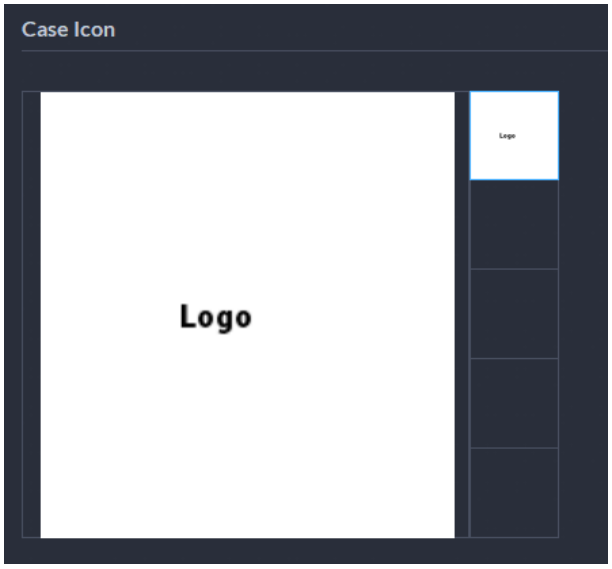
Step 2 click .

Step 3 Click **Add** to add a new case.

Step 4 In the **Case Icon** section, click one of the 5 small squares, drag the image file to the big square on the left, or hover the mouse over the big square, click , and then upload the image file.

The image you select will be displayed on the upper-left corner of the case you export.

Figure 5-71 Select an image for the case



Step 5 Select an image from the right side of the **Case Icon** section, which will be located at the upper-left corner of the case file generated. You can change the icon by dragging the image from the right side to the left side image area.

Only one icon can be added onto the case file.

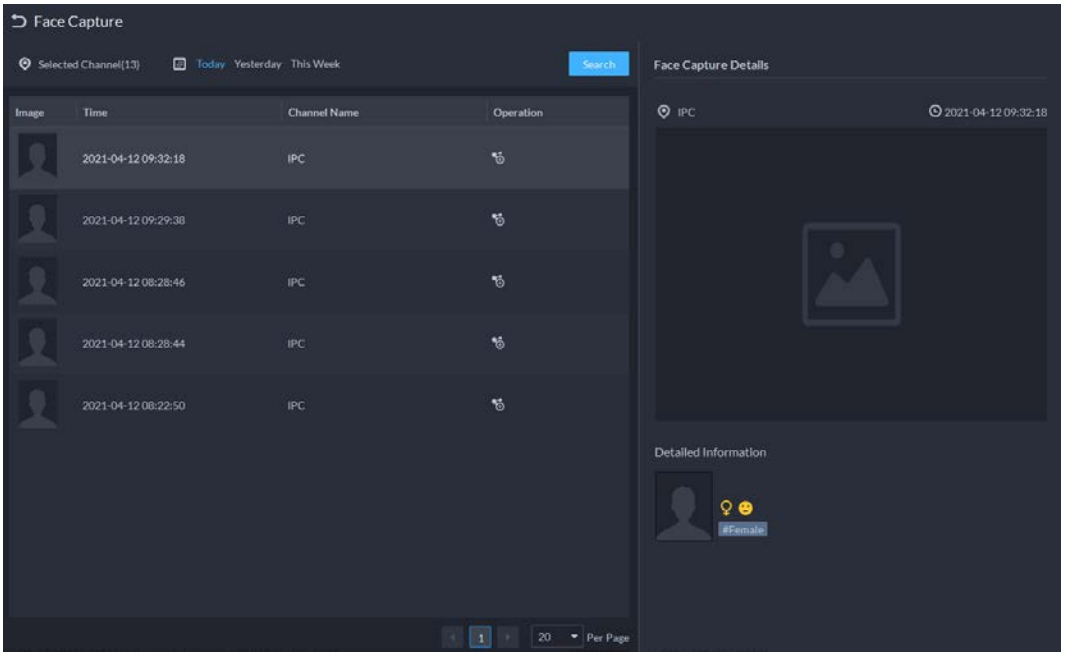
Step 6 Enter the basic information of the case.

- **Case Type**: Used for categorize cases. You can click the drop-down list to select type or create new ones.
- **Status**: Select the case status from **Open** and **Close**. The Platform integrates cases under each status category.

Step 7 Add records, including face capture, body capture, ANPR, access record and more. Records of other categories are added in the same way. In this section, we take **Face Capture** as an example.

1. Click **Add** under **Face Capture**.
2. Select channels and time, and then click **Search**. You can click the record to view its details.

Figure 5-72 Add face capture record



3. Click next to the record to add it to the case.
4. Click to go back to the case adding page, you can add other type of records related to the case.

Step 8 Scroll down and click **Add** under **Attachment** to upload images and videos related to the case.

- The platform supports uploading up to 20 videos, and each video cannot exceed 300 MB. Format includes dav, mp4, avi, flv and asf.
- Up to 20 images can be uploaded. Image format includes png, jpg and jpeg.

The number of all video files and images cannot be more than 20.

Step 9 Click **OK**.

Related Operations

- Delete or replace an icon

  Hover the mouse over a small square, and then click to delete it; click a small square, and then drag an image file to the big square on the left, or hover the mouse over the big square, click , and then upload the image file to replace it.
- Enter case name in the search box at the upper-right corner, and then press Enter or click to search for cases.
- Click under a temporary case to view the case details. If you need to edit the details, click **Edit** and change the information as needed.
- Click under a temporary case to download it, or you can click **Download** in the case details page. Click **Download Progress** at the lower-left corner to check the download progress.
- Click under a case to delete it one by one, or you can select cases, and then click **Delete** to delete them in batches.

5.3.6 Viewing Track of MPT Devices

Search for and view the track of an MPT device on the map within the defined period.

Prerequisites

- Configure the vector map. For details, see "4.2.2.1 Adding Vector Map".
- Add MPT devices to the platform. For details, see "3.2.2.4 Adding Devices".
- MPT devices upload their GPS information to the platform. For details, see their user's manuals.

Procedure

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

Step 2 Select an MPT device, configure the time, and then click **Search**.

The track of the MPT device will be displayed on the map.

You can only search for up to 24 hours of track in the same day. For example, 00:00 to 23:59:59, or 3:00 to 23:59:59.

5.4 Access Management

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

5.4.1 Access Control Application

You can unlock and lock doors, view details of bound videos and event, and the access control logs. Make sure that you have finished the access control configuration before application. For details, see "4.5 Access Control". You can also click Access Control Configur... to go to the access control configuration page.

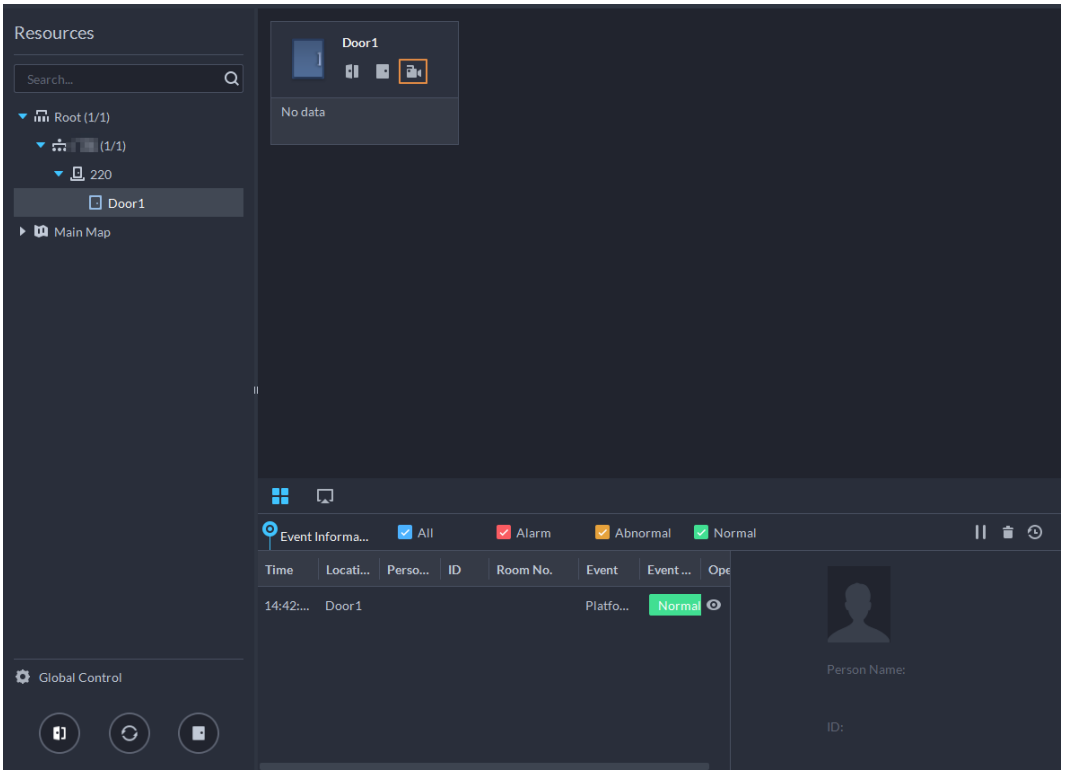
5.4.1.1 Viewing Videos

If you have already bound a video channel to the access control channel, you can view the real-time videos of the channels on the console. To bind video channels, see "3.2.3 Binding Resources".

Log in to the DSS Client. On the **Home** 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.

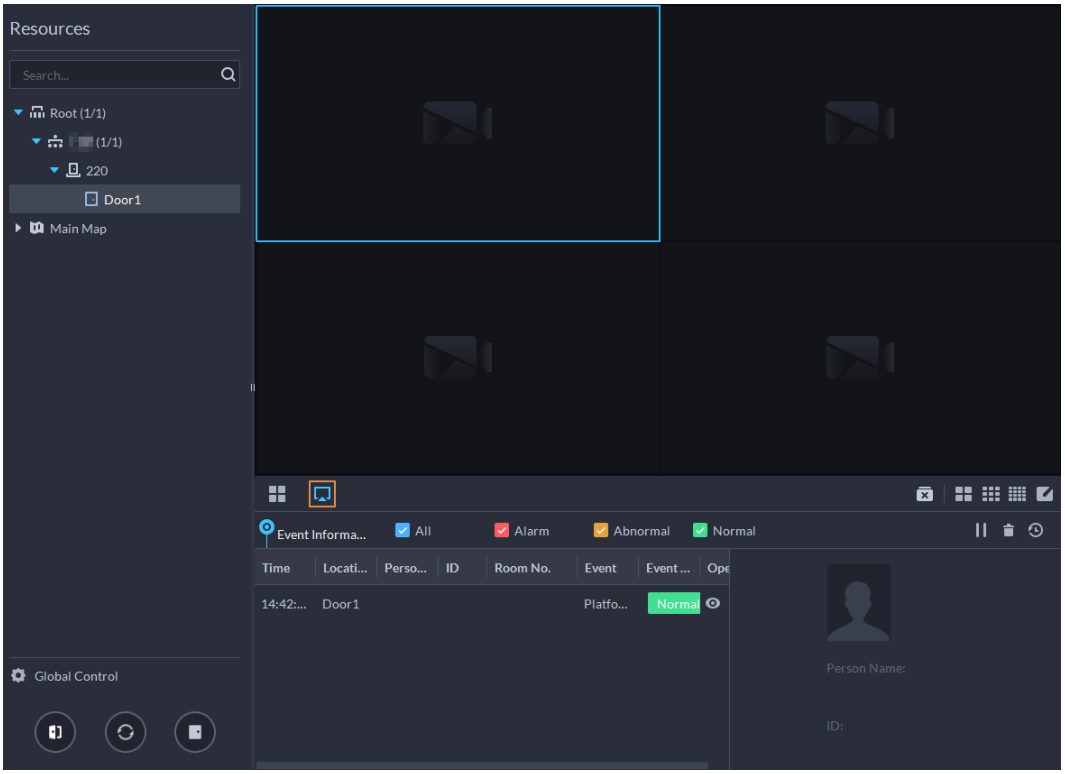
Figure 5-73 Viewing video (1)



- 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 5-74 Viewing video (2)



5.4.1.2 Unlocking Door

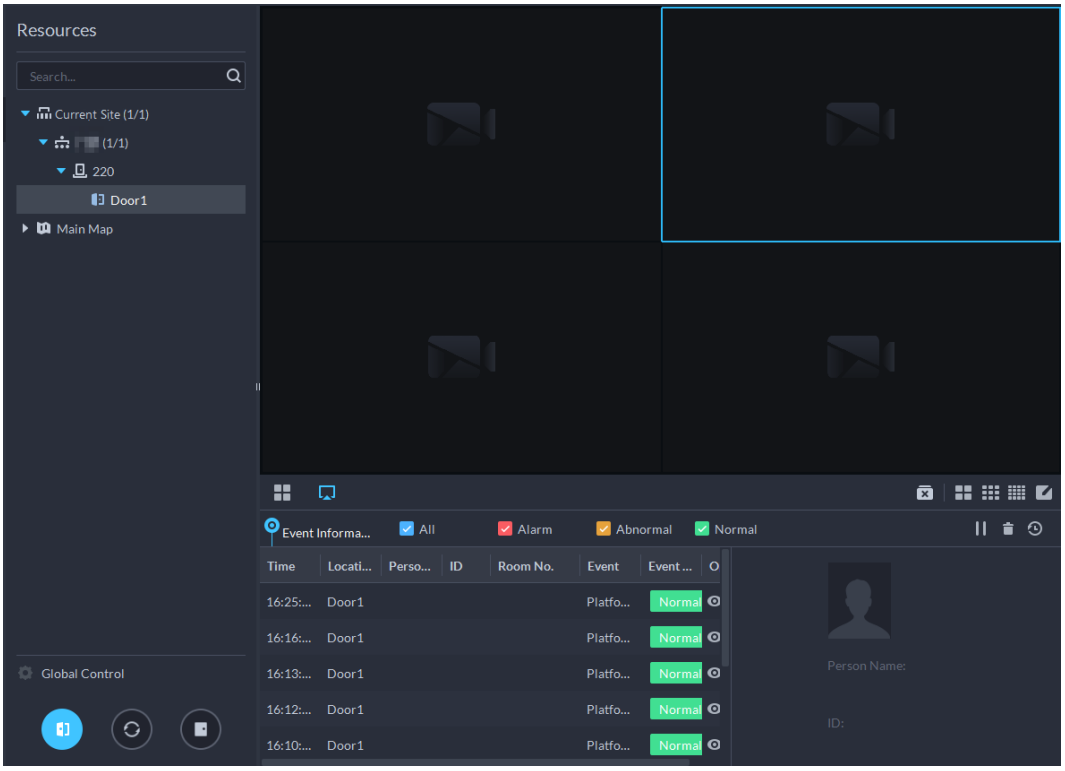
In addition to Always Open or linked unlock in specified periods, the console also supports unlocking by manually controlling the access control channel. After unlock, the door automatically locks up after a specified period (5 s by default, and 10 s in this example) set up in **Door Config**.

This section introduces the unlocking operations on DSS client. For unlocking by fingerprint, card, and face recognition, you can operate on devices. If advance functions are configured, unlock doors according to the requirements of advance functions.

There are the following ways to unlock door:

- On the left side of the 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 5-75 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.

5.4.1.3 Locking Door

In addition to Always Close or linked lock in specified periods, the console also supports locking by manually controlling the access control channel. You can lock the door in the following ways:

- On the left side of the 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.

5.4.1.4 Viewing Event Details

View details of the events reported on door locking and unlocking, including event information, live view, snapshot, and recording.

- Live view is only available when a video channel is bound to the access control channel. To bind video channels, see "3.2.3 Binding Resources".
- To see snapshots and videos of access control, you need to configure video linkage action for the access control channels. For details, see "4.1 Configuring Events".
- Details except locking door are displayed on the console, such as unlocking door, entry with the duress card, and no right.

Step 1 In the event list below the console 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 the captured image and person profile.

Figure 5-76 Event information

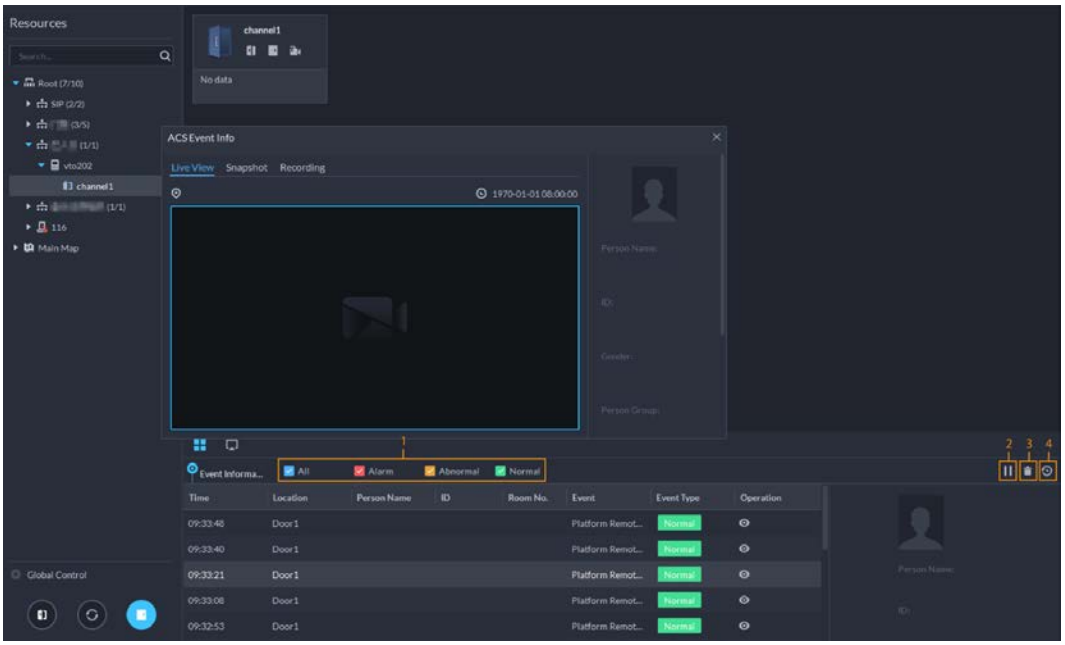


Table 5-11 More operations

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.

5.4.1.5 Viewing Access Control Records

You can view access control records on the platform or directly on a device. For records on a device, see "8.1 Managing Logs".

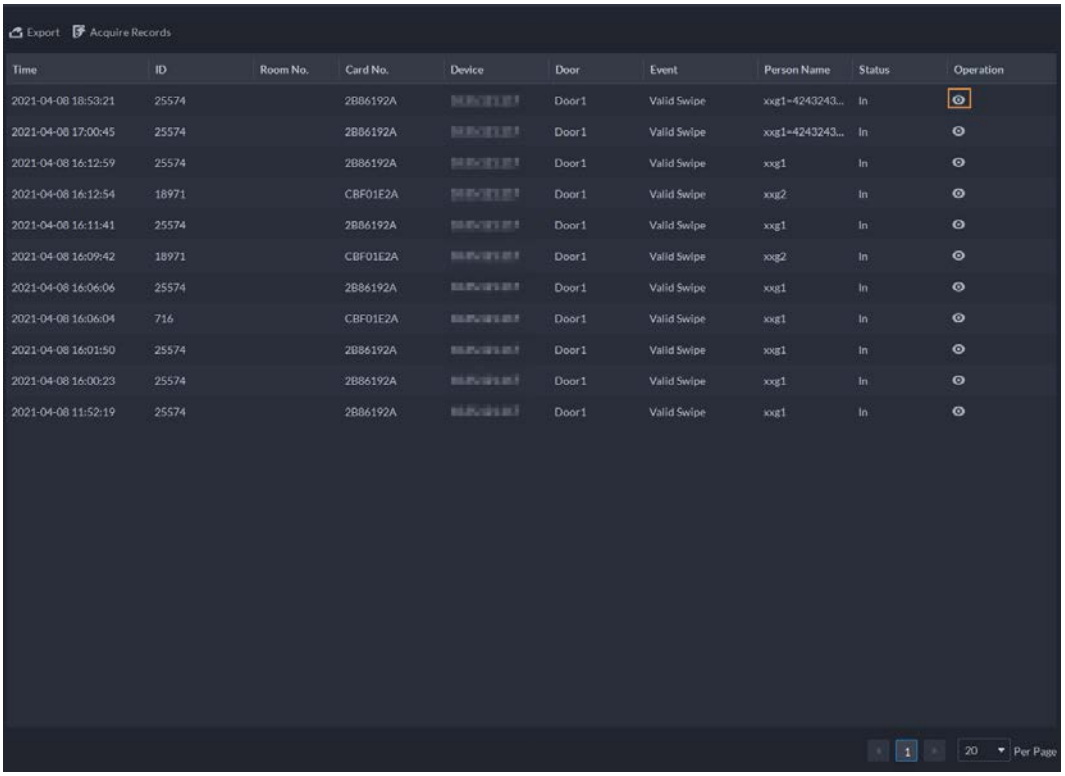
5.4.1.5.1 Online Records

The access control records stored on the platform.

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

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

Figure 5-77 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.

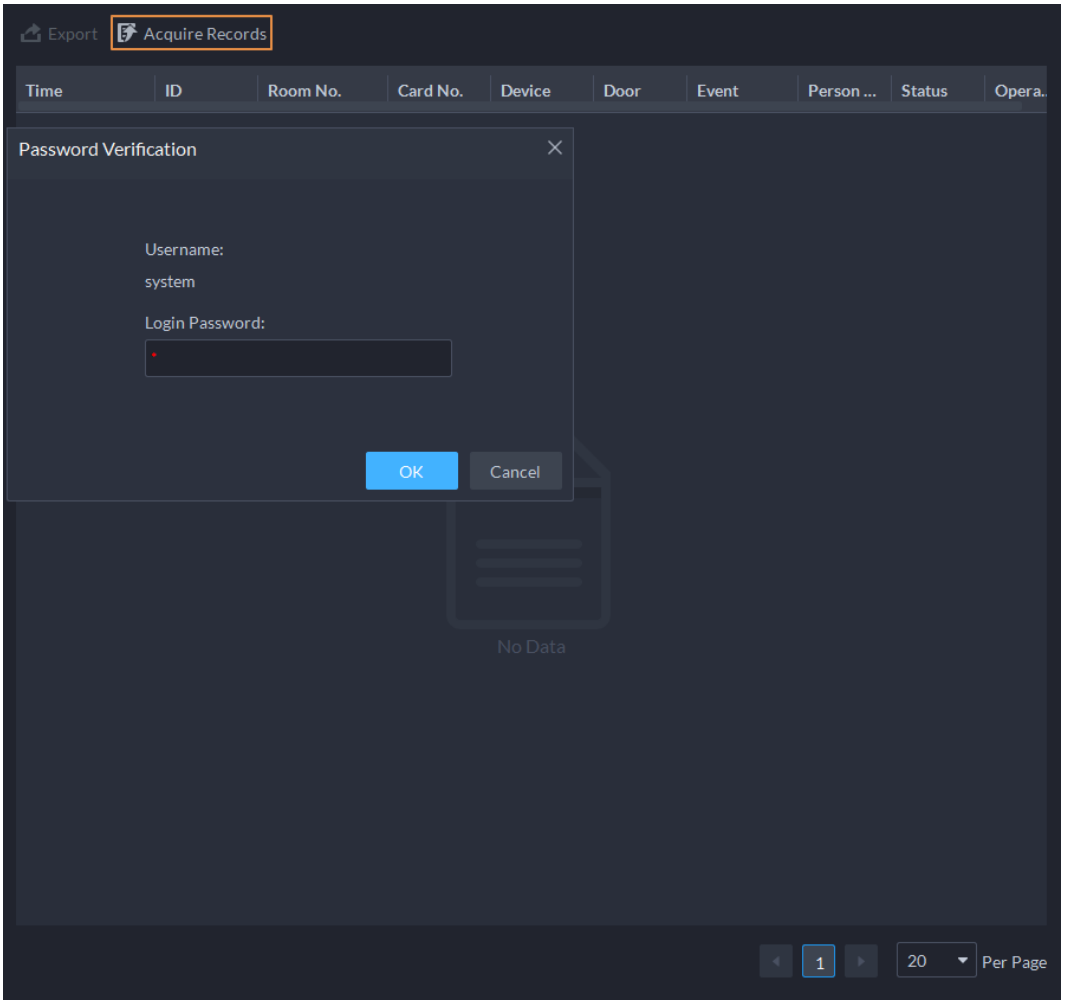
5.4.1.5.2 Offline Records

The access control records stored in the device when it was disconnected from the platform. After the device gets reconnected to the platform, you can retrieve the records generated during the disconnection.

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

Step 2 Click Acquire Records at the upper-left corner.

Figure 5-78 Extract records during disconnection



Step 3 Enter the login password for verification.

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

- You can select up to one week.
- The types of logs supported include door not closed in time alarms, intrusion alarms, anti-passback alarms, duress alarms, device temper alarms, blocklist alarms, too many attempts on invalid passwords and cards alarms.

Step 5 Click **OK**.

5.4.2 Lift Control Application

You can control lifts, view linked real-time videos and event details, and the lift control records. Before using these functions, you must:

- Add lift control devices to the platform. For details, see "3.2.2 Managing Device".
- Assign lift control permissions to people. For details, see "4.3.1.2.1 Adding a Person".

5.4.2.1 Viewing Videos

If a lift control channel has been linked to a video channel, you can view its real-time video in the lift control console so that you can monitor what is happening near the lift. For how to link a lift control channel to a video channel, see "3.2.3 Binding Resources".

Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Lift Control** > **Lift Control Console**, and then view the linked real-time videos in the following two methods.

- Click , and then click of a lift control channel.
- Click , and then drag a lift control channel to a window on the right, or select a window on the right, and then double-click a lift control channel.

5.4.2.2 Global Control

You can select multiple lift control channels, and then set them to the no authentication mode, authentication mode or lock mode.

- No authentication mode: All people will have permissions to use the selected lift control channels.
- Authentication mode: All people will need to verify if they have permissions to use the selected lift control channels.
- Lock mode: No person will have permissions to use the selected lift control channels.

Step 1 Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Lift Control** > **Lift Control Console**.

Step 2 Click next to **Global Control**.

Step 3 Select multiple lift control channels, and then click **OK**.

Step 4 Click , , or to set them to no authentication mode, authentication mode or lock mode.

5.4.2.3 Viewing Event Details

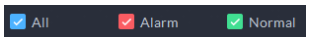
View details of the events reported when someone used a lift, including event information, live video, snapshots, and record videos.

- Live videos are only available when a lift control channel has been linked to a video channel. For details, see "3.2.3 Binding Resources".
- To view snapshots and videos in an event, you need to configure the event for the lift control channels. For details, see "4.1 Configuring Events".

Step 1 Log in to the DSS Client. On the **Home** page, select > **Access Management** > **Lift Control** > **Lift Control Console**.

Step 2 In the event list on the bottom of the page, double-click an event to view its details.

Table 5-12 More operations

Icon	Description
	You can choose to view only certain types of event. For example, if you select **Normal**, the list only displays normal events.
	• 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 it so that new events can be reported again. • Click  to clear all events in the list, but it will not delete them from the lift control records. • Click  to go to the lift control records page.
	Clear the events from the current event list without removing them from the log.
	Click to view access control records.

Step 3 Click the corresponding tab to view the live video, snapshots, and recorded videos.

5.4.2.4 Viewing Lift Control Records

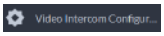
Step 1 Log in to the DSS Client. On the **Home** page, select  > **Access Management** > **Lift Control** > **Lift Control Records**.

Step 2 Configure the search conditions, and then click **Search**.

Step 3 Manage the records.

- Click  to view the information, real-time video, snapshots, and recorded video of an event.
- Click **Export** on the upper-right corner, and then follow the on-screen instructions to export records to your computer.

5.4.3 Video Intercom Application

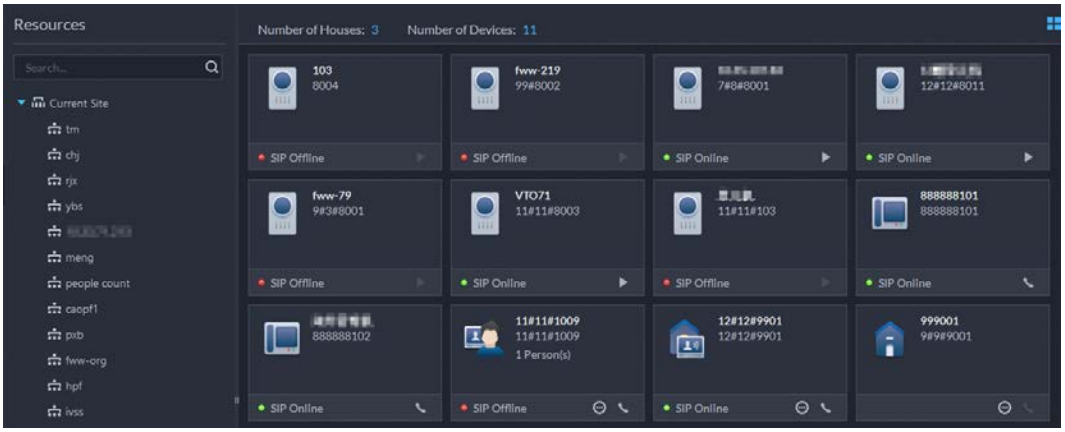
- You can call, answer, release information and view video intercom records.
- Make sure that you have configured the video intercom configuration before application. For details, see "4.6 Video Intercom". You can also click  to go to the video intercom configuration page.

5.4.3.1 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  > **Access Management** >  > **Call Center**.

Figure 5-79 Call center



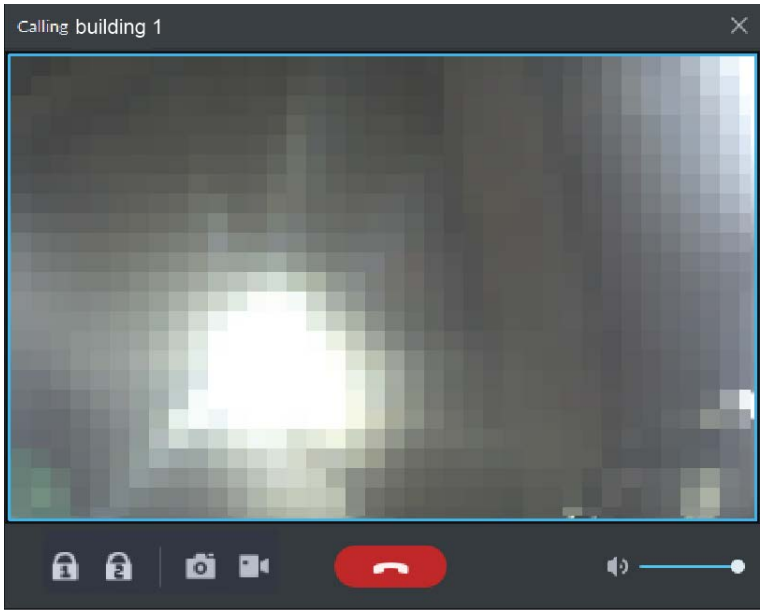
Step 2 You can call different devices.

- Call from the platform to VTO

  Select VTO in the device list; click corresponding of VTO or dial a number on the dial pad to call the 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 "8.3.5 Configure File Storage Settings".
  - : Click this icon to start record, click again to stop record. The video is saved in default path. To change the path, see "8.3.5 Configure File Storage Settings".
  - : Click this icon to hang up.

Figure 5-80 Call



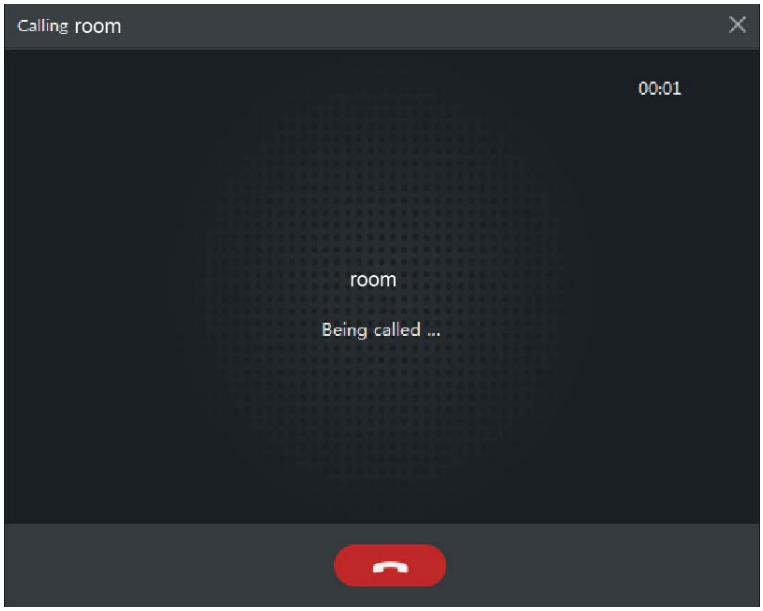
- Call from the platform to VTH

  Select VTH from the device list, click on the VTH or dial corresponding VTH on the right (such as 1#1#101). The system pops up the dialog box of **Calling now, please wait...**. There are two modes for answering the call.

  - Answer by VTH, bidirectional talk between client and VTH. Press to hang up when you answer the call.

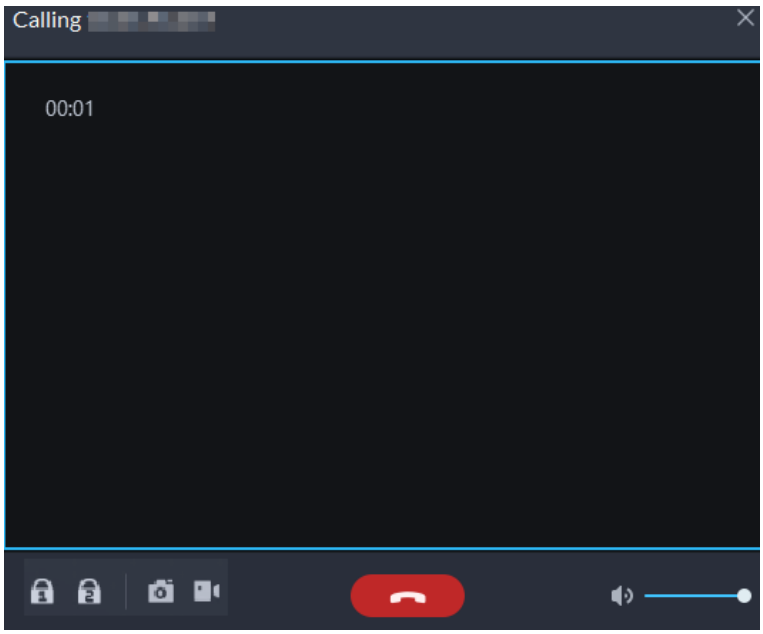
- If VTH fails to answer over 30 s, hangs up directly or is busy, then it means the call is busy.

Figure 5-81 Calling



- Call from the platform to an access control device that supports video intercom
  Select a device from the device list, click 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 to hang up when you answer the call.
  - If the device fails to answer over 30 s, busy or hang up directly, then it means the call is busy.

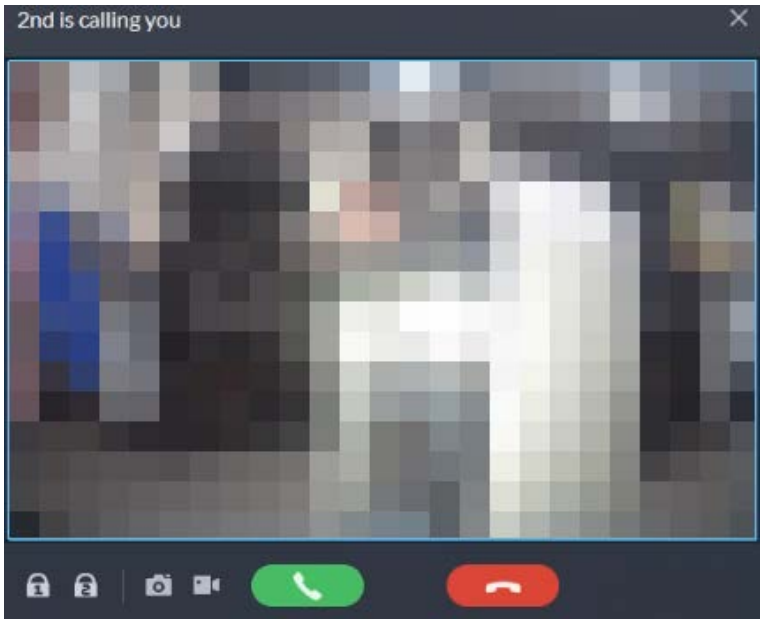
Figure 5-82 Calling



- Call from VTO to the platform
  VTO calls Pro, client pops up the dialog box of VTO calling.

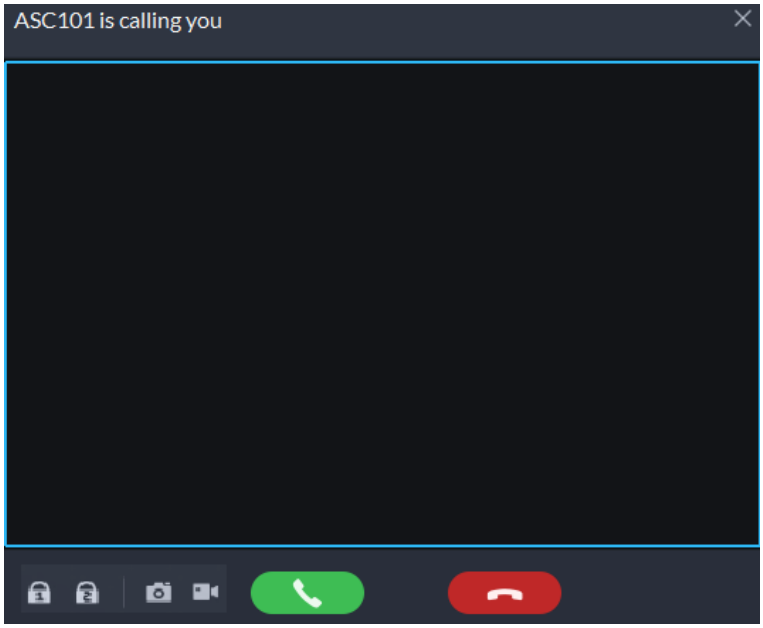
- : If VTO is connected to lock, click this icon to unlock the door.
- : Click this icon to answer VTO, realize mutual call after connected.
- : Click this icon to hang up.

Figure 5-83 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.

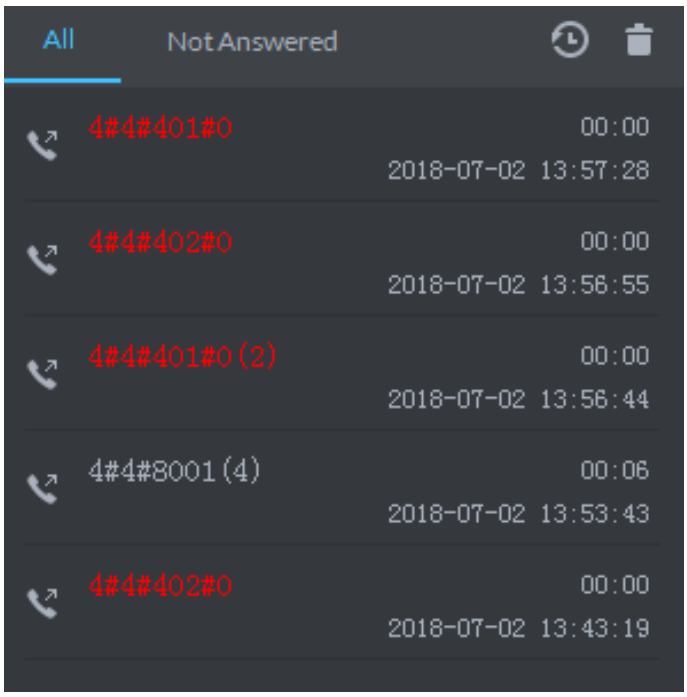
Figure 5-84 Call from an access control device that supports video intercom



- 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 5-85 Call records



5.4.3.2 Releasing Messages

Send message to VTHs.

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

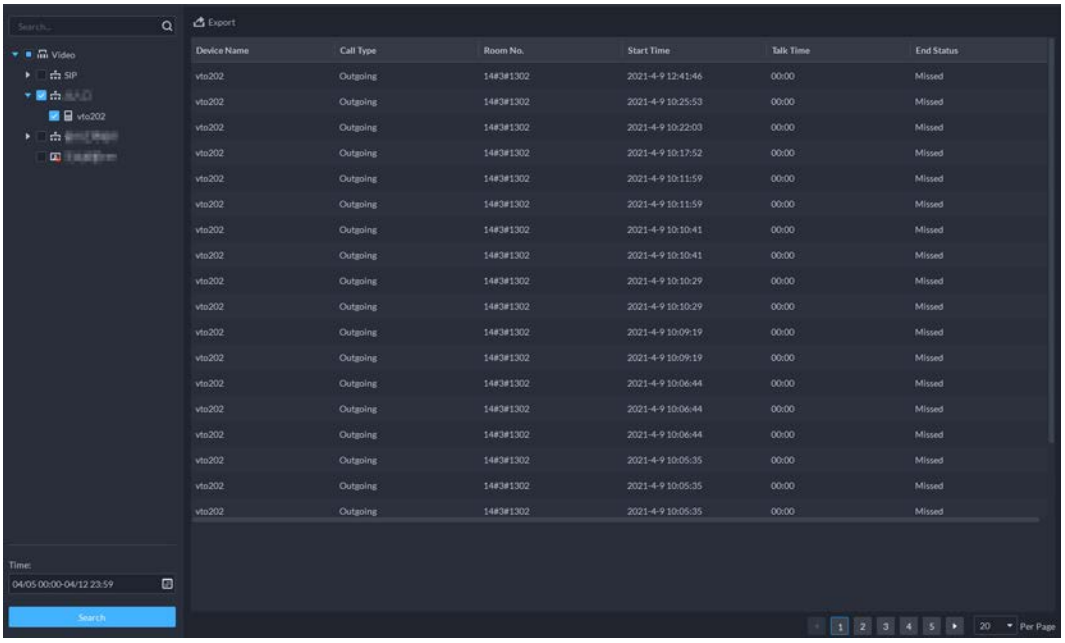
5.4.3.3 Video Intercom Records

View log records and you can trace recorded calls.

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

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

Figure 5-86 Video intercom records



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

5.4.4 Viewing Attendance Data

View attendance data, displayed in the form of report, including card swiping record table, attendance report, abnormality table, overtime table and away table. This section takes **Card-swiping Record** as an example.

Prerequisites

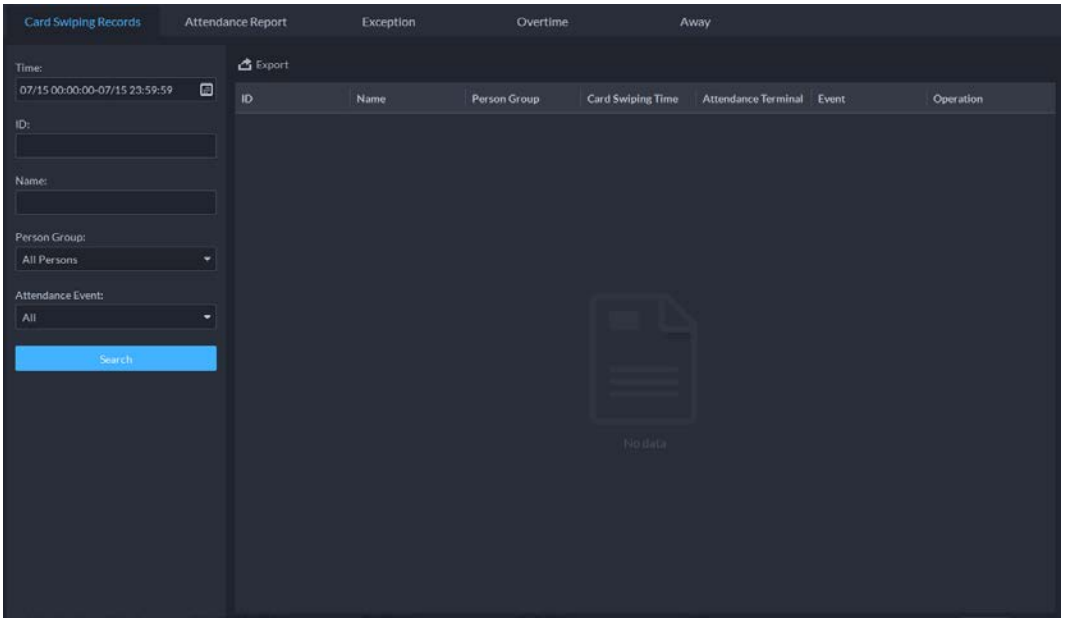
You have configured the attendance configuration before application. For details, see "4.7 Attendance Management". You can also click Attendance Configuration to go to the attendance configuration page.

Procedure

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

Step 2 Click corresponding tab, set search condition, and then click **Search**.

Figure 5-87 Attendance



Step 3 Manage search results.

- Click **Export** at the upper-left corner of the page, and then export records as the screen instructs.
- When card swiping records are displayed in list, click to view the details of the corresponding user.

Related Operations

When viewing attendance report, you can manually synchronize attendance records from devices. Click **Sync Offline Records**, configure the time and channels, and then click **OK** to synchronize the records from the channels you selected to the platform. The attendance report will be updated accordingly. To automatically synchronize attendance records, see "4.7.4 Synchronizing Attendance Records".

5.4.5 Visitor Application

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

5.4.5.1 Preparations

- You have configured the deployment of the video intercom devices, access control devices and entrance and exit device. For details, see the corresponding user's manual.
- You have configured the basic configuration of the platform. For details, see "3 Basic Configurations".
- Make sure that you have configured the visitor configuration before application. For details, see "4.8 Visitor Management". You can also click Visitor Configuration to go to the video intercom

configuration page.

5.4.5.2 Visitor Appointment

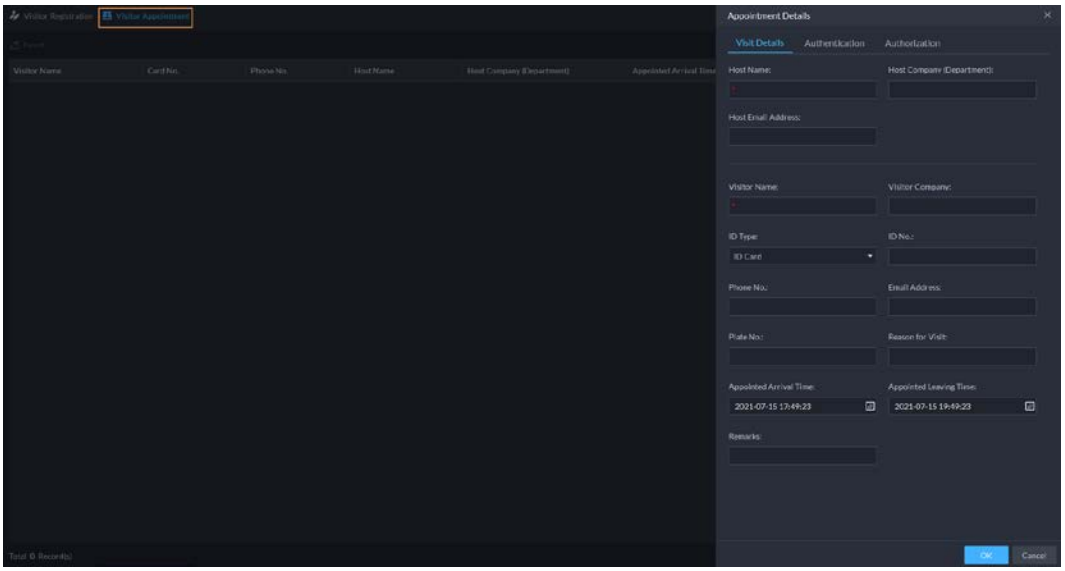
Register visitor information on the platform.

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

Step 2 Click **Visitor Registration**.

Step 3 Click the **Visitor Details** tab, enter the information of the visitor and the one to be visited.

Figure 5-88 Visitor details

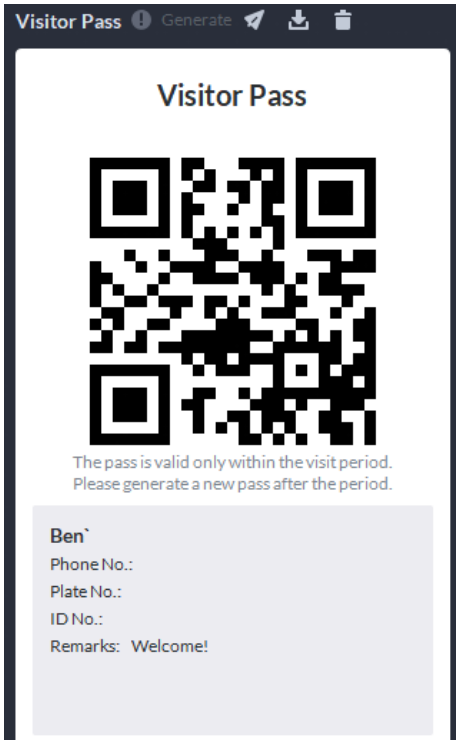


Click in the appointment list to enter the **Visitor Details** tab.

Step 4 (Optional) Click the **Authentication** tab, select the room number to be visited, and then click **Generate** to generate the QR code of the pass.

You can click to download the QR code, and click to send it to the visitor by email.

Figure 5-89 Authentication



Step 5 Click **OK**.

5.4.5.3 Checking In

When a visitor with an appointment arrives, you need to confirm their information and give them access permission. On-site registration is supported when there is a walk-in visitor. Visitors can get access by card swipe or face recognition.

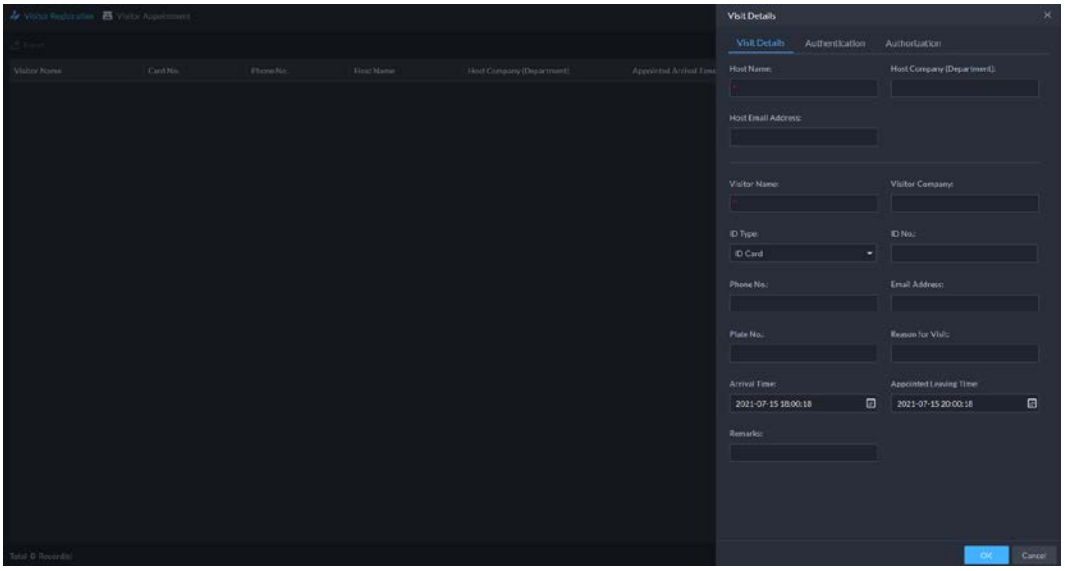
Procedure

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

Step 2 Enter the information of the visitor.

1) Go to the visit registration information page.
   - If a visitor has an appointment, find their visitor information, and then click .
   - If a visitor does not have an appointment, click **Visit Registration**.
2) Confirm or enter visitor information.

Figure 5-90 Visitor information



Step 3 (Optional) Click the **Authentication** tab, and then set authorization information.

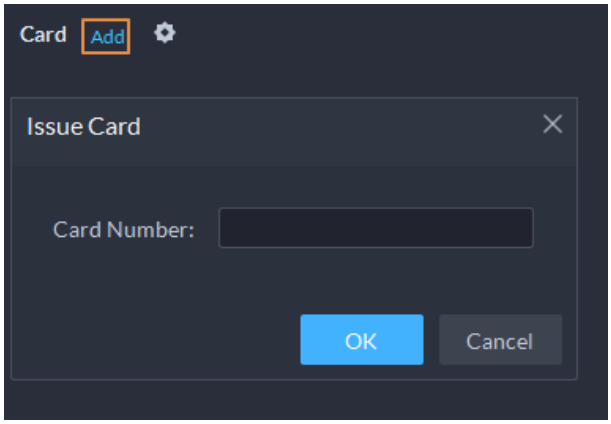
1) Select the room number.
2) Issue cards.

   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**.

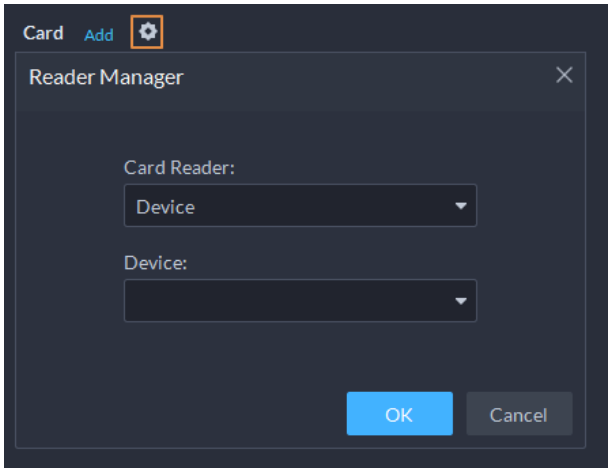
Figure 5-91 Issue card



   - Issue card by using a card reader

     Click , select a card reader or device, and then click **OK**. Swipe card through the reader or device, and then a new card will be issued.

Figure 5-92 Reader manager

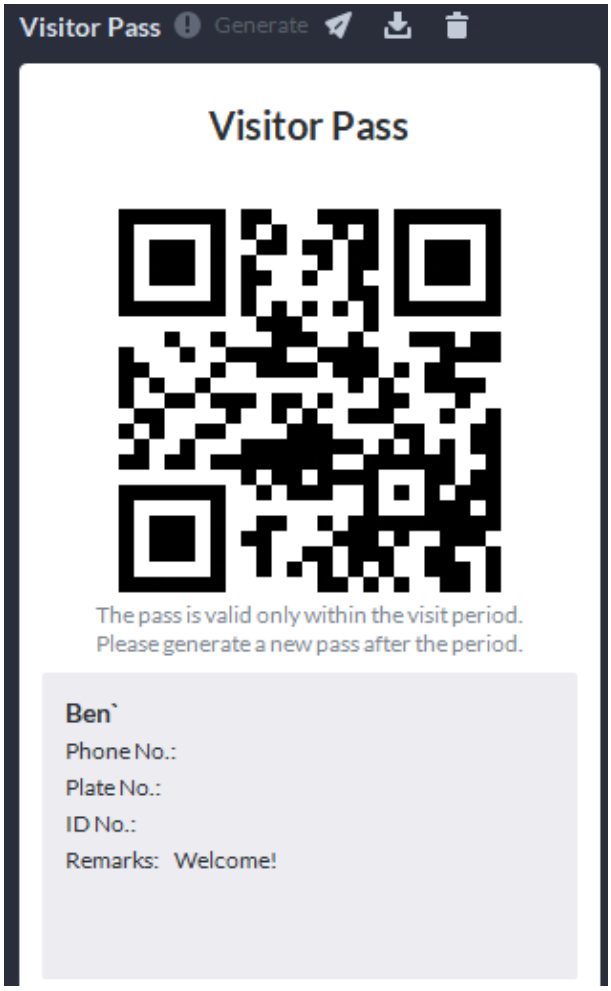


3) Set face picture. Position your face in the snapshot area, and click **Upload Picture** to select a picture or click **Snapshot** to take a photo.

Figure 5-93 Take a face photo

4) Click **Generate** to generate a QR code for the pass.
You can click to download the QR code, and click to send it to the visitor by email.

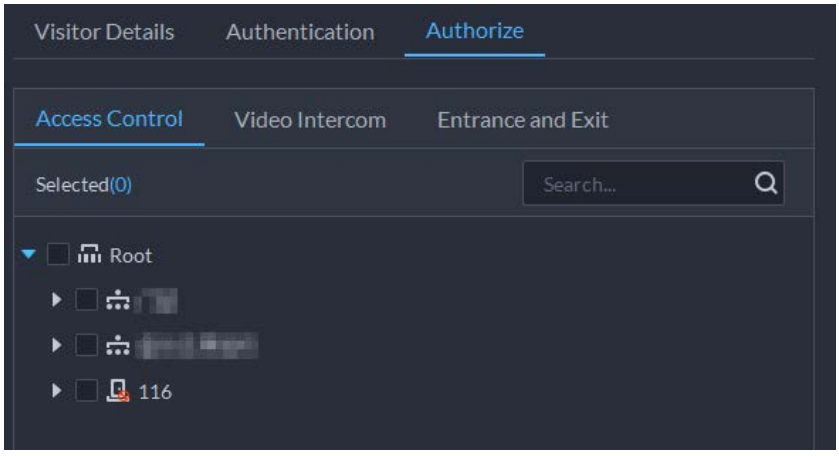
Figure 5-94 Authentication



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 5-95 Authorize



Step 5 Click **OK**.

Related Operations

- End visit.

Click to end a visit.

- View card swiping records.
  Click the **Card-swiping Record** tab, or click in visitor record to view visitor card swiping records.
- Cancel appointment.
  Click , and cancel the appointment as the screen instructs.

5.4.5.4 Checking Out

When visitors are leaving, remove their access permissions.

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

Step 2 Find the appointment record of the visitor, and then click .

Step 3 Click **OK** to remove access permission.

If you have issued a card to a visitor, make sure the visitor returns the card before leaving.

5.4.5.5 Searching for Visit Records

Search for visit records, and view visitor details and card swiping records.

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

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

The results are displayed.

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

Step 3 Click to view visitor details and card swiping records.

5.5 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, and manage parking lots intuitively through their different layers.

5.5.1 Entrance and Exit Monitoring

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

Step 2 Select the number of windows you want from .

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 5-96 Monitor entrances and exits

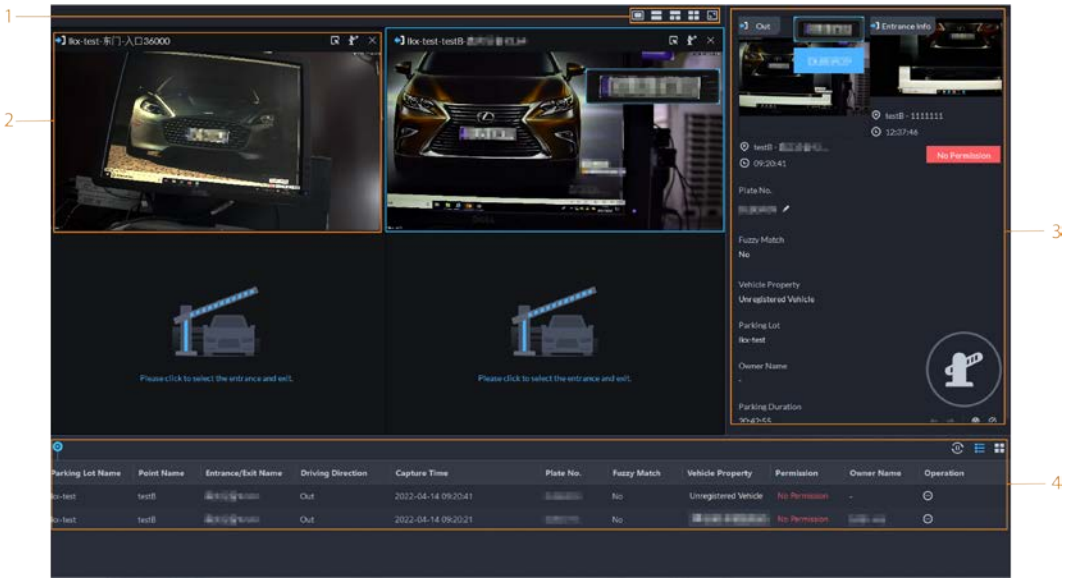


Table 5-13 Page description

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. This operation will not generate an enter or leave record. ◇ **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	Displays records of barriers not opened. • 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.

5.5.2 Searching for Records

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

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

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

5.5.2.1 Searching for Entrance Records

Step 1 Log in to the DSS Client. On the **Home** page, click > **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 , and the detailed information is displayed on the right. Click the play icon to play the recorded video, and then click to download it.
  Click 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.
- Click **Layer Info** to view the location of the channel that captured the vehicle on the layer.
- Forced exit.
  If **No** is displayed under **Already Exited** when the vehicle has exited, click 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 and then select the items to be displayed.

5.5.2.2 Searching for Exit Records

Step 1 Log in to the DSS Client. On the **Home** page, click > **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 , and the detailed information is displayed on the right. Click the play icon to play the recorded video, and then click to download it.

Click 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.

- Click **Layer Info** to view the location of the channel that captured the vehicle on the layer.
- 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.

5.5.2.3 Searching for Forced Exit Records

Step 1 Log in to the DSS Client. On the **Home** page, click > **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 , and the detailed information is displayed on the right. Click the play icon to play the recorded video, and then click to download it.

  Click 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.
- Click **Layer Info** to view the location of the channel that captured the vehicle on the layer.
- 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.

5.5.2.4 Searching for Parking Records

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

Step 2 Click the **Parking 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 , and the detailed information is displayed on the right, including entry and exit records. Click the play icon to play the recorded video, and then click to download it.
  For the dual camera mode, click each channel to view the information it captured.
- Click **Layer Info** to view the location of the channel that captured the vehicle on the layer.
- 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.

5.5.2.5 Searching for Capture Records

Step 1 Log in to the DSS Client. On the **Home** page, click > **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 , and the detailed information is displayed on the right. Click the play icon to play the recorded video, and then click to download it.
  Click 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 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.

5.5.3 Visualized Parking Lot

Quickly understand your parking lot by viewing the information on the layers.

Step 1 Log in to the DSS Client. On the **Home** page, click > **Parking Lot** > **Visualized Parking Lot**.

Step 2 Select a parking lot, and then double-click a layer.

Step 3 View the information on the layer.

Table 5-14 Operation description

Icon/Parameter	Description
	View the total and available parking spaces on the layer.
	View all the resources on the layer.
	Zoom in and out on the layer.
Display Selected Layers	Select which resources you want to display on the layer.
Pane	Click and hold on the layer to select multiple devices. After you select multiple devices, you can perform the following operations: •  : View the capture records from the selected devices. •  : View the entrance records from the selected devices. •  : View the exit records from the selected devices. •  : View the parking records from the selected devices. •  : Open a video player and you can view the real-time video of each device you selected. If you are viewing the real-time video from an entrance or exit point, you can click  to open the barrier. •  : Open a video player and you can search for and view the recorded videos from the devices you selected.
Reset	Reset the layer to its default size and position.
Hide Plate No.	If reserved parking spaces have been configured on the layer, you can hide partial information of the number plates displayed on the parking spaces.

5.6 Intelligent Analysis

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

5.6.1 People Counting

5.6.1.1 Real-time Count

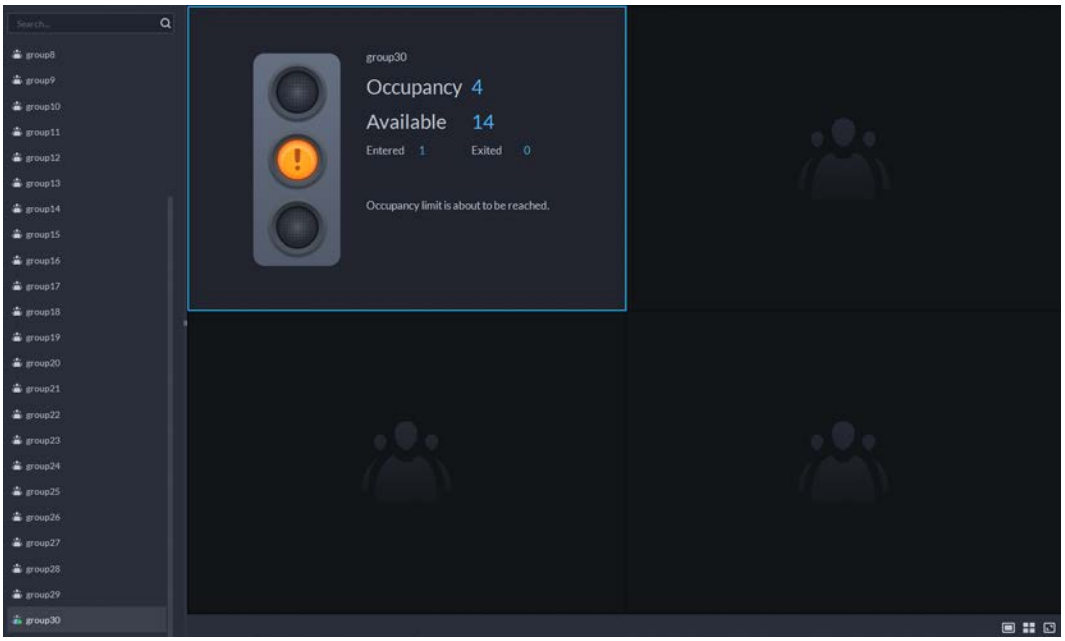
Step 1 Log in to the DSS Client. On the **Home** page, click  > **Intelligent Analysis** >  > **Real-time Count**.

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.

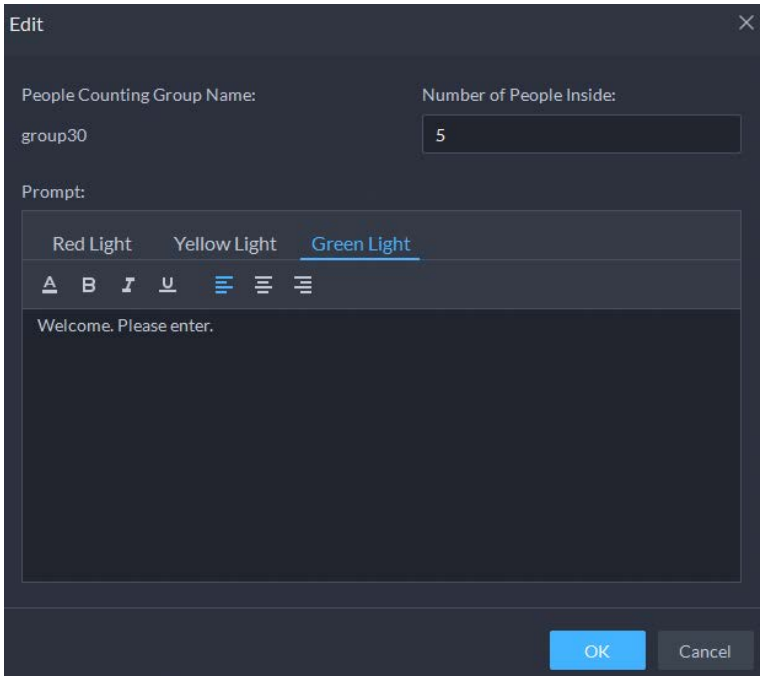
Figure 5-97 Real-time count



Step 3 Hover you mouse on the window displaying real-time data, and then click .

Step 4 You can enter a number of people to overwrite the current data, and customize the content to be displayed for green, yellow and red light.

Figure 5-98 Edit the content and data



Step 5 Click **OK**.

5.6.1.2 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 5-99 Historical people counting data

Related Operations

- : Change the display format of the data.

  Only weekly report supports will display the number of retention.

- **Export**: Export the data into a .zip file to your computer.

5.6.2 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 "3.2.2.5.2 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 > **Intelligent Analysis** > .

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.

5.6.3 In-area People Counting

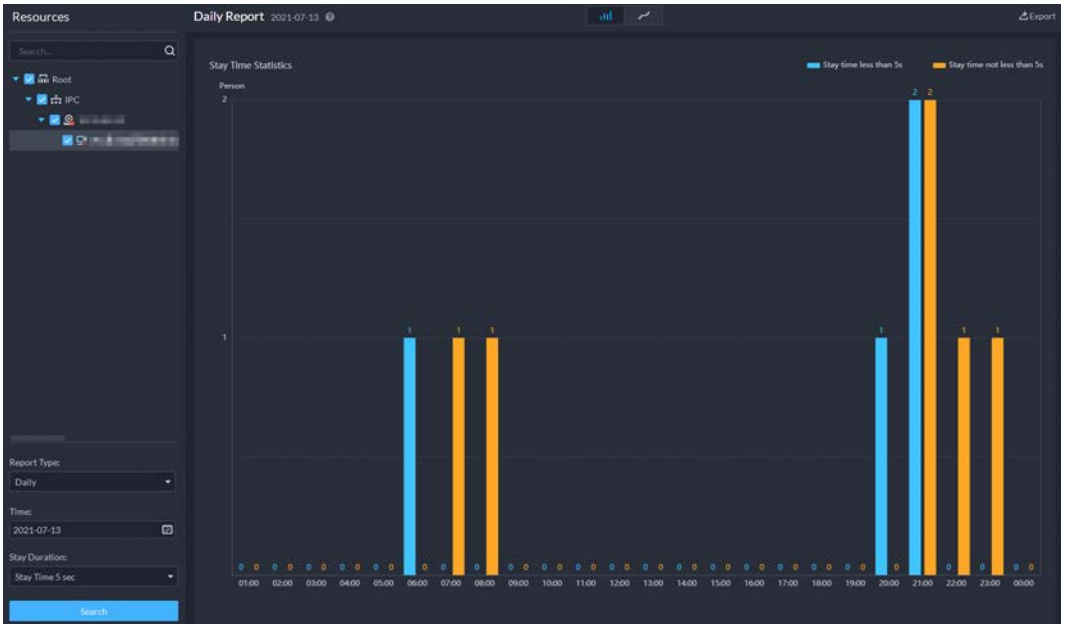
View the in-area people number statistics of one or more channels.

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 5-100 In-area people number statistics



Related Operations

- : Change the display format of the data.
- **Export**: Export the data to your PC.

5.7 Maintenance Center

You can view the overall running status of the platform, including server, channel, and device. Clear view of fault information allows you to locate the fault source and type, and then fix it in time. You can also update the programs of devices.

5.7.1 Viewing System Status

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

Step 2 View system status.

- Click **Overview** to view the overall running status of the platform, including the online status of channels and devices, storage, server status, and faults. You can export the current information as a PDF file to your PC, and change the refresh frequency on the upper-right corner.
- Click **Channel Status** to view the online status, video duration, video integrity, and more for each channel. Click of a channel and you will be directed to the **Fault** page, where you can search for faults related to that channel.
- Click **Device Status** to view the online status, running status, manufacturer, and more for each device. Click of a device and you will be directed to the **Fault** page, where you can search for faults related to that device.
- Click **Server Status** to view the information and running status for each server. Click of a server and you will be directed to the **Fault** page, where you can search for

faults related to that server.

- Click **Disk Status** to view the disk status and RAID information of storage devices.
- Click **Fault** to view faults that occurred with the defined period. You can only search for faults occurred within 7 days.

Related Operations

- On the left of each page, you can configure the search conditions to only display the content you want.
- For channel and device status, click  to filter what information to be displayed.
- Click **Export** and follow the onscreen instructions to export information to your PC.

5.7.2 Updating Device Program

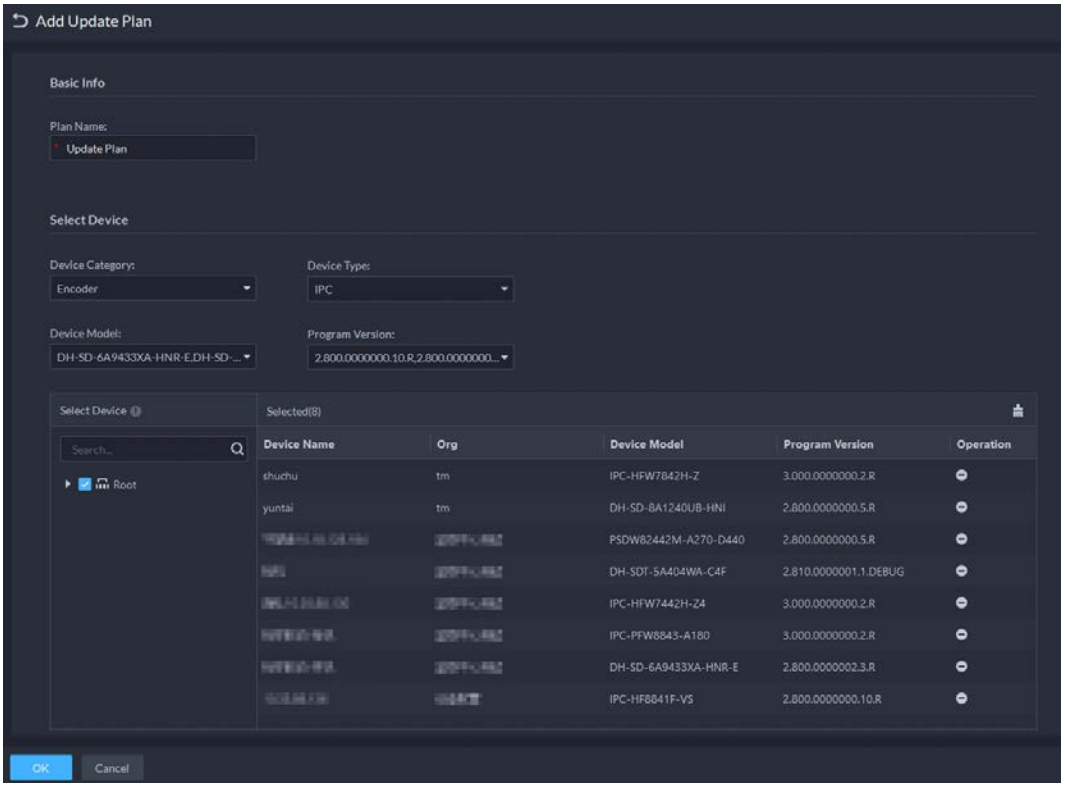
Add a plan to update the programs of selected devices in batches.

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

Step 2 Click  .

Step 3 Click **Add**.

Figure 5-101 Add an update plan



Step 4 Enter a name for the plan, and then select the device category, type, model, and program version.

The platform will only display corresponding devices.

You can only update the programs of IPCs and access control devices of Dahua access protocol and added with an IP address.

Step 5 Select the devices you want to update. Click to cancel selecting all devices.

Step 6 Configure when to update the devices.

- **Now**: Update the devices immediately after the plan is added.
- **Custom**: Update the devices at the defined time.

Step 7 Click **Upload File** to upload the update program.

- Make sure that the uploaded program matches the models and current program versions of selected devices.
- Make sure that the network is stable and the power properly connected for all devices. Otherwise, they might not work properly.

Step 8 Click **OK**.

Related Operations

In the list of update plans, you can view the information of each plan, including name, update program, update start time, and update status.

- Click to delete a plan one by one; select multiple plans, and then click **Delete** to delete them in batches.
- Click to view the update status of the devices in a plan.
  - Click to remove a device from the plan; select multiple devices, click **Delete** to remove them in batches.
  - If one or more devices failed to update, click to update a device again one by one, or select multiple devices, and then click **Update Again** to update them in batches.

6 General Application

This chapter introduces the general businesses, including target detection, face recognition, and ANPR.

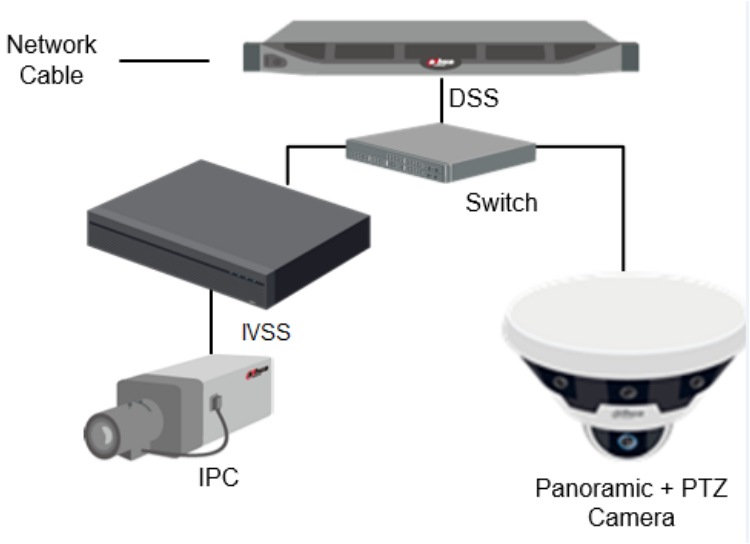
6.1 Target Detection

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.

6.1.1 Typical Topology

Figure 6-1 Typical topology



- General cameras record videos.
- Video metadata cameras such as panoramic + PTZ camera record videos and analyze people, and motor and non-motor vehicles.
- IVSS manages cameras and analyzes people, and motor and non-motor vehicles.
- The platform centrally manages IVSS and cameras, receives analysis results from cameras and displays the reports.

6.1.2 Preparations

Make sure the following preparations have been completed:

- Cameras and IVSS are correctly deployed, and video metadata is enabled on them. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure the parameters, see "3 Basic

Configurations".

- When adding a camera or IVSS, select **Encoder** for device category.
- After adding the camera or IVSS to the platform, select **Target Detection** from **Features** of the device.

6.1.3 Live Target Detection

Step 1 Log in to the DSS Client. On the **Home** 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 6-2 Live view

Step 3 Click and then click to view live metadata events.

Step 4 View live video, and human body, vehicle, and non-motor vehicle information.

- Click an event record to view the event snapshot. You can play back the video of the event. Different events support different operations.
- When playing back video, click to download the video to a designated path.
- Click to play back the video before and after the snapshot.
- Click to delete event information.
- Click to view the most recent events.

6.1.4 Searching for Metadata Snapshots

Search for metadata snapshots by setting search criteria or uploading images.

Step 1 Log in to the DSS Client. On the **Home** 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 "5.3 DeepXplore".

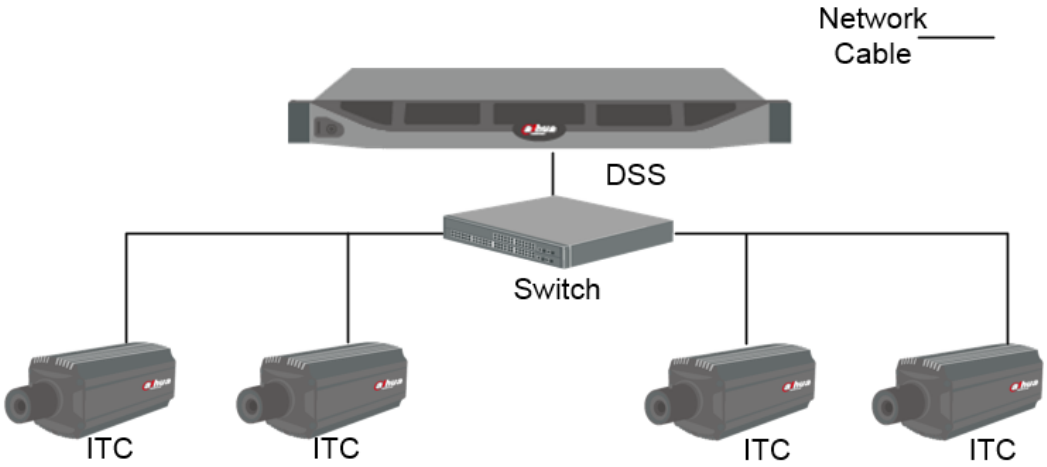
6.2 ANPR

View automatic number plate recognition in real time or search for records. You can view the moving track of a vehicle. This is useful for road monitoring.

- 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.
- Vehicle track
  According to the ANPR camera locations that a vehicle has passed through, the platform displays the driving track of the vehicle on the map.

6.2.1 Typical Topology

Figure 6-3 Typical topology



- ANPR cameras (ITC camera) capture and recognize vehicles.
- DSS centrally manages ANPR cameras, receives and displays vehicle snapshots and information uploaded from the cameras.

6.2.2 Preparations

Make sure that the following preparations have been made:

- ANPR cameras are 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 "3 Basic Configurations".
  - When adding an ITC camera, select **ANPR** for device category, and then select **ANPR Device** for **Device Type**.
  - ANPR snapshots are only stored on **ANPR Picture** disks. On the **Storage** page, configure at

least one **ANPR Picture** disk. Otherwise vehicle pictures cannot be viewed.

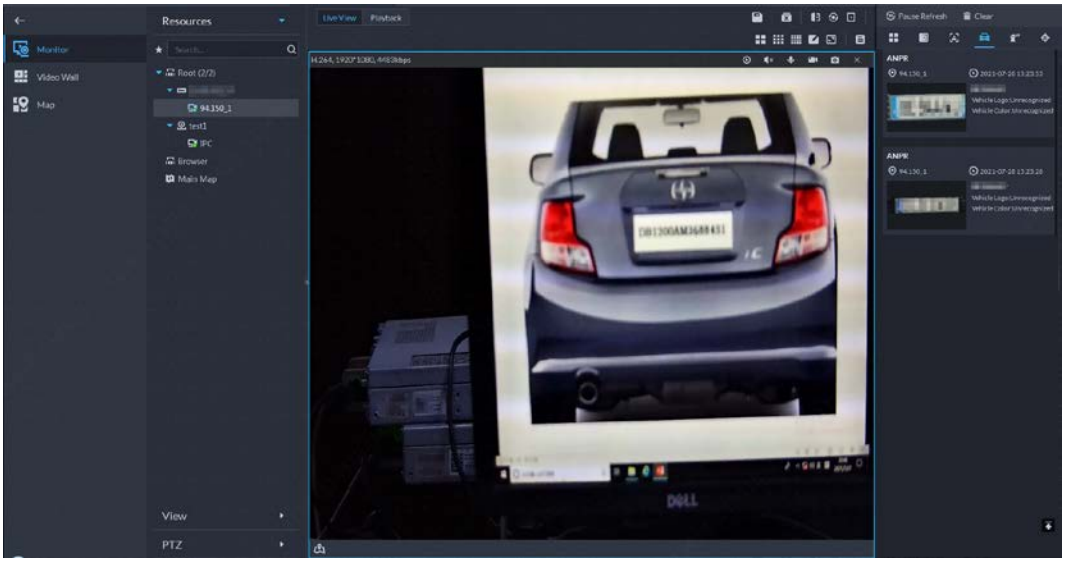
6.2.3 Live ANPR

View ANPR live video and plate snapshots.

Step 1 Log in to the DSS Client. On the **Home** 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 6-4 Live view



Step 3 Click and then click .

Step 4 View live ANPR events.

- Click an event record to view event snapshots. You can also play back the video of the event. Different events support different operations.
- When playing back a video, click to download the video to a designated path.
- Click to play back the video before and after the snapshot.
- Click to delete event information.
- Click to view the most recent events.

6.2.4 Searching for Vehicle Snapshot Records

Step 1 Log in to the DSS Client. On the **Home** 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 "5.3 DeepXplore".

6.3 Face Recognition

Configure face recognition settings on the device and the platform before you can view face

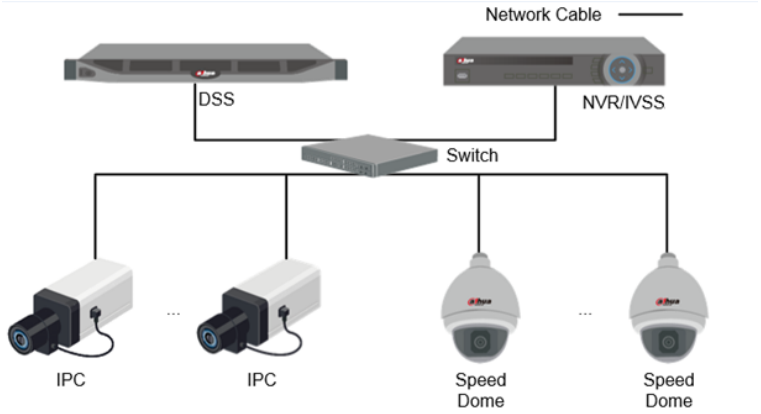
recognition results on the platform.

6.3.1 Typical Topology

The face recognition feature is available on select models of NVR, IVSS and FR cameras.

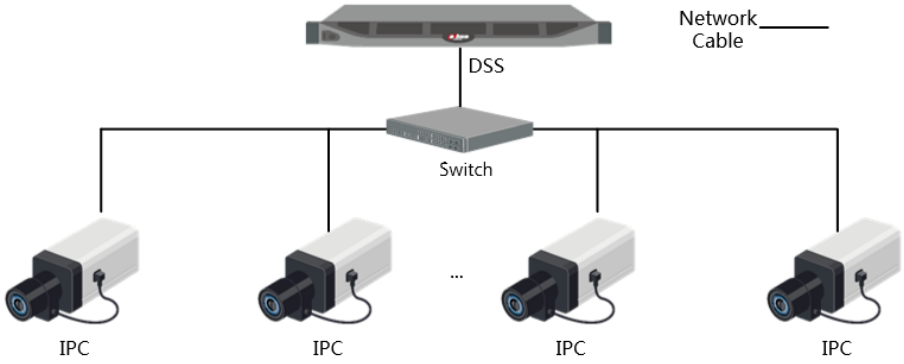
- Face recognition by NVR/IVSS

Figure 6-5 Typical topology (NVR/IVSS)



  - Cameras record videos.
  - NVR/IVSS is used for face recognition and storage.
  - DSS centrally manages cameras, NVRs, and the face database, and provides live view and face search.
- Face recognition by camera

Figure 6-6 Typical topology (camera)



  - Cameras record face videos, and detect and recognize faces.
  - DSS centrally manages cameras, NVRs, and the face database, and provides live view and face search.

6.3.2 Preparations

Make sure that the following preparations have been made:

- Face recognition devices are correctly configured. For details, see corresponding user's manuals.
- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
  - When adding face recognition devices, select **Encoder** for device category.
  - After adding a face recognition NVR or IVSS, select **Face Recognition** for **Features** of the

corresponding channels.

- ◇ After adding face recognition cameras or face detection cameras, select **Face Recognition** or **Face Detection** for **Features**.
- ◇ Face snapshots are stored in the **Face/Alarm and Other Pictures** disk. Configure at least one local disk for picture storage. Otherwise, the platform cannot display snapshots.

6.3.3 Arming Faces

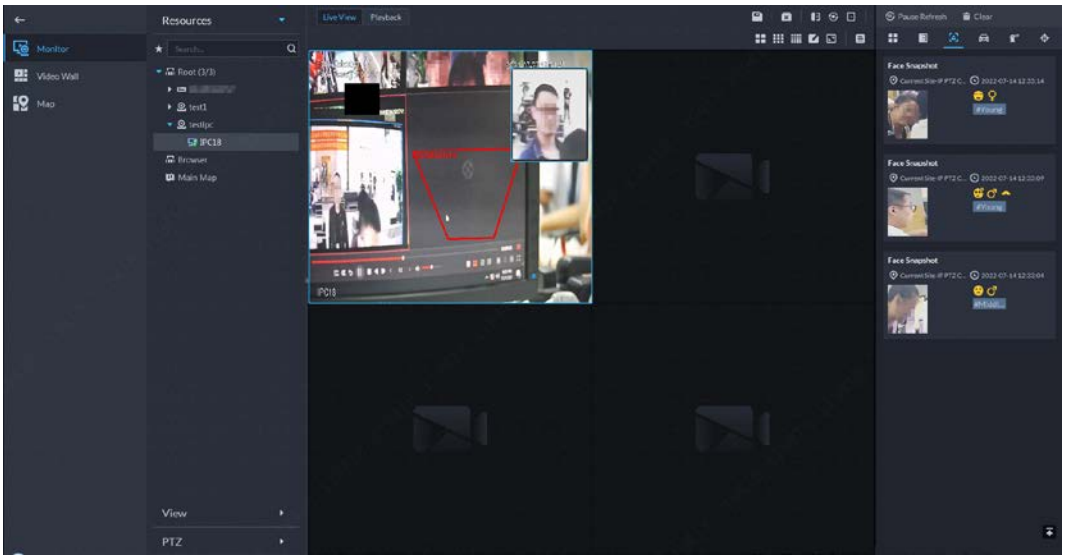
Before arming faces, you need to add the persons to face recognition group. For details, see "4.4.1 Face Watch List".

6.3.4 Live Face Recognition

Step 1 Log in to the DSS Client. On the **Home** 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 6-7 Live view



Step 3 Click and then click to view live face recognition information.

Step 4 View live video, and human body, vehicle, and non-motor vehicle information.

- Click an event record to view event snapshots. You can play back the video of the event. Different events support different operations.
- When playing back video, click to download the video to designated path.
- Click to play back the video before and after the snapshot.
- Click to refresh events; click to pause refreshing.
- Click to delete event information.
- Click to view the most recent events.

6.3.5 Searching for Face Snapshots

Search for face snapshots by setting search criteria or uploading images.

Step 1 Log in to the DSS Client. On the **Home** 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 **Person** section. For details, see "5.3 DeepXplore".

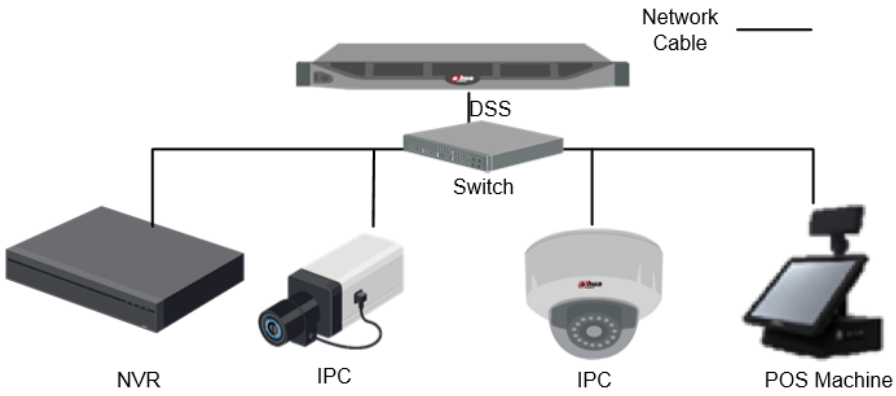
6.4 POS

View POS live video and records.

- Live view
  View live POS video and the transaction details overlapped on the video.
- Playback
  Search for POS transaction records and play the recorded video. The POS video clip can start 10 seconds before or after the POS receipt printing.

6.4.1 Typical Topology

Figure 6-8 Typical topology



- Cameras record videos of each POS transaction.
- NVRs are connected with cameras and POS machines, and store videos.
- POS machines record transaction details and generate receipts. They connect to the platform through NVRs.
- The platform centrally manages NVRs and cameras, and provides live videos and POS transaction video records.

6.4.2 Preparations

Make sure that the following preparations have been made:

- Cameras, NVRs and POS machines are correctly configured. For details, see the corresponding

user's manuals.

- Basic configurations of the platform have been finished. To configure, see "3 Basic Configurations".
  - When adding an NVR, select **Encoder** for device category.
  - At least one POS channel is connected to NVR.
  - On the **Bind Resource** page, bind video channels to the POS channels. See "3.2.3 Binding Resources".

6.4.3 Setting POS End Sign

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 **POS End Sign** tab.

Step 3 Set the end line of POS receipt.

Step 4 Click **OK**.

6.4.4 POS Live View

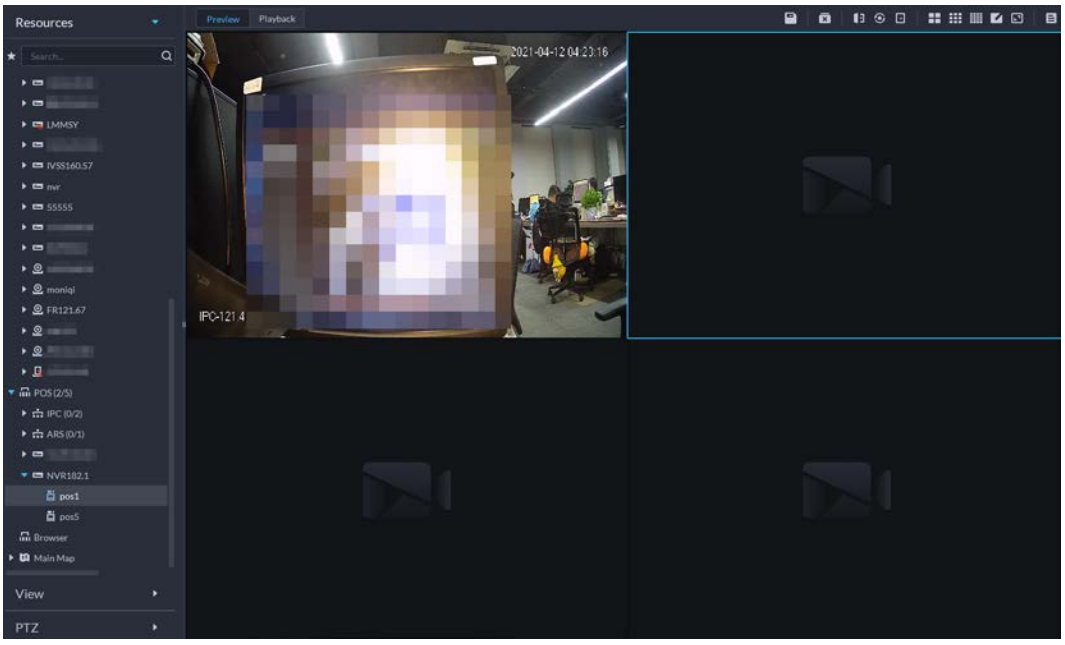
View real-time POS transaction video and details.

Make sure that the POS channel has been bound to video channel. For details, see "6.4.4 POS Live View".

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

Step 2 In the **POS** list in the **Resources** section, select a channel, device or organization, double-click or drag it to the window.

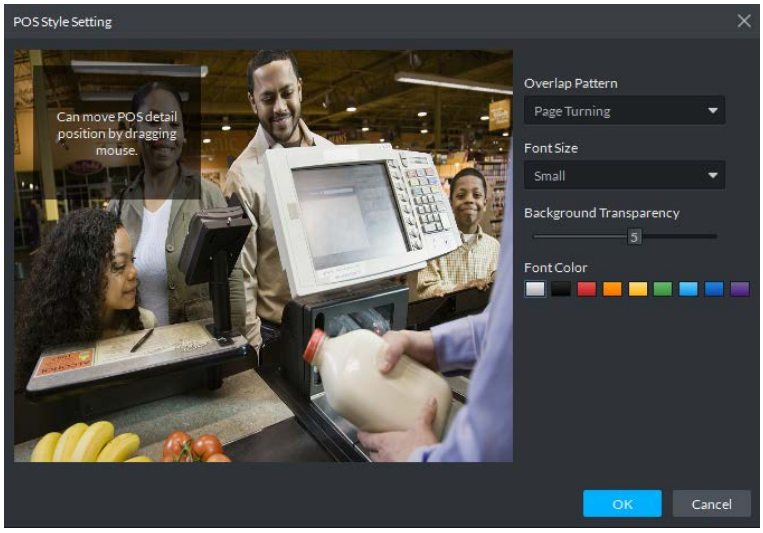
Figure 6-9 POS video



Step 3 (Optional) Set POS information style.

1) Right-click and select **Set POS Style**.

Figure 6-10 POS style setting



2) Set **Overlap Pattern**, **Font Size**, **Background Transparency** and **Font Color**.
3) Point to POS information overlay area, press mouse left button and move it to adjust POS information overlay position.
4) Click **OK**.

6.4.5 Searching for POS Receipts

Search for POS receipt to view related video of receipt. You can search for the video half an hour before and half an hour after the time when POS receipt is printed, and you can start to play video 30 s before the time when POS receipt is printed.

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

Step 2 Click .

Step 3 Select channel and time, select **POS Record**, and then click **Search**.

Step 4 Double-click a POS record to view related snapshot and video. For more operations, see "5.3.1 Searching for Records".

7 System Configurations

This chapter introduces system parameters configuration, license, service management and backup and, restore.

7.1 System Deployment

The platform supports managing server information and adjusting the upper-level server of a server or device.

7.1.1 Distributed Deployment

Set the server type, and assign devices to different servers.

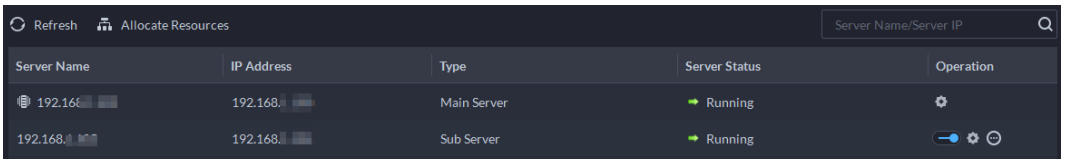
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Deployment**.

Step 2 Click .

Step 3 Manage servers.

- Click to view server details.
- Click corresponding to a server to define the server type. A server can be set to sub server or standby server when it is not in use.
- Click to enable the server. means the server is enabled.
- Click to delete the server.

Figure 7-1 Servers



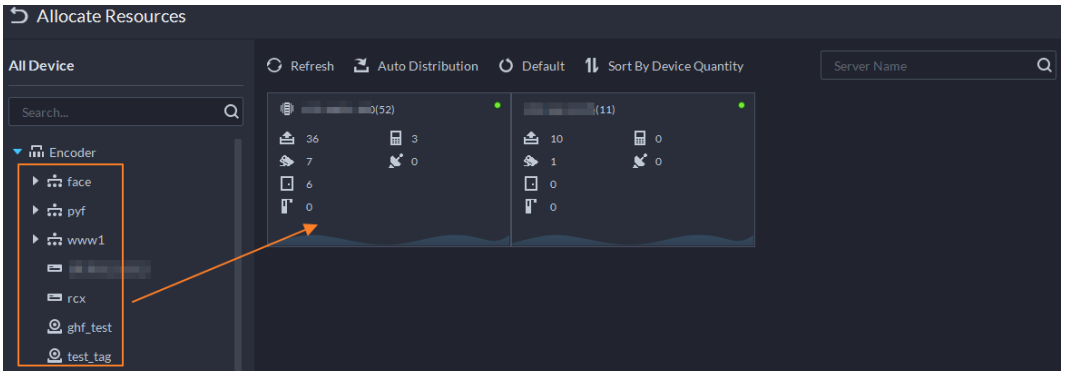
Step 4 Assign devices to different servers.

- Manually

  Click **Allocate Resources**, and then select devices or channels on the left side, and drag them to the server on the right. The number of corresponding devices in the target server increases, and the devices in the original server reduces.

- Click **Default**, the servers are sorted in the order in which they were added.
- Click **Sort By Device Quantity**, the servers will be sorted by the number of devices.

Figure 7-2 Resource allocation

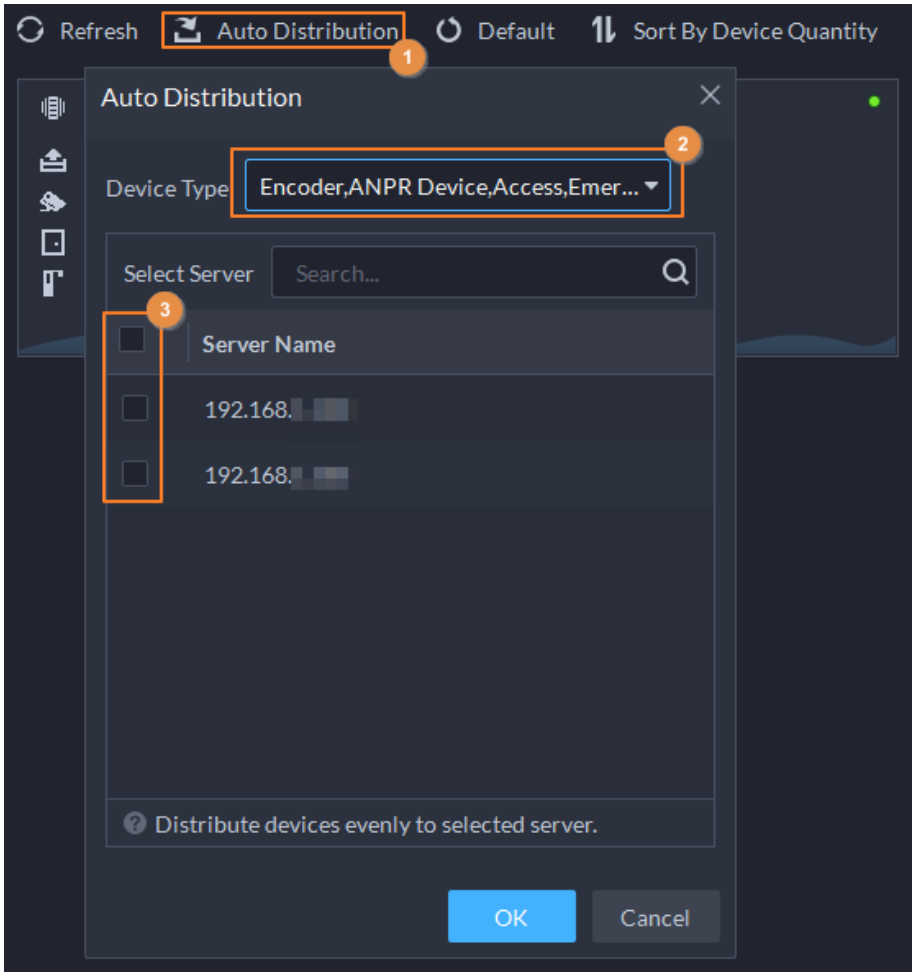


- Automatic allocation

  Allocate the same type of devices evenly to different servers.

  1. Click **Auto Distribution**.
  2. Select **Device Type**. Multiple types are supported.
  3. Select the server to which the devices belong. Multiple servers can be selected.
  4. Click **OK**.

Figure 7-3 Auto allocation



7.1.2 Cascade Deployment

Cascade deployment allows you to add a lower-level platform to an upper-level platform. After cascading, you can view the live video and recorded video of the lower-level platform from the upper-level platform. Also, you can display the videos on the lower-level platform on wall from the upper-level platform. 3 levels can be added at most.

Prerequisites

Make sure that the deployment of all relevant platforms has been completed.

- You need to configure the lower-level platform information on the upper-level platform.
- Supports adding DSS Express to lower-level platform.

Procedure

Step 1 Log in to client of the upper-level DSS platform. On the **Home** page, click and then in the **System Config** section, select **System Deployment**.

Step 2 Click .

Step 3 Click **Add**, and then configure parameters.

Step 4 After configuration, click **OK**.

Figure 7-4 Add cascade

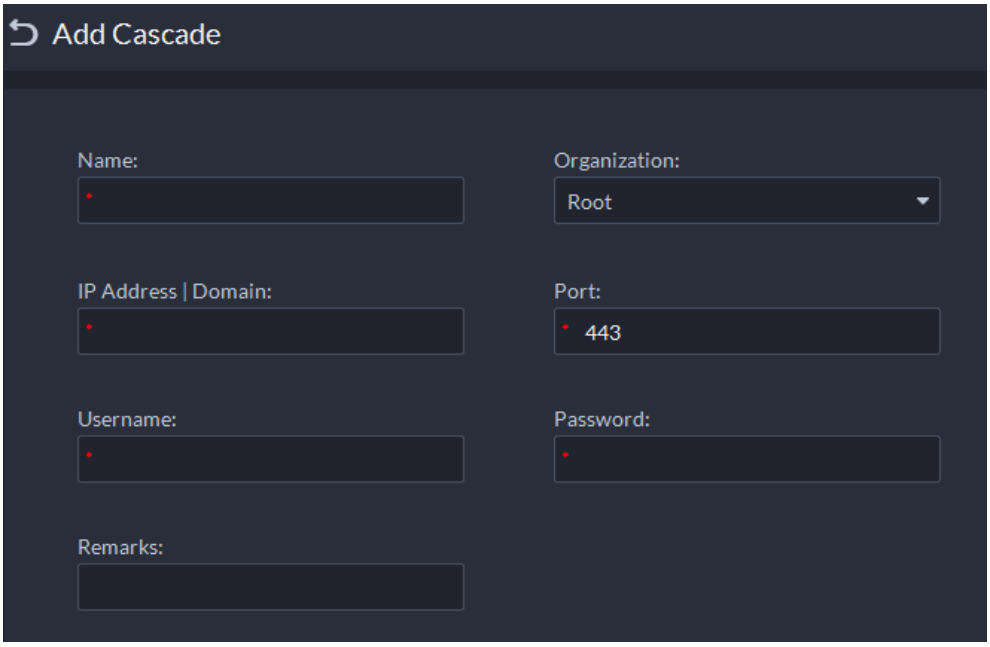


Table 7-1 Description of cascade parameters

Parameter	Description
Name	The name that identifies the platform to be added.
Organization	The organization that the added (lower-level) platform belongs to. The devices and channels of the added platform can be viewed on the upper-level platform from the organization that you have defined.
IP Address/Domain	The IP address or domain name, and the port of the added (lower-level) platform.
Port	
Username	The username and password for logging in to the added (lower-level) platform.
Password	

7.2 License

The system controls channel and function availability through the license. User can buy a license according to the channels and functions as needed.

The platform is unlicensed by default after being deployed.

License Types

- Trial
  A trial license is limited in capacity and expires in 90 days.
- Paid
  To acquire full control of the features and permanent use, you need to buy a formal license. After activating the first paid license, if you want to increase your license capacity, you can buy more license codes. For example, if you have 500 channels currently, you can buy another 500

channels. After activating the new 500 channels, you will have 1,000 channels in total.

- Unlicensed
  Lack permissions to use the system. This occurs after deactivating.

For expired trial version and unlicensed version, all modules are displayed as unauthorized, except for the resources, license, tools, and management modules.

Activation Methods

- Normal online activation
  When the platform server is connected to the Internet, it can connect to the license server, which supports online license activation by verifying the activation code.
- Normal offline activation
  When the platform server is on a local area network, it cannot connect to the license server. You need to obtain the license file from a computer with Internet access, and then import the license file to the platform to activate it.
- Upgrade from DSS Express to DSS Pro
  - Online activation
    When the platform is upgraded from Express to DSS Pro, and the original Express has a purchased license, and the platform server has Internet access, you can activate through verifying the new activation code and Express activation code (or importing Express deactivation file).
  - Offline activation
    When the platform is upgraded from Express to DSS Pro, and the original Express has a purchased license, the platform server cannot visit the license server. You can activate through verifying the new activation code and Express activation code (or importing Express deactivation file) and then importing the license obtained from a computer with Internet access.

7.2.1 Activating License

You can get the desired features or number of channels only after you load the corresponding license.

For details about activating a license, see "2.1.6.2 Activating License".

7.2.2 Deactivating License

After deactivation, the platform will be unauthorized. A deactivated license can be activated again on other servers, allowing users to change servers. The license can be deactivated with online and offline deactivation. If the server is connected to the network, use online deactivation. Otherwise use offline deactivation.

- You can only deactivate the license 3 times.
- After you deactivate the license, the system returns to the inactive state.
- Deactivated license can be used again. Keep it properly.

7.2.2.1 Online Deactivation

Background Information

Select this method if your platform sever is connected to a network.

Procedure

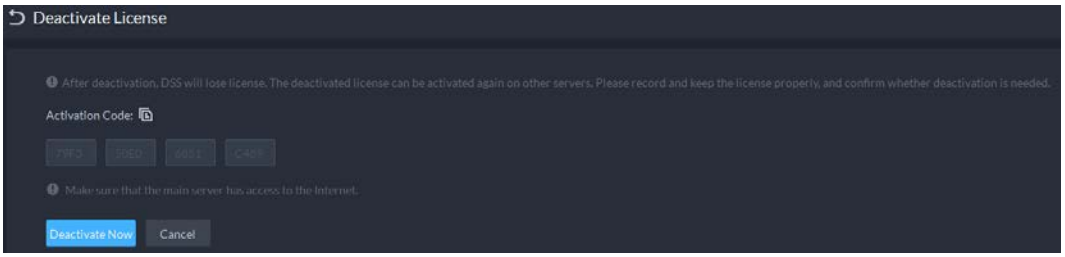
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **License**.

Step 2 In the **Deactivate License** section, click **Online Deactivate License**.

The license is reusable. We recommend copying the license code by clicking and then saving it locally.

Step 3 Click **Deactivate Now**, and then follow the onscreen instructions to finish deactivation.

Figure 7-5 Online deactivation



7.2.2.2 Offline Deactivation

Background Information

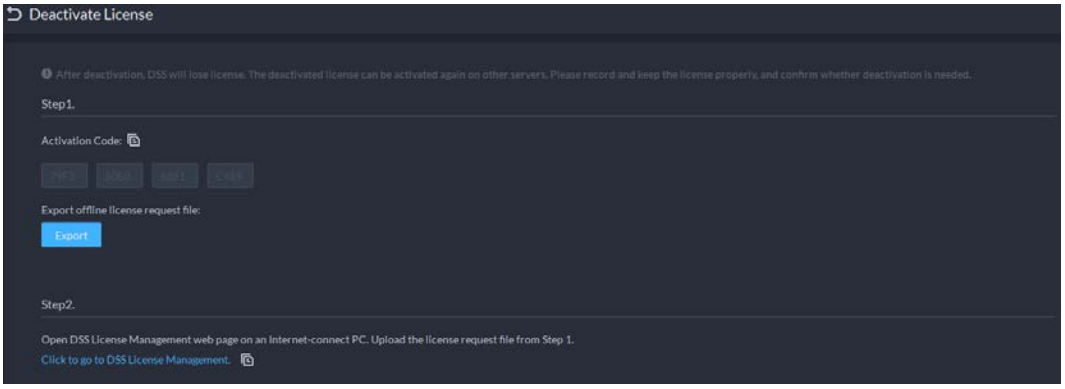
Select this method if your platform server has no Internet access.

Procedure

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

Step 2 In the **Deactivate License** section, click **Offline Deactivate License**.

Figure 7-6 Offline deactivation



Step 3 Click **Export** to export and save the license deactivation file locally.

After the license deactivation file is exported, the platform will become unauthorized, and you cannot use any function.

Step 4 Move the request file to a computer with Internet access. On that computer, open the system email that contains your license, and then click the attached URL go to the license management page.

Step 5 Select **DSS** > **Deactivate License**.

Step 6 Upload the license request file obtained from Step3, and then follow on-screen instructions to finish the process.

7.3 System Parameters

Configure security parameters, storage retention duration, email server, time sync, remote log, login method, and more.

7.3.1 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 , and then in the **System Config** section, select **System Parameter** > **Security Parameter**.

Step 2 Click 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.
  - ◇ For all users that log in to the platform, they do not need to enter the password when exporting or downloading 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.

7.3.2 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, POS messages, 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 , 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**.

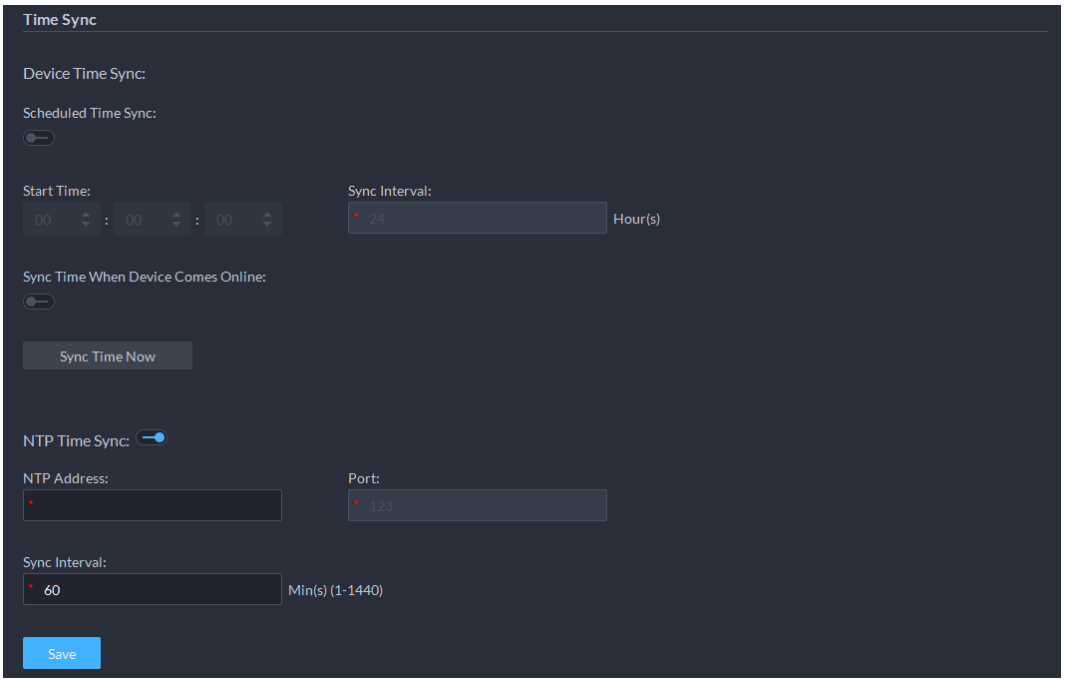
7.3.3 Time Synchronization

Synchronize the system time of all connected devices, PC client, and the server. Otherwise the system might malfunction. For example, video search might fail. The platform supports synchronizing the time of multiple devices, which have the same time zone as the platform. You can synchronize the time manually or automatically.

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 **Time Sync** tab. Enable the sync methods, and then set parameters.

Figure 7-7 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.

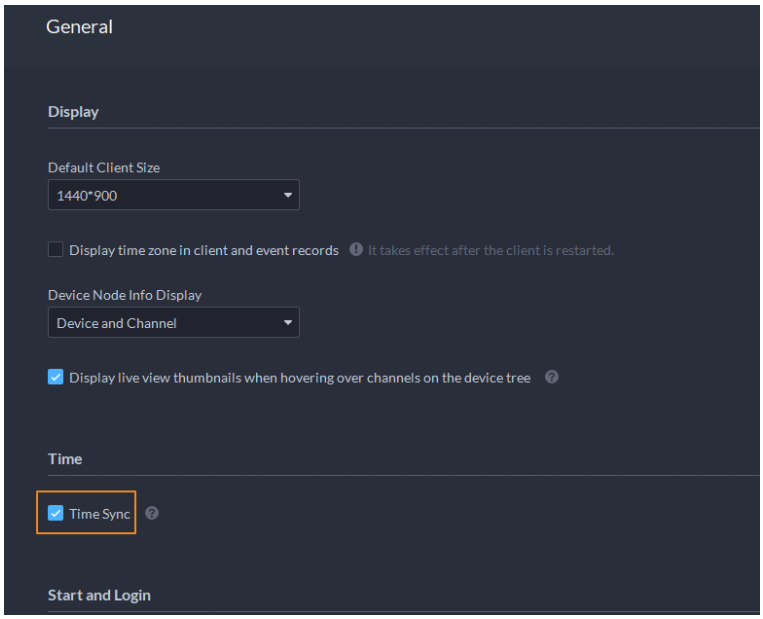
Step 3 Click **Save**.

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 restart the client to keep the time of the server and the PC client the same.

Figure 7-8 Enable time sync



3) Restart the client for the configuration to take effect.

7.3.4 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 7-9 Set email server

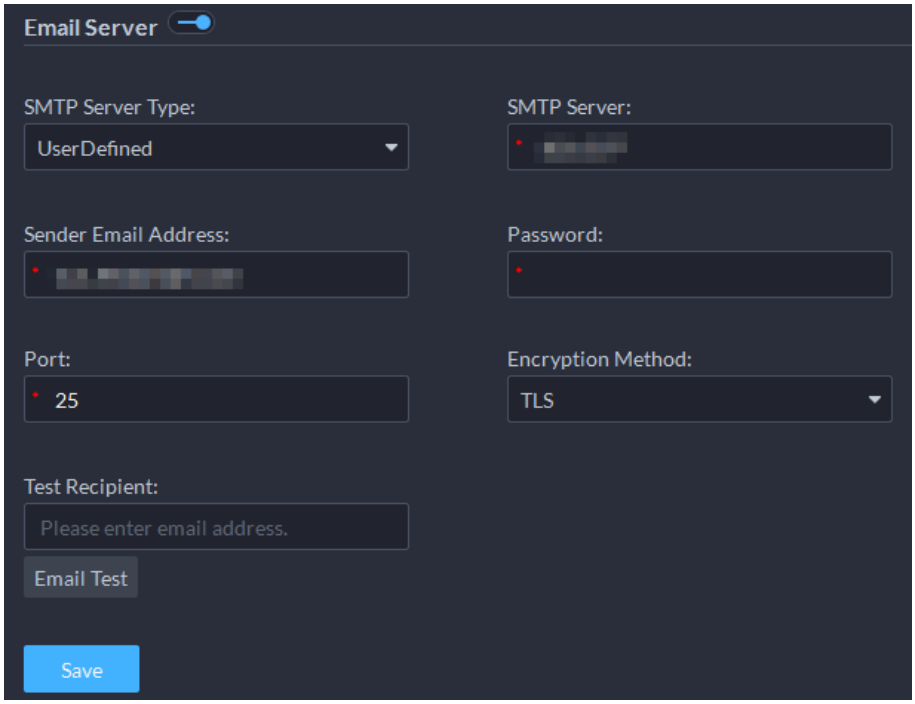


Table 7-2 Description of email server parameters

Parameter	Description
SMTP Server Type	Select according to the type of SMTP server to be connected. The types include **Yahoo**, **Gmail**, **Hotmail**, and **UserDefined**.
Sender Email Address	The sender displayed when an email is sent from DSS.
SMTP Server	IP address, password, and port number of the SMTP server.
Password	
Port	
Encryption Method	Supports no encryption, TLS encryption, and SSL encryption.
Test Recipient	Set the recipient, and then click **Email Test** to test whether the mailbox is available.
Email Test	

Step 3 Click **Save**.

7.3.5 Configuring Device Login Mode

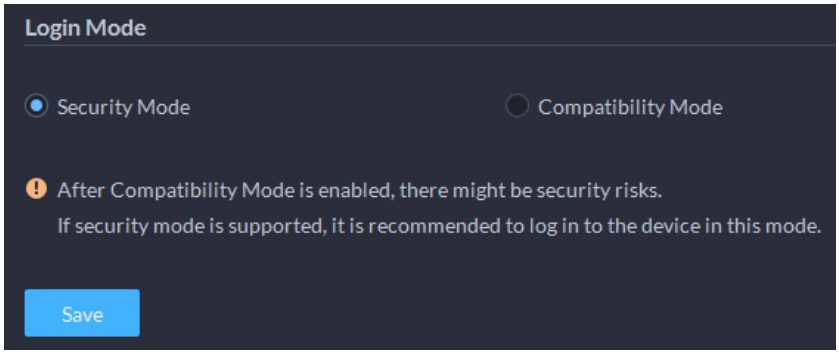
To ensure that you can use the device safely, we recommend using the security mode (if the device supports this mode. Otherwise, select compatibility mode).

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 7-10 Select a login mode



Step 4 Click **Save**.

7.3.6 Customizing POS End Sign

Configure the sign that prompts the end of a POS receipt.

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 **POS End Sign** tab.

Step 3 Enter the POS end sign, and then click **OK**.

Figure 7-11 POS end sign

7.3.7 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.

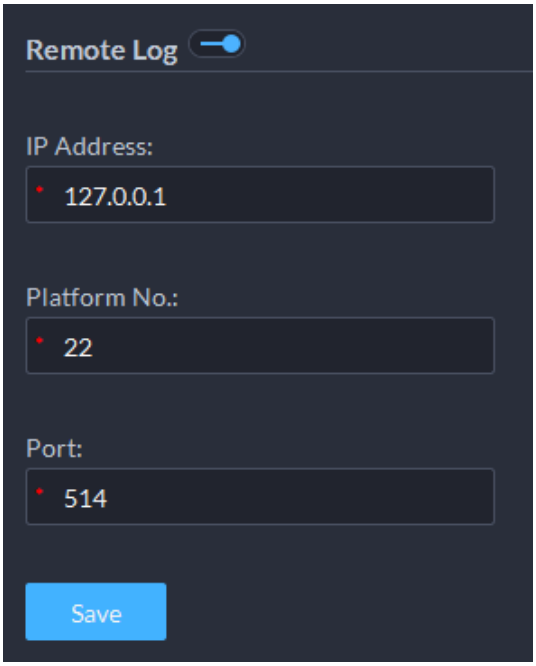
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter**.

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 7-12 Enable remote log



Step 4 Click **Save**.

7.3.8 Configuring Active Directory

When domain is deployed, and domain users are DSS platform users, you can import users quickly with this function.

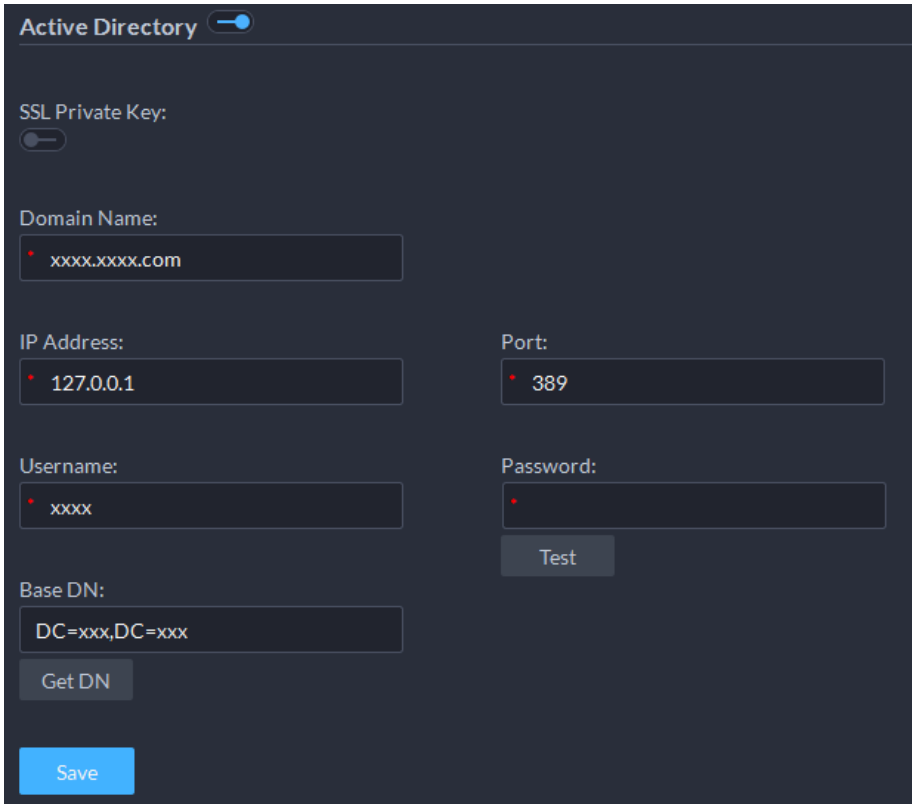
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **System Parameter**.

Step 2 Click the **Active Directory** tab.

Step 3 Click to enable the function, and then configure the parameters.

1) Enter domain information, including domain name, IP address, port, username, and password, and then click **Get DN** to automatically get basic DN information.
2) Click **Test** to check whether the domain information works.
3) Click **Save**.

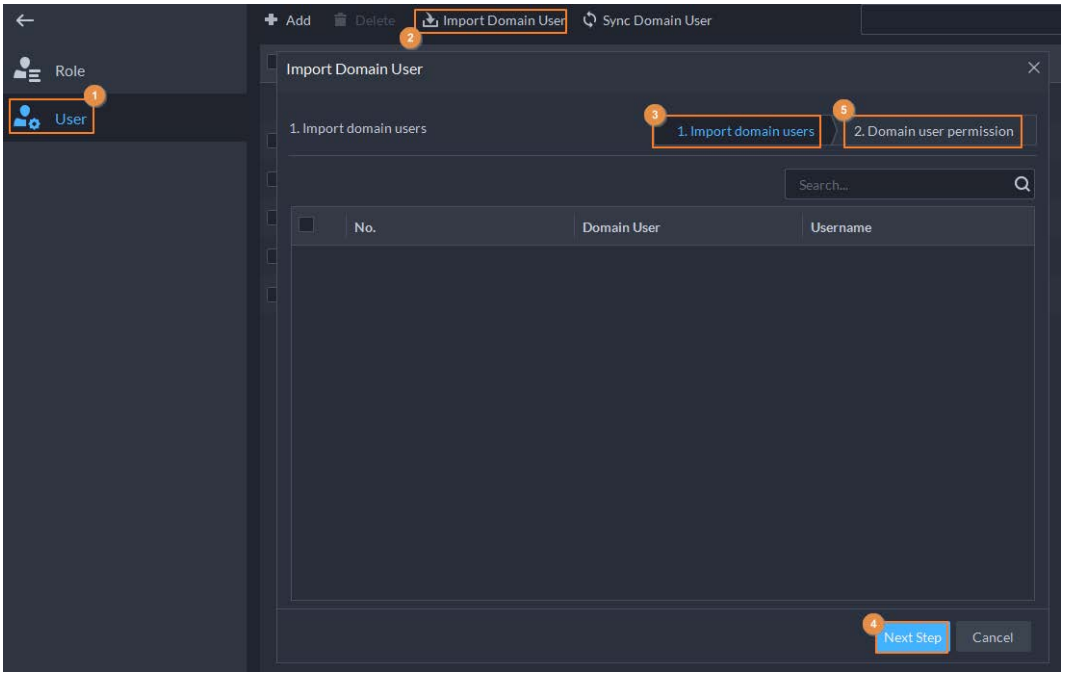
Figure 7-13 Active directory



Step 4 Import domain users.

1) Log in to the DSS Client. On the **Home** page, click , and then in the **Basic Config** section, select **User**.
2) Click the **User** tab.
3) Click **Import Domain User**.
4) Select the users to be imported, or search for and select the users, and then click **Next Step**.
5) Select role, and set permissions for the users.
6) Click **OK**.

Figure 7-14 Add domain users



7.3.9 Configuring Independent Database

The platform supports connecting to an independent database and storing data in it, including face images, video metadata, events, and ANPR information. But when you search for related data, the data in both the independent database and the platform database will be searched. Only official licenses support this function.

Prerequisites

You have prepared a ready-to-run database.

Procedure

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 **Independent Database Deployment** tab.

Step 3 Click to enable the function, and then configure the parameters.

Figure 7-15 Configure the independent database

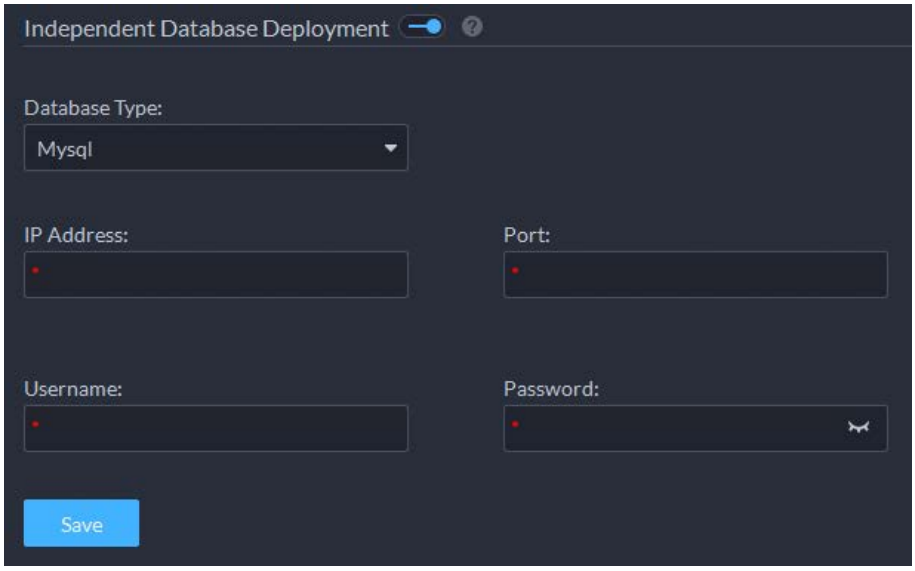


Table 7-3 Parameter description

Parameter	Description
Database Type	Only supports MySQL.
IP Address	Enter the IP address of the database.
Port	Enter the port of the database.
Username/Password	Enter the username and password used to log in to the database.

Step 4 Click **Save**.

An independent database can only connect to one platform.

7.4 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.

7.4.1 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**.

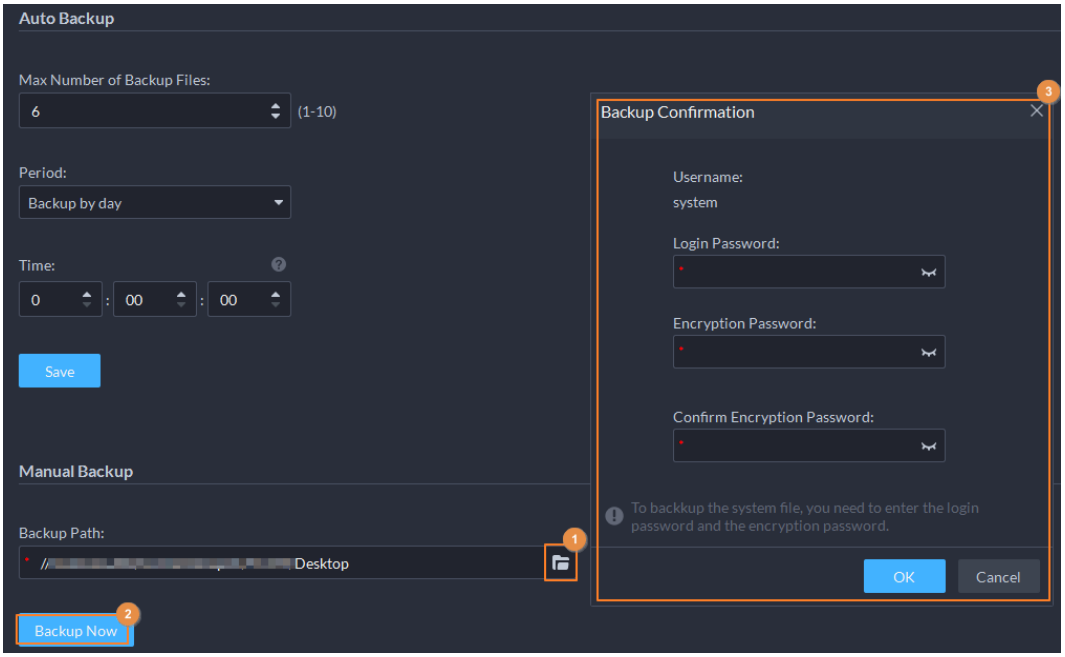
Step 2 Click the **Backup** tab.

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.

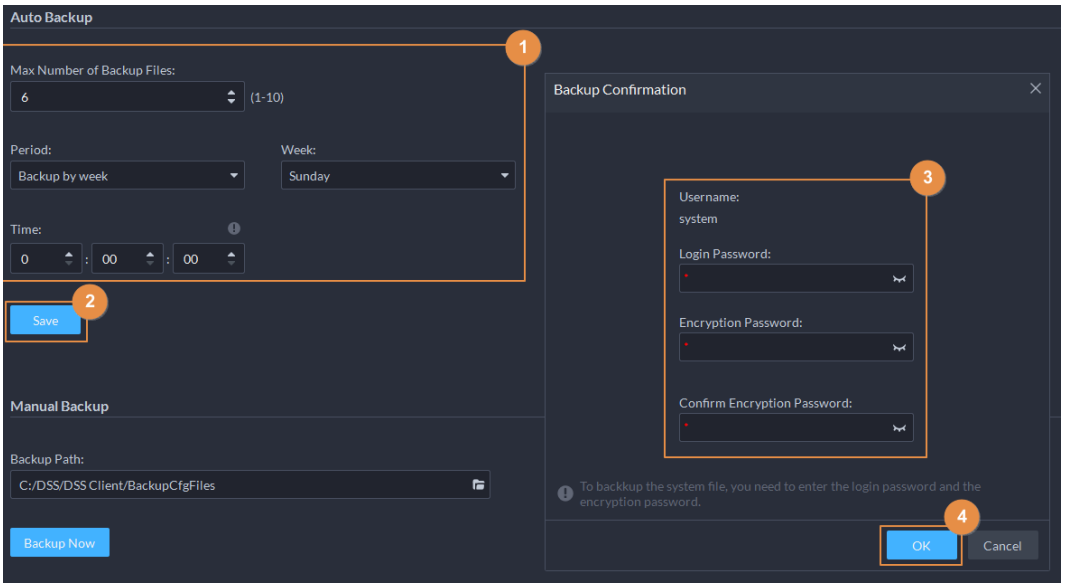
Figure 7-16 Manual backup



- 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 7-17 Auto backup



7.4.2 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.

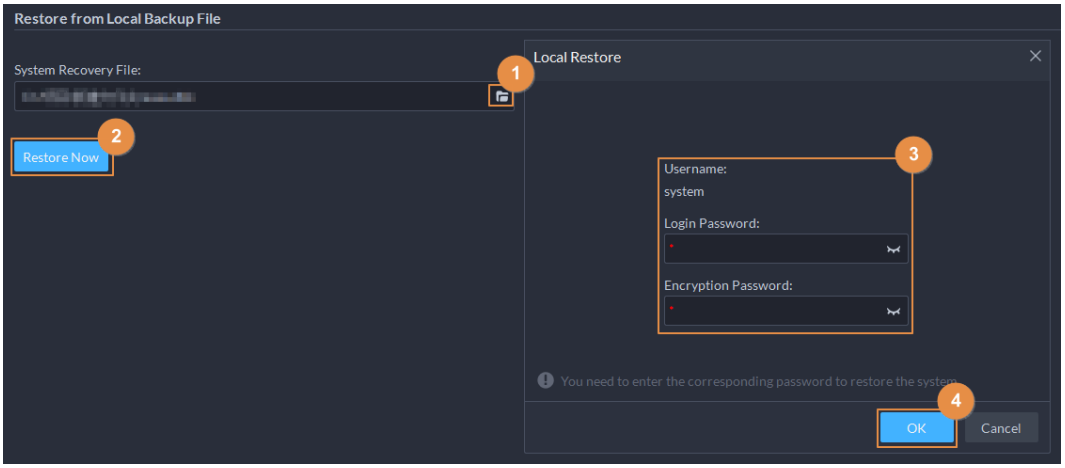
Step 1 Log in to the DSS Client. On the **Home** page, click , and then in the **System Config** section, select **Backup and Restore**.

Step 2 Click the **Restore** tab.

Step 3 Restore data.

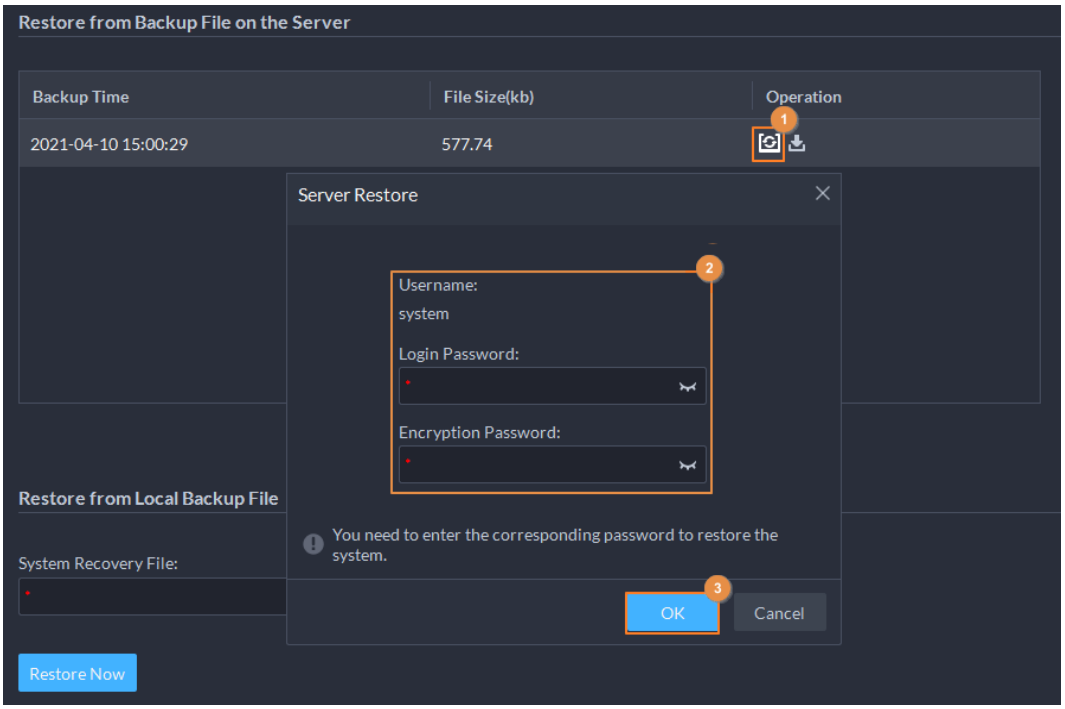
- Restore from local backup file: In the **Restore from Local Backup File** section, select the backup file path, click **Restore Now**, and then enter the passwords (the **Password** is the same as the system user's. The **Encryption Password** is the one created when the file was backed up).

Figure 7-18 Local restore



- Restore from backup file on the server: In the **Restore from Backup File on the Server** section, click , enter the passwords (the **Password** is the same as the system user's. The **Encryption Password** is the one created when the file was backed up), and then click **OK**. After restoration, the platform will automatically restart.

Figure 7-19 Restore from backup files on the server



You can click to download the backup file.

8 Management

8.1 Managing Logs

View and export operator logs, device logs and system logs, and enable the service log debug mode for troubleshooting.

8.1.1 Operator Log

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Logs**.

Step 2 Click .

Step 3 Click , 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**.

8.1.2 Device Log

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Logs**.

Step 2 Click .

Step 3 Select a device and time, and then click **Search**.

Step 4 To export the logs, click **Export**.

8.1.3 System Log

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Logs**.

Step 2 Click .

Step 3 Click , 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.

8.1.4 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 .

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.

8.2 Downloading Videos

You can download videos stored on the server or the device. They can be saved in are in .avi, .mp4, or .asf formats. Three ways to download videos are:

- Download a portion of a video by selecting a duration on the timeline.
- Download videos by files. The system will generate files every 30 minutes from the time the video starts. If the video does not start on the hour or the half hour, the first file will start from the earliest start time to the half hour or the hour. For example, if a video starts from 4:15, the first file will be from 4:15 to 4:30.
- Download a period before and after a tag.

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Download Center**.

Step 2 Configure the search conditions, and then click **Search**.

Step 3 Download videos.

You need to verify your password by default before download. You can configure whether to verify the password. For details, see "7.3.1 Configuring Security Parameters".

- Download a video by selecting a duration on the timeline.
  Click the **Timeline** tab, and then select a period on the timeline.
  You can also click **Select All** on the upper-left corner, and then you can select and download the same period of all videos at the same time.
- Download a video by file.
  Click the **File** tab, and then click  of a file.
  You can also select multiple files, and then click **Download Selected File** on the upper-left corner to download them at the same time.
- Download a period of a video before and after a tag.
  Click the **Tag** tab, click  of the file you want to download.
  You can also select multiple tags, and then click **Download Selected Tagged File** to configure and download them at the same time.

Step 4 (Optional) Click  , select the format of the video, and then click **OK**.

- **Timeline**: You can further adjust the start and end time of the duration.
- **File**: If you download multiple files at the same time, you cannot configure the formats of the videos you want to save.
- **Tag**: You can configure how many seconds or minutes before and after the tag you want to download.

After download, you can click  to delete the tag.

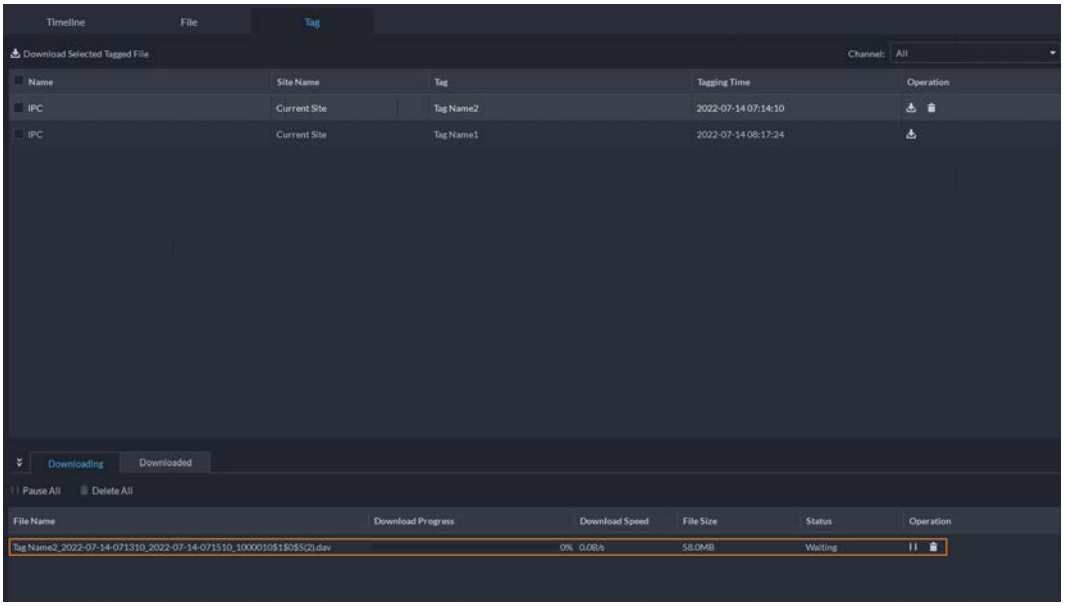
Step 5 When downloading clipped videos, in the **Download Recorded Video** dialogue box,

confirm the time span, and then, if necessary, click to select a video format. Click **OK**.

Related Operations

- You can pause, resume, and delete a download task.

Figure 8-1 Download progress



- After download completes, click to go to the path where the video is saved to, or click in the prompt on the upper-right corner to play the video directly in **Local Video**. For details, see "8.4 Playing Local Videos".

8.3 Configuring Local Settings

After logging in to the client for the first time, you need to configure the following fields under system parameters: Basic settings, video parameters, record playback, snapshot, recording, alarm, video wall, security settings and shortcut keys.

8.3.1 Configuring General Settings

Configure client language, client size, time, and more.

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **General**, and then configure the parameters.

Figure 8-2 General parameters

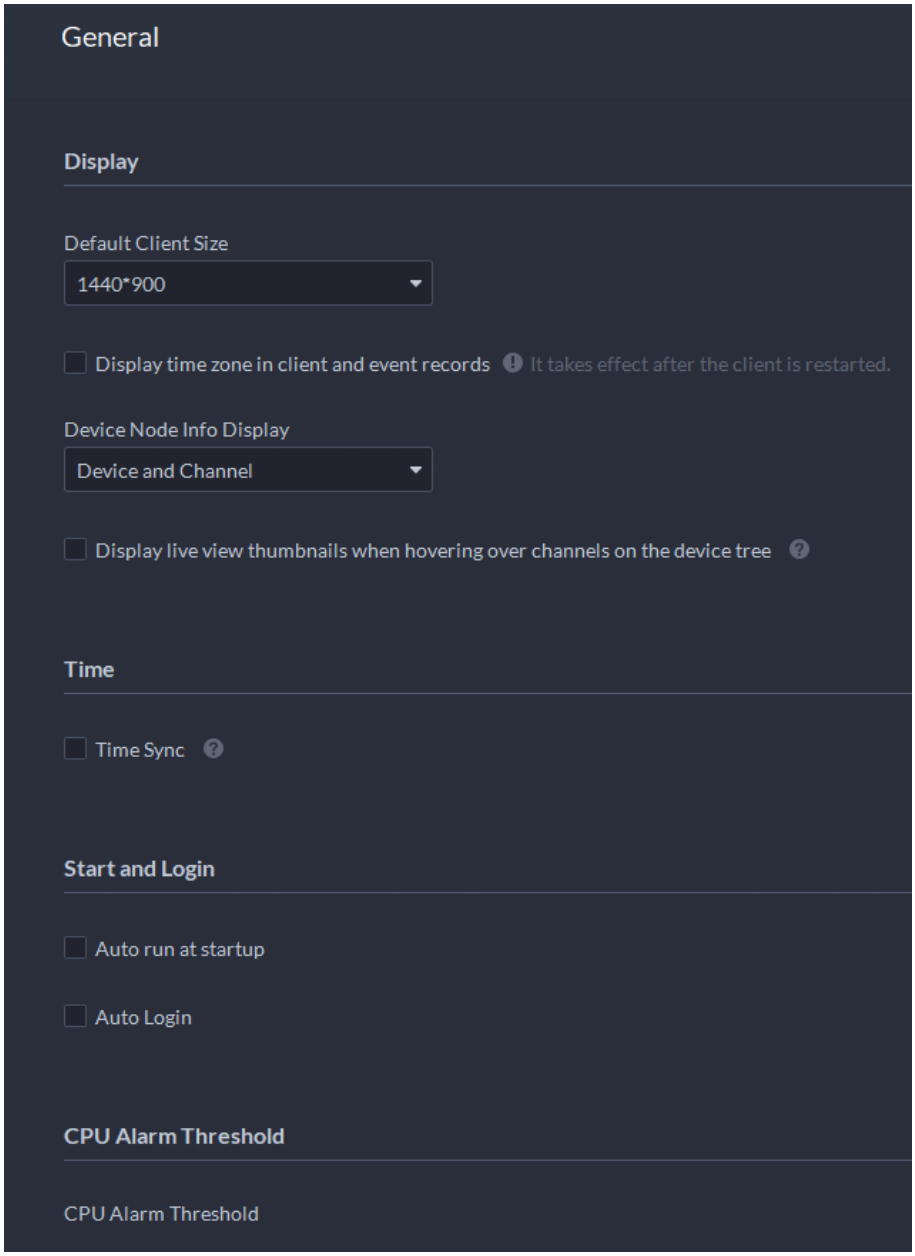


Table 8-1 Parameter description

Parameters	Description
Default Client Size	Select a proper resolution for the client according to PC display screen.
Display time zone in client and event records	When selected, the client and the time of alarms will show both the time and time zone.
Device Node Info Display	Select that the device tree displays devices and their channels or only channels.
Display live view thumbnails when hovering over channels on the device tree	When selected, you can hover the mouse over a channel in the device tree in **Monitoring Center** and a snapshot of its live video image will be displayed.

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**.

8.3.2 Configuring Video Settings

Configure window split, display mode, stream type and play mode of live view, and instant playback length.

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **Video**, and then configure the parameters.

Figure 8-3 Video parameters

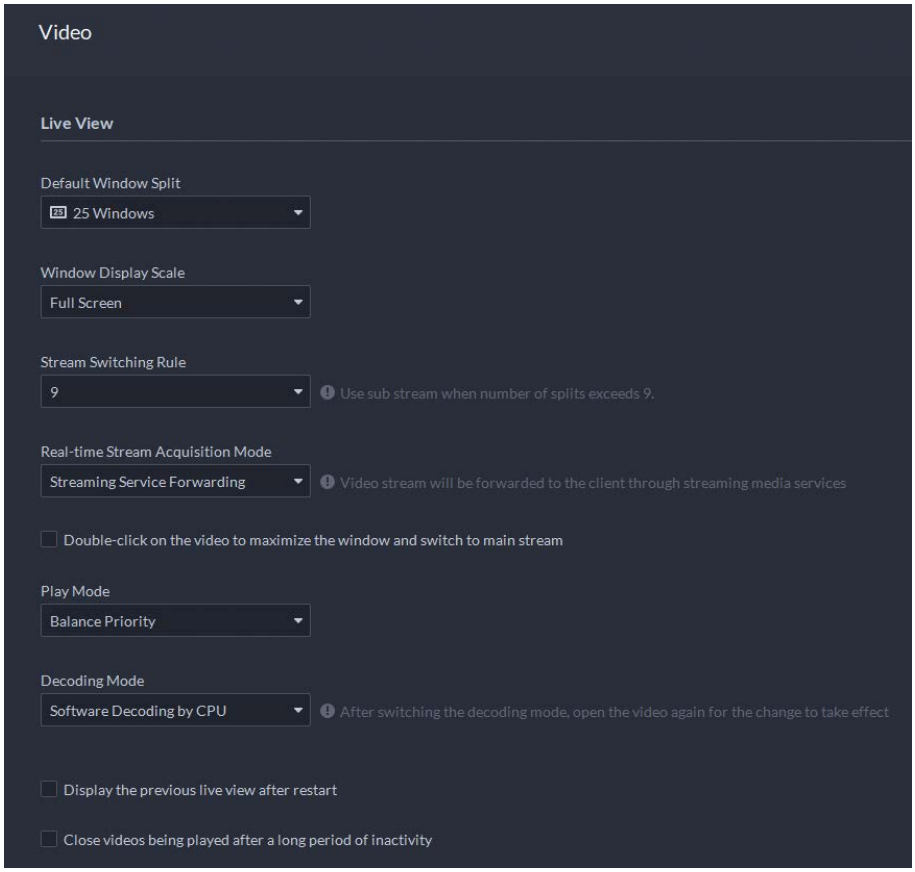


Table 8-2 Parameter description

Parameters	Description
Default Window Split	Set split mode of the video window.
Window Display Scale	Select from **Original Scale** and **Full Screen**.
Stream Switching Rule	When the number of window splits is greater than the defined value, the live video will switch from the main stream type to sub stream type.
Real-time Stream Acquisition Mode	Select the one according to your situation. If you select **Acquire directly from the device**, clients will acquire video streams directly from the channel. If direct acquisition fails, the platform will forward the video streams to clients. When the device and clients are properly connected to the network, direct acquisition can reduce the use of the platform's forwarding bandwidth. If too many clients are acquiring video streams from a channel, acquisition might fail due to insufficient performance of the device. Video streams will be forwarded to clients by the platform.
Double-click on the video to maximize the window and switch to main stream	If selected, you can double-click a video window to maximize it and switch from sub stream to main stream. Double-click again to restore the window size, and then the system will switch it back to sub stream.

Parameters	Description
Play Mode	• **Real-time Priority** The system might lower the image quality to avoid video lag. • **Fluency Priority** The system might lower the image quality and allow for lag to ensure video fluency. The higher the image quality, the lower the video fluency will be. • **Balance Priority** The system balances real-time priority and fluency priority according to the actual server and network performance. • **Custom** The system adjusts video buffering and lowers the impact on video quality caused by unstable network. The bigger the value, the more stable the video quality will be.
Decoding Mode CPU Threshold	• **Software Decoding by CPU**: All videos will be decoded by the CPU. When you are viewing live videos from large amount of channels, it will take up too much resources of the CPU that affects other functions. • **Software Decoding by GPU**: All videos will be decoded by the GPU. The GPU is better at concurrent operation than the CPU. This configuration will free up resources of the CPU significantly. • **Performance Mode (CPU First)**: All videos will be decoded by the CPU first. When the resources of the CPU is taken up to the defined threshold, the platform will use the GPU to decode videos.
Display previous live view after restart	If selected, the system displays the last live view automatically after you restart the client.
Close videos being played after long period of inactivity Inactivity Time	The system closes live view automatically after inactivity for a pre-defined period of time. Supports up to 30 minutes.
Instant Playback Time	Click on the live view 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**.

8.3.3 Configuring Video Wall Settings

Configure the default binding mode and stream type of video wall.

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **Video Wall**, and then configure the parameters.

Figure 8-4 Configure video wall settings

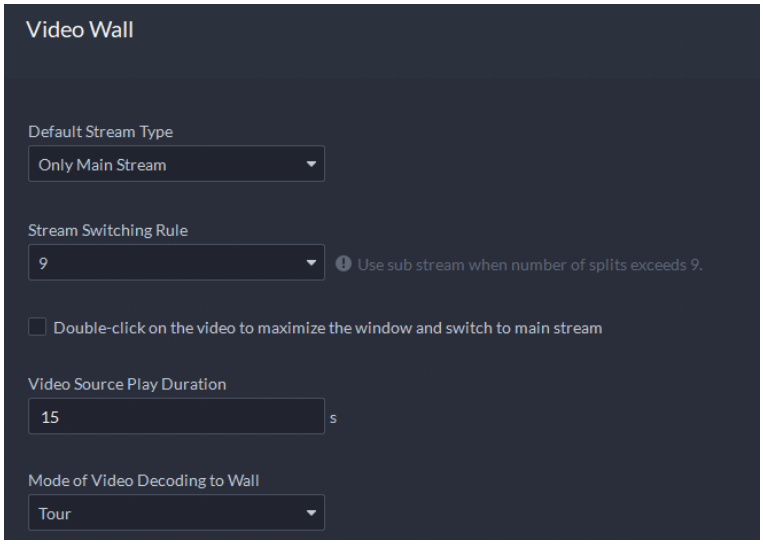


Table 8-3 Parameter description

Parameter	Description
Default Stream Type	Select **Main Stream**, **Sub Stream 1**, **Sub Stream 2** or **Local Signal** as the default stream type for video wall display.
Stream Switching Rule	When the number of window splits is greater than the defined value, the live video will switch from the main stream type to sub stream type.
Double-click on the video to maximize the window and switch to main stream	Double-click 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**.

8.3.4 Configuring Alarm Settings

Configure alarm sound and alarm display method on the client.

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **Alarm**, and then configure the parameters.

Figure 8-5 Configure alarm settings

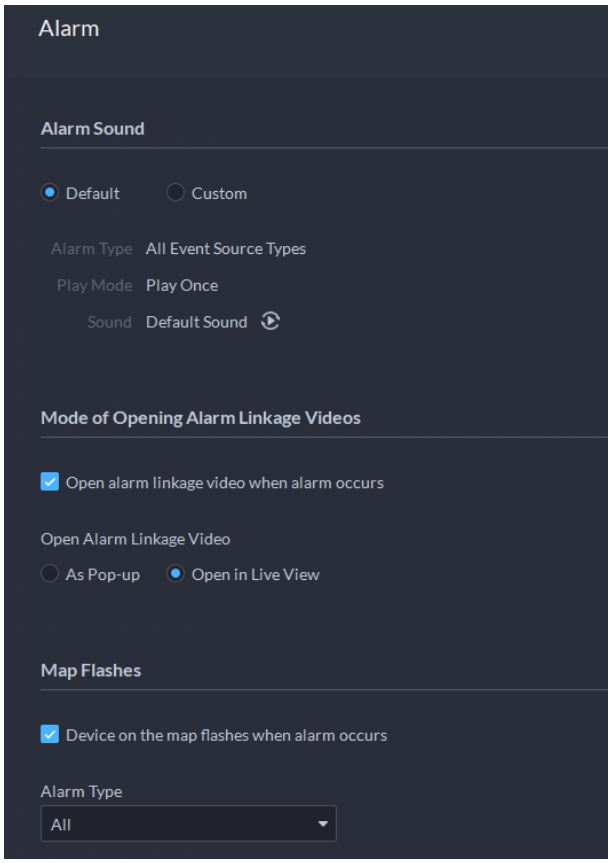


Table 8-4 Parameter description

Parameters	Description
Default	All types of alarms will use the same default alarm sound when triggered.
Custom	Click **Modify Alarm Sound**, and then you can change the alarm sound and its play mode of each type of alarm.

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 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 "4.1 Configuring Events".
Open Alarm Linkage Video	
Device on the map flashes when alarm occurs	Set one or more alarm types for alarm notification on the map. When an alarm occurs, the corresponding device will flash on the map.

Step 3 Click **Save**.

8.3.5 Configure File Storage Settings

Configure the storage path, naming rule, file size, and format of recordings and snapshots.

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **File Storage**, and then configure the parameters.

Figure 8-6 Configure file storage settings

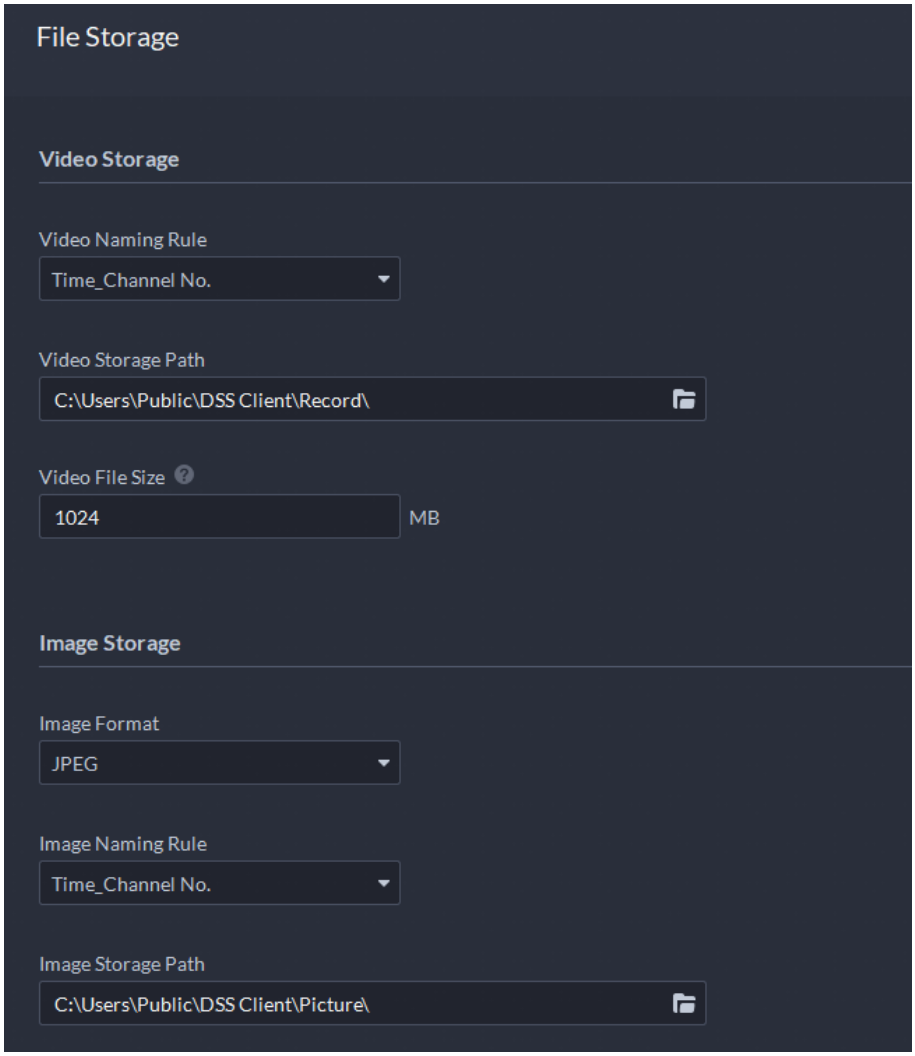


Table 8-5 Parameter description

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**.

8.3.6 Viewing Shortcut Keys

View shortcut keys for operating the client quickly.

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Settings**.

Step 2 Click **Shortcut Key** to view shortcut keys of the PC keyboard and USB joystick.

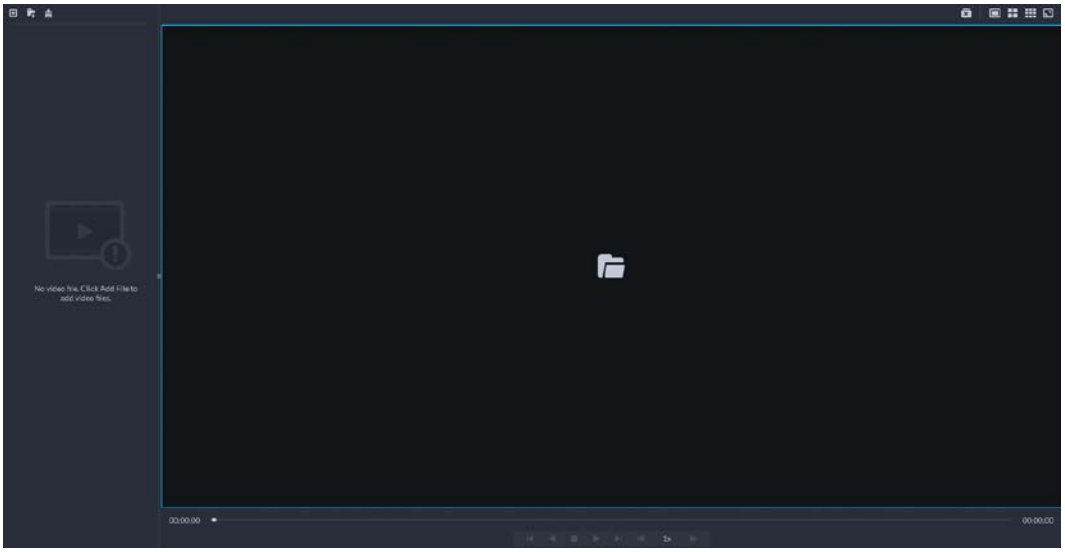
Figure 8-7 View shortcut keys

8.4 Playing Local Videos

You can play local videos directly on the platform.

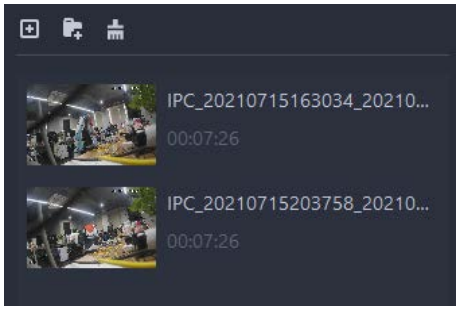
Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Local Video**.

Figure 8-8 Local video



Step 2 Click  to select one or more files, or  to open all files in a folder.

Figure 8-9 Play list



Step 3 Drag a file to the window on the right or right click it to play.

Related Operations

Table 8-6 Interface operation

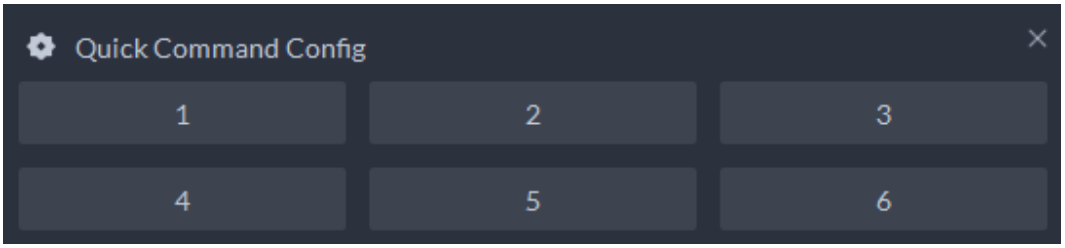
Icon/Function	Description
Right-click menu	• **Continuous Snapshot**: Take snapshots of the current image (three snapshots each time by default). The snapshots are saved to ..*DSS**DSS Client**Picture* by default. To change the snapshot saving path, see "8.3.5 Configure File Storage Settings". • **Video Adjustment**: Adjust the brightness, contrast, saturation, and chroma of the video for video enhancement. • **Digital Zoom**: Click it, and then double-click the video image to zoom in the image. Double-click the image again to exit zooming in.
	Close all playing videos.
	Split the window into multiple ones and play a video in full screen.
	Take a snapshot of the current image and save it locally. The path is C:\DSS\DSS Client\Picture\ by default.
	Close the window.
	Stop/pause the video.
1x	Fast/slow playback. Max. supports 64X or 1/64X.
/	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.

8.5 Quick Commands

Customize HTTP commands and execute them quickly. Request methods of GET, POST, PUT and DELETE are supported.

Step 1 Log in to the DSS Client. On the **Home** page, select **Management** > **Quick Commands**.

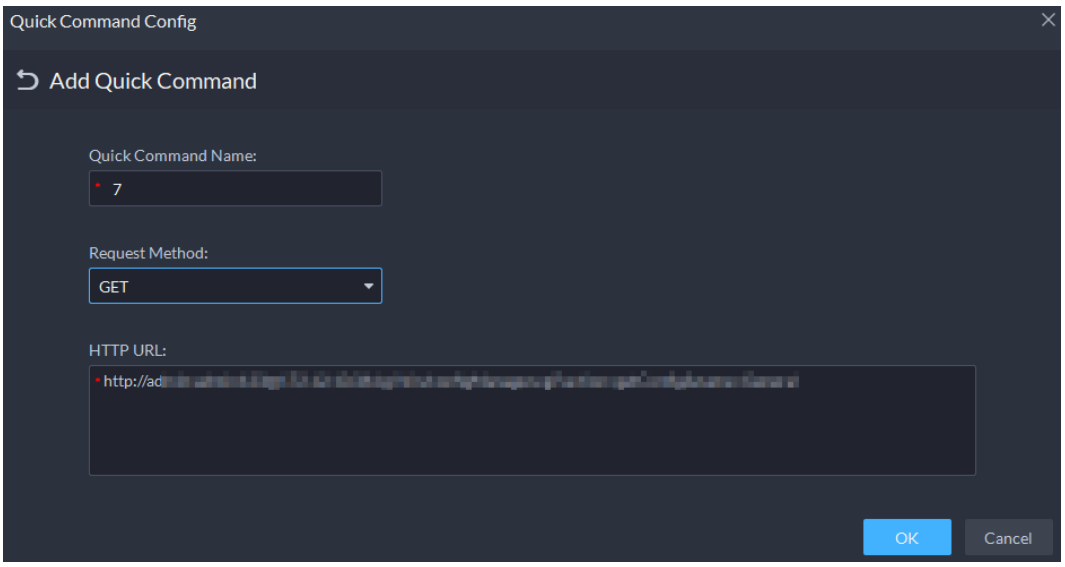
Figure 8-10 Quick commands



Step 2 Click .

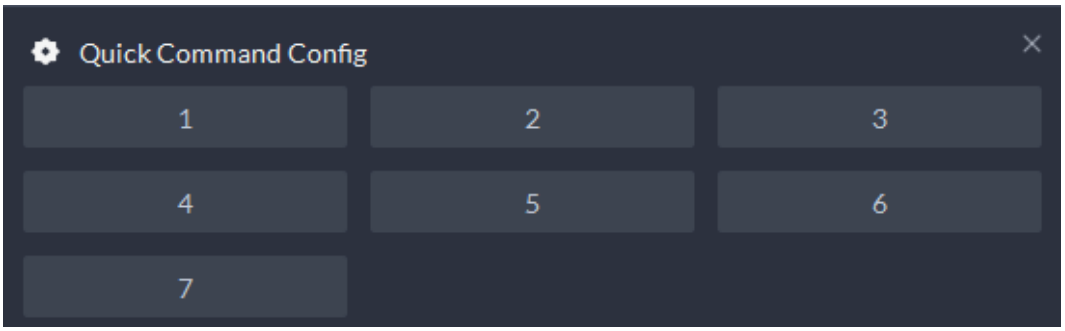
Step 3 Click **Add**.

Figure 8-11 Add a quick command



Step 4 Configure the parameters, and then click **OK**.

Figure 8-12 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

Appendix Table 1-1 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.
Configuration Service	CFGS	Manages disks, such as read-and-write operations.
Alarm Dispatch Service	ADS	Sends alarm information to different objects according to defined plans.
Media Transmission Service	MTS	Gets audio/video bit streams from front-end devices and then transfers the data to DSS, the client and decoders.
Media Gateway	MGW	Sends MTS address to decoders.
Storage Service	SS	Stores, searches for and plays back recordings.
Object Storage Service	OSS	Manages storage of face snapshots and intelligent alarm pictures.
Object Storage Service	SubOSS	Mainly manages storage evidence recordings and pictures.
Picture Transfer Service	PTS	Manages picture transmission.
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.
Device Management Service	DMS	Registers encoders, receives alarms, transfers alarms, and sends out the sync time command.
Auto Register Service	ARS	Listens, logs in, or gets bit streams to send to MTS.

Service Name		Function Description
ProxyList control Proxy Service	PCPS	Logs in to ONVIF device, and then gets the stream and transfers the data to MTS.
Access Control Service	ACDG	Manages access control and other related operations.
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.
Power Environment Server	PES	Manages access of dynamic environment monitoring devices.
Video Matrix Service	VMS	Logs in to the decoder and sends tasks to the decoder to output on the TV wall.
Video Intercom Switch Center	SC	Manages PC client and App client login as SIP client, and also forwards audio-talk streams.
Device Update Service	UPDATE	Updates devices.
Group Talk Service	POC	Manages the group talk functions and related 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

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188